Master's thesis

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

Eivind Standal

# Mission critical services in commercial 5G networks

Master's thesis in communication technology
Supervisor: Eirik Larsen Følstad
Co-supervisor: Knut Baltzersen
June 2021

NTNU
Norwegian University of Science and Technology

Eivind Standal

# Mission critical services in commercial 5G networks

Master's thesis in communication technology
Supervisor: Eirik Larsen Følstad
Co-supervisor: Knut Baltzersen
June 2021

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

NTNU
Norwegian University of
Science and Technology

**Title:** Mission critical services in commercial 5G networks

**Student:** Eivind Standal

**Problem description:**

Current Public Safety Networks (PSNs), owned by the governments, are dedicated wireless communications networks deployed and operated for emergency service organisations like police, fire and health. In Europe, PSNs are typically based upon the TETRA standards developed and maintained by European Telecommunications Standards Institute (ETSI). The Norwegian Nødnett is an example of such a PSN. Current LTE networks and the coming 5G networks have increasing capabilities for providing lower latency, higher capacity/throughput, higher reliability and higher number of connected devices that enable a variety of services with very different requirements and needs. The LTE and 5G specifications are developed by the 3rd Generation Partnership Project (3GPP). These specifications, and still to be completed, define a number of functions and capabilities that are especially targeted for mission critical services like MCPTT, MCVIDEO and MCDATA.

There is an emerging development in to use LTE and 5G networks for mission critical services that cannot be provided with the current PSNs based on e.g. TETRA. Services like MCVIDEO and MCDATA cannot be provided with TETRA due to the limited throughput. While LTE will play an important part in facilitating broadband mission critical services, in order to limit the scope, the objective of the thesis is to explore the technical and operational challenges related to deploying mission critical services in coming 5G networks. This includes suggestions for which parts of the 5G core and service network the government should potentially own/operate and which parts that may be outsourced to the mobile network operators (MNOs) or service providers. In regards to this, the Norwegian Nødnett and the collaboration between the Norwegian government and Norwegian MNOs may be examined as a case study.

The project consists of the following tasks:

- Study background literature for TETRA and 5G for mission critical services.
- Identify arguments for the government to own/operate parts of the 5G core and service network.
- Propose which parts of the 5G core and service network such a need may apply to.

**Date approved:** 2021-02-08

**Supervisor:** Eirik Larsen Følstad, IIK

## Abstract

Together with the emergence of new 5G mobile networks there is a growing need among Public Safety Network (PSN) users for Mission Critical Services (MCX) that have greater bandwidth requirements than what traditional Terrestrial Trunked Radio (TETRA) based PSNs are capable of. As the Norwegian government, alongside several other governments around the world, have decided against the construction of dedicated broadband radio networks for PSN purposes, the next generation of public safety communications will have to be realized in collaboration with commercial Mobile Network Operators (MNOs).

This project examines the challenges related to the collaboration with commercial MNOs, taking a particular interest in the role of the state in this collaboration and the potential ways in which the state could be involved in the deployment model of a next generation PSN. The Norwegian situation of Next Generation Nødnett (NGN) is explored as a case study, and serves as a foundation on which to construct arguments in favor and opposition of various alternative deployment models for next generation PSNs. Deployment models of other countries, such as the UK, the US and Finland, are studied, and various stakeholders involved with NGN are interviewed, such as Norwegian MNOs, state actors and users of the existing TETRA-based Nødnett.

Criteria for comparison of deployment models against each other are defined and subsequently employed as a tool for weighing the strengths and weaknesses of various alternative deployment models for next generation PSNs. Based on findings from related literature, studies made of other countries' solutions, and considerations made by interview subjects, a recommendation is made regarding the deployment model of NGN. This recommendation involves the establishment of a state-owned and operated Mobile Virtual Network Operator (MVNO), and describes the ways in which we believe that this could potentially result in the strongest overall solution for NGN.

## Sammendrag

Sammen med fremveksten av nye 5G-baserte mobilnett er det et økende behov blant brukere av nødnett for oppdragskritiske tjenester (MCX) som krever større båndbredde enn det tradisjonelle Terrestrial Trunked Radio (TETRA) baserte nødnett er i stand til å levere i dag. Ettersom norske myndigheter, på lik linje med andre myndigheter rundt omkring i verden, har bestemt at det ikke skal bygges dedikerte bredbåndsnett i nødnettsammenheng, så vil neste generasjon av kommunikasjonssystemer for nødetater være nødt til å bli realisert i samarbeid med kommersielle mobile nettverksoperatører (MNOer).

Dette prosjektet undersøker utfordringene relatert til samarbeidet med kommersielle MNOer, med spesiell interesse for statens rolle i dette samarbeidet og de mulige måtene staten kan involveres i en modell for neste generasjons nødnett. Den norske situasjonen med Neste Generasjons Nødnett (NGN) blir utforsket som et casestudie, og fungerer som et fundament for konstruksjonen av argumenter for og imot ulike alternative modeller for neste generasjons nødnett generelt. Andre lands modeller, som Storbritannias, USAs og Finlands, blir studert, og ulike interessenter involvert i NGN blir intervjuet, som norske operatører, statlige aktører og brukere av Nødnett, det eksisterende TETRA-baserte nødnettet i Norge.

Kriterier for sammenligning av modeller opp mot hverandre blir definerte, og blir deretter brukt som et verktøy for å veie styrker og svakheter ved ulike alternative modeller for neste generasjons nødnett. En anbefaling blir gjort angående modellen for hvordan NGN bør implementeres basert på funn fra relatert litteratur, studier gjort av andre lands løsninger og intervjuobjekters vurderinger. Denne anbefalingen involverer opprettelsen av en statlig eid og driftet virtuell mobil nettverksoperatør (MVNO), og beskriver hvordan vi ser for oss at denne modellen potensielt kan resultere i den sterkeste overordnede løsningen for NGN.

# Preface

This thesis is submitted to the Norwegian University of Science and Technology (NTNU) and concludes my Master of Science (MSc) in Communication Technology at the Department of Information Security and Communication Technology (IIK). The research was carried out between January and June of 2021.

Much of the work being done in relation to this thesis, especially regarding interviews, has been done in cooperation with my friend and co-student, Lina Hexeberg Hovden, who has been working on her own thesis titled "Autonomous operation of mission critical base stations in 5G." While we are each writing our own separate theses, the related nature of the two works and the fact that they share a supervisor has allowed us to work together in the preparation for and conduction of interviews. I would like to thank Lina for her excellent contributions to our united effort, as well as for her encouraging spirit which has kept me going throughout the semester.

Furthermore I would like to thank the interview subjects who participated in this project and who provided valuable insights into the exciting world of broadband public safety communications. Without their contributions this project would not have been possible to carry out.

I would also like to thank my two supervisors, Eirik Larsen Følstad and Knut Baltzersen, who guided me through the process of writing this thesis and who helped recruit relevant interview subjects to participate in the project. Throughout the course of the project they provided detailed feedback and thoughtful considerations on the work that had been done that helped shape this thesis into what it is today, and for that I am grateful.

Lastly I would like to thank my mother, Sylvi Høiland, who helped proofread parts of this thesis, and who, more importantly, made considerable efforts to lift my spirits after I had expressed concerns of not being able to see the light at the end of this academic tunnel.

*Eivind Standal*
*Trondheim, June 2021*

I met a traveller from an antique land
Who said: Two vast and trunkless legs of stone
Stand in the desert. Near them, on the sand,
Half sunk, a shattered visage lies, whose frown,
And wrinkled lip, and sneer of cold command,
Tell that its sculptor well those passions read
Which yet survive, stamped on these lifeless things,
The hand that mocked them and the heart that fed:
And on the pedestal these words appear:
"My name is Ozymandias, king of kings:
Look on my works, ye Mighty, and despair!"
Nothing beside remains. Round the decay
Of that colossal wreck, boundless and bare
The lone and level sands stretch far away.

— Percy Bysshe Shelley, Ozymandias

# Contents

# List of Figures

# List of Tables

# List of Acronyms

**3GPP** 3rd Generation Partnership Project.

**AF** Application Function.

**AGA** Air-Ground-Air.

**AMF** Access and Mobility Management Function.

**AUSF** Authentication Server Function.

**CESC** Cloud-Enabled Small Cell.

**DMO** Direct Mode Operation.

**DN** Data Network.

**DSB** Norwegian Directorate for Civil Protection.

**eMBB** Enhanced Mobile Broadband.

**ESN** Emergency Services Network.

**ETSI** European Telecommunications Standards Institute.

**LST** Local Site Trunking.

**MCData** Mission Critical Data.

**MCPTT** Mission Critical Push-to-Talk.

**MCVideo** Mission Critical Video.

**MCX** Mission Critical X.

**MEC** Multi-Access Edge Computing.

**mMTC** Massive Machine-Type Communications.

**MNO** Mobile Network Operator.

**MOCN** Multi-Operator Core Network.

**MSB** Swedish Civil Contingency Agency.

**MVNO** Mobile Virtual Network Operator.

**NAO** National Audit Office.

**NEF** Network Exposure Function.

**NFV** Network Function Virtualization.

**NGN** Next Generation Nødnett.

**Nkom** Norwegian Communications Authority.

**NRF** Network Repository Function.

**NS** Network Slicing.

**NSSAAF** Network Slice-Specific Authentication and Authorization Function.

**NSSF** Network Slice Selection Function.

**P25** Project 25.

**PCF** Policy Control Function.

**PLMN** Public Land Mobile Network.

**PMR** Professional Mobile Radio.

**ProSe** Proximity Services.

**PSN** Public Safety Network.

**PTT** Push-to-Talk.

**QoS** Quality of Service.

**RAN** Radio Access Network.

**SA** Standalone.

**SBA** Service-Based Architecture.

**SCP** Service Communication Proxy.

**SDN** Software-Defined Networking.

**SMF** Session Management Function.

**TETRA** Terrestrial Trunked Radio.

**UDM** Unified Data Management.

**UE** User Equipment.

**UPF** User Plane Function.

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

**VNF** Virtual Network Function.

# Chapter 1
# Introduction

Of all the narrow subcategories of critical infrastructure a nation possesses, public safety communications may be one of the most important. The ability of an ambulance worker to communicate and coordinate efficiently with fellow first responders at the site of an emergency, or the ability of a police officer to call for backup in the heat of the moment is difficult to put a price on. As the telecommunications infrastructure that currently supports these lifesaving capabilities gets more and more dated, governments and public safety agencies throughout the world look upon the future with bright eyes as the next era of public safety communications is being ushered in. This thesis examines some of the challenges that governing authorities and network operators will have to overcome in order to realize the next generation of public safety communications, and considers the benefits and drawbacks of several alternative ways the Norwegian government, in particular, could choose to approach the task at hand.

## 1.1 Public safety networks

The facilitation of reliable electronic communications between first responders out in the field, as well as between first responders and control rooms, depend on the existence of a highly available, robust, and secure mobile communications system. Such a system needs to be able to provide extensive coverage, including in remote areas where regular cellular networks may not have coverage. Public safety actors may, for instance, be required to conduct search and rescue operations in such areas, and depend on mobile communications to carry out their mandate in an efficient manner. Additionally, the system needs to be able to withstand extraordinary circumstances that would cause outages in a regular cellular network, such as infrastructure-ruining landslides and extreme weather conditions. Situations like these are prime examples of situations in which the services of public safety actors are needed the most, and as such the mobile communications system is also needed. Lastly, the system needs to be able to provide public safety actors with secure communications channels that

can not, for instance, be listened in on by unauthorized entities, as information exchanged between public safety actors could be sensitive in nature.

It has been common for nations to provide their public safety agencies with public safety communications services on a dedicated cellular network called a Public Safety Network (PSN), separate from commercial network infrastructure. The main reason for this is that there did not exist any alternatives for implementing the types of services public agencies relied on in commercial networks when these networks were planned and established. As such, in order to continue the tradition of Push-to-Talk (PTT) type voice communications, which were previously typically provided as analog radio solutions, governments needed to construct their own networks based on technological standards that supported these types of public safety relevant communications services. However, having a dedicated network for public safety communications provides the added benefit of separating your critical traffic from the commercial traffic of regular cellular network consumers. This means that first responders will, for instance, not have to compete for network resources with civilian bystanders when trying to communicate with each other at the scene of an accident, and that governments have been free to strengthen the infrastructure of their dedicated network without having to take commercial telecom considerations into account. Most commonly these networks are narrowband solutions designed to offer highly reliable and secure communications services such as PTT voice communications and low bandwidth data applications, like simple messaging. In Europe, as well as in Asia, Latin America, and the Middle East, Terrestrial Trunked Radio (TETRA) has been the favored standard for constructing PSNs. Australia, New Zealand, and North America, however, have to a large extent made use of the closely related standard by the name of Project 25 (P25) [Yar20].

## 1.2 Nødnett and TETRA

The PSN of Norway is called Nødnett. It is governed by the Norwegian Directorate for Civil Protection (DSB), and is based on the TETRA standard. As such, TETRA will be the considered technology when discussing the current generation of PSNs, although much of that which is said about TETRA could probably also be said about its American cousin, P25. After some years of planning and decision-making, the construction of the Nødnett TETRA network finally began in 2006 and lasted approximately ten years, with a slight hiatus midway through [SHM21]. Today the network constitutes around 2075 dedicated base stations, as well as a dedicated core network [DSB20]. As a connotation of being a dedicated network, this infrastructure is entirely separated from the commercial mobile networks of Norway apart from fiber lines in parts of the backhaul which are leased from commercial operators. In terms of where the communications services are available, the radio network covers close to 100% of the Norwegian population and around 86% of Norway's geographical

mainland. Additionally, in order to ensure the availability of the service during times of distress, base stations are provided with emergency power supplies able to keep some base stations online for a minimum of 8 hours, and some up to 20 or even 48 hours, after experiencing a total blackout [DSB20]. Another measure taken to improve the robustness of Nødnett is that base stations are connected to the transport network in rings, with up to nine base stations per ring, effectively providing two transmission lines to all base stations. Both of the aforementioned robustness measures are things that could be of great help to public safety actors in the all too familiar scenarios of harsh weather conditions tearing down power lines or landslides disrupting fiber lines.

TETRA is a standard for Professional Mobile Radio (PMR) developed by the European Telecommunications Standards Institute (ETSI) [ETS20]. It is intended for PMR users such as public safety agencies, and emphasizes high reliability and availability of communications. A key feature of an PMR technology, like TETRA, is the ability to perform rapid call setup of PTT group conversations, in order to, for instance, let a control room operator give instructions to a police unit over a secure communications channel. PTT implies that only one person in the talk group is able to speak at a time, and must hold down a button on their device to do so. Usually this means that one has to wait for one's turn in order to be allowed to speak in the talk group. However, users with a higher priority are able to preempt an ongoing conversation in order to deliver important information. Other features of TETRA include the ability for terminals to communicate directly with other terminals in range of them through Direct Mode Operation (DMO) in the event that connection to the network is lost, as well as the ability for base stations to act in what is called Local Site Trunking (LST) mode. This mode enables a base station that has lost connection to the backhaul to still connect terminals in range of that disconnected base station to each other [KPMP16].

While Nødnett has proven itself to be robust and is performing well in terms of PTT voice communications and simple messaging services, the TETRA based technology has severe limitations when it comes to more bandwidth intensive communications services. In [DSB20], DSB presents the data transmission rate of Nødnett as being between 3 kbit/s and 12 kbit/s. This is far from sufficient if you would like to provide communications services that make use of real-time video, imagery, or even simple file transfers. As these types of bandwidth intensive services are becoming exceedingly more in demand among public safety actors, governments around the world are coming to the conclusion that it is soon time to abandon narrowband PSNs in favor of solutions based on broadband cellular network technologies such as 4G LTE and, eventually, 5G. To add to this, the contract between DSB and

Nødnett's current operator, Motorola Solutions,[1] is set to run out at the end of 2026, leaving Nødnett at a potential crossroads [DSB20]. As such, the Norwegian government could either attempt to negotiate a new contract for the maintenance and operation of the TETRA network, or choose to abandon it in favor of a new broadband PSN solution. While the hope seems to be that a broadband solution will be able to be deployed before the aforementioned contract runs out, there is still a significant amount of work yet to be done before one could even think to start deploying such a solution nationwide. To mention just some of the ongoing work, standardization organizations like the 3rd Generation Partnership Project (3GPP) and ETSI are doing significant work in relation to the standardization of public safety related communications services in 4G LTE and 5G. Additionally, DSB are conducting extensive inquiries into alternative deployment models for what is being called Next Generation Nødnett (NGN), which will have to be implemented in cooperation with the commercial Mobile Network Operators (MNOs) in Norway [DSB18].

## 1.3 An introduction to 5G

5G is the fifth generation of mobile cellular networks as defined by 3GPP. In comparison to its predecessor, 4G LTE, 5G will improve on a number of fundamental aspects of mobile communications networks, such as bandwidth, latency, reliability, coverage, and battery efficiency, to mention some. In fact, the improvements made in 5G look so promising that some researchers are favoring the term "revolutionary leap" to the more modest "incremental improvement" when describing the transition from 4G LTE to 5G [SMS+17]. Combined with the extensive application of technologies like Network Function Virtualization (NFV) and Software-Defined Networking (SDN), which will facilitate the construction of an entirely new kind of network infrastructure, providing unprecedented flexibility, one might be able to start imagining how 5G will redefine the ways in which we consider mobile communications.

It is envisioned that 5G will support a wide variety of use cases, which are commonly sorted into three broader categories: Enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (mMTC), and Ultra-Reliable Low Latency Communications (URLLC) [SMS+17]. eMBB is perhaps the most familiar, as it is similar to the mobile broadband we know from 4G LTE. The difference being that data rates in 5G will in many cases be significantly improved compared to 4G LTE. In addition to higher throughput, one also expects to be able to provide a generally improved user experience in the form of, for instance, seamless mobility management, a high degree of coverage, and capacity to serve areas of extreme user density. The second category, mMTC, deals with use cases related to the

[1] Although Nødnett is entirely owned by the Norwegian state, the operation of the network has been outsourced to the commercial provider Motorola Solutions.

myriad of IoT sensors that is expected to permeate every aspect of infrastructure and everyday life in the future. While this category contains a wide variety of use case subcategories, and while many of these subcategories have yet to be properly defined, the expectation is for the network to be able to handle a tremendous amount of concurrently connected devices that each transmit a relatively low volume of traffic. For the third and last category, URLLC, the name itself implies that this is a category for use cases with strict requirements for reliability and latency, as well as availability. This category encompasses usage scenarios related to for instance tactile internet applications, such as remote surgery, and intelligent transport system applications, such as traffic control of autonomous vehicles. This last category is where it would be most natural to place public safety communications, although, while reliability is the first priority with low latency perhaps being the second, parts of the two other previously mentioned categories will also be relevant for next generation PSNs. One could for instance envision mission critical applications that make use of augmented or virtual reality, requiring high bandwidth in addition to low latency, or a number of IoT type applications where different types of sensors placed strategically throughout communities could provide information helpful to public safety actors.

Two key technologies of 5G networks are the previously mentioned SDN and NFV. While these two concepts are not new, 5G will make use of them as core building blocks in a way that has not been done in previous generations of mobile networks. In combination they make for a highly flexible and resilient network, with the core network functionality running as Virtual Network Functions (VNFs) on general purpose hardware in data centers, instead of on specialized hardware. By separating the user plane and control plane functions, SDN allows a centralized control plane entity to dictate the routing of packets throughout the network. This centralized entity is able to keep track of information regarding aspects of network provision such as policies and subscribers and update the network topology in response to constantly changing circumstances, thereby simplifying the process of managing large networks providing a multitude of services [SMS+17]. In [3GP20b], the 3GPP state that the network functions in the 5G system architecture shall make use of service-based interactions to communicate amongst themselves, giving rise to the concept of a Service-Based Architecture (SBA). An illustration of this SBA in a non-roaming scenario can be seen in Figure 1.1. Simply put, non-roaming means that the User Equipment (UE) is connected to its home core network through its home Radio Access Network (RAN), and is typically the least complicated scenario to model. The lowest level of the figure depicts the user plane consisting of the UE, the RAN, the User Plane Function (UPF) and the Data Network (DN). Above the user plane the figure shows the service-based control plane, containing network functions like the Access and Mobility Management Function (AMF), the Session Management Function (SMF), the Authentication Server Function (AUSF), the Unified Data Management (UDM), the Network Exposure Function (NEF), the

Network Repository Function (NRF), the Policy Control Function (PCF), and the Application Function (AF). In addition a Service Communication Proxy (SCP) is shown, which can be used for indirect communication between network functions if deployed.

