Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Sigrid Andersen Syverud

# Security of 5G-Enabled Next Generation Emergency Communication in Norway

Master's thesis in Communication Technology

Supervisor: Ravishankar Borgaonkar & Maria Bartnes

June 2020

NTNU
Norwegian University of Science and Technology

Sigrid Andersen Syverud

# Security of 5G-Enabled Next Generation Emergency Communication in Norway

Master's thesis in Communication Technology
Supervisor: Ravishankar Borgaonkar & Maria Bartnes
June 2020

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

**Title:** Security of 5G-Enabled Next Generation Emergency Communication in Norway

**Student:** Sigrid Andersen Syverud

**Problem description:**

Nødnett is the current solution for critical communication in public protection and disaster relief in Norway. Currently, Nødnett is a TETRA-based network physically separated from the commercial mobile networks. The Norwegian government has decided, based on a socioeconomic study, that the 700 MHz frequency band currently in use in Nødnett will be made available for the commercial mobile networks (Telenor, Telia, and Ice) [25]. Hence, after the year 2026, the Norwegian Directorate for Civil Protection (DSB) reports that a dedicated TETRA network for mission critical communication is no longer an option for Norway. Further, DSB presents three different models for how Next Generation Nødnett (NGN) can be deployed in parallel with the commercial mobile networks using 4G or 5G technology, possibly after 2026 [25].

The 5th generation of mobile architecture (5G) is the latest generation of mobile technology specified by the 3GPP group. The technology is expected to have a revolutionary impact on our digitally connected society [44]. The 5G system is evolved from 4G and utilizes softwarization, virtualisation, web-based protocols, and Multi-access Edge Computing (MEC) technologies to provide enhanced mobile broadband (eMBB), massive IoT, and critical communications [44]. This results in a highly complex system compared with 4G, bringing forth new security issues and challenges [6, 18, 63].

Deploying NGN in public 5G networks would result in an even more complex system in terms of security and resiliency aspects. The information being communicated in Nødnett is highly critical compared with normal 5G networks, and vital in securing a resilient society. Therefore, there are strict requirements for coverage, reliability, and availability in NGN [26]. Hence, it is important to assess how 5G security architecture and control functions can fulfil strict the NGN requirements.

This thesis will investigate different deployment scenarios, security requirements, and threat landscape for 5G enabled NGN networks. When NGN deployment scenarios are identified, we will perform a systematic risk assessment by following the ISO/IEC 27005:2018 standard. The methodology includes defining the NGN

stakeholders, assets, threats, and threat agents. We believe our results will assist relevant stakeholders to identify and assess security risks for making secure-by design 5G enabled NGN network.

**Responsible professor:** Maria Bartnes, SINTEF
**Supervisor:** Ravishankar Borgaonkar, SINTEF

# Abstract

Public Protection and Disaster Relief (PPDR) services such as police, fire fighters, and ambulances are a critical part of our society as they keep law and order, and perform lifesaving operations. An important tool these services depend on in order to collaborate and operate efficiently is radio communication. The current solution for emergency communication in Norway is a dedicated Terrestrial Trunked Radio (TETRA)-based network. However, over the last couple of years the need for higher data rates and a more economical solution for public safety communication has grown. The term Next Generation Nødnett (NGN) refers to the future Norwegian public safety communication network. One promising solution is to integrate NGN in the commercial mobile networks, eliminating the need to operate a dedicated radio network for public safety. The commercial mobile networks are currently rolling out the new 5th generation of mobile architecture (5G) standard that is expected to facilitate innovation with one of the main use cases being critical communication. Integrating a 5G enabled NGN in the commercial mobile network could free up radio resources, be more economic, and support new and high data rate services.

However, integrating such a critical system with the commercial mobile network using new and complex technology completely changes the threat landscape. This thesis aims to assist relevant stakeholders in making 5G enabled NGN secure by design. The thesis proposes an architecture based on relevant literature and available information about similar solutions in other countries.

For such a critical system as NGN simply following best practices that aim to mitigate common vulnerabilities may not be enough as it fails to identify vulnerabilities specific to the system [59]. Hence, we perform a systematic risk assessment following the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27005 standard. Firstly, we identify NGN stakeholders, assets, and threat sources. Then, we systematically go through one section of the proposed NGN architecture at a time and identify vulnerabilities, threats, risks, and risk scenarios. The risk assessment provides a foundation and framework for future threat modellings, characterisations, and discussions related to the security of NGN. This first iteration of risk assessment may be further elaborated to cover more technical details in the future. The results may be used to prioritise resources with respect to risk mitigation techniques or prepare for different cyber failure scenarios in the future.

# Sammendrag

Nødetatene er helt avhengige av radiokommunikasjon for å samarbeide når de er på utrykningsoppdrag. Den nåværende løsningen for slik kommunikasjon i Norge heter Nødnett, og er et landsdekkende mobilt nettverk basert på Terrestrial Trunked Radio (TETRA) standarden. Vi har i løpet av de siste årene har sett en økende interesse for å oppgradere Nødnett. Neste Generasjons Nødnett (NGN) kan potensielt bli integrert i de kommersielle mobile nettverkene. I så fall trenger ikke NGN å operere et eget radionettverk kun for beredskapstjenester. 5G er den nyeste standarden brukt i kommersielle mobile nettverk og forventes åpne opp for nye bruksområder og tjenester inkludert kritisk kommunikasjon. Integrasjon av NGN i et kommersielt mobilt nettverk som bruker 5G teknologi kan frigjøre frekvensressurser, være mer økonomisk og støtte høyere datahastigheter.

Trusselbildet vil endre seg drastisk dersom man integrerer et så kritisk system i de kommersielle mobile nettverkene som bruker ny og kompleks teknologi. Vi ønsker å hjelpe relevante aktører med å designe NGN med et fokus på sikkerhet. I denne oppgaven foreslår vi en NGN arkitektur i kommersielle mobile nettverk som bruker 5G teknologi. Arkitekturen er valgt på bakgrunn av relevante artikler og lignende løsninger fra andre land.

Standardløsninger for sikkerhet kan være utilstrekkelig da de beskytter mot vanlige sårbarheter og ikke oppdager sårbarheter som er spesifikke for systemet. Derfor har vi valgt å utføre en systematisk risikoanalyse basert på ISO/IEC 27005 standarden. Først identifiserer vi NGN aktører, verdier og trusselskilder. Så går vi systematisk igjennom hver seksjon av den foreslåtte NGN arkitekturen og identifiserer sårbarheter, trusler, risikoer og risikoscenarier. Risikoanalysen bidrar med et rammevekt som kan brukes i framtidige risikoanalyser, karakteriseringer og diskusjoner relatert til NGN sikkerhet. I framtiden er det mulig å legge til eller utdype risikovurderingen med flere tekniske detaljer. Resultatene kan bli brukt til å prioritere ressursbruk til risikoreduserende tiltak eller forberede seg på ulike scenarier.

# Preface

This Master's thesis was written as the final part of a degree in Communication Technology at the at the Department of Information Security and Communication Technology (IIK) at the Norwegian University of Science and Technology (NTNU). The research was carried out between January 2020 and June 2020.

First, I would like to thank my supervisor, Ravishankar Borgaonkar, for his time, guidance, and feedback throughout this process. Also, I would like to thank my responsible professor, Maria Bartnes, for her time and input.

On a personal note, I would like to thank my family and friends for your support throughout this semester. A special thanks to my brother, Aksel Andersen Syverud, proofreading and providing comments.

# Contents

# List of Figures

# List of Acronyms

**1G** 1st generation of mobile architecture.

**2G** 2nd generation of mobile architecture.

**3G** 3rd generation of mobile architecture.

**3GPP** Third Generation Partnership Project.

**4G** 4th generation of mobile architecture.

**5G** 5th generation of mobile architecture.

**5G NSA** 5G Non-Standalone.

**5G SA** 5G Standalone.

**5G-GUTI** 5G Globally Unique Temporary Identity.

**AI** Artificial Intelligence.

**AKA** Authentication and Key Agreement.

**AMF** Access and Mobility Management Function.

**ARPF** Authentication Credential Repository and Processing Function.

**AS** Access Stratum.

**AUSF** Authentication Server Function.

**AV** Authentication Vector.

**CU** Centralised Unit.

**D2D** Device-to-Device.

**DDoS** Distributed Denial of Service.

**DoS** Denial Of Service.

**DSB** The Norwegian Directorate for Civil Protection.

**DU** Distributed Unit.

**EAP** Extensible Authentication Protocol.

**eMBB** enhanced Mobile Broadband.

**ENISA** The European Union Agency for Cybersecurity.

**eSIM** Embedded Subscriber Identity Module.

**EU** The European Union.

**gNB** next Generation' Node B.

**GSMA** Global System Mobile Association.

**IEC** International Electrotechnical Commission.

**IOPS** Isolated Operation for Public Safety.

**IoT** Internet of Things.

**IP** Internet Protocol.

**ISO** International Organization for Standardization.

**ITU** International Telecommunication Union.

**LTE** Long Term Evolution.

**MEC** Multi-access Edge Computing.

**MNO** Mobile Network Operator.

**MOCN** Multi-Operator Core Network.

**MVNO** Mobile Virtual Network Operator.

**NAS** Non-Access Stratum.

**NF** Network Function.

**NFV** Network Function Virtualisation.

**NGN** Next Generation Nødnett.

**NIST** National Institute of Standards and Technology.

**Nkom** The Norwegian Communications Authority.

**PPDR** Public Protection and Disaster Relief.

**QoS** Quality of Service.

**QR** Quick Response.

**RAN** Radio Access Network.

**RU** Radio Unit.

**SDN** Software Defined Networking.

**SEAF** Security Anchor Function.

**SEPP** Security Edge Protection Proxy.

**SIDF** Subscriber Identity De-concealing Function.

**SIM** Subscriber Identity Module.

**SLA** Service Level Agreement.

**SMS** Short Message Service.

**SUCI** Subscription Concealed Identifier.

**SUPI** Subscriber Permanent Identifier.

**TETRA** Terrestrial Trunked Radio.

**UDM** Unified Data Management.

**UDR** Unified Data Repository.

**UE** User Equipment.

**URLLC** Ultra-Reliable Low-Latency Communication.

**VNF** Virtualised Network Function.

# Chapter 1
# Introduction

Over the last couple of years, there has been a growing need for a mobile network that can support high data rates and new services for Norwegian PPDR services. This demand has proven to be hard to realise with the current isolated TETRA-based mobile network. One possible solution, that may also be more economic than maintaining a separate network running on a dedicated frequency, is to integrate public safety communication in the commercial mobile networks. 5G is currently in the standardisation and deployment stage, and is expected to introduce new use cases. One of them being mission critical communications. However, several security issues with 5G networks have already been highlighted.

In case of a 5G enabled next generation emergency communication integrated in the commercial mobile networks the threat picture may drastically change. This thesis will investigate different deployment scenarios and do a threat modelling of 5G enabled NGN. We believe our results will help provide structure to the threat picture and work as a foundation for further discussions.

## 1.1 Background and Motivation

The police, fire fighters, and ambulances are examples of PPDR services. These services play a critical part in the society by keeping law and order, rescuing lives, and responding to emergencies or disasters. When PPDR services are on rescue missions time is of the essence and even the smallest delay or disruption can have detrimental consequences.

An important tool that enables collaboration for PPDR services is radio communication. The ability to, for example, call for backup or update information about missions to other PPDR entities is vital. The different Norwegian PPDR services used to operate separate analog solutions for radio communication. In 1995 an initiative to create a shared nation wide solution for all Norwegian PPDR services started. The chosen solution for emergency communication, a nation wide mobile

network based on the TETRA standard, was officially opened in 2015. The mobile network was named Nødnett, which means emergency network in Norwegian [41, 43].

However, over the last couple of years several reasons to update Nødnett has emerged. Firstly, the Norwegian government decided in December 2017, based on a socioeconomic study [8], that the frequency band currently used by Nødnett (700 MHz) will be used by the commercial mobile networks [25, 26]. Secondly, the need for higher data rates in PPDR services has grown. Technologies like live video, augmented/virtual reality, artificial intelligence, big data, and Internet of Things (IoT) are difficult to realise with the limited data capabilities of Nødnett [25]. Hence, the Norwegian PPDR services are currently not able to benefit from these new technologies. Lastly, the current Nødnett operates 2,100 radio sites [25] that provide coverage to 86 % of the country [41]. This has proven to be both expensive and inefficient energy vice. Hence, a more sustainable solution for emergency communication is desired.

The Norwegian Directorate for Civil Protection (DSB) and The Norwegian Communications Authority (Nkom) have started to investigate different possibilities for a new solution to public safety communication in Norway, called NGN [25, 26]. They highlight that NGN can be realised inside the commercial mobile networks. These networks are currently rolling out the 5G standard specified by Third Generation Partnership Project (3GPP). DSB describe three different solutions for realising NGN inside of the commercial mobile networks [25]. The solutions have different security and economic implications.

5G aspires to deliver speed up to 1 Gbit/s with less than 10 ms latency [44]. The network utilises innovative technologies like Network Function Virtualisation (NFV), Software Defined Networking (SDN), Multi-access Edge Computing (MEC), and network slicing. This is expected to facilitate innovation and new use cases in a number of fields. 5G can provide the underlying infrastructure for future innovations such as, but not limited to, artificial intelligence, IoT, big data, and augmented/virtual reality. Such innovative technologies may be beneficial to PPDR services in the future.

Several 5G security issues have already been pointed out [6, 12, 18, 27, 63]. The ENISA threat modelling highlights issues in 5G networks that could lead to problems like leakage of confidential information, compromised subscriber privacy, loss of data, or Denial Of Service (DoS). If NGN is to be implemented using 5G technology these security issues may have detrimental consequences for the Norwegian PPDR services. There is a lack of information about implications that these security issues may have for a 5G enabled NGN architecture. This thesis aims to provide structure to the NGN threat picture and work as a foundation for further discussions.

## 1.2 Goals and Research Questions

This thesis aims to assist relevant stakeholders to identify and assess security risks for making secure-by design 5G enabled NGN network. The research questions from the project proceeding this thesis are maintained [61].

**Research question 1** *What are the misuse scenarios for NGN when 5G technology is being used?*

**Research question 2** *What are the different risks to NGN and the involved actors?*

**Research question 3** *How can we perform threat modelling for the scenario of this complex system?*

## 1.3 Related Work

Previous work has been done on the security of 5G networks. ENISA has conducted a risk assessment for 5G networks in The European Union (EU) [27]. The report follows the ISO/IEC 27005 standard and identifies 5G stakeholders, network design and architecture, assets, threats, and threat agents. The NIS cooperation group [18] has also done a risk assessment of 5G in EU. They asked all EU member states to conduct a national risk assessment which is combined to get a final report. Both of these reports are aimed at 5G in general and not a specific use case.

Milan Stojkovic [60] present different scenarios for the evolution from TETRA to Long Term Evolution (LTE) networks for public safety in Norway. However, this work focuses on LTE and not 5G networks.

The transition to NGN has been considered in different reports. Nexia Management Consulting AS and Menon Economics published a socioeconomic study of the 700 MHz frequency band ordered by Nkom [8]. They consider the growing need for broadband in emergency communication, current solutions for critical communication in different countries, and different groups of interest. They recommend that the 700 MHz frequency band gets auctioned to the commercial mobile networks. Nkom and DSB outlines the process of future work on NGN [26]. Requirements and future work related to responsibility, coverage, functionality, robustness, and security are investigated. Further DSB presents three deployment scenarios for NGN in commercial mobile networks [25]. The previous work only considers some aspects of NGN security on a high level. A risk assessment of NGN deployed with 5G technology has, to the best our knowledge, never been done before.

## 1.4 Thesis Structure

This thesis is organized into seven chapters. Following is a brief description of the chapter contents:

**Chapter 1 - Introduction** presents and motivates the topic. The research questions for the thesis is formulated and related work is mentioned.

**Chapter 2 - Background** provides relevant background theory for the thesis. The topics threat modelling, NGN, and 5G networks are presented.

**Chapter 3 - NGN architectures in 5G** establishes a 5G enabled NGN architecture based on relevant literature and solutions for public safety communication in other countries. Then, the sections of the network architecture is presented.

**Chapter 4 - 5G Security Issues** highlights security issues from the ENISA report [27].

**Chapter 5 - NGN Risk Assessment** is conducted using the ISO/IEC 27005 standard. NGN stakeholders, assets, threat sources, and security issues to NGN at specific network sections are presented.

**Chapter 6 - Discussion and Future Work** looks at limitations, open questions, and future work for the thesis.

**Chapter 7 - Recommendations and Conclusions** rounds of the thesis with a conclusion and recommendations to NGN stakeholders.

# Chapter 2
# Background

This chapter presents the background material for the thesis. Firstly, the thesis introduces what a threat modelling is, why threat modelling is important, and presents three standards that may be used for threat modelling. Then, the thesis describes background on NGN. This includes the motivation to upgrade the current public safety network, the requirements to NGN and three models for realising NGN in the commercial mobile networks. Lastly, a basic introduction of 5G networks and relevant technologies was included in the project preceding this thesis [61]. This is reviewed and amended with more relevant articles in Subsection 2.3.1 and 2.3.2. The two main parts of the 5G architecture, namely the radio access and core network are presented in Subsection 2.3.3 and 2.3.4. Lastly, in Subsection 2.3.5 important 5G services for NGN are presented.

