Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Henrik Hyndøy

Cyber Security in Cellular Internet of Things

Theory versus Empiricism

Masteroppgave i Experience-based Master in Information Security
Veileder: Geir Olav Dyrkolbotn
Desember 2022

NTNU
Kunnskap for en bedre verden

Henrik Hyndøy

Cyber Security in Cellular Internet of Things

Theory versus Empiricism

Masteroppgave i Experience-based Master in Information Security
Veileder: Geir Olav Dyrkolbotn
Desember 2022

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU

Kunnskap for en bedre verden

Abstract

With the entrance of cellular technologies such as 4G and 5G telecommunication networks has become an attractive carrier option for Internet of Things (IoT). Cellular carriers comes with security implemented by the Telecommunication Operators (TELCO), a distributed access possibility and several different carriers for different use cases. However, while the cyber security of conventional IoT is broadly discussed the cellular IoT domain is less mature. Through this thesis we have tried to gain a better understanding of the threats, vulnerabilities and security measures present through a theoretical and empirical approach. By collecting perspectives from the current theory, as well as private and public actors we have gained an elevated knowledge within the cyber security of cellular IoT. The results show gaps between the theory and empiricism in both the threats, vulnerabilities and security. We believe our findings are a valuable contribution in the ongoing work to improve the security of cellular IoT and a good starting point for much needed future work.

Sammendrag

Med inntoget av mobilteknologier som 4G og 5G har telekommunikasjonsnettverk blitt et attraktivt operatøralternativ for Internet of Things (IoT). Nettene tilbyr sikkerhet implementert av mobiloperatørene, en distribuert aksesssmulighet og flere forskjellige alternative bærere ut fra brukstilfeller. Videre er det kjent at cybersikkerheten i konvensjonelle IoT er bredt diskutert, det mobile IoT-domenet er dog mindre modent. Gjennom denne oppgaven har vi forsøkt å få et helhetlig perspektiv på trusler, sårbarheter og sikkerhetstiltak som finnes i domenet. Dette har vi gjort gjennom en teoretisk og empirisk forskningsmetodikk. Ved å samle perspektiver fra teorien, samt private og offentlige aktører, har vi fått en økt kunnskap rundt cybersikkerheten i mobil IoT. Resultatene viser gap mellom teori og empiri i både truslene, sårbarhetene og sikkerhetstiltakene. Disse funnene bør brukes i videre arbeid med å sikre det mobile IoT-domenet og perspektivene diskutert i oppgaven bør vurderes i arbeidet.

Contents

Figures

Tables

Acronyms

4G Fourth Generation of Wireless Cellular Systems. iii, v, 1, 3, 10, 13–16, 31, 32, 34, 35

5G Fifth Generation of wireless cellular systems. iii, v, 1, 3, 10, 13–16, 31, 32, 35, 39, 59, 60, 63, 70

AKA Authentication and Key Agreement. 31, 32, 34, 35

APN Access Point Name. 34, 35, 38, 42

APT Advanced Persistent Threat. 7, 28, 37, 39, 40, 42, 43, 45, 51–54

BAC Building Automation and Control. 12

CA Certificate Authority. 33

DDOS Distributed Denial of Service. 8, 44

DoS Denial of Service. 30

DTLS Datagram Transport Layer Security. 33

eSIM Embedded SIM. 33

GUTI Globally Unique Temporary Identifier. 32, 34, 35

HVAC Heating, Ventilation, and Air Conditioning. 12

IETF Internet Engineering Task Force. 1, 12

IMSI International Mobile Subscriber Identity. 31, 32, 35

IoT Internet of Things. iii, v, vii, viii, 1–5, 8–13, 16, 17, 19, 21–23, 27–30, 33, 34, 37–49, 51–73, 75, 76

IoTSAFE IoT SIM Applet For Secure End-to-End Communication. 33, 41, 46, 48, 69, 70, 76

IP Internet Protocol. 1, 10, 11, 13, 14, 30, 32–34, 69, 70

IT Information Technology. 4, 39, 46, 59, 60, 62, 70

LPWAN Low Power Wide Area Network. 16, 17, 31

LTE Long Term Evolution. 13, 16, 32

LTE-M Long Term Evolution Machine-Type-Communication. 1, 3, 10, 13, 16, 31

M2M Machine-to-Machine. 2, 10, 38, 75

MAC Media Access Control address. 10

MIB Master Information Block. 32

MitM Man in the Middle. 1, 30, 32, 33, 70

MPC Mobile Packet Core. 13

NAS Non-Access Stratum. 31, 32

NBIoT Narrow Band IoT. 1, 3, 10, 13, 16, 31

NIST National Institute of Standards and Technology. 5, 8

OFDM Orthogonal frequency-division multiplexing. 15

OS Operating System. 33

P2M People-to-Machine. 2, 10

P2P People-to-People. 2, 10, 75

RAN Radio Access Network. 11, 13, 31, 59, 60

RFID Radio Frequency Identification. 10

SCTP Stream Control Transmission Protocol. 32

SIB System Information Block. 32

SIM Subscriber Identity Module. 11, 13, 33, 38–41, 47, 48, 56, 66

SMS Short Message Service. 43

SUCI Subscription Concealed Identifier. 35

SUPI Subscription Permanent Identifier. 35

TAU Tracking Area Update. 32

TELCO Telecommunication Operators. iii, 1, 2, 8, 10, 34, 39, 41, 43, 44, 46, 55, 59–62, 68, 69

TLS Transport Layer Security. 33

WAN Wide Area Network. 13

WWW World Wide Web. 1

Chapter 1

Introduction

1.1 Intro and Research Problem

The telecommunication industry is an industry that has been heavily impacted by the creation of the Internet. From being a manually line switched medium for voice calling it has turned into a medium for internet access and World Wide Web (WWW) based services[1]. A technology that has taken advantage of this is the Internet of Things (IoT) where cellular connections are one of the possible carrier technologies to serve the connectivity that the devices need to operate[2]. Technologies such as Fourth Generation of Wireless Cellular Systems (4G), Fifth Generation of wireless cellular systems (5G), Long Term Evolution Machine-Type-Communication (LTE-M) and Narrow Band IoT (NBIoT) are all examples of this and they come at a fraction of the cost compared to building conventional Internet Protocol (IP) networks to the IoT devices[3].

However, the convenience of the cellular networks comes at the price of more exposure towards a new field of threats that are not found in conventional IP networks. IoT devices are already known to be vulnerable to cyber attacks through many of the IP related protocols[2]. This has been acknowledged by Internet Engineering Task Force (IETF) though their security considerations which they have studied the past 11 year. On top of this, when introduced to the cellular network they will get exposed to additional threats specific for the domain such as eavesdropping, signal jamming and Man in the Middle (MitM) attacks[4].

It has also been acknowledged that the lack of security in cellular carried IoT environments is a theme that has not been discussed as much as regular IoT security. Tian et al claimed in [5] to be the first who had conducted an empiric study on the matter. However, this study was made with the intent to protect the Telecommunication Operators (TELCO) and not specifically the IoT devices. In 2016 Lange wrote his thesis on "*Cybersecurity in Internet of Things*" he mentioned cellular connections as a hot option for IoT[6]. However, the security challenges related to them were not discussed.

Another challenge we should address is that IoT devices typically are made to solve simple tasks such as temperature measurements, wind speeds or operate simple electric engines. Because of this the IoT devices often suffer from tight resource constraints. According to [7] this has lead the manufacturers to leave out heavy security implementations to the benefit of longer battery life. [6] also mentions this in his thesis and that the use of asymmetric crypto could lose the battle between security and battery life time even though this kind of security would give beneficial security gains.

1.2 Motivation and Justification

With the cellular networks expansion from people-to-people to also include Machine-to-Machine (M2M) and People-to-Machine (P2M) the need for cellular IoT security has increased significantly. These devices are vulnerable to threats such as (cyber)viruses, jamming and botnet recruitment and countless more. These are threats that the TELCO are not used to dealing with in the conventional People-to-People (P2P) type of communication. Because of this there is a need for better understanding of the cyber security in cellular IoT in order to protect them from the threats. However, as of now there is a lack of studies on what the threats, vulnerabilities and security measures are in the cellular IoT domain. The lack of concrete results in this field makes it difficult to secure it. Bits and pieces from papers will tell something about the problems and solutions for singular use cases, but it is not enough to gain a complete picture of the situation. Nokia, one of the largest cellular network developers, acknowledged this problem in a journal from 2019[8]. In their outlook they mention that further work should look for feasible and scalable solutions.

This thesis will seek to put light on cyber security in cellular IoT with a broader perspective than others have done before. By reading this thesis the reader should end up with a better understanding of what the possibilities, threats and values are. In addition we will compare the solutions used by organisations today against the threats that are present in the current threat picture. We believe a better understanding of the gaps between what is actually in use and what is available is essential knowledge in order to improve the security in cellular IoT.

1.3 Research Questions

Considering the challenges discussed above we will in thesis seek to get a better understanding of the cyber security in cellular IoT. This will include three main parameters that we see as natural parts of the cyber security term. First the threats, second the vulnerabilities and last the security.

The first step in achieving this will be to conduct a theory study that will review scientific work and papers. From this we should be able to identify state of the art within the scientific field of cyber security in cellular IoT. Following the three main parameters mentioned in the latter we will build a basis of information that we can later use in comparison to the next phase of the study.

Next we will conduct an interview phase where we will collect answers from private and public actors who rely on IoT as a part of their value chains. Here we will talk to actors with different perspectives on the matter such as telecommunication operators, network operators, security firms and manufacturers. This will give us a better understanding of their situation awareness and concerns on cyber security in cellular IoT. Also here we will follow the same template as mentioned with threats first, followed by vulnerabilities and security.

From the above mentioned we will be left with two data sets that will help us contribute to the general understanding of the cyber security in cellular IoT. By comparing the two data sets we should be able to better understand the gaps between theory and empiricism. We believe that by identifying these gaps and presenting them through this thesis we should be able to contribute to further work on improving the cyber security in the cellular IoT domain.

Main **What are the gaps between theoretical and empirical Cyber Security in Cellular IoT?**

1.1 What are the theoretical threats towards cellular IoT?
1.2 What are the theoretical vulnerabilities in cellular IoT?
1.3 What is the theoretical state of the art in cellular IoT security?

2.1 What are private and public actors perceived threats towards cellular IoT?
2.2 What are private and public actors perceived vulnerabilities in cellular IoT?
2.3 What security mechanisms are private and public actors missing in cellular IoT?

1.4 Scope

In this chapter we will discuss the scope of the thesis and what obstacles and restrictions that might affect the final result. We discuss the scope through three main topics. Technology, litterateur study, interview phase.

1.4.1 Technology

The thesis will be limited to look at the cellular carriers mentioned in the lattice; 4G, 5G, LTE-M and NBIoT. Because of this there might be cellular carriers that are more or less secured than the once we are investigating. However, these four

seem to be the most common carriers in today's and the close future's cellular IoT and we therefore assume the results are valid for most cases. In addition to studying the cellular carriers we will also look into security technology and implementations for cellular IoT devices. Here we will exclude material related to conventional IT carried IoT as the cellular domain is the one we want to put our focus into.

1.4.2 Litterateur Study

The thesis will seek to investigate as many sources and as much litterateur as possible given the time frame of the thesis, which is one semester. Limited time means the litterateur is not formal or comprehensive, but we believe we should be able to cover a sufficient amount anyhow. However, niche studies, new studies, and foreign language ones might end up not being noticed as the widely discussed and easily available ones will be discovered first.

1.4.3 Empirical Study

The interview phase of the study will have the same time constrains as the litterateur study will have. Because of this we will prioritized to find as many different sectors to interview as possible instead of multiple within the samey. Therefore, the thesis might not represent a specific sector perfectly as there might be differences between companies within the same sector. The in-group and between-group differences is, due to the limited time, left for future work. However, we still believe our focus will add valuable insight.

1.5 Outline

The thesis is divided into 7 chapters. The first one being the introduction we are currently in. Chapter 2 will provide some initial theory before moving into the research phases. These we will start off with the methodology in chapter 3, followed by the results from the litterateur study in 4 and empiricism in 5. Chapter 6 will discuss the results, compare them and also discuss strengths and weaknesses of the thesis. Last we will conclude the thesis in chapter 7 which will also propose future work.

Chapter 2

Background

We will now present some background theory for the thesis that will help us better understand the definitions, terms and technologies that are relevant within the cellular IoT domain. The information presented in this chapter will set the premise of the thesis and prepare us for the discussions and argumentation's for the following two research phases.

2.1 Definitions

First we will present the three different topics we are going to study in the two research phases; Threats, Vulnerabilities and Security. By defining them prior to the research phases we believe that the results from the two will be more "in tune" with each other and allow for a better discussion and conclusion.

2.1.1 Threat

The therms threats and vulnerabilities are ones that are often misunderstood, therefore it can be difficult to decide where the boarder between the two lies. In this subsection we will look closer at how the term threat is defined in the cyber security context. According to National Institute of Standards and Technology (NIST) the cyber threat is defined as follows;

> *Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service[9].*

We can see that they mention "any circumstance or event with the potential to adversely impact". From this we can read that the term threat involves something that has to do with an action or something being actively executed or happening. Looking towards studies on the matter it has been pointed out that in order to categorize something as a threat there are four criteria that need to be met. The

first one is that it must consist of several elements. These we can see in Figure 2.1. The next one is that the elements involved must relate to each other in certain formal relations. Third, the relations must connect the elements to each other. And last the total relations of all elements is characteristic for the complex in question[10].

Figure 2.1: Elements defining a threat

In order to fill these criteria we are in most cases talking about an actor or actors who has a motivation(intent) and skills(capacity) to exploit a vulnerability(opportunity). These actors can be categorised in several ways, but for this thesis we will use; nation-state, cyber criminals, terrorist groups, hacktivists, script kiddies and thrill seekers. Each of them shown in Figure 2.2 and described more detailed in the following.

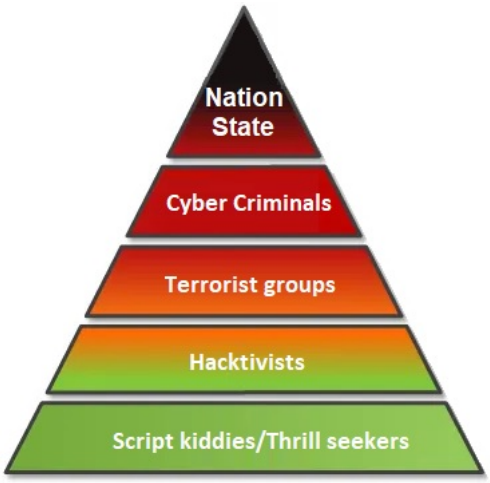


Figure 2.2: Threat Actor Pyramid

Nation-State

Nation-state actors are considered the most advanced threat actors and are often discussed as an Advanced Persistent Threat (APT). They have dedicated personnel and resources, conduct extensive planning and are well coordinated. Nation-state also indicates that they are organised and funded by their government, but can also include or have relations to the private sector. Nonetheless, these are the most sophisticated actors and are placed on the top of the threat actor pyramid[11].

Cyber Criminals

Cyber criminals are the second most sophisticated threat category. They can be moderately sophisticated compared to state-nation and don't receive funding from the government. They are often organised and coordinated similar to a regular professional business and are highly skilled and capable. Along with state-nation actors they also belong to the group that can be categorised as a APT[11].

Terrorist groups

Terrorist groups and the next category(hacktivists) are often considered ideology motivated threat actors. Terrorists are often under pressure from states or other groups that they want to harm or inflict terror on in order to advance in their cause. They are highly motivated, but unlike the APT actors they may lack the coordination and skills that the higher tier threat actors poses[12].

Hacktivists

Hacktivists are groups of people that are ideologically motivated and that seek to use the cyber domain to advance in their cause. However, compared to the terrorists they have very different goals for their work. While terrorists are seeking to inflict harm and terror, hacktivists are often seeking to spread info or stop activities that are contrary to their values. They are often skilled and have some degree of coordination, but they are often not well funded, thus reducing their availability to advanced tools[12].

Script kiddies/Thrill seekers

Script kiddies or thrill seekers are often individuals with limited skills and low availability of tools - thus the name "script" as open source scripts are often their attack possibilities. Higher skilled hackers can also be categorised here, however they do not have the funding, capabilities or coordination to carry out advanced attacks or inflict significant damage. Any modern system with baseline modern security should be able to withstand this threat actor[12].

2.1.2 Vulnerabilities

Vulnerabilities is the next definition we need a deeper understanding of. As mentioned in the threat section they are often mixed and misunderstood as being threats, but there is a clear distinction. While the threat is a a result of several different factors, the vulnerability consists of one thing; an opportunity. In this section we will define what these can be and how they might be perceived. NIST defines it as follows;

> *A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)[13].*

From this we can read that the vulnerability is about something that is present in the system and that does not involve any third party actors. The vulnerability is not dangerous in itself without a threat actor that has an intent and capacity. However, when these criteria are met, the vulnerability could be considered the enabler for an attack.

It is also interesting looking into what an attack is as it is common to discuss them and vulnerabilities as the same thing. E.g when saying a system is vulnerable to Distributed Denial of Service attacks we might as well be speaking about a vulnerability in the system that can be exploited in a certain way[14]. Thus, when reading about a form of cyber attack it might as well be the vulnerability that is being discussed, not the action committed by a threat actor.

2.1.3 Security

Security is last term we need to understand and in the context of this thesis it is not security in the physical domain we are talking about. What we will be discussing is the cyber domain related matter which is often refereed to as cyber security. This term has many definitions, but in this thesis we will stick to Frankenfield's who defines it as follows;

> *Cyber security refers to measures taken to protect Internet-connected devices, networks, and data from unauthorized access and criminal use. Additionally, cyber security ensures the confidentiality, integrity, and availability of data over its entire life cycle.[15].*

In the definition Frankenfield mentions three key areas of cyber security which are devices, networks and the data within them. For this thesis devices would be the cellular IoT devices and the networks would be the TELCO ones. In addition Frankenfield mentions confidentiality, integrity and availability. These are

important factors in cyber security and are often referred to as the CIA-triad. It is considered a benchmark model for governance and evaluation of how storage, transmission and processing of data is handled within a system[16].

- **Confidentiality** - Data should not be accessed or read by unauthorized actors.
- **Integrity** - Data should not be modified or compromised in any way. It assumes that data remains in its original state and that it has not been tampered with between its intended authorized users.
- **Availability** - Data should not be available to unauthorized users, but it should also be available to those who need it and are authorized for it.

With this we have defined our three overall most important terms which will help us with the in depth investigations in the study. Threats, vulnerabilities and security will be used according to how we have defined and described them above. We are now ready to move on with the more technical part of the litterateur study.

2.2 Defining an IoT Device

In this section we will present device specific definitions and information that we will be using when discussing device specific cyber security. This we will do by first looking at what defines an IoT device on a general basis. This will give us a better understanding of what it could be and what characterizes it regardless of what carrier it is using. Next we will define what we regard as a cellular IoT device. This will help us better understand what we consider to be a part of the cellular IoT domain and what is not. In the last sub section we will look closer into the life cycle of the devices as different threats and vulnerabilities are present at different times in their lifespan. This will help us categorise the different findings throughout the following research phases.

2.2.1 Defining an IoT Device

The "Internet of Things" is a term that was first coined by the innovator and sensor expert Kevin Ashton back in 1999[17]. He used it to describe the phenomena of devices connected to the Internet without the intention of being controlled by a human. Since then the devices have developed a lot and the numbers exploding with an estimated number of devices reaching 50 billion in 2020 as opposed to a mere 500 million back then[18]. The description tells us a little bit about the phenomena, but in order to really understand what it is about we need to break it further down.

For this thesis we have chosen to define the general demography of IoT using a pyramid approach shown in Figure 2.3. At the top we find the common name that all devices would fall under in a pragmatic approach under the name IoT. Next we see the two sub categories; Consumer IoT and Industrial IoT[19]. These

describe the two primary user groups of IoT. The third tier of the pyramid tells us the communication pattern of the devices; M2M, P2M and P2P. For this thesis we most likely will not see much of the P2P type of communication as the cellular IoT often is deployed in unmanned environments. At the bottom we see the different carrier possibilities. They are numerous and vary from long to short range as well as being parts of different underlying technologies. 4G, 5G, LTE-M and NBIoT are the ones we will focus on as these are the most common ones in the TELCO networks; where we find what we will define as cellular IoT devices.