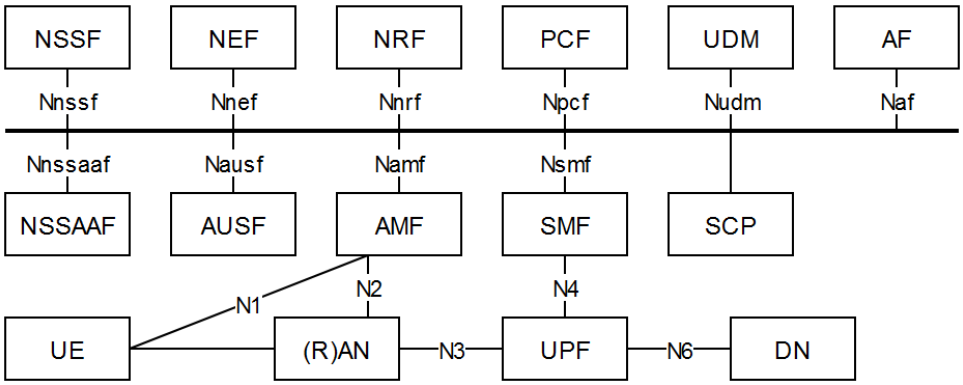


**Figure 1.1:** 5G SBA in a non-roaming scenario adapted from [3GP20b]

In addition to the already mentioned functions, the Network Slice Selection Function (NSSF) and Network Slice-Specific Authentication and Authorization Function (NSSAAF) can be seen at the top left of Figure 1.1. Network slicing, or just slicing for short, is a concept of dividing shared physical infrastructure between multiple network slices that are logically isolated from each other [BAMH20]. If we are to implement the next generation of PSNs in commercial networks, then the type of traffic isolation that a technology like network slicing can provide could become essential. In addition to providing traffic isolation, adjacent network slices have the ability to be configured to provide different types of services to different types of subscribers, all with different Quality of Service (QoS) requirements. Examples of this are the three previously mentioned categories of use cases, which require significantly different QoS guarantees based on the type of service being provided. For instance, in a scenario where both eMBB and mMTC services are needed, separate network slices could be created for each of the different types of use case. This makes it simpler for network operators to ensure that the eMBB services meet their requirements for bandwidth and such, while also ensuring that the mMTC services are capable of handling a huge number of concurrently connected devices. In a similar vein, network slicing allows operators to tailor slices to communications that fall under the category of URLLC, and subsequently separate these services from their more lenient counterparts in the eMBB and mMTC categories. With the help of Network Slicing (NS), operators would be able to prioritize URLLC traffic, and make sure that strict requirements for reliability and latency are met for these critical communications

services, without imposing the same demanding QoS requirements on other types of services that do not need them. As an example, a URLLC dependent application might require the help of Multi-Access Edge Computing (MEC) in order to reach a satisfactory level of latency. In order to achieve this a network operator could then create a specific network slice that makes use of network infrastructure located at the edge of the network, so that traffic related to that URLLC dependant application would not have to travel all the way into a centralized core network with the added latency that would incur. Similarly, eMBB slices would be programmed to not make use of that edge infrastructure in order to not congest the system, as the capacity in the edge would most likely be severely limited compared to the capacity in the centralized core network. Facilitated by the adoption of SDN and NFV, network slicing is a central concept of 5G which will play an important part in providing both businesses and governments alike with highly reliable low latency communications services [BAMH20].

An interesting point to note in Figure 1.1 is the difference in naming convention between the communications interfaces connecting components in the upper part of the figure as opposed to the lower part. While the signalling between the components in the lower part resemble the traditional type of signalling one is used to from earlier iterations of this kind of network architecture, the signalling in the upper part, the part which, as mentioned previously, now lives on generalized hardware in data centers, is actually more akin to HTTP API calls than what it is to previously employed signalling protocols like SIGTRAN and Diameter [Sch18]. The thick horizontal line through the upper part of the figure which connect the interfaces of the VNFs is meant to illustrate a signalling bus which they all use to communicate with each other. Now, while this is indeed an interesting note and a good example of how 5G is reshaping the network architecture mindset, these interfaces will not be explored further in this thesis. What will, however, be explored further are some of the VNFs. The AMF, which is responsible for mobility and such, the UDM, which contains subscriber information, will, for instance, be examined in particular in relation to alternative deployment models for NGN, as they both deal with important aspects of the network that the state could have interest in controlling themselves, and not outsource to a commercial provider.

As an illustration, Figure 1.2 attempts to show how concepts in 5G build on each other by abstracting the ecosystem into layers. At the top you have the all-encompassing 5G term, under which the various subjects discussed in this section fall. On the layer second from the top you have virtual networks designed to accommodate a variety of different use cases, as imagined previously when describing the possibilities that technologies such as slicing allows for. You could for instance have a virtual network designed with autonomous vehicles in mind next to a public safety one for first responders and a general purpose one for regular cellular network consumers. Thereafter you have the layer containing the enabling technologies themselves, several of which have been mentioned as central to the promised functionality of 5G, such as NFV, SDN, and slicing. And then, lastly, at the bottom of the stack you have the physical substrate on which all of the aforementioned concepts live and breathe. As a whole, this stack encompasses what we consider to be 5G.

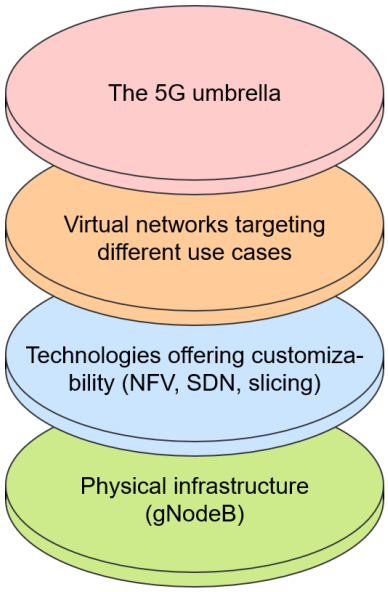


**Figure 1.2:** Abstracted layers of 5G adapted from [HLS+18]

## 1.4 Mission critical services

Mission critical services could perhaps be considered to be yet another synonym for public safety communications. A common denominator used to describe communications services employed by organizations that provide critical societal functions or that own and operate critical infrastructure, like for instance the police, fire and rescue services, emergency health services, power grid operators, and so on. In this thesis, however, the term mission critical services refers to the 3GPP definition of three specific types of mission critical communications services contained under the umbrella term Mission Critical X (MCX), in which the X stands for either PTT, Video, or Data. Mission Critical Push-to-Talk (MCPTT) encompasses PTT voice communications, while Mission Critical Video (MCVideo) facilitates real-time video communications, and Mission Critical Data (MCData) deals with other types of data transfer services such as file distribution and various forms of messaging. Despite these three types of MCX services describing different forms of communication, they share a number of requirements pertaining to their mission critical nature [3GP20a]. As the users of MCX services depend on reliable and available communications ser-

vices to perform their duties, and considering the fact that those duties in many cases involve the saving of lives, strict QoS requirements are needed to ensure the delivery of critical information in a secure and efficient manner. The technical specifications and requirements for MCX services are developed by the 3GPP, which is a constellation of telecommunications standard development organizations that provides technical specifications and requirements for a wide variety of telecom related technologies.

### 1.4.1 Mission critical push-to-talk

MCPTT as defined by the 3GPP specifies PTT voice communications between two or more users, where each user can request permission to talk by, for instance, pressing a button on a handheld device [3GP19]. In addition to describing the primary use case of group conversations, the specification also describes related topics such as the possibility for conducting one-to-one conversations, as well as how MCPTT should function in relation to 3GPP defined Proximity Services (ProSe) to provide direct communication between terminals in the event that the cellular network should become unreachable. A state diagram showing a simplified scenario of a user interacting with the MCPTT service can be seen in Figure 1.3. The figure shows how a user can select an MCPTT talk group from a number of groups the user has access to, and how the user may then receive and transmit in the selected group.

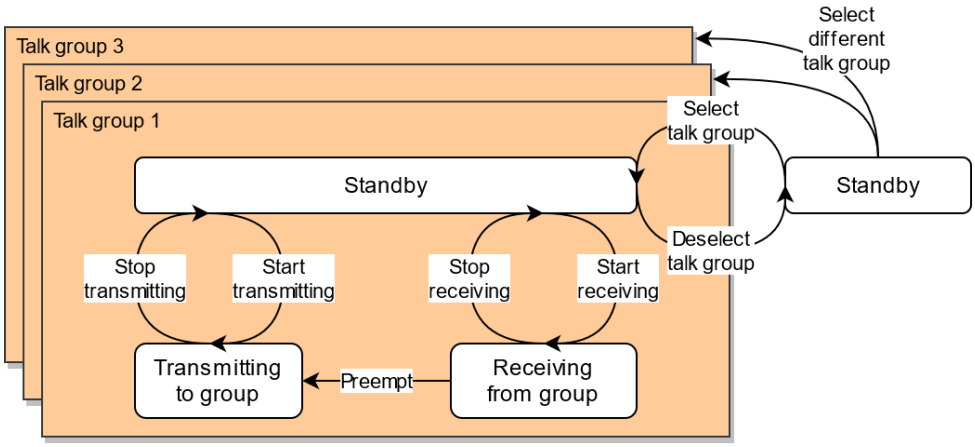


**Figure 1.3:** Simplified MCPTT state diagram adapted from [3GP19]

To start transmitting in a group a user will have to request permission from the system by, for instance, pushing a button on their device. Once the system decides that it is that users time to transmit, usually once the previous speaker has ended their transmission and the medium is free, the user is allowed to speak to the rest of the group. With that said, a user of a higher priority class than the

current speaker has the ability to interrupt an ongoing transmission in order to deliver their own message. This is what is known as priority preemption and it is illustrated by the state transition in Figure 1.3 going straight from the receiving state to the transmitting state. Priority preemption is an important concept in PTT communications, due to the fact that only one talk group member may speak at a time. This means that there will exist times when someone like a squad leader, who possesses a higher level of priority than regular users in their talk group, has a need to interrupt a transmission in progress in order to transmit an important message regarding, for instance, changing circumstances of an ongoing operation [3GP19].

### 1.4.2 Mission critical video and data

The MCVideo service provides public safety actors with the ability to communicate through live video feeds, such as broadcasting content from body cameras or surveillance cameras to the equivalent of a talk group. In addition, 3GPP describe related functionality such as video capture, annotation, and processing as part of the MCVideo specification [3GP18b]. The design philosophy behind MCVideo is in many ways very similar to MCPTT, for instance in how they both put emphasis on group communications and a user's ability to join and switch between available groups. However, when it comes to something like simultaneous broadcasting, it may not be as disruptive to the flow of communication for multiple users to transmit their respective video feeds at the same time as it would be to have several users speaking at the same time. This is due to the fact that a recipient of multiple concurrent video feeds, such as a control room, could, for instance, display several video feeds side by side and relatively easily discern which is most worthy of their attention at any given time. As such, the request and preemption mechanisms deciding who gets to transmit in a group can be configured to be more lenient, should user equipment and bandwidth capacities allow for multiple video feeds to be transmitted simultaneously from within a group.

While the recording and live streaming of video falls under the jurisdiction of MCVideo, the transmission of the video file after the fact is the concern of the MCData service. In contrast to MCVideo and MCPTT, MCData provides a set of features meant to cover a more general range of use cases related to data transfer [3GP18a]. Such use cases could for instance be an operational command center sharing an image or video file with a police squad in pursuit of a criminal, or an ambulance worker making a database enquiry to determine whether or not a patient is suffering from any preexisting conditions when administering medical aid in the field. Additionally, mission critical messaging applications are another of the many imagined applications also covered under MCData. According to the specification, the intention behind the MCData service is to provide open interfaces on which a variety of multimedia applications can be built to serve user organizations with

everything from simple messaging services to internet access and remote control of robots.

Together with MCPTT, MCVideo and MCData form the trinity of MCX services. However, there is a key difference between the more traditional PTT functionality and the new video and data services. Namely, that while PTT services already are deployed in TETRA based PSNs around the world today, the additional bandwidth required to transfer high quality video and data means that these two newer types of services ultimately depend on the realization of MCX in broadband cellular networks such as 4G LTE and 5G. As mentioned previously, this need for higher bandwidth is a primary reason governments and public safety agencies throughout the world are currently looking to leave their TETRA networks and transition to broadband MCX solutions.

## 1.5 Research questions

In relation to the development of the next generation of PSNs, and with particular interest in the Norwegian situation, the following research questions have been proposed for this project.

**RQ1** What are the alternative deployment models for MCX in 5G, and what are the drawbacks and benefits of each one?

**RQ2** What challenges does the state face related to cooperating with commercial MNOs in providing broadband MCX solutions, and how can these challenges best be solved?

The intention behind these research questions is to provide an overview of the different possibilities countries have to choose from when charting a course for the establishment of broadband public safety communications solutions. While the ambition could be considered to be quite broad, the scope is restricted by limiting the project to looking at the technical challenges, as well as by focusing primarily on Norway. In addition to this, and in keeping with the tasks given in the problem description to this thesis, there is also a particular interest taken in challenges faced by the state and how the state should solve the questions of ownership and operation of next generation PSNs in cooperation with commercial actors. The primary research method chosen as a means to attain answers to the aforementioned questions is that of the interview, which will be covered in greater detail in Chapter 3.

## 1.6 Scope

It is difficult to avoid the fact that the decision for how to move forward with the development and deployment of the next generation of Nødnett in Norway is political in nature, and that the final decision rests with the Norwegian parliament. Similarly, it is also difficult to ignore the fact that a significant guiding factor for this decision are the economic ramifications of the different alternatives. Despite both of these facts, however, this project will attempt to focus solely on the technical challenges related to deploying MCX in commercial 5G networks with Norway as a leading case study, and will not consider either the political or economical consequences of such a deployment to any significant degree. With that said, and without trying to delve into the economics or politics of it, it may in some circumstances be considered relevant to examine potential consequences a choice of deployment model could have on the competitive aspects of the Norwegian mobile market. The greater concern in regards to this is that an NGN contract awarded to an operator could prove so valuable to that operator that they would gain a significant advantage over their competitors in terms of attracting other customers, and thereby disrupt the entire Norwegian telecom market. While this is obviously bad enough in and of itself, it would not be difficult to imagine that such a disruption to competition could then also negatively impact the diversity and quality of technical solutions available to NGN.

In addition to narrowing the scope in regards to economic and political perspectives, the project will also mostly refrain from discussing deployment of MCX in 4G LTE, as well as challenges related to the period of transition from the current TETRA network to the new broadband solution. Instead, the focus will be on painting a detailed picture of how MCX could and should be deployed in 5G networks in the future, with the requirements and considerations of the Norwegian situation in mind, as a contribution to the ongoing development of the next generation of PSNs. While it seems unrealistic that 5G Standalone (SA) will be fully deployed by 2026, the utilization of a next generation core network will be important to gain the full benefit of technologies such as SDN, NFV, and, by extension, NS [SMS+17]. For this reason, the majority of the considerations made in regards to solving challenges related to the realization of proper PSN functionality in 5G networks will be made with a standalone 5G core network in mind. However, as Yarali points out in [Yar20], there is little reason to wait for a standalone 5G network before deploying broadband PSN solutions, as 4G LTE can provide much of the same functionality, albeit in a lower capacity. Though, in terms of this project, we deem the deployment in 4G LTE to be part of the transitional period which will not be considered in detail, as we instead look to 5G and the future. This choice of restricting the scope to mainly focus on 5G SA does, however, not come without an accompanying set of hurdles to overcome. As the focus of policy makers and network operators alike

is still mainly on 4G LTE, particularly in relation to the topic of next generation PSNs, a large part of the available literature, including, among other things, official decrees from governments around the world, concerns itself with 4G LTE and not 5G. Additionally, to further complicate matters, considerations regarding 4G LTE are made by interview subjects from time to time throughout the interviews, as 4G LTE are what they are most familiar with at the current point in time. Saying that we will not consider MCX services in 4G LTE to a considerable degree does not mean that there is not something to be learned from the current process surrounding it. However, we are committed to primarily examining 5G solutions, as the transition from 4G LTE to 5G is already on its way, and that, as such, 5G looks to be the long-term solution.

## 1.7 Structure

The thesis is divided into six chapters. The introductory chapter, Chapter 1, aims to give a brief overview of the problem at hand, as well as provide some motivation for why one should care about research into facilitating broadband MCX solutions. In Chapter 2 we provide some insight into the current developments of next generation PSNs around the globe, with a special emphasis on the work being done in Norway. Further on, Chapter 3 outlines the methodology being employed in the thesis, which is the conduction of interviews. The chapter provides some reasoning for why this type of research technique is chosen, as well as a discussion on the drawbacks and benefits of this type of method. From there we go on to present the results of the research in Chapter 4, discussing the findings in Chapter 5, and finally offering some conclusions and suggestions for future work in Chapter 6.

# Chapter 2
# Background

The exploration of ways to enable mission critical communications services in broadband networks is by no means a new venue of research, even in the context of the Norwegian Nødnett. Industry partners, standardization organizations, and government agencies have been looking at ways to improve the data rate of PSNs for years. This chapter presents some of the work that has been done on the facilitation of critical communications in broadband networks and attempts to give an overview of the different alternative approaches governments are taking to realize next generation PSNs in their respective countries. Particular interest is awarded to the developments of Nødnett in Norway, as it is the primary concern of this project. However, approaches of other countries are also examined as a way to learn from their experiences, and to have an opportunity to analyze deployment models that might not be under current consideration in Norway. Additionally, we present some of the research being done on this subject matter by academia, both in order to provide insights into current academic developments of, for instance, relevant technology and as a way to help position our own research in the academic space. Finally, this chapter attempts to define some characteristics of alternative deployment models that enable them to be compared against each other, such that the pros and cons of each model are able to be weighed in a structured and unbiased fashion.

## 2.1 Alternatives for mission critical services in 5G

There are a number of different deployment models to consider when discussing how to best realize mission critical broadband communications. We examine three different dimensions of the models which are explored throughout this thesis. The first dimension is that of dedicated assets, where dedicated means that the resource an asset represents is only available for PSN purposes. The second and third dimension is ownership and operation, respectively pertaining to questions regarding who owns and operates each asset. Dedication of assets is examined first, while the latter two are covered later on in this section. An illustration depicting different deployment

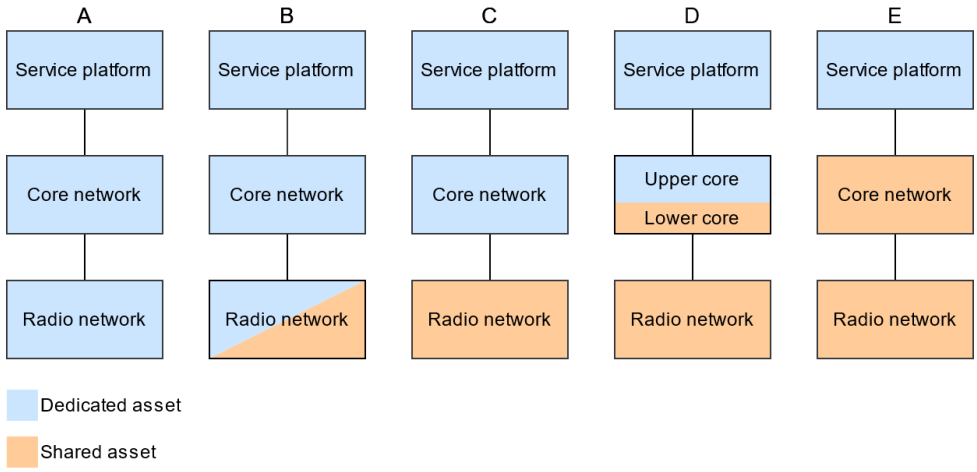


**Figure 2.1:** Figure of deployment models inspired by Nicklas Spångberg at Ericsson

models in terms of how much dedicated network infrastructure is being employed can be seen in Figure 2.1. The leftmost model in the figure, model A, shows a completely dedicated network, while the rightmost model, model E, shows a PSN where the dedicated service platform is running on top of infrastructure shared with an operator's commercial customers. One could imagine the set of possible deployment models as a spectrum where you have the fully dedicated network on the one end, and a network deployed entirely on shared commercial assets on the other. While the TETRA based PSNs of today are typically on the side of dedicated networks, utilizing their own radio and core networks, the PSNs of tomorrow are likely to move towards being deployed on shared assets, at least to some extent. There are two intertwined reasons for this, with the first being that deploying a dedicated 4G LTE or 5G RAN may be considered to be too costly of an endeavor to undertake for PSN purposes alone. When you combine this with the fact that new technologies like network slicing make the absence of dedicated network assets more bearable in terms of providing, for instance, necessary traffic isolation, it seems reasonable that many countries are exploring avenues of collaboration with commercial network operators in conjunction with the planning and deployment of the next generation of their respective PSNs.