## 2.1 Threat Modelling

This thesis performs a threat modelling of 5G enabled NGN networks. This section provides background on threat modelling. Firstly, we describe what a threat modelling is. Further more, the section looks into why threat modelling is important. Lastly, we present three threat modelling methodologies.

### 2.1.1 What is a Threat Modelling?

A threat modelling of a system is a representation of threats presented in such a way that it provides a structure, foundation for further discussions, and analyses the system [11]. The model may also be used to identify risks, understand the causes, and impact on the system [68].

The term threat is important in a threat modelling. The term has many definitions. Williams and Cavallaro define threats as a risk factor [68]. By this they mean that a threat is something or someone that can cause or increase a risk. National Institute of Standards and Technology (NIST) defines threats as any circumstance or event

that has a potential to negatively impact the organization, assets, individual, or the nation [59].

A threat modelling highlights and structures the threats of the system that is modelled. This can be done in a number of different ways. Subsection 2.1.3 will look at three specific methodologies that can be used when conducting a threat modelling. In general, different threat modeling methodologies have a different focus. Some are data-centric and focuses on protecting particular data in the system [59]. Other methodologies may be more focused on, for example, people, system, operations, or privacy concerns [57].

A risk assessment is a special case of threat modelling. Bodeau et al. states that a risk assessment is a combination of a threat model and an environmental model [11]. This environmental model can, for example, be an architecture like the 5G enabled NGN architecture presented in Chapter 3. The combination of an environmental model and a threat modelling can be used to better evaluate the likelihood and potential consequences of a threat. Chapter 5 contains a risk assessment of NGN.

Generally a threat modelling should be a continuous and dynamic process. The threat landscape is evolving with new technology and threat actors. So should the threat modelling of the system. If the threat modelling is properly conducted and updated it can be a valuable tool in making informed decisions regarding the security of the system [11].

### 2.1.2 Why is Threat Modelling important?

The goal of threat modelling is to identify threats to the system. A threat modelling can assist in catching threats from a wide spectrum of threat types [57]. If a threat modelling is performed early in the development it may identify and mitigate potential issues before the system is deployed [57].

The basic concept of threat modelling is that there is a limited amount of resources that can be used to securing the system [59]. A threat modelling may be used to make an educated prioritisation of what risk mitigation techniques to implement in the system. If this prioritisation is followed and the threat modelling is well done, and well managed, it may be a key tool in making the most cost-efficient decisions for risk mitigation in the system [68].

A result of a threat modelling is a better understanding of the root causes of risks. One threat may lead to several risks. Understanding the root causes of the risks may help to best apply risk mitigation techniques [68]. In some cases it can be beneficial to apply mitigation techniques to the threat while in other cases it may be

best to apply it on the risk. However, a threat modelling provides an overview of and assists in making educated decisions.

Performing a threat modelling is great when following best practices for security is not enough. Following best practices that aim to mitigate common threats and vulnerability may be sufficient in more simple and less critical systems. However, for more complex and security sensitive systems, best practices may be insufficient. Best practices fails to identify security issues and prioritisation that are specific to the system. For such systems, a threat modelling is usually a better solution [59].

The threat landscape is constantly changing with updates in technology. A maintained threat modelling may be used to adapt the system to the constant change. If a threat modelling is conducted and then put on a shelf it may get outdated pretty fast. An organization should constantly reassess their security defences to best protect the organisations assets.

### 2.1.3 Threat Modelling Standards

In the project proceeding this thesis the NIST Guide to Data-Centric System Threat Modeling [59], ETSI (European Telecommunications Standards Institute) TVRA [1], and ISO/IEC:27005 methodologies where presented [61]. These are widely adopted standards from reputable organisations and may be used for the threat modelling of NGN. These methodologies where reviewed in the project proceeding this thesis [61]. The presentation from the project report has been reviewed and is included below.

ISO and IEC have collaborated in the development of the ISO/IEC 27005 standard [35]. The standard contains guidelines for information security risk management. Information security risk management is crucial to efficiently identify and assess risks. It also underlines the importance of communicating risks in such a way that different stakeholders understands them. This standard has been used by the NIS cooperation group in the report on cybersecurity of 5G networks [18] and by ENISA in the threat landscape for 5G networks report [27].

The method consists of these main steps: context establishment, risk identification, risk analysis, risk evaluation, risk treatment, risk acceptance, monitoring and review, and risk communication and consultation. The standard visualises the steps in Figure 2.1.

The context includes general considerations, basic criteria, scope and boundaries of the risk assessment. Then relevant risks should be identified, analysed, and evaluated in the risk assessment. The output of the risk assessment may be used to consider risk treatments. The risks should be evaluated based on their risk level and a soothing treatment should be chosen.

In Figure 2.1 we see that the monitoring and review step may trigger a new iteration of the process described above. This step ensures that the risks are kept up to date. Communication and consultation involves reaching out to the stakeholders with relevant information about the risks. Ultimately, if conducted correctly the process may improve information security, awareness, and support decision making for the system [35].

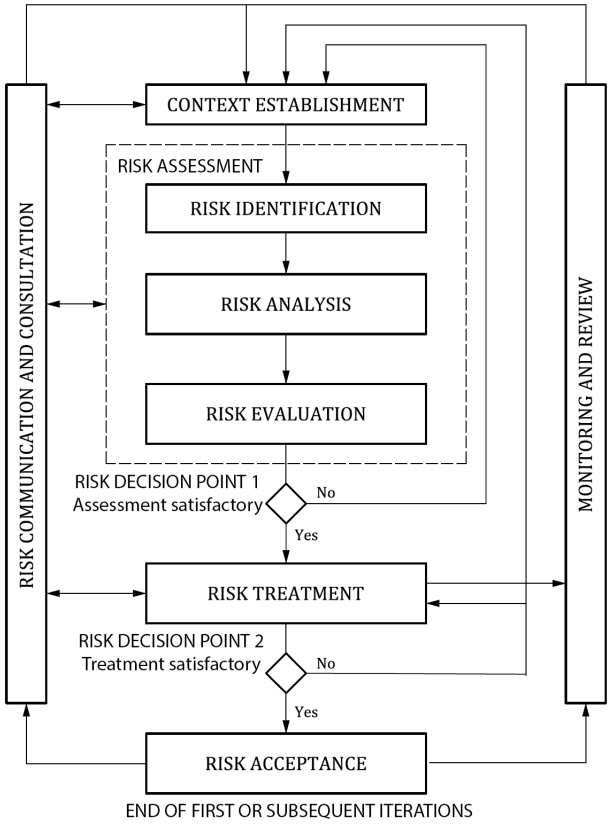



**Figure 2.1:** The information security risk management process from ISO/IEC 27005 [35]

NIST has a Guide to Data-Centric System Threat Modeling [59]. The model is called data-centric because it focuses on protecting specific types of data with an approach that goes beyond following "best practices" by considering the requirements of the specific system. NIST defines the following steps: Identify and characterize the system and data of interest, identify and select the attack vectors to be included in the model, characterize the security controls for mitigating the attack vectors, and analyze the threat model [59].

The last threat modelling methodology to be considered is the ETSI (European Telecommunications Standards Institute) TVRA (Threat Vulnerability and Risk Analysis) [1]. The process starts with identifying evaluation methods, objectives, and requirements. Then, an inventory of the assets is created. The vulnerabilities may be based on weaknesses, attack methods, and practicality. The next steps calculate the likelihood and impact of an attack and establishes risks. This can be used to find countermeasures and specify requirements for the system. UML (Unified Modelling Language) is used throughout the process to model dependencies between the system.

## 2.2 NGN

NGN is, as presented in Chapter 1, the term used for the next generation emergency communication network in Norway. One promising way of realising NGN without a dedicated broadband is to implement it in the commercial mobile networks. We want to look at models, requirements, and expectations to NGN in commercial mobile networks in order to get input as to how NGN may be deployed in a commercial 5G networks. This is revisited in Chapter 3.

This section looks at why we need NGN, the requirements of NGN, and, lastly, describes three alternatives for deploying NGN in the commercial mobile networks.

### 2.2.1 Why NGN in Commercial Mobile Networks?

There are different reasons as to why we look at NGN integrated in commercial mobile networks. Firstly, the integration may free up the dedicated frequency band currently used in the TETRA-based solution. The Norwegian government announced in 2017 that the 700 MHz radio frequency, currently used in Nødnett, will be handed to the commercial mobile networks [25]. Hence, Nødnett will no longer be able to operate on a dedicated frequency band. The background for the decision was a socioeconomic analysis of the frequency band. The conclusion, based on the growing need for broadband communication and solutions from other countries, was that running NGN in parallel with the commercial mobile networks would have the best socioeconomic effects [8].

Over the last couple of years there has also been a growing need for higher data rates in Nødnett. New technologies and innovations like live video, augmented/virtual reality, artificial intelligence, big data, autonomous cars, IoT, and other high data-rate applications have been proven hard to realise in the current TETRA-based network [25, 60]. Integrating NGN in the commercial mobile network may, therefore, open up for new possible use cases and services.

Sharing infrastructure between NGN and the commercial mobile networks may be resource-saving. NGN may save money as they do not need to manage and operate dedicated base stations for their subscribers. Also, sharing infrastructure may decrease the total power usage. Hence, it would be a more sustainable solution, compared to operating a dedicated radio network.

### 2.2.2 Requirements to NGN

PPDR services rely heavily on communication services. Therefore, it is crucial that NGN is able to meet these requirements. We presents a high level description of requirements related to coverage, reliability, and functionality.

NGN is expected to have coverage close to everywhere [25]. PPDR services may be on rescue missions in remote areas and it is desirable that they still can utilize NGN services. Currently, Nødnett has better coverage than the commercial mobile networks. Investments may be needed if NGN is to rely on the commercial mobile networks radio network by itself [25, 26].

In disaster scenarios such as extreme weather conditions, major incidents, and terrorist attacks the PPDR services may play an important part in restoring law and order. It is, therefore, important that NGN has high availability and can withstand such pressing circumstances [25]. This may, for example, be a solution that is able to operate without a radio tower or that the radio stations have backup power available.

PPDR services such as the police may handle confidential information about a current investigation. Hence, NGN will need to provide strong data security [25]. It is also important that, for example, the location of a police car is hidden, and that the NGN service is available at all times. To ensure this NGN has to provide subscriber privacy and protection against other attacks [25].

### 2.2.3 Alternatives for NGN in Commercial Mobile Networks

DSB outlines three possible deployment methods for NGN in the 2018 report about alternatives for mission-critical services in public mobile networks in Norway [25]. The report focuses on how the responsibility for the network and its components may be divided between the state, and the three mobile operators in Norway (Telenor, Telia and Ice).

The three commercial mobile network operators where asked to present how they think NGN may be realised. DSB summarized the answers into three models. In the first model (Model 1) NGN will be implemented as an MVNO where the State owns the core network and arrange to use the radio access network of all the mobile network operators. This model will, in contrast to traditional roaming-based MVNOs,

be based on the Multi-Operator Core Network (MOCN) interface, which is more secure. MOCN allows sensitive user information such as location and user activity to be hidden from the mobile operators. In this model the State has full responsibility for the end-to-end functionality and performance of the system [25].

In the second model (Model 2) the NGN services are provided by a single turnkey provider. This means that one mobile network operator will be responsible for the entire system. In Model 2 the State will not own any infrastructure. The solution can be complimented with a roaming solution for NGN users. This would add some redundancy in the radio access network [25].

The last model (Model 3) extends Model 2 by introducing several competing providers. In this model the government must decide on certain criteria the providers need to comply with in order to offer NGN services. The providers who offer NGN services would then have to compete to get customers. The responsibility for the end-to-end NGN functionality for a subscriber would then lie with the operator they are subscribed to. It is important that full interoperability for NGN on an application level is kept across operators.

These models will be revisited in Chapter 3 where we propose a 5G enabled NGN architecture based on Model 1.

## 2.3 5G Networks

This section will describe the 5G system with emphasis on the components and technologies most relevant to NGN. Firstly, we will look at what 5G is, then describe the key technologies in 5G. Further more, we will consider the two main parts of the 5G network architecture. Namely, the 5G core and access network. Lastly, we present important 5G services for NGN.

### 2.3.1 What is 5G?

Mobile communication standards are often categorised into generations where each generation represents a set of capabilities, characteristics, and requirements [62]. 1st generation of mobile architecture (1G) provided analog voice communication services. Almost all of these 1G systems are extinct, and replaced with the digital 2nd generation of mobile architecture (2G) systems. 2G is also heavily based on voice communication [62]. For the 3rd generation of mobile architecture (3G) and 4G systems the main change has been higher data throughput for the subscriber.

The 5G system poses a significant change from 4G. The new generation of mobile networking introduces softwarisation, virtualisation, web-based protocols, and MEC

technologies to provide enhanced Mobile Broadband (eMBB), massive IoT, and critical communications [44].

#### 5G Impact and Use Cases

5G is expected to have a huge impact on our society as it opens up for new use cases and facilitates innovation across industries [39]. Global System Mobile Association (GSMA) identifies five goals for the mobile industry. Namely, boundless connectivity for all, deliver networks innovatively with optimal economics, accelerate transformation of industry verticals, transform the mobile broadband experience and open up for new use cases such as IoT and critical communication [44].

The potential 5G use cases may change the way PPDR services operate. One example is the automotive industry. This is one of the industries that may potentially benefit from the 5G networks. PPDR services will often use cars or trucks when they are on rescue missions (for example police cars, ambulances or fire trucks). Potential 5G use cases in the autonomous industry like intelligent navigation, driver assistance, and data collection have a huge potential in PPDR services [39].

However, some challenges to the rollout of 5G infrastructure have been highlighted by International Telecommunication Union (ITU). They argue that 5G may increase the digital divide because it is less commercially attractive to roll out 5G in rural areas compared to cities. The digital divide may be more present in 5G compared to previous generations because of the high investment cost of 5G [65]. If NGN is implemented using 5G technology the digital divide may have negative effects on PPDR services in rural areas.

#### The Evolution from 4G to 5G

5G system will be rolled out in two phases. In the first phase, often referred to as 5G NSA, the access network will be upgraded but the system will still rely on the 4G core network [15]. Figure 2.2 illustrates the 5G NSA system. The radio access network is highlighted in red as it is different from 4G networks in a 5G NSA network.

The next deployment phase, often referred to as 5G Standalone (5G SA), includes an upgraded core network. This full 5G network supports network slicing, MEC, and the other 5G use cases. 5G SA is the system this thesis will be referring to when mentioning 5G.

### 2.3.2 5G Key Technologies

This section describes key technologies to 5G. Namely, NFV, SDN, network slicing, and MEC.

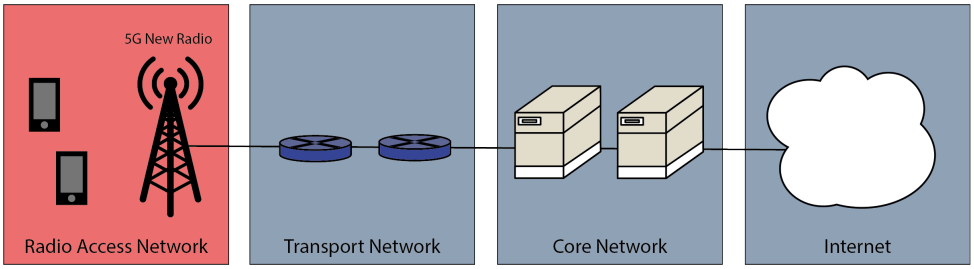



**Figure 2.2:** 5G NSA system. The illustration is derived from Vodafone [15]. The RAN is upgraded from 4G and marked in red.

### Network Function Virtualization

5G core network components will be deployed as Virtualised Network Functions (VNFs) instead of using general-purpose hardware [70]. Such VNFs may be deployed using common cloud infrastructure. The shift to NFV will make it faster and cheaper to set up new Network Functions (NFs) [30].

When different NFs are deployed on the same general-purpose hardware, isolating them from each other becomes a challenge. The VNFs may have different security requirements and have access to different information. NGN components may, for instance, be deployed on the same hardware as VNFs for commercial use. These have different security and performance requirements and should be properly isolated. Even different VNFs in the NGN architecture may have different security requirements. Proper isolation of network components is an important challenge in securing the 5G networks [6].

### Software Defined Networking

SDN is a network paradigm where network logic is decoupled from specialised pieces of hardware and moved to a centralised controller. This results in a more flexible and programmable network [30]. The 5G system benefits greatly from SDN because it makes the process of setting up network connections between VNFs fast and agile [70].

The traditional network routers would then, following the SDN paradigm, be changed into two components types, namely a centralised controller and forwarding elements. The controller controls how the forwarding elements behaves with flow rules [4]. These rules are sent over the control plane [30].

However, there are some security challenges related to SDN. The SDN controller

becomes an attractive target for an attacker as the network is so dependent on it. One way of minimizing the possible impact is by introducing multiple controllers, but that comes with challenges as well [4].

