Can NL trust 5G?

A conceptual model for cyber security supervision of 5G in the Netherlands

Master Thesis for the Executive Master Cyber Security

Cyber Security Academy

Farley Wazir

First Supervisor: prof. dr. J. van den Berg (Delft University of Technology & Leiden University)

Second Supervisor: prof. dr. S. Gijrath (Leiden University)

January 2019

Management Summary

In 2020 at least one major city in every Member State of the European Union will have to provide 5G connectivity. 5G is expected to present new opportunities in many sectors - the so-called “verticals” - such as education, manufacturing, processing, healthcare, media and entertainment, logistics, and energy and to deliver new functions to people and society bringing the likes of autonomous cars and intelligent transport, eHealth, augmented reality, virtual reality, and smart grids.

As 5G is about to seep through the pores of our connected society and there is much at stake, it is not strange that the EU and NL are busy drafting regulations regarding 5G.

The Dutch Cyber Security Council states that trust in, and the security and reliability of the digital infrastructure play an important role in market uptake and economic success and that it should not be taken for granted since cyber threats are constantly increasing while digital dependency (on technological applications) is growing.

The Inspectieraad[1] (Dutch Inspection Council) argues that in our fast-changing society citizens, companies and institutions have the need for an authoritative supervisor providing legal certainty and normative clarity. Accordingly, the role of 5G cyber security supervision is that it must see to it that the cyber security requirements demanded by law and regulations are met, and by doing so foster public confidence.

For society to put their trust in 5G telecommunications, the security of 5G in cyberspace is of the utmost importance. It concerns the security of every aspect of 5G ranging from software and hardware to data and privacy in all the different layers of cyberspace. From a governance perspective, it implies end-to-end security for the public at large.

In NL there are legally designated sectoral supervisory bodies such as national inspectorates and market regulators. As a consequence of this dispersed policy, cyber security supervision of 5G is not so straightforward and all stakeholders have the need for a clear approach.

The goal of this thesis is to deliver a proposal for cyber security supervision of 5G in the Netherlands. To achieve that goal, a design science approach has been employed. From a risk management perspective in the governance layer, it was analysed if the current arrangements for supervision in NL ensure the cyber security of 5G in cyberspace (i.e. end-to-end security of 5G) to foster public trust. For the limitations that surface, remedies are suggested.

In comparison to earlier generations of mobile telecommunications, 5G constitutes a paradigm shift because, not only is it required to perform significantly better on all key indicators like latency, data rates and energy usage, but with virtualization of network functions and decoupling of control and service layers, the focus is now on serving so-called verticals with tailor-made functions and different Quality of Service (QoS). Specifications for a full 5G System are expected by the end of 2019 and older generations like 4G are expected to play an important but supportive role.

The key technical requirements set for 5G by ITU-R in IMT-2020 will give rise to three kinds of usage scenarios (i.e. eMBB, URLLC and mMTC) based on a new trust model and employing advanced technologies (e.g. NR, NFV, SDN, MEC, mWT, massive MiMo and NS) in the designated frequency

[1] The Inspectieraad (Dutch Inspection Council) consists of the Inspectors-General and heads of the national inspectorates.

bands 700 MHz, 3,6 GHz and most likely 26 GHz. NL will auction spectrum for 5G in 2019 and 2020 after market analysis and European decision making.

With 5G the telecom business sector will see changes in its value chain due to novel business propositions by new stakeholders alongside those of the traditional stakeholders. It is expected that the realization of 5G potential will be a step-by-step process, with the first focus on improving the existing broadband propositions. The 5G use cases from the sorts of eMBB, URLLC and mMTC serve vertical sectors reaching far beyond the typical telecommunications domain.

With its vast amount of applications and services, the 5G threat landscape will span from end-user devices to the Radio Access Network (RAN), to the mobile core network and the Internet.
If 5G is to serve as a utility, or critical infrastructure itself, providing connectivity to other critical infrastructures and a range of other verticals the threat landscape of 5G will be unprecedented.
The 5G System is IP-based and it will therefore inherit most of the existing threats to 4G, and on top of those, it will have to cope with the security challenges in SDN, NFV, MEC, Cloud computing, and communication channels due to softwarization and virtualization.
The use cases of the eMBB, URLLC and mMTC usage scenarios for 5G require different cyber security levels and security challenges for confidentiality, integrity, authenticity and availability range from the misuse of personal data to APT.

A regulatory environment is composed of architecture, markets, social norms and legal aspects. The ITU, the IETF, 3GPP, IEEE, 5G-PPP have a decisive influence on the architecture of 5G. Market players united in NGMN Alliance, GSMA, and SIMalliance try to shape the resulting form of 5G from a business perspective. In the meanwhile social norms demand that everybody is ubiquitously connected, there is virtually no latency and telecommunication systems are “green”. The legal framework for the cyber security of 5G in NL is dominated by the EU Framework Directive (to be repealed by the EECC on 21 December 2020), the e-Privacy Directive and the NIS Directive since the addressees (i.e. electronic communications services providers, Essential Service Operators (ESOs) and Digital Service Providers (DSPs)) could be directly involved in the provisioning of 5G telecommunications, and by the GDPR because of its horizontal obligations. These instruments are transposed into the NL laws Tw, Wbni and UAVG and adjusted to national preferences. The main risks identified in these laws are damage to the security of networks, information systems, services, personal data and privacy. Wbni also identifies risks to the continuity of vital providers and appoints telecommunications networks part of vital national Infrastructure in NL. The legal provisions aim in the first place at prevention and mitigation of security breaches, appropriate technical and organizational measures relevant to the risk and a notification to a supervisory authority of a breach of security that is likely to cause significant harm. In cyber security supervision of 5G with a risk-driven approach, these provisions can be used as basic preventive and corrective controls.

The Tw appoints the authorities AT, AP and ACM to play a role in supervision. AT is the designated supervisory body for among more the use of frequency space, equipment or requirements regarding radio equipment, authorized tapping, and the continuity of public electronic communication networks and public electronic communication services. AP is charged with supervising compliance regarding the notification of personal data breaches. ACM with regards to market regulating aspects of the Tw, roaming provisions, net neutrality requirements (i.a. user experienced data rates) and the protection of privacy in electronic communications (e.g. against spam and cookies).
The Wbni appoints national supervisory authorities for DSPs (i.e. cloud computing services, online marketplaces, online search engines) and for ESOs. The most relevant to 5G cyber security is AT. The

CSIRT for ESOs is delegated to the NCSC, and the role of CSIRT for DSPs is assigned to the Ministry of Economic Affairs and Climate Policy. The UAVG designates AP as supervisory body.

In classical supervision there is a norm regulatees abide by, information collection, and monitoring of compliance, and intervention by a supervisory body. While good supervision stays within legislative mandate and intent, follows due process, reflects expertise and is efficient.

Based on statements from the Ministry of the Interior and Kingdom Relations, the WRR, the Dutch Cabinet and the Inspectieraad (Dutch Inspection Council) it can be concluded that the objective of good NL 5G cyber security supervision (i.e. efficient, stays within legislative mandate and intent, follows due process, and reflects expertise) would be to ensure the trustworthiness of 5G to its users and the public at large by applying (a) a risk-driven approach (b) in a cooperation of supervisory bodies to (c) collect information and monitor compliance with (d) the norms for cyber security, and (e) intervene in case of non-compliance.

Analyzing this objective against the regulatory environment and provisions, the limitations were identified and subsequently the following requirements for an improved model for 5G cyber security supervision have been derived:

(a) Deploying a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors;

(b) Cooperation between relevant NL 5G supervisory bodies, between NL and European[2] 5G supervisory bodies (and ENISA), and between NL and non-European[3] supervisory bodies;

(c) Collection of information by sector-specific supervisory bodies to address the dissemination of providers and subcontractors, relevant information dispersed to supervisory bodies (and stakeholders) to create cyber situational awareness, and monitoring of compliance coordinated between collaborative 5G supervisory bodies by AT to gain overview;

(d) Supervisory bodies to fill in the open norms on 5G cyber security with their sector and harmonize them across the supervisory bodies (see also (b));

(e) Intervening by the supervisory bodies based on the identified controls in legislation and supplementary supervisory controls developed in close cooperation with all involved supervisory bodies with consideration of adjacent sectors.

The first identified requirement for an improved conceptual model for 5G cyber security supervision is (a) the deployment of a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors.

The provisioning of 5G is modelled, according to the conceptualized cyberspace model, in the 5G Use Case Layer, the 5G Provisioning Layer, the 5G Building Blocks Layer and the 5G Supervision Layer.

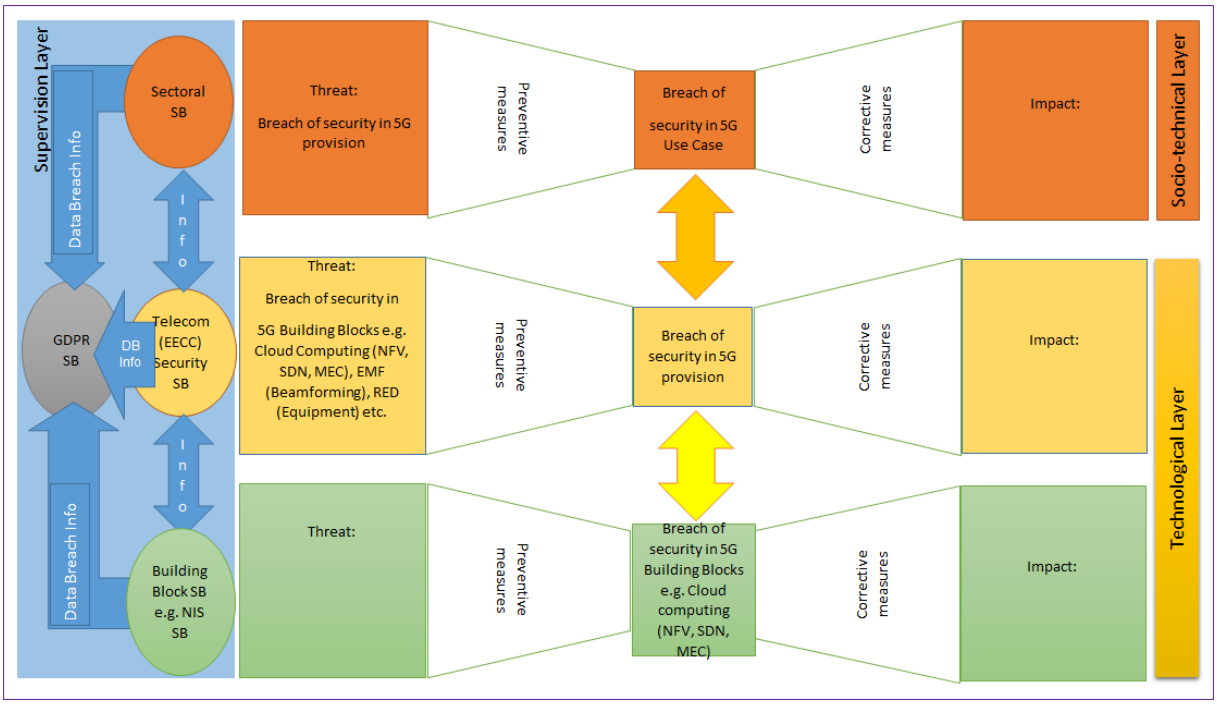
The steps of the risk management cycle are performed to identify, assess and analyse risks related to the compromise of an end to end multi-stakeholder 5G System.
The estimates for likelihood and consequence of a breach of trust in the security of the 5G System consequently result in a high risk level.

[2] Recital 98 and Art. 40(1) of the EECC and Recital 4 of the NIS Directive mention the cooperation between European supervisory bodies and ENISA in this regard.
[3] Non-European cooperation, based on Art. 218 TFEU, is mentioned in Art. 13 of the NIS Directive.

A triple Bow Tie is constructed depicting the critical event in each layer and cascade effects. Controls are proposed for the designated supervisory body within a suitable risk treatment strategy from a governance perspective.

The remaining requirements (b), (c), (d) and (e) imply intensive interaction between the supervisory bodies in the governance layer of 5G cyberspace. These requirements together with requirement (a) are incorporated in a conceptual model for cyber security supervision of 5G in NL.

The conceptual Triple Bow Tie Supervision model for 5G cyber security in NL incorporates a risk-driven approach to supervision in the 5G Building Blocks Layer, the 5G Provision Layer and the 5G Use Case layer and cooperation between relevant supervisory bodies to share information (e.g. on norms, threats, risk assessments, cascading effects, interventions) and create cyber situational awareness in order to better ensure that NL can trust 5G.



The Triple Bow Tie 5G Cyber Security Supervision model.

Contents

1. Introduction

On the 5G Cyber Security Governance Challenge

Mobile telecommunications are an essential part of modern daily life. From the outset, it has brought the world mobility while sharing information and the next generation of mobile telecommunications, commonly referred to as 5G, promises even more benefits.

5G is expected to present new opportunities in sectors - the so-called "verticals"- such as education, manufacturing, processing, healthcare, media and entertainment, logistics, and energy and deliver new functions to people and society bringing the likes of autonomous cars and intelligent transport, eHealth, augmented reality, virtual reality, and smart grids [1]. Table 1.1 presents some examples of new functions, enablers, and 5G requirements for some verticals [2].

Verticals	Functions	Enablers	5G Requirements
Education	Remote delivery Immersive experiences	Video streaming Augmented Reality/ Virtual Reality	Large bandwidth Low latency[4]
Manufacturing	Industrial automation	Massive IoT[5] networks [3]	High connection density Ultra-reliability Low power consumption
Healthcare	Remote diagnosis and intervention Long-term monitoring	Video streaming Augmented Reality/ Virtual Reality Embedded devices, advanced robotics	Low power High throughput Low latency
Energy / Agriculture	Smart Grid Intelligent demand/ supply control Smart Farming and Precision Agriculture	IoT networks	High reliability Broad coverage of network Low latency
Entertainment	Immersive gaming and media industry Multimedia experience at 4k, 8K resolution	Video streaming Augmented Reality/ Virtual Reality	Large bandwidth Low latency
Automotive / Autonomous Cars	Collision avoidance Intelligent navigation and transportation systems	Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Intelligent Transport Systems (ITS)	Large bandwidth and low latencies (< 5 ms) and high connection reliability (99.999%)
Smart Cities	Connected utilities, Transportation, Healthcare, Education and all amenities	Massive IoT networks Automation Cloud Infrastructure Artificial Intelligence	Large bandwidth High throughput High connection density Low latencies

Table 1.1 An example of new functions, enablers, and 5G requirements for some sectors [2].

[4] Latency is the time from when the source sends a packet to when the destination receives it.
[5] The collection of devices (or "things") - embedded with electronics, software, sensors, and unique addresses – able to interact through network connectivity.

The European Commission[6] has called upon every Member State of the European Union[7] (EU) to provide 5G connectivity in at least one major city in 2020, and have uninterrupted 5G coverage in all urban areas and major terrestrial transport paths by 2025 [4], [5]. It invested 700 million euro in a Public-Private-Partnership (i.e. 5G-PPP) in 2013 with the aim of making sure that 5G is available in Europe by 2020 [4]. The EU will and has already set regulation in place to create a fertile environment for 5G deployment (e.g. Art. 56[8] of the recently published European Electronic Communications Code (EECC)[9] [6]).

Lemstra [7] argues that "*the main raison d'être for the European Union is the creation of union-wide markets that increase the economies of scale*…" to counter the dominance, due to "natural" advantage, of firms in large countries like the USA (and now China) over those in European countries. Consequently, the aim of the EU is to harmonize industrial policies, technological developments, and economic and social progress with instruments such as regulations, directives and guidelines. Furthermore, Lemstra states that since telecommunications are important for the development of society as a whole and the economy in particular, it has become fundamental to EU policy-making and implementation, and subsequently explains the interest of EU politicians in the success of 5G [7].

The Netherlands (NL) has launched a *Digitization Strategy* [8] and an *Action Plan Digital Connectivity* [9] in response to this call from the EU and in an effort to keep its leading role as one of the most advanced digital economies [10] in the EU.

As 5G is about to seep through the pores of our connected society and there is much at stake, it is not strange that governments are busy drafting regulations regarding it. More specifically, and to avoid being at the mercy of any (commercially motivated) whims of suppliers in this regard [11], regulations concerning the cyber security of 5G and the supervision thereof are put in place (e.g. with the recent EECC [6]).

The Dutch Cyber Security Council states in its *Recommendation regarding the Dutch National Cybersecurity Agenda 2018* [12] that trust in, and the security and reliability of the digital infrastructure play an important role in market uptake and economic success and that it should not be taken for granted since, according to the *Dutch National Cybersecurity Agenda 2018* [13], cyber threats are constantly increasing while digital dependency (on technological applications) is growing.

The Inspectieraad[10] (Dutch Inspection Council) states that in our fast-changing society citizens, companies and institutions have the need for an authoritative supervisor providing legal certainty and normative clarity [14]. Accordingly, the role of 5G cyber security supervision is that it must see to it that the cyber security requirements demanded by law and regulations are met, and by doing so foster public confidence [15].

---

[6] The European Commission is the politically independent executive arm of the European Union (EU), with the responsibility of drawing up proposals for new European legislation, and implementing the decisions of the European Parliament and the Council of the EU [16].

[7] The EU is an international organization founded in 1993 with the aim of extending the economic cooperation established under the European Economic Community (founded in 1957). It has 27 Member States among which NL.

[8] "Competent authorities shall not unduly restrict the deployment of small-area wireless access points."

[9] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast).

[10] The Inspectieraad (Dutch Inspection Council) consists of the Inspectors-General and heads of the national inspectorates.

In 1G to 4G mobile telecommunications, with a subscriber (and their terminal) and two network operators (home and serving), who trusts whom to do what was implicitly built-in and reasonably straightforward [16]. With 5G come multiple (virtual) network operators and many more stakeholders in software-defined and virtualized networks [17] with novel use cases [18], which create an enlarged threat landscape and greater security concerns for NL [13], the EU [19] and consequently global society as a whole.

The proliferation of 5G can be modelled in a conceptualized cyberspace, in accordance with Van den Berg et al. [20], which consists of the basic technology layer based on the TCP/IP protocol stack[11], a socio-technical layer enabling the (cyber) activities, and the governance layer in which governance of both the technical layer and the socio-technical layer take place. This cyberspace is divided into several cyber sub-domains like the manufacturing sector, the processing sector, the logistics sector and so on. Figure 1.1 presents an illustration of this conceptualized cyberspace [20].

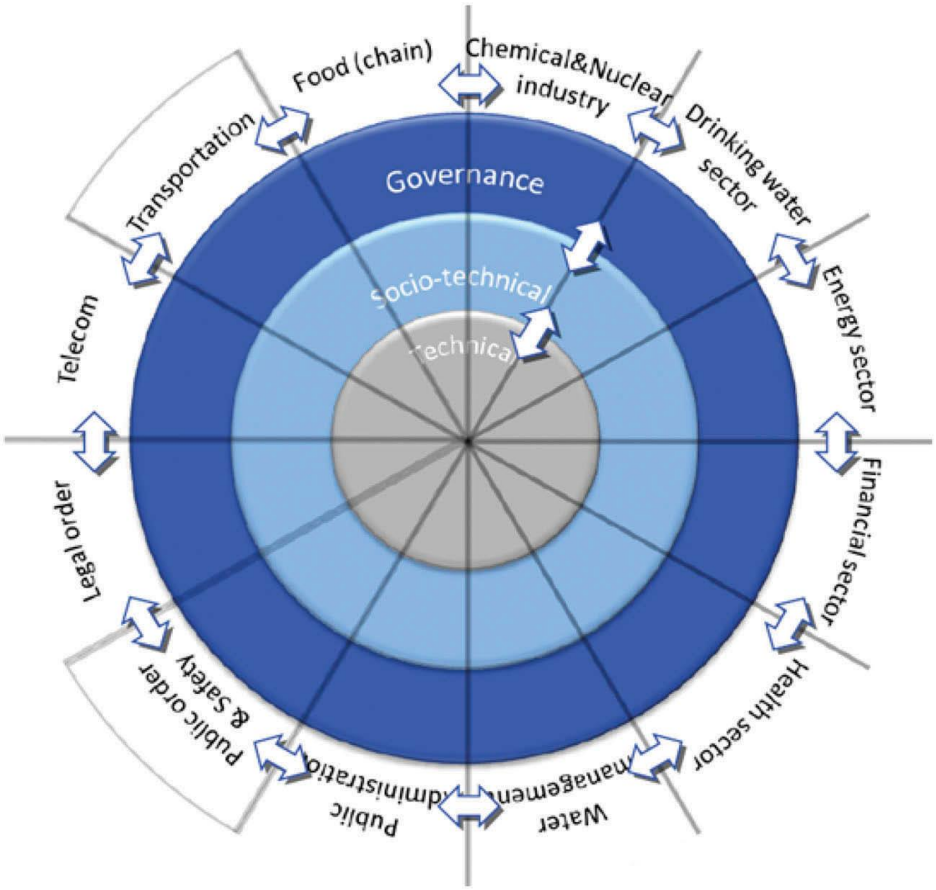


Figure 1.1 The conceptualization of cyberspace [20].

[11] Although 5G might instead be enriched with the Next Generation Protocol (NGP), a proposed successor of TCP/IP [22].

For society to put its trust[12] in 5G telecommunications [21], the security of 5G in cyberspace (i.e. the cyber security of 5G) [20] is of the utmost importance. Cyber security of 5G concerns the security of all aspects of 5G ranging from the purely technical (i.e. regarding the typical information security canons confidentiality, integrity, authenticity) to the socio-technical (i.e. regarding the security of cyber activities) in cyberspace. From a governance perspective, it implies end-to-end security of 5G for its users and the public at large.

In NL there are legally designated sectoral supervisory bodies such as national inspectorates and market regulators [22]. As a consequence of this dispersed policy, cyber security supervision of 5G, as in end-to-end security for the public from a governance perspective, is not so straightforward and all stakeholders have the need for a clear approach.

Scope

The focus is on the cyber security supervision of 5G telecommunications as 5G becomes available to the public in NL. It is assumed that any other barrier to market take-up of 5G will be resolved (eventually).

Research Goal

This thesis examines the governance challenges that NL faces with regards to the cyber security of 5G. The goal is a proposal for integral[13] cyber security supervision of 5G in NL. From a risk management [23] perspective in the governance layer [20], it is analysed if the arrangements for supervision in NL ensure the cyber security of 5G in cyberspace (i.e. end-to-end security of 5G) to foster public trust. For the limitations that surface, remedies are suggested.

Research Methodology

To achieve that goal the design science approach is employed [24], which reflects in the four parts of the thesis.

Part 1: Understand what 5G is;
Part 2: Understand the cyber security challenges of 5G;
Part 3: Determine requirements for the design of an improved supervision model;
Part 4: Design the supervision model and communicate.

Research Approach

Research is conducted in literature and publicly available papers regarding the concepts of 5G, the cyber security challenges of 5G, the regulatory environment for 5G in NL and the arrangements of (integral) cyber security supervision in NL.

The technological features of 5G, the goals that NL has set following the aims of the European Commission, the all-embracing impact of 5G on society, the corresponding potential cyber security issues and the importance of trust for 5G to flourish have been explored.

[12] Trust in a system is a belief in users that the system will behave and provide benefits to them as expected and that the system will not harm them or allow them to be harmed. Trustworthiness is, literally, the property of being worthy of trust, i.e. a system is trustworthy if one can be sure it will not breach the trust placed in it (according to 5G-ENSURE, the security working group of 5G-PPP) [21].
[13] Integral in the sense of a combined use of existing governmental supervision to achieve end-to-end security of 5G.

The European and Dutch law are examined for legal requirements referring to cyber security of 5G. Integral cyber security supervision of 5G is defined as an activity, to secure trust in the end to end security of 5G, from within the governance layer covering the technology and socio-technical layers of cyberspace conform Van den Berg et al [20].

Research has been conducted into Dutch law for supervisory bodies that have legal and subject matter jurisdiction for cyber security supervision of 5G in NL. Their competence is highlighted from a governance perspective.

The approach that the identified supervisory bodies take for cyber security supervision of 5G in NL is examined from a risk management perspective. The limitations are identified and improvements suggested.

Having followed the first two steps[14] in a conceptualization process conform Kefalas [25], finally a conceptual model is proposed to address the identified challenges, taking into account all relevant supervisory bodies, to arrive at integral cyber security supervision, so NL can trust 5G.

Structure of the thesis

The remainder of this thesis consists of four parts. The first part sets the scene; what is 5G? It consists of four chapters; background and historical development of 5G, its definition, and the roadmap ahead is described, key technological features are presented, business impact of 5G and sectoral use cases highlighted. The second part of the thesis elaborates on the cyber security challenges for 5G in the system architecture, in sectoral use cases and for public order services and critical infrastructure. Part three concerns the regulatory environment for 5G on a global, European and Dutch level: the influence from architecture, markets, social norms and regulations. Also, the supervisory authorities are highlighted. The fourth and final part examines what cyber security supervision is, what the objectives (regulatory goals) are and models a proposal for cyber security supervision of 5G in NL. Figure 1.2 presents a schematic overview of the structure of this thesis with the parts and chapters.

[14] The three steps in a conceptualization process are: (1) identification and definition of the main concepts, (2) identification and definition of the main relationships that tie these concepts together, and (3) statement of propositions regarding the most likely states of these relationships at certain times [27].

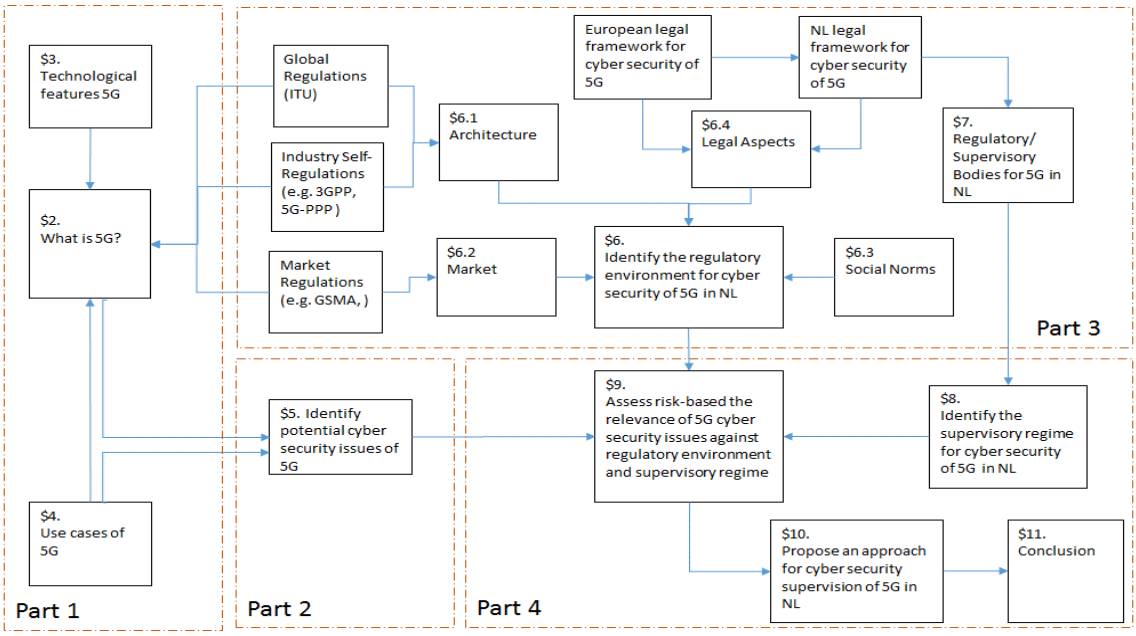


Figure 1.2 A schematic overview of the structure of this thesis with the parts and chapters

Part 1. What is 5G?

2. Background and context of 5G

This chapter investigates the background and context of 5G by highlighting the historical development, presenting a description of 5G and providing insight into the roadmap for deployment. It is recognized that 5G constitutes a paradigm shift compared to earlier generations of mobile telecommunications.

2.1 Historical development of 5G

Each transition to a new generation of mobile telecommunications was driven by the arrival of new capabilities. A short summary is presented on the evolution of cellular networks based upon *Shahabuddin et al* [26].

First generation mobile telecommunications (1G)
In the early eighties the first generation of commercial cellular network systems, the Advanced Mobile Phone Service (AMPS) and its alternative Total Access Communication Systems (TACS), supporting international roaming and automatic handover, were implemented based on analog modulation and Frequency Division Multiple Access (FDMA) to provide voice services.

Second generation mobile telecommunications (2G)
Overall system performance improved with a shift from analog to digital modulation, implementing time division, digital speech codecs for compression and decompression, and Code Division Multiple Access (CDMA) to enable more users on the same channel. Furthermore, Short Messaging Service (SMS) was introduced as a feature.

The "Groupe Spéciale Mobile" (GSM) of the Conference Des Administrations Europeans Des Posts et Telecommunications (CEPT) developed specifications for a standardized European mobile communications network system targeting spectrum efficiency, low terminal costs, international roaming, better voice quality and compatibility with other systems (e.g. Integrated Services Digital Networks (ISDN)) and support of new services. In 1990 the European Telecommunications Standards Institute (ETSI) released the first version of the GSM standard. It was subsequently implemented by global operators and the standard was renamed "Global System for Mobile Communications".