The reason why all of the presented models in Figure 2.1 show a dedicated service platform is that an MCX platform will likely have to be tailored to the needs of public safety agencies, and could be considered to be of little interest to regular mobile network consumers. One could, however, imagine some scenarios where MCX services would be of interest to businesses like, for instance, mining companies, and that

that could potentially result in a shared service platform. In any case, a dedicated service platform does not necessarily imply that it will be owned and operated by the state, as questions regarding ownership and operation are somewhat adjacent to questions regarding dedication of assets. The same reasoning also applies to the core network, as a core network that is owned and operated by a commercial MNO would still be considered to be dedicated as long as the PSN related network assets are separated from the MNO's commercial core network. A dedicated radio network does, however, to a large degree imply state ownership, as it seems unlikely that a commercial MNO would construct a dedicated radio network solely for public safety communications purposes. In regard to the models presented in Figure 2.1, the radio network in the second model from the left, model B, stands out as it is modelled as being both dedicated and shared at the same time. This is meant to illustrate a model that makes use of radio frequencies dedicated to PSN purposes, but where those frequencies are being used as part of a commercial radio network and could also be used for commercial purposes if circumstances allow for it. A radio network solution such as this is reminiscent of the approach they are taking in the US, which will be covered in Section 2.2. Speaking of things that stand out in Figure 2.1, the core network in the second model from the right, model D, differentiates between the upper core and the lower core. This illustrates the way in which the upper core network functions could make use of core network infrastructure dedicated to PSN purposes, while the lower part of the core could be implemented as part of an operator's commercial core network. Considerations regarding this are something that will be examined in greater detail when talking about Mobile Virtual Network Operators (MVNOs) and Multi-Operator Core Network (MOCN) type solutions later on.

In December of 2017, the Norwegian government officially decided that the 700 MHz band would not be dedicated to PSN purposes, and would instead be released to commercial operators [Sam17]. A consequence of this is that there will be no dedicated radio network for the next generation of Nødnett, leaving out deployment models A and B on the left in Figure 2.1. Since 2017, DSB and the Norwegian Communications Authority (Nkom) have been working on exploring possible alternative deployment models for NGN [DSB17]. As there will be no dedicated spectrum to rely on, NGN will be realized by making use of one or more of the radio networks belonging to commercial MNOs in Norway. However, as illustrated by Figure 2.1 and as will be made clear later on in this section, there are several alternative solutions for how to proceed with NGN in the core network. The differences between these solutions are in how the infrastructure and operational assignments are going to be divided between governmental agencies and commercial actors. In 2018 DSB released a report outlining three primary alternative models of deployment for NGN proposed by operators as a result of a request for information (RFI) sent to the three Norwegian MNOs along with some related parties like infrastructure equipment

providers [DSB18]. For the sake of clarity, in 2018, as well as in 2021, the three Norwegian MNOs were Telenor, Telia, and Ice.

The first model proposed in this DSB report is that of the secure MVNO. In this model the state would acquire their own core network and service platform, and only collaborate with the commercial MNOs in order to gain access to radio network resources. While this gives the state a large amount of agency over how the service is provided, it also puts the responsibility for ensuring proper performance of the PSN on the shoulders of the state. In relation to the RAN, a decision would have to be made regarding whether the state should collaborate with one or several MNOs. Something that is worth taking note of in regard to this model proposed in [DSB18] is that it describes the state acquiring both a core network and a service platform themselves. These two do, however, not necessarily have to be acquired as a couple. An alternative solution could, for example, be that the state owns the service platform, but serves it to the users over a core network owned and operated by a commercial operator. In regard to ownership and operation it should be emphasized that there is a clear distinction made between owning assets and operating the network or the services running on top of those assets. As such, we will first concentrate on the different ways in which ownership of the different parts of the core network could affect a deployment model, before subsequently introducing the additional dimension of operation. An illustration of various ways in which parts of the core network could be owned by either the state or a commercial actor can be seen in Figure 2.2. While the service platform and the radio network naturally also have their respective owners, we choose to focus our attention on the core network for now, for the sake of clarity and brevity.

Two of the models in Figure 2.2, models A and B, depict scenarios in which the state owns the whole or part of the core network. These are examples of scenarios where the state might opt to establish their own state-owned MVNO controlling either the whole core network, in a MOCN type setup, or part of the core network, in a more traditional MVNO setup. After also having introduced the dimension of operation, these two concepts are examined further. Moving on, model C depicts a scenario in which both the lower and upper core network are owned by a commercial actor, although with the lower core being shared while the upper core is dedicated. Even though the commercial actor owning each half of the core network might be one and the same, this type of split typically implies the involvement of different commercial actors. An example of such a deployment model from the real world involving several commercial actors is the one employed in Britain, although in that case both the upper and the lower parts of the core network are dedicated. This model along with those of some selected other countries are examined in Section 2.2. The reason the aforementioned core network split typically implies the involvement of multiple commercial actors is that if there were only a single operator involved it

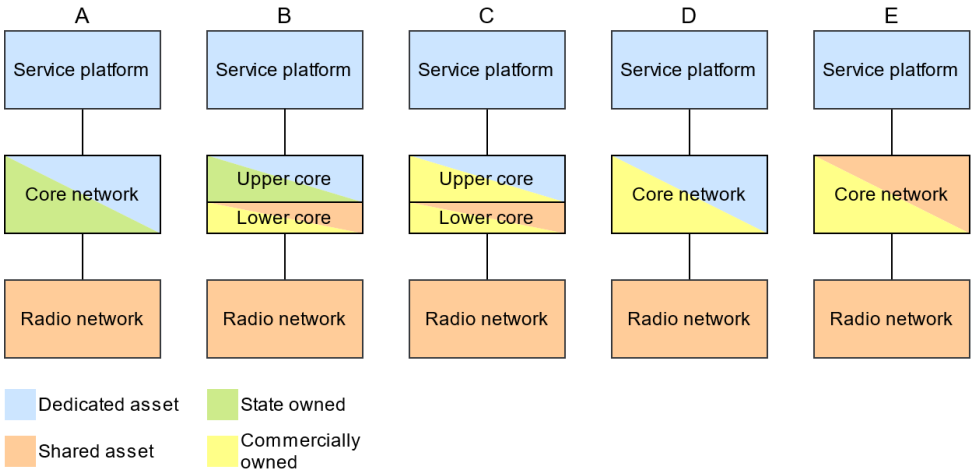


**Figure 2.2:** Figure illustrating ownership of core network assets

would likely be that the model would instead look like what is being illustrated in model D of Figure 2.2, where a single operator owns the entire core network. This model, model D, combined with the radio network solution depicted in model B of Figure 2.1, is reminiscent of the approach they are taking to next generation public safety communications in the US. Lastly, one could also imagine a deployment model making use of a core network wholly owned by a single operator that is also shared with that operator's commercial customers. In such a scenario heavy logical traffic isolation such as that provided by network slicing would likely be necessary in order to fulfill the stringent requirements of a PSN. A final remark that might be worth mentioning in regard to ownership in particular is that it seems highly unlikely that the state would own any assets that are shared, as state acquisition and subsequent ownership of an asset would essentially only be done with the intention of dedicating that asset to PSN related purposes.

We now attempt to introduce the dimension of operation in to the mix in addition to the dimensions of dedication and ownership of assets. While the owner of an asset will in many cases also be responsible for the operation of that asset, that might not necessarily always be the case. One could, for instance, imagine a scenario where the state owns a core network dedicated to PSN purposes, but goes on to hire a commercial actor to operate it, akin to how things are done with the existing Nødnett. Figure 2.3 takes Figure 2.2 and adds the dimension of operation to the different models in an attempt to illustrate some examples of deployment models incorporating all three overarching dimensions. Some of the models are now starting to resemble actual deployment models that are being implemented or planned throughout the

world. While the British and American models have already been mentioned, it could additionally be pointed out how model A in Figure 2.3 resembles the way in which state-owned MVNOs play central parts in the next generation PSN deployment models of our neighboring countries, Sweden and Finland.

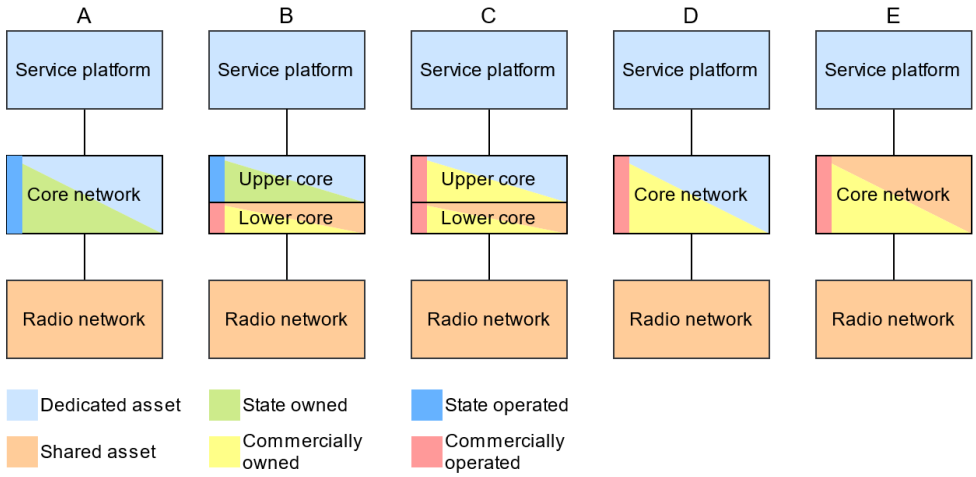


**Figure 2.3:** Figure illustrating operation of core network assets

In relation to the topic of MVNOs the aforementioned concept of a MOCN solution needs to be elaborated on. In models B and C of Figure 2.3 the state or a commercial actor acts as an MVNO and operates the upper part of the core network that handles network functionality related to, for instance, subscriber information. One of the most important VNFs in a 5G scenario related to this functionality would be the UDM. However, as has been alluded to previously, the possibility also exists for the state to own and operate the entire core network themselves, like it is illustrated in the leftmost model of Figure 2.3, model A. In this model the state would, in addition to being responsible for the upper core, also be responsible for the lower core. The lower core handles network functionality related to, for instance, mobility, with the AMF being the most important VNF in that regard. This gives the state a greater control over what happens in the core network, but could prove to be more complex than a traditional MVNO setup, especially in relation to the interface between the core network and the radio network. If the state, for instance, wants to make use of more than one RAN, concerns may be raised in regard to whether or not that could then potentially require the state to operate several AMFs, one for each RAN they would want to make use of. Challenges related to this are examined in conversation with interview subjects when discussing the prospects of state involvement in NGN.

Coming back to the previously presented DSB report in which a model involving a state-owned MVNO was the first to be proposed, the second and third model describe scenarios in which commercial operators provide mission critical communications services without the need for state-owned infrastructure or operations [DSB18]. This is akin to something like what is being illustrated by the two models on the left, models D and E, in Figure 2.3. The difference between these two proposed deployment models is that the second one relies on a single provider, while the third one incorporates all three Norwegian MNOs by letting them compete to provide services and attract PSN users to their respective networks. The second model, where only one provider has the sole responsibility for providing the PSN service, would most likely be the simplest solution of the two by far from a technical point of view. However, relying on a single provider could result in giving this provider an unintended competitive advantage in the commercial mobile market at large, and might also leave the state vulnerable to potential supplier lock-in effects, which is a concept that will be explained shortly. In terms of the RAN, this single provider may opt to use their own or enter into agreements with other MNOs in order to expand their coverage and capacity. The third model, on the other hand, might result in a healthier competitive commercial environment between the MNOs, and could also perhaps ensure that the state would not get locked in to an unfavorable agreement with a single provider. However, when several different providers are providing PSN services in the same country it is absolutely paramount that the services provided are interoperable. This means that all PSN users that need to communicate with each other, have to be able to do so regardless of what provider they are subscribed to. Without a guarantee from the providers that their services will be interoperable with services provided by their competitors, this third model will not be a feasible alternative. With that said, it is worth noting that an alternate version of this multi-operator model in which the service platform itself is shared across the three networks could be a feasible alternative in the event that interworking between separate MCX platforms proves to be a challenge.

Since [DSB18] was released in 2018, DSB along with other Norwegian governmental bodies, like Nkom, have continued to work on questions regarding deployment models for the next generation of Nødnett. The culmination of this work is a report that was delivered to the Norwegian parliament in the summer of 2020 for them to deliberate on. Unfortunately, as of conducting this project, this report has not yet been made available to the public, and the contents of it are therefore unknown to the author of this thesis. While the aims of this project intersect to a large degree with the subject matter of the aforementioned state-led investigation into alternative deployment scenarios, we aspire to provide results and conclusions that are complementary to this report by Nkom and DSB, despite our relatively limited resources.

### 2.1.1 The dangers of supplier lock-in

Supplier lock-in is an economical concept in which a customer who is dependent on a service or a product delivered by a particular supplier is unable to switch to another supplier without incurring significant switching costs. The term supplier is meant to encompass both service providers like MNOs, in the event that a PSN is purchased as a service, as well as vendors like infrastructure equipment providers, in the event that the state chooses to procure infrastructure of their own. In the context of alternative deployment strategies for PSNs, supplier lock-in is a relevant concept to keep in mind when weighing the pros and cons of committing to a commercial provider or vendor. For instance, if one were to enter into a contract with a single MNO tasking them with the provision of the RAN for a national PSN, one might have to invest in enhancing that MNO's already existing capabilities in order to meet the stringent requirements of the PSN in question. Now, suppose that the contract is nearing its termination and that the governing authority of the PSN would like to engage a different MNO in providing radio access. The switching costs would then be the extra costs incurred by getting this second MNO's RAN up to the performance level of the previous MNO's RAN that one had already invested into improving. While this is merely one example, it illustrates the danger of technical supplier lock-in that should be considered carefully when selecting suppliers.

One might call supplier lock-in a necessary downside of entering into agreements with commercial suppliers in general, as some switching costs will most likely always have to be endured when deciding to make a change to a major provider or vendor in any project of significant size. However, different deployment models may result in different degrees of supplier lock-in, and as such it will be important to attempt to minimize the potential for incurring such switching costs when deciding on a model. The most straightforward way to mitigate the downsides of supplier lock-in effects is to rely on standardized solutions, as that would make it easier for an alternative provider to come in and take over after another. One could also imagine a scenario in which a state would be interested in owning and operating more of the network themselves in order to reduce their reliance on commercial providers. Care should be taken, however, as the state might end up trading in one type of supplier lock-in for another. On the one hand, if one opts to minimize dependency on commercial providers by taking on some of the operational tasks of providing PSN services oneself, one could certainly end up in a situation where one does not have to worry as much about being locked in to commercial providers. On the other hand, opting to go for an approach in which one procures and operates one's own infrastructure could result in other types of supplier lock-in effects, such as being locked in to vendors of infrastructure equipment instead of service providers. In either case, considerations regarding the potential downsides of supplier lock-in effects need to be taken into account when deciding on how to deploy a next generation PSN.

## 2.2 Learning from other countries' experiences

As mentioned previously, Norway is far from the only country exploring their options in regard to the provisioning of broadband MCX services. In an attempt to learn from other countries' successes and failures, some solutions that have been proposed and deployed in other parts of the world are examined in this section. While some countries are taking different approaches than Norway to questions like whether or not to dedicate parts of the radio spectrum to PSN purposes, there are still a number of challenges faced and considerations made in regard to broadband MCX that are shared between Norway and several other countries throughout the world. In addition to learning from other countries' experiences, examining different deployment models being considered around the world is a way to contextualize the decisions being made in Norway, as well as contrasting the approaches of NGN against alternative approaches to, what is often, quite similar real-world challenges. The countries and corresponding PSNs that are examined in particular are FirstNet in the US, ESN in the UK, Rakel Generation 2 (G2) in Sweden, and Virve 2.0 in Finland. The reason for choosing to examine the US and the UK is that they are two of the countries that are leading the charge on next generation public safety communications, and, interestingly, are taking two quite different approaches to doing so. Sweden and Finland are examined as they are neighboring countries of Norway, meaning that Norwegian public safety actors have to cooperate closely with Swedish and Finnish public safety actors in a number of scenarios. They are also both further along in the decision making process than Norway currently is in terms of implementing their own next generation PSNs. As an additional note, documentation and reporting done on any particular country's PSN has a tendency to be written in that country's own language. While this is not an issue in regard to the UK and the US, it could impact our ability to gather information about, in particular, the Finnish process, and also, to a certain degree, the Swedish one.

### 2.2.1 ESN in the UK

In the United Kingdom the next generation PSN that will be offering broadband MCX services is called the Emergency Services Network (ESN). To be precise, the network will actually only cover the area known as Great Britain, meaning that Northern Ireland is being left to fend for themselves. However, as it is the British government who are making decisions in regard to ESN, we will refer to the country of ESN as the UK for the sake of brevity. With that said, the UK's original intention was to start using ESN in September of 2017 and be able to phase out their TETRA solution, called Airwave, by the end of 2019. Despite this ambition, however, as covered in a report from 2019 by the British National Audit Office (NAO), a number of hindrances were encountered that have resulted in the transition being significantly delayed [NAO19]. An extension on the Airwave contract has been negotiated by

British authorities with Motorola Solutions which extends the lifetime of Airwave until the end of 2022, effectively representing a new deadline for moving PSN users over to ESN three years after originally planned. However, this contract includes options for the British authorities to extend the lifetime of Airwave even further, should ESN not be ready for large scale adoption by the end of 2022. In regard to that, recent comments made by British authorities as well as by the CEO of Motorola Solutions, Greg Brown, indicate that the Airwave contract will probably be extended all the way to 2025 [Jac21].[1] This lines up with how the NAO report identifies specific uncertainties related to, for instance, various aspects of user adoption that could in a near worst-case scenario delay the Airwave shutoff by an additional four years. In addition to taking a more cautious approach to the shutting down of Airwave, British authorities are taking a different approach to the rolling out of ESN in general. Instead of sticking to the original vision, which was to launch ESN as one complete package, they will be rolling out individual services in an incremental fashion. Adopting a more flexible approach to the transition seems reasonable in light of the fact that there is still significant uncertainty tied to how developments will progress. As an example, a comprehensive plan for switching off the Airwave network does not yet exist, as specifics regarding when and how will have to be agreed upon by authorities and user organizations once the transitional process is further along and one has a clearer picture of the practical realities of the situation [NAO19].

As it is the situation at hand, it seems only natural that the current focus for the British authorities, as well as for most other authorities around the world, is on the ongoing transition from traditional TETRA based networks to broadband PSN solutions. Despite the fact that the primary interest of this project is 5G and potential future solutions for MCX in 5G networks, there are still some lessons to be learned from the challenges faced in this transitional period. As an example, it is interesting to regard relationships developing between governmental agencies and commercial providers. In Britain, the most prominent commercial actor in this regard is the MNO EE, which will be providing British authorities with the required mobile network infrastructure that ESN will be deployed on. In much the same way that Norwegian authorities will have to cooperate with commercial MNOs in order to gain access to their respective RANs, the British authorities are cooperating with EE. The NAO report mentions EE's agreed upon responsibilities in regard to radio network coverage as being to expand and upgrade their infrastructure, such that they will be able to provide coverage on land, including in tunnels and other locations specified in the contract, 12 nautical miles out to sea, and up to 500 feet into the air [NAO19]. However, while the majority of the coverage of ESN will be provided by EE, there are some coverage responsibilities that fall on the British Home Office to handle themselves. These include coverage in the air above 500 feet, as well as

[1] As of June 2021 the British authorities have negotiated an extension on the Airwave contract with Motorola Solutions that will keep the TETRA network running until at least 2026 [HC21].

areas of land described in the NAO report as being not covered by the market. This means that it is the British authorities' own responsibility to build base stations in remote areas where it does not interest EE. These areas could be imagined to be areas of low or no population, such as national parks or other areas of what is presumably wilderness. In a presentation given at a conference in March of 2021, ESN program director John Black notes that 430 new EE masts have been activated so far out of around 1100 new masts that will have to be built in order to meet the coverage requirements of ESN [Bla21]. If we consider the challenge of providing coverage to the most rural areas of a nation from the Norwegian perspective, the nature of the Norwegian geography makes it seem clear that this is something that could easily become a point of contention when moving towards NGN. Regardless of which deployment model that is eventually selected as the one we will base NGN on in Norway, the problem of ensuring coverage in rural areas where commercial MNOs have little economic incentive to do so is one that needs to be addressed.