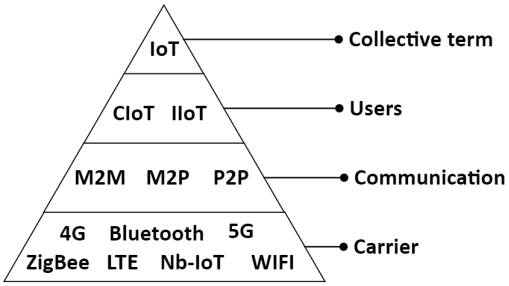


Figure 2.3: IoT Pyramid

This tells us how the IoT domain is logically categorised. Next, it is necessary to understand what the atomic IoT device consist of. Dr. Barrett, a leading scientist in the field, describes the characteristics of an IoT device according to Figure 2.4.

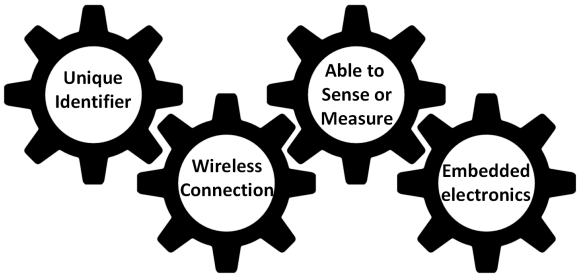


Figure 2.4: The characteristics of a thing

The first thing it needs is an unique identifier. This could for example be a Radio Frequency Identification (RFID) tag in an offline systems, a Media Access Control address (MAC) in an IP network or a phone number in a cellular network[20].
The next one Dr. Barrett mentions is wireless communication as we saw in the bottom layer of Figure 2.3. However, others argue it can also be in the form of a wired connection[21]. This would not be considered to be a cellular carrier and therefore outside the scope of this thesis.
The ability to sense or measure something is the next characteristic he mentions. Arguably this could be considered the essence of what IoT is. To allow a machine to sense or learn something about its environment without the help of human interaction or input[18].

The last characteristic, embedded electronics, is also of significance as it is the one that stand for the challenges connected to the technology. Embedded electronics or an embedded system is as a set of hardware and software designed to carry out predefined tasks[22]. This characteristic is the one that lead to the tight constraint challenges mentioned in chapter 1. The devices are designed to carry out their predefined tasks and have been rigged for just that and often nothing more.

2.2.2 Defining a Cellular IoT Device

Now that we know more about what defines an IoT device we can continue on with the cellular part. From this we should get a better understanding of what makes cellular IoT differ from conventional IP-network carried IoT and where the cellular domain begins.

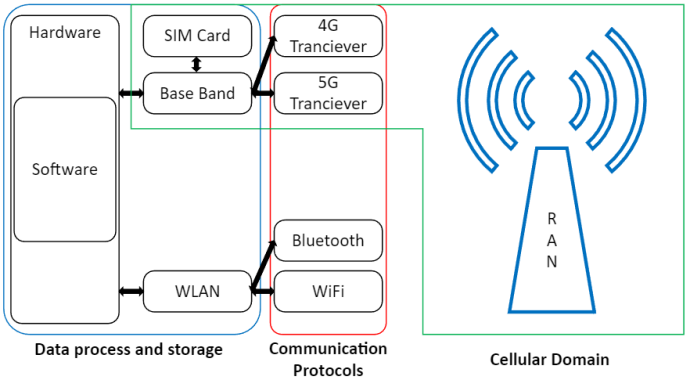


Figure 2.5: Basic Cellular Device Architecture

In Figure 2.5 we can see a block schematic visualisation of the basic building blocks in a cellular device. As we can see in the data processes and storage part of the figure we notice that the Subscriber Identity Module (SIM)-card is directly associated with the base band unit which again is connected to the miscellaneous hardware on the device. In addition it has a connection to the communication protocol section. This is where the different cellular technologies are first seen and is also the interface against the Radio Access Network (RAN). In this section we also find the other carriers on the device. However, these do not rely on SIM-cards and cellular modems such as the cellular carriers do and are not directly connected to the cellular carriers. This is where the difference between cellular and conventional IP based communication really lies. From this we can define the interface against the cellular domain and also pinpoint the initiation point of cellular in the term cellular IoT[23].

2.2.3 IoT Life Cycle

The last IoT device specific background we need to understand is the life cycle. This is necessary as all of the phases are exposed to different kind of threats and vulnerabilities. By knowing the different phases we will be able to categorise our findings in the following research phases and also discuss them more structured.

IETF describe the life cycle of a thing in a Building Automation and Control (BAC) where the devices serve purposes in the Heating, Ventilation, and Air Conditioning (HVAC) of a building. However, the life cycle will likely apply to all kinds of Internet of Things (IoT) as the described cycle is quite general for devices in static environments[24].

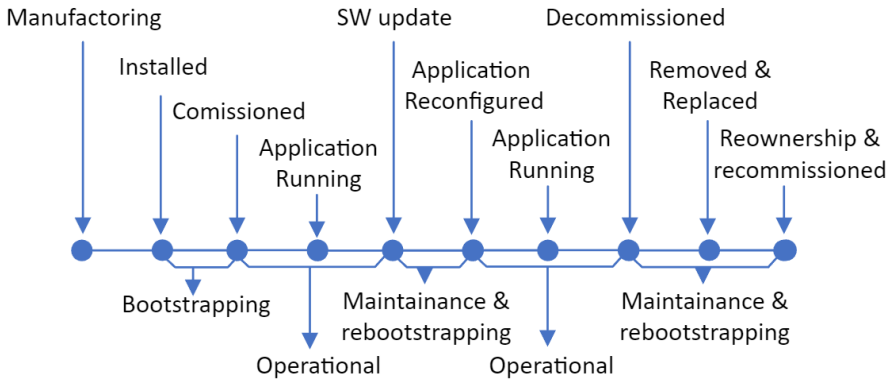


Figure 2.6: IoT Life Cycle

In Figure 2.6 we can see a timeline which has the different steps above the line and the phases below. This figure is presented in [24] which we also mentioned in Chapter 1. It is discussed that the figure might not be perfectly accurate and that it can be discussed what is the first and last step of a devices' life. However, the phases we are the most interested in are manufacturing, bootstrapping, operational and maintainance. The rest of the phases described by IETF after the first maintainance phase are either equal to one of the previous phases or the off boarding. Because of this the threats and vulnerabilities are either equal or not existing if the devices are not in use anymore.

2.3 Cellular Networks

In this section we will take a closer look at the cellular network technologies. First by presenting a simplified network architecture that applies to all of our chosen cellular technologies. Thereafter, we will present some background information on the different carrier technologies before we continue on to the research sections of the thesis.

2.3.1 Basic Network Architecture

Both 4G and 5G share the same basic network architecture. LTE-M and NBIoT typically run as secondary carriers on one of the two Gs and the shared architecture therefore will apply to them as well. With the following architecture combined with the presented device architecture in the previous section we will have defined the cellular IoT domain as a whole also.

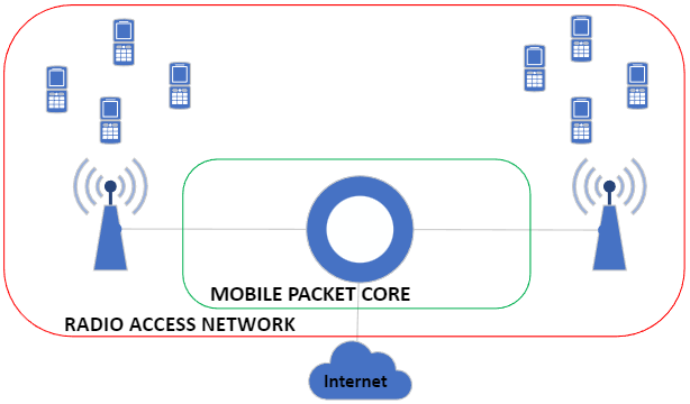


Figure 2.7: Basic Cellular Network Architecture

In Figure 2.7 we can see a graphical presentation of the architecture where we are presented with the main components of a modern cellular network. The first component is the Radio Access Network (RAN) which is the wireless part of the network. This is the interface that the devices need to connect to and which is done through a cellular modem using a SIM-card[25].

The next component in a cellular network is the Mobile Packet Core (MPC) which is a WAN type of network that is used for orchestration and trafficking within the cellular domain. This is what transports the communication feeds between base stations in the RAN and that is the non-wireless part of the cellular networks. With today's standards 4G and 5G the packet core operates more or less similarly to with what we are familiar with from the traditional IP-networks. Another task that the MPC serves is providing the cellular networks with breakouts towards The Internet. This means that in addition to serving as a WAN for the RAN it provides the cellular IoT devices with internet access[25].

2.3.2 Fourth Generations of Wireless Cellular Systems (4G)

4G is the first standard that was all-IP based and is also the oldest of the cellular technologies we are looking into. Its development started in the early 2000's, but the standard was not formally in place until 2008[26]. Later releases of the standard such as 4G-Long Term Evolution (LTE) are also commonly discussed and in later years the standard we often are faced with on a day to day situation[27].

This standard was the first step in the cellular history which really enabled internet connectivity and which served the service that the modern smart phones really needed in order to work to their full potential. With the old 3G technology you could send e-mails or browse light weight web pages, however, with the 4G technology's entrance the possibilities for streaming and real time services made its entry. This was really the essence and goal of the 4G, to enable higher capacity data transmission and to do so for more users and in a more efficient way.

Higher speeds - 4G has a theoretical maximum bandwidth of 100 Mbps which is roughly a 100x improvement compared to it predecessor.

Higher Capacity - With the modern technology's advance since the 3G standard it is now possible to serve up to 400, which is a 4x more than the previous cap pr. base station.

Reduced Latency - The latency of the 4G standard is within the 50 millisecond limit which is required to call something real time. With this there would be no echo if transmitting voice over IP.

Spectrum Efficiency - 4G utilizes the signal spectrum in a much more efficient way than before, thus enabling to send more bits of data pr hertz than previously possible[28].

To summarise 4G is the first standard to support and integrate "The Internet" functionalities into the cellular networks. In addition it does so with a service delivery that is fit for the services that the users want to use. It is no longer a secondary network that is for calling and texting only, its a part of the bigger picture that interconnects all users to the rest of the world.

2.3.3 Fifth Generation of wireless cellular systems (5G)

5G is the second and most recently released standard of the cellular technologies discussed in this thesis. Early deployments began in the late 2010's, but it is not expected to be broadly available until mid 2020's. Equally to 4G, 5G also is an all-IP based standard. However, where 4G used an adapted protocol stack 5G uses the standard stack. The differences are shown in Figure 2.8[29].

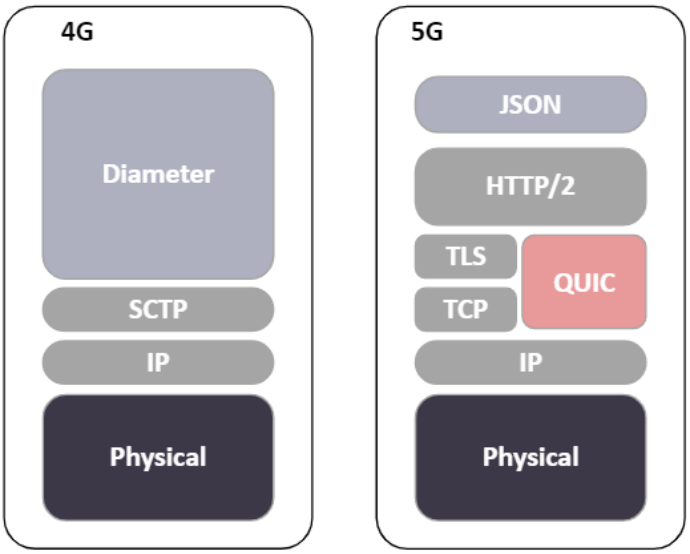


Figure 2.8: Network core signalling and protocols

In addition to the new protocol stack 5G comes with new additional features that allow for higher speeds and better capacity. First, the standard supports what is known as slicing, which in practise allows for a virtual private network within the public infrastructure. This enables tuning of the capacity to the specific users needs. For example higher download rates, lower latency or specific frequencies. Slicing is also possible to combine with private networks, which we mentioned in the security section of 4G. However, in 5G we can carry and extract this private infrastructure both on premise and from a private slice in the commercial network. Second, it uses Orthogonal frequency-division multiplexing (OFDM) which allows us to split different wireless signals into separate channels. This prevents interference as well as it lets us utilize the same frequency for multiple users. In other word it increases the capacity of the network by reusing the same frequencies. Last we have the numbers that we also mentioned for 4G. The capacity, speed and latency related matter has increased greatly with the introduction of this new cellular generation[30].

Higher speeds - 5G supports millimeter wave communication which allows for speeds up to 10 Gbps of download. In addition the regular air interface has improved and speeds up to 1 Gbps is not unheard of in commercial networks.
Higher Capacity - With OFDM and higher cell density in the 5G networks we can expect as much as a 100x increase in connected devices pr base station as compared to 4G.
Reduced Latency - The latency of the 5G standard har been raised to a whole new level with an distributed cellular core. This allows for latency in the single digit of milliseconds which allows for the networks to support critical real time-demanding use cases[31].

With these new features and abilities 5G has become an attractive standard for commercial actors. Big data can be exchanged over the cellular networks with a latency and efficiency never seen before. While 4G was the first enabler for broad access to the internet with speeds and integration's that made it work seamlessly, 5G provides flexibility in architecture and tune-ability towards specific use cases[32].

2.3.4 Low Power Wide Area Network (LPWAN)

LPWAN is the common name of carrier technologies that have been developed with the intent of serving battery constrained, remote devices with low demands for throughput[33]. For this thesis we have chosen to look into Long Term Evolution Machine-Type-Communication (LTE-M), which is a modified version of 4G-LTE, and Narrow Band IoT (NBIoT) which is a separate standard made specifically for IoT devices in cellular networks[34].

Long Term Evolution Machine-Type-Communication (LTE-M)

NBIoT is a modified version of the 4G variety LTE mentioned in the 4G subsection. It uses the standard as a basis on order to reduce costs by making it widely available with the already enrolled equipment in the market. The technology seeks to reduce battery drainage, extend range, and reduce the costs for cellular IoT. The technology allows for a battery lifetime of up to 10 years and a modem cost at 20-25% of the price of current edge modems type modems[35]. In terms of network LTE-M typically is hosted on the underlying 4G network. However, even though it is a descendent of this standard it is mentioned also to be supported in 5G[36].

Narrow Band IoT (NBIoT)

NBIoT is a technology specifically made for cellular IoT. Equally to LTE-M it increases battery lifetime and extends range. However, with NBIoT the gains are a little higher thanks to spectrum efficiency and lower data speeds as we can see in Table 2.1. With this the standard allows for battery lifetime surpassing 10 years[37]. Even though NBIoT was not developed from an already existing standard like LTE-M, it does run on the same infrastructure with the same modems and radio networks. Because of this NBIoT also is secured by the underlying cellular networks security, thus also suffering from the same cyber security challenges[37].

	LTE-M	**NB-IoT**
Downlink Peak Rate	1-4 Mbit/s	26-127 kbit/s
Uplink Peak Rate	1-7 Mbit/s	16.9-159 kbit/s
Latency	10-15 ms	1.6-10 sec
Duplex Mode	Full or Half	Half
Bandwidth	1.4-20 MHz	180 kHz

Table 2.1: LTE-M compared to NB-IoT

To summarize we can say that the LPWAN technologies seem appealing to IoT environments where there are constraints of resources, especially battery power. We can also read that they inherit vulnerabilities and security from their underlying cellular networks.

Chapter 3

Methodology

Next we will present the methodology used in the thesis. As mentioned in Chapter 1 we were seeking to enlighten the gaps between the theoretical and empirical view on the cyber security in cellular IoT. To do this we used two different methodologies during the study. The first one being a litterateur study to map state of the art within the field as well as understanding the domain of interest. Second, an empirical study where we approached different actors in the public and private sectors to get their input from an operational point of view. The data gathered using the two methods we will discuss in Chapter 6 to see whether there actually are any gaps. In the following sections we describe in detail how the methodologies were used and how data was collected for each of the research phases.

3.1 Research Methodology

Even though different methodologies were used in each of the phases we also have an overall approach to research that applies to the thesis as a whole. The deductive research approach is described as the methodology that follows logic the most[38]. By that we understand that the research approach is following the human logical to answer a problem. We use our prior knowledge and experience (theory) to compare what is being studied and try to understand how a phenomenon works or what actors and forces influence the situation before us. Then we create ourselves an assumption (hypothesis) that describes how the phenomenon will react or how the situation will develop. Thereafter, we create some form of test to specifically trigger what we expect to happen, or not. The observed outcome of the testing is used to confirm or reject the hypothesis proving the theory (our knowledge) right or wrong. If the theory is proven wrong new versions of understanding must be put forward and new hypothesis created to allow them to be tested. The visualised steps of the approach can be seen in Figure 3.1.

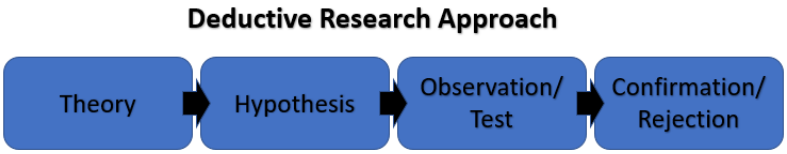


Figure 3.1: The steps of a deductive research approach

In addition it has been described by [39] as a study in which theory is tested by empirical observations. This description describes our study quite well as we were using a litterateur study to establish our theory and hypothesis, before conducting an empirical study based on real life interviews.

Another research methodology that we could have used was the inductive reasoning. This is a methodology which is somehow opposite to the deductive research methodology. Where deductive reasoning starts with theory the inductive reasoning is based on empiricism [40]. For this thesis it would have required us to do our research in revers where we would have started with interviews, before generating theory that could be proposed as knowledge. However, with this thesis we were seeking to find what the theory is missing and because of that the deductive methodology was the one that suited our work the most.

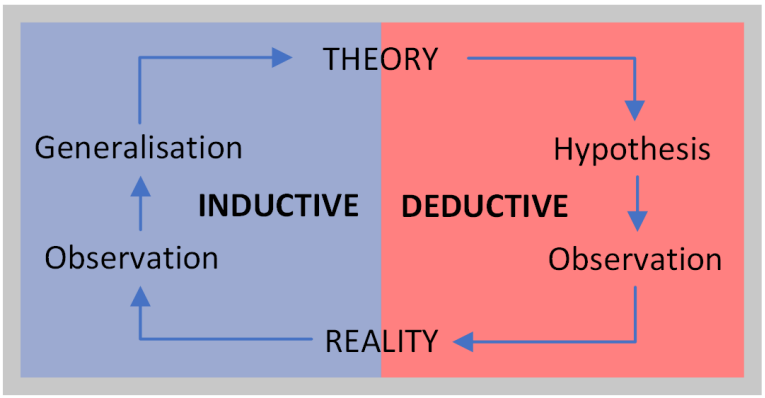


Figure 3.2: Inductive-Deductive loop

However, if we look at it in the bigger picture we might still consider the thesis to be a part of the inductive-deductive loop[41] of the scientific field we are working in as some of the theory in the litterateur study is based on inductive reasoning. We can see how the two methodologies relates to each other in Figure 3.2.

3.2 Litterateur study

Litterateur study is the first step of the deductive approach. In this chapter we will go into detail on how we conducted this phase of the thesis, why we used the

specific methodology and how the information was gathered.

3.2.1 Methodology

This first research phase of the thesis was conducted to answer research questions 1.1, 1.2 and 1.3. These were related to the theoretical threats, vulnerabilities and security measures in cellular IoT and would establish the basis for discussion against the results of the empirical research. This was the first step in answering the main research question regarding the gaps.
There were several different methodologies that could have been used to conduct this part of the thesis. However, as the intention of this research phase was to map a seemingly narrow scientific field we chose to use a methodology known as narrative or traditional litterateur review technique[42]. In contrast to many other litterateur methodologies this is one that uses objective reasoning and that does not seek to change or challenge the material presented. It is simply a methodology that systematically seeks to gather information to give context and substance to the authors overall argument[43].

Some argue that this methodology can become biased by the authors prior beliefs and overall subjectivity[44]. To mitigate the risk of this happening we chose to seek advice from professionals on what litterateur to review. During the writing of this thesis, the author was employed at Telenor Norge AS[1] while studying at NTNU. By seeking advice from the professionals at work the author was helped to stay objective. Also these advice contributed to finding relevant litterateur. We believe this has mitigated the risks of using a narrative methodology as well as it has helped finding appropriate and relevant litterateur for the thesis.