With the introduction of packet data services and the Wireless Access Protocol (WAP) to deliver internet content, 2G evolved to 2.5G.
ETSI introduced the standard for GSM Packet Radio Systems (GPRS) in the nineties enabling higher data rates. In 1997 ETSI published the Enhanced Data rates for GSM Evolution (EDGE) standard increasing the data rate even further.

*Third generation mobile telecommunications (*3G)
The GSM network architecture formed the basis of the next generation system. The International Telecommunications Union[15] (ITU) requested proposals for 3G early 1990s, known as IMT-2000 [27], aiming for global harmonization and interoperability of mobile telecommunications. Requirements were set to provide higher data rates, better Quality of Service (QoS) for voice telephony and

[15] ITU was founded in Paris in 1865 as the International Telegraph Union. It took its present name in 1934, and in 1947 became a specialized agency of the United Nations. ITU currently has a membership of 193 countries and almost 800 private-sector entities and academic institutions.

advanced features from interactive gaming to internet browsing, e-mailing, and streaming multimedia applications.

*Fourth generation mobile telecommunications (*4G)
ITU defined the requirements of 4G systems, the current generation of mobile telecommunication, in IMT-Advanced [28]. It requires data rates of 100 Mbps up to 1Gbps, global roaming, compatibility with fixed, International Mobile Telecommunications (IMT) and other Radio Access Networks (RAN), high-quality mobile devices and cost efficiency.

Table 2.1 presents an overview of generations of mobile telecommunications to date including the acronyms for deployed technologies.

Generation	Year	Network	Technology	Throughput	Data
1G	Early 1980s	Circuit switched	TACS, AMPS	14.4 Kbps (peak)	Analog Voice
2G	Early 1990s	Circuit or Packet Switched	D-AMPS, GSM, CDMA	9.6/14.4 Kbps	Digital Voice + Data
2.5G	1996	Circuit or Packet switched	GPRS, EDGE, EVDO, EVDV	171.2 Kbps (peak) 20-40 Kbps	Digital Voice + Data + Multi-Media Service
3G	2000	Packet or Circuit switched	WCDMA, CDMA2000, UMTS	3.1 Mbps (peak) 500-700 Kbps	Digital Voice + High-speed Data + Video streaming
3.5G	2006	Packet switched	HSPA	14.4 Mbps (peak) 1-3 Mbps	Digital Voice + High-speed Data + High Definition Video streaming
4G	2012	All IP based, Packet switched core network.	WiMax, LTE, Wi-Fi	100-300 Mbps (peak) 3-5 Mbps 100 Mbps (Wi-Fi)	Digital Voice + High-speed Data + High Definition Multimedia + End to end Security

Table 2.1 Generations of mobile telecommunications and deployed technology [29], [30], [31], [32].

It is important to note that due to the evolutionary development of mobile telecommunication all the generations from 2G onwards are still in use (as fall back for the latest generation).

2.2 Description of 5G

The fifth generation of wireless mobile telecommunications networks is commonly referred to by the term 5G. The Next Generation Mobile Network (NGMN) Alliance, an association of more than 80 partners from the mobile telecommunications industry and research, defines 5G as *"an end-to-end ecosystem to enable a fully mobile and connected society. It empowers value creation towards customers and partners, through existing and emerging use cases delivered with consistent experiences, and enabled by sustainable business models"* [1].

Expected to build on the legacy of his predecessors, 5G is required to handle a hundred times higher data rates, a hundred times higher traffic density, greater reliability[16], a factor of fifty lower latency, connectivity for hundred times more devices per area and a hundred times lower energy usage in support of for example the Internet-of-Things (IoT) [33], [34].

Although some of these capacities can be considered evolutionary, the focus in 5G is now on serving so-called vertical markets with tailor-made functions and different QoS, based on virtualization of networks and network functions, and the use of application program interfaces (APIs) [1], [17].

5G-PPP[17] has presented a concept of the integrated architecture as foreseen for 5G in their white paper *5G empowering vertical industries* [35] consisting of the following layers (see Figure 2.1):

The basic layer is the infrastructure layer consisting of a) large-scale heterogeneous access systems (e.g. cellular, fixed, satellite) and (high-capacity) transport networks; b) massively distributed cloud computing and storage centres with various capacities (e.g. ultra-low latency); c) all connected devices (e.g. smartphones, sensors, robots, drones).

The Network Function Layer offers virtual 5G network functionality (through SDN and NFV), independent of its kind (e.g. network, computational, storage) or implied resource (e.g. optical, wireless, satellite, cloud), as service to the user. The key element in this layer is the management and orchestration mechanism required to assemble virtual resources running network functions and making them available to the upper layer.

The Multi-service Control Layer, as the intermediary between the network-focused service layers and the verticals-focused service layers, enables the creation, operation, and control of multiple dedicated communication networks running on top of a common infrastructure. These networks each have functionality and capabilities for mapping business service requirements to network service topology and address the requirements defined by the network tenant. Since administrative domains will considerably increase because of fragmentation, tenant isolation management and shared function control are important to guarantee isolation and QoS in multi-tenancy support.

The Business Function Layer has function repositories with sets of typical vertical sector application related functions (e.g. related to sensors, positioning, distance measurement) and application independent functions (e.g. logging). These functions are defined in an abstract and implementation independent manner with rules for their invoking, operating and results. Because the functions are

[16] Reliability is the capability of transmitting a given amount of traffic in a fixed time duration with high success probability.

[17] 5G-PPP is the public private partnership initiative for 5G between the European Commission and the European industry aiming to secure Europe's leadership in the areas where Europe is strong or where there is potential for creating new markets e.g. smart cities, e-health, intelligent transport, education or entertainment & media [38].

used by networked resources they define the QoS of the underlying communications (e.g. latency, availability, security).

The Business Service layer defines the business processes of the verticals like media and entertainment, manufacturing and autonomous driving. These processes consist of a combination of vertical-specific activities which in turn, are carried out by combining functions provided by the Business Function Layer. Each activity has specific application-related constraints (e.g. security and safety requirements, energy consumption, quality requirements) setting the QoS requirements for the underlying layers.

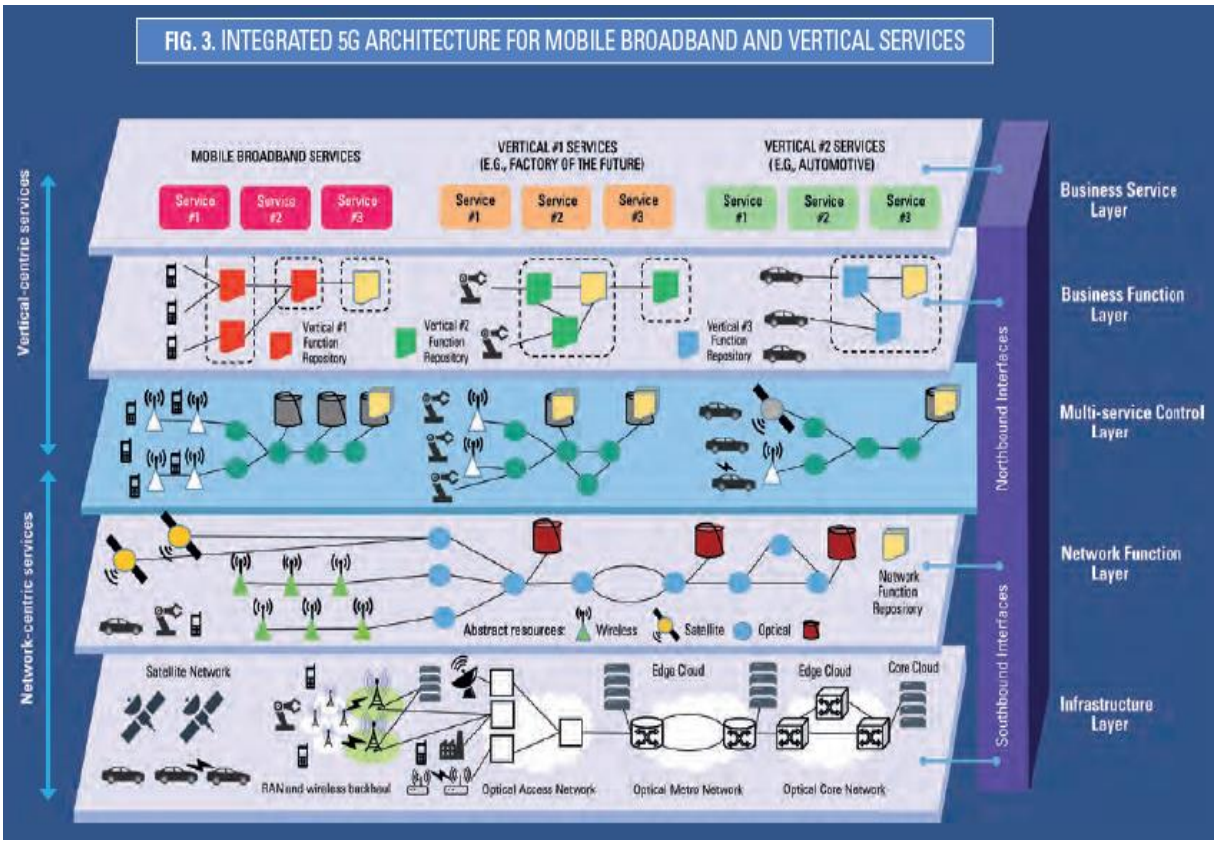


Figure 2.1 An overview of the integrated 5G architecture for mobile broadband and vertical services [35].

Note that the 5G-PPP architecture model (see Figure 2.1) subdivides the technical layer from Van den Berg et al. [20] into multiple layers and contains some aspects of a socio-technical layer in the Business Service Layer.

2.3 Definitions for 5G

In this thesis the following definitions with regards to 5G, as introduced by the NGMN Alliance [1], are used.

RAT: Radio Access Technology.

5G RAT (5GR): A component radio interface of the 5G RAT family.

5G RAT Family (5GRF): The set of one or more standardized 5GRs that, as a part of the entire 5G system, together support NGMN 5G requirements. The 5GRF should provide wide coverage, as this is a critical factor for marketing new technology.

5G Network Function (5GF): Provides a particular capability to support communication through a 5G network. 5GFs are typically virtualized, but some functions may be provided by the 5G infrastructure using more specialized hardware. The 5GFs comprise RAT-specific functions and access-agnostic functions, including functions to support fixed access. The 5GFs can be classified into mandatory and optional functions. Mandatory functions are common functions necessary for all use case categories, e.g. authentication and identity management. Optional functions are the functions that are not always applicable for all the use cases and may also have different variants tailored to the traffic type and use case.

5G Infrastructure (5GI): The hardware and software basis for the 5G network, including transport networks, computing resources, storage, Radio Frequency (RF) units and cables supporting the network functions providing the 5G network capabilities. 5GRs and 5GFs are implemented or realized using the 5GI.

5G End-to-end Management and Orchestration Entity (5GMOE): Creates and manages the 5G slices. It translates use cases and business models into concrete services and 5G slices, determines the relevant 5GFs, 5GRs and performance configurations, and maps them onto the 5GI. It also manages to scale the capacity of individual 5GFs and their geographic distribution.

5G Network (5GN): The 5GFs, 5GRs, the associated 5GI (including any relaying devices) and the 5GMOE supporting communication to and from 5G devices. In other words, a 5GN is realized when a 5GR utilizes any subset of functions from the 5GFs implemented on the 5GI to support communications with a 5G device. On the contrary, the network created when the 5GFs are used to support communications with a 5G device through a non-5GR is not considered a 5GN.

5G Device (5GD): The equipment used to connect to a 5GN to obtain a communication service. 5GD can support machines as well as human users.

5G System (5GSYS): A communications system comprising a 5GN and 5GDs.

5G Slice (5GSL): A set of 5GFs and associated device functions set up within the 5GSYS that is tailored to support the communication service to a particular type of user or service.

2.4 Roadmap for 5G deployment

In 2012 ITU-R, the Radiocommunications sector of the ITU, launched the programme “International Mobile Telecommunication for 2020 and beyond” (IMT-2020) [36] setting the requirements for 5G. The Third Generation Partnership Project[18] (3GPP), founded in 1998 and also involved in the development of technical specifications and standards[19] for 3G and 4G, has set out a roadmap in 2016 for the development of 5G global specifications for a new radio access technology and a next-generation network architecture to address these requirements. In phase one the 5G new radio (5G NR) access specifications were defined and announced in December 2017 with 3GPP Release 15 [37]. In phase two with 3GPP Release 16 [38], which is supposed to be finalized by the end of 2019, the specifications for an initial full 5G System are expected to come to completion. It must be noted that in the meanwhile specifications for older generations continue to evolve and 4G is even expected to play an important albeit supportive role in 5G Networks.

[18] 3GPP unites seven regional telecommunications standard development organizations ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, and TTC.

[19] Actually 3GPP develops technical specifications and these are then transposed into standards by the seven regional standard development organizations.

2.5 Summary

In comparison to earlier generations of mobile telecommunications 5G constitutes a paradigm shift because, not only is it required to perform significantly better on all key indicators like latency, data rates and energy usage, but with the virtualization of network functions and decoupling of control and service layers, the focus is now on serving so-called verticals with tailor-made functions and different QoS. Specifications for a full 5G System are expected by the end of 2019 and older generations like 4G are expected to play an important but supportive role.

3. Technological features of 5G

This chapter examines the key technical capabilities of 5G. It emphasizes that these requirements, employing advanced technologies, open up possibilities for novel usage scenario's.

3.1 Key technical capabilities of 5G

ITU-R has set the following targets for eight key technical capabilities for 5G mobile telecommunications in IMT-2020 [39].

1. *Peak data rate: 1 - 20 Gb/s*

The achievable data rate under ideal conditions per user/device.

2. *User experienced data rate: 10 - 100 Mb/s*

The achievable data rate that is available ubiquitously[20] across the coverage area to a mobile user/device.

3. *Spectrum efficiency: 15 - 30 bits/s/Hz*

Average data throughput per unit of spectrum resource and per cell[21].

4. *Peak Mobility: 350 – 500 km/h*

Maximum speed at which a certain QoS and seamless transfer are achieved between radio nodes (belonging to different layers or radio access technologies).

5. *Latency: 1 – 10 ms*

The time from when the source sends a packet to when the destination receives it.

6. *Connection density: 10.000 – 1 million devices/km^2*

The number of connected or accessible devices.

7. *Network energy efficiency: 90% more efficient (than in IMT-Advanced[22]* [40]*)*

The number of information bits transmitted to or received from users, per unit of energy consumption of the radio access network (RAN) (in bit/Joule).

8. *Area traffic capacity: 0.1 – 10 Mb/s/m^2*

Total traffic throughput served per geographic area.

Figure 3.1 presents the targeted improvements of IMT-2020 [39] compared to its predecessor IMT-Advanced [40].

The relevance and applicability of these key capabilities will depend on the usage scenarios. Trade-offs will have to be made, for not all these capabilities can be maximized simultaneously.

[20] "ubiquitous" should not relate to an entire region or country but to the considered target coverage area.
[21] The radio coverage area over which a mobile terminal can maintain a connection with one or more units of radio equipment located within that area. For an individual base station, this is the radio coverage area of the base station or of a subsystem (e.g. sector antenna).
[22] The ITU-R current standard for mobile telecommunications, referred to as 4G or sometimes 4.5G.

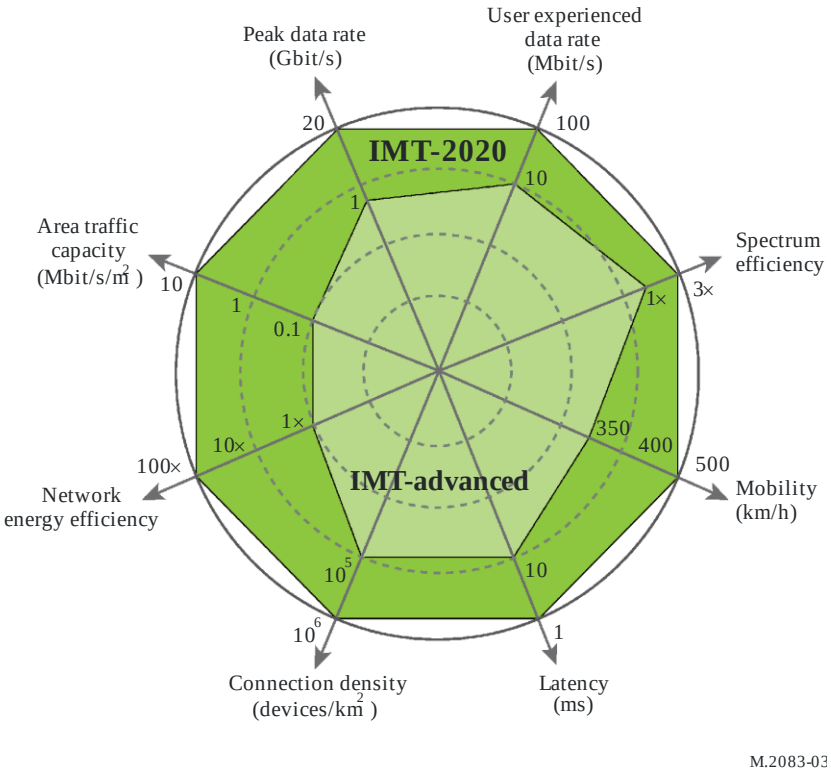


Figure 3.1 Improvements of IMT-2020 against IMT-advanced [39].

ITU-R also recognizes that other capabilities like spectrum and bandwidth flexibility, reliability, resilience, operational lifetime, privacy, and security might also be important for certain services in the intended usage scenarios [39].

The ITU-R targets [39] lead to a set of minimum requirements, related to the technical performance of 5G [41]. Figure 3.2 presents an overview of the requirements for 5G and the possibilities that emerge when these requirements are achieved [42].

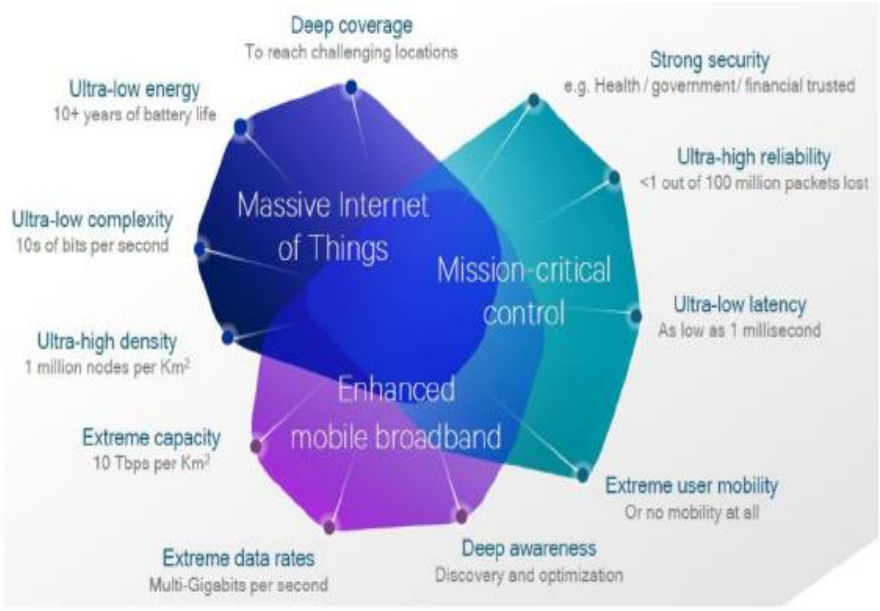


Figure 3.2 An overview of the requirements and opportunities for 5G [42].

3.2 Main families of usage scenarios in 5G

According to ITU-R the usage scenarios for IMT for 2020 and beyond include [39]:

- Enhanced Mobile Broadband (eMBB)

These are the human-centric scenarios with highly improved mobile broadband services with regards to user experienced data rates, traffic volumes, coverage, and seamless mobility. It concerns both wide and dense area (e.g. hotspot) coverage cases with each different requirements. The wide area coverage case desires seamless coverage and medium to high mobility, with improved but less stringent data rates compared to the hotspot case. In the hotspot case with low mobility and high user density, very high traffic capacity is needed and the user data rate is higher than that of wide area coverage. Examples of 5G services in this scenario are augmented reality, virtual reality, and ultra-high definition video.

- Ultra-reliable and low latency communications (URLLC)

These are the scenarios with strict and demanding capability requirements like very low latency, very high reliability, and high availability as well as throughput. Examples of 5G services in this scenario are industrial automation, autonomous driving vehicles, remote surgery, and smart grids.

- Massive machine type communications (mMTC)

These are the scenarios with very large numbers of connected low-cost devices. They have very long battery life and transmit a relatively small amount of data not so sensitive to delays. Examples of 5G services in this scenario are smart metering, inventory control, agriculture sensors, and Internet of Things (IoT) [3] in general. Figure 3.3 presents the envisioned usage scenarios of IMT-2020.

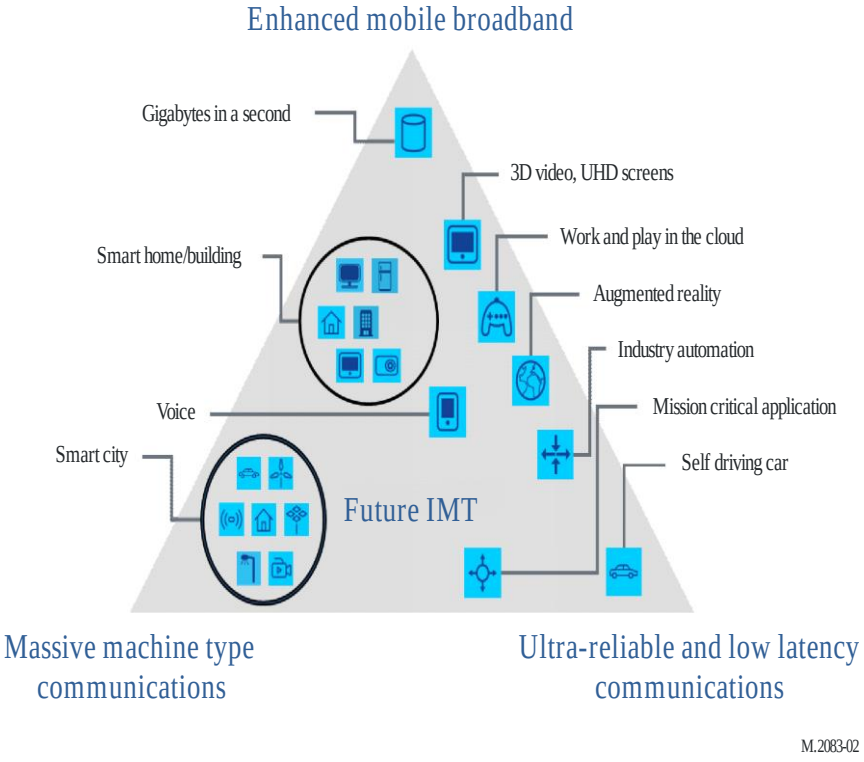


Figure 3.3 The envisioned usage scenarios of IMT-2020 [39].

The importance of key capabilities in different usage scenarios of IMT-2020 such as peak data rate, latency and connection density is shown in Figure 3.4 [39].

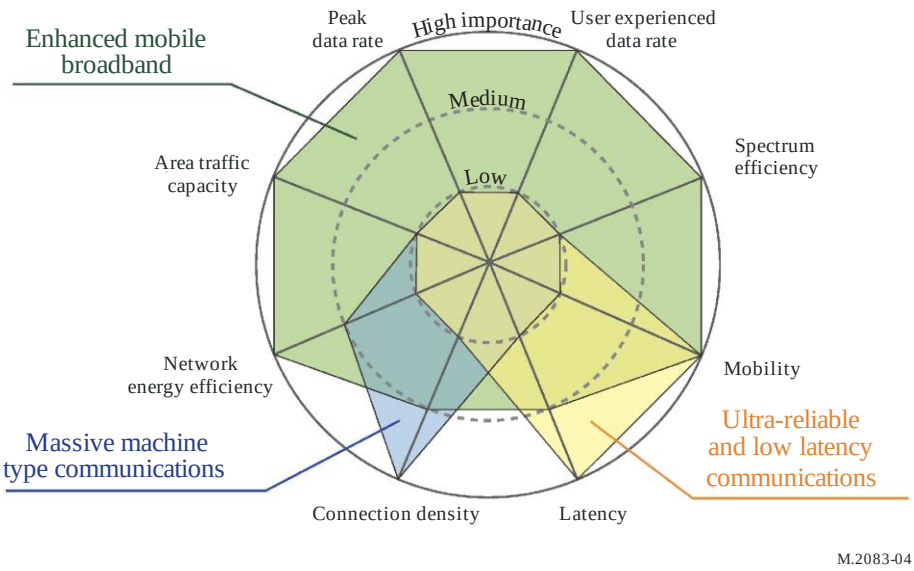


Figure 3.4 The importance of key capabilities in different usage scenarios [39].

3.3 Technologies to enable 5G

To fulfil the usage scenarios, 5G will have to combine several new technical capabilities and technologies. Therefore 5G is not just faster radio access technology, it is a paradigm shift with new trust models and fundamental changes in network architecture such as separating the data, control, management and orchestration, and service layer and creating the possibility for several virtual networks on the same physical infrastructure through softwarization and virtualization [17].

Network architecture

It is foreseen for 5G to be a mixture of current radio access technologies (e.g. LTE) and the newly proposed New Radio (NR) access technology, as well as to support interworking with Wireless Local Area Network (WLAN) [43]. Furthermore as a distinguishing factor 5G is supposed to be flexible and adaptive to simultaneously accommodate different usage scenarios by deploying key enabling techniques [44] such as Network Function Virtualization[23] (NFV) [45], Software Defined Networking[24] (SDN) [46], Mobile-Edge Computing[25] (MEC) [47], Millimetre Wave Transmission[26] (mWT) [48], Next Generation Protocols[27] (NGP) [49], massive multiple-input-multiple-output[28] (MiMo) [50] and Beamforming[29], and Network Slicing[30] (NS) [51]. Figure 3.5 presents the setup of the 5G end-to-end network architecture.

[23] With NFV specific network functions are implemented in software running on generic hardware, without the need for specific machines, thereby making sharing and reuse of functionality possible.
[24] SDN, complementary to NFV, allows third parties to control network resources and their performance.
[25] MEC is cloud computing at the edge of the network and close to the user so as to reduce latency.
[26] mWT is the use of millimeter waves from small cells to drastically increase network capacity at short range.
[27] NGP is an initiative for the development of a successor to TCP/IP that better suits 5G demands.
[28] Massive MiMo can increase the capacity of mobile networks by using a lot of antennas in one single array.
[29] Adaptive antenna arrays with narrow beams can reduce the impact of interference, and increase long distance capacity.

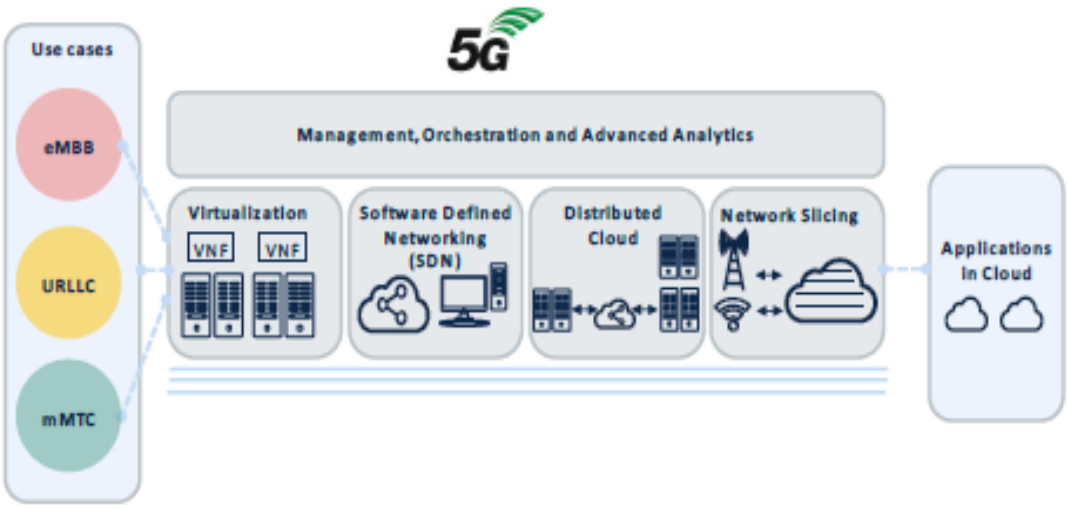


Figure 3.5 The setup of a 5G end-to-end network architecture [18].

Trust model

Whereas in 4G the trust model is formed between users and mobile operators, in 5G new actors and new vertical service delivery models call for a new trust model in order to provide end-to-end security [52]. Figure 3.6 illustrates the difference between the trust models in 4G and 5G. The earlier mobile communications networks are responsible for authenticating the user for network access only. The authentication between user and services are not covered by the legacy networks. However, in 5G networks the trust model includes the vertical service provider, so networks can for example cooperate with service providers to carry out secure and more efficient identity management.