In terms of the core network the British authorities have opted for a dedicated core with responsibilities split between EE and Motorola Solutions. EE takes care of the lower core, as an extension of the RAN they are providing, while Motorola Solutions are responsible for the upper core as well as the services that will run on top of the network [NAO16]. As for the RAN, in relation to alternative deployment models, ESN will share spectrum with commercial users, similar to how it will be done in Norway. Following the modelling scheme of Figure 2.3, the deployment model of ESN would look something like what is presented in Figure 2.4. A solution consisting of a shared commercial RAN, a dedicated core network split between two commercial actors, and a commercially owned and operated service platform on top. Aside from the dedicated lower core, the approach taken in the core network is akin to that which is presented in model C of Figure 2.3.

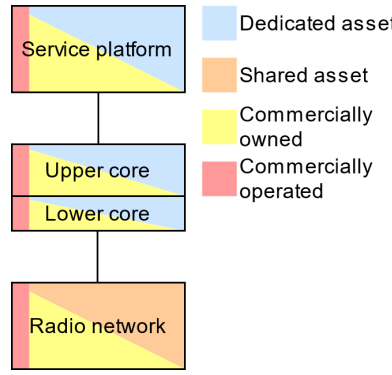


**Figure 2.4:** The ESN model

The fact that the responsibilities in the core network could be split between several commercial actors, and not just between a commercial actor and the state, is interesting to take note of. If one imagines taking the approach of a dedicated core network for NGN in Norway, questions regarding who will own and operate this dedicated core need to be thoroughly answered. Naturally, it would be possible to do as they are doing in the UK, and let one or more commercial providers take care of the network functionality. However, one also has to weigh the pros and cons of the

involvement of state actors in the establishment and operation of a dedicated core network, something that has presumably been done in the UK and decided against by authorities. Some of the benefits of heavily involving commercial actors in ESN are presented in the 2016 NAO report as making it easier for the service to stay up to date with market trends, such as, for instance, the transition from 4G LTE to 5G when that time comes [NAO16]. In addition, the report argues for the involvement of a multitude of commercial actors on shorter contracts as being beneficial for avoiding potential supplier lock-in effects, leaving each supplier susceptible to being dropped in favor of a cheaper or better one. If one were to turn this argument on its head, this would imply that the selection of a smaller number of providers on longer contracts could potentially risk tying governments up with suboptimal providers due to supplier lock-in effects.

### 2.2.2 FirstNet in the US

In the Middle Class Tax Relief and Job Recovery Act of 2012, the US congress dedicated part of the 700 MHz radio frequency band in the US, also known as Band 14, to public safety communications. In line with this band allocation, the act also established the First Responder Network Authority, commonly referred to as FirstNet [USC12]. FirstNet's mandate is described in this act as being to "deploy and operate a nationwide public safety broadband network." In order to fulfill this mandate, FirstNet entered into a contract with the American MNO AT&T in 2017. This contract describes AT&T's responsibilities in regard to the delivery of public safety communications in the US, and provides specific task orders concerning topics like the deployment of the core network and the enhancement of the existing radio network infrastructure in order to fulfill coverage requirements [FN21]. Deployed and operated by AT&T, FirstNet makes use of a dedicated core network in which the traffic of FirstNet's users is processed separately from AT&T's regular users' commercial traffic. In regard to the RAN, the task order requires AT&T to be able to provide coverage for the dedicated Band 14 across all states and territories in accordance with locally negotiated agreements. An interesting task order which was delegated later, in June 2020, describes how AT&T is required to upgrade the network to 5G when the time comes, and to ensure that the transition process goes smoothly without disrupting services [FN21]. The obvious ambition of the state being that as the FirstNet PSN is heavily intertwined with AT&T's infrastructure in general, the FirstNet users will be able to piggyback off of AT&T's commercial interests in upgrading their network to 5G.

In a similar fashion to how ESN is modelled in Figure 2.4, an attempt is made to illustrate the deployment model of FirstNet in Figure 2.5. As mentioned as an example when introducing the concept of dedicated and shared assets in Section 2.1, the radio network component of the FirstNet solution could, in a sense, be considered

to be both dedicated and shared at the same time. This is because, while there is dedicated spectrum to public safety communications in the US, this spectrum may be used by AT&T for commercial purposes if circumstances allow for it. AT&T guarantees that spectrum will be available to PSN users when they need it, but serves regular customers over that same spectrum while it is not needed for PSN purposes explicitly. The core network of FirstNet is a dedicated one, as shown in Figure 2.5, and is operated and owned by AT&T on behalf of the FirstNet authority. As for the service platform, detailed information is a bit hard to come by, but it seems like it will be a commercially owned and operated platform going by the name of FirstNet PTT. All in all, the deployment model of FirstNet slots nicely into the category of being a single turnkey provider, which is being considered as one alternative for NGN in Norway. To relate the deployment model of FirstNet to the models discussed in Section 2.1, the setup for the core network is similar to that which is illustrated in model D of Figure 2.3.

One interesting fact to note about the PSN situation in the US is that, unlike in, for instance, Britain, there are multiple providers of PSN type services in addition to the FirstNet/AT&T partnership. The most prominent of these competing networks being Verizon's Frontline network,[2] which offers seemingly similar services to FirstNet. As a side note in regard to the competitive aspects of providing PSN services in the US it is interesting to note that although the US government has dedicated a part of the radio spectrum to public safety, these frequencies are exclusively available to AT&T through their agreement with FirstNet. This means that Verizon have to make use of their own commercial spectrum for the provision Frontline, something that it could be argued puts them at a competitive disadvantage to AT&T in the public safety communications market. Additionally, as mentioned previously, this dedicated spectrum could also be used for commercial purposes by AT&T if circumstances allow for it, putting them at an even greater advantage, as spectrum is generally considered to be a quite limited natural resource. This competition with Verizon does, however, incentivize FirstNet/AT&T to provide top-of-the-line services to their customers or risk losing them to competitive offerings, which could result in better services for American public safety actors in general. However, distributing public safety agencies across a number of PSNs puts a heavy

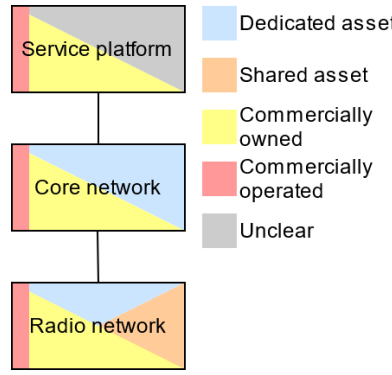


**Figure 2.5:** The FirstNet model

[2] https://www.verizon.com/frontline

emphasis on interoperability between these networks, as public safety agencies subscribed to different PSN providers will need to communicate with each other from time to time. This is something that will have to be kept in mind in any country where multiple PSNs are deployed.

### 2.2.3 Virve 2.0 in Finland

Finland has taken yet another approach to the implementation of their next generation PSN, involving the state directly to a much greater degree than the UK and the US. Erillisverkot, a company owned by the Finnish state that has been responsible for the orchestration of their current TETRA network Virve, have been tasked with deploying, operating, and otherwise procuring services related to the Finnish next generation PSN, Virve 2.0 [CCA18]. Like in Norway and Britain, no dedicated spectrum for broadband MCX services has been awarded in Finland and no dedicated RAN will be built. As such, Erillisverkot has selected to partner with the Finnish MNO Elisa in order to gain access to their radio resources [RR20]. When it comes to the core network, however, the Finnish strategy deviates significantly from the ones seen in the UK and the US. The state-owned operator Erillisverkot will deploy and operate their own core network as an independent MVNO, with core systems being delivered by the infrastructure equipment provider Ericsson. So, while the core network in both the UK's and the US's models are also dedicated, the Finnish core network will additionally be owned and operated by a state-owned MVNO instead of by a commercial provider. As for the service platform, the tendering process related to procuring a service platform which presumably will be owned and operated by the state is set to commence in 2024 [Eri21]. While a temporary solution will be provided in the meantime, we include the future plan for the service platform in Figure 2.6, depicting the Finnish deployment model. Erillisverkot's strategy is noted as being to engage a number of providers on shorter contracts that adhere to open standards, with the ambition of creating a competitive environment in which each provider involved in the solution could be changed out for another one if the need or desire should arise [Toi21]. The timeline set by Erillisverkot is that all user should be migrated away from TETRA by the end of 2025.

As mentioned in the introduction to this section considering other countries solutions, the language in which documentation related to a country's PSN is most often found is the native language of the country in question. As such, much of the documentation regarding Virve 2.0 is in Finnish. This, in addition to the fact that the Finnish government seem to be keeping their cards quite close to chest in regard to the reasoning behind opting to go for an MVNO based deployment model, makes it somewhat challenging to get a detailed overview of the Finnish process apart from the broad strokes. Despite this, an attempt to model the Finnish deployment model for Virve 2.0 is made in Figure 2.6. As one can see, the core network component of

this figure is quite different from the ones in the figures of FirstNet and ESN, as it incorporates a state-owned MVNO.

There is, however, one assumption being made in relation to the core network presented in Figure 2.6, and that is in regard to the previously presented concept of a MOCN type setup versus more of a traditional MVNO setup. In Figure 2.6 it is assumed that Erillisverkot will be operating a full core network themselves in a MOCN type of way, meaning that they will own and operate, among other things, their own AMF. While this is not necessarily the ways things are going down in Finland, the assumption is made as an extension of the Finnish argument of state control over the PSN ecosystem, as employing a MOCN setup is likely to increase the control a state has over the way things are done in the core network. As an additional supporting argument of the assumption, the Finnish authorities seem to have intertwined themselves quite closely with the commercial operator Elisa in general, and a MOCN setup is something that would require exactly this kind of close cooperation between the operator of the RAN and the operator of the core network. Finland is one of the countries who are furthest along in the process of deploying a broadband PSN, and they make for an interesting case study in regard to state involvement in next generation PSNs. However, whether or not Norway will embrace the same level of state involvement is something that remains to be seen. Considering the deployment model of Virve 2.0 in regard to the models that were discussed in Section 2.1, the approach taken in the Finnish core network is similar to that of model A in Figure 2.3.

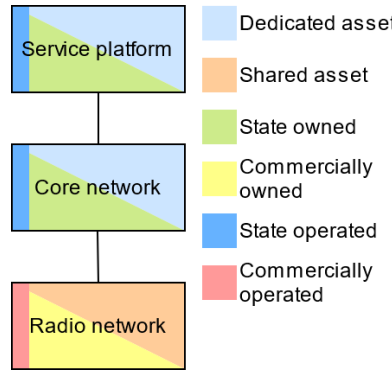


**Figure 2.6:** The Virve 2.0 model

### 2.2.4 Rakel G2 in Sweden

Like for many of the countries discussed in this thesis the decision to move towards broadband public safety communications has been in the works for some time in Sweden. However, in the summer of 2020 a minesterial decree was finally put out by the Swedish justice department tasking the Swedish Civil Contingency Agency (MSB) with procuring a state-owned core network to be used for PSN purposes, officially marking the start of the Rakel G2 establishment process [SJD20]. As a start, MSB is tasked with providing the current users of the Swedish TETRA network, Rakel, with mobile data communications services. However, the decree specifies that the procured core network should be able to be expanded upon to facilitate the

establishment of a broadband PSN, in the event that the Swedish government decides to move forward with the Rakel G2 project. Like in Norway, the authorities, which would be MSB in the case of Sweden, have their work cut out for them in terms of collaborating with the user organizations of the current TETRA network and other relevant authorities in defining requirements for the broadband services in question. Specifically, the ministerial decree tasks MSB with identifying and categorizing the Rakel users' needs for various types of broadband communications services, and from them developing a set of requirements for the system that will ensure sufficiently high availability, security, and robustness. Unlike in Norway, however, the Swedish government has decided from the get-go that a state-owned core network will be a part of the solution [SJD20]. Whether or not the Norwegian government will follow suit in terms of incorporating a state-owned MVNO into NGN is, however, something that remains to be seen. The reasoning given by the Swedish government in the aforementioned minesterial decree for making this decision is that Swedish authorities, by owning their own core network, will be able to ensure that subscriber information, traffic data, and other sensitive information is being handled securely within Swedish jurisdiction. Furthermore, the Swedish government is under the impression that, in order to increase the long-term prospects of agreements entered into and decisions made, MSB should be responsible for the core network in Rakel G2. However, in regard to the operation of said core network, sources with knowledge of the Swedish process have informed us that MSB is looking to outsource the operation to another organization. Whether this other organization is a commercial service provider or another state-owned entity is not yet entirely clear, and as such the operations part of the core network modelled in Figure 2.7 is left unclear.

In regard to the question of whether or not a Swedish next generation PSN should make use of dedicated radio frequencies, the Swedish authorities seem to still be somewhat on the fence, giving rise to the uncertainty in the radio network component of the model in Figure 2.7. In late 2018 a report was released by the Swedish government in regard to a governmental inquiry into the future regulation of radio spectrum in Sweden [SOU18]. This report concerns changes to legislation regarding how spectrum is awarded, and seems to suggest that Swedish authorities have adopted a newfound preference towards a more competitive approach to, for instance, auctioning off frequencies. According to the report, frequencies that have typically been hogged by various branches of government may in

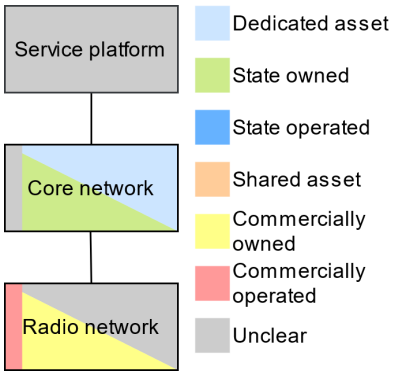


**Figure 2.7:** The Rakel G2 model

the future be made available for commercial purposes, although it is noted that the needs of, for instance, the Swedish armed forces or the police could in some scenarios still outweigh that of other actors. With this in mind one may then consider the fact that, while there does seem to be some tendencies in government towards opening the door to more commercial interests in frequency land, the minesterial decree from before additionally tasks MSB with exploring any possible needs for the use of dedicated frequencies, as well as ways in which such needs might be met [SJD20]. One could, for instance, imagine a radio network solution reminiscent of the one they have employed in the US, where spectrum is both dedicated and shared according to circumstances.

All in all, there are still a number of aspects of the Swedish solution that are not yet in place. In Figure 2.7, several components are marked as unclear and several assumptions are made. For instance, it is assumed that the RAN will still remain in commercial hands even if dedicated spectrum is allocated, and it is assumed, as it was similarly assumed in the Finnish model, that a MOCN type solution will be employed in the core network. Naturally, neither of these two aspects are entirely clear in regard to Rakel G2. As there are still a number of decisions yet to be made by the Swedish authorities, one might consider their situation to be that of the countries' mentioned here that most closely resembles the Norwegian. While the decision to establish a dedicated core network seems to be final, no decision seems to have been made in regard to spectrum as of yet. However, if the Swedish authorities were to go with only commercial spectrum, the Swedish approach might start to closely resemble what we describe in this project a potential Norwegian MVNO type solution.

## 2.3 Related academic work

Although most of the development being done in relation to next generation PSNs is being done by standardization organizations, operators, equipment providers, and governments, there is still some academic work that is of interest to this project. There is a lot of work being done on the topic of 5G and related technologies in general, but there are also studies being done with regard to public safety in particular. This section aims to give a brief overview of some of the work we have discovered, and that we believe to be of relevance to next generation PSN projects. Some of the examined studies focus on how to best utilize particular technologies for PSN purposes, such as [PRVS+19] by Pérez-Romero et al. that explores how network slicing can be employed to provide mission critical services in various states of emergency and [SSA+18] by Solozabal et al. that presents a distributed MCPTT architecture making use of MEC, while other studies relate more generally to the topic of next generation PSNs as a whole, such as [VS21] by Volk and Sterle that examines a number of

5G related technologies with regard to public safety and provides results from field experiments with relevant equipment conducted on the ground in Slovenia.

Here at home, in Norway, some of the relevant research being published is coming out of research facilities associated with Norwegian MNOs, such as 5G-VINNI, which is associated with the research department at Telenor. In [GGM+20], for instance, Pål Grønsund of Telenor et al. examine the implementation of network slices for a military use case in collaboration with the Norwegian defense materiel agency. As the concept of traffic isolation is an important aspect of the deployment of mission critical communications services in commercial broadband networks, the topic of network slicing is naturally one that is of interest to many researchers. Höyhtyä et al. examine a number of technology enablers for broadband PSNs, such as network slicing and SDN, and provide experimental results relating to both the enablement of priority communications in commercial broadband networks and the feasibility of rapidly deploying network assets in the event of substantial outages due to, for instance, natural disasters like earthquakes. Also related to the concept of network slicing, among other things, [ON20] by Othman and Nayan provide an overview of the concept in general and examine the underlying technologies that make slicing possible, such as NFV and SDN. Lastly [SPRS+19] by Spada et al. present the 5G ESSENCE architecture based on Cloud-Enabled Small Cells (CESCs), while Sanchoyerto et al. take a step back and examine the QoS characteristics of MCPTT services in [SSBL19].

As one can tell from the aforementioned work, there does indeed exist a number of research avenues related to 5G and mission critical services. One interesting thing to note, however, is how much of the presented research on 5G revolve around implementations of various reference architecture. While there exists little doubt that the results gathered from these experiments are inherently valuable to the development of 5G as a whole, it exemplifies how there are numerous aspects of the implementation of 5G networks in real world contexts that are still somewhat uncertain. In terms of this project finding its own place amid what is slowly becoming a host of related research, we have discovered little research that deal directly with the challenges related to alternative deployment models for next generation PSNs. As noted previously, the subject matter of broadband PSNs is one that is typically of interest to commercial and state actors. Something we believe to be especially true for considerations regarding benefits and drawbacks of various deployment models in the context of a particular country. However, despite the fact that this thesis does not delve into the details of particular 5G MCX related technologies, it will hopefully be able to stand on its own as a high-level analysis of considerations related to the deployment of next generation PSNs, particularly in regard to Norway and NGN.

## 2.4 Defining comparison criteria

In order to be able to provide a fair assessment of differing deployment strategies for the next generation of PSNs, an attempt is made to define some criteria on which to base the comparison effort. As we are dealing with PSNs here, the selected criteria aim to describe what we believe to be fundamental qualities of critical communications systems, such as reliability and robustness, as well as some less obvious qualities that may prove consequential in terms of selecting a deployment model, such as aspects regarding the dangers of technical supplier lock-in and technological complexity. Before going into each criterion and the reasoning behind selecting it in more detail, the following high-level criteria for comparison of alternative deployment models for NGN have been defined.

| | |
|---|---|
| **Robustness** | Ensuring robustness of the RAN as well as the core network in order to be able to provide reliable communications under challenging circumstances. |
| **Complexity** | Refraining from employing technological solutions that introduce technological uncertainty and unnecessary costs in terms of challenging implementation and maintenance. |
| **Flexibility** | Making use of standardized technological solutions in order to encourage commercial competition and avoid being extensively locked-in to any particular supplier. |
| **Security** | Ensuring confidentiality of information, both in terms of the contents of the communications themselves, as well as metadata concerning these communications. |

Now, while these definitions might at first glance appear somewhat vague and broad, they outline the four primary focus areas for the comparison of alternative NGN deployment models. The reason for their apparent vague- and broadness is that these criteria all concern aspects of great nuance. For instance, when discussing the necessity for constructing a robust network, the satisfactory level of robustness and the severity of the considered challenging circumstances under which the network is expected to perform will depend on the individual viewpoints of parties involved in such a discussion. However, while establishing a precise requirement for robustness in the network appears to be a challenging exercise, comparing different alternative deployment models against each other and concluding that one appears more robust than the other might be a more accessible task.