It should also be mentioned that as an additional safe net we also added questions to the empirical study to catch any theory that we might have missed. However, with the limited scope of the thesis it was never the intention to find all relevant theory and all threats, vulnerabilities and security mechanisms. But we do see it as a strength that we asked to be informed if there were any obvious voids that the litterateur study did not cover.

Last we had scoped the thesis to only look into cellular IoT, thus excluding conventional IoT related litterateur. This was done to find the niche litterateur for the specific cellular IoT domain. However, this has likely resulted in the thesis missing out on relevant theory from the more broadly discussed conventional IoT.

3.2.2 Data Collection

Next we will describe the methods used for collecting the data in this phase. The goal of doing this is to provide the readers with an insight into how the results

[1] `https://www.telenor.no/`

can be reproduced. The main strategy when searching for relevant litterateur was to use open source available content that was written in either English or Scandinavian language. Arguably this could be a huge limitation as the same topics most likely have been discussed in other languages as well. However, due to the language barriers we were not able to review them. Next, as mentioned earlier, we were able to request information on where to find relevant litterateur from professionals working in the telecommunication sector. The provided litterateur was in most cases also available through open sources. However, we had not managed to find it through our own searches. This raises a the concern that more relevant theory has gone unnoticed even in our speaking languages. However, we still believe that the litterateur study has captured enough relevant theory to enable us to contribute to a better understanding of cyber security in cellular IoT and answer our research questions.

Practically the collection of data was conducted through open source searches using, preferably, Google Scholar[2], but also NTNU open [3], and default Google[4] search engine. It is also worth mentioning that when scientific papers were not found directly in some cases we were able to reverse-track relevant litterateur by examining the sources in articles and other kinds of publications. However, in some cases we chose to use material that was not of high scientific quality. This might have had a negative effect on the reliability and validity of the research results, but with the focus of primarily using scientific publications we believe our results are relevant anyhow.

3.3 Empirical Study

The empirical study was our second step in the deductive approach. In this chapter we go into the details on the empirical methodology and why it suits the second research phase of this thesis along with how the data was collected. We describe this process as clearly as possible in the Data Collection section in order to ensure the repeatability of the study.

3.3.1 Methodology

In this part of the study we try to answer research questions 2.1, 2.2 and 2.3, which again could be used to answer the main research question of the thesis when comparing the theory with the empiricism. In contrast to the theory study this part of the study seeks to observe the real world. There are many ways this can be done, but there are two main methodologies that are typically recognized within the empirical research methodology; qualitative and quantitative[45]. With our research questions being non numerical and with the intent of gaining an understanding

[2] https://scholar.google.com/
[3] https://ntnuopen.ntnu.no/
[4] https://www.google.com/

on what the gaps in the field are we found the qualitative methodology to be the best suited one. We also wanted the research to be as objective and as little biased as possible and therefore went with a semi-structured interview form. This allowed the interview subjects to talk past our questions in addition to allowing ourselves to follow up on interesting topics with follow up questions. This will to some degree reduce the repeatability of our interviews, but by using our questions listed in Appendix B later interviews probably will lead to the same discussions as we found ourselves during this thesis interviews[46]. A big part of this phase of the research was the data collection which we will describe next.

3.3.2 Data Collection

As mentioned above this research phase used semi-structured qualitative methodology. This meant we had to do interviews with relevant actors that could tell us about the domain from a practical point of view. Through 7 one-to-one interviews and 1 one-to-two with professionals that works with IoT in public and private businesses, primarily in Scandinavia, we were able to collect the data the empirical research has accumulated.

Practically all the interview subjects were found through the authors work-related network or through the social media platform LinkedIn[5]. We first reached out to them with a short request asking them whether or not they would be interrested in taking take part in the study. 3 out of 4 times this would result in rejection, but when someone agreed to an interview they were sent the information letter in Appendix A and we made an appointment for a 60 minutes interview. We also sent the interview questions from Appendix B in advance of the appointment. This gave us the opportunity to remind them of the appointment and to prepare them on what topics they could expect us to be talking about.

The questions asked during the interview were categorised into four main topics that were closely related to the research questions. However, in addition to covering these categories we also had a category with general questions. These we used to understand how they as interview subjects understood the cellular IoT domain as well as figuring out how their company or establishment used the technology in their daily work. The general questions was the first category discussed during the interviews. Next we addressed the questions related to the threats where we wanted to know who they considered the greatest threat actors to be, what their motivations might be and overall how big of a threat they are considered to be in the bigger picture. The third category covered vulnerabilities which allowed the subjects to mention any vulnerability they felt relevant to the cellular IoT domain. Last topic was the security questions which had two purposes. First to enlighten us on whether there was any theory we had missed and secondly what security mechanisms they felt were missing in cellular IoT.

[5] `https://www.linkedin.com/`

During the actual interviews we tried to follow the questions chronologically, but in some cases the discussions got energetic and some of the information was hard to place in the right places when writing down the answers. However, by having the questions printed out and by trying to get back on track the data was collected quite structured into the respective topics and questions we were discussing.

As mentioned our interview subjects were selected among public and private actors, but we also tried to cover network specialized, device specialized, and also culture and human factor specialized subjects. Some of them did not want their personal details published and we therefore had to anonymize them to a certain degree. However, we were allowed to use some meta data in order to give the reader an understanding of what kind of company and person that was answering the questions during the different interviews. These details are listed in Table 3.1

Number	**Company**	**Department**
1	Telenor Sweden	Connexion(IoT)
2	Cisco Nordic	Sales
3	Thales Norway	Encryption
4	Telenor Norway	Business
5	Emcom Norway	Chief Technical Officer
6	Microsoft USA	Cellular/Cloud IoT
7	Norwegian Defence Research Establishment	Strategic Analysis
8	Norwegian National Security Authority	Security Culture

Table 3.1: Interview Subjects

Next, it is important to understand why the interview phase was ended after 8 interviews. It was discussed by [47] that a qualitative research becomes valid once the answers from the subjects go in to saturation. By this they describe that the answers from the subjects start to repeat and that further interviews would led to redundancy. For this research we started to see this kind of saturation at a stage where many of the subjects mentioned the same topics for certain questions. However, we continued on with the interview at least until we felt comfortable that we had covered all the perspectives mentioned in the previous section. In addition the time frame was a limiting factor that prevented us from reaching saturation on all of our questions. However, with the 8 interviews we felt comfortable the content from the results would contribute to answering the research questions.

After the interviews were done we collected the answers in a digital medium for the rest of the writing process. This was needed in order to facilitate that all the

answers could be reviewed in parallel while writing the results and discussion parts of the thesis. However, once the thesis was complete that medium was wiped entirely to ensure no information from the interviews could be traced back to the actual persons representing their businesses. That action assures that the only information related to the actual interviews is to be found in this very document and nowhere else.

Chapter 4

Results - Litterateur Study

In this chapter we will present the results of the litterateur study described in the methodology chapter. The goal of this research phase was to answer research questions 1.1, 1.2 and 1.3 and to establish the theoretical basis for later answering the main research question. First, we will present the theoretical threats in the cellular domain as a whole. Second, the vulnerabilities which in difference to the threats will be presented in separate categories; device and network specific. Lastly we will present the security mechanisms. This will also be done using the same categories as for the vulnerabilities.

4.1 Threats

The litterateur study presented a threat picture much like the one we saw in the background. However, in difference to the background, which presented five different groups, the litterateur used three categories. The first was high tier actors which would include state-nation from the background, but also state funded criminals. Next was mid tier actors with terrorists, hacktivists and non state funded cyber criminals. And last was low tier actors with hackers and thrill seekers. For the rest of the tests we will continue using these three categories.

High Tier Threats

[48] describes the high tier threat actors as those who possess the biggest threat in the IoT domain. It is claimed that the actors would have great access to resources both in terms of people and skills, but also in terms of sophisticated tools and platforms. Further, it is claimed that in order to stay protected from such actors one would need to implement tight surveillance and monitoring in order to detect their presence in the networks. In terms of motivation it is mentioned that the these actors primarily are interested in acquiring information about foreign nations through methods such as espionage. [49] also argue that in addition to these attacks the high tier actors could be motivated to conduct attacks that would

result in physical damage as well. An example is the attack on Iran's nuclear program that was targeted and sabotaged - most likely by a foreign nation in the form of an APT.

Mid Tier Threats

Mid tier threat actors are described as financially stable and possessing a skill set that enables them to target all users of the IoT domain. It is described that in addition to having motivation towards information gathering, like the high tier threat actors, they are also motivated by economical and disturbance objectives. However, in difference to high tier actors they might have other motives for collecting the data as well. While high tier actors want to collect information for use in political situations, mid tier actors often are motivated by the economical aspects of selling it. This again underlines their economic motivation. In terms of disturbance it could be in the form of denial of service or even trying to sabotage infrastructure. By conducting such attacks they might wish to promote their idealistic greater cause[48]. [49] agrees on the motivations in the latter, but argues that the sabotage attacks are not as frequent as with the high tier threat actors.

Low Tier Threats

Low tier threat actors are described by [48] as actors that do not have any specific skills or economic funds to conduct their attacks. They are relying on open source tools and guidance in addition to using human engineering to figure ways to attack their targets. These actors are further described as not having any large impact with their attacks and thus neglected to a certain degree compared to the higher tier actors. The low tier threat actors are furthermore described as being motivated by economic gains, personal gains as well as revenge.

Summarised for the three different categories of threat actors both [48] and [49] agree on the motivations and severeness that each of the groups possesses in the IoT domain. They state that the high tier possess the most skills, resources and therefore also constitute the biggest threat. In the same way the mid tier threats are less skilled and less dangerous and the low tier are equally the smallest threat. However, they do also state that each of the actors have different motivations and therefore may present themselves differently in the IoT domain.

4.2 Vulnerabilities

Next, we will present the results regarding the theoretical vulnerabilities in the cellular IoT domain. First, the ones related to the devices, which will categorise into the different life cycles mentioned in the background. And next the ones related to the cellular networks which are categorised by the cellular technology they are present in.

4.2.1 Cellular IoT Vulnerabilities

For the device specific vulnerabilities it was observed that vulnerabilities and attacks were discussed in the same context. As mentioned in the definitions these two are often mixed and misunderstood, but in order for an attack to be carried out there needs to be an underlying vulnerability that can be exploited. In other words, the attacks presented in the following will represent a vulnerability even though they are presented as an attack. However, as the litterateur presented them this way we will do it as well, but also try to understand which vulnerability they represent.

Manufacturing

For the manufacturing the litterateur only presented one vulnerability, which was discussed as software vulnerability. This vulnerability is one that could occur because of bugs and flaws in the software of an IoT device. This can lead to an attacker compromising the device and gaining control over it.

Another vulnerability related to software is poor, but deliberate implementations. This could be weak authentication mechanisms or easy to guess credentials. This was discussed to be one of the most common vulnerabilities in IoT and which is often targeted in opportunistic attacks. In [24] it is discussed that manufacturers are prioritising cheap and quick to deploy implementations rather than secure ones, which might add costs.

Bootstrapping

The bootstrapping phase of the IoT life cycle was not directly addressed. However, the software related vulnerability mentioning credentials might as well belong to this phase where the devices have not had their password changed before being deployed. Whether [24] had this in mind or not when describing the vulnerability is uncertain, but arguably the action of leaving default passwords in place could constitute what they describe as a software vulnerability.

Operational

The operational phase was the one that was discussed the most in the litterateur. Here we will present both what was described as attacks and also vulnerabilities. Because of this there might be overlapping vulnerabilities in some of the sections, but we will present them as they were discussed in the litterateur anyhow.

Device attacks are attacks where the device itself is exposed to some kind of threat that end up with it being compromised. By doing this the malicious actor would be able to control the device which again could lead to several different outcomes. One that is especially common in IoT is recruitment to bot nets in order to conduct distributed denial of service attacks. Typical vulnerabilities that could lead to

this is IP misconfiguration, memory corruption, and code that has been wrongly executed in either the operating system or middle ware of the device[50]. The fact that devices are often left physically unprotected could also be considered a vulnerability. Without physical control an attacker might gain access to the device without being obstructed[24].

Application service attack is a type of attack that targets to compromise applications running on the IoT devices or the back end systems. These applications are often hosted or provided by third party operators who does not have the same insight in the devices as operators do. This could be argued to be a vulnerability in itself, but [50] has not mentioned it directly. However, when discussing vulnerabilities they mention different kinds of attacks such as SQL injections, code execution or Denial of Service (DoS)[50]. It could be argued that the vulnerability they are really pointing towards is the one related to the IoT devices dependence on applications and back end systems.

Legacy vulnerability is one that is a result of backwards compatibility. By enabling old carrier technologies to run on the devices we also expose them to threats that are related to these. However, when designing a device that you want to be relevant and compatible with future carrier technologies you also leave them exposed to toady's threats and vulnerabilities "tomorrow". The vulnerability also rises when the device developers want to support areas of use where the newest carriers are not implemented. This exposes the device to vulnerabilities that have already been patched even though we are running on new safer carriers - the "backdoor" is still present[51].

Web interface attacks seek to gain access to the web interface of the IoT devices in order to control them. It is usually done through stealing the credentials or by brutefully guessing or cracking them. Devices could be targeted for these kinds of attacks due to poor account policies where default passwords would be easy to guess. However, it could also occur as a result of cross site scripting, SQL injections, Cross-site reference forgery or IP misconfiguration[50].

A data integrity attack is an attack that attempts to compromise data by inserting, altering or completely deleting data in order to compromise the devices ability to solve its tasks. The result of such attacks can be that the devices are manipulated to give false information or operate wrongly as a result of its data being altered. This could also have an effect the opposite way with outgoing data being altered which would result in the receiver of the data being deceived[50].

During certain phases of the devices communication cycles, such as initial key exchange, they might be vulnerable to third party malicious actors and MitM attacks. By collecting unprotected data an attacker might gain access through parameters shared by the device itself. This might occur in an environment where

pre-configuration is not possible or considered necessary and where an attacker is in position to eavesdrop this vulnerable stage of communication[24]. The vulnerability that seem to be discussed in these kind of attacks might seem to be related to data being unprotected in transition between the device and receiver. Exactly what kind of protection is uncertain, but lack of or poor encryption might be a possible answer.

Maintenance

During the devices maintenance phase they are mentioned to be vulnerable to firmware attacks. It is discussed that patching or firmware updates might be possible attack vectors. Malicious actors could disrupt or falsely provide firmware updates which have been modified to install back doors or malicious pieces of code on the device. By doing so the device will be tricked into implementing features that benefit the attacker when it in reality though it was a new patch or firmware update available[24]. From this we can read that the devices are vulnerable during their maintenance phase, however not exactly why.

4.2.2 Cellular Network Vulnerabilities

Next we will present the network specific vulnerabilities for each of the technologies we have chosen to study in the thesis. We will start with the oldest technology 4G followed by 5G. As these are the underlying technologies for the two LPWAN technologies LTE-M and NBIoT the vulnerabilities will also apply to them, but vary according to which one they are hosted on. We will therefore not discuss the vulnerabilities of the LPWAN technologies further but assume that they inherit their host technologies vulnerabilities.

Vulnerabilities 4G

4G was designed to address a number of vulnerabilities from the old standards such as, weak encryption and lack of authentication between base stations and devices. This could lead to a number of different attacks. One of the most common were IMSI catching which involves fake base stations that would allow malicious actors to interfere with the cellular networks and its users. Some of the vulnerabilities have been mitigated in the new standard, however not all. In this chapter we will shed light on some of them based on scientific work on the 4G-standard.
Authentication and Key Agreement (AKA) is a protocol which aims to strengthen authentication and encryption in the cellular networks. This is meant to prevent eavesdropping and IMSI-catching, which again can lead to multiple sorts of attacks. However, the protocol is vulnerable in its initiation phase where messages need to be exchanged uncrypted. This means that the protocol is not as secure as it could be, thus allowing for a threat actor to attack the initiation [52].
Non-Access Stratum (NAS) is a request that the devices will send to the RAN in order to initiate a session. This request is always sent in plain text from the devices

which makes it vulnerable towards injections and hijacking. It can also be used as a first step in an attack where further vulnerabilities can be exploited from[53].
Tracking Area Update (TAU) is a request sent when roaming between different base stations. It is vulnerable towards MitM attacks where a Rouge LTE Network (RLN) can be used to hijack the device in the transition. By catching uncrypted broadcast messages, such as NAS, related to the movement the attacker can put the end user into a denial of service state. This is done through tricking the device into thinking it is about to receive service even though the RLN is done with its attack[54].
Globally Unique Temporary Identifier (GUTI) is an identifier used with the intent to hide the IMSI of devices in the network. The intention is to use the IMSI as little as possible and to protect the device from identification by third part actors. However, the GUTI is vulnerable to triangulation as the identifier is not reassigned once issued. As a result of this an attacker with fake base stations is able to locate where the device is based on the movement of the specific GUTI[55].
MIB and SIB are equals to the above protocols broadcast messages which are vulnerable to signal injection. However, in difference to the others this attack can be conducted over simple software defined radios and not using fake base stations as many of the above needs. The vulnerability related to the protocol is that the broadcast messages go uncrypted, thus making them available to anyone who can read the signals. By doing so a malicious actor can conduct a "signal over"-attack which sends a more powerful signal than other units in the cellular network. Which again lets a malicious actor deny the devices of service[56].

Vulnerabilities 5G

5G is architecturally more secure than it predecessor with new virtual private networking functionalities and all around more flexible in terms of design. However, there are still flaws and vulnerabilities in the standard. Actually many of the vulnerabilities discussed in the 4G chapter are still present. We will not go into detail on these again, but the same vulnerabilities related the initiation with NAS and AKA are still left in the new generation. Also the SIB, MIB and TAU broadcasting messages are passed uncrypted, thus making the standard vulnerable to the same kind of attacks as we saw in the 4G chapter[57]. The only vulnerability that was discussed in the 4G vulnerabilities that has been resolved is the one related to GUTI.

A new vulnerability, or rather set of vulnerabilities, that has been introduced with the 5G standard is that the all-IP concept has been taken a step further. Where 4G used cellular adapted IP-protocols such as Stream Control Transmission Protocol (SCTP)[58], 5G has taken the step to implement the regular set of protocols related to the internet. With this comes a whole new world of vulnerabilities that threat actors already are familiar with and know how to attack. Because of this the cellular networks using 5G has become vulnerable to attacks previously only

seen in the conventional IP-networks[29].

4.3 Security

Last we will present the results regarding the theoretical security in the cellular IoT domain. Equally to the vulnerabilities we will use the two categories device and network when presenting the results. Additionally the network will be divided into the different network technologies presented in the background. The results in the following will answer research question 1.3.

4.3.1 Cellular IoT Security

For the device specific security mechanisms related to cellular IoT we were only able to identify a single technology. This could be a result of our chosen scope that was focused on the cellular domain, thus excluding conventional IoT security that could have been relevant. Whether this is the case or not is left for future work.

IoT SIM Applet For Secure End-to-End Communication (IoTSAFE)

IoTSAFE is a security mechanism that enables secure end-to-end encryption[59]. This is typically a mechanism that ensures the confidentiality of the communication. This means that the information is useless for anyone between the encryption and decryption point as it would not be readable without the appropriate keys. In a cellular point of view this would not make the information secured against jamming or other kind of signaling attacks[60]. However, it would ensure that if anyone intercepts the packets in a MitM scenario they would not be able to do anything useful with the information they have captured.

The mechanism is provided through an applet which in placed on a Subscriber Identity Module (SIM) or Embedded SIM (eSIM). This is done to keep the TLS or DTLS keys apart from the devices OS and applications. By doing so the technology is utilizing the already secure and well developed SIM as a vault for keys, encryption and the management of them. On the other end of the communication chain we find the IoTSAFE back end systems. This would consist of a Certificate Authority (CA), which would distribute encryption keys and a IoT application server which would receive keys equally to the SIM before serving the applications it is hosting. This kind of technology already exists today. However, in resource constrained environments, such as IoT devices, there is often a lack of security in other parts of the software that might expose the regular TLS stack to vulnerabilities and attacks. By using the all ready secure SIM for this purpose we end up with two beneficial effects. The first one is that the developers of IoT software can be pragmatic to the security in their applications as the underlay will handle the end to end security. And the second one, the key managements and encryption will become more secure by being managed inside the SIM[59].