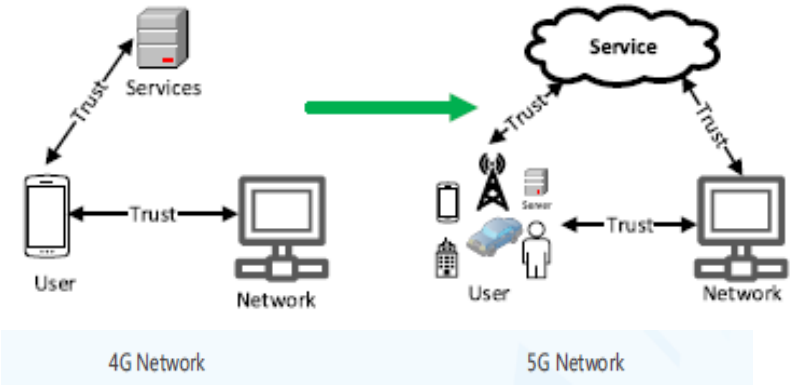


Figure 3.6 Trust model 4G evolvement to trust model 5G (adapted from [16]).

Spectrum allocation

5G will need (a lot more of) new spectrum to handle the predicted amounts of connected devices, the high-density networks, and to bolster some use cases. With widespread coverage and capacity in

[30] Network Slicing allows for virtual networks on a common infrastructure; within the overall constraints of that infrastructure, characteristics of particular network slices can vary agilely through software reconfiguration.

mind the World Radio Conference 2015 (WRC-15) [53] has identified three frequency ranges for the spectrum needs of 5G; < below 1 GHz, between 1 and 6 GHz, and above 6 GHz.
The WRC-15 [53] has allocated the 700 MHz[31] band, which is also designated in the EU [54] [55], for the sub-1 GHz spectrum. In the 1-6 GHz range, WRC-15 has given the 3.6 GHz[32] band priority and furthermore the 1.5 MHz[33] band [53]. For the supra-6 GHz spectrum, the 26 GHz[34] band is identified as a candidate band by the Radio Spectrum Policy Group[35] (RSPG) [56] and the European Commission has mandated the Conference of Postal and Telecommunications Administrations (CEPT) to develop harmonized technical conditions [57], but the World Radio Conference 2019 (WRC-19) will ultimately decide on the so-called Millimetre Wave (mmWave) spectrum for mobile broadband in frequencies between 24.25 and 86 GHz based on requested studies by ITU-R [58].

NL is planning to auction the 700 MHz, 1400 MHz and 2100 MHz bands in 2019 [59] [60], after European approval of a merger of two large telecom providers[36] [61] and a market impact analyses by the Authority for Consumers and Markets (ACM). The current issuance policy for the 3.5 GHz band will be evaluated also. Furthermore, after European decision making in 2020, the 26 GHz band will be made available to the market for both national and company-specific applications [62].

3.4 Summary

The key technical requirements set for 5G by ITU-R in IMT-2020 will give rise to eMBB, URLLC and mMTC usage scenarios based on a new trust model and employing advanced technologies like NR, NFV, SDN, MEC, mWT, massive MiMo and NS in the designated frequency bands 700 MHz, 3,6 GHz and most likely 26 GHz.
NL will auction spectrum for 5G in 2019 and 2020 after market analysis and European decision making.

[31] 700 MHz is a proxy for the range 694-790 MHz.
[32] 3.6 GHz is a proxy for the range 3400-3800 MHz.
[33] 1.5 MHz is a proxy for the range 1427-1518 MHz.
[34] 26 GHz is a proxy for the range 24.25-27.5 GHz.
[35] Radio Spectrum Policy Group (RSPG) is a high-level advisory group that assists the European Commission in the development of radio spectrum policy.
[36] The merger has been approved on November 27th 2018 [65].

4. Business implications of 5G and cross-sectoral use cases

This chapter sketches the potential impact of 5G on the telecom business sector and highlights some cross-sectoral use cases for 5G illustrating the possible influence on society far beyond the typical telecommunications domain.

4.1 Business impact

It is expected that 5G will give rise to a rearrangement of the telecom business value chain with new roles for the traditional stakeholders [18] and the introduction of new stakeholders.

5G can provide possibilities for micro-operators to deploy local small cell radio access networks with tailored services as a supplement to Mobile Network Operator (MNO) propositions [63].

The MNO could still deploy its own infrastructure (i.e. small cells) in private sites. On the other hand, the role of the small-site owner can become very important in service provisioning, with the construction of networks with a high density of small cells, to increase network capacity in specific locations (e.g. malls, stadiums, hospitals) [18], [64], [65]. If multiple operators want to use his site, negotiations will follow regarding access and practicalities as power and backhaul. So the site owner could offer exclusive access, and the operator may (or may not) then offer wholesale access for other operators (see 'New model 1' in Figure 4.1) or new players can acquire sites, deploy their own 5G infrastructure to offer wholesale services to 5G operators (see 'New model 2' in Figure 4.1).

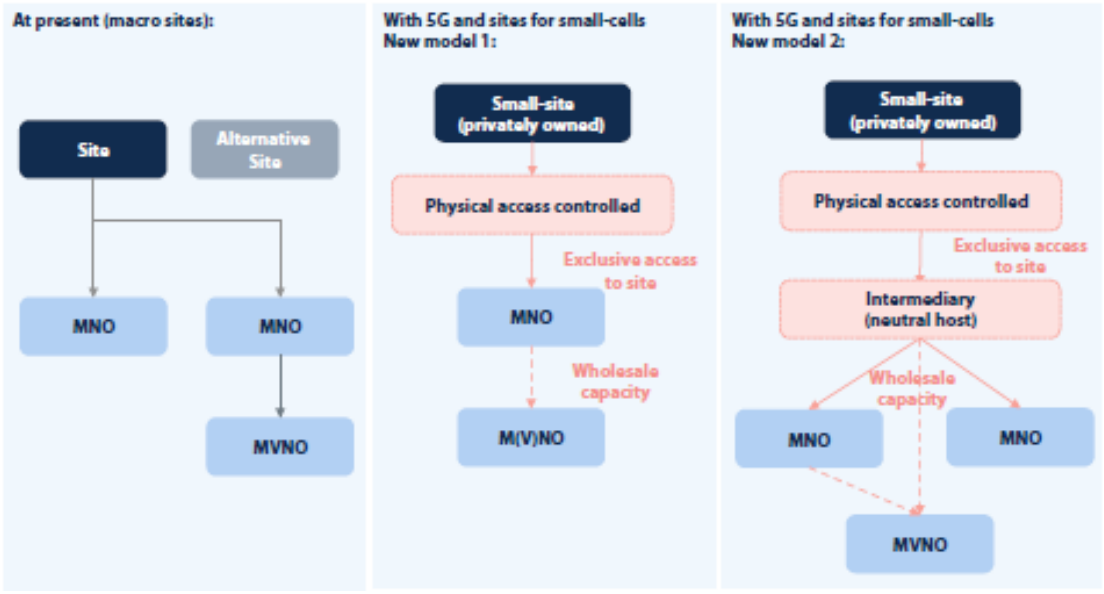


Figure 4.1 Alternatives of access to small cell sites [18].

The roles of (local) content service providers also change, leading, for instance, to close collaborations with MNO [66] e.g. VodafoneZiggo's exclusive contract with HBO [67].

With network slicing a 5G Slice broker can offer Mobile Virtual Network Operators (MVNOs), over-the-top (OTT) service[37] providers, and vertical sector market players network resources on-demand as a service adopted from infrastructure providers such as MNOs or infrastructure vendors.

Where embedded connectivity is required (e.g. in cars) a renegotiation between MNO and the device manufacturer might be necessary [18]. Some likely options are:

• The MNO continues to provide connectivity and negotiates with the vertical and/or original equipment manufacturer (OEM) bilaterally to provide customized connectivity (see option A in Figure 4.2);

• The vertical might prefer a self-supplied (i.e. private 5G network) solution with specific requirements and/or because there are concerns about relying on a public network (option B in Figure 4.2);

• Like in the case of content service providers (see above) there is room for joint ventures between the vertical and/or OEM and the network operators (option C in Figure 4.2);

• New intermediaries who negotiate deals (across borders) with a large number of MNOs (and fixed operators) to market connectivity to that vertical (option D in Figure 4.2).

[37] Service in which content reaches the end-user directly via the internet (e.g. WhatsApp, Netflix) [70].

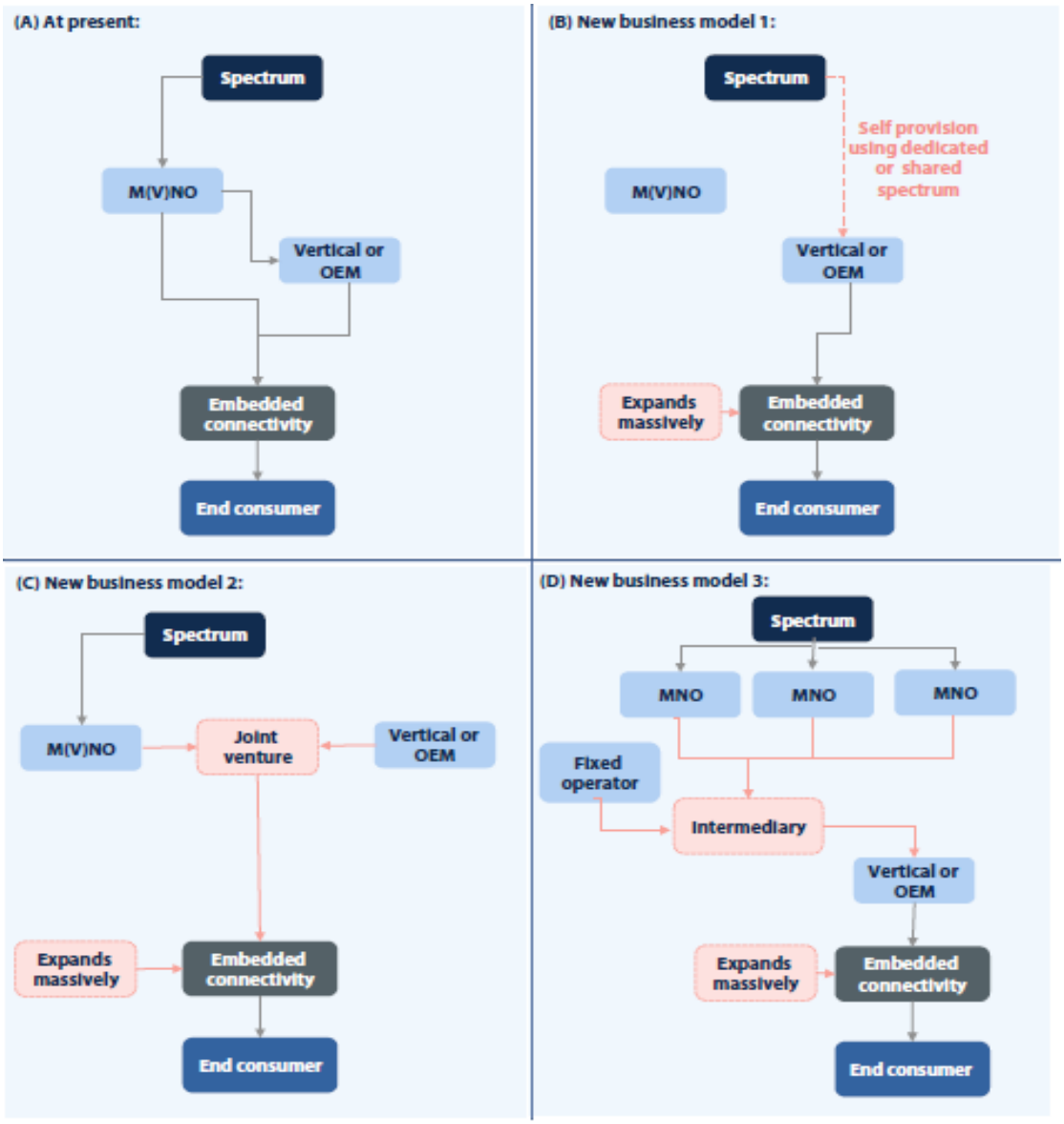


Figure 4.2 Business models for embedded connectivity [18].

With SDN and NFV in 5G MNOs can reduce costs for the provisioning of Public Order and Safety services, currently offered over an independent network Infrastructure, when offered over the same network infrastructure as commercial networks but in a separate 5G Slice with specific requirements.

Furthermore, 5G is expected to allow new stakeholders to exploit many more opportunities opened up by technical innovations in the fields of connectivity services, content services, context services and commerce platforms with many kinds of verticals, IoT and digital data processing solutions. Figure 4.3 provides a summary of the expected impact of 5G on telecom business.

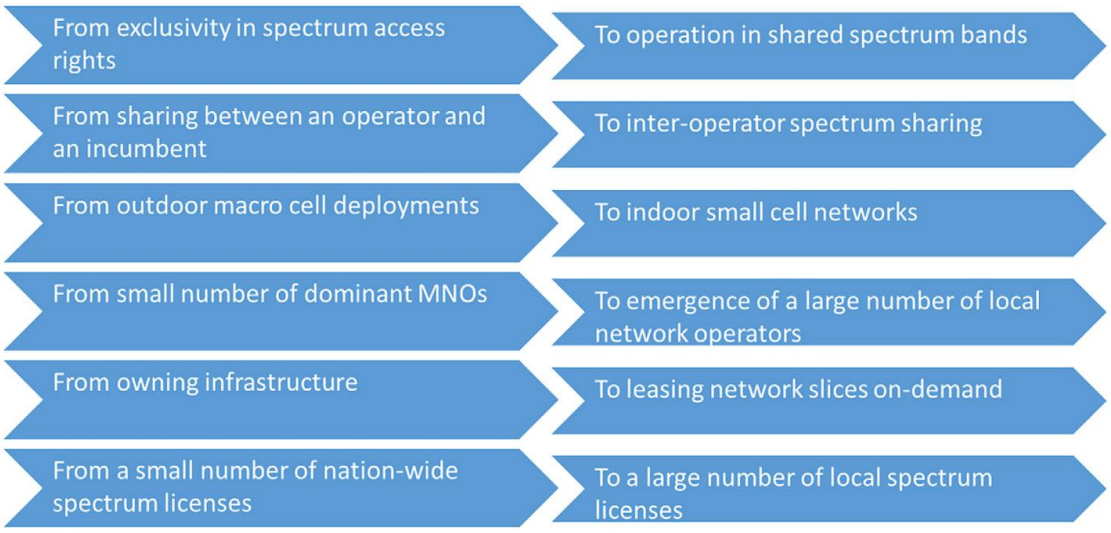


Figure 4.3 Expected impact of 5G on telecommunications business [63].

As a consequence supervisory bodies will be confronted with a great many more stakeholders in 5G.

4.2 Use Cases

According to 5G-PPP, several so-called verticals will be empowered by 5G [35]. It is expected that the realization of 5G potential will be a step-by-step process, with the first focus on improving the existing broadband propositions [18]. However, the attention of the public is drawn towards use cases where 5G brings new business opportunities or spectacular change to existing services (e.g. virtual reality, connected cars, and precision farming) [49]. To illustrate the possible consequences of 5G across society, one use case that transcends the telecom domain is described for each of the usage scenarios eMBB, URLLC and mMTC (see also Table 1.1).

4.2.1 eMBB: Virtual Reality

In this example of an eMBB use case, demand for connectivity and data requirements will increase when spectators at live events can enjoy immersive media services for an improved experience using virtual reality headsets. It is estimated that at least 0.75 Tbps will be needed for broadband access in a full stadium in 2020 [1]. 5G can achieve this with spectral efficiency and massive MIMO plus techniques in interference mitigation and receiver technology [68]. Due to the propagation characteristics of the mmWave spectrum multiple 5G small cells, with seamless hand-over between cells, will be needed in support of this use case. Virtual Reality can also come of aid in sectors like medicine, military and aviation (for training purposes for example). For virtual reality to meet performance expectations it will demand robustness of architecture, as well as high reliability of interacting 5G System components. The overall requirements are presented in Table 4.1.

Data Rate	**Latency**	**Reliability**	**Device Density**	**Traffic Density**	**Service Deployment**	**Network Slicing**
15-30 Mbps	10 ms	99%	150000/km2	3.75 Tbps/km2	90 minutes	Effective

Table 4.1 Requirements for virtual reality [18].

4.2.2 URLLC: Connected Driving

To enable the vision of fully autonomous vehicles over time, vehicles will need to exchange information such as position and speed with each other (vehicle-to-vehicle (V2V) communication), the surrounding infrastructure (vehicle-to-infrastructure (V2I) communication with e.g. traffic lights

and road signs), other road users (e.g. pedestrians and cyclists), and possibly the vehicle manufacturer and the mobility service provider (vehicle-to-internet (V2N) communication). All these types of communication are referred to as vehicle-to-everything (V2X) communication [69].

The 5GAA[38] states that "*The Cellular-V2X (C-V2X) technology is already available but to support the autonomous vehicles of tomorrow, the technology must evolve to meet more demanding safety requirements. 5G will facilitate this evolution. Its extreme throughput, low latency, and enhanced reliability will allow vehicles to share rich, real-time data, supporting fully autonomous driving experiences."* [69].

Once cars are "connected" and large amounts of data are collected on the car's movements, locations and possible sensor data (such as acceleration and braking) could allow for the development of business models like in the insurance industry with calculations to determine vehicle insurance premiums, but also pay-as-you-drive concepts, charging for real-time in-car entertainment, and sale of data to interested third-parties [18]. The overall requirements are presented in Table 4.2.

Data Rate	Latency	Reliability	Mobility	Device Density	Position Accuracy	Network Slicing
> 10 Mbps	< 5 ms	99.999 %	> 200 km/h	10000 /km2	30 cm	Preferable

Table 4.2 Requirements for connected driving [18].

4.2.3 mMTC: Agriculture Sensor Networks (IoT)

Smart farming and precision agriculture with 5G and sensor networks (IoT) can help in the efficient increase of farming produce. Data collected wirelessly from agricultural machinery can be used for example to determine when, where and how much of fertilisers are to be used with over time positive environmental effects for farmland and watercourses. Even so, the collected data can be used to trigger the deployment of agriculture drones for sowing. The overall requirements are presented in Table 4.3.

Data Rate	Latency	Reliability	Device Density	Traffic Density	Service Deployment	Network Slicing
15-30 Mbps	10 ms	99%	150000/km2	3.75 Tbps/km2	90 minutes	Effective

Table 4.3 Requirements for Agriculture Sensor Networks [18].

The 5G use cases from the sorts of eMBB, URLLC and mMTC serve vertical sectors reaching far beyond the typical telecommunications domain subsequently creating a major challenge for the supervisory bodies concerned with the cyber security of 5G.

4.3 Summary

With 5G, the telecom business sector will see changes in its value chain due to novel business propositions by new stakeholders alongside those of the traditional stakeholders. As a consequence supervisory bodies will be confronted with a great many more stakeholders in 5G.

[38] 5G Automotive Association is a global, cross-industry organisation of companies from the automotive, technology, and telecommunications industries (ICT), working together to develop end-to-end solutions for future mobility and transportation services.

It is expected that the realization of 5G potential will be a step-by-step process, with the first focus on improving the existing broadband propositions. The 5G use cases from the sorts of eMBB, URLLC and mMTC serve vertical sectors reaching far beyond the typical telecommunications domain subsequently creating a major challenge for the supervisory bodies concerned with the cyber security of 5G.

Part 2. Cyber security of 5G

5. Cyber security challenges for 5G

This chapter concerns the identification of security risks for 5G in several key areas. First, the security challenges in the mobile telecommunication generations are described in general, then the focus is on the security challenges (in the architecture) of the (proposed) 5G System. Finally, use cases are examined for specific challenges.

5.1 Historical overview of security challenges in mobile telecommunications

Security challenges in 1G

Security in 1G was very poor; illegal mobile phone cloning was easy and although the number being dialled could be encrypted, with any FM receiver on similar frequencies eavesdropping was simple.

Security challenges in 2G and 2.5G

Message spamming, broadcasting incorrect information or unwanted marketing became common. Rogue base stations presenting fake network authentication intercepted mobile traffic. Subsequently, data confidentiality and security became important.

GSM was an improvement when it introduced the Subscriber Identity Module (SIM) as a security module and focused on user authentication, application of encryption algorithms for data and signalling, and confidentiality of user identity.

Security challenges in 3G and 3.5G

The introduction of Internet Protocol (IP) based communication also paved the way for internet security challenges into mobile communications. User equipment and its operating system were targeted. Malicious code (i.e. malware and spyware) were injected into applications to exploit vulnerabilities and access personal information (e.g. passwords, contacts information, and location data).

Security challenges in 4G

With the step to end-to-end IP-based communication and multimedia traffic, new services for smart devices emerged leading to a more complex threat landscape. Distributed Denial of Service (DDoS) attacks and Advanced Persistent Threats (APT) came about with attackers following a more systematic and organized approach making it hard to detect anomalies, and protect and mitigate.

Figure 5.1 depicts the security challenges in mobile telecommunications from the beginning to date [70].

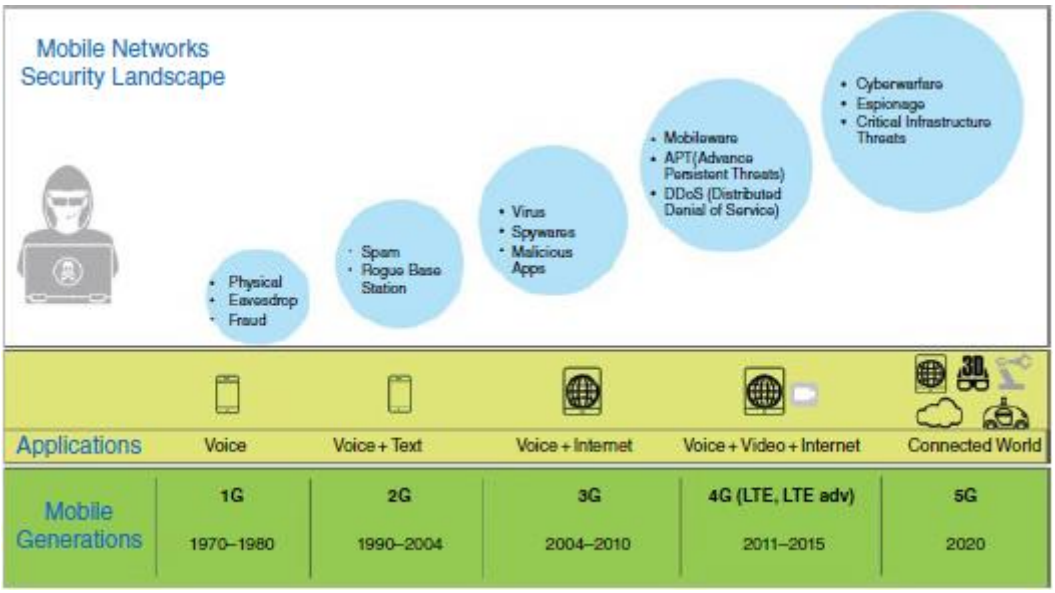


Figure 5.1 The security challenges in the generations of mobile telecommunications [70].

5.2 Security challenges in 5G

With its vast amount of applications and services, the 5G threat landscape will span from end-user devices to the Radio Access Network (RAN), to the mobile core network and the Internet (see Figure 5.2). Figure 5.2 also highlights several types of threats for every subdomain within the 5G network.

If 5G is to serve as a utility, or critical infrastructure itself, providing connectivity to other critical infrastructures, and several sectors like for instance media and entertainment, logistics, energy, manufacturing, automotive, and healthcare the threat landscape of 5G will be unprecedented.

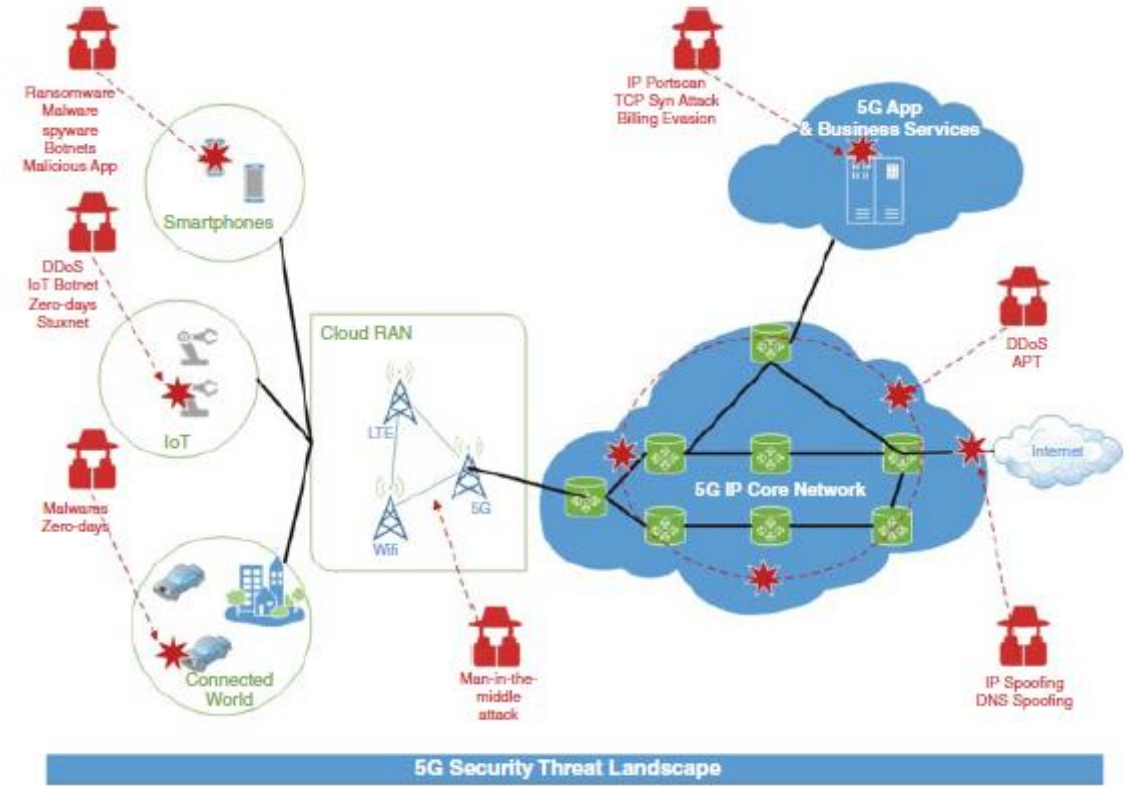


Figure 5.2 5G Threat landscape [70].

5.3 Security challenges in the 5G System architecture

Some of the most striking security challenges in the 5G System will be touched upon without the intention to be complete.

As the architecture for 5G is being defined and standardized, security functions are to be embedded from the outset (i.e. native security). The IEEE 5G and Beyond Technology Roadmap Security Working Group [2], ETSI [49], NGMN [1], 3GPP [43] and 5G-PPP [16] are developing security requirements for 5G networks. The NGMN highlights of the security requirements of 5G wireless networks is shown in Table 5.1. Furthermore, privacy needs to be considered in the requirements as well since with massive numbers of user and IoT devices a lot of personally identifiable information will be carried over the 5G network.

Security requirements with respect to 4G	Security requirements regarding radio access
Resilience and availability against signalling based threats including malicious and unexpected overload	System robustness against smart jamming attacks
Specific security design for low latency use cases	Improved security for 5G small cell nodes
Compliance of network virtualization to 4G 3GPP standards	
Resilience and high availability of public safety and mission-critical communications	

Table 5.1 NGMN security requirements of 5G wireless networks [71].

These requirements must not only cover the physical, control, and application layers but also all the parts of an end-to-end 5G network as to contribute to the cyber security of 5G i.e. the security of 5G in cyberspace.

As 4G networks will play an important supportive role to 5G Networks and the 5G System itself is also IP-based it will inherit most of the existing threats to 4G. The security architecture in 5G Networks must, therefore, contain “backward compatibility of security”. Table 5.1 presents threats to the 5G System inherited from 4G [70].

Threat	**Threat Description**
Insecure Mobile OS (Operating System)	Attackers can exploit mobile operating systems vulnerabilities
Malicious apps	Download and installation of harmful apps
Insecure apps	Legitimate apps leaking sensitive data
Virus	Malicious software code with a specific purpose to damage mobile functions or files
Malware	An advanced virus or malicious app that can propagate and self-reproduce causing large-scale, network-wide damage
Spyware	A malware type used to steal end-user data or sensitive information to transmit to remote attackers
DDoS (Distributed Denial of Service[39])	A coordinated attack involving hundreds of thousands of devices infected with malicious code targeting the availability of the mobile network

Table 5.1 Threats to the 5G System inherited from 4G [70].

[39] A Denial of Service (DoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled [75].