It is also worth noting that although a distinction is being made between them, the comparison criteria could in some cases be quite dependent on each other. For

example, it is not difficult to imagine that a robust and technologically flexible solution could turn out to be more technologically complex than a less robust and flexible one. An example of such an interdependence might, for instance, be the influence a reliance on properly standardized solutions would have on both the complexity and the flexibility of a solution. The implication being that one, by employing technology subject to comprehensive standardization, would gain improved flexibility in terms of supplier-agnosticism and, at least perhaps intuitively, may also be able to reduce technical complexity by avoiding heavily tailored implementations. However, regarding this assumption concerned with technical complexity, it is worth noting that such an assumption may not turn out to be true in practice, and that there exist entirely different interdependencies between comparison criteria that are not mentioned here. The bottom line in either case being that it seems reasonable to assume at least some interdependencies, and that the compartmentalization by comparison criteria is mainly employed as a tool for lending some structure to the presentation of data collected during interviews, as well as to the subsequent discussion of that data, rather than as formal definition for describing aspects of the highly complex systems in question.

So, to expand a bit on the definition of each criterion, starting from the top with robustness. The quintessential quality of any PSN is that it is able to withstand some level of adversity. Something that is especially true when you consider the fact that adverse situations often are the ones in which critical communications services are most sorely needed. Robustness would, in this regard, entail redundancy and possibly autonomy among other concepts, in the event that network resources become unavailable due to some undesirable event. Redundancy here meaning, for instance, being able to make use of one of the other available RANs should your primary RAN for some reason become unavailable, and autonomy meaning the possibility for regions on the edge of the network to keep functioning locally in the event that connection to the centralized core network is lost. In short, the criterion of robustness is intended to describe each deployment model's ability to maintain a satisfactory user experience in the event of unforeseen disruptions of the network at large, with a greater degree of robustness being favorable when comparing models against each other.

As for the criterion of complexity, the intention is to attempt to distinguish alternative deployment models from each other by examining the broad strokes of their respective technical solutions, and to determine whether one model depends on a more technologically complex solution than another. The reasoning behind selecting this as a relevant criterion for the purposes of comparison is that we consider a less technically complex solution to be beneficial. This again is attributed to the fact that we perceive less complexity to imply less room for error and a less intensive resource requirement for implementation and maintenance. Additionally, it could

be assumed that a less complex solutions also implies a lesser need for tailoring of that solution, thus giving rise to more flexibility. However, as mentioned previously, such an assumption may or may not turn out to be true in practice, which is part of the reasoning for considering complexity and flexibility as separate criteria, despite any possible interdependencies. Now, with all of this being said, this criterion of complexity is probably the most contentious of the four in terms of comparing models against each other. The reason for this being that the scope of this project considers the future more so than the current situation, and that, as is mentioned throughout this thesis, many aspects of 5G and related technologies remain shrouded in uncertainty, at least in terms of implementation, but also in some cases in terms of standardization. As such, judging how much complexity a certain decision regarding a deployment model model for a next generation PSN might incur, could be challenging to do accurately. Lastly, for the sake of clarity, we consider less complexity to be favorable when comparing deployment models against each other.

Although it has already been touched on in the preceding paragraphs, as well as in Section 2.1 when considering the dangers of supplier lock-in, we would like to summarize the intent behind selecting flexibility as one of the comparison criteria. The reason for doing so is to facilitate the comparison of alternative deployment models for NGN in terms of how well they make use of standardized technological solutions, as well as their respective outlooks with regard to supplier lock-in. Now, it seems likely that the final solution will be required to be compliant with international standards by government decree, regardless of which model is chosen. However, it is our belief that, while it is impossible to avoid supplier lock-in effects altogether, some solutions might be considered to allow for lower or higher degrees of supplier lock-in than others. In conjunction with this it is important to note that it is not the same to be locked in to a single supplier as it is to simply be supplied by a single supplier, although the latter could in some cases lead to the former. An additional aspect to consider in regard to this comparison criterion of flexibility is that a reliance on standardized solutions and an attempted avoidance of supplier lock-in scenarios could facilitate greater commercial competition in the marketplace for PSN related technologies, due to the fact that more flexibility for the state means more room for the purchase of technologies from alternative providers. This in turn would incentivize the incumbent provider to improve their solution in fear of losing their contract to a competitor. By this reasoning, we consider a higher degree of flexibility to be beneficial when comparing deployment models against each other.

Finally, there is the comparison criterion of security. As much of the information transmitted over a PSN could be considered to be sensitive in nature, the safeguarding of this information is important. Communications between first responders could, for instance, concern patients or victims, or other mission critical information regarding ongoing operations that public safety agencies do not want to be publicly known.

As such, this comparison criterion is defined in order to examine the ways in which different deployment models facilitate the protection of this confidentiality. In addition to the contents of the communications, it also seems reasonable to assume that there will, in a PSN setting, exist metadata about these communications that could in some cases be considered to be sensitive. Mobility data, for instance, is intrinsic to the functionality of handover in a mobile network, but could also help reveal information about the location of users. In a scenario like a covert police operation, or any other operation in which the users of a PSN would prefer their location to be concealed, the ability of a commercial operator to potentially extract this mobility data could be considered to be a security risk. The comparison criterion of security aims to include both of these matters of confidentiality, and a higher degree of security is naturally considered to be favorable for a deployment model when comparing it against its peers.

# Chapter 3
# Methodology

This chapter describes the methodology we have chosen for carrying out this project, as well as justification for why we believe the chosen methods to be best suited for our project. In Section 3.1 we provide contextual information on the nature of interviews, and present the unstructured interview as our data collection method of choice. The chapter then goes on to describe the selection procedure for the selection of interview subjects in Section 3.2, the way in which we conduct the interviews in Section 3.3, and how we process the results of the conducted interviews in 3.4. Additionally, in 3.5, we describe methodology for the comparison of the different deployment models for MCX in 5G, in order to give each alternative what we believe to be a fair assessment.

The reason we have chosen to conduct interviews instead of, for instance, sending out a questionnaire is due to the nature of the problem at hand. We are less interested in polling attitudes towards MCX in 5G than we are in actually understanding the underlying issues that providers and regulators will be forced to tackle going forwards. In a sense, conducting interviews could from this point of view be considered to be a method of information gathering somewhat like a literature review. However, by combining literature with the opportunity to speak directly to interview subjects with relevant and updated firsthand knowledge about questions central to our research, we believe the information we gain to be deeper, more nuanced, and more closely related to real-world challenges than what we would be able to achieve from consulting the literature on its own.

## 3.1 On the nature of interviews

While one could argue that a questionnaire-like approach to data collection could be characterized as a sort of quantitative interview, interviews are in general considered to be of a qualitative nature. Interviews come in many different shapes and sizes, differing in areas such as communication medium, group size, and structure. One

could, for instance, assume that an interview conducted by telephone might yield different results from one conducted in person, and that answers given by a respondent in a group interview might be different from answers given in a one-to-one interview. However, disregarding these two dimensions of differences for a minute, a common way to categorize interviews is by their structure, of which there are three main categories [RM16]. The fully structured interview emulates the sort of data collection one would typically associate with a questionnaire by employing a set of predetermined questions with fixed wording. The main difference from a questionnaire-like approach being the interview setting and an emphasis on open-ended questions. The second category of interviews would be the semi-structured interview, in which the researcher may adapt to the flow of the conversation by, for instance, asking follow-up questions, or by tweaking the wording of the questions. It is important to note that while the semi-structured interview gives the researcher more freedom, there still exists a clear agenda or checklist for the interview which the researcher must adhere to. The last category of interviews is found at the other end of the spectrum from the fully structured interview, and is called the unstructured interview. As implied by its name, unstructured interviews have no predetermined questions or structure and the researcher lets the conversation develop based on the subject and a general field of interest [RM16].

The type of interview we have chosen for this project is the unstructured interview. While there are a number of pitfalls and drawbacks to be aware of when conducting unstructured interviews, there are also some benefits. The main reason for why we have chosen this allowing form of interview is that the line of questioning we would want to take in each interview depends heavily on the knowledge and experience of the individual interview subjects. This means that, while it would have been pleasant to be able to write out a list of all relevant questions and have them be answered in a satisfactory manner, and while each interview is closely tied to an area of interest, the questions have to be adapted in regard to the interview subject's particular expertise. Adaptation of the line of questioning serves two purposes in this context. For one, it allows for a more efficient extraction of information from the participants, as asking them questions on topics of which they seemingly know little and subsequently receiving subpar answers seems counterproductive. On the other and perhaps more important side of that coin, asking the participants questions on that which is their areas of expertise has a far greater chance of providing us with the insight we are seeking, and may even reveal answers to questions that we did not know we were in fact wondering. The downside of this of course being that some questions may remain unanswered at the end of an interview, due to those questions being outside the interview subject's area of expertise. However, receiving unsatisfactory answers will always be a potential consequence of conducting interviews with open-ended questions. By adapting the line of questioning to each individual subject we believe that we are able to improve the quality of the answers to the questions that they are

particularly knowledgeable about, while sacrificing some less interesting answers.

Due to the free-form nature of unstructured interviews, there are, as mentioned previously, some important pitfalls to be aware of when conducting them. Robson and McCartan present some general disadvantages of conducting interviews in [RM16] that become even more pronounced in an unstructured interview than they would have been in a fully structured one. Due to the inherently loose structure of the interview, it is up to the interviewer to keep the interview on course. This includes keeping track of the time, making sure the conversation stays within the boundaries of relevancy to the research project, and ensuring that important and poignant questions are asked when appropriate in order to maximize the value of the interview in terms of results. In addition to this there is the question of bias, certainly on the part of the subject, but also, although perhaps to a lesser extent, on the part of the interviewer. One has to account for the possibility that an interview subject who is personally invested in the topic of discussion will give answers that are in line with their convictions and personal interests. For instance, when interviewing an employee in a governmental agency that deals with their respective nation's PSN, one should expect to receive answers that may be swayed towards recommending more governmental control and involvement in the deployment of MCX in 5G, especially in comparison to answers one might get from an employee of a commercial MNO. This kind of bias is very difficult to eliminate, as the interviewer obviously has a limited influence on the answers received outside of asking the right questions. However, recognizing this bias and keeping its existence in mind when processing the results is paramount to being able to provide a fair assessment of the underlying topics. On the other hand, bias on the part of the interviewer is simpler to deal with, given that one is careful to be aware of oneself in the process of conducting an interview. The main challenge lies with the wording and presentation of the questions asked to the participant. As such, the interviewer should make an effort to avoid asking leading or loaded questions that might entice the interview subject to answer in a particular way [RM16].

## 3.2 Selection of interview subjects

As mentioned, it seems inevitable that interview subjects will give somewhat biased answers to questions concerning aspects of their employment. When discussing the topic of governmental involvement in the creation and operation of the 5G PSN, it is reasonable to assume that a subject with a background from the commercial side of the divide may give different answers to someone from the state side. For this reason, it is important to select a wide variety of interview participants. Being able to examine responses from interview subjects holding different viewpoints provides more valuable and nuanced insight than examining answers from a narrower scope of

respondents. In addition, it increases our ability to recognize and mitigate potential biases in the results.

When conducting research by for instance a questionnaire, reaching out to a representative sample of the population is of the utmost importance [RM16]. This sampling might be done randomly, or by systematically ensuring that predefined subgroups of the population are all represented in the sample, in order to mitigate bias. However, as opposed to sending out a questionnaire, conducting interviews is a time-consuming enterprise. This means that the sample size of people that are interviewed amounts to a small part of the population, ruling out the probability for random sampling to create a representative sample. Instead, we attempt to work systematically in order to obtain a representative sample based on employment, both in terms of role and employer. With that said, stating that a systems engineer at a Norwegian MNO is representative for system engineers across all three Norwegian MNOs might be considered to be a crude generalization. Unfortunately, because there is a limit to how many interviews we are able to conduct in the course of the project, such generalizations may in some cases have to be made. It is important to keep these generalizations in terms of representativeness in mind when processing the results of the interviews, in the same way that the existence of bias must be kept in mind.

While selecting interview subjects we consider potential participants to be in one of three main subject categories. The first category contains the users of Nødnett and the user organizations they are affiliated with. From this category we expect to gain some insight into user behavior, wants and needs, as well as expectations for NGN from the point of view of the user. This information is valuable because it may provide us with a better understanding of the shortcomings of the existing Nødnett, shed light on how those shortcomings are currently being dealt with by users and user organizations, as well as help us reflect on how the challenges of today could potentially be solved in NGN. As an example of a measure taken by users to address the aforementioned shortcomings of Nødnett, many Norwegian public safety agencies are already involving commercial providers in their communications solutions as a supplement to Nødnett. The second and third category are the commercial actors and the state actors respectively. With these two categories the ambition is to understand each of their perspectives in regard to collaborating on realizing MCX services in 5G. For the commercial actors it might, for example, be interesting to examine aspects regarding the commercial viability of providing MCX services, while it, for the state actors, makes more sense to inquire about regulatory requirements or perceived operational obstacles on the path to NGN. In addition to attaining this broader understanding of perspectives, we also take the opportunity to ask interview subjects about technical real-world challenges and potential solutions, both in regard to the Nødnett of today, the one of tomorrow, and of 5G in general. Dividing the interview

subjects into three categories like this gives us an opportunity to compartmentalize our research in terms of when to schedule interviews, as well as what topics to cover in which kinds of interviews. It also simplifies the task of balancing bias related to being a member of one of these categories by balancing the number of participants we interview from each of these predefined categories.

When planning and scheduling the interviews we attempt to approach one subject category at a time. First, we interview the users and user organizations, then the commercial actors, and lastly the state actors. There are a couple of reasons for doing it in this particular order. When discussing next generation service procurement with MNOs and government agencies, it helps having interviewed the users first. Interviewing users first helps us develop a clear understanding of what the services in question actually are, and in which types of scenarios they will need to be employed. Additionally, the users and user organizations may know the most about their own activities, and less about the affairs of commercial and state actors, while commercial and state actors might know something about user requirements in addition to knowing their own and each other's business. The intuition here then being that information extracted from interviewing users is more useful when conducting interviews with commercial and state actors than information extracted in interviews with commercial and state actors is useful when conducting interviews with users. The reason for opting to interview commercial actors prior to interviewing state actors is perhaps less clear cut, although it is largely similar. We believe information gained from interviewing commercial actors will be more useful when conducting interviews with state actors rather than vice versa. This is because we believe the state actors to possess the most holistic view of the situation at hand, and, as such, we would like to be able to discuss the ideas and solutions presented by each commercial actor with them. Now, the assumption that state actors have a clear view of the whole playing field while each commercial actor only sees their own ideas and solutions is obviously a simplification. As is the assumption that users know little about the affairs of other actors in this space, as this may obviously vary heavily from interview subject to interview subject. However, in addition to the reasons previously stated, we make these generalized claims in order to be able to structure the interview process in such a way as to be able to focus our efforts on one compartmentalized part of the research at a time. With that said, when considering the limited time frame in which we conduct these interviews, as well as any potential unforeseen complications and delays when scheduling interviews, the strategy of interviewing one category of subjects at a time has to be adhered to as a guideline rather than as a strict rule.

## 3.3 Conducting the interviews

As mentioned in the preface to this thesis, the interviews are conducted by two interviewers with largely, although not entirely, aligned interests. While there are benefits to being two, there are also some pitfalls to be aware of, especially considering that while the two involved projects are related, they are still distinct. The most important aspect of the interview to keep in mind in order to ensure that both interviewers get something out of it is time. Keeping an eye on the time, and dividing it fairly between the two projects, is paramount to ensuring that both interviewers get the opportunity to engage the interview subject in their respective lines of questioning. In addition, the general execution of the interviews has to be planned and rehearsed in order to create a good conversational dynamic between us, the two interviewers, and the subject. This includes how we introduce ourselves and the project and how we, as the interviewers, communicate during the interview to ensure that it is conducted in an orderly fashion, for instance by indicating to each other that it is time for the first interviewer to wrap up their line of questioning in order to make room for the second.

Due to the pandemic, as well as other challenges related to traveling, the interviews are conducted by video conference. While this medium of communication is suboptimal in comparison to face-to-face interviews, as visual cues and body language may be more easily overlooked on video than in person [RM16], they are certainly practical. Barring any technical difficulties, conducting interviews over video conference allows much flexibility when scheduling and rescheduling appointments, especially when an in person interview would involve traveling to a different city. This added flexibility makes more potential interview subjects available to us that would otherwise be hard put to schedule an in person meeting, for instance due to them being unavailable during the limited time we would have been available in that particular interview subject's geographical vicinity.

To aid us in the conduction and subsequent analysis of the interviews, we record the audio of the conversations. Recording the sound of the interviews allows us to focus on what is being said instead of having to take extensive notes [Tjo20]. Considering the unstructured nature of our interviews, being able to concentrate on the conversations and to ask follow-up questions to what the subjects are saying is important to maximizing the informational value of the interviews. The ability to consult a source that does not consist of hastily scribbled notes and memories also helps when considering the technical nature of what is being discussed, as it will be easier to return to the source material at a later time with a different understanding of the underlying technical concepts. However, the employment of audio recordings as a tool does not come without its share of caveats. The most prominent drawback of using audio recordings is that the interview subject might restrict what they say

based on the fact that it will be recorded [Tjo20]. This is, however, a trade-off we are prepared to make in order to reap the aforementioned benefits of using audio recordings. Another challenge with recording the interviews is related to the privacy of the participants. We are committed to ensuring the privacy of our interview subjects, and do therefore delete the audio recordings after having transcribed them. The transcriptions make use of pseudonymization techniques in order to, to a large degree, eliminate identifying details. A more detailed description of the transcription procedure can be read in Section 3.4. The Norwegian center for research data (NSD) have been consulted in regard to processing the personal information of the participants as well as the recordings. The application for this project to the NSD, which was approved in November of 2020, can be seen in Appendix A.

As a final note regarding the conduction of interviews it should be pointed out that the interviews are being conducted in the Norwegian language. The reason for this is as simple as the fact that Norwegian is the mother tongue of both the interviewers, as well as of all the participating interview subjects. While this does not inhibit the collection of information in any degree, it does make it more complicated for non-Norwegian speakers to examine the collected data for themselves, as all the attached transcripts are in Norwegian. One thing that could potentially have an impact on the validity of the results is that excerpts taken from interviews and presented in Chapter 4 have had to be translated from Norwegian to English. However, we believe this impact, if it exists at all, to be negligible.

### 3.3.1 Continuous improvement of interviews and lessons learnt

It is no secret that the interviewers involved in this project are inexperienced in the discipline of interviewing. This means that a number of things are learnt as the interview process progresses, which subsequently are employed to improve later interviews. One of the most obvious, but also possibly one of the most impactful, is the mere sense of the interviewers growing more confident in their task of conducting interviews as more interviews are successfully conducted by them. This includes confidence in one's ability to ask poignant and carefully crafted questions, as well as developing an aptitude for asking follow-up questions to interesting remarks made by interview subjects in order to get them to elaborate on perceived topics of relevancy. In addition to the interviewers growing accustomed to the interview setting, later interviews also benefit from the fact that the interviewers have had more time to research the subject matter, and thus are able to ask better and more specific questions tailored to each interview subject in accordance with the current knowledge gaps of the interviewers.

The arguably most tangible and prominent improvement of later interviews as opposed to earlier ones is perhaps the one presented in Section 3.2 when considering

the ordering of interviews in relation to interview subject categories. Namely, that information discovered in earlier interviews may be used to improve questioning in later interviews. The questioning in later interviews could be improved both due to the fact that the interviewers then would have a more educated understanding of the subject matter in general, but also due to the interviewers then being able to ask for clarifications and elaborations on topics discussed with previously interviewed subjects, as many of the interview subjects possess somewhat overlapping areas of knowledge. For instance, when interviewing a subject they may introduce some technical term or solution that the interviewers have yet to discover. Given that this then is not the final interview of the project, the interviewers would be able to question other participants about this technical term or solution, and subsequently gain a deeper understanding of the subject matter that perhaps would not have been gained had that initial interview subject not introduced the interviewers to that particular technical term or solution. A natural consequence of this being, however, that any revelations unearthed in the later interviews will not be able to be discussed with previously interviewed subjects without conducting follow-up interviews. This is precisely why the order in which the interviews are conducted is important to consider and take note of, as discussed in Section 3.2.

Another of the lessons to be learnt is that it is difficult to completely avoid asking leading questions. We believe this to be mainly due to two facts. The first is that presenting your own understanding of technical solutions and subsequently asking the interview subject what they think of it seems like a good method for uncovering gaps and misconceptions in one's own knowledge, particularly when you consider the fact that the interview subjects in general are significantly more knowledgeable than the interviewers about the subject matter in question. Secondly, it is our belief that human beings have a tendency to seek affirmation in casual conversation, especially when speaking with someone of considerably higher standing, such as, in our case, experienced and knowledgeable interview subjects employed in respectable positions throughout government and the telecom industry. The implication here being that this could add an additional layer of difficulty to playing the part of interviewer, as one might in some cases need to suppress one's intuitive conversational tendencies.