4.3.2 Cellular Network Security

Next we will present the findings in the network specific security. In difference to the device specific ones we were able to find relevant litterateur that discussed this area more thoroughly. An explanation to this could be the many other use cases except from IoT that has been present in the TELCO networks, thus enabling for broader discussions outside of the seemingly narrow field of cellular IoT.

Fourth Generations of Wireless Cellular Systems (4G)

In 4G there are both implemented security in the standard and in possible modifications to gain another dimension through different protocols and architectural tweaks. We will now present the findings from the litterateur study related to these.

Architecture - The 4G architecture is based on a lower degree of trust than earlier generations. Mechanisms such as separate management and user plane, or authentication when roaming between service providers are examples of this. By having separate channels for different purposes and having multiple authentication nodes in the networks we achieve a higher degree of control and security with 4G than with the previous cellular technologies[61].

Protocol - As mentioned in the vulnerability chapter there are vulnerabilities related to many of the new protocols introduced in the 4G networks. However, the idea and fact that the mechanisms such as GUTI and AKA are present in the networks are in most cases increasing the security within the networks. These mechanisms ensure anonymity, integrity and confidentiality and even though they have vulnerabilities they are nonetheless raising the overall security in the networks[61].

Private Access Point Name (APN) - Is a access point between a device and the internet or a corporate network. Unlike a public APN the user of the private APN can to a much greater extent control what is allowed or not in its cellular network. An approach much like what we might be familiar with in regular IP-networks firewalls with additional features that allow for full control of the devices connected to it. By using this technology the owner of the devices in the network can create a safe environment based on tuned rules and white/blacklisting as well as he/she can control parameters such as IP-addresses of the devices. This allows both for a secure infrastructure as well as a better insight and management opportunity in a fixed environment such as in a IoT context[62].

Private 4G - This is a solution where the security is introduced by making a private offline network which is not available to anyone else but those the owner allows. This solution would be very expensive and demanding to run as it typically would not be run by a TELCO. It would also be exposed to the same vulnerabilities that

exists in public networks. However, by having the network in house and offline you can be sure that remote attackers are not able to reach the infrastructure unless you have made an opening for it yourself. In short the increased security is in the form of reduced availability for the threat actors in addition to full availability to all resources to the benign users[63].

Fifth Generations of wireless cellular systems (5G)

5G is a standard that has been developed in a time where cyber security has become more important to businesses. With this increased focus on information security we have seen the 5G standard being designed to be so called - Secure by Design[64]. In addition to the features and solutions seen in 4G the standard has an even tighter trust model with a new mutual authentication mechanism, enhanced subscriber identity protection, and virtual private networks through "slicing".

Mutual Authentication - In the 4G chapter we mentioned the AKA protocol which is used for authentication and key agreement. For the 5G standard it has been renewed and now supports mutual authentication. This means that not only does the user get authenticated for the network, but the user also authenticates the network. The protocol is now called 5G-AKA and is part of the tightened trust mentioned above. With this the availability is strengthen by making it harder for fake base stations to take subscribers from the benign networks[65].

Enhanced subscriber identity protection - In 4G we discussed the GUTI. In 5G this implementation has been enhanced with what is known as Subscription Permanent Identifier (SUPI) and SUCI. By sending a SUCI to the network a user ensures the confidentiality of its IMSI even in the initial phase of the communication. The network will be able to decipher the SUCI and authenticate with the SUCI, before sending back a GUTI. This means that the identity of the users in5G is even safer now then it was with its predecessor[66].

Virtual Private Networks - 5G supports virtual networking, which will allow an operator to distribute its packet core. This allows for a distributed network which has many benefits in addition to making it more scaleable when needed. Another feature known as slicing also adds significant security gains. In 4G we had the possibility to add private APNs to seemingly get a private network. In 5G this can be established completely within the network, creating a virtual private network with all the specifications of the network tailor made for the user. This could include interaction with the outside of the slice, additional security, quality of service and much more. In other words, 5G's virtual networking and slicing allows for integrated solutions where as previous generations has made adaptions, thus increasing the security and security potential vastly[64].

Chapter 5

Results - Empirical Study

In this chapter we will present the results from the empirical research phase. The following should be read as a re-caption of the interviews which we will present one by one. For each of the interview we will the results following the four categories of questions used in Appendix B. General, which tells us about the company the subjects are representing as well as how they position towards IoT. Vulnerabilities, which we will answer reseach question 2.1. Threats, that will answer research question 2.2. And last, security which will answer research question 2.3. This gives us a brief presentation on the subjects' views on cyber secuirty in the cellular IoT domain before we continue on to the discussion part of the thesis.

5.1 Telenor Sweden - Connexion

General

Telenor Connexion is company related to the telecommunication operator Telenor Group and specializes in IoT solutions for large global customers with specialized solutions. They are not a big user of IoT themselves, however they deliver connectivity service to millions and over all possible cellular carriers. [1]

Threat

Subject 1 points out APTs as the most relevant threat actor in the cellular IoT domain. This is claimed as the value and potential gained through a single device, which potentially would be the scope of lower tier threat actors, is not that big. However, for a state actor or funded organisation with skilled individuals the potential attack surface of a big distributed IoT network on a potent cellular infrastructure could create huge societal impacts. The subject further claims that the motivation of the lower tier actors would not be present as their lower skills would not enable them to conduct larger distributed attacks which would be needed to earn them the money they often seek. However, it was discussed that once they

[1] https://iot.telenor.com/company/telenor-connexion/

would figure a way to gain financial growth from attacking it would become a threat.

Vulnerabilities

When talking about vulnerabilities the subject points out that the choice of not using the security functionalities and possibilities that already are present is a vulnerability in itself. By prioritising commercial needs over security the manufacturers expose the devices to threats that could easily have been avoided. A very interesting example mentioned during the interview was one related to the subject's dog and a GPS collar. The collar was connected to the cellular network using a regular SIM card and was supposed to help the owners track their dogs if they got lost. However, 1 tried calling the collar and the call was answered by default. Further, the collar carried on playing sound that was captured by a microphone inside the collar. Certainly a feature that is not useful for the owner, but it was argued whether it was a result of poor hardening or an intentional hidden feature. Next, it was pointed out that the cellular technologies enables a geographical spread that is not possible with any other networks. This creates a vulnerability in terms of availability where attackers are able to tamper with the devices without being detected by its owner. The subject also points out that the long downtime certain devices are operating under also reduces the ability to detect such attacks. Lastly it is pointed out that cellular devices are vulnerable to signaling attacks where rouge base stations and jamming can lead to battery drainage and denial of service.

Security

Subject 1 discuss that security in their cellular IoT is largely dependant on the protection mechanisms implemented in the cellular carriers through solutions such as private APN's, data restriction to the necessary bandwidth, and firewall-like policing with restricting traffic on a need to access basis. Further, 1 discuss that security should be considered on two separate planes in the cellular IoT. First in the cellular networks, where it was claims the traditional telecommunication networks are not ready for the M2M kind of technology. Where humans traditionally interacted with the networks and detecting abnormalities on they way, IoT lacks these mechanisms. In other words the need for monitoring and control has risen within the cellular networks with the use of IoT on cellular carriers. The second topic discussed by 1 was the device specific security. Cheap chip sets are often installed without hardening, thus creating back doors and functionalities that are not supposed to be on the specific devices. Again the subject exemplifies the GPS dog collar which is cellular connected and that has a microphone and default answering configuration. This is functionalities that should have been disabled in the collar, but had been left intact. In other words the manufacturing process should include security hardening to exclude excess functionalities.

5.2 Cisco Nordic - Sales

General

Cisco is a leading technology within multi-protocol routing and has also moved on to other segments since its funding in 1984. The company does not use cellular IoT broadly, but are big users of IT-carried IoT with devices numbering the millions.[2]

Threat

Subject 2 points out hacktivists as the biggest threat actors in the cellular IoT domain. This is claimed as the security level that is common in today's IoT are attractive targets for thrill seekers with resources such as campus server parks. This would put the actors into the category hacktivists or even in some cases hackers. APTs were also discussed and it was acknowledged that the potential of cellular IoT is great with the size of the cellular IoT. However, the subject did not see this as the biggest threat as these actors probably would target more critical infrastructure over cellular IoT and that the probability of these actors attacking was lower than for the other actors. To wrap up for the threats it was pointed out that the size of cellular IoT in the millions without a doubt is a threat and that anyone who could utilize it would gain an effective cyber weapon.

Vulnerabilities

When discussing vulnerabilities 5G came up as an interesting topic. It was pointed out that the possibility of distributed core, possibly in a public cloud, would make it vulnerable toward threats that were not present in the TELCO's on premise core networks. In addition the use of conventional internet protocols open the cellular networks to threats that have decades of experience in the very domain in which TELCOs are now fresh. It was also discussed that the implementation of the same domains security technology also might be a strength, but that it would need maturing. In the same discussion the security feature of having separate protocols in earlier generations of cellular technology could be a strength as attackers would be unfamiliar with the protocol stack they run on, thus reducing their ability to conduct attacks. Subject 2 also mentioned the vulnerability of insecure distribution chains and the possibility for malicious actors to implement hidden back doors to access the devices. The lack of hardening and control in distribution and production possibly make such vulnerabilities go unnoticed.

Security

Subject 2 points out the use of embedded SIM as a security feature they are using in their products. By having it embedded they are assured that unauthorized actors are not able to extract the unit for other purposes but what it was intended for.

[2] `https://www.cisco.com/`

In addition the programmability of the eSIM was pointed out as a strength as it allows for ease of use in multi-operator environments. On the improvement and lack of functionality question it was pointed out that the insight in traffic is a problem. The subject claims that functionality for traffic analysis is not present and this reduces the IoT users and providers ability to control their devices. It was also pointed out that the communication patterns of an IoT device often are scheduled, thus making it easy to detect in the signaling domain. It is therefore pointed out that functionality for pseudo random communication could be useful in certain situations where devices are prone to targeting.

5.3 Thales Norway - Security

General

Thales Norway is a leading actor within the crypto- and high-grade communication segment and delivers solutions and advisory services to the Norwegian government and NATO. Opposed to the previous subjects Thales are more device specific and has their focus on confidentiality rather than trusting or tweaking the carrier technologies. They do not have very much IoT in the Norwegian department, but for their mother company its in the millions. This means that IoT is not a critical part of the Norwegian portfolio, but the company as a whole has a strong position in the cellular segment.[3]

Threat

When talking about threats subject 3 mentioned the whole stack of threat actors as potential attackers against cellular IoT. For APT the believed motivation could be to impact infrastructure in the society and use it as a cyber weapon inflicting harm in the real world. For hacktivists and terrorist groups it could be used for financial gains as well as the same reasons an APT with inflicting real world harm. More specific in terms of financial gains was the threat of ransomware and the fact that actors might seek to hide themselves behind benign devices in order to distribute malware. The lower tiers of threat actors such as hackers and script kiddies were mentioned with the most likely motivation being financial gains. However, a very interesting note on script kiddies or rather consumers is the motivation to tamper with externals ability to monitor them using cellular IoT. An example was that truck drivers might want to trick their driving monitor to allow them to speed or drive past their restricted hours.

Vulnerabilities

Subject 3 discuss three main concerns in cellular IoT domain. The first one was related to the vulnerability the cellular networks expose by enabling geograph-

[3] https://www.thalesgroup.com/nb/countries/europe/norway

ical widespread which again reduces the owners ability to gain physical control of the devices. This would let a malicious actor to tamper with the devices without being detected by the owner. The second one was related to the massive number of devices with the same configurations. By cracking one device you would easily be able to crack another similar device later. 3 discussed that this also could be seen in combination with the vulnerability of insufficient hardening processes in the bootstrapping where parameters could be kept to the default, but non the less the vulnerability related to the massive distribution was a concern. Third the vulnerability of data being tampered with was discussed. By changing the parameters the devices sends back to their centralised systems an attacker would be able to create false feed back from the cellular IoT sensors. It was discussed that this enables a threat actor to trick a benign user into committing unintended or even destructing actions on the false data they received. In short a vulnerability towards data integrity.

Security

Subject 3 sees the use of cellular carriers over others as a security related feature in itself. It is pointed out that the TELCOs often are part of a country's critical infrastructure and that this forces them to protect it abidingly. However, it is further made a note that confidentiality is a great hardening measure to improve the security even more. A project that the company is running related to this is the use of IoTSAFE where they are trying to see what the uses cases for the technology could be outside the scope that it already covers. Further we discussed what is missing in today's cellular IoT security. The one thing that 3 was concerned about was the ability to ensure the integrity of data and the ability to detect whether some data has been tampered with or not. In some protocols this kind of security is implemented, but if someone heated a censor with a lighter it would not be automatically detected. It was also pointed out that the physical security was a problem with the geographical spread cellular carriers allow for and the ability to detect a physical breach in a device. In other words, the ability to monitor and raise alarms. Lastly we discussed the importance of being able to identify an individual, however it was acknowledged that this was taken care of in cellularIoT already in the form of a SIM and that it was rather a problem in "conventional IoT"

5.4 Telenor Norway - Business

General

Telenor Norway Business is the part of Telenor Norway that is dealing with the business segment within the country. They deliver services spanning telecommunication, infrastructure and security and are a growing business area for the company. In this interview we spoke with two representatives from the company, but

they will now be referred to as subject 4. In the IoT domain they do not have any devices themselves. However, they sell and co-create such solutions with their customers, thus giving them an integrity in the field. In addition they tell us that in most cases it is cellular IoT they are dealing with as telecommunication is the core delivery of Telenor[4].

Threat

Subject 4 mentions APTs and hacktivists as the most relevant actors in the cellular IoT domain. They discuss this because of the motivation these actors would have in the widespread platform and the big data they can provide. They point out that both sabotage and espionage are possible attacks in state and commercial settings and can be carried out over such networks. Because of the low endpoint security it would work as an effective measure to extract data from them or even tamper with the integrity to create false reading for those who are using the devices for monitoring their environments. Lower tier actors were also discussed. However they were not considered to be the most significant actors in the domain as their gains from an attack would not be significant considering the work required and the values behind a single node, which was pointed out as their probable attack surface.

Vulnerabilities

Subject 4 point towards the IoT devices as the vulnerability in cellular IoT. They mention the hybrid networks that the devices might be connected to as a vulnerability as regular mesh networks are more prone to attacks than cellular networks are. The actual vulnerability in this case would be the lack of segmentation which again can be seen as a lack of hardening on the devices software. They point out that unless the carriers and accesses on the devices are separated or segmented from the cellular domain it is hard to protect the value chains. The next vulnerability they discussed was the one related to the geographical widespread that cellular networks allow for. Because of this it might be hard for the owner of the devices to control whether or not the devices has been tampered with. In short the two vulnerabilities 4 discussed as the most concerning ones were the lack of hardening within the devices as well as the physical availability for malicious actors without mechanisms for controlling for tampering.

Security

In terms of security subject 4 tells that they are utilizing all possible restrictions they are able to apply to their cellular networks. Private APNs, white and blacklisting, restricted bandwidth speeds, encrypted air interface, as well as the implemented authentication mechanisms within the different generations of cellular

[4] `https://www.telenor.no/bedrift`

carriers. They also mention the strength of having a centralized managed network where the operator is able to apply security for all its customers versus having each of them do it themselves. This gives a better overall security as the big data the TELCO possesses enables a better overall situational awareness in the networks. In addition they mention the fact that the TELCOs often are subject to national guidelines and regulations giving bilateral effect into the customers services. When discussing what is missing they mentioned the endpoint as the weak link in cellular IoT. As they often are cheaply made and with resource constraints they need to have some kind of added security layer in order to stay protected. They mention that proper tuning of the cellular network and its policy can solve much, but it is not enough to achieve total control. An example discussed was the problems with speeding in traffic. The roads can be secure and properly made, but it is hard to enforce that it is being used in the way it was intended (within the speed limit). In the same context 4 argues that we need better control of the users and endpoints in the cellular networks in order to protect the entire communication chain.

5.5 Emcom Norway

General

Emcom is a company that specializes is cellular IoT with devices such as industrial routers, cameras, and different kind of sensors. Compared to the other subjects these are more device orientated than the previous ones. They deliver in the 10-thousands and provide technology to the Norwegian TELCO, industrial actors and a little bit to the private consumer market. The company was established in 2005 and our interview subject has been there from the early stages[5].

Threat

Subject 5 mentioned hackers as the biggest threats towards cellular IoT where it was mentioned the economic benefits of infiltrating a device before using it as a proxy for own free use of the cellular network. Examples mentioned were sending large amounts of commercial ads or phishing attacks over Short Message Service (SMS). These kind of attacks can end up generating huge costs for the owner of the device. Second we discussed the threat from other actors such as script kiddies or APTs. The subject was not afraid of the lower tier actors as these would lack motivation in addition to the gains of attacking a cellular IoT device that would not result in anything interesting. The APTs on the other hand were seen as potent threats towards devices that control or exist in the vicinity of critical infrastructure. If they are able to control dams, electrical grids, traffic, etc... They would be able to inflict great harm in the real world through these kinds of sabotage attacks. However, the subject did not see this as the most likely or biggest threat and by

[5] `https://emcom.no/`

focusing on lower level threat actors one would gain a better overall security in the networks.

Vulnerabilities

In terms of vulnerabilities subject 5 mentioned some human related ones such as lack of education and control routines. These human related vulnerabilities might be considered the underlying ones that are the reason for the technical vulnerabilities. The first vulnerability, related to lack of education was primarily discussed in the consumer context. It was mentioned that the manufacturers often are experts in their own production field and the TELCOs are experts in cellular technology, but the consumers on the other hand often are experts in their own specific field. This was discussed to possibly reduce the consumers ability to apply appropriate measures and mechanisms to secure their devices as a result of not knowing what the possibilities are. Next the one regarding control routines was mentioned to be a matter of controlling their inventories. Checking for tampering, patch and upgrade the software, etc. By not conducting such controls the devices could be kept in working environments even though they are exposed to malicious activity. Furthermore, 5 mentioned the manufacturing of the devices as a potential vulnerability. Many devices or even components are produced abroad and can intentionally or unintentionally have back doors or implemented malicious content. These can lead to attacks such as DDOS, espionage, battery drainage or even remote control. Lastly 5 discussed the vulnerability related to the physical control. As cellular IoT can be left in places without any kind of physical protection or control there is a risk that actors might tamper with the device unnoticed. They can abuse poor policy implementations such as default username and password, insert malicious compute in unprotected data ports or simply physically damage the device.

Security

In terms of security subject 5's company is not a big user of cellular IoT themselves. However, they do guide their customers to some degree on how to protect their devices and that is usually done through security features in the cellular networks. Private APNs, enable pin when disable, as well as restricting access to only the necessary addresses for it to function. Subject 5 also mentions the use of cellular networks in the first place as a good choice for achieving security as the TELCOs need their network to operate in order to sell their services. Consequently they will protect their networks accordingly in order to make sure that their customers will prefer them as well as ensuring the customers connectivity. When discussing what is missing in cellular IoT security subject 5 mentions a common certification as something that could be beneficial. Certifications are common in most other segments, but to the best of our knowledge it does not exist for cellular IoT. Next he mentions a more technical security feature that is missing, which is anomaly detection. These devices in most cases should be very predictable in terms of their

communication patterns. This is a great basis for anomaly detection, but something we have not heard of.

5.6 Microsoft USA - Cloud IoT

General

Microsoft is a multinational technology company established in 1975. They specialize in software development, where they are biggest in the world, as well as consumer electronics, computers and related services to the latter. Subject 6 belongs to the azure(cloud) IoT department and works in the development of services within the IoT cloud domain. Before starting in this position the subject has been working with cellular technology in one of the larger cellular technology companies in the world. Microsoft are currently hosting hundreds of millions IoT devices in their environments and our subject estimates that about 20% of these are cellular connected and that the number is increasing[6].

Threat

When discussing threats the first topic that was raised was critical infrastructure and how cellular IoT can be used as a gateway to tamper with it. Subject 6 stated that in order to conduct these kinds of attacks you would need skills and economic powers such as categorises APTs. We also discussed the lower level tier threat actors where script kiddies were neglected as they would lack motivation and skills to attack a cellular device. However, hacktivists and terrorists also were pointed out as potential threat actors in the domain, but they would presumably not be as critical as APTs. It was discussed that these actors would be financially motivated and that they might hide their malicious activities behind the cellular IoT in order to distribute malware such as ransomware. Summarised the biggest threat was seen as APTs with motivation of real world sabotage and mid-tier actors with economic motivations.