5.3.1 Security challenges due to softwarization and virtualization

As a 5G network infrastructure will be more open and programmable, because built with SDN and NFV, the security issues of softwarization and virtualization become challenges of 5G as well (e.g. the security of the communication between the control and data planes, and the security and isolation of dedicated network slices). Figure 5.3 illustrates the set-up of the software-defined 5G architecture.

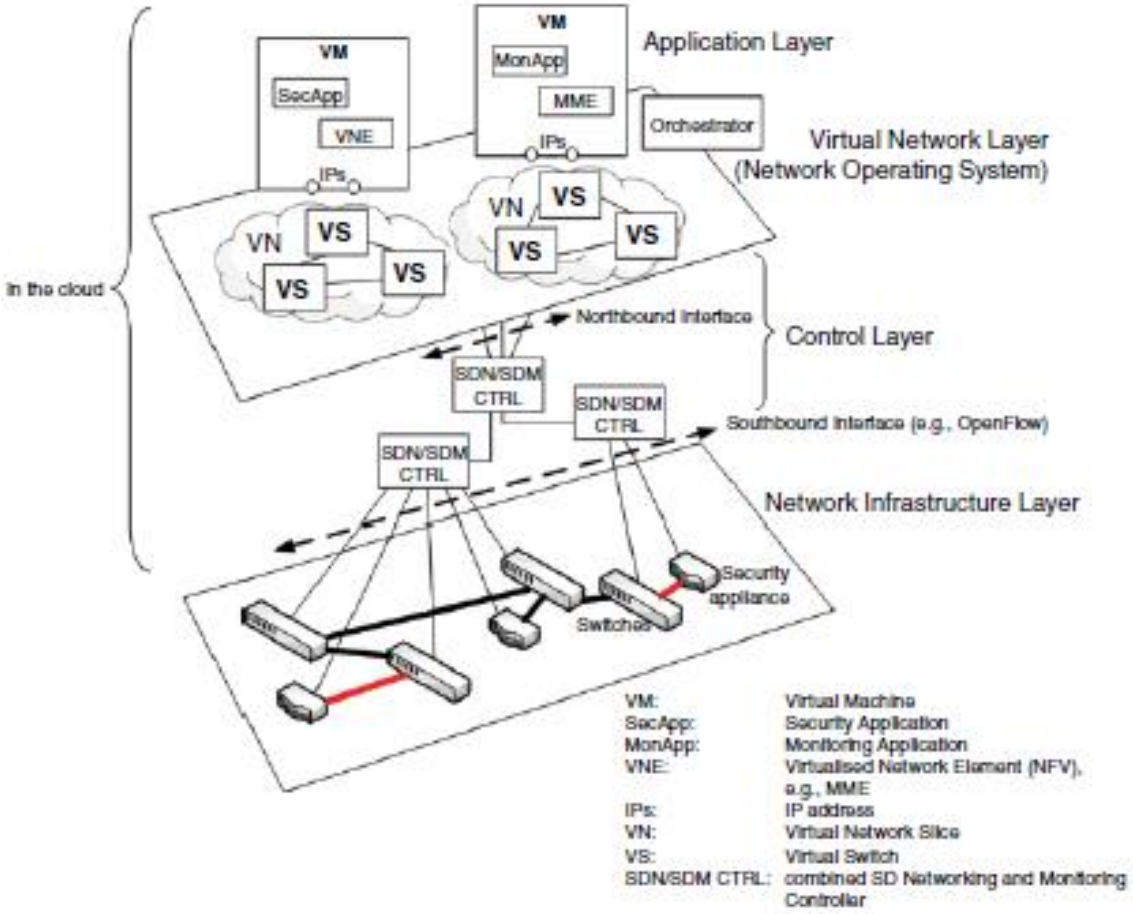


Figure 5.3. The set-up of the software-defined 5G architecture [72].

On top of the threats inherited from 4G the 5G System, with its software-defined architecture, will have to cope with advanced threats to with possibly greater impact. Table 5.2. presents some advanced threats to the 5G System [70].

Threat	**Threat Description**
Ransomware	Specialized malware that exploits, encrypts and locks access to critical data.
Advanced Malware	Advanced malware targeting millions of mobile, IoT and 5G network resources with the capability to exploit vulnerabilities
Botnets	IoT and mobile devices misused for both passive and active attacks on network resources
Critical Infrastructure Threats	Threats that are focused, on damaging critical infrastructure services such as SCADA
Zero-day Attacks	Advanced attacks exploiting the undiscovered vulnerabilities of a system. Can be a combination or package of multiple attack types, malware, and botnets

Table 5.2. Advanced threats to the 5G System [70].

SDN and NFV

SDN enables the centralization and programmability of network control and separate data layers. However, this centralized control can be threatened by DoS attacks, and exposing critical Application Programming Interfaces (APIs) to malware can render the whole 5G System down.
Since most network functions can be implemented as applications, malicious applications if granted access can spread havoc across a network.
NFV is very important in 5G, but it has basic security challenges such as confidentiality, integrity, authenticity and nonrepudiation.
The main challenge is that the whole network can be compromised if the hypervisor is hijacked [73].

Cloud computing

The proliferation of cloud-based services will enable application portability across multiple devices and domains and will offer major opportunities for enterprises. At the same time, this imposes challenges that have to be managed properly (e.g. security, privacy, network configuration conflicts) [1]. The threat landscape on the user platform, with applications and interfaces required to access the cloud facilities, may range from physical threats to the mobile device and other integrated hardware components, to application-based threats (e.g. malware, spyware) to disrupt applications or gather sensitive information. The security threats on the core network are targeted towards the RATs that interface user devices to the cloud (e.g. DoS attacks, address impersonation, and session hijacking). The back-end platform consists of the cloud servers, data storage systems, virtual machines, hypervisor[40] and protocols required to offer cloud services. Here the scope of security threats may range from data-replication to DoS attacks.

MEC

Present-day core network functions will be deployed at the edge of the network, where not all the (virtualized) network equipment will be owned by the same party. The MEC platform will have a limited size of hosts, which cannot deliver the same level of protection as conventional data centers. This diverse environment is susceptible to malicious attacks. In these networks, special care has to be taken with regards to for example privacy and integrity across access networks elements [51]. Threats such as Denial of Service (DoS) Attack, Man-in-the-Middle (MitM) Attack[41], Virtual Machine (VM) Manipulation[42], and Privacy Leakage[43] have been identified [74].

Furthermore, in 5G usage scenarios, inconsistent or unpunctual (firewall) security policy sharing among network operators and MEC servers could jeopardize the security of users traffic, wireless functionality and subscriber content at the edge of the network. Due to the need for reduced latency, roaming traffic will be routed over partner networks and inconsistent or irreconcilable firewall security policies among roaming partners can equally prevent roaming from working correctly.

---

[40] In a virtualized system, the hypervisor is the software or firmware that controls the system. In this case, it is the cloud operating system.
[41] A MitM attack is a third malicious party interposing between two or more communicating entities and secretly relaying or altering the communication between such entities [78].
[42] VM manipulation by a malicious insider can cause numerous attacks such as logic bombs, malware and could compromise the security of other data centers when such VM migrates to another physical location on the network [78].
[43] However, the MEC paradigm limits the scope of privacy leakage at the edge.

5.3.2 Security challenges in communications channels

The 5G System is expected to include drones, cloud-driven virtual reality, connected vehicles, smart factories, robots, transportation and eHealth. These applications need secure communication systems that support more frequent authentication at network access and service levels, and exchange of sensitive data. In SDN based 5G mobile networks the communication can be categorized into three channels i.e. data channel, control channel and inter-controller channel. These channels are protected by using TLS[44]/ SSL[45] sessions. However, TLS/SSL sessions are highly vulnerable to IP layer attacks among more and lack strong authentication mechanisms [73].

With regards to radio access, unlike eavesdropping and traffic analysis, jamming can completely disrupt the communications between legitimate users. A malicious node can prevent authorized users from accessing radio resources and generate intentional interference that can disrupt the data communications between legitimate users [75].

5.3.3 Security challenges for privacy

In previous generations, operators had direct access and control of all the telecommunications system components. In the 5G System, operators will have to rely also on new actors and intermediaries like Communications Service Providers (CSPs) for control of the system. In a shared environment where the same infrastructure is shared among various actors, for instance VMNOs and other competitors user and data privacy can be challenged.

With the use of cloud-based data storage and NFV features, there are no more physical boundaries of 5G Networks. Consequently, the 5G operators no longer have direct control of the data storing place. As countries can have different data privacy rules, the privacy can be challenged if the data is stored in a different country [73].

For users privacy-sensitive information concerns identity, location and application data. Most smartphone applications require details of subscriber's personal information before the installation without mentioning how the data is stored and for what purposes it is going to be used. Threats like semantic information attacks, timing attacks, and boundary attacks target the location privacy of subscribers.

At the physical layer level in 5G mobile networks, location privacy can be leaked by access point selection algorithms.

By catching the International Mobile Subscriber Identity (IMSI) of the subscriber's User Equipment (UE) the identity of a subscriber can be traced. Such IMSI catching attacks can also be caused by setting up a fake preferred base station for the UE and subscribers to respond to with their IMSI.

An overview of security challenges for 5G System architecture is presented in Table 5.3.

[44] Transport Layer Security

[45] Secure Sockets Layer

Security Threat	Target Point/Network Element	Effected Technology				Privacy
		SDN	NFV	Channels	Cloud	
DoS attack	Centralized control elements	✓	✓		✓	
Hijacking attacks	SDN controller, hypervisor	✓	✓			
Signaling storms	5G core network elements			✓	✓	
Resource (slice) theft	Hypervisor, shared cloud resources		✓		✓	
Configuration attacks	SDN (virtual) switches, routers	✓	✓			
Saturation attacks	SDN controller and switches	✓				
Penetration attacks	Virtual resources, clouds		✓		✓	
User identity theft	User information data bases				✓	✓
TCP level attacks	SDN controller-switch communication	✓		✓		
Man-in-the-middle attack	SDN controller-communication	✓		✓		✓
Reset and IP spoofing	Control channels			✓		
Scanning attacks	Open air interfaces			✓		✓
Security keys exposure	Unencrypted channels			✓		
Semantic information attacks	Subscriber location			✓		✓
Timing attacks	Subscriber location				✓	✓
Boundary attacks	Subscriber location					✓
IMSI catching attacks	Subscriber identity			✓		✓

Table 5.3 Security challenges in 5G System architecture [73].

5.4 Cyber security challenges in sectoral use cases

Different security levels will be required for the various 5G service offerings. Critical services for instance, like those regarding public order and safety, might require more measures than services like augmented reality or virtual reality.

The cyber security challenges in the use cases of the eMBB, URLLC and mMTC usage scenarios for 5G presented earlier are highlighted.

5.4.1 eMBB: Virtual Reality

According to ENISA [76], the use of virtual reality with 5G can be a challenge for cyber security because this field will be attractive for the collection and possible misuse of specific (personal) data, the attack surface will be huge due to the integration of many components, confidentiality, integrity and availability requirements will be demanding, and weaknesses for operation, maintenance and insider abuse need to be controlled.

5.4.2 URLLC: Connected Driving

In this use case of connected driving, the success or failure of security controls can have an impact on safety. The 5G System will need to be resilient to various classes of failures to avoid personal injury, loss of life, severe damage or loss of assets. The confidentiality, integrity and availability of trust functions among (external) components need to be safeguarded and trust in the security of critical functions must be established (i.e. non-repudiation of performed actions) [76].

5.4.3 mMTC: Agriculture Sensor Networks (IoT)

With the large numbers of IoT devices, the attack surface will be huge. Available ill-secured devices or ill-protected interfaces can be abused to gain data (e.g. espionage), to be hijacked and misused for nefarious activities (e.g. Botnet attacks). ENISA states that the absence of product life-cycle functions (e.g. updates) makes the elimination of vulnerabilities impossible, so instead of “micro”-protecting each element in an IoT environment, a focus on protecting architecture components on the right level may be more appropriate [76].

5.5 Security challenges for public order and safety

NGMN Alliance recognizes that with the provisioning of 5G "*public order and safety organisations will need enhanced and secure communications. The main challenge is to ensure end-to-end (ultra) reliable communication for the emergency services across land, sea, air, in-building and some underground areas such as basements and subway systems. It will also require priority over other traffic (in networks shared with other users), the ability for direct communication between devices, and high security"* [1].

5.6 Security challenges for the critical infrastructure

If 5G Networks are to be considered critical infrastructure themselves[46] or provide connectivity to other critical infrastructure, major cyber security challenges may arise due to Advanced Persistent Threats (APT)[47] motivated with the aim of subversion[48], espionage[49], and sabotage[50] to quote Rid [77].

5.7 Summary

With its vast amount of applications and services, the 5G threat landscape will span from end-user devices to the Radio Access Network (RAN), to the mobile core network and the Internet.
If 5G is to serve as a utility, or critical infrastructure itself, providing connectivity to other critical infrastructures and a range of other verticals the threat landscape of 5G will be unprecedented.
The 5G System is IP-based and it will, therefore, inherit most of the existing threats to 4G and on top of those, it will have to cope with the security challenges in SDN, NFV, MEC, Cloud computing, and communication channels due to softwarization and virtualization.
The use cases of the eMBB, URLLC and mMTC usage scenarios for 5G require different cyber security levels (e.g. augmented reality compared to public order and safety services) and security challenges for confidentiality, integrity, authenticity and availability are many i.e. from the misuse of personal data to APT.

[46] Large telecommunications networks are part of vital national Infrastructure in NL [82].
[47] Advanced Persistent Threats use sophisticated techniques, can stay covert for a long time, are hard to detect, and evolve after every failed attempt [73].
[48] The deliberate attempt to undermine the authority, the integrity, and the constitution of an established authority or order.
[49] The purpose of extracting sensitive or protected information.
[50] The deliberate attempt to weaken or destroy an economic or military system.

Part 3. Cyber security regulatory framework

6. The regulatory environment for 5G

According to Lessig [78] a regulatory environment is composed of architecture, markets, social norms and legal aspects. This chapter depicts the regulatory environment for 5G in the European Union with a focus on NL.

6.1 Architecture

The following organisations have a decisive influence on the architecture of 5G.

6.1.1 ITU

The International Telecommunications Union[51] (ITU) intends to *"maintain and extend international cooperation among all the Member States of the Union for the improvement and rational use of telecommunications of all kinds"* [79].

ITU Radiocommunication Sector (ITU-R) has a mission *"to ensure rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including those using satellite orbits, and to carry out studies and adopt recommendations on radiocommunication matters."* [80]. To achieve these goals ITU-R intends:

- *To ensure interference-free operations of radiocommunication systems by implementing the Radio Regulations and regional agreements, as well as updating these instruments in an efficient and timely manner through the processes of the world and regional radiocommunication conferences;*
- *To establish recommendations intended to assure the necessary performance and quality in operating radiocommunication systems;*
- *To seek ways and means to ensure the rational, equitable, efficient and economical use of the radio-frequency spectrum and satellite-orbit resources and to promote flexibility for future expansion and new technological developments.*

As discussed in chapter 3, ITU-R has set minimum requirements for 5G in IMT-2020 [41]. The specifications of an end-to-end 5G system are not yet finalized but according to the last annual ITU IMT-2020/5G Workshop[52] future directions with regards to security may include [81]:

- Built-in security i.e. a security by design approach;
- Incorporation of increased flexibility in security setup to meet the requirement for a programmable, dynamic, and sliced 5G network;
- Secure key components, such as SDN/NFV/network slicing, since they provide a key foundation for implementing a programmable 5G network;
- Privacy controls to comply with data protection regulations and contractual agreement with other organizations;
- A high level of automation in security orchestration due to a highly dynamic 5G network.
- Adoption of Artificial Intelligence (AI) and Machine Learning (ML) based attack detection and mitigation.

[51] ITU was founded in Paris in 1865 as the International Telegraph Union. It took its present name in 1934, and in 1947 became a specialized agency of the United Nations. ITU currently has a membership of 193 countries and almost 800 private-sector entities and academic institutions.
[52] Third Annual ITU IMT-2020/5G Workshop and Demo Day Geneva, Switzerland, 18 July 2018.

6.1.2 IETF

The Internet Engineering Task Force (IETF) is the Internet standards body. The IETF is a large open international community of network designers, operators, vendors, and researchers developing open standards for the Internet architecture and the smooth operation of the Internet through open processes [82]. With regards to 5G, the IETF works closely together with 3GPP as they have done since 3G/4G when it was agreed to use IETF internet standards whenever possible to avoid duplication of functionality. IETF has developed much of the standards (e.g. IPv6[53], BGP[54], SNMP[55] and TCP[56]) that will be used (possibly after adjustment) in 5G.

6.1.3 3GPP

As noted earlier the Third Generation Partnership Project (3GP, as the global union of the seven regional telecommunications standard development organizations, has set out a roadmap in 2016 by 3GPP for the development of 5G global specifications for a new radio access technology and a next-generation network architecture to address the requirements of IMT-2020. In phase one the 5G new radio (5G NR) access specifications were defined and announced with 3GPP Release 15 in December 2017 [37]. In phase two, with 3GPP Release 16 [38], which is supposed to be finalized by the end of 2019, the specifications for an initial full 5G system are expected to come to completion.

6.1.4 IEEE

IEEE, world's largest technical professional organization, is a leading developer of international standards, with a portfolio of over 1300 standards and more than 600 standards under development, that lay the foundation for many of today's telecommunications, information technology, and power generation products and services.

Developments of standards typically related to 5G wireless communications like for instance those for enhanced mobile broadband, massive machine type communications, and ultra-reliable and low latency communications are underway [83].

As mentioned earlier the IEEE 5G and Beyond Technology Roadmap Security Working Group [2] focusses on the security aspects in the development of 5G.

6.1.5 5G-PPP

5G-PPP is the public-private partnership initiative for 5G between the European Commission and the European industry, aiming to secure Europe's leadership in the areas where Europe is strong or where there is potential for creating new markets e.g. smart cities, e-health, intelligent transport, education or entertainment and media.

As noted in chapter 2, 5G-PPP presented a concept of the integrated architecture as foreseen for 5G in their white paper 5G empowering vertical industries [40]. This architectural model consists of the infrastructure layer with heterogeneous access systems, transport networks, storage and computing centres, and all connected devices; the Network Function Layer that manages the offerings of virtual resources to the Multi-service Control layer responsible for dedicated networks; the Business

[53] Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet.
[54] Border Gateway Protocol (BGP) for routing of internet traffic between providers.
[55] Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring.
[56] Transmission control protocol (TCP) is a network communication protocol designed to send data packets over the Internet.

Function layer with typical vertical sector application related functions and the Business Service layer defining the business processes of the verticals.

6.2 Markets

According to Lessig the market rules (e.g. determining costs and price) have a regulating effect [78]. The following parties have significant influence in the marketplace of 5G provisioning.

6.2.1 NGMN

The Next Generation Mobile Network (NGMN) Alliance, an association of more than 80 partners from the mobile telecommunications industry and research. NGMN has established co-operation with leading industry organisations like 3GPP (i.a. ETSI) and GSMA to promote its vision.

NGMN has for example outlined qualitative and quantitative end-to-end 5G requirements in the White Paper [1], with a business view and from an operator perspective, in the areas of user experience, system performance, enhanced services, business models and management & operations.

6.2.2 GSMA

The GSM Alliance (GSMA) represents the interests of nearly 750 mobile operators and some 350 companies in the broader mobile sector, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. It has set as a goal to focus on *how to influence the development of 5G technologies and standards, support the rollout of 5G networks and development of new business models for the 5G era, guide the development of government agenda and policies, and moderate the messaging around 5G* [84]. GSMA promotes its vision on for example spectrum (i.e. support for 26 GHz, 40 GHz and 66-71 GHz, a plea for 45.5-52.6 GHz) in the run-up to WRC-19 [85].

GSMA warns that the success of 5G will depend on minimizing business risk in five areas:

1. The required investments for 5G are huge, particularly because of dense small cell deployments and backhaul provisioning, to provide reliable connectivity. The industry challenge is to explore new business models while optimizing the 5G costs.
2. Spectrum will remain a critical and scarce 5G resource in both the licensed and unlicensed bands. The availability of spectrum, at what frequency bands, and at what cost, will have a major impact on the business case for 5G.
3. It will be a challenge for 5G New Radio to deliver improved spectral efficiency, latency below 10 ms will challenge the laws of physics and network topology, and mWT will demand technological breakthroughs in devices and networks.
4. It must be ensured that operator services are included in the standards to avoid fragmentation, as was the case in earlier mobile generations, and to achieve scale benefits.
5. Regulatory modernization is encouraged and policymakers should provide a transparent and predictable pro-investment and pro-innovation framework given the heavy investment required to deliver 5G with reliable connectivity.

6.2.3 SIMalliance

SIMalliance represents 90% of the global SIM card[57] manufacturers and promotes the role of this hardware module in the delivery of secure mobile applications by participating in standardization working groups and by clarifying and recommending relevant technical standards to the industry [86]. Note however that the specifications for the 5G SIM are set by 3GPP in TS 21.111 version 15.1.1 Release 15 [87].

6.3 Social Norms

Lessig contends that social norms set constraints on the regulatory environment [78]. The influence that social norms have with regards to 5G are highlighted with some examples.

6.3.1 Everybody connected

The norm is nowadays that everybody is reachable via a (personal) device. This resonates in the requirement of high connection density for 5G. The target set by IMT-2020 is 1 million devices/km^2.

6.3.2 Ubiquitously connected

Besides from the social norm that everyone is connected, another norm demands excellent telecommunications connectivity everywhere and all the time. IMT-2020 has set the goal for total traffic throughput served per geographic area i.e. area traffic capacity at 0.1 to 10 Mb/s/m^2

6.3.3 Instant response

It is not acceptable anymore nowadays that response time in telecommunications interaction is not the same as in real life communication. IMT-2020, therefore, aims at a latency between 1 and 10 ms.

6.3.4 Energy consciousness

With awareness of the impact of human technology on the natural environment comes the social norm of energy efficiency for new “green” telecommunication systems. IMT-2020 strives for 90% less energy consumption in 5G compared to earlier generations.

6.4 Legal aspects

The goal of this section is to explore the legal provisions that have been set regarding 5G i.e. in risk management terms, based on perceived risks, identify the preventive and corrective controls regarding a breach of security of 5G.

6.4.1 The legal framework for 5G in the EU

Porcedda [88] points out that the EU legal framework for cyber security consists of at least eleven instruments. In the Area of Freedom, Security and Justice (AFSJ)[58] there are five instruments[59] regarding criminal liability for perpetration, aiding and abetting breaches [89]. And in the internal

[57] A subscriber identity module or subscriber identification module (SIM), widely known as a SIM card, is an integrated circuit to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).

[58] Title V of the Treaty on the Functioning of the European Union, deals with legislation in the area of criminal law, police and judicial cooperation. Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU), OJ C 83/01 (Lisbon Treaty).

[59]The generic instruments for computer crime-related investigations are: the European Investigation Order Directive; the Proceeds of Crime Directive; and the European Arrest Warrant. The fourth and the fifth more specific instruments are the Directive on attacks against information systems and the Europol Regulation.

market part, to counter the danger of underinvestment in cyber security due to misaligned incentives, information asymmetries and externalities [90] and the most relevant to the supervision of the cyber security of 5G, six instruments containing the legal obligations to protect systems and data, and the notification of breaches to a supervisory body and the affected stakeholders. These instruments have their legal basis mostly in Article 114 of the Treaty of the Functioning of the European Union (TFEU, former Article 95, internal market).

6.4.1.1 EU Regulations and Directives[60] on cyber security

The EU rules on cyber security (breaches) were introduced in three tranches, as noted by Porcedda [88]. The first tranche was the so-called Telecom Package containing the Citizens' Rights Directive[61] (amending the e-Privacy Directive[62] by adding rules on the prevention and mitigation of data breaches) and the Better Regulation Directive[63] (amending the Framework Directive[64] with the introduction of rules on security breaches).

The second tranche consisted of four instruments, namely the Electronic Identification and Trust Services (eIDAS) Regulation[65] based on Art. 294 TFEU, the Payment Services Directive (PSD2)[66], the Network and Information Security (NIS) Directive[67] and the General Data Protection Regulation (GDPR)[68] based on Arts. 16 and 114 TFEU. The eIDAS Regulation contains rules on breaches of security of identity assurance services and trust services. PSD2 has provisions on operational and security incidents of electronic payments enabled by payment services providers. The NIS Directive prescribes rules on security incidents with regards to essential services operators[69] (ESOs) and digital

[60] Directives must be incorporated into national law requiring EU Member States to achieve a certain result, but free to choose how to do so, whereas Regulations automatically become legally binding throughout the EU on the date they take effect.

[61] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 Amending Directive 2002/22/EC on Universal Service and Users' Rights relating to Electronic Communications Networks and Services, Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector and Regulation (EC) No 2006/2004 on Cooperation between National Authorities Responsible for the Enforcement of Consumer Protection Laws, OJ L 337 (Citizens' Rights Directive).

[62] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, OJ L 201 (e-Privacy Directive). The e-Privacy Directive is sometimes popularly referred to as the "the cookie law".

[63] Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services, OJ L 337 (Better Regulation Directive).

[64] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), OJ L 108.

[65] Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.

[66] Directive 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on Payment Services in the Internal Market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337.

[67] Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, OJ L 194.

[68] Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1.

[69]Public or private entities whose service: (a) is 'essential for the maintenance of critical societal and/or economic activities'; (b) its provision 'depends on network and information systems'; and (c) would be highly

service providers (DSPs), while the GDPR is a horizontal instrument and has rules covering all data breaches regardless of the addressee.

The third regulatory tranche concerns a complete renovation of the Telecom Package. The European Commission, the European Parliament and the Council of the EU have reached an agreement in June 2018 [91] on the proposed EECC updating the Framework Directive on many points like among others increasing the number of addressees considerably. Just recently the EECC has entered into force allowing the Member States two consecutive years for transposition into national legislation (Art. 125 of the EECC)[70].
As lex specialis to the GDPR the proposed e-Privacy Regulation[71], to be based on Arts. 114 and 16 TFEU, will no longer contain norms on data breaches. The e-Privacy Regulation, originally planned to be approved simultaneously with the enforcement of the GDPR, is now expected to be finalized somewhere in 2019. Thereafter, a period will be granted for familiarization before the e-Privacy Regulation is enforced.

6.4.1.2 Addressees

Porcedda identifies seven addressees for these six instruments [88]. The addressees of the Framework and e-Privacy Directives are "electronic communications services" (Art. 2(c) Framework Directive)[72] while Art. 2(d) of the Framework Directive defines "communications" as "any information exchanged or conveyed between a finite number of parties". Since communications via a public electronic communication service take place on a public communications network, consequently the Directives also apply to telecommunications providers using public electronic networks but do not concern content providers or Information Society Services[73] (as defined in the Transparency Directive[74]) i.e. web-based businesses.

---

disrupted by 'an incident' (arts. 4(4) and 5(1)). Annex II of the NIS Directive contains a list of essential services, which are in the sectors of energy, transport, banking, financial market infrastructures, health, the drinking water supply and distribution, as well as digital infrastructure. The last one includes Internet exchanges (IXPs), domain name system (DNS) service providers and Top Level Domain name registries, which can be exposed to breaches.

[70] Directives 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC, as listed in Annex XII, Part A, are repealed with effect from 21 December 2020, without prejudice to the obligations of the Member States relating to the time-limits for the transposition into national law and the dates of application of the Directives set out in Annex XII, Part B. Article 5 of Decision No 243/2012/EU is deleted with effect from 21 December 2020. References to the repealed Directives shall be construed as references to this Directive and shall be read in accordance with the correlation table in Annex XIII.

[71] European Commission, Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ((Communication) COM (2017) 10 final, 2017/0003(COD), 2017).

[72] "A service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services (…) which do not consist wholly or mainly in the conveyance of signals on electronic communications networks".

[73] "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of the recipient for services".

[74] Directive 98/48 EC amending Directive 98/34 EC laying down a procedure for the provision of information in the field of technical standards and regulations (the Transparency Directive).

Note that the EECC will broaden the definition of electronic communications service[75] to also contain internet access services and interpersonal communications services[76] in addition to those conveying signals and that it consequently introduces a more general meaning to remuneration[77] as one of the typical prerequisites to fall within the scope of the definition of electronic communications service [92].

The eIDAS Regulation is aimed at two addressees: e- identification schemes notified by the Member States, and providers of trust services[78] to the public established in the EU.
The PSD2 addresses payment service providers[79], payment institution services (PIS) i.e. third parties enabling online merchants to accept credit transfers, and account information services (AIS) that processes financial information on the payer's behalf (Art. 4(3) and Annex I PDS2).
The NIS Directive has two addressees: (1) ESOs and (2) three types of DSPs: search engines, online marketplaces and cloud computing (Art. 4(5) NIS Directive). The latter are three of the types of Information Society Services[80] offered in the EU.
Finally, the GDPR addresses any entity established in the EU that processes whosoever personal data, or any entity not established in the EU that offers goods or services to data subjects in the EU.

6.4.1.3 Goals of the EU legal framework

In every one of the six instruments, there is an obligation to maintain the security of the service provided by the addressee, followed by rules on the mitigation and notification of security breaches [88].