Additionally, a lesson may be learnt regarding the added difficulty of formulating good questions when the interview subject does not immediately understand what you actually want to know. As in any form of conversation, the interview is dependent on a certain dynamic between the participating parties. Considering the in many cases significant knowledge gap between the interview subjects and the interviewer, it is a great help to the interviewer if the subject is able to understand and illuminate the underlying obstacles to understanding that the interviewer's questions suggest, instead of just answering the questions themselves. This might be particularly true for the earlier interviews, where the interviewers have had less time to familiarize

themselves with the subject matter and are generally less knowledgeable. Conversely, this implies that in a scenario where the interview subject does not pick up on this uncertainty on the part of the interviewer and subsequently tries to assist the interviewer in figuring out what they are actually wondering, the result might end up being a poorly worded question paired with an answer that does not touch on the core of the matter. Interestingly, this is one of the ways in which being two interviewers with adjacent interests could be a significant help, as the interviewers could help each other out with rephrasing and the like, should one of them get stuck on a attempting to ask a difficult question. The same is also true on the part of the interview subject, in regard to helping each other out, in the event that two or more subjects who are familiar with one another's respective fields of expertise are being interviewed together.

## 3.4 Processing the results

The qualitative research data analysis software Nvivo[1] is used to process the information accumulated during the interviews and to transcribe the audio recordings. After the audio recordings are transcribed they are deleted, and only the transcriptions are available for examination as appendices to this thesis. As mentioned in Section 3.3, we are committed to ensuring the privacy of the interview subjects who participate in our project. According to Tjora in [Tjo20], striking a good balance between preservation of privacy and effective communication of research data may in some cases be tricky. Despite this, we feel like we have reached a solid middle ground in terms of anonymization. Protecting the privacy of the participants in our project is important to us because many participants may be speaking in a mix between a professional and a personal capacity, and it is vital to the authenticity of the results of this project that the participants feel free to speak their mind.

In order to preserve the privacy of the participating interview subjects we employ a technique of pseudonymization to the transcriptions in which identifying details are substituted in favor of more general descriptions. For instance, each interview subject is presented by a general description of their role and relation to the topic at hand instead of by their name and the name of their employer. We do not publish any transcripts without their contents first being approved by the participating subject or subjects. As mentioned repeatedly, the reason for this is that we find it important to ensure that the interview subjects are comfortable about speaking to us without having to be concerned that the nature of their answers could lead to any consequences for them in their professional or personal lives. In order to earn the trust of the interview subjects parts of some of the transcripts are also redacted entirely in scenarios where subjects say things that they would rather not have said

[1] https://qsrinternational.com/nvivo

publicly. While it appears unlikely that all participants would have demanded a level of anonymity in order to agree to participate, due to the relatively harmless nature of the topics at hand, we still believe that awarding all participants the same unconditional anonymity is the most orderly way to go about it. Although generalizing the identities of the interview subjects by its very nature directly results in data loss, our belief is that many of the statements made by individual subjects can be considered to be representative for individuals sharing their generalized category, and that the contextual data loss resulting from generalization therefore can be expected to be small. For instance, we deem it probable that a systems architect working at an MNO share a number of opinions related to NGN with other systems architects working at MNOs. While this may not always hold true, we attempt to strengthen any claims of representativeness by interviewing multiple participants belonging to the same or similar generalized categories, observing what they do and do not agree on.

## 3.5 Comparing alternatives

In the social sciences, comparative research methods are often used to analyze differences between demographics, countries, viewpoints of political opponents, etc. While this project will attempt to compare deployment strategies and technological solutions for next generation public safety communications, there are some important lessons to be learnt from the social sciences where this type of comparative effort seems to be more common. The Writing Center at Harvard University provides us with some valuable insight into the general themes of comparative analysis [Wal98]. Firstly, there is a need to establish a frame of reference. In the case of this research project, this has already been presented quite comprehensively as the question regarding how to best solve the challenges related to the next generation of public safety communications in Norway. Secondly, the grounds for comparison has to be made clear. Which particular models will be examined, why, and which aspects of these models will be considered? As there are a significant number of potential ways to solve the problems at hand regarding NGN, a representative selection of models will have to be presented in order to facilitate the assessment and comparison of a variety of the qualities these models possess. For instance, going by the alternative deployment models presented in Section 2.1 with regard to [DSB18], a selection of a model in which the state acts as its own MVNO, a model with a single turnkey-provider, and a model involving a multitude of commercial providers could allow for the analysis of a number of interesting qualities of next generation PSNs in different relevant settings. Now, this is where the comparison criteria defined in Section 2.4 come in. These criteria represent the qualities of the models that will be examined, and thereby provide a common ground on which to compare the drawbacks and benefits of each of the models in relation to each other. Just like it is important

to justify the selection of models for comparison, the justification also has to be made for the selection of these comparison criteria. The reasoning behind selecting each of the comparison criteria can be examined in Section 2.4. Lastly, there are different organizational schemes for performing such a comparative analysis [Wal98]. Will each model be analysed in its entirety in turn, or will the focus be on one quality at a time, such that each model will be analysed in regard to the quality in question before moving on to the next quality? To better understand the differences and similarities between the models, we primarily concentrate on one comparison criterion at a time. Each of the models then have their qualities analyzed in regard to this one criteria, before taking a step back and looking at the models as wholes later, once all comparison criteria have been examined in detail.

It is vital to the integrity of this research that all evaluated models be analyzed on equal grounds. However, as with the conduction of interviews, there are several ways we as researchers may inadvertently introduce bias into the equation. Preconceived notions on the behalf of researchers may end up skewing anything from the attitude of the wording and the amount of allotted attention each topic receives to the conclusion itself. We believe this to be especially true in a study like this, where alternatives are to be compared against each other. A truth that is amplified by the fact that there are significant uncertainties associated with several of the qualities of the alternatives that are being used as a grounds for comparison. As an attempt to reduce the amount of bias each researcher's preconceived notions are able to introduce to the project, we define clear methods for comparison that are adhered to when presenting and discussing any findings. We also attempt to provide sufficient justification for the choices that are made, for instance in regard to the selected comparison criteria, as mentioned previously. However, the process of selecting these comparison criteria, no matter how justified, may also be susceptible to bias, as there is no guarantee that a selected comparison criteria will, in colloquial terms, treat all models equally. By this we mean that one selected set of comparison criteria may result in a favorable outcome for one of the models, while one of the other models perhaps would have fared better had another set of comparison criteria been selected. Unfortunately for us, this issue of bias seems, at least to some degree, intrinsic to the nature of conducting research like this. However, while we are unable to remove bias entirely from the equation, we attempt to mitigate it by justifying the choices we make, and we believe it important to be aware of in any research project.

# Chapter 4
# Results

In total, 16 interviews are conducted, two of which involve two interview subjects, bringing the total count of interview subjects to 18. This chapter presents the findings from those interviews, ordered by category of interview subject as described in Section 3.2. Selected excerpts from interviews regarding relevant topics are highlighted in tables throughout the chapter in an attempt to shed light on, among other things, the benefits and drawbacks of alternative deployment models for NGN. Five interviews are conducted with users and user organizations, six with commercial actors, and five with state actors. An overview tallying the number of interviews and corresponding participating interview subjects can be seen in Table 4.1. A more detailed overview separating the participating subjects into subcategories based on, for instance, which type of public service they represent can be seen at the start of each corresponding section. Additionally, complete transcripts of all interviews may be examined as appendices to the thesis. For the users and user organizations we present experiences with the existing Nødnett, as well as expectations and concerns in regard to NGN from the user perspective, while we, for the commercial and state actors, focus more directly on aspects of the alternative deployment models. Finally, at the end of the chapter we provide a short summary of the overarching themes of the findings in an attempt to establish a foundation before heading off into Chapter 5.

**Table 4.1:** Number of conducted interviews overall

| Subject category | No. of interviews | No. of participants |
|---|---|---|
| Users and user organizations | 5 | 7 |
| Commercial actors | 6 | 6 |
| State actors | 5 | 5 |

## 4.1 Users and user organizations

When interviewing users and representatives of the user organizations of the existing Norwegian Nødnett, questions are aimed at the discovery of current user behavior and needs, relations to commercial providers today, and expectations for 5G and NGN. All three primary emergency services are represented among the interviewed, in addition to the Norwegian customs authority. An overview of the distribution of interview subjects across different public services can be seen in Table 4.2. While all users of Nødnett have similar baseline needs and requirements in terms of reliable communications and interoperability between services and systems, the scenarios in which they utilize Nødnett's capabilities differ from service to service. The same can be said for what type of communications they value, as well as which actors from each service is involved in the communications flow during typical operations. For instance, while all interview subjects emphasize the need for PTT voice communications as a baseline requirement, their expectations of and subsequent expected reliance on other types of communications, such as video, differ.

**Table 4.2:** Number of conducted interviews of users and user organizations

| Subject subcategory | No. of interviews | No. of participants | Appendix |
|---|---|---|---|
| Police services | 1 | 2 | K |
| Fire and rescue services | 1 | 1 | J |
| Health services | 2 | 3 | B, D |
| Customs authority | 1 | 1 | C |

While the interviews with users and user organizations have not focused directly on specific deployment models, there are still some interesting pieces of information to take away in regard to more general expectations for NGN. However, as a natural consequence of this fact, the findings from interviewing users are not presented in relation to the comparison criteria defined for the deployment models. Instead, we present users' and user organizations' experiences with the current Nødnett and their expectations of NGN as a way to map out lessons learned and chart the way forward, before heading off into the lands of alternative deployment models.

### 4.1.1 Experiences with the existing Nødnett

In general, the conducted interviews show that users and user organizations are generally pleased with the performance of the existing Nødnett. A table containing some excerpts form the interviews regarding positive experiences with Nødnett can

be seen in Table 4.3. The superior quality of the group-based speech communication capabilities of TETRA is something several interview subjects emphasize as one of the key features of Nødnett. Another quality of Nødnett that the customs authority in particular remark on is Nødnett's extensive coverage is scarcely populated areas, such as along the border where the customs authority operate. This being particularly noticeable for the customs authority when compared to the radio communications systems they were using prior to Nødnett. Additionally, a feature of Nødnett that is brought up during interviews as a key to its success is the way in which Nødnett facilitates interagency cooperation through the use of shared interagency talk groups. In a similar vein of cooperation, the customs authority explicitly remarks on Nødnett's capability of sharing talk groups with authorities of neighboring countries through bilateral agreements [Appx. C, 12, 108].

**Table 4.3:** Positive experiences with the current Nødnett

| Reference | Comment |
|---|---|
| Customs [Appx. C, 9] | The sound was so much clearer and we had coverage where we hadn't had any coverage previously. |
| Health [Appx. D, 15] | There was much talk in the media about TETRA being old-fashioned. However, time has shown that the speech functionality in TETRA is superb. |
| Fire [Appx. J, 32] | [The interagency talk group] is commonly used in the initial phases of an incident, on the way out to the incident location, in order to give everyone a common understanding of the situation. |
| Police [Appx. K, 83] | What's most important for us in regard to NGN is to maintain the good experiences and the cooperative platform that the existing Nødnett has afforded us together with the other actors. |

However, while the PTT functionality in the network receives high praise, users are also painfully aware of the limitations of the TETRA technology. A selection of excerpts from the interviews regarding some of the critiques that are raised against Nødnett can be seen in Table 4.4. Critique is being directed towards Nødnett's ability to provide services more commonly associated with commercial mobile networks, such as one-to-one conversations and data services. The ladder has been a crux of Nødnett for a long time, and is frequently brought up as one of the main reasons fueling the need for NGN. This lack of data transfer capabilities in Nødnett is what has propelled public services towards commercial mobile broadband solutions. However, several interview subjects note limitations with these commercial solutions, citing in particular the difficulty of sharing information across agencies when every agency

has its own proprietary commercial solution [Appx. D, 26]. Some comments are also made about the user friendliness of Nødnett's user equipment, most notably by the fire brigade, as they employ a number of part-time firefighters who have limited training and experience with Nødnett. As suggested in [Appx. J, 40], it might for instance benefit these part-time corps members if the interfaces they use to interact with Nødnett would share a greater similarity with their personal mobile phones. Lastly, issues with the function in Nødnett which allows Nødnett terminals to call regular cellphones that are connected to commercial mobile networks are raised in [Appx. B, 19] in relation to ambulance workers needing to communicate with hospital personnel who do not necessarily carry their own Nødnett terminals.

**Table 4.4:** Negative experiences with the current Nødnett

| Reference | | Comment |
|---|---|---|
| Health | [Appx. B, 16] | Take for example doctors ... who often are in need of one-to-one conversations. This is an area where the system has shown itself to have some limitations, especially in regard to speech quality. |
| Health | [Appx. D, 15] | That's probably the biggest challenge with today's Nødnett. That it doesn't support the data and video services that the users are in need of. |
| Fire | [Appx. J, 34] | The problem is that [Nødnett's user equipment] isn't particularly user friendly. It's incredibly simple, yet still very complicated. There are a lot of menus and options to consider for a part-time firefighter. |
| Police | [Appx. K, 18] | We are, as of today, reliant on commercial actors [to provide data services,] and use ordinary 4G with the limitations that that entails. That's why we haven't made ourselves critically dependent on data services. |

### 4.1.2 Expectations and concerns in relation to NGN

Users and user organizations are in general heavily involved in the NGN project, and many of the interview subjects have expressed clear expectations for the new network. Some expectations are aimed at addressing previously presented limitations of Nødnett, while others relate to brand new possibilities, for instance in terms of new technological capabilities and functionality. A table containing some excerpts from the interviews regarding users' expectations of NGN can be seen in Table 4.5. The limitation of Nødnett in regard to bandwidth is obviously the main challenge expected to be solved by NGN, but several of our interview subjects mention the possibility of, for example, improving on various aspects of the Nødnett user experience as well.

Video, in the form of body cameras or such, appears to be the most interesting use case for the interview subjects in general, along with the improvement of systems providing mission specific information such as maps and other contextual information. The latter being what is typically provided by way of commercial providers as a supplement to Nødnett today. On that note, a previously noted limitation of such commercial solutions is the difficulty of sharing information across agencies. One of the expectations that several interview subjects have of NGN in exactly this regard, is that sharing video and data across agencies will become easier once you get rid of proprietary commercial solutions and implement standardized systems communicating over a common network. We also discuss the possibilities for using NGN to connect aerial drones with different types of video cameras attached in several interviews [Appx. K, 79].

**Table 4.5:** Users and user organizations' expectations of NGN

| Reference | | Comment |
|---|---|---|
| Health | [Appx. B, 67] | As long as the functionality, the information security, and the availability are safeguarded [the deployment model doesn't matter as much.] |
| Health | [Appx. D, 46] | The better the systems get ... the more difficult it will be to go back to the way things were before. The hypothesis being that while [video and data services] aren't mission critical today, they will soon become so. |
| Fire | [Appx. J, 70] | In many ways, I think that [video] is more important than speech. There will of course be some dialogue ... but I think that the control room may benefit just as much from actually seeing what's going on. |
| Police | [Appx. K, 82] | The benefit of a new network won't be that we get a new platform for talking together, but that we get joint applications that contribute to information sharing across agencies. |

In regard to possible improvements on the Nødnett user experience, seamless transitions between different types of communications according to situational needs is one point that is brought up in [Appx. B, 26]. An example of this could for instance be that a talk group of ambulance workers need to include doctors or other non-Nødnett proficient personnel in the conversation, and thus have to switch the conversation from being PTT to being a regular conference call involving cellphones connected to the commercial network as well as Nødnett terminals connected to Nødnett [Appx. B, 22]. In general, there appears to exist a clear expectation among

users that NGN should be at least as good as Nødnett, for instance in terms of coverage and availability, and then for the new services, such as video, to further strengthen the operational capabilities of Norwegian public safety actors as an addition to already existing capabilities.

Unsurprisingly, users and representatives of user organizations also raise some concerns in regard to NGN. The discovery of such concerns is an important step towards deciding on the particulars of NGN, such as deployment model, and must be taken into account by decision makers in order to ensure the continued success of public safety communications in Norway. Table 4.6 shows some selected excerpts from the interviews in regard to potential concerns of NGN. While multiple interview subjects have stated that the particulars of the final deployment model are of no interest as long as the users can trust the network to be available, secure, and provide the best functionality [Appx. K, 69], they still note some important points about, for instance, how we might, in some regards, be putting all our eggs in one basket by eliminating today's redundancy of having a commercial network to fall back on in case the dedicated network for some reason fails [Appx. B, 53].

**Table 4.6:** Users and user organizations' concerns for NGN

| Reference | Comment |
|---|---|
| Health [Appx. B, 53] | If Nødnett is down you still have your mobile phone as a backup, and you still have the data services. If we transition to using an operator who is the same as the one providing the commercial mobile network, we won't have that backup. |
| Customs [Appx. C, 54] | We have to have as good a coverage along the Swedish and Finnish border as we have today, and continue the cooperation with Swedish and Finnish customs and police authorities. |
| Health [Appx. D, 39] | There exists some functionality in the current Nødnett ... such as an AGA network, which enables us to communicate with helicopters, that doesn't exist in commercial networks. |
| Police [Appx. K, 73] | We have to, in a way, ensure that it won't be possible to discern where the police has been ... in such a way that we aren't putting people's privacy at risk or risk this information being used for criminal purposes. |

As mentioned previously, the interview subjects show a strong desire for pre-

serving the benefits the current Nødnett has given them when transitioning to a new technology. The customs authority, for instance, emphasises the importance of preserving the comprehensive coverage along Norway's borders with Sweden and Finland, as well as keeping up the close cooperative work our interworking TETRA networks have allowed for. Such cross-border interoperability relies on neighboring networks being implemented according to compatible standards, which introduces a concern in and of itself [Appx. D, 44]. One important point that is brought up relates to the difference in expected functionality between Nødnett and commercial networks, for instance in the case of Air-Ground-Air (AGA) networks that allow for communications between helicopters and personnel on the ground, as something that has to be addressed when transitioning to commercial networks. There are also some concerns in regard to information security once commercial providers are introduced into the mix. In particular, the police might conduct covert operations that require complete confidentiality not only in terms of encrypted communication channels, but also in terms of metadata regarding this communication. If a commercial operator is involved in the core network of NGN, mobility information might be something that could potentially be available in that operator's systems, despite the contents of the communication being end-to-end encrypted. Lastly, some general concerns are voiced in regard to the commercial operators willingness to spend exorbitant amounts of money on robustifying their networks, as well as letting the relatively small user base of Nødnett users take priority over the operator's paying customers. Among others, both of these last two concerns give rise to questions regarding the necessity for regulations to be imposed [Appx. D, 31, 39].

## 4.2 Commercial actors

All three Norwegian MNOs are represented among the interviewed, along with one representative of a Norwegian MVNO and one representative of an infrastructure equipment provider. An overview of the number of conducted interviews and the appendices in which transcripts from these interviews may be viewed can be seen in Table 4.7. As each interview is conducted with a single person, the column detailing the participating number of interviews is left out. Each Norwegian MNO has delivered their own suggestion to DSB for how to proceed with NGN. As such, the interviews focus on questioning each of these proposed models, as well as on gaining insight into more general topics related to challenges and opportunities presented by NGN and 5G technology. In addition to questioning the MNOs relationships to the state, the MNOs relationships to each other are questioned in an effort to understand potential interoperability challenges and certain competitive aspects in the Norwegian telecommunications market. Furthermore, an MVNO is interviewed in order to obtain a clearer view of what an MVNO might look like in the 5G ecosystem, and what it could entail for DSB to operate it's own MVNO as a part of NGN. Lastly,

an infrastructure equipment provider is interviewed to increase our understanding of technological challenges related to 5G and NGN, as equipment providers are the ones who will be delivering this technology to the operators.

**Table 4.7:** Number of conducted interviews of commercial actors

| Subject subcategory | No. of interviews | Appendix |
|---|---|---|
| Mobile network operator | 4 | E, F, I, L |
| Mobile virtual network operator | 1 | G |
| Infrastructure equipment provider (IEP) | 1 | Q |

Something that is worth keeping in mind while examining arguments proposed during interviews in favor of or against certain deployment models, is that there might be some overlap in argumentation in terms of pros and cons. An argument that could be considered to be in favor of one model, might at the same time be considered to be in opposition of a competing model. As there is an attempt made to avoid too much repetition of seemingly identical argumentation, the results presented in regard to alternative deployment models in this section have to be considered as a whole. To give an example, an argument presented as a drawback of involving multiple operators in NGN could, on the other hand, perhaps be considered to be an argument in favor of the alternative of only involving a single turnkey provider.