Vulnerabilities

Subject 6 points towards both ends of the cellular communication link when discussing vulnerabilities. First, from the IoT perspective where devices might have poor software and hardware implementations, legacy support, low access security, lack of segmentation and long distribution lines where each step introduces new potential security risks. Second, from the back end system side where devices might be reliant on communication with centralised servers. If these are not protected sufficiently it might also be possible to tamper with the devices ability to run as they were supposed to. In other words 6 did not have any concerns about the cellular part of cellular IoT, but was rather concerned about the consumers

[6]https://www.microsoft.com/

trust in cellular as a secure communication medium. It was pointed out that by choosing cellular carriers over other options one might get a false sense of protection that leaves them exposed at the endpoint and in the centralized areas.

Security

As discussed in the vulnerabilities the subject points out cellular networks as more secure than the other IT carriers. The TELCOs have a day to day focus on securing their infrastructure as well as the built in possibilities that allows the users to tune the networks to their own specific needs. IoTSAFE was pointed out as a technology that could harden the cellular networks even more, but the flexibility of key management was raised as a concern. 6 mentioned that the ability to decentralise key management and even give the customer the option to handle it themselves would be a step in the right direction. When discussing what is missing in cellular IoT the problem with multiple operators providing hardware and software for their own components. This leads to numerous different solutions and implementations from different producers which makes it harder to implement a common security solution across different platforms. From this the subject concluded that a standard or predefined integration would be beneficial for the cyber security in cellular IoT.

5.7 Norwegian Defence Research Establishment - Strategic Analysis

General

The Norwegian Defence Research Establishment is a government actor that is adjacent to the Norwegian Defence and has the responsibility of conducting research on behalf of the armed forces. The establishment is mainly organised with scientists and researchers with high academic degrees within their separate fields. Subject 7 was a Ph.D in the security domain and specialized in cyber security in autonomous systems, such as cellular IoT. It was reported that the establishment does not have large numbers of IoT devices themselves. However it was reported being a field of interest that they continuously were conducting research in.[7]

Threat

When discussing threats subject 7 did not point out any specific actors as more relevant than others. It was pointed out that the context and situation had to much of an effect on the threat picture in order to make any general assumptions. However, in the military context state actors were mentioned as natural threats in an operation between national and foreign military powers. By sabotaging censoring devices such as cellular IoT or even manipulating the input to the devices a

[7] https://www.ffi.no/

state actor could hamper the defending nation's ability to defend themselves. Another motivation discussed was a foreign state's motivation to conduct espionage through cellular IoT. Through this a nation might gain critical knowledge about the opposing nation that might give them leverage in a warfighting situation. Activists were also mentioned during the discussion as political stands could lead to motivation for harming the military. These actors would typically be know as hacktivist in the cyber domain, but the subject was equally concerned about physical damage as a result of high availability and autonomy. Low tier threat actors were also mentioned, but first as not being a threat. However, after discussing for a while it was mentioned that in consumer or consumer close IoT could be prone to attacks for the consumers personal well being. Motivations could be lower data bills, reduce monitoring, tamper with data to gain personal benefits, etc.. This was not considered a big threat, but was mentioned as a possible outcome by having devices on cellular networks that are often distributed far out from the service providers and that are hard to control.

Vulnerabilities

Subject 7 had many interesting vulnerabilities to discuss during the interview. The first ones were related to integrity where devices might be both physically and digitally tricked into react to faked data. In the physical domain one might abuse the censoring of the devices to have someone focus in a specific area before putting their main effort into areas that have had a reduced focus as a result of the first. This is related to the lack of intelligence in the devices and ability to sense what is and what is not an actual incident. In addition the data can be digitally manipulated in order to give the operator a false reading, thus trigger mechanisms that are not needed. This might not be a cellular specific vulnerability, but the distribution and low degree of physical control of some cellular IoT devices might lower the threshold for such attacks. Next subject 7 discussed the resource constraints of typical cellular IoT devices and how this could lead to different attacks. Information overload can occur if sensors are exposed to more information than they are supposed to handle, battery can be forced to drain faster or light security can be implemented to the benefit of longer battery lifetime. Somewhat related to this the virtualisation of SIM was also mentioned as a vulnerability as the level of security a physical SIM provide is better than what can be emulated in a processor. It can save some space in an embedded system, but on the other hand it will reduce the security. Last, the subject discussed the vulnerability in the cellular networks, where it was mentioned that packet core traffic was uncrypted. With components in the core being delivered by numerous different actors it was discussed that the possibility for malicious back doors is possible. Another network related vulnerability mentioned was the one related to legacy support and how old and well known vulnerabilities still were present through these kinds of implementations.

Security

When discussing security subject 7 mentioned IoTSAFE and that it might not give as much additional security as one might wish. Because it is utilizing security mechanisms that already exist it is not something that could not already be delivered with the previous technology. However, it was mentioned that the security in the SIM was something that could be beneficial and that managing the encryption keys in it could be more secure than doing it in the operating system. Considering the vulnerability mentioned with digitised SIM on the other hand it was mentioned that it should be kept on the traditional physical card format. When discussing what is missing some of the discussions from the vulnerability questions were raised again. First the problem with packet core packets being uncrypted. It was discussed that by adding such mechanisms to the cellular infrastructure the domain might gain a better confidentiality and assurance of integrity. Anomaly was also discussed with communication and data from cellular IoT being to some degree predictive. By adding some kind of intelligence to recognize this one might point out an infected device with ease. A last and interesting point on security conflict was raised. How secure should a device be made considering the conflict of confidentiality against availability? However, it seemed cellular IoT had some maturing to be done before these conflicts would be relevant.

5.8 Norwegian National Security Authority - Security Culture

General

National Security Association Norway is Norway's directorate for national preventive security. They provide advisory, security controls, review private and public companies security routines and also have a responsibility to uncover and manage severe cyber attack incidents. Subject 8 works in the security culture department and has been working for the association for about 20 years. In terms of cellular IoT the association is not a large user or distributor, but they do however work actively in the field through their governance and advisory. [8]

Threat

Subject 8 did not mention any of the threat actors as more or less relevant than others in the context of cellular IoT. It was discussed that any malicious actor that was presented with a vulnerability would have an opportunistic and perhaps even thrill seeking motivation to try and exploit it. It was mentioned that state actors might often come to the conclusion that the value of a vulnerability only is of interest when it can give them some kind of intelligence input. Typically in the form of espionage against foreign nations. Other than this there were no specific

[8] https://nsm.no/om-oss/dette-er-nsm/

motivations mentioned. However, it was acknowledged that the skills of the higher tier threat actors were more sophisticated than the lower ones, thus making them more potent in terms of damage potential. It was also discussed that lower tier threat actors might completely lack the ability to conduct any attacks. This was again discussed with the prerequisite that any subject was secured to an acceptable minimum. Because of this it can be interpreted that subject 8 sees higher and mid level tier threat actors as the most relevant ones in the cellular IoT domain and that they are motivated by opportunistic possibilities.

Vulnerabilities

In terms of vulnerabilities subject 8 pointed out the lack of security patching during the life cycle of the devices that have been deployed in their working environments. It was discussed that the culture for so called "fire-and-forget" was a vulnerability towards the systems as the manufacturers prioritise time to market and quantity over security and maintenance. Further it was discussed that back doors, both intentional and unintentional ones, were vulnerabilities. Not only in cellular IoT, but as a general one for the entire cyber domain. However, with IoT and cellular in particular one would gain an entry to a hugely distributed network with robust carriers that can take part in distributed kind of operations where huge number of devices could be controlled simultaneously. This vulnerability was also discussed further in the intentional back door track. A state actor could ally with national industry in order to have vulnerabilities or back doors implemented on behalf of the national state for abroad surveillance or attacks. This again relates to the espionage motivation discussed by 8 in the threat section. In short the two main concerns were the ones related to post deployment routines as well as potential back doors.

Security

Security is the speciality of 8's company and they put great effort into helping actors in the Norwegian society to stay educated, aware and up to date on what the possibilities and recommendations are. They even do security assurance tests for certain actors who have special needs for the kind of information certain actors are working with. For example the police and defence forces who need to be sure their communication is not compromised and that they can use their equipment without being concerned of information leakages. In such cases the association can do lab tests on the equipment to dig into the technology and test for vulnerabilities and even harden the devices. When discussing what is missing in the cellular IoT domain it was discussed relating to a note from the threats on a basic security level. As of today there are no legally anchored laws that require organisations to meet specific demands and levels in terms of security. This is something 8 mentioned as being a form of security that could raise the general security floor of the devices and which would benefit the society positively. It was mentioned that this has been implemented in some kind of way in California, but there is still no good examples

on how this can be done within the frames of a nation. Next, the deployment process of devices was discussed. It has been mentioned in other interviews that standard password and default chip sets can be a vulnerability. Subject 8 discussed that by implementing security through mechanisms such as enabling/disabling features as well as having to create new passwords would be beneficial and could reduce the mainstream attacks greatly. In short, according to 8 the main factors missing was security legislation as well as security on boarding and/or deployment processes.

Chapter 6

Discussion

In this chapter we discuss the results from our two research phases in order to answer the main research question. However, before doing this we find it necessary to discuss the results from the empiricism to pinpoint what was identified throughout the 8 interviews. Next, we will be able to compare the results of the empiricism against the litterateur study results in order to reveal the gaps between the two. Before continuing on to the conclusion in the next chapter we also discuss strengths and weaknesses of the thesis. This helps us evaluating the validity of our findings as well as outlining the scope of what future work should include.

6.1 Cyber Security in Cellular IoT - Empiricism

In this section we compare the answers from the results in order to get a better understanding of the empirical study. We collect the key takeaways from each of the interviews different sections and present them in three subsections, same as in Chapter 5, with threats, vulnerabilities and security. As far as it is possible we have strived to divide each of the subsections into logical topics during the discussion. This is a help us in the last part of the discussion where we discuss these results with the theory.

6.1.1 Threats

During the interview phase all threat actors from Chapter 4 were discussed by our subjects as more or less relevant in the cellular IoT domain. However, there were some actors that stood out from the rest as more potent in terms of weaponizing and for abusing the technology with different kinds of motivations. We continue on discussing each of the actors from top tier downwards and in relation to what they are motivated by in the eyes of the subjects. First the high tier withAPTs as state actors and state funded groups. Next, mid tier with terrorists and hacktivist and last, and last low tier with script kiddies and hackers.

High Tier Threats

Subject 1, 4, 6 and 7 all mentioned the high level tier threat actors as the one they feared the most in the cellular IoT. They discussed that the actors in this tier would be the ones that could inflict the greatest amount of damage in the real world, thus making them a bigger threat than lower level tiers even though they might not be as frequent. The other subjects also acknowledged APTs as potent threat actors in the domain. Subject 3 and 8 did not discuss any of the actors as a bigger threat compared to others, but subject 2 and 5 was not as concerned about APTs as other actors. This was discussed because of the lower frequency and probability of such actors conducting attacks compared with other actors. Subjects 1, 4, 6 and 7 all mentioned sabotage and espionage as potential attacks for these actors in the cellular IoT domain. They mentioned that these actors would not be economically motivated as many other actors probably would be, but rather seek to use the benefit of the largely distributed networks to inflict real world damage or to collect nation critical information. 8 additionally mentioned opportunism as a motivation and that the potential and more concrete use case would appear as vulnerabilities are tested. However, it was agreed that this also could lead to the motivations discussed by 1, 4, 6 and 7. As the two different attacks can have different motivations and outcomes we should discuss them further in separately.

Sabotage is an type of attack that typically would reveal the actors presence in the cellular IoT and would have some kind of notable effect in the networks or even the real world. Because of this the threshold for conducting such attacks might to some degree be anticipated as a result of an already existing conflict. The subjects that identified these actors as the biggest threat pointed out that attacks on critical infrastructure such as power grids, traffic controlling and communication networks would have potential to harm societies relying on the services greatly. With this they discussed that the threat actors could gain leverage to carry on further physical attacks or merely use this domain alone as an attack vector to gain their will against other nations.

Espionage on the other hand is an attack that most likely would go unnoticed when dealing with the high tier threat actors. Because of this it is hard to argue whether or not it is happening. The subjects mentioned this kind of attack as more likely than the former as it could be carried out without creating a real world conflict. They would simple use the sensors of the cellular IoT covertly. On a general basis a single device's data might not be very interesting, but when an actor is able to collect big data or very specific data it might yield an detailed situational awareness in sensitive areas. For example tracking of traffic and being able to detect military movements could be important, or infiltrating an important persons closed environment. These kinds of attacks could give a foreign state important data that could help them conduct further real world attacks or perhaps even protect themselves.

As mentioned subjects 2, 3, 5 and 8 did not consider APTs to be the biggest threat. They did agree on the possible attacks and the severity of them. However, they did not fear the two attacks mentioned above for each their separate reasons. 2, 3 and 5 pointed out sabotage as the most harmful attack that could be carried out by these actors, but they didn't see it as very likely to happen. They also argued that the skills and persistence of these actors would make it challenging to prevent them from conducting an attack if they are determined to carry them out. Subject 2 and 3 discussed that by having a healthy view and focus on security implementations and by focusing on the most frequent threat actors in the network we would better serve the general users of the cellular IoT networks. Subject 8 didn't mention sabotage, but was more concerned about espionage.

Espionage was not discussed by subjects 2, 3 or 5 directly, but through the vulnerability questions it was mentioned by subject 2 that the use of foreign hardware developers could result in unintentionally having implemented back doors and remote access possibilities. Through this the threat of espionage was indirectly mentioned as a result of poor hardware and software hardening. In difference to the other subjects, 8 mentioned espionage as a possible outcome of opportunistic attacks, thus under building it as an actual threat even among those who do not consider high tier threat actors as the scariest.

Mid Tier Threats

Subject 2 pointed out mid tier threat actors as the biggest threats to cellular IoT. It was discussed that these actors had access to great resources and that they might want to explore their skills in the real world for thrill seeking purposes. Typical actors that was mentioned beloning to this category was students with access to campus lab environments with great compute resources. 1, 3, 5 and 6 saw mid tier actors as a threat with motivation by economical gains. 1 did however not see how they would be able to do that as of now, but both 3, 5 and 6 thought it was a possible threat. 5 even discussed the possibility of using the cellular IoT devices as proxies for criminal activities on the economic expense of the benign user. 8 on the other hand did not have any specific thoughts on why mid level tiers would have an interest in attacking cellular IoT other than the thrill seeking factor.

An interesting topic discussed by subject 4 was the hacktivists as a equally potent threat as the APTs with real world effects from their attacks. However, in difference to subjects 1, 3, 5 and 6 who discussed these actors being economic and thrill seeking motivated, subject 4 argued that these actors could also be motivated to conduct sabotage and espionage. Equally subject 7 argued that hacktivist could be motivated to conduct sabotage attacks against cellular IoT especially against public companies that often are targeted by idealists that do not believe in the governmental practices or politics.

In its most dangerous form it was discussed that mid level tier actors can conduct attacks on the same infrastructure discussed in the high tier chapter. Subject 4 and 7 both discussed this, thus believing that mid tier threat actors to be possible actors to conduct attacks that can result in damage in the real world infrastructure and with equal motivations as APTs. However, subject 7 discussed that the skills these actors posses makes it more likely that these kinds of attacks would happen in the form of a real world sabotage rather than a sophisticated digital one. Subject 4 also put the list a bit lower for a probable attack where they mentioned industrial espionage. However, the skills needed to conduct these kinds of attacks are probably as sophisticated as the ones used for the same kinds of attacks done by higher tier threat actors. From this it can be discussed that subjects 4 and 7 argues that the skills of mid tier threat actors are as potent as the higher level threat actors.

A less dangerous form of attack that 1, 3, 5 and 6 mentioned as the biggest threat towards cellular IoT from mid tier actors is the financially motivated attacks. They discuss that criminals might actively seek to attack cellular IoT in order to abuse the cellular functionalities on the devices at the expense of the benign users. This ends up with the devices being used massively by the malicious actor, but with the benign user having to pay the bill. Subjects 3 and 6 additionally discussed the possibility of using devices as a seemingly benign jump station in order to distribute malware with e.g ransomware. These type of attacks would again target private persons or businesses which would get their data encrypted and only released back to them by paying the malicious actor to have the data returned in plain text. These kind of financial attacks would without a doubt be a heavy economic burden for those targeted by them. But in comparison to critical infrastructure damaging attacks it might not be as severe. However, both 1, 3, 5 and 6 saw this as the biggest threat in the mid tier threats and it should not be neglected when protecting the cellular IoT devices.

The last threat that has been mentioned in connection with these actors is the threat from mid tier threat actors with the intention of attacking with the motivation of thrill seeking. Subjects 2 and 8 were the only ones who mentioned this, but it is not unlikely to assume that in the context described by 2 that students who have acquired new skill would want to test them out and maybe even in accordance with a hacktivist group to justify them. With the capacity of data centers related to such institutions this might be a possible way to conduct demanding attacks such as those mentioned to have real world effects.

Low Tier Threats

None of the interview subjects identified low tier threat actors as ones they feared could do any substantial harm within the cellular IoT domain. However, from the

previous section we could read that 2 feared thrill seeking hackers with great resource availability. It could be argued that these actors could be categorised as low tier threat actors, but that would be a matter of definition. Nonetheless, the motivation of thrill seeking, mentioned by 2, would not be categorised as very harmful. The action of conducting an attack on a vulnerability, but without exploiting it for further malicious activities would likely not result in any unrecoverable harm.

The most severe threat identified in this segment was the one identified by 3 and 7. They both discussed consumers as a threat where cellular IoT in the vicinity of people could be targeted for gaining personal advantages. Because these devices are either restricted in terms of functionality or restricting the users of the devices they would be motivated to remove these in order to gain personal advantages. This could be cheaper data by using IoT plans for internet browsing, sharing personal services with others who are not paying for them, or as 3 mentioned removing restricting controls functionalities. To some degree this could lead to economic gains for the consumer on the behalf of the TELCO, but the potential is probably too low for them to put resources into catching the perpetrators. The restricting functionalities on the other hand might be more severe as they often can be demanded by law. In the truck driver case discussed by 3 such attacks might end up enabling the driver to continue driving even though he was supposed to rest. This could result in the driver increasing the risk of a collision which the original restriction in the device might have prevented.

1, 4, 5 and 8 all discussed that the low tier threat actors were missing the skills and motivation to attack cellular IoT. However, 8 argued that this was with the prerequisite that a kind of baseline security had been implemented. The vulnerabilities discussed by the interview subjects does however show that this might not always be the case, thus actualizing the actors regarding 8's statement. On the other hand. As 1, 4 and 5 also mentioned, the skills would still be low. Because of this it could be argued that the results of these actors conducting malicious activities in the cellular IoT domain most likely would be bearable and even negligible. This also matches the consequences discussed by 3 and 7. In short 1, 4, 5 and 8 all agree that the threat presented by the lower tier actors most likely is not one that should receive focus. This because they do not possess the skills or motivation needed to carry out attacks that would result in anything severe worth prioritising over the threat presented by higher tier actors. Also by having a suitable baseline security many of these threats would become irrelevant at once.

It should also be mentioned that 6 did not even discuss the lower tier threat actors. This alone states something about the threat presented by this category in 6's mind. Whether that was a result of many opinions on the other categories in combination with lack of time or if it was because the threat was negligible is uncertain. But with an hour long interview it should have been time to mention them if they were a big concern.

6.1.2 Vulnerabilities

In this section we discuss the vulnerabilities mentioned by our interview subjects in Chapter 5. From the interview we identified three main topics that were discussed through the vulnerability sections of the interviews. The first one was related to the devices. This was also the category that was mentioned the most and which we again could divide into different phases of the IoT devices life cycle discussed in Chapter 4. Next the vulnerabilities were related to the cellular networks. These were more generic and could be discussed under the same header. Last was the human related vulnerabilities which equally to the latter could be discussed under the same header.

Cellular IoT Vulnerabilities

In the following four sections we will discuss the vulnerabilities mentioned in the interviews based on what phase of the cellular IoT device's life cycle they belong.

Manufacturing
The manufacturing of devices was discussed by all interview subjects on one or more topics. From this we can argue that the manufacturing process in itself can lead to big holes in the security of cellular IoT in the mind of our interview subjects. However, there were some topics that were mentioned by many and others that was mentioned by only one. This does not necessarily mean that it is not as bad of a vulnerability, perhaps even opposite that it could be one that has not been broadly recognized yet.