Nevertheless, in the remainder, the focus is on the Telecom Package and the NIS Directive, because their addressees could be directly involved in the provisioning of 5G telecommunications, and on the GDPR because of its horizontal obligations. For instance, providers of public electronic communications services also rely on cloud computing (providers) for parts of their services (e.g. email) as ENISA notices that *"the NIS Directive and the new EECC converge on the incident reporting, as many cloud services of DSPs and digital infrastructure of ESOs share common resources coming from telecom providers."* [93].

---

[75] While "conveyance of signals" remains an important parameter for determining the services falling into the scope of this Directive, the definition should cover also other services that enable communication. From an end-user's perspective it is not relevant whether a provider conveys signals itself or whether the communication is delivered via an internet access service (Recital 15 EECC).
[76] Interpersonal communications services are further subdivided in "number-dependent" and "number-independent" services. The former include standard telephony services, while the latter encompasses the so-called over-the-top services like Skype, WhatsApp and others.
[77] In line with the jurisprudence of the Court of Justice of the European Union on Article 57 TFEU, remuneration exists within the meaning of the Treaty also if the service provider is paid by a third party and not by the service recipient (Recital 16 EECC).
[78] A trust service is an electronic service consisting of the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, and certificates for website authentication, as well as the preservation of electronic signatures, seals or certificates concerning those services (Art. 3(16) eIDAS Regulation)
[79] These include: traditional banking institutions; electronic money institutions; post office giro institutions; payment institutions, like credit card companies, money remittances and forex services; and, under certain circumstances, the ECB, national central banks, as well as Member States and their regional entities (Art. 1(a) to (e) and Recital 24 PSD2).
[80] These are defined in the amended e- Commerce Directive; Directive 2015/1535/EU of the European Parliament and of the Council of 9 September 2015 Laying down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society services (codification), OJ L 241.

The provisions in these four instruments first aim at prevention and mitigation of security breaches; art. 13(a)(1) of the Framework Directive; Art. 4(2) of the e-Privacy Directive; Art. 14(2) of the NIS Directive and Art. 32(1)(c) of the GDPR.

Subsequently, they require appropriate technical and organizational measures to ensure a sufficient level of security relevant to the risk i.e. implying a risk-based approach; Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; Arts. 14(1) and 16(1) of the NIS Directive and Art. 32(1) of the GDPR.

As a third provision, these instruments introduce the notification to a supervisory authority of a breach of security that is likely to cause significant harm to services or individuals[81]; Art. 13(a)(3) of the Framework Directive; Arts. 14(3) and 16(3) of the NIS Directive (names the CSIRT as an alternative to the competent authority[82]) and Art. 33 of the GDPR.

Note that in the EECC the notification provision is broadened with regards to threats[83].

Unfortunately, none of the instruments provide a definition of "significant" or threshold values to determine it. Implementing acts sometimes supplement primary legislation such as Art. 4.1 of Regulation 2018/151[84] concerning Art. 16 of the NIS Directive regarding when an incident shall be considered as having a substantial impact[85].
ENISA and its Art. 13(a) Working Group have provided non-mandatory guidance on relevant criteria [94], just as the Cooperation Group will issue guidelines for ESOs regarding the notification of incidents [95].

Porcedda points out that although the exact wording in the instruments differs with regards to breaches (i.e. "breach of security" in Art. 2(h)(i) of the e-Privacy Directive and Art. 4(12) of the GDPR, "security incidents" in Art. 13(a)(1) and "breach of security or loss of integrity" in Art. 13(a)(3) of the Framework Directive and "breach" in Art. 15(4) and Recital 63, and "incident" in Art. 4(7) of the NIS Directive) the regulatory framework converges on the meaning of breach of security, and its overall goal is to pursue network and information security as a component of cyber security [88]. In which case network and information security concern the security canons: availability, authenticity, integrity and confidentiality. She further states that Art. 2.1 (b) of Commission Regulation 2018/151

[81] The e-Privacy Directive demands from providers notification of all instances relating to subscribers or individuals. This exception is removed in the proposed e-Privacy Regulation.
[82] Art. 1(2)(c) of the NIS directive requires creation of a computer security incident response teams network ('CSIRTs network') in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
[83] Member States shall ensure that in case of a particular and significant threat of a security incident in public communications networks or publicly available electronic communications services, providers of such networks or services shall inform their users potentially affected by such a threat of any possible protective measures or remedies which can be taken by the users. Where appropriate, providers should inform their users also of the threat itself (Art 40(3) EECC).
[84] Lex specialis to the NIS Directive.
[85] An incident shall be considered as having a substantial impact where at least one of the following situations has taken place: (a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes; (b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union; (c) the incident has created a risk to public safety, public security or of loss of life; (d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

clarifies that physical security should also be part of an "all-hazard risk-based approach" for network and information security [96].

Note that in Art. 40(2) of the EECC, as a revision of Art. 13(a) of the Framework Directive, the phrase "breach of security or loss of integrity" does not appear anymore as it now states "a security incident that has had a significant impact on the operation of networks or service" [92]. In which case significant concerns the same criteria[86] as in Art. 16(4) NIS Directive.

Furthermore as measures to counter the harms of breaches these instruments contain provisions regarding the keeping of inventories of the notification of breaches, liability and sanctions but they vary per instrument.

According to Art. 4(4) of the e-Privacy Directive the services must keep an inventory so the supervisory authority can verify compliance, whereas Art. 13(a)(3) of the Framework Directive requires the national regulatory authority to send a summary report of received notifications and actions taken to the Commission and ENISA once a year [97] [98], while Art. 10(3) of the NIS Directive requires the summary to be sent to the Cooperation Group in anonymized form by the single point of contact[87] who needs to be informed by the competent authorities or the CSIRTs.
Art. 33(5) of the GDPR requires the controller, i.e. the party who decides the purposes and means of the processing of personal data, alone or jointly with another controller (Art. 4(7)), to document any personal data breaches, its impact and the actions taken, making it possible for the supervisory authority to verify compliance.

Liability is not addressed in the Framework Directive, and the e-Privacy Directive refers to the liability contained in the Data Protection Directive[88].
According to Art. 14(3) of the NIS Directive "notification shall not make the notifying party subject to increased liability." Note that Recital 50 states that "While hardware manufacturers and software developers are not ESOs, nor are they DSPs, their products enhance the security of network and information systems. Therefore, they play an important role in enabling ESOs and DSPS to secure their network and information systems. Such hardware and software products are already subject to existing rules on product liability.
If the controller(s) prove that they are not in any way responsible for the event giving rise to the damage then under the GDPR they are exempt from liability. If not, the provisions in Art. 82 apply stating that "any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation." Processor(s), i.e. the material executor of the processing on behalf of the controller (Art. 4(8)), on the other hand are "liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or

[86] a) the number of users affected by the incident; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident; (d) the extent to which the functioning of the network or service is affected; (e) the extent of the impact on economic and societal activities.
[87] Art. 8(3) of the NIS Directive requires each Member State to designate a national single point of contact on the security of network and information systems ('single point of contact'). Member States may assign this role to an existing authority. Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact.
[88] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281, superseded by the GDPR.

where it has acted outside or contrary to lawful instructions of the controller"(Art. 82,). Liability may thus apply with or without intention i.e. negligence.

Regarding sanctions the e-Privacy Directive refers to sanctions stated in the nationally implemented Data Protection Directive, allowing pecuniary fines and other types of sanctions.
The GDPR allows for administrative fines, proportional to the degree of intention, negligence, and gravity of the omission, which can amount up to 20 million euro or four per cent of the total worldwide annual turnover of the fined party (Art. 83). For infringements which are not subject to administrative fines, the GDPR gives leeway to the Member States to establish other penalties (Art. 84).
The NIS Directive (Art. 21) and the Framework Directive (Art. 21) leave it to the Member States to decide on effective and dissuasive penalties.

6.4.1.4 Types of risk mentioned in the EU legal framework

The risks that the considered instruments mention are:

- The risk to the security of networks and services (Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; Arts. 14(1) and 16(1) of the NIS Directive and Art. 32(1) of the GDPR);
- The risk of damage to network and information systems security (Art. 4(9) NIS Directive);
- The risk for personal data and privacy (Recital 61 of the Citizens' Directive and Recital 85 of the GDPR);
- The risk to the rights and freedoms of natural persons, resulting from personal data processing, that may lead to damage (Recital 75 GDPR);
- Data (processing) security risk (Recital 83 GDPR).

None of the instruments states clearly how risks and related damage should be calculated. ENISA [98] and the Art. 29 Working Party[89] [99] have issued non-binding guidelines for the telecom sector [100]. In the case of the NIS Directive implementing act Regulation 2018/151 regarding Art. 16 of the NIS Directive provides further parameters for when an incident is to be considered as having a substantial impact.

6.4.2 ENISA

The European Union Agency for Network and Information Security (ENISA) promotes itself as a centre of expertise for cyber security in Europe contributing to a high level of network and information security within the Union and thus contributing to the proper functioning of the internal market since its founding in 2004 by European Regulation[90].

ENISA has a fixed-term mandate to support the development and implementation of the European Union's policy and law on matters relating to network and information security thereby working together with the Members States (e.g. establishing norms and threshold values for incident reporting in the Art 13(a) Framework Directive Working Group). Furthermore, ENISA produces

[89] The Article 29 Working Party was an advisory body made up of a representative from the Data Protection Authority of each EU Member State, the European Data Protection Supervisor and the European Commission. On 25 May 2018, it has been replaced by the European Data Protection Board (EDPB) under the GDPR.
[90] Regulation 460/2004/EC of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, OJ L 77.

guidelines and advises on several topics including the development of National Cyber Security Strategies, CSIRTs[91] cooperation and capacity building, but also studies on secure Cloud adoption, addressing data protection issues, emerging technologies, electronic IDs and trust services, and identifying the cyber threat landscape. Some of these ENISA products are regarded as “soft law”.

With the Cybersecurity Act,[92] the role of ENISA is to be strengthened as a permanent[93] EU cybersecurity[94] agency, assisting with the development of international standards, and supervising the voluntary Union-wide cybersecurity certification framework to increase the cybersecurity of products and services as well as coordinate response to large-scale cybersecurity incidents and crises. Discussions on the implementation and impact of the Cybersecurity Act, between ENISA, the Member States and the sector are underway [101].

6.4.3 NL legal framework for 5G

European Directives are transposed into Dutch law. The Framework Directive and the e-Privacy Directive into the Dutch Telecommunications Act (*Telecommunicatiewet* - Tw) [102], and the NIS Directive into *Wet beveiliging netwerk- en informatiesystemen* (Wbni) [103]. As a Regulation, the GDPR is immediately binding throughout the EU since May 25th 2018, but it gives the Member States some leeway in about thirteen provisions. NL has taken this liberty to attune it to national insights in the GDPR Implementing Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*) [104].

6.4.3.1 Dutch Telecommunications Act (Tw)

From the moment that the EECC is officially published, NL will have two years to revise the Tw to reflect the contents of the EECC [6]. The following analysis examines the current Tw, but indicates where relevant changes are to be expected due to the EECC.

6.4.3.1.1 Addressees

The addressees of the Tw are “public electronic communications networks” and “publicly available electronic communications services” and constructs or associated facilities (Art. 2(1)(1) of the Tw). Note the explicit separate mentioning of “public electronic communications networks” in comparison to the Framework Directive.

With the EECC the addressees in the Tw will come to include the so-called over-the-top services.

6.4.3.1.2 Goals of the Tw

The Dutch Telecommunications Act (Tw) aims to: protect the rights of Dutch citizens on all forms of digital communication, ensure a coherent infrastructure for telecom services, and regulate the free competition of these services.

Until the Tw is repealed the relevant features for 5G are:

- The addressees are to register with ACM (chapter 2);
- The regulatory framework for use of radio spectrum (chapter 3);

[91] Computer Security Incident Response Teams
[92] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'') COM/2017/0477 final - 2017/0225 (COD).
[93] The European Parliament, the Council of the European Union, and the European Commission have reached a political agreement on the Cybersecurity Act on 10 December 2018 [110].
[94] Here cybersecurity seems to mean information (systems) security in contrast to Van den Berg et al [20].

- The regulatory framework for laying network cables in public grounds (chapter 5);
- The requirements for radio equipment (chapter 10);
- Privacy and continuity clauses (chapter 11);
- The obligation for addressees to ensure that services offered to end users can be intercepted upon request by the competent authority (paragraph 13);
- Emergencies (chapter 14);
- Supervision (chapter 15);
- Provisions regarding the jurisdiction of authorities and links to European legislation (chapter 18 and 19).

For obligations to maintain the security of the service provided by the addressee, and the rules on the mitigation and notification of security breaches other than the European, the focus here is on chapter 11 of the Tw.

Art. 11.3(3) of the Tw contains the provisions aiming at prevention and mitigation of security breaches as the counterpart of art. 13(a)(1) of the Framework Directive; Art. 4(2) of the e-Privacy Directive; Art. 14(2) of the NIS Directive and Art. 32(1)(c) of the GDPR.

Arts. 11.3(1) and 11a.1(1) of the Tw require appropriate technical and organizational measures to ensure a sufficient level of security relevant to the risk as a counterpart to Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; Arts. 14(1) and 16(1) of the NIS Directive and Art. 32(1) of the GDPR.

Nevertheless, three specific demands are stated, with regards to personal data, in Art. 11.3(2) of the Tw, providers must, in any case, ensure that only authorized personnel has access to personal data, that stored and sent personal data are protected and that there is a security policy.

Art. 11a(2)(1) of the Tw resonates the provisions of the notification to a supervisory authority of a breach of security or loss of integrity that is likely to cause significant harm to services or individuals as in Art. 13(a)(3) of the Framework Directive; Arts. 14(3) and 16(11) of the NIS Directive and Art. 33 of the GDPR.

Art. 11.3(4) of the Tw announces the possibility of the issuance of a general administrative order to impose further obligations and restrictions on the providers, for the sake of the protection of personal data and the protection of the privacy of subscribers and users, for the safety and security of the networks and services offered.

6.4.3.1.3 Types of risk identified in the Tw

The risks that the Tw mentions, other than identified earlier in the European instruments, are:

- The risks to the existing physical infrastructure (e.g. electronic communication networks, antenna sites) due to sharing (i.e. risks to the integrity and security of existing networks or critical national infrastructure, risks of serious disruption, risks to safety or public health) (Art. 5a.4(2) of the Tw);
- Equipment causing risk to the health or safety of persons or to the protection of general interests or that cause inadmissible impediments in the ether or in other devices or radio equipment (Art. 10.8(2) of the Tw);
- The risks to safety in and at the antenna site, insofar as they are important for the continuity of the dissemination of programs by means of public electronic communication networks that are supported by that site (Art. 11a.3(1) of the Tw).

Note that telecommunications networks are part of vital national Infrastructure in NL as they are considered fundamental to economic success and they support every aspect of public and private life. As a consequence since December 2017, a duty applies on a provider of an electronic communications network or service that manages a network or infrastructure that is used directly or indirectly for the purpose of providing a telephone, SMS or internet access service to at least 1.000.000 end-users to report serious ICT incidents [105]. This obligation has become part of the Wbni requirements (see next paragraph).

6.4.3.2 Wet beveiliging netwerk- en informatiesystemen (Wbni)

NL has transposed the NIS Directive into the *Wet beveiliging netwerk- en informatiesystemen* (Wbni) [103] and the Wbni has entered into force on November 9th 2018.

6.4.3.2.1 Addressees

The Wbni specifies as the addressees vital providers; which consists of ESOs (Art. 5.1(a) of the Wbni) and providers of other services whose *continuity* is of vital importance for Dutch society (e.g. providers of an electronic communications network or service to at least 1.000.000 end-users) (Art. 5.1(b) of the Wbni) and DSPs conform Annex III of the NIS Directive: search engines, online marketplaces and cloud computing (Art. 4.2 of the Wbni).

The appointed ESOs in NL are to be found in the sectors energy (electricity, gas, and oil), digital infrastructure (i.e. internet exchanges, domain name registrars, DNS[95] services providers), transport, banking and financial market infrastructure, drinking water supply and distribution [106].

Other vital providers concern those in the sectors nuclear, flood defense systems or parts thereof, financial services and electronic communication networks and services / ICT [106].

The definitions in Annex III of the NIS Directive regarding DSPs are further specified by the Ministry of Economic Affairs and Climate Policy to entail companies with more than 50 employees or an annual turnover of more than 10 million Euro, and for instance that cloud computing services are to be divided into three main categories: Software as a Service (SaaS[96]), Platform as a Service (PaaS)[97] and Infrastructure as a Service (IaaS)[98] [107].

6.4.3.2.2 Goals of the Wbni

The goal of the Wbni is to prevent or limit the unavailability or loss of integrity of network and information systems of vital providers, and of other providers that are part of the national government, to further strengthen the digital resilience of Dutch society and to implement the NIS directive.

[95] Domain Name System (DNS) is a hierarchical decentralized naming system for resources (e.g. computers) connected to the Internet.
[96] Software as a Service (SaaS): an "online" application that can be operated from a web browser, location and time independent (e.g. a financial package, online office) [112].
[97] Platform as a Service (PaaS): an "online, organized" platform on which the user or customer can run their own software services or platforms that offer specific functionality (e.g. a "virtual PC with an operating system", an authentication platform or a storage) [112].
[98] Infrastructure as a Service (IaaS): the virtual hardware layer in which the user or customer can create and manage their own networks, storage, servers and workstations (e.g. virtual workspaces, data storage, network equipment). Here the user or customer can install their own operating systems and configurations [112].

Clearly, the implementation in NL takes a different approach than set in the NIS Directive. If this is the same in the other Member States it may hamper communication, cooperation and reaching the objectives of the NIS Directive across the EU.

6.4.3.2.3 Types of risk identified in the Wbni

Other than the risk identified earlier in the NIS Directive (i.e. risk to the security) it is noted that the Wbni also identifies risks to the continuity of vital providers (Art. 10 of the Wbni).

Note that in Art. 10.3 of the Wbni it is demanded only from the provider of an essential service to report an incident at a digital service provider without delay, if that incident has significant consequences for the continuity of its essential service and even if that digital service provider does not fall under the jurisdiction of the Netherlands (Art. 10.5 of the Wbni). Consequently, this is no obligation for the other vital providers such as providers of an electronic communications network.

6.4.3.3 UAVG

In NL the GDPR Implementing Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG)*) became effective on May 22nd, 2018 repealing the Dutch data protection Act (*Wet bescherming persoonsgegevens*). The UAVG has some particularities compared with the GDPR.

According to Art. 2.2(a) of the GDPR it does not apply to the processing of personal data which falls outside the scope of Union Law. This provision is reversed in the UAVG (Art. 3.1(a) of the UAVG).

Besides the standard provisions, the GDPR demands from national or competent authorities to take action in the establishment of a list of processing operations for which a data protection impact assessment is (not) required (Art. 35(4) GDPR) and processing of personal data for journalistic purposes and the purposes of academic, artistic or literary expression (Art. 85 GDPR). To this regard, the UAVG states that many provisions and sections of the GDPR do not apply to processing activities for solely journalistic, academic, artistic or literary purposes.

National or competent authorities are allowed to take action in several other areas: age limit for consent by children (Art. 8 GDPR); specific requirements for the application of certain processing grounds (Art. 6 GDPR); processing of sensitive data (Arts. 9 and 10 GDPR), NL has used this discretionary authority to include specific provisions to adopt legislation permitting or conditioning the processing of sensitive data, in particular genetic data, biometric data (for authentication or security purposes (Art. 29 of the UAVG)) and data concerning health; automated decision-making (Art. 22 GDPR), in NL the UAVG states that the right not to be subject to automated decision-making is waived if such decision-making is necessary to comply with a legal obligation or to perform a task in the public interest (Art. 40 of the UAVG); restrictions on the rights of data subjects (Art. 23 GDPR), NL may restrict the rights of data subjects and the controller's obligations in this regard, provided such restrictions are in accordance with fundamental rights and freedoms and are necessary and proportionate measures to safeguard a democratic society; adoption or approval of compliance instruments (Art. 57 GDPR); prior consultation (Art. 36.5 GDPR); processing of national identification numbers (Art. 87 GDPR), the UAVG provides that a national identification number may only be processed in order to comply with the law or for purposes provided by law; and processing in the context of employment (Art. 88 GDPR), NL has introduced restrictions on the rights of data subjects with regard to processing activities for archiving, scientific or historical research, or statistical purposes.

6.4.4 Risks and Controls in the legal framework for 5G

With regards to the legal framework for 5G in NL, as transposition of the Framework Directive, the e-Privacy Directive and the NIS Directive, the Tw, the Wbni and the UAVG provide provisions to the

supervisory bodies that can be of use as basic preventive or corrective controls for the identified risks. Since these risks and controls are stated in general terms further assessment from the supervisory bodies will need to determine exact applicability.

An overview of the identified risks and controls for the legal framework for 5G in NL is presented.

Identified risks:

- The risk to the security of networks and services (Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; Arts. 14(1) and 16(1) of the NIS Directive and Art. 32(1) of the GDPR);
- The risk of damage to network and information systems security (Art. 4(9) NIS Directive;
- The risk for personal data and privacy (Recital 61 of the Citizens' Directive and Recital 85 of the GDPR);
- The risk to the rights and freedoms of natural persons, resulting from personal data processing, that may lead to damage (Recital 75 GDPR);
- Data (processing) security risk (Recital 83 GDPR);
- The risks to the existing physical infrastructure (e.g. electronic communication networks, antenna sites) due to sharing (i.e. risks to the integrity and security of existing networks or critical national infrastructure, risks of serious disruption, risks to safety or public health) (Art. 5a.4(2) of the Tw);
- Equipment causing risk to the health or safety of persons or to the protection of general interests or that cause inadmissible impediments in the ether or in other devices or radio equipment (Art. 10.8(2) of the Tw);
- The risks to safety in and at the antenna site, insofar as they are important for the continuity of the dissemination of programs by means of public electronic communication networks that are supported by that site (Art. 11a.3(1) of the Tw);
- The risks to the continuity of vital providers (Art. 10 of the Wbni).

Preventive controls:

- Duty of care i.e. appropriate technical and organizational measures to ensure a sufficient level of security relevant to the risk (Art. 13(a)(1) and (2) Framework Directive; Art. 1 and 1(a) e-Privacy Directive; Arts. 11.3(1) and 11a.1(1) of the Tw; Art. 14(1) and 16(1) NIS Directive;
- Prevent breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) ePrivacy Directive; Art. 11.3(3) of the Tw; Art. 32(1)(c) GDPR, and Art. 14(2) NIS Directive;

Recovery controls:

- Mitigate breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) ePrivacy Directive; Art. 11.3(3) of the Tw; Art. 32(1)(c) GDPR, and Art. 14(2) NIS Directive);
- Notification of the supervisory authority (always, without undue delay, if related to individuals or subscriber (e-Privacy Directive); if likely to cause harm to services of individuals (Art.33 GDPR (within 72 hours)); Art. 13(a)(3) Framework Directive (without undue delay); Art. 11a(2)(1) of the Tw and Art. 14(3) and 16(11) NIS Directive (without undue delay));
- Notification of the data protection authority (Art.33 GDPR);
- Notification of law enforcement authority (Art. 13(a)(3) Framework Directive);
- Notification to natural persons (when their rights are likely to be affected by the breach (Art. 4 E-Privacy Directive) or there is a high risk thereof (Art. 34(1) GDPR));
- Disclosure of breach to the public (at the discretion of the supervisory authority (Art. 13(a)(3) Framework Directive).

6.5 Summary

According to Lessig [78] a regulatory environment is composed of architecture, markets, social norms and legal aspects.
The ITU, the IETF, 3GPP, IEEE, 5G-PPP have a decisive influence on the architecture of 5G.
Market players united in NGMN Alliance, GSMA, and SIMalliance try to shape the resulting form of 5G from a business (i.e. cost and benefits) perspective. In the meanwhile social norms have come to demand that everybody is ubiquitously connected, there is virtually no latency and telecommunication systems are “green”.
The legal framework in NL for the cyber security of 5G is dominated by the EU Framework Directive (to be repealed by the EECC on 21 December 2020), the e-Privacy Directive and the NIS Directive, because their addressees (i.e. electronic communications services providers, ESOs and DSPs) could be directly involved in the provisioning of 5G telecommunications, and by the GDPR because of its horizontal obligations. These instruments are transposed into the NL laws Tw, Wbni and UAVG and adjusted to national preferences. The main risks identified are damage to the security of networks, information systems, services, personal data and privacy. Wbni also identifies risks to the continuity of vital providers and appoints telecommunications networks part of vital national Infrastructure in NL. The legal provisions aim in the first place at prevention and mitigation of security breaches, appropriate technical and organizational measures to ensure a sufficient level of security relevant to the risk and a notification to a supervisory authority of a breach of security that is likely to cause significant harm.
In cyber security supervision of 5G with a risk-driven approach, these provisions can be used as preventive and corrective controls.
ENISA has a mandate to support the development and implementation of EU policy and law relating to network and information security. ENISA facilitates working groups with Member States and produces i.a. guidelines and advises on several topics some of which are regarded as “soft law”.

7. Supervisory authorities for 5G in NL

It is examined who the competent authorities for supervision of 5G cyber security are in NL related to the transposed European instruments (i.e. in the Tw and the Wbni) and the GDPR.

7.1 Dutch Telecommunications Act (Tw)

The Dutch Telecommunications Act (*Telecommunicatiewet* - Tw) [102] dedicates chapter 15 to supervision, appointing the authorities AT, AP and ACM to play a role in supervision.

7.1.1 AT

By ministerial decree [108] the Radiocommunications Agency of the Ministry of Economic Affairs and Climate Policy - *Agentschap Telecom* (AT) is the designated supervisory body (Art. 15.1(1) of the Tw) for:

a. the use of frequency space;
b. the provision of data for the antenna register referred to in Art. 3.23;
c. prioritization of emergency numbers as referred to in Art. 7.7, third or fourth paragraph;
d. technical regulations as referred to in Article 8.4a (i.e. regarding television broadcasts);
e. obligations concerning the broadcasting of program offers, imposed on the basis of Art. 8.3;
f. equipment or requirements regarding radio equipment as provided for in Chapters 10 and 20;
g. the use of traffic data and location data as regulated in Arts. 11.5, 11.5a and 11.13 respectively;
h. legal interception (i.e. authorized tapping) and storage of data as regulated in Chapter 13;
i. extraordinary circumstances as regulated in Chapter 14;
j. further topics as referred to in Arts. 11a.1, 11a.2, 11a.3 (regarding continuity), 12.6 (dispute resolution), in so far as it concerns powers of Our Minister, Art. 18.2 (necessary decrees for implementing European directives), in so far as it concerns powers of Our Minister, Art. 18.4, second paragraph (compliance with the International Telecommunication Convention regarding frequency usage), Art. 18.7 (obligation to provide requested information), insofar as it concerns powers of Our Minister, Arts. 18.9, 18.12 (possibility of binding instructions to providers), in so far as it concerns powers of Our Minister, Arts. 18.16, 18.17, 18.17a (regarding eIDAS qualified means), 20.2 (regarding licenses), in so far as it concerns powers of Our Minister, and Art. 20.14 (expired);
k. the provision of trust services by trust service providers established in the Netherlands as provided for in chapter III of the eIDAS regulation, including the annexes referred to in that chapter, and Art. 18.15a, insofar as it concerns Our Minister, Arts. 18.15b and 18.15e, and Art. 18.18 of this law.

Article 11a.(2)(1) of the Tw demands notification to AT without delay from the providers of public electronic communication networks and public electronic communication services of (a) a breach of security, (b) a loss of integrity, as a result of which the continuity of public electronic communication networks and public electronic communication services was interrupted to a considerable extent.

7.1.2 AP

According to Art. 15.1(2) of the Tw the officials appointed by the Data Protection Authority - Autoriteit Persoonsgegevens (AP) shall be charged with supervising compliance with the provisions under or pursuant to Arts. 11.3a (regarding the notification of personal data breaches) and 11.5b (for processing trust services) and, in so far as it infringes the security or loss of integrity that has

significant consequences for personal data, the provisions in and pursuant to Art. 18.15a and Art. 19, second paragraph of the eIDAS Regulation.

7.1.3 ACM

Art. 15.1(3) of the Tw states that ACM is charged with supervising compliance with the provisions in or pursuant to other provisions in the Tw than referred to in Arts. 15.1(1) and (2) and the provisions under or pursuant to the "Roaming Regulation"[99] and the "Net Neutrality Regulation"[100]. The previous sentence does not apply to the provisions under or pursuant to articles 5.1, 5.4, 5.5, 5.6, second, third paragraph, fourth and fifth paragraphs, 5.7, 5.13 (regarding cabling in public areas), 5.14 (regarding public bodies as provider) and 5a.6 (network operator coordinating license sharing) of the Tw and insofar as Our Minister is the addressee.

It can be concluded that ACM is charged with supervision of the market regulating aspects of the Tw, roaming provisions, net neutrality requirements (i.a. user experienced data rates) and the protection of privacy in electronic communications (e.g. against spam and cookies).