### 4.2.1 The single turnkey provider model

One of the possible solutions for how to proceed with NGN involves the employment of a single turnkey provider. This implies that the state would task one of the Norwegian MNOs with delivering the NGN solution in its entirety. Such an approach is argued in favor of most prominently by the representative of a Norwegian MNO interviewed in Appendix E. Some of the apparent benefits of selecting a model for NGN such as this can be seen in Table 4.8. Interestingly, one can already observe the previously mentioned cross contamination of argumentation, as it is difficult to consider the benefits of a turnkey model without also considering the alternatives.

The overarching theme regarding the single turnkey provider model seems to be that it could provide a solid and, most prominently, less complicated foundation for NGN. As can be seen in the excerpts from interviews presented in Table 4.8, arguments revolve around the fact that the more operators you involve in a technical solution, the more complicated it gets. However, as can also be noted from the comments presented in the table, this simplicity does not necessarily come without sacrifices. In particular, it is noted in [Appx. F, 16, 52] that while opting to go for a single turnkey provider may provide you with the best and simplest solution, you

**Table 4.8:** Arguments in favor of a turnkey provider model

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. E, 7] | We observe that a turnkey model provides synergy and an improved overall experience, for instance in terms of interoperability on several levels. A multi-operator model is not an impossibility, but it makes things more difficult. |
| MNO | [Appx. E, 62] | [A multi-operator model] requires coordination between involved providers that are not necessarily interested in cooperating, as they are competitors in other areas. |
| MNO | [Appx. F, 16] | [A turnkey provider model] won't give you interoperability issues, but could give you vulnerability issues. |
| MNO | [Appx. F, 52] | The mainstream solution is to give it all to one [provider]. That will give you the fastest deployment, but also the lowest level of robustness and diversity. |

could risk ending up with an overall worse solution, as you give up benefits relating to, for instance, robustness and diversity that could have been gained by involving more than one provider.

In regard to the arguments opposing a single turnkey provider model more explicitly, there seem to be two concerns that stand out. The first is the one covered by the first two quotes in Table 4.9, and the second is covered by the last two comments. As put by a representative of an MNO in [Appx. I, 40], if the state awards a long-term contract for the delivery of NGN to a commercial provider, the concern is that that provider will have little incentive to continuously develop and improve their delivery, as the likelihood that there would exist any significant amount of threatening competition would be slim. In this regard, the state, by selecting a model such as this, could potentially end up as the victim of severe supplier lock-in effects. A similar concern is put forward by a representative of a Norwegian MVNO in [Appx. G, 16]. Due to the nature of the state's procurement process, the state would likely need to develop a complete specification that they would then task a single provider with delivering. As such, the representative of the MVNO argues, what you specify is what you get, and there would be little incentive for the turnkey provider to deliver anything more than what has been agreed upon in advance.

The second opposing argument expressed by interview subjects in regard to the

**Table 4.9:** Arguments opposing a turnkey provider model

| Reference | | Comment |
|---|---|---|
| MVNO | [Appx. G, 16] | If Nødnett is bought from a single provider ... it will become very static. You've provided a spec, and then that is what you get. There won't be any development. |
| MNO | [Appx. I, 40] | [If a single provider is awarded a twenty-year contract], how interested would they be in developing the solution? In providing a quality service? They can't be switched out. There is no competition present. |
| MNO | [Appx. F, 14] | State-funded investments into the strengthening of radio networks in sparsely populated areas will disrupt competition if they're awarded to a single provider. |
| MNO | [Appx. I, 8] | If the state buys the service [from a single provider], and invest in the robustification of a single network, they will have destroyed the competition in the Norwegian mobile market for the foreseeable future. |

turnkey model, concerns the consequences the selection of such a model could have on competitiveness in the Norwegian commercial mobile market. These consequences could potentially be so severe that it is argued by a representative of an MNO that this concern trumps any other technical considerations made in relation to the single turnkey provider model [Appx. I, 8]. Specifically, the concern regards how state-funded investment into the robustification of radio networks could give the selected turnkey provider a significant competitive advantage in the commercial telecom market. As mentioned as a prime example in [Appx. F, 14], state-subsidization of infrastructure development in remote and sparsely populated areas would turn the business case for otherwise unprofitable endeavors completely on its head. Instead, it is argued in [Appx. F, 28], state-funded investment into the strengthening of telecom infrastructure should be awarded to every MNO in turn. Such a solution, it is argued, could preserve competitive relations in the commercial market while still providing NGN with the required robustness and coverage. While this directly implies that NGN would have to make use of all three Norwegian RANs, consensus throughout interviews seems to be that that is not something that should be an issue. In fact, as eloquently put by a representative of an MNO in [Appx. I, 8], not making use of something as simple as traditional roaming techniques in order to ensure that NGN has the best possible coverage would be completely crazy.

### 4.2.2 Pros and cons of involving multiple providers

As an alternative to only enlisting the services of a single provider, solutions involving multiple providers have been proposed. In particular, in the interview which may be examined in detail in Appendix I, a model is proposed which involves all three Norwegian MNOs supplying a full stack of services for NGN purposes. It is proposed that public safety agencies could then choose which provider they would like to purchase their services from, and that interagency cooperation between agencies supplied by different providers could be ensured through a common MCX application implemented across the top of the three networks [Appx. I, 12]. While it is emphasized by the interview subject in question that this model is being proposed with mercantile considerations in mind, in regard to how the previously mentioned turnkey provider approach could end up disrupting the commercial telecom market in Norway, there is also an argument to be made for the robustness the use of multiple core networks could add to an NGN solution [Appx. I, 20]. A couple of comments regarding this use of multiple networks can be seen in Table 4.10.

**Table 4.10:** Arguments in favor of involving multiple providers

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. I, 18] | We realize that [a multi-provider model] is a more complex alternative. However, three independent systems gives you an overall improved availability compared to just a single one. |
| MNO | [Appx. I, 20] | How are you going to make sure that the public safety agencies over time get the best possible communications services? Why wouldn't you compete on service offerings? |

There are two main arguments for using the full stacks of multiple providers. As mentioned, the argument concerning the conservation of competitiveness in the commercial mobile market is one, with the argument of added robustness by being able to make use of more than one provider's core network being the other. While you would still expect core networks to fail as often as you would in a model relying on a single network, this multi-network approach allows two thirds of your user base to stay connected in the event of such an outage, given that the public safety agencies are evenly spread out across all three providers [Appx. I, 18]. A suggestion, also given in [Appx. I, 18], for how this third of the user base may even continue to stay connected in a scenario where the provider they rely on is unable to provide service, is to simply borrow a terminal from or cooperate with sibling agencies who are subscribed to other providers. Regardless of the benefits of this added robustness, however, a model like this, which involves multiple providers, must be considered as

a way to deal with the potential mercantile challenges of alternative models, such as any kind of turnkey-type model. The comment from which the second excerpt in Table 4.10 is taken reminds us that competition could very well be a powerful driver for the quality of the available service offerings.

**Table 4.11:** Arguments opposing the involvement of multiple providers

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. E, 60] | If your two providers start implementing tailored solutions between themselves ... you might end up just as locked in to those two, as you would have been to one. |
| MNO | [Appx. I, 20] | You are going to get interdependencies [between the networks]. Do they support the same types of functionality? What happens when one network provides more functionality than another? |
| MNO | [Appx. L, 43] | You always have redundancy in the core network. Geographically, for instance, such that [all your core sites] don't get affected by the same blackout. |

Naturally, a deployment model involving a multitude of providers also carries some downsides, as alluded to by the first half of the first comment in Table 4.10, stating that the interview subject realizes the model in question to be one of the more complex alternatives for NGN. Table 4.11 lists some excerpts taken from interviews that regard concerns of involving multiple providers in the NGN solution, both in general, and in particular relation to the aforementioned multi-network approach. Firstly, starting with the uppermost comment in Table 4.11 taken from [Appx. E, 60], the supplier lock-in argument that was noted as a potential drawback of the single turnkey provider model could also, in some circumstances, end up applying to a solution involving multiple suppliers. As mentioned by the interview subject, there is a risk that suppliers will have to develop tailored interfaces to get their different systems to work together, and that they, in doing so, could make you just as locked in to several suppliers as you would have been to a single turnkey one. In somewhat the same vein, but more specifically directed towards the multi-network approach described earlier, the second comment in Table 4.11 expresses concern over the potential complexity that could be incurred by your three providers not having implemented the same types of functionality in their networks. The comment notes how this complexity could potentially end up in the hands of the control rooms of the public safety agencies, for instance, by forcing them to make decisions about which network to use for interagency cooperation. Lastly, a comment from Appendix L states that the MNOs core networks already are subject to a number of robustness

measures. While the proposed multi-network model might be referring to software problems rather than blackouts when talking about incidents that could take down an entire network, it is worth considering the possibility that there could be other ways of ensuring service availability in the face of core network failures, apart from using a full stack at every Norwegian MNO.

### 4.2.3 Considerations regarding a state-owned MVNO

Regarding alternative deployment models, there is also the question of whether or not the state should own or operate its own MVNO. Of our pool of interview subjects, the commercial actors the ones who are the most intimately familiar with the intricacies of operating mobile network today. As such, an area that is of particular interest when interviewing subjects of this subject category, are the possible solutions one could envision for a state-owned MVNO, as well as the benefits and drawbacks of such solutions. The representative for an MNO interviewed in Appendix F proposes a deployment model where the state establishes its own MVNO, and subsequently makes use of all three Norwegian radio networks. Thus, it is argued, you could deploy a solution which would preserve competition in the commercial Norwegian telecom market, while at the same time avoiding the technical complexities of a multi-operator model [Appx. F, 10]. It is proposed that such a model could make use of an NGN specific Public Land Mobile Network (PLMN) code defined in such a way that it would make terminals associated with NGN able to treat all three Norwegian RANs as their home network [Appx. F, 14]. Some excerpts from interviews that consider the possible benefits of an MVNO solution can be seen in Table 4.12.

There are a couple of key considerations made by the comments contained in Table 4.12, some of which, incidentally, touch directly on some of the comparison criteria defined in Section 2.4. While the comment made in [Appx. F, 10] claims that an MVNO solution could allow you to spread yourself across all commercial networks without having to worry about the technical challenges of a multi-operator approach, it might be worth questioning whether or not DSB as an organization possess the capabilities required to establish an MVNO themselves. In an attempt to dissuade any such notion, a comment made in [Appx. F, 26] professes confidence in DSB's ability to run an MVNO themselves. A sentiment which is backed up by a representative of an MVNO in [Appx. G, 43]. Additionally, in this same comment made by a representative of an MVNO, it is suggested that large contractual agreements entered into with correspondingly large providers could hamper the long-term quality of the NGN solution by restricting flexibility and possibilities for development. In addition to these arguments in favor of an MVNO solution, the last comment highlighted in Table 4.12 touches on the topic of state control and the potential security benefits associated with state control. As less of the solution's network functionality would be hosted by commercial operators, it could be argued that a state-owned MVNO

**Table 4.12:** Arguments in favor of an MVNO solution

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. F, 10] | [By using an MVNO] you get the strength of three [radio networks] ... without having to think about things like interconnection [between multiple operators]. |
| MNO | [Appx. F, 26] | DSB already have experience with the TETRA network. The challenge for an operator is always robustness ... but I think that DSB is a professional organization who will handle that nicely. |
| MVNO | [Appx. G, 43] | I think that if you want flexibility you have to take control yourself. You want partners, not suppliers, if you want to get anything done with this PSN aside from the basics. |
| MNO | [Appx. F, 10] | An MVNO model would ensure confidentiality by encrypting traffic that passes through the operators' networks. Even mobility data could be safeguarded if you include the AMF in the MVNO. |

enables the state to keep closer tabs on, for instance, the people who have access to sensitive information regarding the communications of NGN. The comment also mentions how the state could even safeguard mobility data if they were to include their own AMF in the state-owned MVNO, thereby creating a MOCN type setup.

As with all the alternative deployment models there are both benefits and drawbacks to the establishment of a state-owned MVNO. A selection of arguments put forward by interview subjects opposing an MVNO solution are presented in Table 4.13. While the first comment in the table could perhaps be considered to be stating the obvious, it might be valuable to think of it in comparison to the previously mentioned multi-operator model. One of the presented benefits of the MVNO model is that it could alleviate some of the technical challenges related to a model like the multi-operator one. However, as pointed out in [Appx. F, 16], the associated drawback of this benefit is that you will not have other networks to fall back on should your own MVNO solution for some reason fail. As an additional argument attempting to dissuade the state from establishing their own MVNO, a comment made in [Appx. I, 8] suggests that the state should leave the mobile networking to operators, and instead focus on controlling the service through carefully crafted requirements and agreements. It is argued that choosing to establish a state-owned MVNO could contribute to the risk of ending up with an out-of-date solution, as the

**Table 4.13:** Arguments opposing an MVNO solution

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. F, 16] | [If you are sitting] on top as an MVNO you could experience downtime in all networks in the event that you mess things up. |
| MNO | [Appx. I, 8] | Make SLA-based demands [of providers instead of doing it yourself]. Make use of the continuous development work that operators are doing, instead of ending up [with a network] that is outdated before it is completed. |
| MNO | [Appx. I, 121] | Whether the MVNO of tomorrow [will make use of the NEF], or if it will still be like a traditional MVNO that has its own core network infrastructure, I'm really not sure. |

state would not be able to keep up with the operators' continuous development work. The TETRA based Nødnett is mentioned as an example of a system which over time has become outdated in comparison to commercial offerings when it comes to broadband services. Moreover, the final comment highlighted in Table 4.13 touches on an interesting point regarding the debate of whether or not a state-owned MVNO is a good idea. While can perhaps not be considered to be an explicit argument in opposition of a state-owned MVNO, it is definitely worth noting that several interview subjects have noted how the constitution of an MVNO in 5G is something of which the details are still not known [Appx. L, 13].

**Table 4.14:** Comments regarding a MOCN based solution

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. L, 11] | The operator will have more information about your location etc. compared to if you're hosting the AMF in your own network. |
| MNO | [Appx. L, 17] | [A MOCN solution] gives you a much closer integration, as you have a direct connection from the RAN to your own AMF. So it demands much more coordination [between you and the operator]. |
| MNO | [Appx. I, 125] | It's not a given that we will allow someone else's AMF to be in our network and talk to our base station. |

Hosting your own AMF as an MVNO was mentioned in [Appx. F, 10] as a potential way to ensure the confidentiality of mobility data. While this may very well be a sound solution, as pointed out by the first comment in Table 4.14, the other highlighted comments attempt to shed light on some potential drawbacks of such an approach. First and foremost, comments suggest that a taking a MOCN approach to this problem could result in a significant amount of added complexity to the overall MVNO solution. [Appx. L, 17] remarks on how connecting your own AMF directly to the base stations create some complicated interdependencies between your own core network and the core network of the operator you are collaborating with, as any changes being made in the RAN would have to be accounted for by both core networks. The approach is elaborated on in [Appx. L, 25], where it is described as being perhaps one of the more complicated solutions in question, and as something that demands a great deal more expertise of DSB than a regular MVNO setup would. To further complicate matters, combining multiple operators' RANs with a solution like this could turn out to be quite challenging. It could, for instance, necessitate having a separate AMF for each of the RANs you want to connect to, as using the same AMF on multiple RANs could create interconnections between operators' networks in an undesirable way [Appx. L, 76-78]. As a final and similar note to how the specifics of regular type MVNOs in 5G are still somewhat unknown, so too are the specifics regarding this type of MOCN approach. The last comment highlighted in Table 4.14 emphasize how MNOs might not even accept that someone else's AMF is directly connected to their base stations, and as such it remains to be seen if the MOCN approach is something that is eligible for use at all.

### 4.2.4 Slicing and edge functionality

In addition to matters directly concerning alternative deployment models for NGN, other topics related to 5G and PSNs in general are also discussed with commercial actors. As the deployment of a PSN in commercial networks presupposes that operators will, in some way, be able to separate the public safety related traffic from the commercial traffic flowing through their networks, one topic that comes up in discussion during interviews is 5G network slicing technology. While it is noted in comments like [Appx. E, 11] and [Appx. I, 14] that slicing is merely one of the ways in which operators can achieve the necessary traffic isolation, slicing is suggested as a useful way to think about a collection of conceptually related technologies. Some comments regarding the usefulness of network slicing can be seen in Table 4.15. The feature that is most prominently put forward by interview subjects is the way in which slicing allows you to direct traffic in a certain slice to specific network components in the core network. As pointed out by both comments highlighted in Table 4.15, this allows public safety communications to be routed to dedicated network components that could, for instance, only be accessible to specially authorized personnel. It is argued that this could contribute to the overall security of the system by making it

easier to ensure confidentiality, as well as to the robustness of the system by allowing for the use of dedicated core infrastructure.

**Table 4.15:** Comments regarding 5G network slicing

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. I, 14] | A slice allows you to select which core network components will serve that slice, [and as such] could contribute to the operational security [by letting you use dedicated components and personnel]. |
| MNO | [Appx. F, 44] | The slice could send you to your own core network which you could then secure in your own way. I think the slicing will give you the robustness [NGN] requires. |

Another topic that is discussed in interviews in addition to slicing related concepts, are the challenges and possible solutions related to how functionality could be implemented in the network edge in NGN. While solutions that make use of edge computing to lower latency and increase throughput are relatively straight forward to implement, the NGN related functionality of autonomous base stations is not. As noted by the interview excerpts presented in Table 4.16 there are a number of related concerns to address, for instance in regard to the fact that an autonomous edge solution would most likely require at least some of the subscriber database to be stored in the edge. [Appx. F, 20] points out that, while user plane functions are usually the one's being distributed in network edges in order to lower latencies, an autonomous edge would likely require the distribution of control plane functions that are not typically intended for distribution, such as functions dealing with authentication of subscriber. Additionally, the second and third comment highlighted in Table 4.16 note how distributing sensitive information, like subscriber information and authentication keys, could pose a security risk, as it would likely be difficult to secure every edge site in the same way you would be able to secure your centralized core network. The biggest questions related to the edge in regard to some of the previously mentioned deployment models involving either multiple operators or a state-owned MVNO, however, are perhaps the one's posed in [Appx. E, 56]. For instance, in a deployment model where the state is its own MVNO and has its own core network, will they also own edge infrastructure as an extension of that core network in order to provide autonomous operation in the edge, or is that something they would leave up to their partnered operators? It is suggested by the same interview subject posing these questions that this might be an area in which the turnkey provider model could save the state some headaches, as the turnkey provider would naturally also be responsible for what happens in the edge. In terms of the other deployment models

it is admitted in [Appx. G, 24-27] that autonomous operation in the edge might be a difficult case to solve in an MVNO model. However, it might also be that it simply is a difficult case for every type of model, as it is noted in [Appx. F, 22] that the conundrum of the edge is still one that remains to be solved by operators in general.

**Table 4.16:** Comments regarding edge solutions in NGN

| Reference | | Comment |
|---|---|---|
| MNO | [Appx. F, 20] | The greatest challenge for full autonomy is to move the HLR/HSS type functions all the way out [into the edge], as they are functions that are typically centralized. |
| MNO | [Appx. I, 66] | Whenever you decide to distribute information where you're keeping secrets, the risk of leaks increases. |
| IEP | [Appx. Q, 56] | When you have authentication vectors and the likes stored in the core network [in the edge], you don't want to have many lying about if someone tries [to steal them]. |
| MNO | [Appx. E, 56] | Who is going to pay for [a core network in the edge], and who is going to operate it? Suddenly your deployment models are starting to get more complicated, which is why we prefer a turnkey solution. |

## 4.3 State actors

The state actors subject category contain three different subcategories. As DSB is the primary actor related to NGN, as well as being responsible for the existing Nødnett, the majority of interviews in this subject category are held with them. In addition to DSB we interview on representative of Nkom, which acts as a regulator and supervisory authority for the Norwegian telecommunications industry, as well as one representative of the Norwegian defense sector. An overview over the conducted interviews and the appendices in which transcripts from these interviews may be viewed can be seen in Table 4.17. As all interviews being conducted in this subject category are conducted with a single interview subject, the column detailing the number of participants for each interview has been left out.