The first vulnerability was related to back doors on the devices. These could be both intentional or unintentional ones that would allow an attacker to access the unit unauthorized. 1, 2, 5 and 8 all discussed this vulnerability in one way or another in their answers and argued that the lack of control over the manufacturers or the manufacturers malicious intention could lead to this vulnerability.

The second vulnerability was the one related to the hardening process of the devices once they had been assembled. Problems such as the one described by 1 with a pet GPS collar with a microphone inside it are prime examples of what these vulnerabilities can be. Whether they are intentional or unintentional wouldn't really matter, they do pose a threat anyhow and could be exploited by an actor with knowledge of them. 1, 2, 5 and 8 all agreed that the lack of proper hardening during manufacturing was a problem that posed a problem for the users of the cellular IoT

The third vulnerability is one that was only mentioned by 7 and is related to virtualisation of the SIM. 7 mentioned that the security in a physical SIM is quite good and that by virtualising it we would loose some of the security benefits provided from the physical one. It was discussed that by putting parts of the cellular domain

into the common areas of the device we might possibly gain a negative security effect as the cellular related data should be kept separate from the rest of the devices hardware.

The last vulnerability discussed that relates to the manufacturing was the one related to resource constraints. It could be discussed whether or not it is a result of the manufacturing process. However, it would be during the manufacturing and component shopping that the constraints would get applied to the devices. Nonetheless the vulnerability of resource constraint is one that 7 argued cellular IoT suffer from and which further makes them vulnerable towards overload and outage kind of attacks in their operational phases.

Bootstrapping
Bootstrapping is the next phase in the life cycle of the cellular IoT devices. This would be the phase where the users of the devices have received them and are configuring them to become a part of their networks prior to putting them into operation in their appropriate working environments. There was only one vulnerability discussed directly under this phase, but it could also be connected to human related vulnerabilities which we discuss later.

1, 3, 4, 5, 6 and 8 all mention the vulnerability of not implementing security mechanisms on their devices before putting them into operation. This could happen in many different ways, but there were some that were mentioned more often than others. For example the use of default usernames and passwords were pointed out as a huge vulnerability as it would leave the devices exposed towards distributed opportunistic types of attacks. If a threat actor was to trying to log in with default user names and passwords in a broadcast type of manner and would meet such devices the actor would essentially gain full access to the devices. This vulnerability would result in all other security mechanisms being pointless in many cases as a direct entry on a device would allow an attacker to roam freely. This in combination with the some of the vulnerabilities we discuss in the operational phase could lead to an easy entry for an attacker and this vulnerability could therefore be seen as a quite severe one. Essentially the vulnerability that was being discussed by the subjects was the one related to consumer-related hardening. It might also appear in the form of poor network tuning where the cellular networks security potentials have not been utilized to the fullest, thus leaving openings to the devices that are not needed and that malicious actors can use to attack from.

Operational
The operational phase of the IoTs life cycle was the next one discussed. This was also the phase where the most vulnerabilities was pointed out and naturally so with this phase covering the main part of the devices life time. In this phase the devices would typically be in their working environments with the pros and cons this would include - typically unguarded and geographical spread in a cellular IoT

context. The subjects primarily discussed one vulnerability as the most concerning, but some of the subjects also had additional ones they were concerned about.

The vulnerability discussed by most in the operational phase was the one related to the geographical widespread the cellular networks allow for. 1, 3, 4, 5 and 7 all argued that this was a vulnerability introduced by the cellular carriers. It could be discussed that this was not a vulnerability in itself. However, it was discussed as a core problem when dealing with cellular IoT. Because of the geographical widespread it would become hard to monitor and control the devices physically. This could be seen in combination with the vulnerability of undetectable tampering which 1, 3, 4 and 5 all mentioned in the same discussion. 1 further discussed this lack of physical control in combination with the low frequency of certain devices coming online. It was argued that this could further hamper with the owners ability to digitally detect tampering as well.

The next vulnerability discussed in the operational phase was related to integrity of data. 3 and 7 discussed that by digital manipulation of data at the cellular IoT devices an attacker could narrate the situational awareness of the benign users. E.g by giving a false reading on how full a dam is an attacker might trick the operator to either flood or empty it in an effort to adjust the level. 7 additionally discussed that this could be done physically as well by using simple methods such as a glass of air placed over a censor under water. Either way how it is conducted the vulnerability toward integrity of data is one that could lead to great harm in attacks where they are being exploited.

The third vulnerability was only discussed by 1 and was related to signaling. 1 discussed that cellular IoT was vulnerable to different kinds of signaling attacks that could result in several different outcomes. The first one was related to fake base stations where a malicious actor would send out cellular network based protocol messages that would trigger the devices to attach to them. By doing so it was argued that the malicious actor could either deny the device of service or generate traffic that would force it to drain its battery. Next 1 discussed a vulnerability toward position tracking where a malicious actor could collect signals from the device in order to uncover its physical position. By doing so the actor would be able to find the devices and further exploit the vulnerabilities related to the low physical control.

The last vulnerability discussed in the operational phase of the devices life cycle was one related to back end system dependencies. 6 argued that some cellular IoT devices were depending on their back end systems in order to operate the way they are supposed to. It was discussed that such dependencies could lead to malfunction or even no function on the devices if the systems were not running in the back end. It could be argued whether or not this vulnerability is directly related to the cellular IoT domain, but it could certainly have an effect on it. However,

the devices could arguably be configured to run even when the back end systems were down so that when everything is up and running again the data would still be available regardless.

Maintenance
Maintenance was the last phase of the cellular IoT devices life cycle discussed during the vulnerability questions. In this phase the devices would typically have been running in their environments for a period of time and be in need of some kind of maintenance or patching before continuing into a new operational phase. This phase was only discussed by 8 and only one vulnerability was mentioned.

8 discussed that the devices were vulnerable during patching or software upgrades were back doors could knowingly or unknowingly be added into the devices by benign or a malicious actors. This would result in equal outcomes as those discussed in the manufacturing phase where back doors also were mentioned as vulnerabilities.

Cellular Network Vulnerabilities

In difference to the above four categories of vulnerabilities the next ones are related to the cellular networks. This would be the other TELCOs side of the cellular network consisting of the RAN and packet core which were described in chapter 4.3. An interesting note on this section is that only 2 and 7 discussed the vulnerabilities present in the cellular networks. Whether this was a result of high focus on the device specific vulnerabilities from the other subjects or if they didn't know about any is uncertain. However, many of the other subjects mentioned the cellular networks as a source of added security, which might explain the observation. The first two vulnerabilities were directly related to the core network and the next two could be both RAN and core related.

The first vulnerability was discussed by 2 and was related to 5Gs possibility of distribution of core functionality in non-cellular environments such as clouds or edge compute. It was argued that by having these roles deployed in environments outside of the TELCOs premises one would be more exposed towards traditional IT-network threats and vulnerabilities. This means the vulnerability was more about losing the safeguarding that the TELCOs provide and that the added availability exposes the core networks towards additional threats. This form of distribution of the cellular network was discussed to only be possible in 5G networks and would therefore not apply to earlier generations of cellular technologies.

The next core related vulnerability was discussed by 7 and was related to the lack of encryption within the cellular core networks. 7 described that by default only the air interface(RAN) had applied encryption in order to protect data when it is exposed on wireless carriers. However, in the core networks it was mentioned

that TELCOs had to apply encryption themselves if they wanted the added confidentiality as the standards did not specify any. 7 discussed that this often lead to the core ending up being uncrypted exposing the user traffic to potential back doors in the core nodes. As a result of this it was discussed that malicious actors could listen in on the traffic by remotely accessing a node in the core network.

The next vulnerability was related to 5Gs full stack internet protocol support. 2 argued that the 5G cellular networks would inherit the vulnerabilities that had been present in traditional IT-networks with this integration. What the exact vulnerabilities would be was not mentioned, but the concept as a whole was seen as a vulnerability as opposed to the earlier cellular networks adopted protocol stacks.

The last vulnerability discussed related to cellular network vulnerabilities was the vulnerability of legacy support. 7 discussed that by allowing for old protocols and generations of cellular technologies to run in modern infrastructures one would have to live with the vulnerabilities present in those. This means that even though new protocols and generations of cellular technologies have been patched, improved and implemented, the security gains would be lost as a result of unpatched legacy support. 7 argued that this was a vulnerability that would be present in both the RAN and the core networks.

Human Related Vulnerabilities

The last vulnerabilities mentioned during the interviews were related to human factors or routines. 5 and 6 were the only ones who addressed this topic directly, but it could be argued that many of the vulnerabilities mentioned above are direct or indirect results of the same vulnerabilities we now discuss. It could also be discussed whether or not they are directly and specifically related to the cellular IoT domain, but as our subject mentioned them we discuss them either way.

The first vulnerability mentioned by 5 was related to the potential lack of education in the personnel working with cellular IoT. It was discussed that consumers without knowledge of security in devices or cellular networks could lead to them placing their cellular IoT devices in production environments with severe vulnerabilities open for exploitation. It could be argued that this vulnerability should be mitigate by the manufacturers and TELCOs by implementing appropriate security measures for their customers, but it would arguably be hard for these to tailor solutions for all their customers with different needs without being able to discuss with the consumers.

The next vulnerability discussed by 5 in terms of human related vulnerabilities was the vulnerability towards bad control routines. With the cellular IoT being exposed to geographical widespread and possible back doors several places in the cellular domain it might be wise to have implemented control routines to be able

to detect tampering and other forms of malicious activity on their devices. With this in mind it could be discussed that this vulnerability would reduce the users of the cellular IoT devices ability to detect whether or not their devices have been compromised or tampered with.

The last vulnerability discussed related to human factors was discussed by 6 and was related to false sense of security in the cellular domain. As mentioned under the cellular network vulnerabilities many of the interview subjects had a considerable trust towards the cellular networks being a source of security. These subjects were interviewed as people with good knowledge on cellular IoT. It would therefore be possible to think that actors with less insight in the domain could have the same thought, but without the same knowledge on the vulnerabilities. This could lead to consumers relying on cellular carriers alone as a security feature for their IoT. But with a poor implementation this could leave them being exposed to numerous vulnerabilities. Arguably this is a result of poor knowledge or lack of education, but the specific risk of consumers thinking the cellular networks provide proficient security alone based on the TELCOs reputation of being secure is very interesting.

6.1.3 Security

Security is the last category we discuss related to the empirical review of the thesis. In this chapter we discuss the answers regarding what security mechanisms that are missing in today's cellular IoT in the eyes of our interview subjects. Equally to the vulnerability chapter there were 3 main categories of mechanisms mentioned by the subjects. The first ones were related to cellular IoT devices, next cellular networks and last human related ones.

Cellular IoT Security

In this section we discuss security mechanisms that would be implemented on, or that are closely connected to the end point devices in the cellular domain. These could be overlapping with some of the mechanisms that we discuss in the network section, but we discuss them according to how the subjects described them.

The first security mechanism we discuss was mentioned by 4 and is related to control over end points. 4 claimed that the endpoint was the weak link in the cellular IoT domains security. 4 discussed that having better insight of what is happening on the devices could allow for a better ability to detect whether any malicious activity is happening. It could be argued that these kinds of systems already exist and are broadly available from multiple vendors. However they would in most cases be connected to some kind of back end system outside of the cellular domain. Because of this it is most likely that 4 was talking about these sorts of mechanisms missing within the stand alone cellular networks. Further this could be discussed as a cellular network security mechanism, but with regards to the vulnerabilities

discussed at the devices side of the network it was mentioned in this context by 4. In their eyes the cellular networks were already proficiently secure and had enough possibilities to mitigate possible malicious activity on the devices.

The next security mechanism was discussed in the context of a vulnerability discussed by 5. It was related to the lack of acknowledged certifications in the cellular IoT domain. 5 argued that by having some kind of stamp on the devices stating that they comply with a certification could help consumers more easily chose the secure devices over poorly developed ones. It was stated that these kinds of certifications would have to be made or at least supported by some kind of acknowledged organisation within the cellular domain for consumers to put their trust in it. 5 discussed that by having some kind of backing from an organisation we trusted in and that have approved a certification could be a step towards increasing the devices base line security.

Cellular Network Security

In this section we will discuss the security mechanisms that our interview subjects argued were missing in the cellular networks. This is the section that was discussed the most during the interviews which could be seen as strange with many of the subjects mentioning the cellular networks as one of the sources of security within domain. However, the network security features mentioned as missing might have been discussed in this context as a way of controlling or monitoring the devices rather than securing the networks better. This would make sense as the data on the network might give some indications on what is happening on the end points.

2 and 3 both discussed that the cellular networks are missing the ability to monitor data in the cellular core. They both discussed that such mechanisms exist in conventional IT-networks, but that from a cellular network point of view they do not exist. It is an interesting note and also something that we didn't read about in the theory sections. By implementing such mechanisms the TELCOs might be able to provide services such as those provided in conventional IT-networks through security operation centers. With the paths the cellular technologies are taking with higher integration towards traditional communication protocols one could perhaps imagine that services could live within the cellular networks only and that services such as monitoring would be a natural part of the security implementation needed to control for malicious data in the networks. Further, 2 argued that the ability to detect anomaly should be a key element. Especially for cellular IoT where communication patterns in most cases are predictive. This note was also mentioned by 1, 5 and 7 who pointed out the exact same argument about the predictiveness of cellular IoT. They did however not mention it in the context of monitoring, but one could argue that it was implied in their claims. Lastly it was discussed that the integrity of data should also be possible to predict to some de-

gree. It was argued that if a device suddenly claimed to be in a location farther away than physics would allow for within the given time frame there should be an alarm raised. It could also be claimed that this is a form of anomaly, but with regard to the vulnerabilities regarding integrity of data it is an important note.

The next and also last security mechanism that was discussed as missing in the cellular networks was the fact that the data in the core was uncrypted. From the vulnerability chapter we could read 7 claims on this and how it created a vulnerability towards back doors in the core nodes. By implementing encryption mechanisms in the core network this would deny such back doors to allow for extraction of data in plain text as the situation is today according to 7. It could be argued that these kinds of mechanisms already exist, but only in the conventional networks. However, with the implementation of full stack internet protocols in 5G it might be a simple adoption to implement those encryption mechanisms in the cellular networks as well. Nonetheless the missing security mechanism would most likely add another dimension of security in the cellular networks if the claims are true.

Human Related Security

The last category of security mechanisms that was discussed as missing in the cellular IoT domain was those related to human actions. This would typically be topics that would fit under category risk, governance and compliance(GRC), which is often a separate information security field in private and public sectors. There were only two topics discussed under this category and it was done by 6 and 8.

First was the lack of standardisation where both 6 and 8 mentioned that some kind of approved and acknowledged standardisation would be beneficial in raising the security baseline of cellular IoT. As of today they discussed that such standard does not exist and that the result from it was that users and manufacturers does not have anything to work towards in terms of security. It was also noted that it was a need for educated customers that would be demanding compliance with the standardisation, but it could also be argued that this would need a standardisation to be in place first.

The next and last discussion from the interviews was related to the lack of legislation within the cellular IoT domain. 8 discussed that by implemented lawfully required measures in terms of security no one under those laws would have the options to chose not to comply. This would be a very drastic measure and perhaps also a bit narrow if it was to only apply for cellular IoT. But it could be argued that if legal requirements are made there should at least be a section related to the matter. It was also mentioned by 8 that such legislation had been made in California in order to better regulate how IoT is used. Therefore it is not unlikely that it could happen elsewhere at a later point in time. But as of today in most cases there are no legislation related to cellular IoT security.

6.2 Theory Versus Empiricism

We now discuss the gaps between the litterateur and empiricism. This is where the main research question of the thesis is answered. We discuss each of the topics in their separate sub sections following the categories; threats, vulnerabilities and security.

6.2.1 Threats

First we discuss the gaps between the threats in each of the results chapters. Both of the chapters used the categories high, mid and low tier threats and we therefore compare them in the same way. For each of the categories we first compare the motivations of the threat actors. This tells us something about the severeness of the attacks they might conduct. Second we compare the perceived threats from each of the actors. And lastly we discuss the observed gaps.

High Tier Threats

For the high tier threat actors the theory mentioned acquiring information as the biggest motivation. It was discussed that IoT technologies were potent platforms for espionage and that high tier actors would be drawn towards conducting such attacks on the platforms. It was also mentioned that they would have a motivation towards inflicting damage in the real world through the IoT. This would be considered what the empiricism discussed as sabotage.

The empiricism also pointed towards espionage and sabotage as the most likely attack that could be conducted by high tier actors in the cellular IoT domain. This tells us that both the theory and empiricism agree that these motivations are the greatest ones for high tier threat actors in the cellular IoT.

Next is the perceived threat from this high tier segment. The theory describe them as the biggest threat and the one we should be the most concerned about. With the severeness of sabotage attacks and the kind of damage they could inflict on critical infrastructure they are most likely the most dangerous attacks within the cellular IoT domain. However, from the empiricism it is discussed that the low frequency of such attacks and the skills of the people behind them make them hard to avoid. Thus, it was discussed that the high tier threat actors were not perceived as the greatest threat in the domain and placing them in the middle for our three categories.

In terms of gaps, theory and empiricism do not seem to agree upon the threat posed by these actors. While both agree that the outcome of these actors attacks are the most severe there is a gap in terms of how empiricism and theory rate the overall threat. This could be a result of how they measure threat. While theory might only valuated the severeness of a stand alone attack empiricism may have added the dimension of frequency.

Mid Tier Threats

Theory claimed that the mid tier threat actors would often be monetary motivated, but could also seek to cause disturbance. It was also argued that they could be capable of stealing state and corporate information much like the high tier actors. However, where the high tier threat actors were interested in the information itself, the mid tier actors would want it for the purpose of monetary gains. Lastly it was argued that these actors might have idealistic motivations towards carrying out attacks that could result in real world damage or disturbance.

The empiricism also mentions monetary gains and disturbance or sabotage types of motivations. They agree on the same kinds of attacks and the same kinds of motivations. However, the empiricism mentions the thrill seeking motivation in addition. It could be argued that thrill seeking could be based in idealistic or rebellious kinds of root causes, but 25% of the interviewed subjects stated this as a motivation that the theory did not mention.

In terms of gaps, there is a disagreement both for the motivations and perceived threat. While theory argued these to be the second most dangerous actors, empiricism pointed them out as the biggest. The empiricism based this argument on the persistence of the actors and the high frequently of their attacks. The theory on the other hand only focused on how severe the attacks of the actors where and and not how likely they would be. Because of this the mid tier treats were seen as less dangerous in the theory than in the empiricism. In addition there was a gap in terms of motivations. This could possibly be a question of definition where we saw thrill seekers in the background and later categorised them as low tier threat actors. However, in the context of mid tier actors with their characteristics, the empiricism points towards what we can call a gap.

Low Tier Threats

In terms of motivations both theory and empiricism agree that these actors would seek to gain personal benefits through their attacks. This could either be in the form of monetary gains, by trying to unlocked services or remove constraints in their cellular IoT. Furthermore theory describes a motivation not mentioned in the empiricism which was related to revenge. This is one that very much could be a potential motivation with frustrated employees with the "right" accesses. The last motivation mentioned was discussed only in the empiricism and was related to thrill seeking. It was mentioned that the human curiosity would be a leading factor to this and therefore makes it as relevant as the other mentioned motivations.

In terms of how big of a threat these low tier threat actor pose it was agreed by both theory and empiricism that it was low. Both discussed these threats to be the lowest ones in the cellular IoT domain as the skills and motivations would make

their ability and footprint in the case of an attack negligible.

In terms of gaps theory and empiricism did not agree on all of the motivations. The empiricism discussed thrill seeking as a motivation, but theory did not mention this. However, from the background it was described that thrill seekers were among the lowest threats actors. Because of this it is likely that the litterateur used for the theoretical research was not extensive. Next there was a gap in terms of revenge being a motivation which empiricism did not mention. Arguably this could be a result of the direction of the discussions during the interviews where much of the focus was on the higher tier threats. This in combination with the already low perceived threat from these actors might have lead the discussion to end quicker and passed by the topic of revenge being motivation behind an attack.

6.2.2 Vulnerabilities

Next, we discuss the gaps between the theoretical and empirical vulnerabilities. Equally to the sequence in the results we follow the three categories device, network and human. Human related vulnerabilities were not addressed in the litterateur study at all and consequently there is a gap. However, we discuss these differences as they point to a seemingly incomplete understanding of these important issues.