### Network Slicing

By utilising SDN and NFV, network slicing can be implemented. Network slicing is the concept of creating several virtual networks on the same physical infrastructure. Figure 2.3 illustrates the concept of network slicing. The different layers, or slices, are linked to their own use cases and provides a tailored network service. A slice can be tailored to, for example, IoT, smartphone users, or public safety like Nødnett [31].

Different customers and services have different network requirements. The current solution for creating a specialised network is to set up dedicated hardware for each service. This is a costly and time consuming approach.

Each network slice will have its own requirements specified in a Service Level Agreement (SLA) [31]. An IoT network has different, and even conflicting, requirements to, for example, Ultra-Reliable Low-Latency Communication (URLLC) [31]. A SLA can include both network connection and resource services. Network connection services can be: Near real-time latency, Seamless mobility, or Data security. Network resource services are for example: Big Data analytics, Cloud computing, or Dynamic charging [31].

When such different mobile networks are deployed on the same physical infrastructure the challenge of keeping them properly separated arises. If one slice is infected with malware or attacked by a DoS attack it is desired that the issue does not spread to the other slices. Isolating different network slices from each other is an important part of securing 5G networks.

### Multi-Access Edge Computing

MEC is a technology that decentralises the 5G architecture. Computing services are moved closer to the end-user, thus lowering the end-to-end response time [18]. This technology is key in enabling high bandwidth and low latency services [27, 50]. Different services can be contained in the same MEC host. The MEC servers would have to be deployed in multiple locations in the mobile network, this can for example be in the next Generation' Node B (gNB) [50].

Several security challenges related to MEC have been highlighted. Since the infrastructure is shared, there might be issues with malicious users producing fake traffic in order to compromise the performance of the system. It is also more

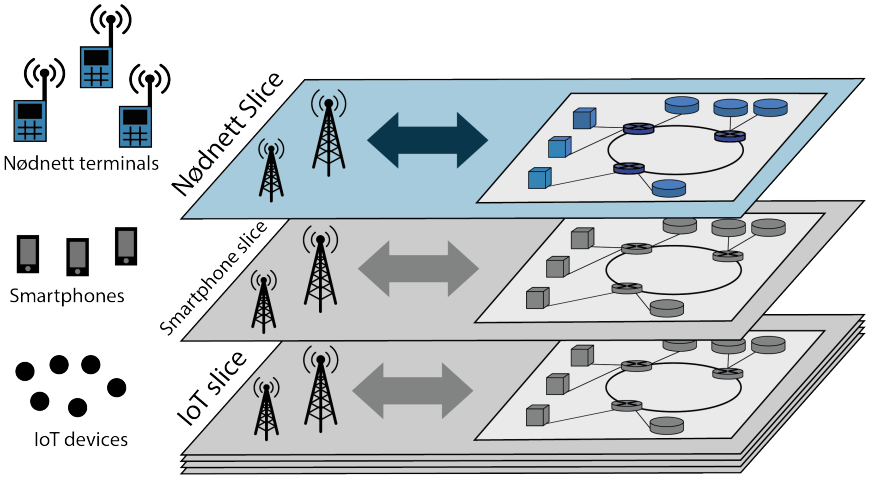



**Figure 2.3:** The concept of network slicing. The three virtual layers have different requirements but is deployed on the same shared physical infrastructure.

challenging to secure a distributed architecture from physical attacks compared to a traditional centralised system [4].

### 2.3.3 5G Radio Access Network

The RAN is the distributed part of the 5G architecture. It consists of the base stations/gNBs, user equipment, and Subscriber Identity Module (SIM). Firstly, this section describes the 5G base stations/gNBs. Then, subscription management in 5G is described. Lastly, the thesis looks at the Authentication and Key Agreement (AKA) procedure which is important for securely connecting to the mobile network and protecting the communication from and to the 5G user equipment.

#### Base Stations

The 5G base stations gNB connects the user equipment to the core network. Figure 2.4 presents the components of the 5G RAN derived from the ENISA threat landscape for 5G networks. The figure contains the gNB, and user equipment. The gNB is divided into two components, namely the Centralised Unit (CU) and the Distributed Unit (DU) [27]. Dividing the gNB into two components opens new opportunities for the access network.

The DU does not have access to any private information as the Access Stratum (AS) terminates at the CU [48]. Therefore, the need for physical protection of the DUs decreases compared to 4G base stations. This opens up for new possible locations for the Radio Unit (RU). As a result there will be more cells that the user can connect

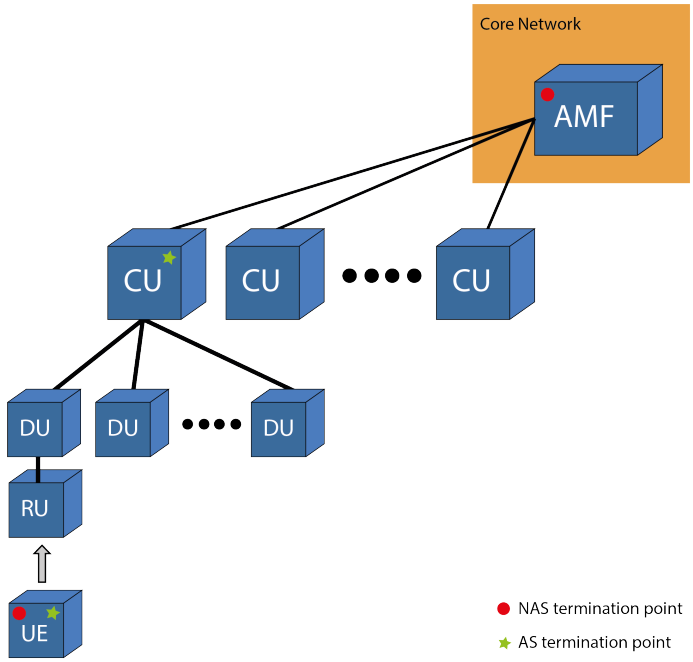



**Figure 2.4:** The 5G RAN derived from the 2019 ENISA threat landscape of 5G networks report [27].

to. The CU will be deployed on sites with a high level of physical security as the subscriber's data may only be protected by IPSec in this component [48].

Non-Access Stratum (NAS) security starts at the user equipment and terminates at the Access and Mobility Management Function (AMF) component in the 5G core network. This network function will be further described in Subsection 2.3.4.

### Subscription Management

Before an NGN device connects to the network, a subscription has to be set up. The mobile network will, traditionally, do this by issuing a SIM card to the subscriber. The SIM card contains keying material, Subscriber Permanent Identifier (SUPI), and security algorithms.

A master key, stored on the SIM, is used to securely connect the User Equipment (UE) to the network and set up a secured channel as explained in Subsection 2.3.3. The key is stored on the SIM (user side) and in the Authentication Credential Repository and Processing Function (ARPF) (network side) and will, in this solution,

never leave these two components. When a user changes to another mobile network provider a new SIM card, with a new master key, must be issued.

Embedded Subscriber Identity Module (eSIM) is an alternative to the removable SIM. The eSIM is embedded inside the mobile device. This eSIM then contains the subscriber profile of the current subscription. This includes the same information that is stored in the removable SIM [32].

When a new subscription is set up, the profile of that subscription will be installed. The user has to connect to the mobile networks remote SIM provisioning system. This can be done using a Quick Response (QR) code that contains the address of the provisioning system. The mobile phone will connect to the SIM provisioning system and download the profile in a secure manner. It is important to note that this includes sending sensitive keying and identifier information over the air and has to be done in a secure manner. Lastly, the profile is installed on the eSIM and the phone is ready to connect to the network [32].

Both eSIM and removable SIM may be used for deploying NGN. This is elaborated in Chapter 3.

#### Authentication and Key Agreement

The 3GPP's TS 33.501 defines the 5G security architecture and procedures [48]. One key part of 5G security is the primary authentication and key agreement between the UE and the core network. This procedure is divided into two phases. The first phase is the initiation of authentication and selection of authentication method. The second phase is the authentication procedure. There are two AKA procedures specified by 3GPP, both the Extensible Authentication Protocol (EAP)-AKA and the 5G AKA. This section will briefly explain AKA in 5G. For more details, look at the 3GPP technical specification [3].

The first phase initiates the authentication and selects the authentication method. The UE initiates the communication by sending a message to the Security Anchor Function (SEAF). The registration request contains a concealed identifier. This can be either a Subscription Concealed Identifier (SUCI) or a 5G Globally Unique Temporary Identity (5G-GUTI) [48].

If the UE is re-authenticating to the network the SEAF will translate 5G-GUTI to the private SUPI. Then the SEAF invokes the authentication service by sending a authentication request message to the Authentication Server Function (AUSF) of the home network of the UE. The message includes an identifier of the UE. The message also contains the name of the serving network.

Upon receiving the authentication request the AUSF will investigate if the SEAF is authorised to use the serving network name from the request. If not, the AUSF will answer that the serving network is not authorised. If the SEAF is authorised, the authentication process can continue.

The AUSF sends the identifier and serving network name to the Unified Data Management (UDM). If the identifier is concealed, the Subscriber Identity De-concealing Function (SIDF) will be invoked to de-conceal it. Lastly, the UDM/ARPF will choose the authentication method.

Now that the AKA has been initiated it is time for the second phase. There are two options for the second phase specified by 3GPP. However, they both rely on a similar procedure. We present a high level version of the procedure. A more detailed description can be found in the 3GPP technical specification [3].

Firstly, the UDM/ARPF generates the Authentication Vector (AV) using the cryptographic key pre-shared with the subscriber. The AV is used to generate a challenge that is sent to the 5G user equipment. The SIM stores the cryptographic keys and algorithms and uses it to calculate a response to the challenge from the core network. Then, the response is sent back to the core network, and the AUSF verifies that it is correct. The result of the AKA is a mutual authentication between the subscriber/user equipment and the core network. As well as the keys are distributed to the different components in the network.

### 2.3.4 5G Core Network

5G core network may be implemented using cloud technology and NFV. This is different from previous mobile networking generations who utilised specialised hardware for the different core components. The 5G core network is expected to be more flexible, agile, and scalable than the core networks of previous generations of mobile networks [70].

Figure 2.5 contains a visualisation of the 5G core network. The illustration is derived from the ENISA threat assessment, but only includes the components that are important to NGN. A more detailed explanation of the 5G core network can be found in the ENISA threat assessment [27] or 3GPP's 5G specifications [2].

The AMF connects the RAN to the 5G core. It plays an important part in the mobility and connection management of the UE [2]. Including management of handovers between gNBs. The AMF also serves as a termination point for NAS security. SEAF is co-located in with the AMF and plays an important part in the AKA procedure presented in Subsection 2.3.3.

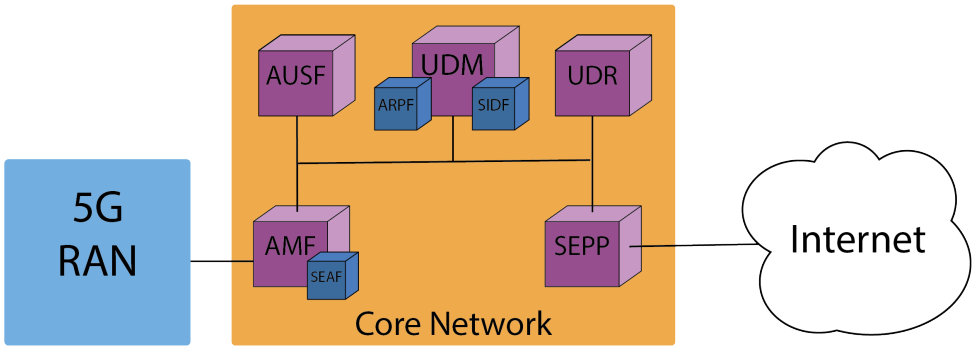



**Figure 2.5:** The 5G core network with the components that are most critical to the security of NGN.

The AUSF handles authentication requests and is essential to the AKA procedure presented in Subsection 2.3.3. It informs the UDM on the outcome of the of the authentication of a subscriber.

The UDM generates AKA credentials, handles user identification and manages subscriptions [2]. After the AKA procedure the UDM stores what AMF serves the UE. This table gets updated when the subscriber moves to the area of a new AMF. The UDM is co-located with the two security components ARPF and SIDF. The ARPF selects the authentication method and computes the corresponding authentication data and keying material [27]. It also stores the long term cryptographic keys used to secure communication in the mobile network. The SIDF de-conceals the SUPI from the SUCI. This function is important in order to ensure the privacy of the subscriber.

The Unified Data Repository (UDR) may store subscription data, policy data, structured data for exposure, and application data [2]. There may be several UDRs deployed in one core network. The UDM retrieves subscription data from the UDR. The stored application data includes packet flow descriptions [27].

The Security Edge Protection Proxy (SEPP) connects the core network to the Internet and Mobile Network Operators (MNOs) all over the world. All messages that enter or exit the core network from the Internet or other MNOs have to pass through this component. The SEPP component protects the core network from malicious packets by acting as a non-transparent proxy node and filtering the messages [3, 6]. The component also performs topology hiding.

### 2.3.5 Important 5G Services for NGN

In a disaster scenario, the physical infrastructure of a mobile network may become unavailable [22]. In such scenarios PPDR services play an important role as first responders who restore peace and rescue lives [47]. It is, therefore, crucial that NGN terminals are able to communicate in different scenarios where parts of the physical infrastructure is unavailable. This section will present different services that offer communication when the infrastructure of a network fails.

#### Device-to-Device Communication

D2D communication enables UEs who are in close proximity of each other to communicate without the involvement of a core network. In some settings they can even communicate independently of a base station. D2D may offload some of the traffic in 5G networks [72]. This technology be crucial for communication in post-disaster scenarios where the physical infrastructure is unavailable [22].

3GPP specifies three scenarios for D2D communication. The scenarios are presented in Figure 2.6. The three scenarios for D2D direct communication are:

**1** Out-of-Coverage is when none of the communicating parties can reach a gNB [37].

**2** Partial-Coverage can be used when one of the communicating parties has access to a gNB [37].

**3** In-Coverage is when both of the communicating parties are within reach of the gNB [37].

This technology is considered important for NGN because if the NGN terminals lose their connection to the gNB they will still be able to communicate. The connection can be lost in disaster scenarios or when PPDR services are on rescue missions where network coverage is limited.

#### Isolated Operation for Public Safety

As presented in Subsection 2.3.1 a mobile network consists of the access, transport, and core network. If the access network looses connection to the core it looses connectivity. Isolated Operation for Public Safety (IOPS) decreases this dependency of the core network by providing connectivity to public safety users when the connection to the core network is compromised. This is done by deploying core networks local to the base stations when needed [47].

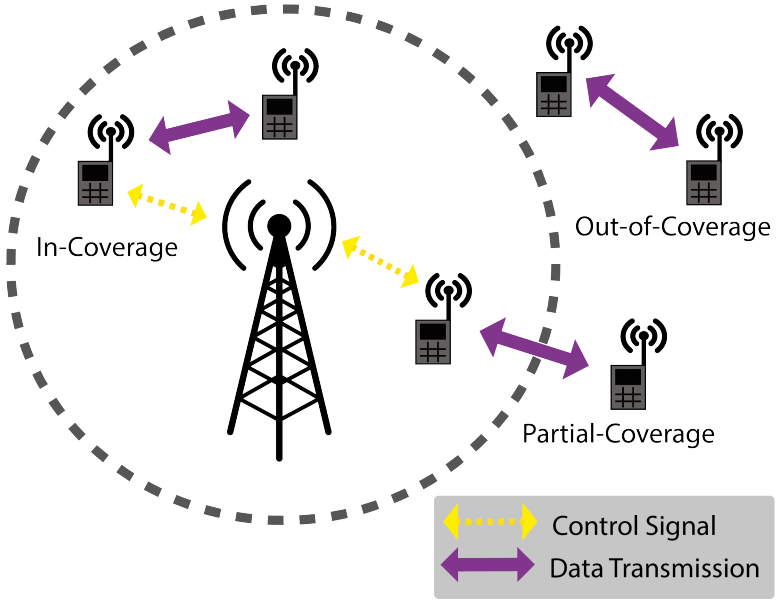



**Figure 2.6:** Three scenarios for D2D communication in 5G networks derived from U. Kar and D. Sanyal [37].

The local core network is co-located with the base station. It can have limited functionality, but must provide the network with basic mobility and security functions. In some cases the base stations are able to connect to make a larger network. In this case, there is no need for one local core for each base station. Therefore, one local core is activated whom all the other base stations are connected to [47].

The security material used when IOPS is activated is not the same as in normal operation. Dedicated IOPS security material is predistributed to the SIM and base stations. In IOPS AKA procedure is used to perform mutual authentication between the local core and UE [47].

# Chapter 3
# NGN architectures in 5G

This chapter describes an architecture for a 5G enabled NGN network. The architecture is used in the NGN risk assessment in Chapter 5. Section 3.1 describes why the thesis decided to look at NGN deployed as an MVNO. Section 3.2 contains a high-level description of the 5G enabled NGN architecture. The following sections describe the RAN and the core network of the architecture.