7.2 Wbni

The *Wet beveiliging netwerk- en informatiesystemen* (Wbni) appoints as national supervisory authorities for ESOs, conform Art. 8.1 of the NIS Directive, the minister of Economic Affairs and Climate Policy for energy and digital infrastructure, the minister of Healthcare for the health sector, the minister of Infrastructure and Water Management for drinking water supply and distribution, and the Dutch Central Bank for banking and financial market infrastructure (Arts 4.1 of the Wbni).

The minister of Economic Affairs and Climate Policy is also appointed the national supervisory authority for DSPs (i.e. cloud computing services, online marketplaces, online search engines) (Art. 4.2(a) of the Wbni).

The minister of Economic Affairs and Climate Policy has delegated his supervisory authority with regards to Arts. 4.1 and 4.2(a) of the Wbni to the Radiocommunications Agency of the Ministry of Economic Affairs and Climate Policy - *Agentschap Telecom* (AT) [109].

The Wbni also assigns, conform Art. 1.2(c) of the NIS Directive, the role of CSIRT for ESOs to the Ministry of Justice and Security (Art. 2(b) of the Wbni) which is delegated to the National Cyber Security Center (NCSC) [106], and the role of CSIRT for DSPs (Art. 4.2(b) of the Wbni) is assigned by decree to the Ministry of Economic Affairs and Climate Policy [110].

7.3 UAVG

In accordance with Art. 51.1 of the GDPR, the Dutch GDPR Implementing Act (Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) appoints Autoriteit Persoonsgegevens (AP) (i.e. the Dutch data protection authority) as the supervisory body (Art. 6.2 of the UAVG).

[99] Regulation (EU) 2017/920 of the European Parliament and of the Council of 17 May 2017 amending Regulation (EU) No 531/2012 as regards rules for wholesale roaming markets, OJ L 147.
[100] Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union, OJ L 310.

Art. 19 of the UAVG encourages AP to seek cooperation with other supervisory bodies in the interests of efficient and effective supervision of the processing of personal data.

7.4 Summary

The Tw appoints the authorities AT, AP and ACM to play a role in supervision.
AT is the designated supervisory body for among more the use of frequency space, equipment or requirements regarding radio equipment, authorized tapping, and the continuity of public electronic communication networks and public electronic communication services.
AP is charged with supervising compliance regarding the notification of personal data breaches.
ACM with regards to market regulating aspects of the Tw, roaming provisions, net neutrality requirements (i.a. user experienced data rates) and the protection of privacy in electronic communications (e.g. against spam and cookies).
The Wbni appoints as national supervisory authorities for DSPs (i.e. cloud computing services, online marketplaces, online search engines) and for ESOs. The most relevant for 5G cyber security is the minister of Economic Affairs and Climate Policy who has delegated this supervisory authority to AT.
The Wbni assigns the role of CSIRT for ESOs to the Ministry of Justice and Security which is delegated to the NCSC, and the role of CSIRT for DSPs is assigned to the Ministry of Economic Affairs and Climate Policy. The UAVG designates only AP as the supervisory body.

Part 4. Cyber security supervision of 5G in NL

8. Cyber security supervision framework in NL

This chapter is about the current framework for cyber security supervision in NL. Is it properly arranged to ensure trust in 5G? What are the limitations and can the requirements for an improved supervision model be identified?

8.1 What is supervision?

In classical regulation supervision consists of three important parts; a norm or standard the regulateees need to abide by, information gathering and monitoring of compliance by the supervisory body and behaviour modification in case of non-compliance [15]. Correspondingly the Dutch Ministry of the Interior and Kingdom Relations states that: "*Supervision is to collect information on whether an action or item meets the relevant requirements, then forming an opinion about it and if necessary intervene in consequence."* [111].

Furthermore, good supervision stays within legislative mandate and intent, follows due process, reflects expertise and is efficient [15]. Accordingly, Roger Brownsword points out "*that regulators dealing with new technologies face the challenges of regulatory prudence, regulatory legitimacy, regulatory effectiveness and regulatory connection"* [112].

In its 2013 report *Supervising public interests - Towards a broader perspective on government supervision* [113] the Dutch Scientific Council for Government Policy (WRR[101]) states that supervision plays an important role in safeguarding public interests and achieving policy objectives but the emphasis on the costs of supervision and enforcement has placed supervision in a negative light, resulting in damage to public interests and depreciation of the social added value of supervision. The WRR calls for *"focusing on the public interests to be served, highlighting and substantiating the societal benefits of supervision in relation to the costs, clarifying the role of supervision in a complex field of influences, and improving the role that supervision plays in reflection and in drawing attention to problems…."*

The Dutch Cabinet supports this call in its reaction to this WRR report and argues to see the (further) development of this insight, i.e. governance based supervision, and the cooperation of different supervisory bodies, as an important task for supervisory bodies for the coming years [114].

In its 2018 letter to the Dutch Cabinet on the Supervision Innovation Program for the next years, the Inspectieraad (Dutch Inspection Council) states among more that the aim is to operate more data-driven, but above all the principle of risk-driven approach remains paramount because only then can limited public funds be used as effectively as possible [115].

8.2 The objective of 5G cyber security supervision

Aligning the definition of supervision from the Ministry of the Interior and Kingdom Relations (i.e. "*to collect information on whether an action or item meets the relevant requirements, then forming an opinion about it and if necessary intervene in consequence"*) with the opinion of the WRR (i.e.

[101] The Dutch Scientific Council for Government Policy (WRR) was founded as a temporary body in 1972. It was established as a permanent body by the Act of 30 June 1976 (Staatsblad, 413). Pursuant to the Act, the Council's task is to advise the Dutch government by providing evidence-based information on trends and developments that may have a long-term impact on society. It is the Council's duty to point out contradictions and anticipate problems at the earliest possible stage, to identify problems related to major policy issues, and to propose policy alternatives.

supervision plays an important role in safeguarding public interests), the instructions from the Dutch Cabinet (i.e. governance based supervision, and cooperation of different supervisory bodies) and the intentions of the Inspectieraad (i.e. data-driven, but above all a risk-driven approach to supervision) it can be concluded that the objective of good NL 5G cyber security supervision (i.e. efficient, stays within legislative mandate and intent, follows due process, and reflects expertise) would be:

> To ensure the trustworthiness of 5G to its users and the public at large by applying (a) a risk-driven approach (b) in a cooperation of supervisory bodies to (c) collect information and monitor compliance with (d) the norms for cyber security, and (e) intervene in case of non-compliance.

Hurdles to the objective

Analyzing the objective of NL 5G cyber security supervision against the background of the provisions depicted in earlier chapters the following hurdles become apparent.

The risk-driven approach (a) applied by the supervisory bodies is limited to the own jurisdiction and does not take in to account cascading effects into other areas (see chapter 7). Sectoral regulation (e.g. aviation regulations for drones, regulations on medical applications) plays a dominant factor in determining if, and when, a particular 5G use case might take off. These regulations are often related to reliability and thus need to consider underlying 5G network reliability and sectoral supervisory bodies are not as well equipped to make assessments of network reliability as specialist telecom supervisory bodies [18].

With regards to (b) the cooperation of supervisory bodies it can be concluded that there is no legal provision for institutionalized collaboration specific to 5G cyber security yet between the NL supervisory bodies, and between NL supervisory bodies and foreign supervisory bodies[102] (see also chapter 6).

Information collection and monitoring of compliance (c) by the supervisory bodies are focused on regulatees in their own jurisdiction (see chapter 7). With the explosive increase of (sub-)providers in the 5G value chain, the international scope of 5G, the lack of jurisdiction over foreign 5G building blocks providers comes the danger of lack of overview and lack of cyber situational awareness, conform Endsley [116], among the 5G supervisory bodies in NL.

With regards to (d) norms: as identified in chapter 7, in the case of 5G cyber security the legislator has sufficed with open norms (i.e. appropriate technical and organizational measures) in the Tw, the Wbni and the UAVG.
Faced with this precondition, 5G supervisory bodies are called to open norms supervision, i.e. supervision based on a preferably internationally recognized standard (e.g. ETSI) that is established in

[102] It must be noted that the website of AT mentions cooperation protocols on other grounds between AT and ACM (e.g. Arts 2.1, 15.1, 16.1(4) of the Tw)) [118], AT and Commissariaat voor de Media (Dutch Regulatory Authority for the Media) [119] [120], and between AT and AP [121], and to inform each other about matters that may be relevant for the exercise of the functions of the other party, without prejudice to his responsibility under the law. Also on a higher governance level the supervisory bodies can as members of the Inspectieraad (Dutch Inspection Council) participate in the joint work agenda and in the so-called do-coalitions in which the cooperation around a specific theme is organized [115].

cooperation with the relevant stakeholders (e.g. ENISA) or in absence thereof based on agreements with the regulatees (e.g. using ENISA guidelines, AT has established an agreement with 4G Telecom providers on the details regarding the duty of care provision in Art. 11(a) Tw [117]).

Regarding (e) intervening in case of non-compliance, the danger of oversight deficit arises i.e. inconsistency of supervisory actions across regulatory domains [15].

8.3 Requirements for an improved supervision model

To address the identified challenges and overcome the hurdles, in an improved conceptual model for 5G cyber security supervision, the following corresponding requirements are derived:

(a) Deploying a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors;

(b) Cooperation between relevant NL 5G supervisory bodies, between NL and European[103] 5G supervisory bodies (and ENISA), and between NL and non-European[104] supervisory bodies;

(c) Collection of information by sector-specific supervisory bodies to address the dissemination of providers and subcontractors, relevant information dispersed to supervisory bodies (and stakeholders) to create cyber situational awareness, and monitoring of compliance coordinated between collaborative 5G supervisory bodies by AT to gain overview;

(d) Supervisory bodies to fill in the open norms on 5G cyber security with their sector and harmonize them across the supervisory bodies (see also (b));

(e) Intervening by the supervisory bodies based on the identified controls in legislation and supplementary supervisory controls developed in close cooperation with all involved supervisory bodies with consideration of adjacent sectors.

In the next chapters, these requirements are explored in the design of an improved conceptual model for 5G cyber security supervision from a classical regulation perspective (i.e. governmental supervision).

8.4 Alternatives to classical regulation

A brief account on self-regulation and market-based regulation is presented in the following paragraphs, since it could be considered to implement some of the requirements for an improved model for 5G cyber security supervision in one of these forms.

Lodge and Wegrich offer three alternatives to classical regulation (i.e. supervision by governmental authorities) [15], namely architecture, self-regulation and market-based regulation. The architecture alternative is elaborated on in an earlier chapter conform Lessig [78].

In its letter to the Cabinet, the Inspectieraad (Dutch Inspection Council) announced to explore the role many forms of private supervision, such as accreditation, certification and international quality certificates can play in public supervision [115].

[103] Recital 98 and Art. 40(1) of the EECC and Recital 4 of the NIS Directive mention the cooperation between European supervisory bodies and ENISA in this regard.
[104] Non-European cooperation, based on Art. 218 TFEU, is mentioned in Art. 13 of the NIS Directive.

Self-regulation

Self-regulation is the reliance on regulatees to behave responsibly in the light of wider public policy goals and in accordance with their own normative framework [15]. The advantage of self-regulation is the dissolvement of the information asymmetry between supervisory body and regulatees. Professional self-regulation is when an individual professional is bound by the code of the profession (e.g. certified information systems security professionals).

In industry self-regulation branch organisations monitor if their member firms adhere to self-developed industry policies and standards. There is hardly any enforcement from external supervisory bodies.

Co-regulation, a form of “soft law”, concerns the set-up of a normative framework in an industry as part of a legal (supervisory) regime and where the supervisory body backs this with its authority.

Market-based regulation

By appealing on commercial self-interest (via e.g. minimum or maximum price levels, tradable permits, subsidies, taxation) regulatory goals can be achieved without formal regimes. Other market mechanisms are the provisioning of information regarding the quality of services (e.g. “naming and shaming”), and the issuing of quality certificates to exploit stakeholder interest and choice.

8.5 Summary

In classical supervision, there is a norm regulatees abide by, information collection and monitoring of compliance, and intervention by a supervisory body. While good supervision stays within legislative mandate and intent, follows due process, reflects expertise and is efficient.

Based on statements from the Ministry of the Interior and Kingdom Relations, the WRR, the Dutch Cabinet and the Inspectieraad (Dutch Inspection Council) it can be concluded that the objective of good NL 5G cyber security supervision (i.e. efficient, stays within legislative mandate and intent, follows due process, and reflects expertise) would be the cooperation of supervisory bodies to ensure the trustworthiness of 5G to its users and the public at large by applying a risk-driven approach to information collection and monitoring of compliance with the norms for cyber security, and intervening in case of non-compliance.

Analyzing this objective against the regulatory environment and provisions the limitations are identified and subsequently the requirements for an improved model for 5G cyber security supervision are derived.

In the next chapters, these requirements are explored in the design of an improved conceptual model for 5G cyber security supervision.

9. Risk assessment of cyber security supervision of 5G in NL

The first requirement derived in the previous chapter for an improved conceptual model for 5G cyber security supervision is explored from a risk management perspective considering the identified 5G challenges and the regulatory environment.

9.1 Context

The first identified requirement for an improved conceptual model for 5G cyber security supervision in paragraph 8.3 is (a) the deployment of a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors.

In this assessment the objectives are to identify, assess and analyse risks related to the compromise of an end to end multi-stakeholder[105] 5G System and propose controls for the designated supervisory body within a suitable risk treatment strategy from a governance perspective.

The provisioning of 5G is modelled according to the conceptualized cyberspace model of Van den Berg et al.[106] [20]. Van den Berg et al. state that *"information security breaches occur in the technical layer while the true impacts (risks) of these breaches work out into the socio-technical layer of cyber activities."* [20]. This observation holds especially true for 5G where failing or absent (technical) controls will have a severe impact on cyber activities in the socio-technical layer of cyberspace.

The technical layer [20] is divided up to consist of two sub-layers: the 5G Provisioning Layer and the 5G Building Blocks Layer. The 5G Provisioning Layer[107] is the layer in which the providers of electronic communications networks are responsible for the availability and security of the 5G provision.

Since a 5G network can be composed of several building blocks due to virtualization and softwarization the 5G Building Blocks Layer is introduced. The 5G Building Blocks Layer[108] is made up of distinct components necessary for the provisioning of 5G such as cloud computing functionalities as in SDN, NFV and MEC, but also antennas, and sub-terrain cables for 5G backhaul[109].

The 5G Use Case Layer[110] is socio-technical layer conform Van den Berg et al. [20] where the users can enjoy the eMBB, URLLC and mMTC applications, functions and possibilities of 5G like for instance autonomous driving, industrial automation, virtual reality and remote surgery.

The 5G Supervision Layer resembles the governance layer in Van den Berg et al. [20] and is typically the layer from which the supervisory bodies oversee the technical and socio-technical layer. Figure 9.1 illustrates the 5G cyberspace model from a governance perspective.

---

[105] Stakeholder is a person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity (ISO 31000).
[106] Consists of the technology layer, the socio-technical layer enabling the (cyber) activities, and the governance layer in which governance of both the technical layer and the socio-technical layer take place.
[107] Note that this layer composes of the radio network, the business enabling layer and the end-to-end management and orchestration entity of the NGMN model [1].
[108] Note that this layer resembles, with the exception of the radio network, the infrastructure resources layer of the NGMN model [1].
[109] The 5G Building Blocks Layer can in itself also consist of a technical and a socio-technical layer, but at the proposed abstraction level for 5G governance it is considered one technical layer.
[110] The 5G Use Case Layer resembles the NGMN business application layer [1].

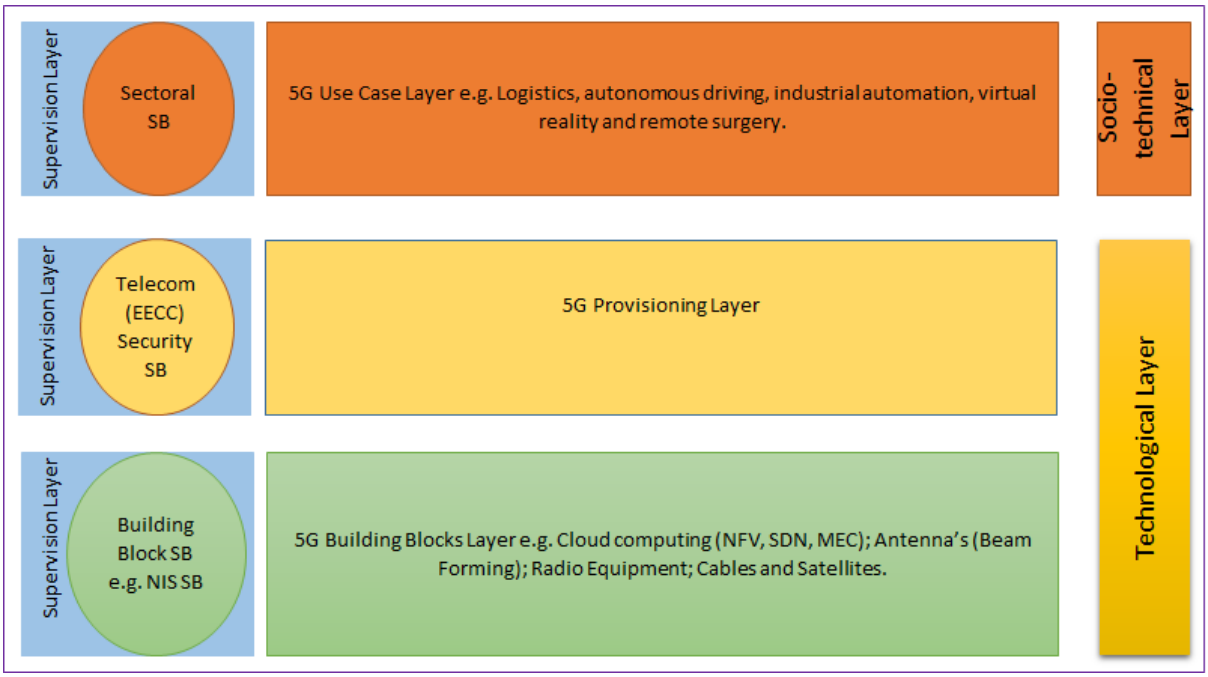


Figure 9.1 The 5G cyberspace model inspired by Van den Berg et al. [20].

The supervisory bodies are required to each focus on ensuring the security in their own sector with a risk-based approach. This invites the use of a risk management process with assessment, categorization and appropriate addressing of risks. Such an approach if further highlighted in the next paragraphs.

9.2 Approach

Based on ISO 31000 [122], the ISO/IEC 31010 [123] is a well-known framework for several methodologies in the domain of risk management. The iterative ISO/IEC 31010 risk management process is depicted in Figure 9.2.

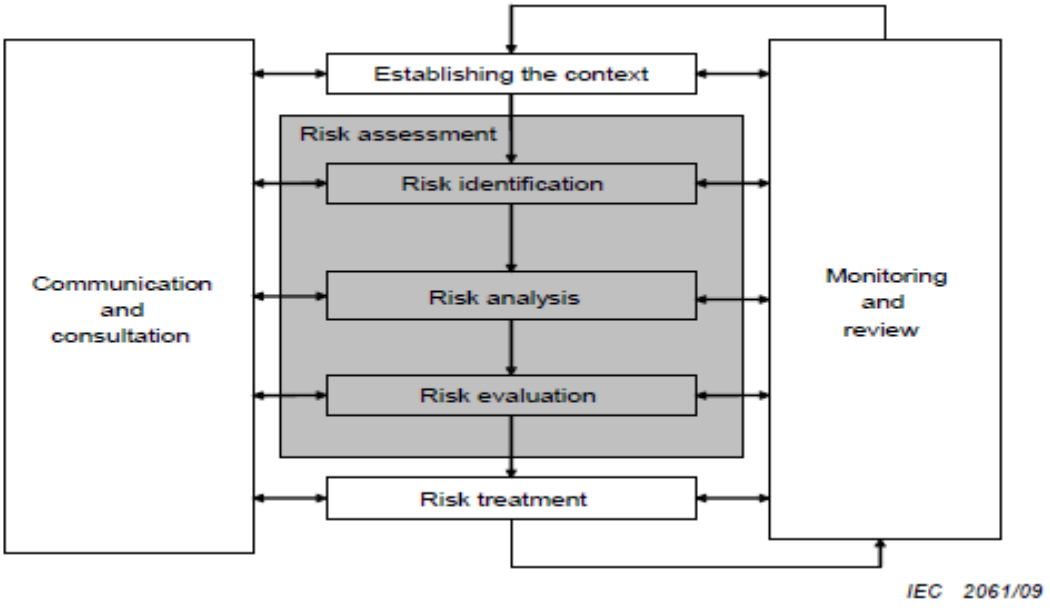


Figure 9.2 ISO/IEC 31010 risk management process [123].

In this risk management process the supervisory body strives to ensure trust in its sector by taking appropriate actions and demanding, where it deems necessary and so required by regulations, measures from supervised parties. The intent being that the supervision of each sector will inspire trust.

The risk management cycle proceeds continuously according to the well-known fixed steps:

1. Context definition;
2. Identify critical assets[111] (the so-called crown jewels);
3. Identify and Assess their risks;
4. Define acceptable risk levels;
5. Decide on manners of dealing with the risks:
    - accept, avoid, mitigate or transfer;
6. Design and Implement risk measures;
7. Monitor effectiveness.

Starting with the context, subsequently the critical assets and activities regarding 5G are identified per layer, and the related risks. Note that, because of the sector-specific focus, a supervisory body in the 5G Building Blocks Layer or the 5G Use Case Layer might be unaware of the criticality of assets and activities in his layer for other layers i.e. the end-to-end security of 5G (see Figure 9.1).

Defining the acceptable risk level is a crucial phase in which the supervisory body has to take cascading effects in other layers into consideration too, if there is to be integral security of 5G i.e. end-to-end security. Guidance has to be sought in for instance harmonized norms, the national 5G policy, international 5G performance guidelines and risk levels defined by supervisory bodies in other layers.

The supervisory body can take measures or require measures to be taken by the supervised parties in dealing with the identified risks (in steps 5 and 6), but again here coordination over all layers and cooperation between supervisory bodies is necessary for end-to-end security of 5G.

To achieve cyber security and ensure trust in the 5G Building Blocks Layer and the 5G Provisioning Layer, as representatives of the technical layer, the focus is on measures regarding the mitigation of risks to the typical information security canons confidentiality, integrity, authenticity and availability [20] aggregated to a macro level (from the supervisory bodies perspective).

On the other hand, in the 5G Use Case Layer the focus is on cyber activity-related measures i.e. measures mostly regarding the mitigation of risks concerning the behaviour of humans and non-human intelligent actors [20].

9.3 Risk identification

The various components that are important in determining the risks to the 5G System are explored.

Critical assets

From the perspective of the supervisory body overseeing 5G provisioning in NL, the critical asset in the 5G Building Blocks Layer is trust in the security of the 5G building blocks such as cloud computing services (e.g. MEC), antenna's, radio equipment, cables and satellites.

[111] Asset: An item, thing or entity that has potential or actual value to an organisation (ISO 27005) [124].

The critical asset in the 5G Provisioning Layer is trust in the security of the 5G provision, while the critical asset in the 5G Use Case Layer is trust in the security of the 5G applications, functions or services e.g. autonomous driving, industrial automation, virtual reality and remote surgery.

Actors

It is expected that there will be many parties involved in the make-up of the 5G System as a whole. An overview of the actors in the 5G System (compared to 4G) is presented in Table 9.1 [52].

5G Actors	
• Network equipment manufacturer	o Terrestrial equipment manufacturer o [5G] Satellite equipment manufacturer
• Infrastructure Provider	o [5G] Virtual infrastructure provider (VIP), providing infrastructure as a service (IaaS) o [5G] Satellite/HAPS provider
• Network software provider; commonly also the network equipment manufacturer	o [5G] Virtual network function (VNF) provider
• Interconnect network provider (provides a network linking one network operator to another)	
• Mobile Network Operator (MNO) (taking the role of “home” or “serving” operator); commonly also the infrastructure provider	o Virtual mobile network operator (VMNO) who purchases bulk capacity from MNOs and may (or may not) have their own HSS o [5G] Virtual mobile network operator (VMNO) who purchases SDN slices from an Infrastructure Provider o [5G] Factory or enterprise owner operating a AAA in a network linked to a (V)MNO
• [5G] Satellite Network Operator; commonly also the satellite/HAPS provider	
• [5G] Network access provider (uses the services from one or more Satellite/Mobile Network Operators to provide bulk transmission resources to Service Providers)	
• Service Provider; commonly also the (V)MNO	o [5G] over-the-top (OTT) service provider
• User equipment manufacturer	o Phone manufacturer o USIM manufacturer o [5G] Sensor manufacturer o [5G] Robot manufacturer
• User equipment software developer/provider	o User equipment operating system developer/provider o User equipment application developer o Application store provider
• End-user	o Common phone users (Service Provider subscriber) o [5G] Wireless Sensor Network (WSN) owner/operator o [5G] Employee of enterprise
• Regulators, law enforcement agencies	

Table 9.1 Actors in the 5G System. The difference with 4G is highlighted with [5G] based on [52].

Vulnerability

Vulnerabilities[112] are perceived from the governance perspective of the supervisory bodies. The vulnerabilities in the 5G Building Blocks Layer (see Figure 9.1) include all the weaknesses of the distinctive building blocks necessary for the provisioning of 5G like vulnerabilities in hardware components (e.g. antenna's, radio equipment and cables), APIs, cloud computing, MEC platform and communication channels.
In the 5G Provisioning Layer vulnerabilities include, but are not limited to, those of the RATs.
The 5G Use Case Layer vulnerabilities are typical of the use cases. For example, in an eMBB usage scenario of virtual reality the vulnerabilities include e.g. third-party application interfacing, in URLLC with connected driving the vulnerabilities entail segmentation and trust functions, and in mMTC deployment of agriculture sensor networks (IoT) the vulnerabilities are ill-secured devices.

Threats

Threats[113] might exploit a vulnerability to breach (the trust in) the security and possibly cause harm. Threats can be intentional (e.g. hackers) or accidental (e.g. cable breakage due to excavation work). While some threats might be similar in all layers e.g. DoS attack, others are specific. Like insecure Cloud APIs or equipment failure in the 5G Building Blocks Layer, MitM attacks in the 5G Provisioning Layer and IoT Botnets in the 5G Use Case Layer. See Table 5.3 for examples of threats to security in the different layers of the 5G cyberspace model.

Threat source

Table 9.2 presents an overview of threat sources according to the NIST[114] *Guide for Conducting Risk Assessments- NIST SP 800-30 r1* [125]. The threat source can be adversarial, structural or environmental. Table 9.2 presents examples for the types of threat sources [125].

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, customer) - Nation-state	Individuals, groups, organizations, or states that seek to exploit society's dependence on cyber resources. • System intrusion, break-ins • Unauthorized system access • Browsing of personally identifiable information • Malicious code (e.g. virus) • System bugs • Identity theft • Spoofing
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.

Table 9.2 Types of threat source [125].

[112] Vulnerability: A weakness of an asset or group of assets that can be exploited by one or more threats (ISO 27005) [124]; (proactive) measures should be taken to correct it.
[113] Threat: A potential cause of an incident, that may result in harm of systems and organisation (ISO 27005) [121]; cannot be controlled (generally).
[114] National Institute of Standards and Technology – US Department of Commerce.

TYPE OF THREAT SOURCE	DESCRIPTION
STRUCTURAL - IT Equipment (storage, processing, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking • General-purpose application • Mission-specific application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Infrastructure failure/outage (e.g. electrical)	Natural disasters and failures of critical infrastructures on which society depends, but is outside the control of the organization. Can be characterized in terms of severity and duration.

Table 9.2 (Continued) Types of threat source [125].

Consequences

As of consequences, these are ultimately the same i.e. a loss of trust in (the security of) 5G among the users and the public at large in NL. Yet per layer, there are specific consequences like unavailability of a service, damage to the reputation of the provider and of the supervisory body, economic loss and financial claims. See Table 9.3 for examples of consequences to security breaches in the different layers of the 5G cyberspace model.

Aggregated to a higher level, an enumeration of relevant assets, vulnerabilities, threats, threat source and consequences, from the supervisory bodies perspective, for an end-to-end multi-stakeholder 5G system is presented in Table 9.3.

Asset:	Trust in the security of the 5G System i.e. building blocks, services, networks and applications
Vulnerabilities:	Weaknesses in 5G usage scenarios and 5G System e.g. SDN, NFV, Cloud computing, Antenna's
Threat events:	Breach of trust in the security of the 5G building blocks; Breach of trust in the security of the 5G Network; Breach of trust in the security of the 5G applications
Threat source: See Table 9.2	Adversarial (e.g. individual, group, nation-state) and non-adversarial (e.g. equipment failure)
Consequences:	Loss of trust in 5G System (i.e. applications, network, building blocks), loss of integrity, unavailability of services, reputation damage for provider, economic loss, financial claims, public unrest, damage to the reputation of the supervisory body.

Table 9.3 Examples of relevant assets, vulnerabilities, threats, threat sources and consequences on an aggregated level for the supervision of the 5G System.