Cellular IoT Vulnerabilities

For the device vulnerabilities we discuss the gaps following the steps of the life cycle described in the background. First, manufacturing phase, followed by bootstrapping phase, operational phase and last maintenance phase.

Manufacturing

The first vulnerability we discuss is the one related to hardening. It was mentioned both in theory and empiricism sections, but not in the same way. Both the research sections described the lack of software hardening as a vulnerability. However, theory did not mention hardening in the form of removing unnecessary components from standard chip sets like empiricism did. Therefore the vulnerability of not conducting hardware hardening is a gap we have identified.

The next vulnerability was related to the virtualisation of SIM. It was mentioned in the empiricism that by implementing the SIM into the rest of the devices hardware one would loose the security it provides. Theory did not mention this vulnerability in the manufacturing phase, thus leaving us with another gap.

The last vulnerability that is related to the manufacturing is the one regarding the constrains of resources. The litterateur results did not mention this, but it was presented in the intro as a trait of IoT. Because of this we will not consider it to be a gap, but rather highlight the limitations of the theoretical study.

Bootstrapping
There was only one vulnerability discussed in the empiricism related to the bootstrapping of devices which was related to the configuration of security parameters prior to being deployed. Factors such as not changing default passwords or configuring traffic policies were mentioned as factors. The theory could be argued to have mentioned this through what it referred to as software vulnerabilities. However, the empiricism points towards a very concrete vulnerability of not having security onboarding routines. It could be that the litterateur had this vulnerability in mind when discussing software vulnerabilities, but the lack of details when describing it makes it hard to decide whether or not this is an actual gap found in the thesis.

Operational
The operational phase was the one that was discussed the most during both research phases. Many of the vulnerabilities were agreed upon and therefore we do not discuss them further. However, we discuss the gaps that was observed between the two.

The first gap we will discuss is from the empiricism where the geographical widespread of cellular IoT. It was pointed out that the devices would be vulnerable as this would allow an attacker to gain physical access to the devices without being noticed. The litterateur results did not discuss this vulnerability and it is hard to argue that any of the less specific vulnerabilities it is discussing could be related to this. However, we can not exclude the possibility that other researches have discussed it, but we did not find that.

The second vulnerability gap was related to integrity of data. Theory discussed this from a digital point of view, which empiricism also did. However, the empiricism additionally mentioned the risk on physically tampering with the data of the cellular IoT devices. Because of this the vulnerability on physical integrity is a gap the empiricism has pointed out and that theory did not reveal.

The third and last gap for the operational phase was related to vulnerabilities towards signaling attacks. The theory only mentioned the use of signaling, but not the fact that the signals could trick the devices into doing what they are told or to track their positions. Because of this it could be argued that there is a gap where the empiricism has added another dimension to the vulnerability the theory discussed.

Maintenance
There was only one vulnerability discussed related to the maintenance phase in the cellular IoT life cycle during the empiric research. This vulnerability was related to patching software, which was also mentioned by theory. Therefore we can not argue to have discovered any gaps in this phase. However, with the lack

of material for both the research phases of this thesis it could be argued there is a need for further work on this topic.

Cellular Network Vulnerabilities

For the gaps in the network vulnerabilities we do not go into detail on all the ones described in the litterateur results as many of these were very technical and low level. Therefore we discuss the gaps in this section more in line with what the empiricism discussed. The more technical details from the litterateur study we categorise as protocol vulnerabilities.
The first gap mentioned stems from comments by the empiricism and was related to the possibility of core distribution in 5G. It was mentioned that this kind of functionality would bring parts of the cellular infrastructure outside of the TELCOs premises, which was argued to be a security layer in the networks. By distributing the core it was argued to increase the attack surface of the network and that it therefore would be a vulnerability versus having it on premises.

Second the empiricism discussed a gap where it was mentioned that the core networks did not have any encryption. It was argued that this exposed the networks towards other vulnerabilities such as back doors in the core network nodes. This was not discussed in the theory and we could therefore argue it to be a gap the empiricism has unveiled.

The last gap was discussed in the litterateur section only and was related to several of the broadcasting protocols of the cellular technologies. It was argued that the lack of encryption in the broadcast messages would enable third party actors to hijack or gain unauthorized details on the devices in the network. This gap is one that is very technical and could not have been expected to be pointed out by our interviewed subjects. The theory within cyber security in cellular networks seems to be much more mature than the one we found for the cellular IoT devices.

Human Related Vulnerabilities

The human related vulnerabilities are the last ones we will discuss. These kind of vulnerabilities were not mentioned in the theory we found, but was discussed broadly in the empiricism. Because of this we chose to add the human category for both vulnerabilities and security.

The first vulnerability was the one related to lack of knowledge in the cellular IoT domain. This could arguably be considered common knowledge and would likely be something theory would have reveal if we had applied the appropriate search criteria. However, due to the initial focus on the technological aspects of the cellular IoT domain this constitute a gap.
The next gap mentioned by the empiricism was related to the lack of control routines. It was mentioned that devices such as cellular IoT would often be left

in environments where remote control would be hard to manage. Because of this the vulnerability of not having control routines in place was pointed out as a gap.

The last vulnerability gap mentioned in the human related context is one that is more likely than the above two not to be known in the theory. The vulnerability is related to the users high trust in cellular IoT networks and TELCO. With this they might think that by using cellular instead of conventional IP-network carrier technologies they would be safe from this alone. This vulnerability of putting all the trust in the TELCOs reputation of being secure might reduce the focus to protect the rest of the value chain, such as the devices and back end systems.

6.2.3 Security

Last we discuss the gaps in the security between the litterateur and empiricism. This is the last part of answering the main research question of the thesis. We follow the same sequence and use the same categories as in the vulnerabilities with device specific security first, followed by cellular network related ones and last human related ones. Equally to in the vulnerabilities the human related security mechanisms were not discussed in the litterateur. We therefore equally discuss these gaps as the litterateur seemingly points towards an incomplete understanding of these human related issues.

Before getting into the details it is also worth mentioning the differences in research questions 1.3 and 2.3. Where 1.3 aimed to discuss current security mechanism, 2.3 was looking for ones that were missing according to the empiricism. In addition the ones from the theory were very focused on cellular IoT only. This was the scope of the thesis, but we might also have excluded ones from conventional IoT that could have been relevant for the cellular IoT as well.

Cellular IoT Security

For the device specific security everything discussed except from the mechanism IoTSAFE can be considered gap. However, the empiricism did not mention too many other device related mechanisms either and we also have to keep in mind that the ones mentioned were related to missing mechanisms.
The first one was related to the control over the cellular IoT devices. It was mentioned that within the cellular domain there was a lack of possibilities to monitor what is happening at the end points. However, these kinds of security mechanisms could be argued to be closer related to the network specific mechanisms. However, as it was mentioned in this context by one of the interviewed subjects we chose to take a note of it under the device security as well.
The next gap was mentioned by the empiricism and was related to certifications. It was argued that by having a common and acknowledged certification on cellular IoT devices it would be easier for consumers to chose the more secure option. It could be argued that also this gap belongs to another section, but it could also be discussed whether it is an actual gap. If the litterateur review had been looking

for a security certification for IoT it is likely that something would have come up. However, in the context it was discussed by the empiricism it might as well be a gap in terms of the lack of an acknowledged and widely used certification.

Cellular Network Security

The next category we discuss is the gaps for the network related security mechanisms. In this section the litterateur discussed many mechanisms that was not directly mentioned in the discussions of the empirical results that tried to answer what was missing. However, in the results from Chapter 4 many of the same mechanisms that already exist were mentioned by both the research phases.
The first gap was discussed by the empiricism and was related to the missing functionality in terms of monitoring. It was claimed that the predictiveness of most cellular IoT devices should make for a great foundation for anomaly detection. Yet it does not exist to our knowledge. It was argued that a monitoring system within the cellular networks would enable for early detection of integrity mismatch, abnormal data use, abnormal communication patterns and unfamiliar communication parties for the devices. These kinds of mechanisms are more common in conventional IP-networks where anomaly detection is commonplace. However, to the best of our knowledge they do not exist in the cellular networks.
The next gap was related to the lack of encryption in the cellular core networks. It was argued that encryption should not only be implemented on the air interfaces, but also within the core networks. By doing so we would ensure protection from potential infected base stations and MitM type of attacks. With the transition towards 5G it should even be possible to adopt mechanisms from conventional IT-networks. Additionally it could be argued that the IoTSAFE mechanism discussed above could be the answer to this problem as its end-to-end encryption could contribute to mitigating it. This means that by looking at this mentioned gap in the context of cellular IoT domain it could be considered not being a gap. However, looking at the stand alone cellular networks without the possibility of using IoTSAFE it could be argued differently.

Human Related Security

The human related security is the last category we discuss the gaps for. These security mechanisms are the non-technical ones and which raises the security level as a result of people following and enforcing them. As mentioned above the litterateur did not look into human related security and we could therefore consider all findings within the category to be gaps. Nonetheless, we will discuss them briefly once more.
The first gap mentioned was pointed out in the empiricism and claims there is no standardisation or certification related to cellular IoT security. It was discussed that without a standard it is hard for both manufacturers and consumers to know what security features should be implemented to reach a sufficient security level. There are guidelines and recommendations, but as far as we could observe it stops

with that.

The next and last security mechanism gap mentioned was the one relating to missing legislation. The empiricism argued that certifications, guidelines and recommendations would not be followed strictly enough unless they would become lawfully mandatory. It was mentioned that IoT had been regulated in California, USA, and that this would be a step in the right direction. However, in order to reach a common baseline and understanding of how to secure cellular IoT it needs to be regulated by some kind of legislation.

6.3 Limitations and Strengths

In this last discussion chapter we take a step back and evaluate the thesis' weaknesses and limitations. This helps us evaluate the validity of the results as well as mapping what parts of the study that are worth looking further into. Specifically we will do this by discussing the two review phases of the thesis followed by the results. However, before we go into these discussions we will start off with some limitations and strengths of the writing process.

6.3.1 Theory Research

The litterateur study phase was the first to be conducted for the thesis and therefore did not benefit from the added insight a second review phase such as the empiricism was given. Because of this it could be argued that the quality of this first research phase was missing the baseline which the empiricism had from this first phase, thus reducing its overall quality and structure. However, the litterateur study had the benefit of open source accessible literature which enabled a broad access to material. Because of this it could be argued it was the better suited one to be used for a first phase. Additionally the value of the thesis contribution arguably is the greatest in the empiricism. Because of this it could be argued that the overall result has become better by conducting the litterateur study first.
The next limitation of the litterateur study is that there appeared to be a lack of scientific contents discussing the problem area of the thesis. While the regular "conventional" IoT domain has been discussed broadly litterateur within the cellular domain seemed to be thin. In addition the carrier related discussion might be mixed in with the scientific papers where cellular is assumed to be "another carrier" rather than a domain. Because of this we probably have a mix of conventional IoT theory along with the specific cellular IoT theory that we were able to find.

The last limitation of the theory research is that the thesis most likely has missed relevant articles and scientific papers that would have been relevant for the thesis. The reasons for this could be many such as language barriers, search criteria and

availability of litterateur. Because of this the thesis might have ended up concluding with gaps mentioned by the empiricism that has already been documented in theory, but that we did not find. However, despite this risk we believe that the thesis overall has contributed to better understanding of the cyber security in the cellular IoT.

6.3.2 Empiric Research

The empiricism was the second research phase of the thesis. The phase was heavily relying on the authors ability to interact and communicate with the interview subjects. In difference to the theory phase where litterateur could have been translated prior to being published the interviews required face to face communication. This restricted the authors abilities to communicate to Scandinavian or English speaking subjects only. Further this limitation in the authors abilities could also have been tampered by the authors geographical location and availability of interview subjects. However, with interviews ranging both Europe and America this challenge has been overcome and something we see as a strength of the thesis.

The next factor we discuss is the results the empiricism has given. In 7 out of 8 interviews we only spoke to one person for each of the companies. This could lead to the answers being biased by the personal thoughts and beliefs within the cellular IoT domain and we might have ended up with other results if we had more than one subject from each company. However, the interview where there were two subjects interviewed at the same time we noticed that their answers were in line with each other. As this was the observation from that interview it could be argued that we would have seen similar results from the other interviews. Another fact that underlines this statement is that our subjects were equals to a certain degree being in the upper half of their careers and in high or professional positions of their companies.

The last factor related to the empiric research phase of the thesis is related to the validity of the results. In the previous section we already discussed the subjects. However, the interviews themselves were semi-structured and followed an interview template with four main topics. It could be argued that the reproducibility of a semi structured interview is hard to achieve with personal biases from both the subjects and interviewers being present. Additionally it could be argued that the anonymization of the subjects could make it even harder. However, by following the interview template with the mentioned one hour to discuss and a subject that could match the subject description it would likely result in similar answers. The semi-structured method and anonymization must however be seen as a limitation with the uncertainty it results in.

6.3.3 Thesis Results

In the thesis' chapter 1.2 it was claimed that there was no wholesome studies on what the threats, vulnerabilities and security measures were in the cellular IoT domain. It was further mentioned in a journal by Nokia that future work should look for feasible and scalable solutions.

The results from this thesis does not answer Nokia's proposal of looking into feasible and scalable solutions. However, we believe it has contributed to a better understanding of the threats, vulnerabilities and security measures of the cellular IoT domain. Because of this the thesis can be seen as an interpretation of the cyber security in cellular IoT domain and be used to further Nokia's proposed work. Arguably the work of mapping and identifying the domain is a very important task that needs to be done before being able to implement appropriate measures to match the traits of the domain and this thesis has done so through both the theoretic and empiric review.

Chapter 7

Conclusion and Future Work

7.1 Conclusion

The telecom networks were originally made for people and P2P type of communication. With the digitisation of our societies and the entry of IoT with M2M communication the cyber security picture has changed rapidly. However, the awareness of threats, vulnerabilities and security measures has not had the time to mature in these environments and this has lead to there being a gap between the knowledge found in theory and empiricism. Through this thesis we have conducted a theoretical review to map the current theoretical state of the art before continuing on with an empiric review in the real world. By seeking out private and public actors within the field of cellular IoT we have been able to identify gaps in the understanding of threats, vulnerabilities and security measures.

The threats were discussed in the theory under the generic perception that state actors were the greatest threat, followed by mid tier actors such as hacktivists and terrorists and lastly on the bottom we would find hackers and script kiddies. However, the empiricism pointed out the mid tier threat actors as the most dangerous ones, followed by state state actors as a second. This was stated because state actors would be less frequent than the mid tier actors and that the mid tier actors would have huge monetary motivations in the domain making them more frequent. The lower tier actors on the other hand were agreed upon by both the theory and empiricism being the least threatening.

The vulnerabilities were discussed under three categories; device, network and human factors. In terms of device vulnerabilities the theory and empiricism agreed to a certain degree. However, the empiricism unveiled gaps in terms of hardening and virtualisation as additional ones. The next was network related vulnerabilities. The theory was very focused on protocol vulnerabilities, while empiricism pointed out lack of monitoring and encryption as ones the theory did not mention. Last were the human related ones. The theory did not discuss these factors, but empiricism pointed out lack of knowledge, poor routines and excessive confidence

in the telecom operators as human related vulnerabilities.

The security measures were the last factors we looked in to. Equally to the vulnerabilities this topic was discussed under the same three categories; devices, network and human factors. On the device related security both the theory and empiricism pointed out IoT SIM Applet For Secure End-to-End Communication as a great technology for securing the end points. Other than this there were no other notes in this category. In the network related security mechanisms both the empiricism and theory agreed that there were many possibilities to tune the network for increased security. Additionally the empiricism argued that monitoring within the cellular networks were missing and that it would have great potential to detect anomaly. Lastly in the human related security there was a gap were only the empiricism discussed there to be missing certifications and legislation for cellular IoT and that it perhaps was the only way to ensure a common basis of security in the domain.

The theoretical part of the thesis has some weaknesses, but we find the interviews from the empiricism to be very interesting. In most cases we arguably can not draw any hard lines considering the gaps between the two, but we believe the thesis has made a contribution towards a better understanding of how cyber secuirty in cellular IoT is viewed by private and public actors working with the technology on a day to day basis. These results serves as an excellent starting point for further work.

7.2 Future Work

Based on the discussion in Chapter 6.3 this thesis has provided a better understanding of the cyber security in the cellular IoT domain. However, Nokia's proposal on finding feasible and scalable solutions was not met during this thesis. Therefore we suggest that further work should use the findings of this thesis as foundation to look for suitable and feasible solutions that are scalable for increasing the security of cellular IoT with regards to the threats and vulnerabilities presented in this very document. With the results from this thesis showing the importance of human related aspects of cyber security in the cellular IoT domain more effort should be focused on this topic.

Bibliography

[1] Telecommunications History Group, *Telecom history timeline*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.telcomhistory.org/resources/telecom-history-timeline.

[2] N. Ravi, R. Chitanvis and M. El-Sharkawy, 'Applications of drones using wireless sensor networks,' in *2019 IEEE National Aerospace and Electronics Conference (NAECON)*, [Accessed 06-Dec-2022], IEEE, 2019, pp. 513–518. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9057846.

[3] S. Li, M. Iqbal and N. Saxena, 'Future industry internet of things with zero-trust security,' *Information Systems Frontiers*, pp. 1–14, 2022, [Accessed 06-Dec-2022]. [Online]. Available: https://link.springer.com/article/10.1007/s10796-021-10199-5.

[4] R. P. Jover, 'Security and impact of the iot on lte mobile networks,' *Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations*, vol. 6, 2015, [Accessed 06-Dec-2022]. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a5cdc75067a4135b28f4e5ac7193eec32bc92ab1.

[5] T. Xie, G.-H. Tu, C.-Y. Li and C. Peng, 'How can iot services pose new security threats in operational cellular networks?' *IEEE Transactions on Mobile Computing*, vol. 20, no. 8, pp. 2592–2606, 2021, [Accessed 06-Dec-2022]. DOI: 10.1109/TMC.2020.2984192. [Online]. Available: https://ieeexplore.ieee.org/document/9055084.

[6] K. W. Lange, 'Cybersecurity in the internet of things,' [Accessed 06-Dec-2022], M.S. thesis, NTNU, 2016. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2406850/14698_FULLTEXT.pdf.

[7] E. Hamadaqa, S. Mulhem, W. Adi and M. Berekovic, 'Contemporary physical clone-resistant identity for iots and emerging technologies,' *Cryptography*, vol. 5, no. 4, p. 32, 2021, [Accessed 06-Dec-2022]. [Online]. Available: https://www.mdpi.com/2410-387X/5/4/32.

[8] A. Jerichow, B. Covell, D. Chandramouli, A. Rezaki, A. Lansisalmi and J. Merkel, '3gpp non-public network security,' *Journal of ICT Standardization*, pp. 57–76, Jan. 2020, [Accessed 06-Dec-2022]. [Online]. Available: https://journals.riverpublishers.com/index.php/JICTS/article/view/1267.

[9] National Institute of Standards and Technology, *Cyber threat - glossary | csrc.nist.gov*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_threat.

[10] E. G. Little and G. L. Rogova, 'An ontological analysis of threat and vulnerability,' pp. 1–8, 2006, [Accessed 06-Dec-2022]. DOI: 10.1109/ICIF.2006.301716. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/4086002.

[11] Canadian Centre for Cyber Security, *An introduction to the cyber threat environment*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

[12] M. Sailio, O.-M. Latvala and A. Szanto, 'Cyber threat actors for the factory of the future,' *Applied Sciences*, vol. 10, p. 4334, Jun. 2020, [Accessed 06-Dec-2022]. DOI: 10.3390/app10124334. [Online]. Available: https://www.researchgate.net/publication/342426828_Cyber_Threat_Actors_for_the_Factory_of_the_Future.

[13] National Institute of Standards and Technology, *Vulnerability - glossary*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://nvd.nist.gov/vuln.

[14] G. Strupczewski, *Defining cyber risk*, [Accessed 06-Dec-2022], 2021. DOI: https://doi.org/10.1016/j.ssci.2020.105143. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0925753520305397.

[15] J. Frankenfield, *Cybersecurity definition*, [Accessed 06-Dec-2022], Sep. 2022. [Online]. Available: https://www.investopedia.com/terms/c/cybersecurity.asp.

[16] Center for Internet Security, *Election security spotlight – cia triad — cisecurity.org*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.cisecurity.org/insights/spotlight/ei-isac-cybersecurity-spotlight-cia-triad.