## 3.1 Why the MVNO Model?

Section 2.2.3 described DSB's three possible models for deploying NGN. Model 1 was a government-owned MVNO where the the State has full responsibility for the end-to-end functionality. In Model 2 the overall responsibility lays on a single provider. This means that one mobile network operator may provide all NGN services. In the 3rd model several mobile network operators may provide NGN services, and the user can choose where to by a subscription.

We have assessed Model 1, the government-owned MVNO, to be the most likely deployment scenario for 5G enabled NGN. This is the model with the most governmental control of the network and user data. The State may be able to hide sensitive information from the commercial mobile network operators while utilizing their already deployed infrastructure [25].

Belgium, The United States of America, and England have implemented public safety using LTE [9, 23, 29]. All of the three networks have a dedicated core network for public safety, and utilizes radio access network's from commercial MNOs. The Belgian LTE solution for public safety communication is called Blue Light Mobile. This solution is implemented as an MVNO and utilizes all three RANs of the Belgian commercial MNOs (Proximus, BASE and Orange) [9]. This is similar to the MVNO model from the DSB report [25].

The MVNO model is a sustainable option. Utilizing the RAN of commercial

mobile network infrastructure means that NGN does not need to build their own RAN infrastructure. Also, NGN does not need to operate dedicated base stations which could save on both operation cost and power consumption.

## 3.2 The MVNO Model Architecture for NGN

This section contains a high-level description of the architecture for 5G enabled NGN deployed as an MVNO.

As seen in Section 2.2.2 and 3.1 the implementation of NGN in commercial mobile networks may benefit from utilizing the RANs of several MNOs. It may also be beneficial that the government is in control of sensitive assets in the core network such as cryptographic keys and subscriber location. If the government is in control they have the opportunity to manage the security of the assets.

Because of these requirements and expectations for NGN we have assessed the Full MVNO model to be the best deployment model for NGN. The MVNO core network in the full MVNO model is a Full core network. Hence, the government would be in control of all core network functions (See Section 2.3.4). This would give a lot of freedom to the government to make their own decisions, implement measures, or add adjustments for NGN security. A Full MVNO may also fully manage subscribers without the MNOs knowledge [19]. The Full MVNO model is also the only model with the possibility to support the utilization of multiple RANs [20]. This could be beneficial for the resilience of NGN.

Figure 3.1 contains a high-level model of a 5G enabled NGN architecture deployed as a Full MVNO. This is the model used in the risk assessment in Chapter 5. The thesis divides the NGN architecture into the RAN and the core network.

The model only includes one RAN even though the model supports the utilization of multiple RANs. For the NGN risk assessment the thesis define security issues at the RAN and MNO core network. To translate this to a scenario with multiple RANs/MNOs the same security issues may originate from multiple MNOs/RANs. For simplicity, however, this thesis looks at the scenario of only one RAN/MNO. The RAN in this model consists of the following sections:

- **User equipment** are the components NGN subscribers may use when they connect to NGN. See Section 3.3.1 for more details on the user equipment.
- **SIM** is the government owned subscriber module on the user side. This may store the subscriber profile and cryptographic keys. Section 3.3.2 describes this in more detail.

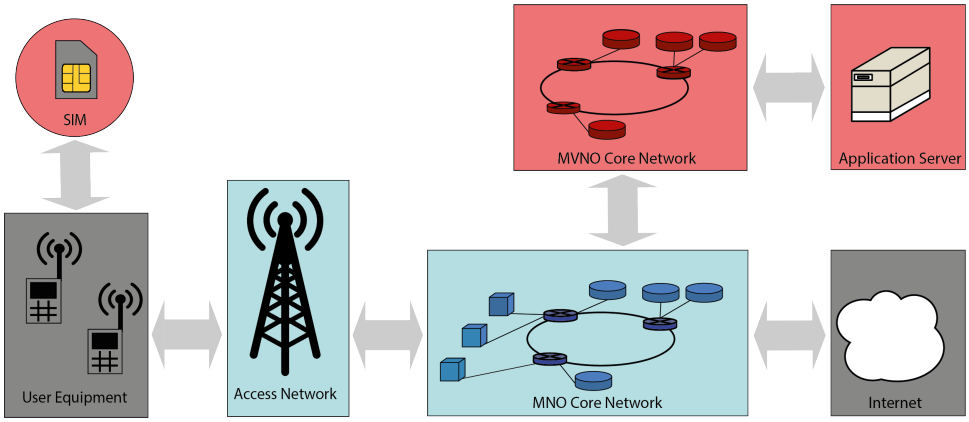



**Figure 3.1:** Architecture of a 5G enabled NGN deployed as an MVNO.

– **Base stations** are the components or radio towers that the user equipment may connect to over the air interface. This infrastructure is owned by a commercially owned MNO and connects the user equipment with the MNO core network. More details on the base stations is provided in Section 3.3.3.

The core network of the model consists of the following sections:

– **MNO core network** connects the RAN to the MVNO core. It is the same MNO that owns the base stations and the MNO core network. The MNO core network is connected to the internet. See section 3.4.1 for more details on the MNO core network.

– **MVNO core network** is the government owned core network. Section 3.4.2 provides more details on the MVNO core network.

– **NGN Application server** is the server that hosts NGN applications. It is connected to the MVNO core network. Section 3.4.3 presents more details on the NGN application server.

The model of the architecture in Figure 3.1 contains the connections between the sections of the architecture. The MNO core network connects the RAN to the MVNO core network and the Internet. The MVNO core network is connected to the NGN application server.

## 3.3 Radio Access Network

The RAN is the part of the network that connects the user to the core network. The RAN of the chosen 5G enabled NGN architecture consists of user equipment, SIM, and base stations. This section will describe the sections of the NGN RAN.

### 3.3.1 User Equipment

The NGN user equipment are the components that NGN subscribers use when they connect to NGN and access NGN services. This may, for example, be a smartphone. This section will describe some options for user equipment in NGN.

One option for NGN is to create custom made devices. Creating custom made user equipment has the benefit that the government has more control over the device and the supply chain. However, creating specialized devices in such small quantities may be expensive compared to mass-produced commercial products.

The other option is to use commercial user equipment. This may be a more cost efficient solution. Another benefit from using commercial user equipment is that NGN may be able to offer a broader selection of equipment. Instead of going through the time-consuming process of creating custom made user equipment NGN may, for example, provide a list of allowed/supported devices. This allows NGN to have some control over the devices that are used without having to go through the process of creating custom made devices. FirstNet, the public safety network in the United States of America, perform tests and certifications of user equipment [23]. They provide a list of certified devices on their web-page[1]. A similar solution may be beneficial for NGN user equipment.

However, the government will have less control over commercial user equipment. There may, for example, be applications that are not possible to delete. The commercial user equipment may also support connection to other wireless technologies like Bluetooth, Wi-Fi, or NFC. Chapter 5 presents how this could lead to security issues for NGN.

The user equipment in NGN is not limited to mobile phones. Over the last couple of years we have seen a massive growth in smart devices and IoT available to consumers. With NGN the PPDR services may utilize new types of user equipment. FirstNet supports user equipment types other than mobile phones. This includes smart watches, gateways, tablets, and laptops [24]. NGN could also support such devices.

[1] https://www.firstnet.com/content/dam/firstnet/white-papers/firstnet-certified-devices.pdf

The user equipment technology evolves rapidly. In the future, brand new user equipment like autonomous cars may be introduced to NGN. Such equipment may increase the dependency that PPDR services have on NGN.

### 3.3.2 SIM

SIM is the user side module that contains cryptographic keys, security algorithms, and subscriber profile. This module is government owned and operated. The module is somehow contained within the NGN user equipment. This sections will describe the NGN SIM in the 5G enabled NGN architecture.

There are two main options for the NGN SIM. Namely, the removable SIM and the eSIM. Section 2.3.3 described the difference between the two. The removable SIM is the traditional solution where the MNO (MVNO for the NGN architecture) issues a card that is inserted into the user equipment. eSIM is a new solution where the SIM is embedded into the phone and the MNO (MVNO for the NGN architecture) is responsible for distributing the subscriber profile. The choice of technology may impact potential vulnerabilities.

Most MNOs buy SIM cards from SIM card manufacturers [52]. The SIM is supplied pre-loaded with the cryptographic keys and security algorithms. Chapter 5 describes how this may cause security issues to NGN.

### 3.3.3 Base Stations

The 5G enabled NGN architecture this thesis considers utilises the base station infrastructure of one commercial MNO. Utilizing the same infrastructure may save money and power compared to operating dedicated base stations. In this architecture the government would have to make a deal with at least one of the three MNOs in Norway (Telenor, Telia, or Ice). The chosen MNO would own and operate the infrastructure highlighted in blue in Figure 3.1. This includes the base stations and the MNO core network.

This thesis will consider the NGN architecture where the radio access network of one MNO is being used. However, the Full MVNO models opens up the option to enter agreements with multiple commercial mobile network operators to use their infrastructure [25]. This may increase redundancy and improve coverage. If the architecture of more than one MNO is to be utilized in NGN the vulnerabilities at the MNO base stations and core network would be similar. This is because the assets at the MNOs would be the same.

Even if NGN decides to combine the coverage of several MNOs it is not very likely that the combined coverage would be sufficient for NGN [25]. Neither can it

be expected that the commercial MNOs will invest in building out the architecture so that it may meet the desired coverage for NGN [25]. It is, therefore, expected that the total coverage will be realised with a combination of commercial and private funding. This private funding should not favor one commercial mobile operator over the other [25, 26].

There are different possibilities as to what can be done on the base station level to support NGN. The base station may support D2D communication, IOPS, or deploy a network slice for NGN. These details have to be decided before the deployment of NGN. However, the thesis has not made any assumptions regarding this.

## 3.4 Core Network

The core network is the central part of NGN that provides services to the users. We consider the 5G enabled NGN architecture core network to consist of three sections. Namely, the MNO core network, MVNO core network, and the NGN application server.

### 3.4.1 MNO Core Network

The MNO core network is commercially owned and operated by the same MNO that owns the base station infrastructure. The commercially owned infrastructure is used both to serve subscribers of the MNO and NGN subscribers. However, this thesis will look at the MNO core network from the perspective of NGN.

Figure 3.1 illustrated that the MNO core network connects the RAN to the MVNO core network. Since we are considering a Full MVNO network, the main task of the MNO core network will be to provide this connection. The connection may be provided by connecting the AMFs in the core networks. The AMF in the MNO core may have a dedicated network slice for NGN.

For the MNO it is required to implement lawful interception. This enables law enforcement to gather information related to investigations. The lawful interception may be able to collect NGN related information. Also, the MNO core network may be implemented using virtual components on third party cloud servers. In Chapter 5 we describe how these implementation options may influence the NGN threat landscape.

The MNO core network is connected to the Internet and other MNOs. This is illustrated in Figure 3.1. The connection will go through a SEPP as explained in Section 2.3.4.

### 3.4.2 MVNO Core Network

The MVNO core network in the Full MVNO model offers all core network services. Hence, it is a full core network as described in Section 2.3.4. The government owned MVNO core network is connected to the MNO core network and the NGN application server as illustrated in Figure 3.1.

There are some details related to the deployment that are not specified by this thesis. Firstly, the MVNO core network may need to have a connection to the Swedish solution for public safety communication. The Swedish and Norwegian PPDR services may need to collaborate on certain operations. This is why the current Nødnett solution is connected to the Swedish public safety network. Therefore, a similar solution may be desirable for NGN as well.

Also, we do not know if NGN will need to support lawful interception. It may not need to support lawful interception as the subscribers of NGN work in public safety. However, it is hard to know at this point in time. This thesis does not specify if the MVNO core network is to be implemented using 3rd party cloud servers or not.

### 3.4.3 NGN Application Server

The NGN application server is a part of the government owned and operated architecture. It is connected to the MVNO core network as illustrated in Figure 3.1. The server may, similarly to the MVNO core network, be deployed on 3rd party cloud servers.

NGN applications can be hosted on the NGN application server. These applications can be group calls, individual calls, critical collaboration tools, live GPS tracking, and on-demand recorded or live-streaming video as seen in FirstNet [23]. The services provided by this application server are crucial for the PPDR services who use NGN. However, in future systems we may see new types of services that PPDR services are even more dependent on. This could be, for example, smart or autonomous cars that may not be able to drive without available NGN service.

# Chapter 4
# 5G Security Issues

This section summarises the security issues identified by ENISA's threat assessment of 5G [27] that are most important for NGN. More specifically, we look at security issues related to the 5G access network, core network, and generic threats.

Due to the complex nature of the system the risks and threats are yet to be fully understood [27]. It is, therefore, important to note that new 5G security issues and challenges may be identified in the future.

## 4.1 Security Issues at 5G Access Network

The access network is the consumer side of the network and consists of base stations, user equipment and SIM cards. The distributed and wireless nature of the systems exposes it to specific security issues. This section presents access network related security issues highlighted by ENISA [27].

The over the air communication from the user equipment to the base station is exposed to a number of threats as it is freely available. An attacker may flood the air interface with requests, signalling storms that overload the bandwidth at the cell, or use a jammer to disrupt the communication. It may also be possible to use spectrum resources without a license by imitating the characteristics of a legitimate user. All of these attacks have the potential to cause a DoS.

An attacker may set up a fake base station posing as a legitimate one. The fake base station can potentially be used to perform a man-in-the-middle attack, obtain the subscribers location information, and cause DoS. These threats still have to be considered in 5G because of backwards compatability with previous generations of mobile networks.

Lack of physical security of the distributed infrastructure may have severe consequences. An attacker with physical access to the mobile network equipment may

destroy, disable, or steal parts of the infrastructure. The infrastructure may also be compromised because of natural disasters causing a DoS.

The transition from traditional SIM cards to eSIM may also cause security issues. If the protocol that manages the life cycle is exploited it may cause DoS or fraud scenarios. Some user equipment, like IoT devices, may also be vulnerable to attacks. An attacker may exploit this and disclose or forge the subscribers data.

## 4.2 Security Issues at 5G Core Network

5G core networks, like the one NGN may rely on, can be deployed on cloud servers using technologies like NFV, SDN, and network slicing. This is in contrast to previous generations of mobile networks that utilize specialized hardware components to provide core network functionality. The new technology introduces new use cases and increased functionality in mobile networks [30, 44]. However, the new technology may cause new security issues. This section looks at security issues related to the 5G core network identified in the ENISA threat modelling.

Cloud servers may share resources amongst different services. This introduces several threats related to the isolation of the 5G core. ENISA highlights that an attacker who has access to one service on the cloud server may find a way to access the 5G core network. One technique that may be used is memory scraping. This is a technique where an attacker searches in physical storage hoping to find confidential information.

Another security issue, is that if one service on the cloud abuses computational resources it may affect the resources the 5G core utilizes. This could lead to reduced operations or even DoS for the 5G network. The attacker may even be able to bypass the virtual separation. This could potentially lead to loss of data confidentiality and availability.

To securely host the 5G core network on third party cloud servers the cloud service provider has to be trustworthy. A dishonest provider may find a way to interfere with the 5G core network data. Since the core network functions are all deployed as virtual components an insider in the mobile network or the service provider may install a malicious network function. The malicious network function may be used to access sensitive network functions in the 5G core network to perform attacks (for example DoS or disclosure of sensitive information).

The 5G core networks are, partly because of the high level of softwarisation and diversity of technologies, considered a highly complex system. The high level of complexity may make it difficult to design, configure, and manage the 5G core network in a secure manner. When working with such a complex systems errors are

often challenging to spot and may go unnoticed. Depending on the type of error it could potentially be exploited by an attacker to, for example, inject malware in the core network or expose confidential data. The complexity may also make it harder to detect the presence of an attacker in the system.

The network functions have a limited amount of resources. This may be exploited to flood the 5G core network components. Such an attack may be performed by using natural traffic spikes and intensify it with even more requests from, for example, an IoT botnet. The total load of traffic may be too much for the network functions to handle. Such an attack may cause DoS for the network function it is directed at.

Functions or tools in the 5G core may be abused by an attacker to obtain confidential data. The lawful interception function and audit tools have access to sensitive data in the 5G core that could be exposed if misused. An attacker may use an inside actor in the MNO to access the components to get the information. The long term cryptographic keys are also stored in the core network and may be disclosed by a privileged insider in the MNO.

Eavesdropping or sniffing of data in the network is another threat to the 5G core network. Network elements may be compromised to route data flows to an attacker to eavesdrop. Another option is sniffing data about network traffic. Network traffic may contain information about flow or traffic rules in the network.

The network traffic and configuration data in the 5G core network may be manipulated by an attacker. This may result in modification of flow priorities, rerouting of data, and unauthorised access to critical platforms. This could lead to DoS or disclosure of confidential data.

## 4.3 Generic 5G Security Issues

5G may be exposed to generic security issues related to mobile networks, IT systems, and threat sources. This section highlights generic security issues identified by ENISA [27].

The 5G network may have software or hardware vulnerabilities. Most systems have known or unknown vulnerabilities, and there is no reason to think that 5G networks will be different. An attacker may exploit vulnerabilities to compromise 5G networks. Known vulnerabilities in 5G are for example vulnerabilities from previous generations of mobile networks that may still be present in the system because of backwards compatibility.