9.4 Risk analysis

Risk[115] is the product of the likelihood of a manifestation of a threat and its consequence. The risks identified in the legal provisions with regards to the cyber security of 5G are:

- The risk to the security of networks and services (Arts. 13(a)(1) and (2) of the Framework Directive; Arts. 1 and 1(a) of the e-Privacy Directive; Arts. 14(1) and 16(1) of the NIS Directive and Art. 32(1) of the GDPR);
- The risk of damage to network and information systems security (Art. 4(9) NIS Directive);
- The risk for personal data and privacy (Recital 61 of the Citizens' Directive and Recital 85 of the GDPR);
- The risk to the rights and freedoms of natural persons, resulting from personal data processing, that may lead to damage (Recital 75 GDPR);
- Data (processing) security risk (Recital 83 GDPR).

For the improved conceptual model for 5G cyber security supervision (and from the perspective of the supervisory body) these risk can be abstracted to: the risks to trust in the security of the 5G Building Blocks Layer, the risks to trust in the security of the 5G Provisioning Layer, and the risks to trust in the security of the 5G Use Case Layer.

Risk level

The critical event in all proposed layers relates to the breach of trust in the security of that 5G layer. With for example the *NIST Guide for Conducting Risk Assessments* a scaling of the likelihood of the threat event (see Table 9.4 and Table 9.5) and a scaling of the consequence (see Table 9.6) can be used to estimate the level of risk (see Table 9.7) [125].

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is **almost certain** to initiate the threat event.
High	80-95	8	Adversary is **highly likely** to initiate the threat event.
Moderate	21-79	5	Adversary is **somewhat likely** to initiate the threat event.
Low	5-20	2	Adversary is **unlikely** to initiate the threat event.
Very Low	0-4	0	Adversary is **highly unlikely** to initiate the threat event

Table 9.4. Assessment Scale – Likelihood of Threat Event Initiation (Adversarial) [125].

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is **almost certain** to occur; or occurs **more than 100 times per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.

[115] Risk: effect of uncertainty on objectives. This can be quantified as likelihood (of a manifestation of a threat) multiplied by impact (ISO 31000) [122].

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per year**.
Low	5-20	2	Error, accident, or act of nature is **unlikely** to occur; or occurs **less than once a year,** but **more than once every 10 years**.
Very Low	0-4	0	Error, accident, or act of nature is **highly unlikely** to occur; or occurs **less than once every 10 years**.

Table 9.5 Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial) [125].

Regarding impact, a scaling of consequences as the potential of the impact of Threat Events is specified in Table 9.6 [125].

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Qualitative Values	Semi-Quantitative Values		Description
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 9.6 Assessment Scale – Impact of Threat Events [125].

A predefined scaling of risk levels is presented in Table 9.7 [125].

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	Threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	Threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 9.7 Assessment Scale – Level of Risk [125].

A heat map showing risk levels as a combination of likelihood and consequences is presented in Table 9.8 [125].

Likelihood (That Occurrence Results in Adverse Impact)	**Level of Impact**				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Table 9.8 Assessment Scale – Level of Risk (Combination of Likelihood and Impact) [125].

Ignoring the likelihood of threat event initiation by an adversary, and only taking into account the reports to AT on 4G continuity incidents and disturbances in 2016 (114 times) [126] and in 2017 (301 times) [127] it can be estimated conservatively that the likelihood of the initiation (non-adversarial) of a critical event in the 5G Provision layer can be (at least[116]) high (see table 9.5).
In correspondence with earlier chapters, it is estimated that the consequence a breach of trust in the security of the 5G System can be (at least) high. These estimates for the likelihood and consequence of a breach of trust in the security of the 5G System consequently result in a high risk level (see Table 9.9).

The results of the risk assessment for a breach of trust in the security of a 5G Provision Layer (due to disturbances), with a conservative estimation of likelihood and impact, is presented in Table 9.9 [125].

Asset	Threat	Vulnerabilities	Likelihood (Table 9.5)	Impact/ Consequences (Table 9.6)	Risk (Tables 9.7 & 9.8)
Trust in the security of 5G Provision Layer	Breach of trust in the security of 5G (due to disturbances) (e.g. in 5G Building Blocks Layer)	Weaknesses in 5G System e.g. RAN, SDN, NFV, Cloud computing, Antennae.	High	High	High

Table 9.9 Risk Assessment Results with a conservative estimation of likelihood and impact [125].

9.5 Risk treatment

According to ISO 27005 [124], there are four risk treatment options:

1. Risk acceptance: accept or tolerate the consequences by informed decision.
2. Risk sharing or transfer: shift the liability (partially or entirely) to another entity.
3. Risk reduction: reduce the risk to acceptable risk levels by implementing controls.
4. Risk avoidance: refrain from certain activities in order to eliminate risk.

In the present case of the provisioning of 5G for NL, the only viable option is risk reduction by implementing controls.

Bow Tie analysis

A qualitative depiction of the relationship between threats, controls and consequences is presented with the Bow Tie method [128], [129], [130].

The critical event in the 5G Building Blocks Layer is a breach of trust in the security of the 5G building blocks such as cloud computing services (e.g. MEC), antenna's, radio equipment, cables and satellites. Likewise, the critical event in the 5G Provisioning Layer is a breach of trust in the security of the 5G provision, while the critical event in the 5G Use Case Layer is a breach of trust in the security of the 5G applications.

[116] The number of reports might contain doubles [126], therefore likelihood high is chosen instead of very high.

Due to cascade effects a breach of trust in the security of the 5G Building Blocks Layer can be considered a threat to trust in the security of the 5G Provision Layer, and a breach of trust in the 5G Provision Layer in its turn can be considered a threat to trust in the security of the 5G Application Layer. Remarkably enough in 5G the cascade effect can also go the other way (e.g. if compromised IoT engage in a DoS attack against the 5G Network infrastructure striking the signalling plane, management plane, support systems, radio resources, logical and physical resources). In Figure 9.3 a triple Bow Tie is constructed depicting the critical event in each layer and cascade effects.

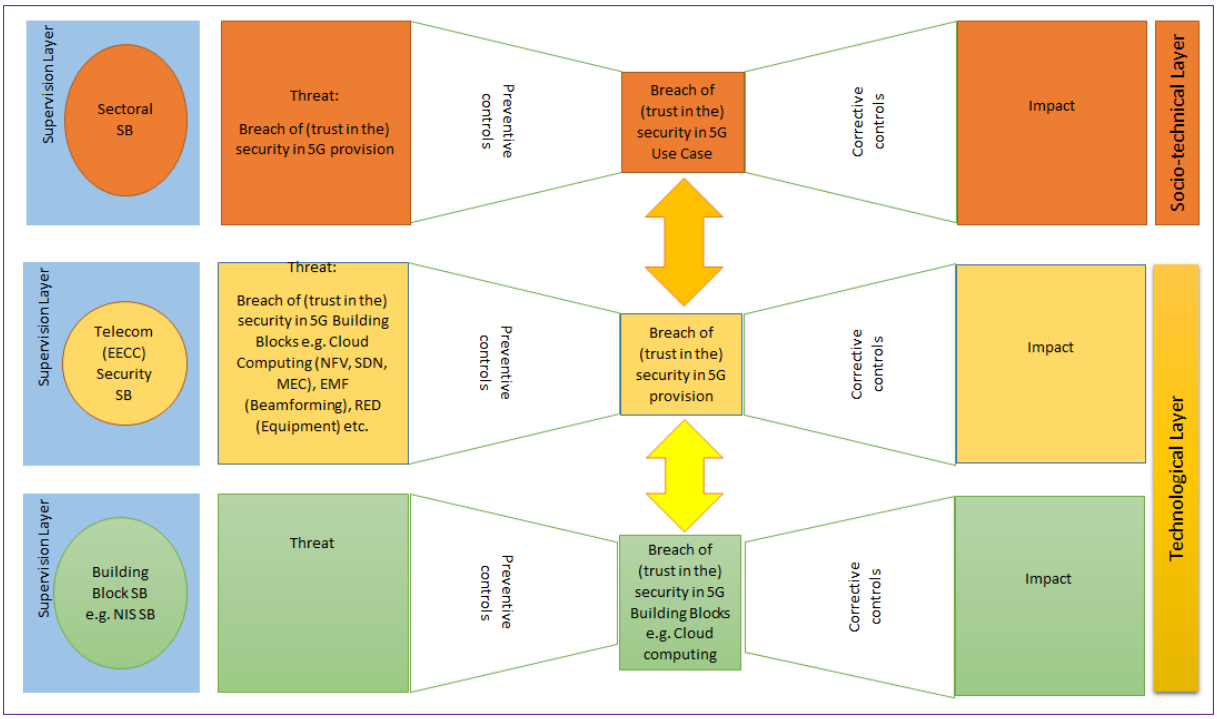


Figure 9.3 Triple Bow Tie depicting the critical event in each layer of 5G cyberspace and cascade effects.

Preventive and Corrective Controls

Preventive controls are the measures that can be put in place to prevent the critical event from taking place, while corrective controls are the measures to be taken in case the critical event has occurred.

Preventive controls in the technological layer [20] can generally consist of physical security measures, logical security measures (e.g. cryptographic techniques), secure architecture (e.g. de-compartmentalization and multi-layer defense), secure development and testing of hard- and software, certification, adequate change and patch management, back up facilities and monitoring and analytics.
Preventive measures in the socio-technical layer [20] generally entail raising of awareness with regards to cyber security risks to achieve adequate behaviour and the preparation for crises.
In the governance layer, the preventive measures can consist of creating awareness at management level regarding cyber security, its legal and financial implications, developing cyber security policy frameworks, engaging in public-private partnerships for cyber security and implementing governance institutions for risk prevention and crises management.

Specifically for regulatory oversight, the UK Civil Aviation Authority has developed five groups with 26 security controls based on international standards (i.e. ISO 27000 series and NIST 800-53r4) as a framework for the regulation of cyber-induced risks [131]. Figure 9.4 presents these controls which can be used by the supervisory body or imposed on the regulatees.

Figure 9.4 Control groups for regulatory oversight [131].

In earlier chapters, legal provisions were identified as a set of basic controls which can be implemented by the supervisory body or imposed on the regulatees depending on the layer in 5G cyberspace. Table 9.10, 9.11 and 9.12 present the legal controls applicable to the layers in 5G cyberspace for specific examples.

Table 9.10 illustrates a set of possible controls for a breach of (trust in the) security in the 5G Building Blocks Layer (e.g. breach at a cloud computing provider). Note that the so-called legal controls do not necessarily include provisions from the Tw, as in this case cloud computing resorts under the Wbni.

5G Building Blocks Layer	Preventive Controls	Recovery Controls
Legal Controls	Obligation to maintain the security of the service with technical and organisational measures to ensure a level of security appropriate to the risk.[117] (Art. 14(1) and 16(1) NIS Directive)	Mitigate breaches (Art. 14(2) NIS Directive and Art. 32(1)(c) GDPR)
	Prevent breaches (Art. 14(2) NIS Directive and Art. 32(1)(c) GDPR)	Notification of supervisory authority: - if likely to cause harm to services of individuals (Art.33 GDPR (within 72 hours)), Art. 14(3) and 16(11) NIS Directive (without undue delay))
		Notification of other supervisory authorities: - Data protection authority
		Notification to natural persons: - if there is a high risk of their rights being affected (Art. 34(1) GDPR)
		Disclosure of the breach to the public (at the discretion of the supervisory authority) (Art. 16(7) NIS Directive)
Extra Controls	See also Figure 9.4	Incident response plan
		Communications plan to inform other stakeholders and

[117] These provisions express a risk-based approach making it plausible to demand from the 5G Building Blocks provider to perform risk management for services offered (e.g. ISO 31010).

		the public.
		Revoke permit of insecure 5G building block provider
		Inform/ Request assistance from 5G Supervisory Body
		See also Figure 9.4

Table 9.10 Preventive and recovery controls for a breach of (trust in the) security in the 5G Building Blocks Layer (e.g. a cloud computing provider).

Table 9.11 illustrates a set of possible controls for a breach of (trust in the) security in the 5G Provision Layer (e.g. at the 5G Network provider).

5G Provision Layer	**Preventive Controls**	**Recovery Controls**
Legal Controls	Obligation to maintain the security of the service with technical and organisational measures to ensure a level of security appropriate to the risk.[118] (Art. 13(a)(1) and (2) Framework Directive; Art. 1 and 1(a) e-Privacy Directive)	Mitigate breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) ePrivacy Directive and Art. 32(1)(c) GDPR)
	Prevent breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) e-Privacy Directive and Art. 32(1)(c) GDPR)	Notification of supervisory authority: - always (without undue delay) if related to individuals or subscriber (e-Privacy Directive but removed from the proposed e-Privacy Regulation); - if likely to cause harm to services of individuals (Art.33 GDPR (within 72 hours)), Art. 13(a)(3) Framework Directive (without undue delay))
		Notification of other supervisory authorities: - Data protection authority - Law enforcement authority (Art. 13(a)(3) Framework Directive)
		Notification to natural persons: - when their rights are likely to be affected by the breach (Art. 4 E-Privacy Directive) - or there is a high risk thereof (Art. 34(1) GDPR)
		Disclosure of the breach to the public (at the discretion of the supervisory authority (Art. 13(a)(3) Framework Directive)
Extra Controls	Awareness Campaigns => AT Program Tele-vulnerability[119] for resilience to telecom failures	Incident response plan
	See also Figure 9.4	Communications plan to inform other stakeholders and the public.
		Revoke permit of insecure 5G system provider
		Inform/Request assistance from 5G Building Block Supervisory Body
		Inform/Request assistance from Use Case Supervisory Body
		See also Figure 9.4

[118] These provisions express a risk-based approach making it plausible to demand from the 5G systems provider to perform risk management for services offered (e.g. ISO 31010).

[119] AT has developed a 5-step program to be prepared in case of failure of telecom [132].

Table 9.11 Preventive and recovery controls for a breach of (trust in the) security in the 5G Provision Layer (e.g. at the 5G Network provider).

Table 9.12 illustrates a set of possible controls for a breach of (trust in the) security in the 5G Use Case Layer (e.g. OTT services[120]).

5G Use Case Layer	Preventive Controls	Recovery Controls
Legal Controls	Obligation to maintain the security of the service with technical and organisational measures to ensure a level of security appropriate to the risk.[121] (Art. 13(a)(1) and (2) Framework Directive; Art. 1 and 1(a) e-Privacy Directive)	Mitigate breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) ePrivacy Directive; Art. 32(1)(c) GDPR)
	Prevent breaches (Art. 13(a)(1) Framework Directive; Art. 4(2) ePrivacy Directive; Art. 32(1)(c) GDPR)	Notification of supervisory authority: - always (without undue delay) if related to individuals or subscriber (e-Privacy Directive but removed from the proposed e-Privacy Regulation); - if likely to cause harm to services of individuals (Art.33 GDPR (72 hours)), Art. 13(a)(3) Framework Directive (without undue delay))
		Notification of other supervisory authorities: - Data protection authority - Law enforcement authority (Art. 13(a)(3) Framework Directive)
		Notification to natural persons: - when their rights are likely to be affected by the breach (Art. 4 E-Privacy Directive) - or there is a high risk thereof (Art. 34(1) GDPR)
		Disclosure of the breach to the public (at the discretion of the supervisory authority) (Art. 13(a)(3) Framework Directive)
Extra Controls	Awareness Campaigns	Incident response plan
	See also Figure 9.4	Communications plan to inform other stakeholders and the public.
		Revoke permit of insecure 5G system provider
		Inform/Request assistance from 5G Building Block Supervisory Body
		Inform/Request assistance from Use Case Supervisory Body
		See also Figure 9.4

Table 9.12 Preventive and recovery controls for a breach of (trust in the) security in the 5G Use Case Layer (e.g. OTT services).

Escalation factors

If controls fail or do not perform as intended the need for escalation factor controls arise [128]. This is the case for instance if notifications of breaches do not reach the supervisory body because of differences in interpretation by the regulatees of the legal provisions. Porcedda notes that there is no need to notify the supervisory body if the *breach "is either unlikely to result in an appreciable risk to*

[120] OTT services are newly incorporated in the EECC.

[121] These provisions express a risk-based approach making it plausible to demand from the 5G systems provider to perform risk management for services offered (e.g. ISO 31010).

the rights and freedoms of natural persons (Article 33 GDPR), for instance because of the adoption of ad hoc or post hoc measures of protection, or if the provision of a service is not significantly, substantially, or majorly impacted (Articles 13a(3) of the Framework Directive, and 14 (3) and 16 (11) of the NIS Directive)".
Another example where notification can fail is that essential service operators must notify significant incidents, whereas cloud providers must only notify substantial ones, while Art. 3 (5) of Commission Regulation 2018/151 implies that a substantial incident is one having a significant impact on economic and societal activities. An additional challenge is that Member States cannot impose higher security requirements on cloud providers than those agreed at EU level (art. 16(10) of the NIS Directive).

9.6 Monitoring and review

Risk management is a continuous endeavor and changes in any facet will necessitate updates and re-evaluation of previously determined risk levels and the selected security controls. In a complex environment as 5G, this in itself can be challenging.

Cyber situational awareness (conform Endsley [116]) of the responsible supervisory bodies can play an important factor in effective risk management for cyber security of 5G.

9.7 Summary

The first identified requirement for an improved conceptual model for 5G cyber security supervision is the deployment of a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors.

The provisioning of 5G is modelled, according to the conceptualized cyberspace model, in the 5G Use Case Layer, the 5G Provisioning Layer, the 5G Building Blocks Layer and the 5G Supervision Layer.

The steps of the risk management cycle are performed to identify, assess and analyse risks related to the compromise of an end to end multi-stakeholder 5G System.
Even when ignoring the likelihood of threat event initiation by an adversary, based on the reports to AT on 4G continuity incidents and disturbances alone it can be estimated conservatively that the likelihood of the (non-adversarial) initiation of the critical event in the 5G Provision layer will be high. In correspondence with earlier chapters, it is estimated that the consequence a breach of trust in the security of the 5G System will be (at least) high. These estimates for likelihood and consequence of a breach of trust in the security of the 5G System consequently result in a high risk level.

A triple Bow Tie is constructed depicting the critical event in each layer and cascade effects. Controls are proposed for the designated supervisory body within a suitable risk treatment strategy from a governance perspective. Risk management is a continuous endeavor and changes in any facet will necessitate updates and re-evaluation. Cyber situational awareness can also play an important factor in effective risk management for cyber security of 5G.

10. A Proposal for cyber security supervision of 5G in NL

The Triple Bow Tie Supervision model for cyber security supervision of 5G

The remaining requirements for an improved model for cyber security supervision of 5G are; (b) to arrange for cooperation between supervisory bodies; to (c) streamline collection and exchange of relevant information; (d) to harmonize norms; and (e) interventions.
This implies intensive interaction between the supervisory bodies in the governance layer of 5G cyberspace.

These requirements together with the first requirement, (a) deploying a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors as depicted with the Triple Bow Tie in Figure 9.3, are incorporated into a conceptual model for cyber security supervision of 5G in NL.

Figure 10.1 depicts the resulting conceptual model for cyber security supervision of 5G in NL with a Triple Bow Tie for the 5G Use Case Layer, the 5G Provisioning layer and the 5G Building Blocks Layer.

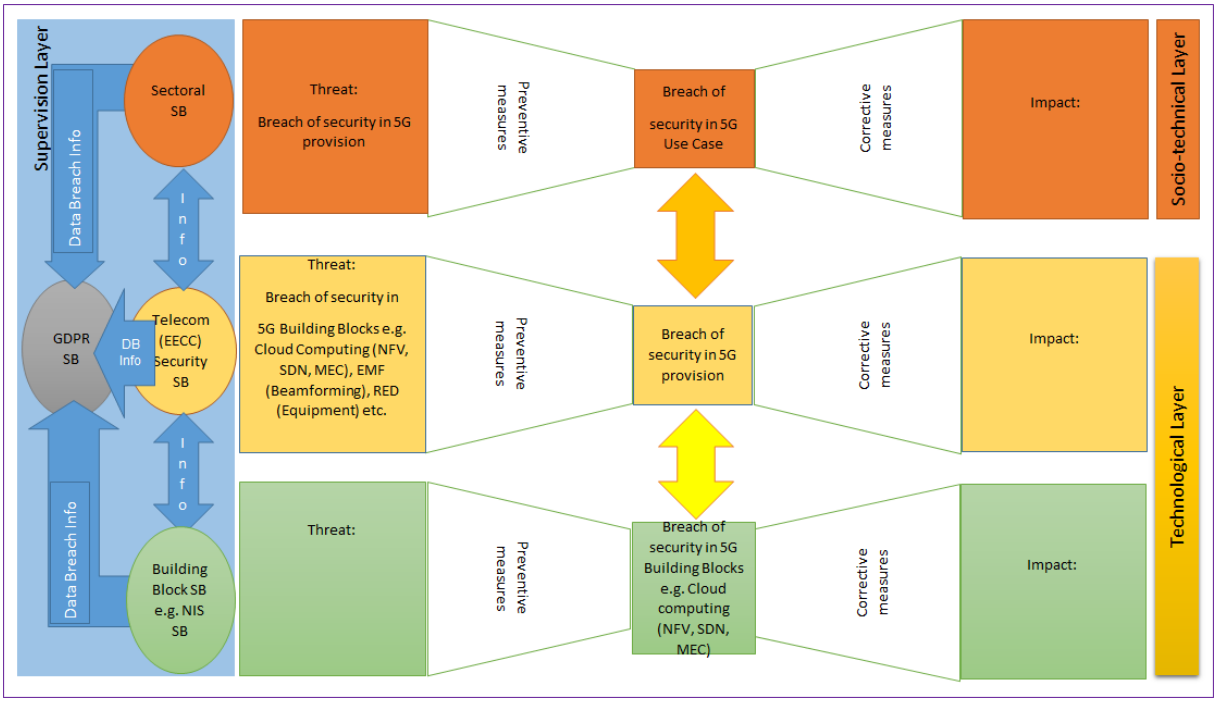


Figure 10.1 The Triple Bow Tie Cyber Security Supervision model with the 5G Use Case Layer, the 5G Provisioning layer and the 5G Building Blocks Layer.

The Triple Bow Tie Supervision model for cyber security of 5G in NL as presented in figure 10.1 meets the identified requirements:

1. Deploying a risk-driven approach by the 5G supervisory bodies with consideration of cascading effects in adjacent sectors;
2. Cooperation between relevant NL 5G supervisory bodies, between NL, European 5G supervisory bodies (and ENISA), and between NL and non-European supervisory bodies;
3. Collection of information delegated to sector-specific supervisory bodies to address the dissemination of providers and subcontractors, and relevant information dispersed to stakeholders to create cyber situational awareness, and monitoring coordinated between collaborative 5G supervisory bodies by AT to gain overview;

4. Supervisory bodies to fill in the open norms on 5G cyber security with their sector and harmonize them across the supervisory bodies;
5. Intervening by the supervisory bodies based on the identified controls in legislation and supplementary supervisory controls developed in close cooperation with all involved supervisory bodies with consideration of adjacent sectors.

Figure 10.2 illustrates as an example the new information flows (in red) that can arise in supervision of a 5G System in NL resulting from the Triple Bow Tie Supervision model.

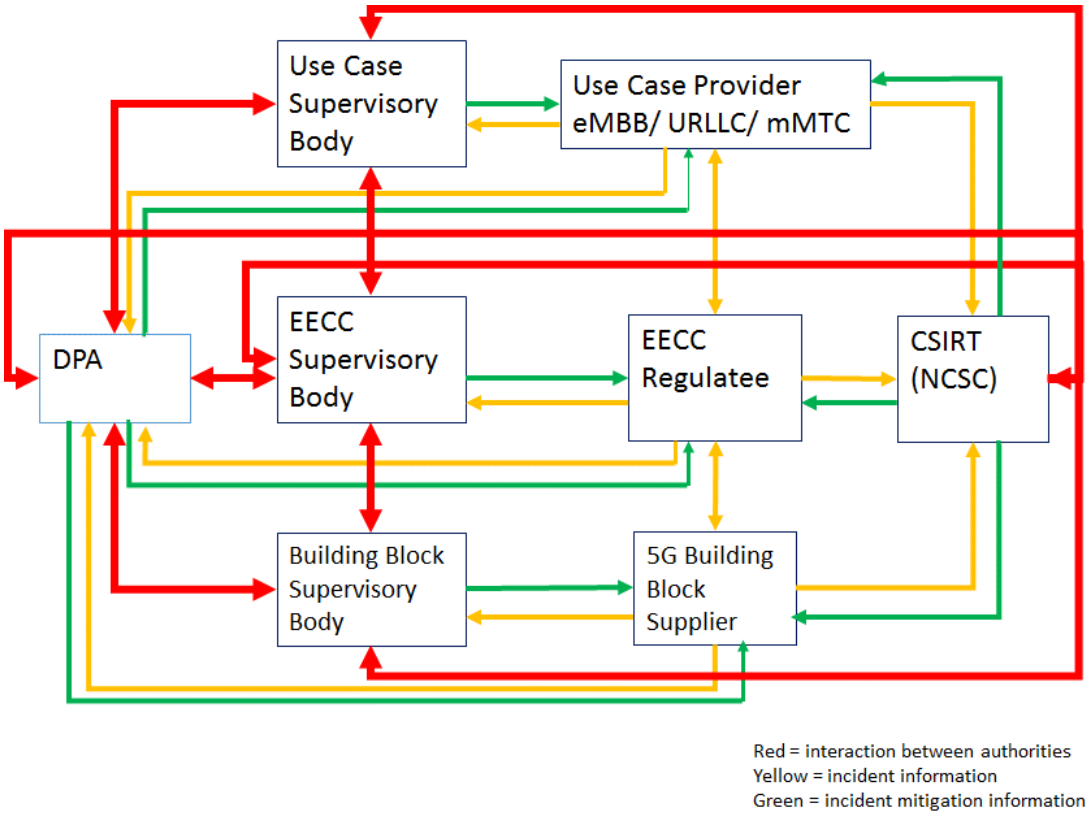


Figure 10.2. Communications regarding 5G security between supervisory authorities, CSIRT and regulatees in NL. In red the new information flows resulting from the Triple Bow Tie Supervision model.

Preconditions

The conceptual Triple Bow Tie Supervision model for 5G cyber security was developed under the following preconditions:

- The legal framework is still under development on EU level;
- NL still has not decided on spectrum arrangement and the implementation of 5G, let alone cyber security supervision;
- The supervisory bodies themselves will most likely also be affected by 5G in the way they (will) operate;
- Private supervisory bodies in NL (e.g. branch organizations) can contribute to the cyber security of 5G by imposing cyber security requirements on their members and enforcing them (see paragraph Alternatives to classical regulation);
- Private 5G networks could also pose a threat to the public networks if there is no monitoring of coupling.

11. Conclusion

To make sure that users and the larger public can trust 5G, appropriate cyber security supervision is mandatory. With the current provisions there will be gaps in oversight of crucial parts of 5G.

To address this the conceptual Triple Bow Tie Supervision model for 5G cyber security in NL incorporates a risk-driven approach to supervision in the 5G Building Blocks Layer, the 5G Provision Layer and the 5G Use Case layer and cooperation between relevant supervisory bodies to share information (e.g. on norms, threats, risk assessments, cascading effects, interventions) and create cyber situational awareness in order to better ensure the end-to-end security of 5G (see Figure 11.1).

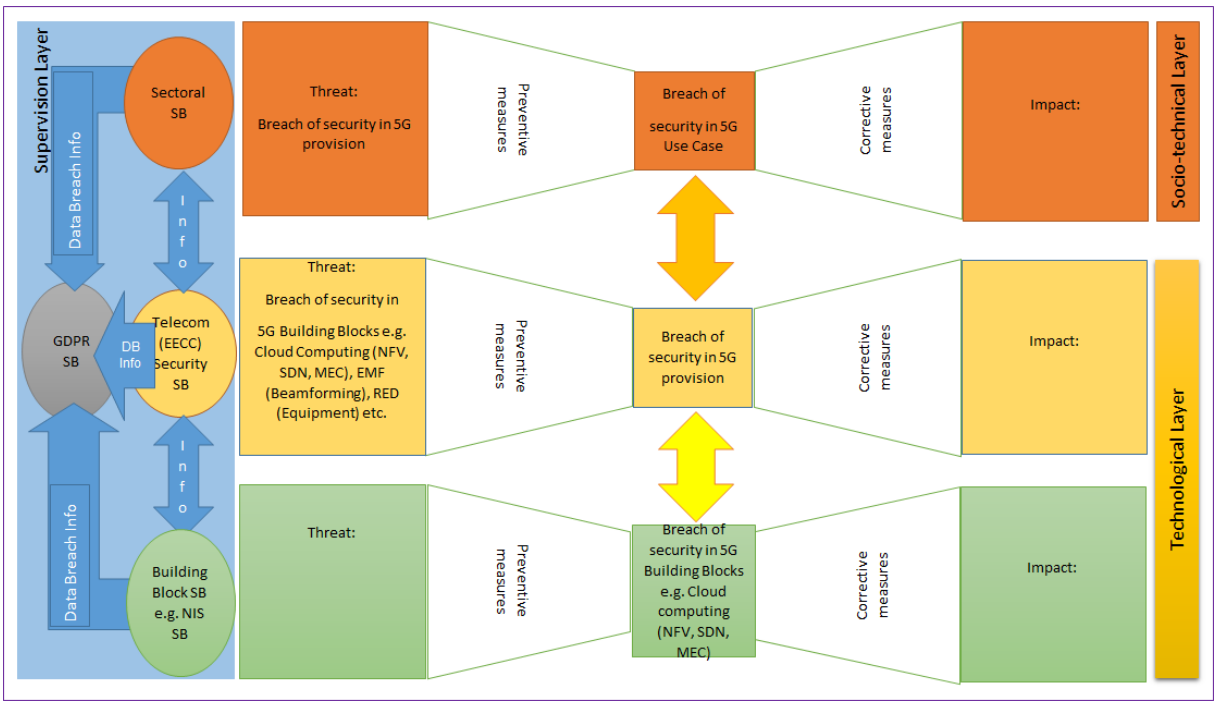


Figure 11.1 The Triple Bow Tie 5G Cyber Security Supervision model.