[17] A. Gabbai, *Kevin ashton describes "the internet of things" — smithsonianmag.com*, [Accessed 06-Dec-2022], Jan. 2015. [Online]. Available: https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/.

[18] SmartBear, *Iot and it's impact on testing — smartbear.com*, [Accessed 06-Dec-2022], Aug. 2019. [Online]. Available: https://smartbear.com/blog/internet-of-things-101/.

[19] Cloud Credential Council, *Knowledge byte: The different types of iot*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.cloudcredential.org/blog/knowledge-byte-the-different-types-of-iot.

[20] Alliance for Internet of Things Innovation, *Identifiers in internet of things (iot)*, [Accessed 06-Dec-2022], Feb. 2018. [Online]. Available: https://euagenda.eu/upload/publications/identifiers-in-internet-of-things-iot.pdf.

[21] Attune, *The truth about iot implementations - wireless vs. wired*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://blog.attuneiot.com/2017/10/10/iot-implementations-wireless-vs-wired.

[22] Elsys, *Embedded electronics — elsys-design.com*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.elsys-design.com/en/embedded-electronics-engineer.

[23] M. A. Khelif, J. Lorandel, O. Romain, M. Regnery, D. Baheux and G. Barbu, *Toward a hardware man-in-the-middle attack on pcie bus for smart data replay*, [Accessed 06-Dec-2022], Aug. 2019. DOI: 10.1109/DSD.2019.00042. [Online]. Available: https://www.researchgate.net/publication/336726401_Toward_a_Hardware_Man-in-the-Middle_Attack_on_PCIe_Bus_for_Smart_Data_Replay.

[24] O. Garcia-Morchon, S. Kumar and M. Sethi, *Internet of Things (IoT) Security: State of the Art and Challenges*, [Accessed 06-Dec-2022], Apr. 2019. DOI: 10.17487/RFC8576. [Online]. Available: https://www.rfc-editor.org/info/rfc8576.

[25] L. Peterson and O. Sunay, *5g mobile networks: A systems approach*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://5g.systemsapproach.org/index.html.

[26] History Computer Staff, *4g: History, origin, and more*, [Accessed 06-Dec-2022], 2021. [Online]. Available: https://history-computer.com/4g-guide/.

[27] S. Dahmen-Lhuissier, *4th generation (lte)*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.etsi.org/technologies/mobile/4G.

[28] N. Chandler, *How 4g works*, [Accessed 06-Dec-2022], Feb. 2012. [Online]. Available: https://electronics.howstuffworks.com/4g.htm.

[29] GSMA, '5g security issues,' Nov. 2019, [Accessed 06-Dec-2022]. [Online]. Available: https://www.gsma.com/membership/wp-content/uploads/2019/11/5G-Research_A4.pdf.

[30] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong and J. C. Zhang, *What will 5g be?* [Accessed 06-Dec-2022], 2014. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6824752.

[31] M. Goss, *5g vs. 4g: Learn the key differences between them*, [Accessed 06-Dec-2022], Feb. 2021. [Online]. Available: https://www.techtarget.com/searchnetworking/feature/A-deep-dive-into-the-differences-between-4G-and-5G-networks.

[32] Ericsson, *5g for business*, [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.ericsson.com/en/5g/5g-for-business.

[33] S. Shea, *Lpwan (low-power wide area network)*, [Accessed 06-Dec-2022], Sep. 2017. [Online]. Available: https://www.techtarget.com/iotagenda/definition/LPWAN-low-power-wide-area-network.

[34] M. Rewers, *5g-iot-lpwan: What is the relationship?* [Accessed 06-Dec-2022], Jan. 2018. [Online]. Available: https://www.linkedin.com/pulse/5g-iot-lpwan-what-relationship-mark-rewers/.

[35] GSMA, *Long term evolution for machines: Lte-m*, [Accessed 06-Dec-2022]. [Online]. Available: https://www.gsma.com/iot/long-term-evolution-machine-type-communication-lte-mtc-cat-m1/.

[36] G. Vos, *With lte-m and nb-iot you're already on the path to 5g*, [Accessed 06-Dec-2022], May 2018. [Online]. Available: https://www.sierrawireless.com/iot-blog/lte-m-nb-iot-5g-networks/.

[37] GSMA, *Narrowband – internet of things (nb-iot)*, [Accessed 06-Dec-2022]. [Online]. Available: https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/.

[38] J. Dudovskiy, *Deductive approach (deductive reasoning)*, [Accessed 06-Dec-2022]. [Online]. Available: https://research-methodology.net/research-methodology/research-approach/deductive-approach-2/.

[39] W. Trochim and J. Donnelly, *The research methods knowledge base*, [Accessed 06-Dec-2022], 2006. [Online]. Available: https://books.google.no/books?id=097mAAAACAAJ.

[40] A. Aliyu, A. Abdu, R. Kasim, D. Martin, P. Raja, B. Pahat, D. Johor and M. Correspondence, 'Research framework development on the effect of intangible location attributes on the values of residential properties in jos, nigeria,' *Developing Country Studies*, vol. 5, Jan. 2015, [Accessed 06-Dec-2022]. [Online]. Available: https://www.researchgate.net/figure/Deductive-and-Inductive-Reasoning-Trochim-and-Donnelly-2006-Deductive-research-is-a_fig3_318982403.

[41] M. Lennartsson and E. Vanhatalo, 'Evaluation of possible six sigma implementation including a dmaic project,' Jan. 2004, [Accessed 06-Dec-2022]. [Online]. Available: https://www.researchgate.net/publication/228378894_Evaluation_of_possible_SIX_SIGMA_implementation_including_a_DMAIC_project.

[42] P. C. Kinjal Aacha, *Different types of literature review techniques followed in a research*, [Accessed 06-Dec-2022], Dec. 2021. [Online]. Available: https://www.projectguru.in/different-types-of-literature-review-techniques-followed-in-a-thesis-research/.

[43] Y. Xiao and M. Watson, *Guidance on conducting a systematic literature review*, [Accessed 06-Dec-2022], 2019. [Online]. Available: https://journals.sagepub.com/doi/full/10.1177/0739456X17723971.

[44] M. Noordzij, C. Zoccali, F. W. Dekker and K. J. Jager, *Adding up the evidence: Systematic reviews and meta-analyses*, [Accessed 06-Dec-2022], 2011. [Online]. Available: https://www.karger.com/Article/Abstract/328914.

[45] R. Streefkerk, *Qualitative vs. quantitative research | differences, examples methods*, [Accessed 06-Dec-2022], Apr. 2019. [Online]. Available: https://www.scribbr.com/methodology/qualitative-quantitative-research/.

[46] QuestionPro, *Empirical research: Definition, methods, types and examples*, [Accessed 06-Dec-2022. [Online]. Available: https://www.questionpro.com/blog/empirical-research.

[47] M. M. Hennink, B. N. Kaiser and V. C. Marconi, *Code saturation versus meaning saturation: How many interviews are enough?* [Accessed 06-Dec-2022, 2017. [Online]. Available: https://journals.sagepub.com/doi/full/10.1177/1049732316665344.

[48] M. Abomhara and G. M. Køien, *Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks*, [Accessed 06-Dec-2022], 2015. [Online]. Available: https://www.riverpublishers.com/journal_read_html_article.php?j=JCSM/4/1/4.

[49] S. Liebl, L. Lathrop, U. Raithel, M. Söllner and A. Assmuth, *Threat analysis of industrial internet of things devices*, [Accessed 06-Dec-2022], 2020. [Online]. Available: https://www.researchgate.net/publication/344943030.

[50] S. Tweneboah-Koduah, K. E. Skouby and R. Tadayoni, *Cyber security threats to iot applications and service domains*, [Accessed 06-Dec-2022], Jul. 2017. DOI: 10.1007/s11277-017-4434-6. [Online]. Available: https://link.springer.com/article/10.1007/s11277-017-4434-6.

[51] F. Winter and R. P. Jover, *Security and impact of the iot on lte mobile networks book: Security and privacy in the internet of things (iot): Models, algorithms, and implementations*, [Accessed 06-Dec-2022], 2015. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a5cdc75067a4135b28f4e5ac7193eec32bc92ab1.

[52] S. Wu, P. L. Yeoh, W. Hardjawana and B. Vucetic, 'Identifying security and privacy vulnerabilities in 4g lte and iot communications networks,' in *2021 IEEE 7th World Forum on Internet of Things (WF-IoT)*, [Accessed 06-Dec-2022], 2021, pp. 512–517. DOI: 10.1109/WF-IoT51360.2021.9595689. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9595689.

[53] A. Shaik, R. Borgaonkar, S. Park and J.-P. Seifert, 'New vulnerabilities in 4g and 5g cellular access network protocols: Exposing device capabilities,' WiSec '19, pp. 221–231, 2019, [Accessed 06-Dec-2022]. DOI: 10.1145/3317549.3319728. [Online]. Available: https://dl.acm.org/doi/abs/10.1145/3317549.3319728.

[54] C. Yu, S. Chen and Z. Cai, 'Lte phone number catcher: A practical attack against mobile privacy,' *Security and Communication Networks*, vol. 2019, 2019, [Accessed 06-Dec-2022]. [Online]. Available: https://www.hindawi.com/journals/scn/2019/7425235/.

[55] N. H. Yee, 'Performing a practical paging attack on the lte network,' 2017, [Accessed 06-Dec-2022]. [Online]. Available: https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1124&context=cscsp.

[56] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim and Y. Kim, 'Hiding in plain signal: Physical signal overshadowing attack on {lte},' pp. 55–72, 2019, [Accessed 06-Dec-2022]. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon.

[57] R. P. Jover and V. Marojevic, 'Security and protocol exploit analysis of the 5g specifications,' *IEEE Access*, vol. 7, pp. 24 956–24 963, 2019, [Accessed 06-Dec-2022]. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8641117.

[58] R. R. Stewart, M. Tüxen and karen Nielsen, *Stream control transmission protocol*, RFC 9260, [Accessed 06-Dec-2022], Jun. 2022. DOI: 10.17487/RFC9260. [Online]. Available: https://www.rfc-editor.org/info/rfc9260.

[59] GSMA, *Iot safe: Robust iot security at scale*, [Accessed 06-Dec-2022], Jun. 2021. [Online]. Available: https://www.gsma.com/iot/iot-safe/.

[60] W. Ding, H. Hu and L. Cheng, 'Iotsafe: Enforcing safety and security policy with real iot physical interaction discovery,' 2021, [Accessed 06-Dec-2022]. [Online]. Available: https://par.nsf.gov/servlets/purl/10285121.

[61] N. Seddigh, B. Nandy, R. Makkar and J. Beaumont, 'Security advances and challenges in 4g wireless networks,' pp. 62–71, 2010, [Accessed 06-Dec-2022]. DOI: 10.1109/PST.2010.5593244. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5593244.

[62] C. Romeika, *Everything you need to know about public and private apns*, [Accessed 06-Dec-2022], Sep. 2022. [Online]. Available: https://pangea-group.net/2022/09/01/everything-you-need-to-know-about-public-and-private-apns/.

[63] Motorola, *What is private lte?* [Accessed 06-Dec-2022], 2022. [Online]. Available: https://www.motorolasolutions.com/en_us/solutions/what-is-private-lte.html.

[64] GSMA, 'Securing the 5g era,' [Accessed 06-Dec-2022]. [Online]. Available: https://www.gsma.com/security/securing-the-5g-era/.

[65] J. Munilla, M. Burmester and R. Barco, 'An enhanced symmetric-key based 5g-aka protocol,' *Computer Networks*, vol. 198, p. 108 373, 2021, [Accessed 06-Dec-2022], ISSN: 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108373. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1389128621003546.

[66] Techplayon, *5g identifiers supi and suci*, [Accessed 06-Dec-2022], Nov. 2019. [Online]. Available: https://www.techplayon.com/5g-identifiers-supi-and-suci/.

Appendix A

Information Letter Interview

Information on the research project

Cyber Security in Cellular Internet of Things

In this information letter we give you information on the goals of the research project and what the project means for you.

Purpose of the project
Cyber Security in the Internet of Things is a topic that recently have been more and more discussed and the technology is growing exponentially in use. However, the topic is typically discussed in the context of regular IP-networks where the threat and vulnerability picture is better established than in the cellular domain. In additions the cellular networks evolve at a much higher pace with 4G on the edge of being replaced by 5G in a matter of years as where TCP/IP based networks have been operating the similarly for decades.

Through this research project we seek to enlighten the potential gaps between security features and possibilities against the threats and vulnerabilities present on the cellular networks. This will be done though a litterateur study on earlier scientific research before collecting real world input from different private and public actors that are faced with the cellular Internet of Things domain daily.

This survey is part of a master thesis intended to examine the experienced and perceived threats and vulnerabilities in the discussed domain. We intend to collect data from as many industries and sectors as possible in order to best cover the general picture.

For the thesis we have defined the main research question as follows: “What are the gaps between theoretical and empirical Cyber Security in Cellular IoT?” which we will seek to solve by answering the sub questions based on respectively 1. theory and 2. empirical.

1.1 What are the theoretical threats towards cellular IoT?

1.2 What are the theoretical vulnerabilities in cellular IoT?

1.3 What is the theoretical state of the art in cellular IoT security?

2.1 What are private and public actors perceived threats towards cellular IoT?

2.2 What are private and public actors perceived vulnerabilities in cellular IoT?

2.3 What security mechanisms are private and public actors missing in cellular IoT?

The goal of this interview is to answer research question 2.1, 2.2 and 2.3.

Institution responsible for the project
The department of Information Security and Communication Technology at NTNU is responsible for the project.

Why are you being asked to participate?
You are being interviewed as you have been appointed or found to be a fitting representative for your sector or industry as a talesman/woman on the cyber security related matters in cellular IoT. We assume you to be the only representative for your specific sector or industry, so we ask you to answer as accurately and precisely as possible to best understand the cellular cyber security domain for your business.

We also welcome you to forward questions within you organization if you feel someone is in a better position to answer certain topics than yourself.

What does participation involve for you?
This interview will ask questions regarding the use, security and threats towards cellular IoT. Meaning IoT devices connected to the cellular networks using SIM-cards subscribed to a telecommunication operators' network such as Telenor, AT&T, Vodafone, Orange, etc… By participating in the interview, you will help enlighten the gaps between theoretical and empirical cyber security in cellular IoT,

The interview will not collect any kind of personal data nor any company related data and you as an interview object will not be identified in any way. All data collected will be stored according to NTNU policies and will additionally be deleted once the thesis is completed. In addition will none other than we, the researcher and supervisor, have access to the answers provided in the interview.

Participation is voluntary and you may protest
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. As all participants are non-identifiable in the submitted data, we rely on your cooperation in identifying your submitted data. All your data will subsequently be deleted. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Your personal privacy – how we will store and use your personal data
We will only use your data for the intents and purposes stated in this information letter. We treat all data confidentially and in accordance with personal data legislature (GDPR, Norwegian Personal Data Act and The Act on ethics and integrity in research).

You will not be identifiable in the collected data or in the finalized thesis.

All data will be stored in accordance with NTNU privacy and security policies and other legislature. The raw data is to be deleted after the completion and submittance of the thesis. Additionally, only we, the researcher and supervisor, will have access to the submitted data.

What will happen to your personal data at the end of the research project?
The planned end date of the project is in December 2022. All submitted data will be deleted at the end of the project. The findings and correlations between the collection methods will however be accessible through the thesis.

Your rights

No participants will be identifiable in the collected data and finalized thesis. However, if you have concerns that you in fact are identifiable, you have the right to:

- protest,
- access your submitted personal data,
- correct personal data about you,
- delete personal data about you, and,
- submit a complaint to the Norwegian Data Protection Services regarding the processing of your personal data.

Yours sincerely,

Geir Olav Dyrkolbotn	*Henrik Hyndøy*
(Supervisor)	Researcher/student

Appendix B

Interview Questions

Interview Template
Cyber Security in Cellular IoT

GENERAL QUESTIONS

- What is your definition on an IoT devices? (Include key features)

- Approximately how many IoT devices does your company have?

- In percentage - how many of the devices are using cellular carriers?

- To what degree does your company's value chain rely on cellular IoT?
  1(Not at all) – 10(Business critical)

THREATS

- Who do you consider to be the biggest threat actor(s) towards your cellular IoT devices?

- What do you think would be their motivation for attacking your cellular IoT?

VULNERABILITIES

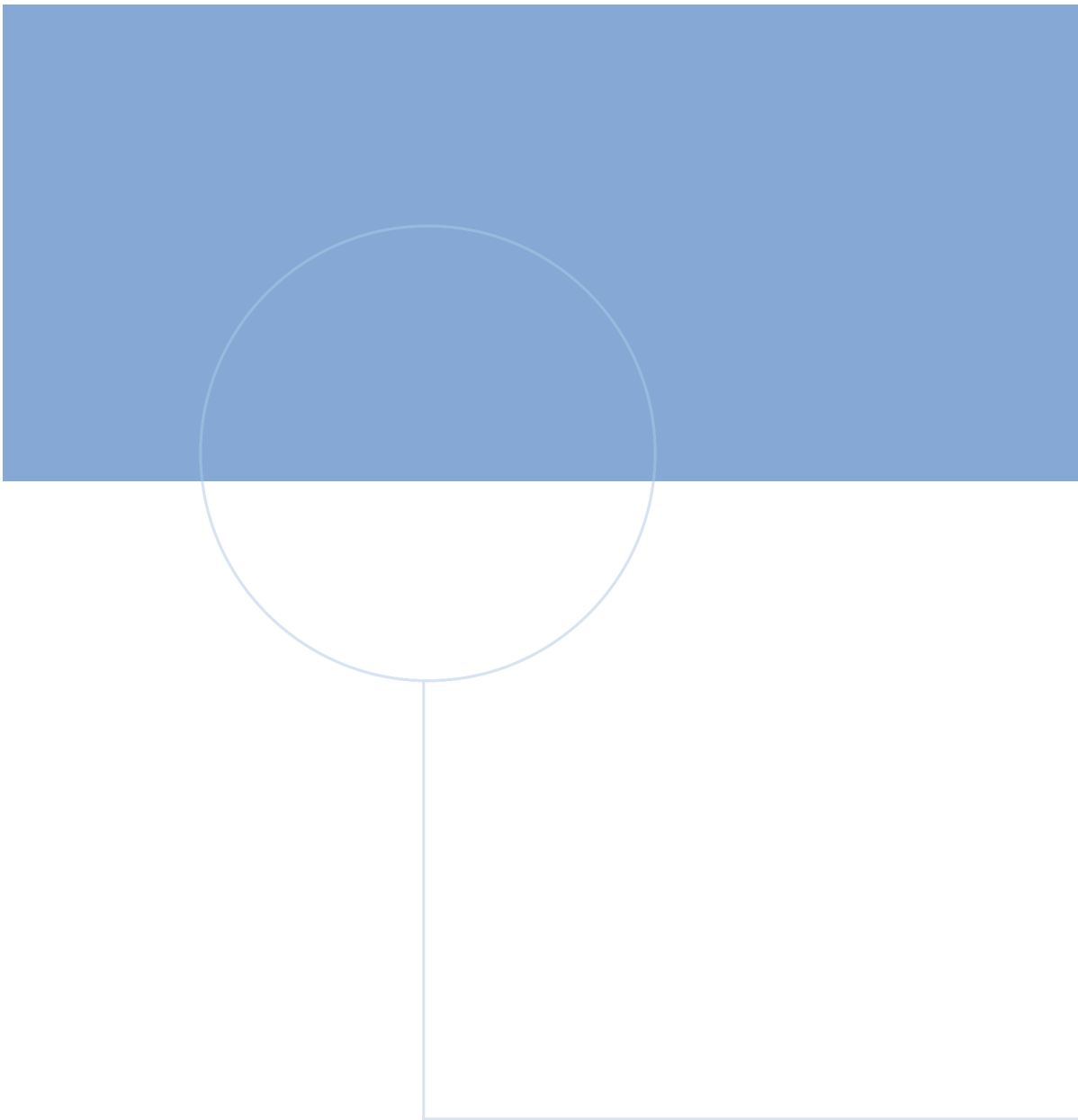
- What vulnerabilities are you concerned about in your cellular IoT devices?

- What kind of attack are you afraid could be launched?

SECURITY QUESTIONS

- What measures have been done to protect your cellular IoT?

- What are today's security mechanisms/technologies/functionalities missing?



NTNU

Kunnskap for en bedre verden