The supply chain for 5G hardware or software may somehow be compromised. A vendor may embed vulnerabilities in the products they produce. Service providers

or third party personnel may also have privileged access to the 5G network and confidential data.

The ENISA report also highlights that other generic threats like DoS, data leakage or destruction, eavesdropping, and malicious code or software may be threats to 5G networks as well [27]. More specific threats that fall under these categories have already been highlighted in section 4.2 and 4.1.

# Chapter 5
# NGN Risk Assessment

In this chapter, we conduct a risk assessment using the ISO/IEC 27005 methodology applied to the NGN architecture from Chapter 3. The methodology has been adapted to fit our scenario and is presented in Section 5.1. Then, the thesis describes NGN stakeholders, assets and threat actors. Lastly, we present the identified vulnerabilities, threats, risks, and risk scenarios to NGN at one section of the 5G enabled NGN architecture at a time.

## 5.1 Method

Risk assessment is an important tool in making educated decisions on what should be done to secure a system. This is done by looking at may happen to a system and the potential consequences are [35]. There are different standards for risk assessments. Section 2.1.3 introduced the NIST (National Institute of Standards and Technology) Guide to Data-Centric System Threat Modeling [59], ETSI (European Telecommunications Standards Institute) TVRA [1], and ISO/IEC:27005 standards. All three standards where considered for the method of this thesis.

We chose to use the ISO/IEC 27005 for the risk assessment in this thesis. This standard has been used by EU in 5G risk assessments [18, 27]. Hence, we assessed it to be suitable for this risk assessment of the 5G enabled NGN architecture. The activities from the method have been adapted to fit our scenario. The altered method is presented in Figure 5.1.

Firstly, the risk assessment identifies NGN stakeholders in Section 5.2. Then, NGN assets, including component and key assets, is presented in Section 5.3. Threat sources are described in Section 5.4. Lastly, the NGN security issues are presented for one NGN network section at a time in Section 5.5 and 5.6. This includes identification of vulnerabilities, threats, risks and risk scenarios. The sections of the NGN network architecture is presented in Chapter 3.

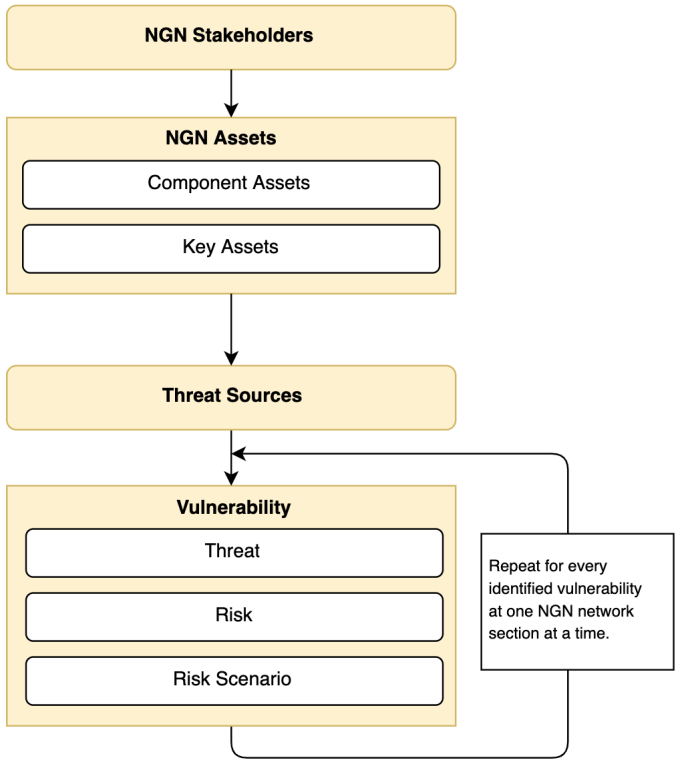



**Figure 5.1:** Activities of the NGN risk assessment.

## 5.2 NGN Stakeholders

Different stakeholders will be involved with NGN. The stakeholders may change based on architecture and technology. We define the following stakeholders for the 5G enabled NGN architecture from Chapter 3.

- **NGN operator (DSB):** The Norwegian directorate responsible for civil protection is DSB. They have the overall responsibility for NGN. However, they may outsource the daily operation and maintenance of NGN similarly to what they have done with the current TETRA-based Nødnett solution.
- **Commercial mobile network operator:** One mobile network operator will be chosen to provide NGN with functionality and access network.
- **NGN users:** Fire, police and health are the core users of NGN. Other users may for example be Red Cross and Customs [42].

– **NGN supply chain:** Different network components in NGN may rely on suppliers to provide for example hardware, operating systems, cloud infrastructure, telecommunication equipment or applications.

## 5.3 Assets

According to the ISO/IEC 27005 standard an asset is anything that has value to the organization and which, therefore, requires protection [35]. The assets in this section have been identified based on the 5G enabled NGN architecture from Chapter 3. We have divided the related assets into component and key assets.

### 5.3.1 NGN Components

A number of different components are important for NGN to operate safe and uninterrupted. These components are considered assets to NGN, and may need protection. We define the following NGN component assets:

**User Equipment:** The user equipment is used by the subscribers to access NGN. This can be for example a mobile phone, vehicle, tablet, computer, camera or a gateway.

**SIM or eSIM:** The SIM contains the cryptographic algorithms, keys and identifier of the subscriber on the client side. This can be a removable piece of hardware, usually referred to as a SIM-card. The other option is a component embedded in the user equipment called eSIM.

**gNB:** The base station (gNB) connects the user equipment with the to the core network (via the transport network). The gNB consists of the DU and the CU (see Subsection 2.3.3).

**MNO Core Network:** The commercial mobile network operator connects the gNB (via the transport network) to the MVNO core.

**MVNO Core Network:** Since we are using the Full MVNO model the MVNO core network is a full core network as described in Section 2.3.4. The MVNO core stores all cryptographic keys, handles the authentication procedure, stores subscription data, and location of all NGN users.

**NGN Application Server:** The NGN application server hosts all NGN applications and stores relevant application data.

### 5.3.2 NGN Key Assets

Key assets include other assets related to the data, privacy and services. We define the following key assets for NGN:

**Cryptographic keys:** Cryptographic keys are used to protect the data being sent in the network. Multiple keys are used in the network. All the keys are derived from a master secret key using a one-way function. The master secret key is stored in the ARPF in the core network and SIM at the client side.

**Subscriber Location:** The location of the NGN subscribers is an important asset for the privacy of the subscribers. This information may for instance be stored in the UDM in the MVNO core network. Criminals may for example want the location of the police forces.

**User Subscription Profile:** The user subscription profile contains information about the user contract. This information is for example Quality of Service (QoS) information, the subscribed user plane security policy, and the static Internet Protocol (IP) address of the user [2]. This information may be stored in the UDR in the core network.

**Subscribers' Data:** Subscribers' data can be for example phone calls, data (audio/video), and Short Message Service (SMS).

**NGN Application Data:** The NGN application server hosts NGN applications. The contents of this data depends on the type of applications that are deployed. It may for example be videos, audio recordings, or information uploaded to a collaboration tool.

**Lawful Interception:** Lawful interception is a function that performs lawful surveillance of the communication in the network. The information may be stored in the MNO or MVNO core network, and may contain information regarding NGN subscribers [27].

## 5.4 Threat Sources

Threat sources have a varying level of motivation and available means to perform a potential attack. Assessing the potential threat sources is a key part of understanding the full threat picture of NGN. We have considered threat sources from relevant literature [18, 27, 35], and applied it to NGN. Table 5.1 gives an overview of the identified threat sources. It is important to note that the threat sources are dynamic and may change over time.

Non-adversary and accidental threats are not driven by motivation. This can

| Title | Description |
|---|---|
| Non-Adversary/ Accidental | These threats may for example be related to human error or natural disasters. They are referred to as accidental because the actor does not intentionally hurt the system. |
| Individual hacker | This category consists of people that use hacking for personal financial gain, as a hobby, or for notoriety. |
| Terrorist | Terrorists usually have a political agenda with their attack. Their goal may be to spread a message, get revenge, blackmail, or get media coverage for their cause. |
| Organised crime group | This threat source is usually motivated my financial gain. However, they may also be motivated to hide criminal activities from law enforcing NGN subscribers. |
| Insider | This refers to a threat actor with access to one NGN network assets. The actor may be an employee at one of the stakeholders. |
| State or state-backed actor hacker | Certain states may be politically motivated to spy on or sabotage operations in other states. |
| Other | This can be for example industrial espionage. |

**Table 5.1:** Threat actors to NGN [18, 27, 35].

make them hard to monitor and/or predict. Human error may for example be misconfigurations, accidentally breaking or loosing equipment, and accidentally leaking information. As the 5G enabled NGN architecture is highly complex it is likely that human error will happen. However, it is hard to say where, when, and how big the error will be.

The other major category of non-adversary threat source is nature. NGN is a distributed system that is dependent on a lot of hardware. The environment the hardware is located has the potential to influence or even harm the service. This can be for example earthquakes, flooding, storm or bushfires. Similar to accidental human error these scenarios are hard to predict.

An individual hacker has limited resources, but may still be able to cause damage. This is because there may be many individual hackers, and the more hackers the more likely it is that one of them may find a vulnerability. 5G system is based on common web based technology instead of legacy protocols for mobile networks. This is different form previous generations of mobile networks. Positive Technologies highlights how this may lead to more hacking as the hackers do not have to familiarize

them selves with complicated legacy systems [63].

NGN provides critical communication that the society depends on. Hence, it may cause huge consequences if compromised. This is something that terrorists may be drawn to because of the potential media coverage. A terrorists group may combine a conventional terrorist attack such as for example a mass shooting or bombing with an attack on NGN. PPDR services are a key part of stopping and saving lives in a the scenario of a terrorist attack. Therefore, the combination of a conventional terrorist attack and an attack on NGN may cause even more damage than the conventional terrorist attack alone. Hence, attacking NGN may result in more media coverage and attention for a terrorists' political agenda.

Organized crime groups are usually more resourceful than a single hacker. They are, usually, motivated by money [18] and will, therefore, want to bring in more money than they spend. Potential consequences can be for example ransom, information bribery or fraudulent act [35]. However, in relation to NGN, an organized crime group may also be motivated to hide illegal activities from the police, obtain information about ongoing investigations, and hinder PPDR services in stopping illegal activities.

An insider will, usually, need less resources to compromise the system. They may have access to assets and a higher knowledge of the system. The motivation may be that they collaborate with one of the other threat actors, financial gain, or that they are angry with the company/stakeholders.

State or state-backed hackers are a highly resourceful threat source. The NIS assessment highlights that several EU-member states have identified particular non-EU countries to be a cyber threat. The Norwegian Intelligence Service's assessment of current security challenges also identifies that nation states may utilize cyber space not only to collect intelligence, but also to for effect-based operations [53].

Other threat sources include industrial espionage. This threat source is not considered relevant to NGN. There are no companies that will compete with NGN for customers. Similar services will mainly be mission-critical communications in other countries and we do not find it likely that they would want to spy on NGN.

## 5.5 NGN Radio Access Network Security Issues

This section describes vulnerabilities, threats, risks, and risk scenarios to NGN at the access network one component at a time. We consider the user equipment, SIM, and base station, respectively.

### 5.5.1 User Equipment

We define the vulnerabilities (V-1 to V-6) and related threats, risks, and risk scenarios to NGN at the NGN user equipment as follows:

**V-1 Lack of protection of NGN user equipment:**

The NGN user equipment is mobile, and will be used by PPDR services on rescue missions. NGN user equipment may be, for example, smartphones, autonomous cars, laptops, or IoT devices. These devices will have different levels of protection.

**Threat:**

**(1)** A threat actor may, if the user equipment is not properly physically protected, steal NGN user equipment from PPDR services. The attacker can use the stolen user equipment, if not protected by a PIN or password, to listen or forge the subscriber's data.

**(2)** A threat actor with physical access to the device may install malware on it then leave it. The NGN subscriber may continue to use the user equipment unknowing of the malware installed. The malware may leak/forge subscriber's data or cause a DoS.

**Risk:**

An attacker may exploit the lack of protection of NGN user equipment to leak/forge subscriber's data or cause a DoS. If the attacker has retained control over infected hardware on the NGN user equipment it will not go away with regular software updates. Hence, the attacker may have control over the user equipment until it is replaced [49].

**Risk Scenario:**

**(1)** An organized crime group has a suspicion that they are being investigated by the police. They locate policemen in the area and steal their NGN user equipment. Then they may use the mobile phone to get information about ongoing police investigations.

**(2)** NGN user equipment may for example be autonomous cars. When an autonomous car is parked it may be possible for a threat actor with physical access (for example terrorists or an organized crime group) to install malware on the car. The malware may leak subscribers data.

**V-2 Embedded vulnerabilities from the supply chain:**

Chapter 3 described how NGN user equipment may be either custom made or commercial. In the custom made scenario the government would have more control of the supply chain. However, NGN will probably rely on third party suppliers in both scenarios.

**Threat:** It may be possible for both software and hardware suppliers to either unintentionally or intentionally embed vulnerabilities in the components [18].

**Risk:** Such vulnerabilities may be exploited by a threat actor to spy on or forge subscriber's data or compromise the availability of NGN services.

**Risk Scenario:** A nation state actor may influence an equipment supplier to embed vulnerabilities in the user equipment. Then, the nation state actor proceeds to exploit these vulnerabilities to collect intelligence on the Norwegian PPDR services [18].

**V-3 Other wireless communication allowed:**

The NGN user equipment may support non-NGN wireless communication such as Wi-Fi, NFC, or Bluetooth.

**Threat:** **(1)** An attacker may use the non NGN access to install malware on the NGN user equipment [33]. This malware may compromise the user equipment and lead to breaches in confidentiality and availability of subscriber's data. The malware may also compromise the availability of the NGN service.

**(2)** Other wireless communication technologies may leak information about what subscriber is in the area. This compromises the confidentiality of subscriber's locations [33, 69].

**(3)** An NGN subscriber may use other wireless communication technologies to send confidential data (subscriber's data). An attacker may compromise this communication link to eavesdrop on the data being communicated [33, 56].

**Risk:** NGN subscribers may use wireless communication technologies other than NGN. This connection is not managed by NGN and may be exploited by an attacker to cause a DoS for NGN subscribers or compromise the subscriber's data and location [33, 56, 69].

**Risk Scenario:** **(1)** An individual hacker or organized crime group sets up a Wi-Fi access point with poor security settings. An NGN subscriber connects to the access point and eavesdrops on all the data being communicated.

**(2)** An organized crime group may use Bluetooth communications to install malware on the NGN user equipment. Bluetooth malware may cause DoS by draining the battery of the phone, corrupting the memory card or steal subscriber's data [33].

**V-4 Lack of control of applications and software installed on NGN user equipment:**

The NGN user equipment may contain software or applications not controlled by NGN. This is primary an issue in the scenario where NGN utilize commercial user equipment.

**Threat:** Non-NGN applications like games, operating systems, or other software are not managed or controlled by NGN and may not meet NGN security requirements.

**Risk:** An NGN user may have an application or software with poor security on the NGN user equipment. An attacker may exploit vulnerabilities in the insecure software and compromise the confidentiality of the subscriber's data, and location [10].

**Risk Scenario:** An organized crime group may use an application downloaded on NGN user equipment to spy on the subscriber's data, and location.

**V-5 Lack of protection against fake base stations:**

An attacker may use a fake base station posing as a legitimate one to compromise location (privacy) of NGN users and intercept critical communication. Fake base

stations are a known security issue in previous generations (2G, 3G, and 4G) of mobile networks [27, 45, 55]. As every 5G smartphone supports connectivity to previous 2G, 3G, and 4G networks, downgrading attacks from fake base stations pose noteworthy and alarming challenges to NGN user equipments.

**Threat:**

**(1)** NGN user equipment may be compatible with previous generations of mobile networks to provide communication in areas where 5G is unavailable. These previous generations are vulnerable to fake base station attacks [27] and NGN equipment needs to be protected against them.

**(2)** 5G may also be vulnerable to fake base station attacks because of vulnerabilities in the AKA protocol.

**Risk:**

**(1)** An attacker may set up a fake base station in an area without or with 5G coverage or use other IMSI catcher techniques [13] to trick the subscriber into connecting to the fake base station over a real one. The attacker may then use the fake base station to compromise the integrity and confidentiality of the subscriber's data as well as the confidentiality of the subscriber's location [27, 36, 49].

**(2)** Borgaonkar et al. presented a privacy threat to the 4G and 5G AKA protocols [7, 12] where an attacker with using a fake base station can identify and monitor subscriber activity remotely for a long time. Activity patterns can be for example number of calls or SMSs in a given time period [12].

**Risk Scenario:**

**(1)** An organised crime group, hackers, or terrorists may set up a fake base station in an area without 5G coverage to spy on the location of the local NGN subscribers.

**(2)** An organized crime group or terrorists are planning illegal activities that they want to go unnoticed by the police. They set up a fake base station, that exploits a vulnerability in the AKA protocol, close to the local police-station to monitor the subscriber activity. The information is then used to time the illegal activities.