Implementing the Triple Bow Tie 5G Supervision model

To implement the Triple Bow Tie 5G Cyber Security Supervision model it is suggested that AT takes the lead in a step-by-step plan consisting of:

Step 1: Identify all relevant supervisory bodies for 5G and create awareness;

Step 2: Request risk analyzes from the supervisory bodies focused on 5G with consideration of cascading effects in adjacent sectors;

Step 3: Request agreements between supervisory bodies and regulatees on common norms (for example ENISA guidelines or norms set by supervisory bodies together);

Step 4: Conclude on a cooperation agreement (regarding information exchange) between relevant 5G supervisory bodies;

Step 5: Set up an information exchange process between relevant 5G supervisory bodies, the Data Protection Authority and the CSIRT.

Note that the implementation of the Triple Bow Tie 5G Cyber Security Supervision model takes place in such a way that innovation is not impeded.

Communication

The proposed Triple Bow Tie Supervision model for 5G cyber security and its implications have been presented to the policy officers and management of AT. They were pleased with the insight that the model provides in the cascade effects in ensuring the cyber security of 5G and the need for cooperation between supervisory bodies. The model and roadmap are therefore much-welcomed tools.

Future work recommendations

Analyse the applicability of the Triple Bow Tie 5G Cyber Security Supervision model in the other EU Member States.

Compare the Triple Bow Tie 5G Cyber Security Supervision model with supervision models for the cyber security of 5G in other EU member states, if any.

Considering the limitations imposed by the regulatory environment explore what further (European) regulations are required in order to make it more straightforward for the involved stakeholders to ensure the cyber security of 5G.

References

[1] Next Generation Mobile Networks (NGMN) Alliance, "5G White Paper," NGMN, Reading, February 2015.

[2] IEEE, "IEEE 5G and beyond technology roadmap White Paper," IEEE, https://5g.ieee.org/images/files/pdf/ieee-5g-roadmap-white-paper.pdf, October 2017.

[3] D. Giusto, A. Iera, G. Morabito and L. Atzori, The Internet of Things, ISBN: 978-1-4419-1673-0: Springer, 2010.

[4] EUROPEAN COMMISSION, "5G for Europe: An Action Plan - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS," EUROPEAN COMMISSION COM(2016) 588 final, Brussels, September 2016.

[5] EUROPEAN COMMISSION, "Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS," EUROPEAN COMMISSION COM(2016) 587 final, Brussels, September 2016.

[6] European Union, " DIRECTIVE (EU) 2018/1972 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 December 2018 establishing the European Electronic Communications Code (Recast)," Official Journal of the European Union, Brussels, December 2018.

[7] W. Lemstra, "Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications," *Telecommunications Policy ,* vol. 2017, no. , p. 1–25, February 2018.

[8] Ministerie van Economische Zaken en Klimaat, "Nederlandse Digitaliseringsstrategie," Ministerie van Economische Zaken en Klimaat, The Hague, June 2018.

[9] Directie Telecommarkt, "Action Plan Digital Connectivity," Ministerie van Economische Zaken & Klimaat, The Hague, July 2018.

[10] European Commission, "The Digital Economy and Society Index (DESI) - 2018," [Online]. Available: https://ec.europa.eu/digital-single-market/en/desi . [Accessed 09 11 2018].

[11] M. Carr, "Public–private partnerships in national cyber-security strategies," *International Affairs,* vol. 92, no. 1, pp. 43-62, 2016.

[12] Dutch Cyber Security Council, "Towards an open, secure and prosperous digital Netherlands - Recommendation regarding the Dutch National Cybersecurity Agenda (NCSA)," CSR, The Hague, June 2018.

[13] NCTV, "National Cyber Security Agenda - A cyber secure Netherlands," The Minister of Justice and Security, The Hague, April 2018.

[14] Inspectieraad, "Naar het toezicht van de toekomst - Toezichtagenda 2017-2018," Inspectieraad, The Hague, April 2017.

[15] M. Lodge and K. Wegrich, Managing Regulation - Regulatory analysis, politics and policy, London: Palgrave Macmillan, 2012.

[16] 5G PPP Security Working Group, "5G PPP Phase1 Security Landscape," 5GPPP, http://5gensure.eu/files/5g-pppwhite-paperphase-1-security-landscapejune-2017pdf , June 2017.

[17] 5GPPP Architecture Working Group, "View on 5G Architecture (Version 2)," 5G-PPP, https://5g-ppp.eu/wp-content/uploads/2018/01/5G-PPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf , 2017-12-15.

[18] DotEcon Ltd and Axon Partners Group, "No BEREC/2017/02/NP3 Study on Implications of 5G Deployment on Future Business Models," BEREC, https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8008-study-on-implications-of-5g-deployment-on-future-business-models, March 2018.

[19] European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU JOIN(2017) 450 final,* Brussels: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, 13.9.2017.

[20] J. van den Berg, J. van Zoggel, M. Snels, M. van Leeuwen, S. Boeke, L. van de Koppen, J. van de Lubbe, B. van den Berg and T. de Bos, "On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education," *Cyber Security Science and Engineering,* pp. Sto-MP-IST-122, 2014.

[21] 5G-ENSURE, "Trust," [Online]. Available: http://5gensure.eu/trust. [Accessed 17 11 2018].

[22] Staatscourant, "Regeling van de Minister-President, Minister van Algemene Zaken van 30 september 2015, nr. 3151041, houdende de vaststelling van de Aanwijzingen inzake de rijksinspecties," *Staatscourant,* no. 33574, October 2015.

[23] H. Berg, "Risk management: procedures, methods and experiences.," *Risk Management,* vol. 17, no. 1, pp. 79-95, 2010.

[24] A. R. Hevner, S. T. March, J. Park and S. Ram, "Design science in information systems research," *MIS quarterly,* vol. Vol. 28, no. No. 1, pp. 5-105, March 2004.

[25] A. G. ". Kefalas, "On Systems Thinking and the Systems Approach," *World Futures, 67:4-5,* pp. 343-371, 2011.

[26] S. Shahabuddin, S. Rahaman, F. Rehman, I. Ahmad and Z. Khan, "Evolution of Cellular Systems," in *A Comprehensive Guide to 5G Security*, Hoboken, NJ, John Wiley & Sons, April 2018, pp. 3-29.

[27] ITU-R, "Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)," ITU, https://www.itu.int/rec/R-REC-M.1457/en ,

2015.

[28] ITU-R, "Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications Advanced (IMT-Advanced)," ITU, https://www.itu.int/rec/R-REC-M.2012/en , 2014.

[29] R. S. Sapakal and S. S. Kadam, "5G Mobile Technology," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. Volume 2, no. Issue 2, pp. 568-571, February 2013.

[30] P. Gupta, "EVOLVEMENT OF MOBILE GENERATIONS : 1G To 5G," *International Journal For Technological Research In Engineering,* vol. Volume 1, no. Issue 3, pp. 152-157, November 2013.

[31] R. Sood and A. Garg, "Digital Society from 1G to 5G: A comparative study," *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* vol. Volume 3, no. Issue 2, pp. 186-193, February 2014.

[32] P. Sharma, "Evolution of Mobile Wireless Communication Networks-1G to 5G as well as Future Prospective of Next Generation Communication Network," *International Journal of Computer Science and Mobile Computing,* vol. Volume 2, no. Issue 8, p. 47 – 53, August 2013.

[33] A. Osseiran, J. F. Monserrat and P. Marsch, 5G mobile and wireless communications technology, New York: Cambridge University Press, 2016.

[34] METIS-II: Mobile and wireless communications Enablers for the Twenty-twenty Information Society-II, "Deliverable/Report D8.3 METIS-II final project report," 5G-PPP, http://www.5g-ppp.eu/, June 2017.

[35] 5G-PPP The 5G Infrastructure public private partnership, "5G empowering vertical industries," 5G-PPP, Brussels, 2016.

[36] ITU, "ITU towards “IMT for 2020 and beyond”," [Online]. Available: https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx. [Accessed 11 09 2018].

[37] Frank Mademann - 3GPP SA2 Chairman, "System architecture milestone of 5G Phase 1 is achieved," 21 12 2017. [Online]. Available: http://www.3gpp.org/NEWS-EVENTS/3GPP-NEWS/1930-SYS_ARCHITECTURE. [Accessed 11 09 2018].

[38] 3GPP, "Release 16," 16 07 2018. [Online]. Available: http://www.3gpp.org/release-16. [Accessed 11 09 2018].

[39] ITU-R, "Recommendation M.2083-0 IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," ITU, Geneva, 2015.

[40] ITU-R, "Recommendation ITU-R M.2012-3 Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-Advanced (IMT Advanced)," ITU, Geneva, 2018.

[41] ITU-R, "Report ITU-R M.2410-0 Minimum requirements related to technical performance for IMT-2020 radio interface(s)," ITU, Geneva, 2017.

[42] ITU , "5G: the new hype?," in *ITU Arab Forum on Emerging Technologies*, Algiers, February 2018.

[43] 3GPP - Technical Specification Group Radio Access Network, "Study on Scenarios and Requirements for Next Generation Access Technologies (Release 15)," 3GPP, Sophia Antipolis, July 2018.

[44] I. F. Akyildiz, S. Nie, S.-C. Lin and M. Chandrasekaran, "5G roadmap: 10 key enabling technologies," *Computer Networks ,* no. 106, pp. 17-48, 2016.

[45] Network Operators, "Network Functions Virtualisation – Introductory White Paper," ETSI NFV ISG, https://portal.etsi.org/nfv/nfv_white_paper.pdf, 2012.

[46] N. Feemster, J. Rexford and E. Zegura, "The Road to SDN," *ACM Queue,* vol. 11, no. 12, p. 20, December 2013.

[47] ETSI, "ETSI GS MEC-IEG 004 Mobile-Edge Computing (MEC); Service Scenarios," ETSI, Sophia Antipolis, November 2015.

[48] ETSI, "ETSI White Paper No.25 Microwave and Millimetre-wave for 5G transport," ETSI, Sophia Antipolis, Februari 2018.

[49] ETSI, "ETSI White Paper No.17 Next Generation Protocols - Market Drivers and Key Scenarios," ETSI, Sophia Antipolis, May 2016.

[50] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta and P. Popovsk, "Five Disruptive Technology Directions for 5G," *IEEE Communications Magazine,* vol. 52, no. 2, pp. 74 - 80, February 2014.

[51] 3GPP - Technical Specification Group Services and System Aspects, "Feasibility Study on New Services and Markets Technology Enablers - Stage 1 (Release 14)," 3GPP, Sophia Antipolis, September 2016.

[52] 5G-PPP, "5G Enablers for Network and System Security and Resilience 5G- ENSURE Deliverable D2.5 Trust model (Final)," 5G-PPP, http://5gensure.eu/sites/default/files/5G-ENSURE_D2.5%20Trust%20model%20%28final%29%20v2.2%20inc%20history.pdf, November 2017.

[53] ITU, "World Radiocommunication Conference allocates spectrum for future innovation," 27 11 2015. [Online]. Available: https://www.itu.int/net/pressoffice/press_releases/2015/56.aspx. [Accessed 25 09 2018].

[54] European Commission Communication, "A Digital Single Market Strategy for Europe," European Commission, Brussels, May 2015.

[55] The European Parliament and the Council, "Decision (EU) 2017/899 of The European Parliament and the Council on the use of the 470-790 MHz frequency band in the Union,"

Official Journal of the European Union, Brussels, 17 May 2017.

[56] Radio Spectrum Policy Group, "Strategic Spectrum Roadmap Towards 5G for Europe - RSPG Second Opinion on 5G Networks," European Commission, Brussels, January 2018.

[57] European Commission - Radio Spectrum Committee, "Mandate to CEPT to develop harmonised technical conditions for spectrum use in support of the introduction of next-generation (5G) terrestrial wireless systems in the Union," European Commission, Brussels, December 2016.

[58] ITU, "World Radiocommunication Conference 2019 - Agenda and Relevant Resolutions," ITU, www.itu.int/go/wrc-19, August 2017 (revised).

[59] State Secretary for Economic Affairs and Climate Policy, "Letter to Parliament regarding the delay of the "Nota Mobiele Communicatie"," Ministry of Economic Affairs and Climate Policy, https://zoek.officielebekendmakingen.nl/ah-tk-20172018-1103.html, February 2018.

[60] State Secretary of Economic Affairs and Climate Policy, "Letter of the State Secretary of Economic Affairs and Climate Policy," *Kamerstuk,* vol. Kamerstuk 26 643 nr. 587, no. Tweede Kamer der Staten-Generaal, January 2019.

[61] European Commission, "Merger Cases: M.8792 T-MOBILE NL / TELE2 NL," [Online]. Available: http://ec.europa.eu/competition/elojade/isef/case_details.cfm?proc_code=2_M_8792 . [Accessed 28 11 2018].

[62] State Secretary for Economic Affairs and Climate Policy, "Letter to Parliament regarding Actieplan digitale connectiviteit," Ministery of Economic Affairs and Climate Policy, https://www.tweedekamer.nl/kamerstukken/detail?id=2018Z13089&did=2018D37595, July 2018.

[63] M. Matinmikko, M. Latva-aho, P. Ahokangas and V. Seppanen, "On regulations for 5G: Micro licensing for locally operated networks," *Telecommunications Policy,* no. Elsevier, pp. 1-14, 2017.

[64] 5gamericas, "Small cell siting challenges and recommendations," 5gamericas , http://www.5gamericas.org/files/9815/3547/3006/195_SC_siting_challenges_final.pdf, August 2018.

[65] J. Zander, "Beyond the ultra-dense barrier: paradigm shifts on the road beyond 1000x wireless capacity," *IEEE Wireless Communications,* vol. 24, pp. 96-102, 2017.

[66] A. D"Annunzio and P. Reverberi, "Co-investment in ultra-fast broadband access networks: Is there a role for content providers?," *Telecommunications Policy,* vol. 40, pp. 353-367, 2016.

[67] Authority for Consumers and Markets (ACM), "Bundling of telecom services and content in the Netherlands - Analysis of the possible consequences for competition," ACM, The Hague, July 2017.

[68] NOKIA, "White paper: Techno-economic simulation results for solid 5G business and technology planning," NOKIA, https://onestore.nokia.com/asset/201088, 2017.

[69] 5G Automotive Association, "White Paper: The Case for Cellular V2X for Safety and Cooperative Driving," 5GAA, http://5gaa.org/news/white-paper-placeholder-news-for-testing/, 2016.

[70] A. Bux Abro, "Mobile Networks Security Landscape," in *A Comprehensive guide to 5G security*, Hoboken, NJ, John Wiley & Sons, April 2018, pp. 59-74.

[71] NGMN Alliance, "5G security recommendations Package #1," NGMN , Reading , May 2016.

[72] M. Liyanage, I. Ahmad, J. Okwuibe, E. Montes de Oca, H. L. MAI, O. López Perez and M. Uriarte Itzazelaia, "Software Defined Security Monitoring in 5G Networks," in *A Comprehensive Guide to 5G Security*, Hoboken, NJ, John Wiley & Sons, April 2018, pp. 231-243.

[73] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "5G Security: Analysis of Threats and Solutions," in *IEEE Conference on Standards for Communications and Networking (CSCN)*, 2017.

[74] J. Okwuibe, M. Liyanage, I. Ahmad and M. Ylianttila, "Cloud and MEC Security," in *A Comprehensive Guide to 5G Security*, Hoboken, NJ, John Wiley & Sons Ltd, 2018 , pp. 373-379.

[75] D. FANG, Y. QIAN and R. QINGYANG HU, "Security for 5G Mobile Wireless Networks," *IEEE Access,* vol. 2018, no. 6, pp. 4850-4874, December 2017.

[76] European Union Agency for Network and Information Security (ENISA), "Looking into the crystal ball - A report on emerging technologies and security challenges," ENISA, Heraklion, January 2018.

[77] T. Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies,* vol. 35, no. 1, pp. 5-32, 2012.

[78] L. Lessig, Code 2.0, New York: Basic Books, 2006.

[79] ITU, "About International Telecommunication Union (ITU)," [Online]. Available: https://www.itu.int/en/about/Pages/default.aspx . [Accessed 1 11 2018].

[80] ITU-R, "Mission statement," [Online]. Available: https://www.itu.int/en/ITU-R/information/Pages/mission-statement.aspx . [Accessed 1 11 2018].

[81] ITU-R, "All Sessions Outcome - Third Annual ITU IMT-2020/5G Workshop and Demo Day-2018," https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201807/Documents/Outcomes_Workshop_IMT-2020_5G.pdf, 18 July 2018.

[82] IETF, "About," [Online]. Available: https://www.ietf.org/about/. [Accessed 17 12 2018].

[83] IEEE Standards Association, "IEEE Standards Activities in 5G," 9 11 2018. [Online]. Available: https://www.google.com/url?q=http://standards.ieee.org/develop/intl/msp/5G.pdf&sa=U&ved=0ahUKEwjT-fWU5Y3fAhUFIVAKHWzyBRAQFggKMAI&client=internal-uds-cse&cx=006539740418318249752:f2h38l7gvis&usg=AOvVaw2ArlFsKSYDrvC_XYR_Aboo.

[Accessed 7 12 2018].

[84] GSMA, "The 5G era: Age of boundless connectivity and intelligent automation," [Online]. Available: https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download. [Accessed 5 12 2018].

[85] GSMA, "5G spectrum guide – everything you need to know," [Online]. Available: https://www.gsma.com/spectrum/wp-content/uploads/2018/11/AI-1.13-Positions.pdf. [Accessed 5 12 2018].

[86] SIMalliance, "An analysis of the security needs of the 5G market - A SIMalliance 5G Working Group marketing white paper," [Online]. Available: https://simalliance.org/wp-content/uploads/2016/02/SIMalliance_5GWhitepaper_FINAL.pdf. [Accessed 5 12 2018].

[87] 3GPP, "3GPP TS 21.111 version 15.1.1 Release 15," ETSI, Sophia Antipolis, July 2018.

[88] M. G. Porcedda, "Patching the patchwork: appraising the EU regulatory framework on cyber security breaches," *Computer Law & Security Review,* vol. 34, no. 5, p. 1077–1098, October 2018.

[89] F. Calderoni, "The European legal framework on cybercrime: striving for an effective implementation," *Crime, Law and Social Change,* vol. 54, no. 5, pp. 339-357, 2010.

[90] R. Anderson and T. Moore, "The Economics of Information Security," *Science,* vol. 314, p. 610–661, 2006.

[91] European Commission, "Press Release - Digital Single Market: EU negotiators reach a political agreement to update," European Commission, http://europa.eu/rapid/press-release_IP-18-4070_en.htm, June 2018.

[92] Council of the European Union, "Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast) - OUTCOME OF PROCEEDINGS," General Secretariat of the Council, Brussels, June 2018.

[93] European Network and Information Security Agency (ENISA), "Annual Incident Reports 2016. Analysis of Article 13a annual incident reports in the telecom sector," ENISA, Heraklion, 2017.

[94] ENISA, "Technical Guideline on Incident Reporting - Technical guidance on the incident reporting in Article 13a - Version 2.0," ENISA, Heraklion, January 2013.

[95] European Commission, "Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Annex to (Communication) COM(2017)," European Commission, Brussels, 2017.

[96] European Commission, "Commission Implementing Regulation 2018/151 of 30 January 2018 laying down rules for application of Directive (EU) 2016/1148," Official Journal of the European Union, Brussels, January 2018.

[97] European Network and Information Security Agency (ENISA), "Technical Guideline on security measures for Article 4 and Article 13a," ENISA, https://www.enisa.europa.eu/publications/guideline-on-security-measures-for-article-4-and-article-13a, 2015.

[98] ENISA, "Technical Guideline on security measures for Article 4 and Article 13a," ENISA, Heraklion, 2014.

[99] Article 29 Data Protection Working Party, "Working Document 01/2011 on the Current EU Personal Data Breach Framework and Recommendations for Future Policy Developments," WP 184, Brussels, 2011.

[100] Article 29 Data Protection Working Party , "Working Document 01/2011 on the current EU Personal Data Breach Framework and Recommendations for Future Policy Developments," WP 184, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp184_en.pdf, 2011.

[101] ENISA, "Conference - Cybersecurity Standardization and the Cybersecurity Act: Where are we today? - January 21, 2019," [Online]. Available: https://www.enisa.europa.eu/events/cybersecurity_standardisation/cybersecurity_standardisation. [Accessed 8 12 2018].

[102] Dutch Government, Dutch Telecommunications Act - Telecommunicatiewet (Tw), vol. nr. 610, https://wetten.overheid.nl/BWBR0009950/2019-01-01: Ministry of Economic Affairs and Climate Policy, 1998.

[103] Dutch Government, Wet beveiliging netwerk- en informatiesystemen, https://wetten.overheid.nl/BWBR0041515/2018-11-09#search_highlight0: Ministry of Justice and Security, 2018.

[104] Dutch Government, Uitvoeringswet Algemene verordening gegevensbescherming, https://wetten.overheid.nl/BWBR0040940/2018-05-25: Ministry of Justice and Security, 2018.

[105] Ministry of Justice and Security, "Besluit van 4 december 2017 tot aanwijzing van aanbieders, producten en diensten ten aanzien waarvan een plicht geldt om ernstige ICT-incidenten te melden (Besluit meldplicht cybersecurity)," *Staatscourant,* vol. 2017, no. 476, December 2017.

[106] Ministry of Justice and Security, "Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesystemen (Besluit beveiliging netwerk- en informatiesystemen)," Staatsblad nr. 388, https://zoek.officielebekendmakingen.nl/stb-2018-388.html, 2018.

[107] Ministry of Economic Affairs and Climate Policy, "Brochure Wet Beveiliging Netwerk- en Informatiesystemen (Wbni) voor Digitale dienstverleners (Wbni for DSPs)," Ministry of Economic Affairs and Climate Policy, The Hague, September 2018.

[108] Ministry of Transport, Public Works and Water Management, "Besluit aanwijzing toezichthouders Telecommunicatiewet," Staatscourant,

https://wetten.overheid.nl/BWBR0010033/2017-03-10, 1998.

[109] Radiocommunications Agency - Agentschap Telecom (AT), "Wet beveiliging netwerk- en informatiesystemen," [Online]. Available: https://www.agentschaptelecom.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen. [Accessed 06 01 2019].

[110] Ministry of Justice and Security, "Besluit van 30 oktober 2018 tot aanwijzing van het CSIRT voor digitale diensten en tot vaststelling van het tijdstip van inwerkingtreding van de Wet en het Besluit beveiliging netwerk- en informatiesystemen," Staatsblad nr. 389, https://zoek.officielebekendmakingen.nl/stb-2018-389.html, 2018.

[111] Ministry of the Interior and Kingdom Relations, "Minder last, meer effect; zes principes van goed toezicht," Tweede Kamer der Staten-Generaal, Den Haag, 2005.

[112] R. Brownsword, "The shaping of our on-line worlds: getting the regulatory environment right," *International Journal of Law and Information Technology,* vol. 20, no. 4, pp. 249-272, 2012.

[113] WRR - Scientific Council for Government Policy, "Supervising public interests. Towards a broaderSupervising public interests. Synopsis of WRR-Report no. 89," WRR, The Hague, 2013.

[114] Ministerie van Wonen en Rijksdienst, "Kabinetsreactie op de rapporten "Toezien op publieke belangen" en "Van tweeluik naar driehoeken" van de Wetenschappelijke Raad voor het Regeringsbeleid.," Tweede Kamer der Staten-Generaal, The Hague, 2013–2014 33 822 Nr.3.

[115] Inspectieraad, "Brief aan de Minister van Binnenlandse Zaken en Koninkrijkrelaties: Programma Innovatie Toezicht," Bureau Inspectieraad, The Hague, 2018.

[116] M. R. Endsley, "Towards a theory of Situation Awareness in Dynamic Systems," *Human Factors,* vol. 37, no. 1, pp. 32-64, 1995.

[117] Agentschap Telecom, "Jaarplan Toezicht 2018 (Annual Plan Supervision 2018)," Ministry of Economic Affairs and Climate Policy - Agentschap Telecom, Groningen, 2018.

[118] Staatscourant, "Samenwerkingsprotocol AT and ACM," *Staatscourant,* vol. 2015, no. nr. 7210, 2015.

[119] AT, "Commissariaat voor de Media en Agentschap Telecom tekenen samenwerkingsprotocol," 06 12 2017. [Online]. Available: https://www.agentschaptelecom.nl/actueel/nieuws/2017/december/6/commissariaat-voor-de-media-en-agentschap-telecom-tekenen-samenwerkingsprotocol. [Accessed 28 12 2018].

[120] Staatscourant , "Samenwerkingsprotocol AT en Commissariaat voor de Media," *Staatscourant ,* vol. 2017, no. nr. 71816, 2017.

[121] Autoriteit Persoonsgegevens (AP), "Nationale samenwerking - Agentschap Telecom (AT)," [Online]. Available: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/convenant_cbp-agentschap_telecom.pdf. [Accessed 18 01 2019].

[122] International Organization for Standardization (ISO), "ISO 31000:2018," [Online]. Available: https://www.iso.org/standard/65694.html . [Accessed 12 11 2018].

[123] International Organization for Standardization (ISO), "IEC 31010:2009 Risk management -- Risk assessment techniques," [Online]. Available: https://www.iso.org/standard/51073.html. [Accessed 19 11 2018].

[124] International Organization for Standardization (ISO), "ISO/IEC 27005:2018," [Online]. Available: https://www.iso.org/standard/75281.html. [Accessed 12 11 2018].

[125] NIST, "Guide for Conducting Risk Assessments - NIST Special Publication 800-30 Revision 1," National Institute of Standards and Technology, Gaithersburg, MD, 2012.

[126] Agentschap Telecom, "Staat van de Ether - Continuïteit van netwerken," 08 06 2017. [Online]. Available: https://magazines.agentschaptelecom.nl/staatvandeether/2016/01/continuiteit-van-netwerken. [Accessed 01 01 2019].

[127] Agentschap Telecom, "Staat van de Ether," 09 04 2018. [Online]. Available: https://magazines.agentschaptelecom.nl/staatvandeether/2017/01/printvriendelijke-versie#continuiteit. [Accessed 01 01 2019].

[128] A. de Ruijter and F. Guldenmund, "The Bowtie Method: a review," *Safety Science,* vol. 88, p. 211–218, 2016.

[129] CGE, "The Bow Tie Method," [Online]. Available: https://www.cgerisk.com/knowledge-base/risk-assessment/thebowtiemethod. [Accessed 12 11 2018].

[130] H. Abdo, M. Kaouk, J. M. Flaus and F. Masse, "A new approach that considers cyber security within industrial risk analysis using a cyber bow-tie analysis.," 2017. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01521762/file/elsarticle-template-harv.pdf. [Accessed 14 09 2018].

[131] UK Civil Aviation Authority, "CAP1574: Twenty-six security controls for regulation," 01 12 2017. [Online]. Available: http://publicapps.caa.co.uk/modalapplication.aspx?appid=11&mode=detail&id=8111. [Accessed 01 01 2019].

[132] AT, "Vijfstappenplan Telekwetsbaarheid (5-step plan for tele-vulnerability)," [Online]. Available: https://www.agentschaptelecom.nl/onderwerpen/telekwetsbaarheid/vijfstappenplan. [Accessed 10 01 2019].

[133] European Union, "European Commission," [Online]. Available: https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en#what-does-the-commission-do?. [Accessed 14 11 2018].

[134] Eurpoean Commission, "Press Release Mergers: Commission clears T-Mobile NL's acquisition of Tele2 NL," [Online]. Available: http://europa.eu/rapid/press-release_IP-18-6588_en.htm. [Accessed 28 11 2018].

[135] 5G-PPP, "5G PPP - The 5G Infrastructure Public Private Partnership," [Online]. Available: https://5g-ppp.eu/. [Accessed 01 12 2018].

[136] US-CERT United States Computer Emergency Readiness Team, "Understanding Denial-of-Service Attacks," 28 06 2018. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015. [Accessed 26 12 2018].

[137] European commission, "Cybersecurity Act," 11 12 2018. [Online]. Available: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en. [Accessed 09 01 2019].

Annex A. Glossary