**V-6 Lack of protection against DoS attacks:**

DoS attacks are a term used for attacks over wired and wireless interfaces that result in a denial of service for NGN users. The NGN user equipment may be vulnerable to such attacks.

**Threat:** An attacker may for example send fake signalling messages [71], malicious SMS [66], signalling storms [28], specially crafted fuzzed packets or flooding the device with messages [21]. Such threats may cause DoS to NGN subscribers.

**Risk:** The attacker sends fake messages to the user equipment that may potentially drain the battery, overwhelm the radio resources, or lock the mobile phone into an odd state ultimately causing a DoS for the NGN user equipment [10, 54].

**Risk Scenario:** A terrorists group may combine a conventional terrorist attack with a DoS attack on NGN devices. The DoS attack on NGN may delay PPDR services in stopping the terrorist attack and saving lives.

### 5.5.2 SIM

The SIM stores the cryptographic keys, SUPI, and executes security algorithms on the user side. Chapter 2 described how the SIM is a key part of NGN subscription management. This section will look at both eSIM and traditional removable SIM as NGN may utilize both of them. We define the vulnerabilities (V-7 to V-10) and related threats, risks, and risk scenarios to NGN at the NGN SIM as follows:

**V-7 Security gap in the key distribution model for eSIM:**

eSIM uses a distribution model where keys and subscriber profiles are sent to the NGN user equipment.

**Threat:** When eSIM is used the subscriber profile is sent over the air to be installed on the user equipment. This may be exploited by an attacker.

**Risk:** Chitroub et al. presents a possible security gap in the key distribution mechanism of the eSIM [17]. An attacker can, potentially, with a combination of eavesdropping on the air interface and powerful brute-forcing tool derive the keyset and decrypt the subscribers profile. This compromises the

confidentiality of the subscriber's cryptographic keys. These keys can be used to forge and spy on the subscriber's data.

**Risk Scenario:** An organized crime group, terrorist, or individual hacker may perform an attack exploiting a vulnerability in the key distribution model of eSIM and obtain the cryptographic keys. Then, they may use the cryptographic keys to leak or forge subscriber's data, or compromise the confidentiality of subscriber's location.

**V-8 SIM card cloning:**

The SIM stores the cryptographic keys on the user side. In order to ensure secure communications, the cryptographic keys should never leave the SIM.

**Threat:** An attacker may find a way to extract the secret information stored on the SIM and make a copy of it.

**Risk:** We have previously seen attacks where an attacker is able to extract secret information from a SIM card [49, 51, 73]. These attacks have both been physical and over the air. If an attacker is able to clone an NGN SIM it would possibly compromise the confidentiality of the cryptographic keys and subscriber's data.

**Risk Scenario:** An organized crime group, terrorists, or hackers want to spy on the local police forces. They steal an NGN terminal, clone the SIM, and puts it back. The cloned SIM gets used to decrypt the subscriber's data that is sent on the air interface.

**V-9 Inadequate protection of cryptographic keys in the supply chain:**

Most telecommunication companies buy SIM cards from other companies with the cryptography keys pre-loaded on the card [52]. In addition, most of the SIM cards are manufactured in China and security keys may be deployed during the manufacturing process.

**Threat:** The supply chain of the SIM card may be compromised and leak long term cryptographic keys.

**Risk:** An attacker may hack the SIM card provider to get the cryptographic key of all NGN subscribers. This may compromise the confidentiality the subscribers data and location.

**Risk Scenario:** A nation state actor hacks a SIM card manufacturer and saves all the cryptographic keys. Further more, these keys can be used to gather intelligence on NGN subscribers data [52].

**V-10 Lack of protection from SIM malware:**

The SIM is a tiny chip running propriety operating system that executes applications related to NGN security like AKA cryptographic algorithms.

**Threat:** It may be possible to, for example, over SMS or physical access install malware on the SIM.

**Risk:** An attacker may install malware on the SIM. This could compromise the privacy of the subscriber as it opens up the possibility to spy on subscriber's data or location [40].

**Risk Scenario:** A nation state actor may use SMS to install malware on the SIM card [40]. This can be used to gather intelligence on the Norwegian PPDR services.

### 5.5.3 Base Station

The NGN user equipment connects to the base stations over a radio interface as described in Section 2.3.3. The base stations are owned and operated by the commercial MNO. Both NGN subscribers and subscribers of the commercial MNO use the infrastructure. We define the vulnerabilities (V-11 to V-16) and related threats, risks, and risk scenarios to NGN at the NGN base stations as follows:

**V-11 Lack of protection against flooding/jamming:**

The communication from the user equipment to the gNB goes over the air. The air interface is available to anyone close by.

**Threat:** **(1)** The base station has a limited amount of resources. Too many requests may flood the resources and cause a DoS for NGN subscribers [27].

**(2)** Jamming is a way to disrupt the radio interface by generating a lot of noise on the correct frequency. If the jamming is successful, messages from a legitimate user will be ruined causing a DoS [51].

**Risk:** An attacker utilizes jamming/flooding technologies to cause a DoS for the NGN subscribers in that area.

**Risk Scenario:** **(1)** An organized crime group may install botware on IoT devices with poor security to create a botnet. The botnet can then be used to flood the local base stations and cause a DoS [6].

**(2)** A terrorists may want to prevent or delay the interference of PPDR in stopping a conventional terrorist attack. They may use a jammer to cause DoS for all NGN subscribers close by. The compromised NGN service may delay the PPDR services in stopping the terrorist attack.

### V-12 Limited physical protection of the DU:

The distributed part of the 5G gNB is the DU. This unit may have limited physical protection as compared with CU. They may in 5G, for example, be placed more on the top of bus sheds or lampposts.

**Threat:** Because of the limited physical protection attackers may get physical access to the DU. The physical access may be used to compromise the service of NGN subscribers.

**Risk:** By obtaining physical access to a DU an attacker can break it to compromise the service in that area. If there is no redundant coverage in the area this DU covers the NGN subscribers in the area may experience a loss of service. The broken DU would also have to be repaired or replaced. This may have financial consequences.

**Risk Scenario:** An organized crime group or terrorists may break DUs causing a local outage and financial loss. The goal for the threat actor may be to get revenge on PPDR services or media coverage on their cause.

### V-13 Limited physical protection of the CU:

The CU is the centralised part of the gNB. It will, more likely, have better physical security than the DU. However, it will still be distributed across the country. Hence, an attacker may be able to obtain physical access to the CU.

**Threat:** **(1)** The attacker with physical access to the CU may use this to break or damage the infrastructure. This may cause local outages and financial loss.

**(2)** An attacker may exploit hardware/software vulnerabilities to bypass the IPSec protection and see the data in clear [14]. This may compromise the confidentiality of subscriber's data.

**Risk:** An attacker with physical access to the CU may compromise the availability of NGN services or the confidentiality of subscriber's data.

**Risk Scenario:** **(1)** An organized crime group, nation state actor or terrorist may obtain physical access to CUs and exploit hardware/-software vulnerabilities to bypass the IPSec protection [14] to spy on the operations of the local PPDR services.

**(2)** An organized crime group or terrorist may obtain access to CUs to break or damage it. This may result in a local outage for NGN subscribers.

**V-14 Dependency on power supply:**

The base stations are dependent on power supply to provide service to NGN subscribers. Some, but not all, of the base stations may have access to backup power, but it would only last for a limited amount of time.

**Threat:** The dependency may lead to a loss of service for NGN subscribers in the scenario of a power outage [18]. A power outage may originate from, for example, natural disasters or cyber attacks.

**Risk:** A power outage would, most probably, result in a limited NGN service [18]. In scenario of, for example, a natural disaster the PPDR services may play a crucial role as first responders. The limited NGN service may therefore be have immense consequences if it delays the PPDR services' operations.

**Risk Scenario:** Either a non-adversary threat like flooding, storm, earthquake or a targeted attack may cause a power outage.

**V-15 Insufficient protection of IOPS security material:**

Chapter 2 described how IOPS may be used in order to provide service to NGN subscribers in scenarios where the access network looses connection to the core network in 5G.

**Threat:** The local core used in IOPS is co-located with the gNB. This includes storage of the IOPS security material [47].

**Risk:** An attacker with physical access to the gNB is able to access the IOPS security material. If NGN gets compromised and has to rely on IOPS the attacker will have access to all subscriber's data.

**Risk Scenario:** An organised crime group gains physical access to the gNB and copies all the secret keys for IOPS. In a future scenario where NGN has to use IOPS the organised crime group is able to eavesdrop on the subscriber's data.

**V-16 Lack of isolation from the commercial MNO:**

The base station infrastructure NGN utilize is, as presented in Chapter 3, owned by the commercial MNO.

**Threat:** The MNO may have access to the information that passes through the base station.

**Risk:** Unauthorised people may be able to see subscriber's information and data that passes through the base station unencrypted.

**Risk Scenario:** An insider in the commercial MNO with access to a base station misuses this access to spy on the subscribers data.

## 5.6 Core Network Security Issues

This section presents security issues at the core network. Firstly, the we cover issues at the commercial MNO network operator. Then, security issues in the government owned MVNO core network are described. Lastly, security issues related to the NGN application server are discussed.

### 5.6.1 MNO Core Network

The MNO core network is, in relation to NGN, responsible for connecting the NGN devices to the MVNO core network. The commercially owned infrastructure is also responsible for serving their own mobile subscribers. However, for this risk assessment the focus is on the functions of the MNO core network that NGN depends on for the connectivity and their potential consequences against the NGN assets. We define the vulnerabilities (V-17 to V-20) and related threats, risks, and risk scenarios to NGN at the MNO core network as follows:

**V-17 Lack of protection against Distributed Denial of Service (DDoS) attacks:**

Botnets are an increasing security concern with the growing number of devices that are expected to be connected to the 5G network [6]. A botnet utilizes components with botware installed in order to launch the attack. Typically, a user equipment is infected by installing (silently) malicious applications or exploiting mobile OS vulnerability.

**Threat:** A botnet may consist of the infected user equipment of NGN users, other users of the commercial MNO or a combination of both. The AMF is connected to the base station, thus responsible for handling signalling traffic of NGN and non-NGN mobile devices. DDoS attack from the infected mobile devices may affect the AMF by potentially overloading its computing resources. In addition, if the base stations are compromised, they can be used to perform DDoS attack against the AMF.

**Risk:** An attacker creates/buys a botnet from an underground dark forum [34] and use it to launch a DDoS attack on the MNO core network [27, 51]. Such an attack may cause DoS for legitimate NGN users.

**Risk Scenario:** A terrorist group, hacker, organized crime group, or nation state actors may buy a botnet made up of user equipment of MNO subscribers to launch a DDoS attack on the AMF in order to get attention from the public and spread a message. The attack causes DoS for NGN subscribers and subscribers of the MNO.

**V-18 Insufficient isolation of the deployment in the cloud:**

The MNO core of 5G SA network will more likely to be deployed in the cloud. There might be other systems (such as different slices from cars or gaming services) deployed on the same third party cloud servers. In case the cloud infrastructure is developed by the MNO, the network slices for different services may be deployed on the same cloud hardware component using virtualisation techniques.

**Threat:** An attacker with malicious access to a network slice may able to bypass the isolation protection by exploiting configuration issues related to virtualisation techniques [6, 27].

**Risk:** An attacker with unauthorised access to one of the other services deployed in the cloud may find a way to compromise NGN. This can for example be by installing malware on the AMF that eavesdrop on all NGN subscriber's data being communicated. The attacker may also find a way to abuse the computational resources on the cloud server to execute DoS attacks [27].

**Risk Scenario:** **(1)** An organized crime group, nation state actor, or terrorists may gain unauthorised access to one of the other services deployed on the same cloud hardware component as the MNO core. The attacker may then find a way to bypass the isolation and install malware on the AMF of the NGN slice. The attacker then spies on NGN subscriber's data.

**(2)** An organized crime group, nation state actor, or terrorists may gain access to one network slice deployed on the same cloud hardware as NGN. The attacker may be able to eavesdrop on NGN subscriber's data on the NGN slice because of weak isolation of the slice [67].

**V-19 Embedded vulnerabilities from the supply chain:**

It may be possible for both software and hardware suppliers to either unintentionally or intentionally embed vulnerabilities in the components [18].

**Threat:** Vulnerabilities may be embedded in the AMF that manages the mobility of NGN subscriber's and all NGN subscribers data goes through. The lawful interception function in the MNO may have access to NGN subscriber's data and

location. Note that, if the NGN subscriber's data is end-to-end encrypted, an adversary needs the cryptography keys in order to decrypt it.

**Risk:** An attacker may exploit embedded vulnerabilities from the supply chain to compromise the confidentiality of the subscriber's data or the availability of NGN services.

**Risk Scenario:** **(1)** A nation state actor may influence an equipment supplier to embed vulnerabilities in the lawful interception function. Then, the nation state actor exploits that vulnerability to leak the subscriber's data and location.

**(2)** An organized crime group may pressure an equipment supplier to embed vulnerabilities in the AMF. The vulnerability may be exploited to spy on subscriber's data and location.

**V-20 Configuration errors:**

The MNO core network has a high level of complexity in terms of network deployments and management thus making it challenging to optimally configure the MNO core network [27]. Positive Technologies reports that a third of successful attacks on 4G networks where related to configuration errors [63]. This may be an even bigger issue with 5G as it is a more complex system due the high level of softwarization.

**Threat:** **(1)** The SEPP connects the MNO to other MNOs and the Internet for enabling international calls and roaming services. It also protects the core network by filtering the messages that enter and exit the network. If this component is compromised due to configuration issues, it may open opportunities for an attacker to enter the core network from anywhere in the world to launch cyber attacks similar to SS7 or Diameter based attacks [49, 51].

**(2)** The AMF may also be misconfigured in a way that leaks subscriber's data or location. If the slice is misconfigured, it can leak data to other or unauthorised network components.

**Risk:** An attacker discovers or re-use previously known configuration flaws on the components in the MNO core network. The attacker exploits such security flaws to launch an attack and may potentially compromise all NGN subscriber's data, location, service, or cause a DoS [63].

**Risk Scenario:**

**(1)** An organized crime group, hackers or nation state actors finds a misconfigured SEPP interface and exploit the related vulnerabilities to access the core network and eavesdrop on the subscriber's data and location.

**(2)** The NGN network slice on the AMF or RAN is misconfigured, resulting in a compromised isolation between the NGN slice and the other slices in the MNO. A botnet made up of IoT devices is connected to a dedicated IoT slice. The botnet is used to execute a DDoS attack on the AMF. Because of the lack of isolation, the NGN slice may be compromised from the attack originating from other network slices.

### 5.6.2 MVNO Core Network

This section considers security issues at the government owned MVNO core network. We define the vulnerabilities (V-21 to V-25) and related threats, risks, and risk scenarios to NGN at the MVNO core network as follows:

**V-21 Configuration errors:**

The MVNO core network, similarly to the MNO core, is a highly complex system. Hence, optimally designing and configuring all network functions is challenging.

**Threat:**

**(1)** The network functions that are involved in the AKA procedure (SEAF, AUSF, UDM and SIDF) are deployed on the MVNO core network. If these components are misconfigured it may result in erroneous authentications that could lead to leakage of confidential data or DoS.

**(2)** The MVNO core network may need a SEPP international exchange to connect to the neighbor countries, for example in case of Norway to the Swedish emergency network. However, the MVNO core network will probably not need to be connected MNOs in other countries. This would need to be configured on the SEPP interface.

**(3)** The MVNO core network may need a lawful interception capabilities if applicable by the local government regulation. Lawful interception interface provides access to all NGN subscriber's data and location. If misconfigured, it may collect information it is not supposed to or leak confidential information to unauthorized entities.

**Risk:** An attacker finds configuration flaws in the MVNO core network components that are exposed over the Internet. The attacker exploits the flaw to launch an attack and may, depending on the misconfigured component, compromise the confidentiality of NGN subscriber's data, profile, location, lawful interception data, secret keys or cause a DoS.

**Risk Scenario:** **(1)** A misconfiguration in the AUSF makes it accept certain authentication requests that are invalid. An organized crime group exploits this misconfiguration to forge subscriber's data or launch wireless attacks using the fake base station.

**(2)** The SEPP in the MVNO core may be misconfigured so that it connects to all MNOs. A nation state actor may use a local MNO to access the MVNO core through the misconfigured SEPP. The threat actor may then use this access to collect intelligence on Norwegian PPDR services.

**(3)** The lawful interception function in the MVNO core network may be misconfigured to collect information that it is not supposed to (for example subscriber's data or location). An insider or an adversary with access to the MVNO core network may gain access to this information and leak it.

**V-22 Insufficient isolation of the MVNO core network deployment in the cloud:**

The MVNO core may be deployed on third party cloud servers. There may be other systems deployed on the same cloud servers.

**Threat:** An attacker with access to one of the other services deployed in the cloud may find a way to install malware in the MVNO core network [27].

**Risk:** The attacker may compromise all NGN subscriber's data, profile, location, lawful interception data, secret keys or cause a DoS depending on the target component.

**Risk Scenario:** A nation state actor, hackers, or an organized crime group may get access to an application with poor security deployed on the same server as the MVNO core network. Then they may use the application to install malware on the UDM in the MVNO deployment. The malware may leak all NGN subscriber's locations.

**V-23 Embedded vulnerabilities from the supply chain:**

It may be possible for suppliers of mobile network equipment to either unintentionally or intentionally embed vulnerabilities in the core network components used by the MVNO [18].

**Threat:**

**(1)** There may be embedded vulnerabilities in the UDM/ ARPF/SIDF network functions. These network functions handle confidential data such as cryptographic keys and locations of all NGN subscribers.

**(2)** The MVNO may need a SEPP to connect to the Swedish public safety network. If the SEPP contains embedded vulnerabilities it may be exploited by a threat actor as a point of entry into the MVNO core network.

**(3)** The UDR may contain NGN subscriber profiles and application data. Embedded vulnerabilities may be exploited to leak this information.

**(4)** AUSF is the network function that handels authentication requests. Embedded vulnerabilities in the AUSF may result in erroneous or false authentications.

**Risk:**

Such vulnerabilities may be exploited by a threat actor to compromise the confidentiality of all NGN subscriber's data, profile, location, lawful interception data, cryptographic keys, or cause a DoS.

**Risk Scenario:**

**(1)** A nation state actor may influence an equipment supplier to embed vulnerabilities in the ARPF core network component. Then, the nation state actor may exploit this vulnerability in a targeted attack that exposes NGN cryptographic keys.

**(2)** A nation state actor may influence a supplier to embed vulnerabilities in the SEPP. Then, the vulnerability could be exploited to enter the network and install malware that exposes subscriber's locations.

**V-24 Lack of isolation from the MNO:**

The MVNO core network is, as presented in Chapter 3, connected to the MNO core network.

**Threat:** The connection to the MNO core may expose the MVNO core network to attacks from the MNO core network.

**Risk:** An attacker with access to the MNO core network may find a way to obtain access to the MVNO core network. The access may then, depending on the sophistication of the attack and the components the attacker has access to, be used to compromise assets on the MVNO core network. The attack may compromise the confidentiality of all NGN subscriber's data, profile, location, lawful interception data, secret keys, or cause a DoS.

**Risk Scenario:** An organized crime group or nation state actor who has gained access to the MNO core network may use this to gain access to the MVNO core network. By doing this they may be able to access subscription data stored on the UDR or the cryptographic keys stored on the ARPF.

**V-25 Flooding of MVNO core network components:**

The network functions in the MVNO core network have limited capacity. An attacker may take advantage of this to cause DoS for NGN subscribers [51]. This can be done for example by using a botnet to perform a DDoS attack.

**Threat:** **(1)** If a massive number of authentication requests are sent to the AUSF at the same time they may not be able to answer authentication requests from legitimate NGN subscribers. ENISA highlights that an attacker may take advantage of natural authentication traffic spikes by amplifying it with even more traffic [27].

**(2)** The AMF may also be subject to flooding attacks. If there are massive amounts of simultaneous requests it may not be able to serve requests originating from legitimate NGN subscribers.

**Risk:** An attacker may use flooding techniques to cause DoS for NGN subscribers [49].

**Risk Scenario:** **(1)** An organized crime group, nation state actor, or hackers may utilize a botnet in combination with natural authentication spikes to cause DoS for authentication in NGN.

**(2)** An organized crime group, nation state actor, or hackers may generate a massive amount of requests from one device to the AMF in the MVNO core network. This may cause a DoS for all NGN communication except for D2D or IOPS.

### 5.6.3 NGN Application Server

The NGN application server hosts NGN applications. This includes storing NGN application data and handling requests from NGN subscribers. We define the vulnerabilities (V-26 to V-28) and related threats, risks, and risk scenarios to NGN at the NGN application server as follows:

**V-26 Lack of protection against DoS attacks:**

The NGN application server may be vulnerable to attacks that cause DoS for NGN subscribers.

**Threat:** **(1)** An attacker may flood the application server with requests by sending a massive amount of requests causing a DoS for legitimate NGN subscribers.

**(2)** Specially crafted messages may exploit a vulnerability on the server and cause DoS for NGN services [16].

**Risk:** An attacker may perform a DoS attack on the NGN application server causing DoS for all NGN subscribers. The NGN subscribers may then be compromised to limited functionality provided by for example D2D communication or IOPS.

**Risk Scenario:** **(1)** A terrorist group may perform a DDoS attack using an botnet of IoT devices. The attack may compromise the service of NGN subscribers causing a lot of media coverage on terrorist group.

**(2)** An organized crime group may send a specially crafted message to the application server causing a DoS for NGN services. The organized crime group may then demand a ransom to stop the attack.

**V-27 Insufficient isolation of the NGN application server deployment in the cloud:**

The NGN application server may, as presented in Chapter 3, be deployed on third party cloud servers. There may be other systems deployed on the same cloud servers.

| | |
|---|---|
| **Threat:** | An attacker with access to one of the other services deployed in the cloud may find a way to compromise the application server deployment. |
| **Risk:** | The attack may compromise all NGN application data or cause a DoS. |
| **Risk Scenario:** | A nation state actor may get access to an application with poor security deployed on the same cloud as the NGN application server. Then they may use that application to install malware that spreads to the NGN application server deployment. The malware collects intelligence on the Norwegian PPDR services and sends it to the nation state actor. |

**V-28 Lack of access control:**

We refer to access control as the restriction of access to NGN information assets. Someone who works in health care or tolls may not need access to information about police investigations.

| | |
|---|---|
| **Threat:** | NGN subscribers work in different fields and on different projects. All NGN subscribers will, therefore, not need access to all NGN application data. |
| **Risk:** | An attacker who has access to one NGN device may use this to collect NGN application data on other PPDR services. |
| **Risk Scenario:** | An insider in health care services who are a subscriber to NGN may sell information about ongoing police investigations to an organized crime group or nation state actor. |

# Chapter 6
# Discussion and Future Work

In this Chapter we discuss the NGN risk assessment from Chapter 5. Firstly, we look at how the risk assessment may be used as a framework for performing risk assessments of other 5G enabled NGN architectures. Then, we look at different reasons why the risk assessment may have insufficient identification of threats to NGN. We look at the full ISO/IEC 27005 standard and discuss what steps the thesis did not cover. Lastly, we look at limitations for the risk assessment and future work.

## 6.1 Risk Assessments of Other NGN Architectures

The thesis consider only one type of 5G enabled NGN architecture. The reasons to choose this architecture are described in Chapter 3. However, there are numerous possible solutions for the deployment of NGN in commercial mobile networks. Three alternative deployment models where, for instance, presented in Section 2.2.3.

If another architecture were to be chosen for NGN in commercial mobile networks the threat picture may change. Hence, it may not be valid to straight forwardly apply the methodology on other NGN architectures.

However, the NGN assets will remain the same. All 5G enabled NGN deployments must, for example, have the same network components for the RAN and the core network. The core will store cryptographic keys, perform authentication, and manage mobility. These general functions are included in the MVNO core network in the NGN risk assessment in Chapter 5. A different NGN architecture may, for example, have these assets in the commercial MNO core network instead of the government owned MVNO core network. The RAN will include base stations, a type of SIM, and user equipment in all NGN architectures as well.

Security issues associated with NGN assets may be relevant in all types of 5G enabled NGN architectures. A network function that stores cryptographic keys is, for example, needed in all architectures and may be subject to similar security issues

independent of the architecture. Therefore, this thesis may be used as a framework for security evaluation of all types of 5G enabled NGN architectures.

## 6.2 Insufficient Identification of Threats

A threat modelling will never be able to include all threats and there is no reason to believe that NGN is an exception [57]. An attacker may only need one unidentified vulnerability from the threat modelling to compromise the system. With a threat modelling, especially one of such a complex system, there may always be the risk that a crucial threat will go unnoticed. If a threat is not identified by the risk assessment, NGN may miss the opportunity to implement mitigation techniques or be prepared for the attack consequences.

A similar problem may arise from the lack of details in a threat model. A model is an abstraction of the system and the threats in the threat modelling have been generalized. There may be nuances or details that the threat modelling does not describe. The thesis does not consider, for example, technical details like the length of security keys or specific software security issues. This may leave a residual unnoticed risk which has the potential to compromise the system.

The threat picture is not always constant due to mobile networks evolving with every generation. Hence, the risk assessment in this thesis may become irrelevant for the future NGN deployments. Some threats may become irrelevant because of the integration of new technologies, updates to the network, or the introduction of the new threat actors or new services exposing the mobile network to the internet.

If the risk assessment is not properly managed and frequently updated to contain future threats it may give a false impression of the overall threat picture. This may lead to decisions about the security of NGN being made based on the outdated information. Security issues may go unnoticed and unprotected. Therefore, they may be exploited by an attacker to compromise NGN.

## 6.3 Information Security Risk Management of NGN

Section 2.1.3 describes three standards that may be used for threat modelling. The ISO/IEC 27005 standard was chosen for the risk assessment of this thesis. However, the standard describes steps of a full information security risk management. This includes more steps than what this thesis covered. The steps this thesis did not cover may be considered for future work to improve the results and effectively assess risks to NGN.

The work in this thesis has mainly been related to context establishment and the risk identification with some exceptions. The main contribution to the context was establishing the 5G enabled NGN architecture. The architecture was chosen based on literature and current public safety communication in commercial mobile networks from other countries [9, 24, 25, 29]. From the risk identification section of the specification we covered the identification of assets, threats, vulnerabilities, consequences, and identified risks.

As a next step it may be interesting to look at the risk analysis, risk evaluation, risk treatment, and risk acceptance steps outlined by the standard. When these steps are completed they would output a concrete plan for how to secure NGN. However, there are some reasons as to why it may be too early to perform these steps. Firstly, the NGN specific architecture is not defined and standardised yet. The risk likelihood and impact may vary based on specific details in the architecture that has not yet been specified. It may, therefore, be early to make concrete plans for the risk treatments of NGN as per the ISO/IEC 27005 specification.

Monitoring and review, and risk communication and consultation are the last two activities described by the ISO/IEC 27005 standard. The monitoring and review ensures that the risks are kept up to date. Communication involves reaching out to the stakeholders with relevant information about the risks. Ultimately, if conducted correctly the process may improve information security awareness and support decision making for NGN [35].

## 6.4 Limitations

This section describes limitations that restricted the work of the thesis.

5G standardisation and deployments are still in the development phase and may be subjected to change before the deployment of NGN. The current Nødnett deployment will be operated and managed by Motorola until the contract ends in the end of 2026. Hence, it is desirable that a solution for NGN will be ready by 2026. By this time the 5G standards and deployments may have gone through substantial change. This is one of the reasons that the focus of this thesis is mainly on larger sections of the 5G enabled NGN network and not too detail-oriented.

Another limitation with the risk assessment of NGN is that there are still unanswered questions related to the actual NGN architecture in 5G. The architecture and some possibilities for deployment are presented in Chapter 3. Some of the open questions and details related to the network architecture may change the results of the risk assessment. This may for example be questions related to if the NGN core needs a connection to the Swedish public safety network core, what applications the

NGN application server will host, or if the NGN core will be deployed on private or public cloud servers.

Lastly, conducting the NGN risk assessment was manual labor as there is no automated tool for threat modelling of NGN. We manually browsed for vulnerabilities, assessed if they are relevant to the sections of the defined NGN architecture, and link them to threats, risks, and risk scenarios. This limits the amount of threats we where able to identify since we had a limited time to perform the steps.

## 6.5 Future Work

As previously highlighted, a threat modelling will never be able to cover all threats. However, it provides a structure, foundation for further discussions, and analyses the system [11]. This section highlights some things that the risk assessment does not cover and may be good to look at in the future.

The focus of this thesis has been more on the network side of NGN and not the application server. Application servers have a long history of being attacked. Such attacks may for example be related to SQL injections, cross site scripting, man in the middle attack, or DoS attacks or broken authentication and session management [5, 16, 38]. This is an important part of the NGN threat picture and may be interesting to explore in future work.

NGN may utilize new technologies in the field of Artificial Intelligence (AI). Virtualization technologies like SDN (Software Defined Networking) and MANO (Management and Orchestration) may utilize AI to optimize processes in the network. AI may also be introduced in NGN user equipment like autonomous cars or IoT. The Norwegian Defence Research Establishment (FFI) highlights AI as one of the future trends that may become a security challenge to electronic communication [46]. These technologies contribute to the complexity of the system and may introduce new vulnerabilities. Hence, AI may make it harder or even impossible to monitor or verify the systems. FFI also highlights that there may be a lack of experts on the topic in Norway and that using experts from other countries may be problematic. All in all the topic may introduce new and complex vulnerabilities to NGN and may be interesting to look at risks to the AI technologies in the future.

New types of user equipment may introduce new vulnerabilities to NGN. In the previous TETRA-based Nødnett the user equipment has been mainly radio terminals specialised on public safety. However, for NGN we have seen that user equipment may be different things like for example cars or IoT devices. In the future new user equipment, that we might not be able to imagine now, may be introduced in the market. If the new user equipment is to be used in NGN it is important that the

vulnerabilities and potential consequences are thoroughly investigated.

This thesis identifies vulnerabilities to NGN. However, we have not ranked or prioritized the vulnerabilities. A systematic ranking of the vulnerabilities may help an organization prioritize their vulnerability management. Common Vulnerability Scoring System (CVSS) is a widely adopted scoring system for vulnerabilities[1]. It may be interesting to apply this scoring to the vulnerabilities identified in this thesis. Such a scoring would go under the risk analysis section of ISO/IEC 27005 information security management method (see Section 6.3).

Section 6.4 presented that the NGN risk assessment in this thesis was limited by having to identify the vulnerabilities, threats, risks, and risk scenarios manually. There exists automated tools for threat modelling such as Microsoft's threat modelling tool[2]. The tool is mainly for software development, however, templates have been created for specific industries such as medical and automotive[3] [64]. Creating such an automated tool for threat modelling of NGN networks may be useful to look at in the future.

Misuse cases, contrary to use cases, is used to describe a sequence of actions that may compromise the system [58]. Sindre and Opdahl highlight how defining misuse cases may be used to define security requirements for the system [58]. This may be considered for capturing security requirements for NGN.

The thesis validated the results with relevant literature, not by arranging a workshop with relevant stakeholders and NGN actors. This may be good to do in the future to ensure that the results are valid for NGN. Relevant stakeholders may be actors at the commercial MNOs (Telenor, Telia, and Ice), DSB, or Motorola Solutions.

[1] https://www.first.org/cvss/
[2] https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
[3] https://github.com/nccgroup/The_Automotive_Threat_Modeling_Template

# Chapter 7
# Recommendations and Conclusions

The Norwegian PPDR services may have massive benefits from embracing 5G technology. Adopting new use cases may help create better and more efficient solutions. However, the new technology comes with new security issues that could have destructive consequences for the operations conducted by the Norwegian PPDR services. It is crucial to assess NGN security so that stakeholders may prepare by implementing tailored risk mitigation techniques or plan for different scenarios. This thesis proposed an architecture for a 5G enabled NGN network based on available literature [25]. The Full MVNO model gives the government most control over NGN and was, therefore, chosen for the risk assessment of the thesis.

In this thesis, following the ISO/IEC 27005 standard, we identified 28 main vulnerabilities and associated threats, risks, and risk scenarios. The risk assessment provides a foundation and framework for future threat modellings, work, and discussions related to the security of NGN. Following best-practices may not be enough, due to the complexity of the critical system. These practices only mitigate common vulnerabilities, and may fail to catch system specific and less common risks. The threat modelling of NGN may be used as a first step in creating specific security requirements and a tailored protection of NGN assets.

However, a threat modelling may never be able to identify all vulnerabilities and a threat actor only need one vulnerability to compromise the system. The thesis highlights that certain technological details, future services, and application server vulnerabilities may not be sufficiently covered by the NGN risk assessment and would be good to look more into in the future.

We recommend that NGN stakeholders create a systematic plan and enable reiterations of and expand the threat modelling to improve the information on threats to NGN. Ultimately, the threat model may be used to effectively prioritise resources and secure NGN in the best way possible. Reiterations post deployment may also be a useful tool to keep the risk mitigations up to date with the evolving

threat landscape due to the introductions of new technologies to NGN.

Creating bridges between NGN stakeholders may also be a great tool for securing NGN. A common platform, sharing of documents, and regular meetings may facilitate collaboration across fields. Such collaboration is crucial in order to detect complex vulnerabilities in the system. This may also be expanded to sharing information with public safety communication stakeholders in other countries.

All in all we see that information and knowledge is key for optimizing NGN security. Available, structured, and extensive information about the NGN threat picture may be used to make educated prioritization of resources and prepare for plausible scenarios. The NGN risk assessment contributes to information about the NGN threat picture and may be used as a framework for risk assessments of other 5G enabled NGN architectures.

# References


[1] ETSI TS 102 165-1. https://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf (Accessed: 2020-02-19), 2011.

[2] 3rd Generation Partnership Project;. 3GPP TS 23.501; System architecture for the 5G System (5GS). https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144 (Accessed: 2020-03-19), December 2019.

[3] 3rd Generation Partnership Project;. 3GPP TS 33.501; Security architecture and procedures for 5G system. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 (Accessed: 2020-03-19), September 2019.

[4] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, March 2018.

[5] O. B. Al-Khurafi and M. A. Al-Ahmad. Survey of web application vulnerability attacks. In *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, pages 154–158, 2015.

[6] 5G Americas. The Evolution of Security in 5G. https://www.5gamericas.org/the-evolution-of-security-in-5g-2 (Accessed: 2020-02-19), July 2019.

[7] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. New privacy issues in mobile telephony: Fix and verification. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, page 205–216, New York, NY, USA, 2012. Association for Computing Machinery.

[8] Nexia Management Consulting AS. Anvendelse av 700 MHz-båndet. https://www.nkom.no/aktuelt/nyheter/samfunns%C3%B8konomisk-analyse-av-700-mhz-b%C3%A5ndet (Accessed: 2020-04-03), February 2017.

[9] Astrid.be. Blue Light Mobile. https://www.astrid.be/en/bluelightmobile (Accessed: 2020-04-27).

[10] Michael Becher, Felix C Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy*, pages 96–111. IEEE, 2011.

[11] D Bodeau, C McCollum, and D Fox. Cyber threat modeling: survey, assessment, and representative framework. *HSSEDI, The Mitre Corporation*, 2018.

[12] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proceedings on Privacy Enhancing Technologies*, 2019(3):108–127, 2019.

[13] Ravishankar Borgaonkar, Andrew Martin, Shinjo Park, Altaf Shaik, and Jean-Pierre Seifert. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *Proceedings of the 11th USENIX Conference on Offensive Technologies*, WOOT'17, page 21, USA, 2017. USENIX Association.

[14] Ravishankar Borgaonkar, Kevin Redon, and Jean-Pierre Seifert. Security analysis of a femtocell device. In *Proceedings of the 4th International Conference on Security of Information and Networks*, pages 95–102, 2011.

[15] Vodafone Business. Your 5G questions. https://www.vodafone.com/business/media/document/1508878349349/vodafone_5g_explained_pocket_guide.pdf (Accessed: 2020-02-17).

[16] Enrico Cambiaso, Gianluca Papaleo, and Maurizio Aiello. Taxonomy of slow DoS attacks to web applications. In *International Conference on Security in Computer Networks and Distributed Systems*, pages 195–204. Springer, 2012.

[17] S. Chitroub, N. Zidouni, H. Aouadia, D. Blaid, and R. Laouar. SIM Card of the Next-Generation Wireless Networks: Security, Potential Vulnerabilities and Solutions. In *2018 2nd European Conference on Electrical Engineering and Computer Science (EECS)*, pages 502–509, 2018.

[18] NIS cooperation group. EU coordinated risk assessment of the cybersecurity of 5G networks. https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security, October 2019. Accessed: 2020-02-19.

[19] R. Copeland and N. Crespi. Modelling multi-MNO business for MVNOs in their evolution to LTE, VoLTE advanced polic. In *2011 15th International Conference on Intelligence in Next Generation Networks*, pages 295–300, 2011.

[20] R. Copeland and N. Crespi. Resolving ten MVNO issues with EPS architecture, VoLTE and advanced policy server. In *2011 15th International Conference on Intelligence in Next Generation Networks*, pages 29–34, 2011.

[21] D. Dagon, T. Martin, and T. Starner. Mobile phones as computing devices: the viruses are coming! *IEEE Pervasive Computing*, 3(4):11–15, 2004.

[22] G. C. Deepak, A. Ladas, and C. Politis. Robust Device-to-Device 5G Cellular Communication in the Post-Disaster Scenario. In *2019 16th IEEE Annual Consumer Communications Networking Conference (CCNC)*, pages 1–6, Jan 2019.

[23] FirstNet. Technology and Tools. https://firstnet.gov/network/TT (Accessed: 2020-04-09).

[24] FirstNet. The Network. https://firstnet.gov/network (Accessed: 2020-05-26).

[25] The Directorate for Civil Protection. Alternatives for mission-critical services in public mobile networks in Norway. https://www.nodnett.no/globalassets/ngn/20180503-conceptual-models-for-ngn-v1.0.pdf (Accessed: 2020-04-03), May 2018.

[26] The Directorate for Civil Protection and Norwegian Communications Authority. Neste generasjon nødnett i kommersielle nett. https://www.dsb.no/globalassets/dokumenter/nyheter/neste-generasjon-nodnett-i-kommersielle-nett---fremgangsmate-for-videre-arbeid.pdf (Accessed: 2020-02-24), Oct 2017.

[27] European Union Agency for Cybersecurity. ENISA THREAT LANDSCAPE FOR 5G NETWORKS. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks (Accessed: 2020-02-19), 2019.

[28] F. Francois, O. H. Abdelrahman, and E. Gelenbe. Impact of Signaling Storms on Energy Consumption and Latency of LTE User Equipment. In *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, pages 1248–1255, 2015.

[29] GOV.UK. Emergency Services Network: overview. https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network#esn-products (Accessed: 2020-04-09).

[30] 5G PPP SN Working Group. Vision on Software Networks and 5G. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_SoftNets_WG_whitepaper_v20.pdf (Accessed: 2020-03-20), 2017.

[31] GSMA. An Introduction to Network Slicing. https://gsma.com/futurenetworks/wp-content/uploads/2017/11/GSMA-An-Introduction-to-Network-Slicing.pdf, 2017. Accessed: 2020-02-19.

[32] GSMA. eSIM Whitepaper. https://gsma.com/esim/wp-content/uploads/2018/12/esim-whitepaper.pdf (Accessed: 2020-05-19), March 2018.

[33] Shaikh Shahriar Hassan, Soumik Das Bibon, Md Shohrab Hossain, and Mohammed Atiquzzaman. Security threats in bluetooth technology. *Computers & Security*, 74:308–322, 2018.

[34] Imperva. Booters, Stressers and DDoSers. https://www.imperva.com/learn/application-security/booters-stressers-ddosers/ (Accessed: 2020-06-24).

[35] ISO and IEC. ISO/IEC 27005:2018. https://www.iso.org/standard/75281.html?browse=tc (Accessed: 2020-02-19), 2018.

[36] Roger Piqueras Jover. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *arXiv preprint arXiv:1607.05171*, 2016.

[37] Udit Narayana Kar and Debarshi Kumar Sanyal. A Critical Review of 3GPP Standardization of Device-to-Device Communication in Cellular Networks. *SN Computer Science*, 1(1):37, 2020.

[38] Puspendra Kumar and RK Pateriya. A survey on SQL injection attacks, detection and prevention techniques. In *2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12)*, pages 1–5. IEEE, 2012.

[39] Arthur D. Little. Creating a GigabitSociety – The role of 5G. https://www.adlittle.com/sites/default/files/viewpoints/_vodafone-and-arthurdlittle-gigabit-society-5g-final.pdf (Accessed: 2020-04-03), March 2017.

[40] Cathal McDaid. Simjacker – Next Generation Spying Over Mobile. https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile/ (Accessed: 2020-05-26), September 2019.

[41] Nødnett. Fakta om Nødnett. https://www.nodnett.no/Nodnett/fakta-om-nodnett/ (Accessed: 2020-04-03).

[42] Nødnett. FAQ. https://www.nodnett.no/en/faq/?blockId=3279 (Accessed: 2020-04-21).

[43] Nødnett. Historien om Nødnett i Norge. https://www.nodnett.no/Nodnett/hva-er-noenett/historien-om-nodnett/ (Accessed: 2020-05-25).

[44] Emeka Obiodu and Mark Giles. The 5G era: Age of boundless connectivity and intelligent automation. https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download (Accessed: 2020-04-03), 2017.

[45] Piers O'Hanlon, Ravishankar Borgaonkar, and Lucca Hirschi. Mobile subscriber wifi privacy. In *2017 IEEE Security and Privacy Workshops, SP Workshops 2017, San Jose, CA, USA, May 25, 2017*, pages 169–178. IEEE Computer Society, 2017.

[46] Lasse Øverlier Ole Ingar Bentstuen, Bodil Hvesser Farsund and Geir Køien. Sikkerhetsutfordringer i fremtidens EKOM-tjenester. Norwegian Defence Research Establishment (FFI), February 2018.

[47] J. Oueis, V. Conan, D. Lavaux, R. Stanica, and F. Valois. Overview of LTE Isolated E-UTRAN Operation for Public Safety. *IEEE Communications Standards Magazine*, 1(2):98–105, 2017.

[48] Anand Prasad, Sivabalan Arumugam, Sheeba B, and Alf Zugenmaier. 3GPP 5G Security. *Journal of ICT*, 6_1 and 2:137–158, May 2018.

[49] Siddharth Prakash Rao, Silke Holtmanns, and Tuomas Aura. Threat modeling framework for mobile communication systems. *arXiv preprint arXiv:2005.05110*, 2020.

[50] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. Mobile edge computing, a survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78:680 – 698, 2018.

[51] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Popper. On security research towards future mobile network generations. *IEEE Communications Surveys & Tutorials*, 20(3):2518–2542, 2018.

[52] Jeremy Scahill and Josh Begley. HOW SPIES STOLE THE KEYS TO THE ENCRYPTION CASTLE. https://theintercept.com/2015/02/19/great-sim-heist/ (Accessed: 2020-05-21), February 2015.

[53] Norwegian Intelligence Service. FOCUS 2020: Assessment of current security challenges. https://forsvaret.no/fokus (Accessed: 2020-04-20).

[54] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. New Vulnerabilities in 4G and 5G Cellular Access Network Protocols: Exposing Device Capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '19, page 221–231, New York, NY, USA, 2019. Association for Computing Machinery.

[55] Altaf Shaik, Jean-Pierre Seifert, Ravishankar Borgaonkar, N. Asokan, and Valtteri Niemi. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016*. The Internet Society, 2016.

[56] Kavita Sharma and B. B. Gupta. Attack in Smartphone Wi-Fi Access Channel: State of the Art, Current Issues, and Challenges. In Daya K. Lobiyal, Vibhakar Mansotra, and Umang Singh, editors, *Next-Generation Networks*, pages 555–561, Singapore, 2018. Springer Singapore.

[57] Nataliya Shevchenko, Timothy A Chick, Paige O'Riordan, Thomas Patrick Scanlon, and Carol Woody. Threat Modeling: a Summary of Available Methods. 2018.

[58] Guttorm Sindre and Andreas L Opdahl. Capturing security requirements through misuse cases. *NIK 2001, Norsk Informatikkonferanse 2001, http://www.nik.no/2001*, 2001.

[59] Murugiah Souppaya and Karen Scarfone. Guide to data-centric system threat modeling. https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf (Accessed: 2020-02-19), 2016.

[60] Milan Stojkovic. Public safety networks towards mission critical mobile broadband networks. Master's thesis, NTNU, 2016.

[61] Sigrid Andersen Syverud. Security of next generation emergency communication in norway. Project report in TTM4502, Department of Information Security and Communication Technology, NTNU – Norwegian University of Science and Technology, Dec. 2019.

[62] Reza Tadayoni, Anders Henten, and Jannick Sørensen. Mobile communications – on standards, classifications and generations. *Telecommunications Policy*, 42(3):253 – 262, 2018.

[63] Positive Technologies. 5G SECURITY ISSUES. https://positive-tech.com/research/5g-security-issues/ (Accessed: 2020-02-19), July 2019.

[64] James Tyrrell. Threat modelling connected and autonomous vehicle cybersecurity: an overview of available tools. https://www.copperhorse.co.uk/threat-modelling-connected-and-autonomous-vehicle-cybersecurity-an-overview-of\-available-tools/ (Accessed: 2019-06-19).

[65] ITU-International Telecommunication Union. Setting the Scene for 5G: Opportunities and Challenges. https://www.itu.int/en/ITU-D/Documents/ITU_5G_REPORT-2018.pdf (Accessed: 2020-04-03), 2018.

[66] Piyush Upadhyay, William James Routt, Patrick David Wilson, Debashis Haldar, and John Chandler Witzgall. Detection and suppression of short message service denial of service attacks. https://patents.google.com/patent/US8255994B2/en (Accessed: 2020-05-26), August 2012. US Patent 8,255,994.

[67] 5G PPP Security WG. 5G PPP Phase1 Security Landscape. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf (Accessed: 2020-06-24).

[68] Tim Williams and Lorenzo Cavallaro. The Value of Threat Modelling. https://www.computerweekly.com/ehandbook/The-Value-of-Threat-Modelling (Accessed: 2020-06-04), 2014.

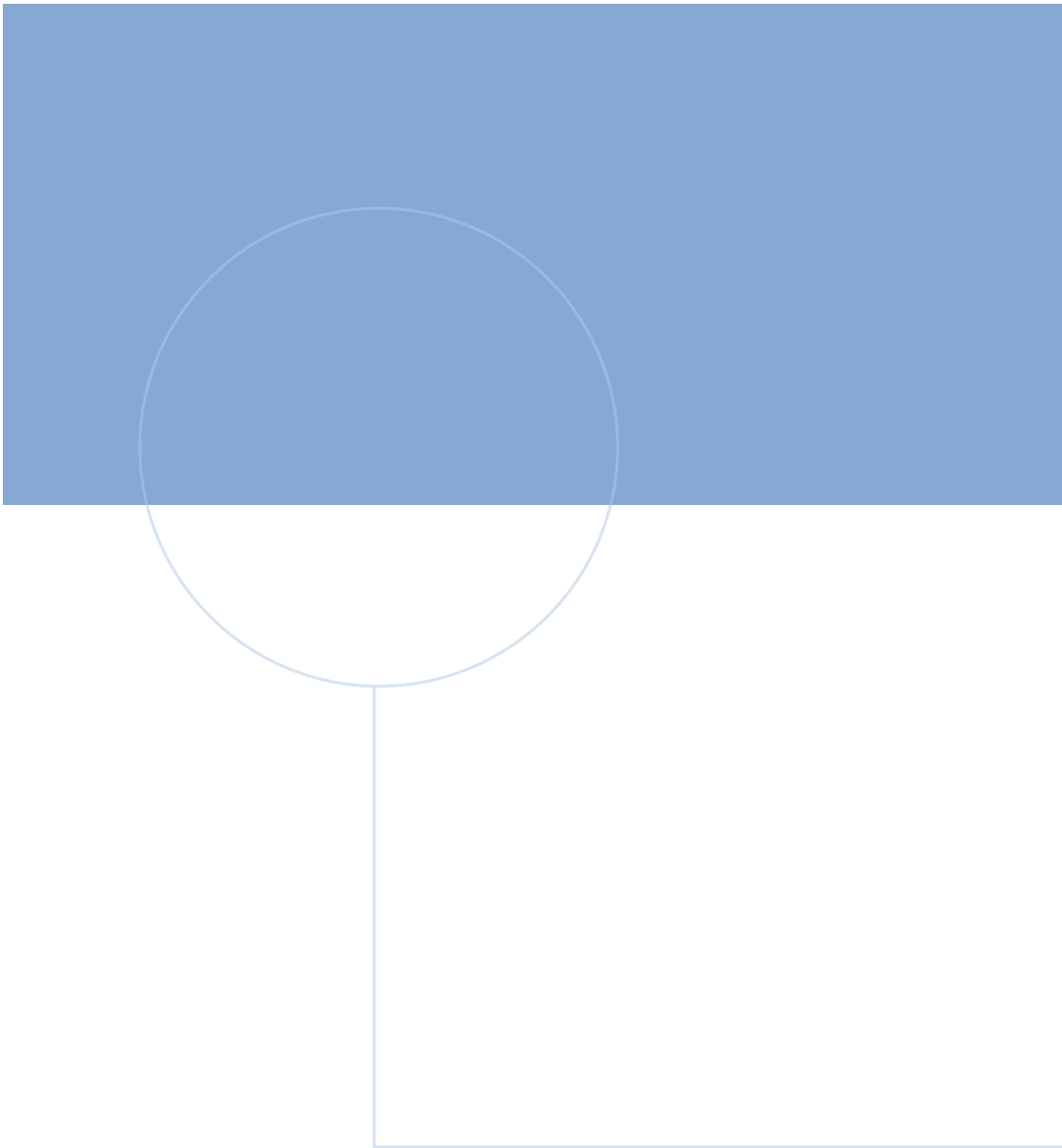
[69] Qing Yang and Lin Huang. *RFID/NFC Security*, pages 71–121. Springer Singapore, Singapore, 2018.

[70] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider. NFV and SDN—Key Technology Enablers for 5G Networks. *IEEE Journal on Selected Areas in Communications*, 35(11):2468–2478, Nov 2017.

[71] C. Yu and S. Chen. On Effects of Mobility Management Signalling Based DoS Attacks Against LTE Terminals. In *2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC)*, pages 1–8, 2019.

[72] A. Zhang and X. Lin. Security-Aware and Privacy-Preserving D2D Communications in 5G. *IEEE Network*, 31(4):70–77, July 2017.

[73] N. Zidouni, S. Chitroub, H. Chebout, and N. Boukais. New safety measure to protect the 3G/4G SIM cards against cloning. In *2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, pages 1–8, 2018.



NTNU

Norwegian University of
Science and Technology