A variety of subjects are discussed when interviewing employees of DSB, Nkom, and the Norwegian defense sector. These are knowledgeable people, many of whom have been involved in Nødnett and related affairs for a significant amount of time. As such, there is a clear interest in collecting information in regard to these subjects'

**Table 4.17:** Number of conducted interviews of state actors

| Subject subcategory | No. of interviews | Appendix |
|---|---|---|
| The directorate for civil protection (DSB) | 3 | H, M, N |
| The communications authority (Nkom) | 1 | P |
| The Norwegian defense sector | 1 | O |

experiences with the existing Nødnett, both technical and operational, as well as reflections surrounding NGN and the future of public safety communications.

### 4.3.1 On the topic of Nødnett and TETRA

As several of the interview subjects have been working with Nødnett for many years, gathering information regarding their experiences with Nødnett and the TETRA technology could assist us in developing a better understanding of the strengths of Nødnett that one should attempt to carry over to NGN, as well as the limitations of the TETRA technology that NGN will address. Examining the circumstances surrounding the establishment of Nødnett could perhaps also give us some pointers in regard to considerations that should be made anew in connection with the establishment of Nødnett's successor. A collection of comments regarding Nødnett and the TETRA technology can be seen in Table 4.18.

By now we know that the main reason emergency services would like to get off TETRA and on to 4G and 5G is that the TETRA technology does not offer satisfactory data transmission capabilities and, as pointed out by a representative of DSB, that technological developments in the TETRA space are few and far between. However, it is by no means a given that the TETRA network will be switched off as soon as the contract with the current operator, Motorola, runs out at the end of 2026. In response to a question regarding DSB's operational capabilities it is said that every possibility should be considered, even the ones where the state takes over the operation of the TETRA network themselves once the Motorola contract is up [Appx. M, 21]. It is however noted in the same reply that this would require the state to recruit additional staff with the goal of establishing an operational environment in mind, as such capabilities do not exist as of today.

As mentioned, an attempt is also made to gain insight into the circumstances surrounding the decision making process that led to the current Nødnett turnkey contract. The interview with a representative of DSB found in Appendix N is particularly permeated with information on this topic. The argument of state control is given as a reason for why the decision was made for the state to own the TETRA

**Table 4.18:** Comments regarding Nødnett and TETRA

| Reference | Comment |
|---|---|
| DSB [Appx. M, 6] | The TETRA technology is a mature technology, albeit a bit stale. There aren't really any new developments going on there. |
| DSB [Appx. M, 21] | After 2026, if we were to prolong the lifetime of the TETRA network, the state could take on Motorola's role as operator themselves. Considerations would have to be made, and an operations environment would have to be established. |
| DSB [Appx. N, 9] | [When deciding on a contract for Nødnett] the most important factor was probably risk. The division of responsibilities, and that the state shouldn't take on too much risk by being a systems integrator. We wanted a single provider to point to as responsible for the end-to-end services. |
| DSB [Appx. N, 15] | The current technology is much more modular [than it was back when Nødnett was established]. There are a lot more open interfaces and greater diversity. |

network itself, in addition to the fact that the state was willing to finance the project in its entirety [Appx. N, 9]. As for why the state chose to delegate the operation of Nødnett to a turnkey provider, the primary reason is given in short in the third comment of Table 4.18. Instead of taking on the responsibility of delivering the end-to-end service themselves, the state decided it would be better to leave this up to a commercial provider. Included in this task of ensuring the quality of the end-to-end services, the commercial provider would be responsible for integrating all the moving parts of Nødnett that came from separate subcontractors with each other. These moving parts included the network itself with its accompanying terminals, as well as the control rooms, whose inclusion resulted in a lot of added complexity to the project [Appx. N, 11]. This task of integrating the different components of the system was not something the state was keen on taking on themselves.

Looking to the future it is noted that technology in general has developed a lot since the inception of Nødnett. Technology has become more modular, more diverse, and there is a greater emphasis on open interfaces [Appx. N, 15]. When Nødnett was first established as a TETRA network the technology employed was decidedly different from the commercial GSM networks of the time. However, now that the worlds of public safety communications and commercial telecom are converging,

the denizens of the former may be able to reap the fruits of the latter in the form of a larger market and abundant technological development. However, it is noted with emphasis that we still do not know how similar next generation public safety technology will in fact be to that which is being offered to the mass market [Appx. N, 15].

### 4.3.2 On the involvement of the state

One of the central areas of interest for this project is to gauge the appropriate degree of state involvement in the establishment and operation of NGN. Which components, if any, should the state consider owning themselves, and should the state, for instance, take on the task of operating parts of NGN themselves, rather than leaving it up to a commercial actor? In this same vein, what are the benefits and drawbacks of the state establishing their own MVNO in relation to NGN? Some comments which are made during interviews in regard to this topic can be seen in Table 4.19.

**Table 4.19:** Comments regarding state involvement in NGN

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. M, 23] | We're looking at having some infrastructure of our own, regardless of who's operating and owning [NGN]. There has to be a strong degree of state control ... We have to safeguard the security, and that the solution is good and stable. |
| DSB | [Appx. N, 19] | [Establishing an MVNO] isn't an issue in and of itself. The question is whether or not the state is willing to take on such a responsibility. |
| DSB | [Appx. M, 31] | You can't say that you need to have an MVNO because it is the most secure. We think that that is a conclusion we cannot draw. |
| Defense | [Appx. O, 24] | We are not going to operate an MVNO. Our core business is warfare, not operation of 5G networks or data centers. |

As one can tell from the comments presented in Table 4.19 there are a number of considerations to be made in regard to the appropriate degree of state involvement in NGN. The argument pulling in favor of more state control and even a state owned MVNO is that of control. Multiple representatives of DSB emphasize the importance of the state having a controlling influence on the operation of NGN. However, whether or not achieving an appropriate level of control necessitates a state controlled MVNO as the primary proprietor of NGN is less clear. Representatives of DSB state that

they think a lot of the challenges related to control can be solved by entering into solid contracts with providers and vendors [Appx. M, 31], although it is also noted that contractually obligated control may not be as good as the real thing [Appx. N, 21].

Another aspect of the state-owned MVNO debate is that which is pointed out by the representative of the Norwegian defense sector in [Appx. O, 24]. Namely, that the operation of 5G networks, data centers, etc. are not part of the armed forces' core business, and should therefore be left to professional operators. The argument being that this would most likely be both cheaper and better than if they were to do it themselves. In relation to this it is mentioned in [Appx. N, 19] that the state has to consider whether or not they are willing to take on the responsibility of being an MVNO in this space, as that would then leave them directly responsible for the end-to-end user experience. However, one important point that is noted, in particular in [Appx. M, 75], and that could potentially be of consequence when considering whether or not to establish a state-owned MVNO, is that the question of what being an MVNO in 5G entails is still somewhat shrouded in mystery.

**Table 4.20:** Comments regarding a MOCN solution to NGN

| Reference | Comment |
|---|---|
| Defense [Appx. O, 87] | Organizational control and organization of personnel [at the MNOs] is important. A mobile network will always know where you are. That is the whole foundation of how handover and such works. |
| DSB [Appx. M, 27] | MOCN is technically and operationally more demanding than traditional roaming, [as you will be] integrating yourself closer to the radio network of your operator of choice. |

Furthermore, there is also the question of a traditional MVNO style solution versus more of an MOCN setup. While it was previously mentioned that uncertainty still reigns in regard to the constitution of an MVNO in 5G, the separation between an MVNO and an MOCN setup is here made in terms of who controls the AMF in the core network. This is a relevant question because the AMF will, by nature of its function, contain location data on users in the network. As noted by representatives of the police in Section 4.1, information about the physical location of NGN users may in some cases be highly sensitive. Some comments about this issue can be seen in Table 4.20. It was previously mentioned that the Norwegian armed forces have no interest in operating their own MVNO. As such, they emphasise the importance of organizational oversight on the part of the MNOs in order to, for instance, restrict

the number of employees who have access to sensitive information regarding, in particular, the would-be NGN users [Appx. O, 87]. If one however does wish to go for an MOCN solution and take control of the AMF oneself, comments warn about the fact that this would likely be significantly more technically and operationally demanding than traditional roaming [Appx. M, 27]. As your own core infrastructure would then be intimately connected to the actual radio network of your selected operator, this same comment suggests that you could potentially risk ending up more locked in to this one operator than you would have been had you opted for a more traditional MVNO setup. However, it is also noted that several MOCN type setups already exist around the world in PSN contexts, such as in England and the US, albeit primarily in 4G as of yet [Appx. M, 27].

### 4.3.3 Related to comparison criteria

The interview subjects in the state actor subject category are in many cases intimately familiar with the challenging task of comparing alternative deployment models for NGN. Either because they are in some way involved in the NGN process themselves, or because they have a good understanding of the challenges faced by the developers of next generation PSNs in general. As such, many of the questions in the interviews concern qualities of possible NGN solutions such as the ones described by the comparison criteria in Section 2.4. Of those, robustness and flexibility have each been awarded their own dedicated subsection within this section. However, concerns regarding technical complexity or security are not considered as separate entities. The reason for this is that such concerns make themselves known as secondhand features of a number of other considerations made throughout the section, for example, in the case of complexity, as a consequence of wanting to make use of more than one core network, which is something that is discussed in relation to the criterion of robustness.

#### Robustness

As a natural consequence of the strict availability requirements for public safety communications, robustness, particularly in the form of redundancy, is a hot topic. Table 4.21 lists some excerpts from the interviews of comments made in regard to redundancy in the core network of NGN. While national roaming seems to be a generally agreed upon minimum requirement in terms of redundancy in the RAN, the topic of redundancy in the core network, for instance in regard to the idea of employing the core network of all three Norwegian operators, appears to be somewhat more contentious.

When talking about state control it was mentioned that DSB are interested in managing some infrastructure of their own regardless of the chosen deployment model for NGN. In regard to core network robustness, DSB once again seem to

**Table 4.21:** Comments regarding robustness in the core network of NGN

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. M, 35] | A core network at a commercial MNO that isn't the same as the commercial core network could be safeguarded against [outages caused by] upgrades and maintenance work. |
| DSB | [Appx. M, 36] | If you're considering backup solutions you could perhaps be looking at letting some users have an alternative SIM card, so that they could use a different core network. However, it is the radio network that fails in practice. |
| DSB | [Appx. M, 34] | [If you're spread across three commercial networks] the outages might happen three times as often, with a third of the users losing service each time. |
| Nkom | [Appx. P, 32] | [In commercial core networks] there were a couple of quite serious events in 2011 and 2014 that affected a large number of customers. With a customer like the emergency services it would be very unfortunate if such an event coincided with a major emergency. |

take an interest in the idea of dedicated infrastructure, albeit this time in the more accommodating form of having a dedicated core network separated from an operator's commercial core network [Appx. M, 35]. The intention being that software updates and the likes could be tested out on the commercial network before being implemented in this NGN core in order to iron out any potential wrinkles that might result in outages. On the subject of employing core networks from multiple operators comments suggest that this could potentially result in outages happening three times as often. While, if one assumes that the emergency services are evenly spread out across operators, such an outage would only affect a third of the users, an interview subject notes that this approach runs the risk of increasing the complexity of the solution significantly for what could be considered to be a debatable gain [Appx. M, 34]. A better approach, it is argued, would be to consolidate investments into robustifying a simpler solution.

While it is said in [Appx. M, 33] that the availability of the Nødnett core network has been very good throughout the past decade, Nkom notes, as presented in Table 4.21, that outages in commercial core networks do in fact happen from time to time, and that the consequences of such an outage when your users are the emergency services could potentially be catastrophic. While Nkom's impression seems to be that

such a responsibility is something that the commercial operators would be taking very seriously, it is noted that it is each operators' own responsibility to have routines and mechanisms in place that would prevent these kinds of faults from happening, and that we have to remain realistic in regard to our expectations for these sorts of outages to also happen in the future [Appx. P, 26]. In light of this, if one does indeed wish to make use of multiple core networks for the added redundancy that that would provide, comments suggest that one could maintain a backup SIM card in one's terminal. This would then allow you to make use of an alternative core network if your primary network for some reason were to become unavailable [Appx. M, 36]. However, in relation to this it is noted that such a solution would likely be uncomfortably expensive to deploy en masse, as users are already complaining about the price of today's Nødnett subscriptions [Appx. M, 38]. Concerns are also raised in regard to the potential challenge of safeguarding subscriber information if users are to spread themselves across multiple networks.

**Table 4.22:** Comments regarding challenges to robustness in the RAN

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. M, 40] | [The reliance on shared infrastructure] is probably most prominent in remote areas where building infrastructure is more difficult. There is also a lesser degree of overlapping coverage [in these areas]. |
| Nkom | [Appx. P, 34] | [Multiple base stations being taken offline by the same fiber breaking] could absolutely happen. What's maybe even more challenging is if the power supply is disrupted. |

Now, while robustifying the core network will be an important part of ensuring availability in NGN it is mentioned by several interview subjects that disruption of service can most commonly be attributed to faults in the access network, such as breaks in fiber cables due to, for example, construction work or landslides [Appx. P, 24]. If a broken fiber acted as a single point of failure for a certain area, that area would then be without coverage. While the use of national roaming would allow the future users of NGN to make use of alternative RANs, this would not help if all the RANs in an area were dependent on the same piece of failed infrastructure though, and thus were all unavailable at the same time. Such co-localization of base stations and subsequent shared dependency on infrastructure like fiber access and power supply pose a challenge to the robustification of the access network. A couple of comments in Table 4.22 touch on aspects of this problem area, such as the fact that the areas were shared dependencies between RANs are prevalent are typically remote and already suffer from less than ideal levels of coverage. As a way

to solve challenges related to robustification of the access network Nkom is engaged in projects that attempt to strengthen the telecom infrastructure in Norway by, for instance, installing emergency power supply units at cell sites and laying redundant fiber lines [Appx. P, 36].

### Flexibility

Another comparison criterion that is frequently discussed during interviews is flexibility. In regard to flexibility the primary two topics are that of relying on standardized solutions and that of avoiding supplier lock-in effects. These are obviously two sides of the same coin, because, as pointed out by a representative of Nkom in [Appx. P, 50], the state as a customer has to rely on the procurement of standardized solutions as a means to avoid being locked in to a particular vendor or provider. This supplier-agnosticism, it is argued by the representative of Nkom, would motivate engaged vendors and providers to strengthen their NGN related deliveries in fear of being replaced by a competitor, and thus the overall quality of the NGN solution would be positively affected.

**Table 4.23:** Comments regarding standardization and its importance

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. N, 15] | We're hoping that we're entering into a standardized world where there is a bit more diversity. However, we still don't know how different [our solution] will be to that which is being delivered to the mass market. |
| DSB | [Appx. M, 12] | 3GPP is working to standardize MCX services ... in 5G and SA, but that work is not yet finished. |
| Nkom | [Appx. P, 50] | There will always be some distance from a standard on paper to an implementation. The specifications do not necessarily give all the needed details ... so the producers have to make some choices. |
| Nkom | [Appx. P, 48] | It will be important to make use of off-the-shelf tooling, and try to avoid tailored tools as much as possible. [Tailored solutions] have the potential to become both poor and expensive after a while. |

Some thoughts and considerations put forward by interview subjects in regard to the standardization of MCX services and the importance of relying on standardized solutions can be seen in Table 4.23. In addition to the aforementioned argument regarding how the reliance on standardized solutions could increase the de facto

quality of NGN, the representative of Nkom also posits that tailored solutions have a history of veering off towards becoming both lacking and expensive [Appx. P, 48].

While there seems to exist little doubt among interview subjects that standardized solutions is the way to go, some sobering comments are made in regard to the feasibility of making exclusive use of such solutions. In particular, as can be examined in Table 4.23, representatives of DSB remind us that uncertainty still reigns when it comes to the actualities of the implementation of NGN related technologies, and that the standardization work regarding MCX services in 5G done by 3GPP is still far from complete. Despite the fact that 3GPP took the LTE specific wording out of the MCX specifications to allow the specifications to also apply to 5G, there is still a way to go [Appx. M, 14]. Additionally, to further complicate the debate concerning standardized solutions, the Nkom representative remarks on the fact that specifications often leave equipment manufacturers with some creative license in terms of how actual implementation should be done [Appx. P, 50].

**Table 4.24:** Comments regarding supplier lock-in in an NGN context

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. N, 23] | There will always be some degree of lock-in, [regardless of what you're buying]. This is something one has to account for when making the contracts. |
| DSB | [Appx. N, 25] | [Things should be standardized] when you enter into the contract, but also when you exit out of the contract. You have to establish mechanisms that enable you to both get in and out of the contract. |

Even though supplier lock-in is something one would like to avoid, any commercial agreement involves some degree of lock-in, as aptly pointed out by a representative of DSB in [Appx. N, 23]. It is subsequently suggested that the solution to this unavoidable lock-in effect has to be to account for and attempt to mitigate this inevitability when planning and deciding on the makeup of contractual agreements. Furthermore, it is argued that contracts should be required to include both terms upon entry as well as upon exit, and that such mechanisms could help ensure, for instance, that solutions that start out as being standardized also remain that way for the duration of the contract [Appx. N, 25]. This is something that would then help to facilitate the previously mentioned beneficial vendor- and provider-agnosticism. On this topic of contracts it is also noted by a representative of DSB that, when taking the speed of contemporary technological developments and the previously mentioned modularity of this technology into account, it seems unlikely that the state will enter into a new twenty year long contract with a provider [Appx. N, 25]. Excerpts from

comments regarding contractual mechanisms to mitigate supplier lock-in effects can be seen in Table 4.24.

### 4.3.4 Competitiveness, cooperation, and life on the edge

Finally, this section acts as a catchall for comments and considerations made by interview subjects in the state actor subject category that do not fit into any of the previous sections. The three main topics that are regarded here are the challenge of maintaining competitiveness in the mobile market in Norway, the facilitation of cooperation between NGN users and, for instance, the Norwegian armed forces, as well as between neighboring countries, and challenges related to enabling autonomous edge operation in NGN. Some comments related to these topics can be seen in Table 4.25.

**Table 4.25:** Additional comments made in relation to NGN

| Reference | | Comment |
|---|---|---|
| DSB | [Appx. M, 88] | The competitive aspect is something the authorities are focusing on. It will affect the decision. It is an important parameter. |
| Nkom | [Appx. P, 57] | [Your choice of deployment model] should not have an effect on cooperative capabilities [with neighboring countries], as long as you make sure that your provider is delivering a standardized solution. |
| Defense | [Appx. O, 15] | It's important for us to be able to cooperate [with NGN users] on an application layer independent of MCX, [as the armed forces will not be pursuing MCX solutions]. |
| DSB | [Appx. M, 65] | There are two primary challenges [to autonomous edge operation]. There is the cost [of the infrastructure], and then there is the security aspect, as you're exposing a larger attack surface by distributing subscriber information geographically. |

The general impression from the interviews seems to be that the decision regarding what kind of deployment model to go with for NGN is one that could potentially have large consequences for the competition in the Norwegian telecom market. As such, it is no surprise that a representative of the DSB emphasises that this part of the debate is something that the government is keeping a close eye on [Appx. M, 88]. The representative of the Norwegian defense sector also remarks on the fact that the armed forces are interested in investments being spread relatively evenly out across

all three mobile networks, such that they may all be made use of for broadband critical communications [Appx. O, 77]. The comment where this remark is made also mentions how the fact that the armed forces are procuring their next generation communications services separately to NGN could help alleviate pressure in regard to competitiveness, as there are more than one big contract in play.

In regard to the users of NGN's ability to be able to cooperate with adjacent networks of a similar nature, such as the Norwegian armed forces' own broadband network or neighboring countries' PSNs, comments suggest that employing standardized solutions gets you a long way [Appx. P, 57]. In relation to this, however, it is noted by the representative of Nkom that, while standardized MCX solutions should be able to communicate with each other, there will likely be a time during the period of transition to MCX when some countries will still be mainly reliant on TETRA while others have completed the transition. As such, a remark is made about how interworking functions between MCX and TETRA will be vital to Norwegian emergency services continued ability of close cooperation with the emergency services of neighboring countries [Appx. P, 55]. Also as a side note, the representative of the defense sector stress the importance of having a common application layer for communication that is independent of MCX, as the Norwegian armed forces are not intending on employing MCX services for their own use cases [Appx. O, 15].

Lastly there is the question of the edge and autonomous edge operation. Two primary concerns are raised in regard to this topic by a representative of DSB, as can be seen in Table 4.25. Firstly, work needs to be done in terms of defining where the edge should be placed [Appx. M, 65]. The implication being that authorities will have to decide on which areas, and, in particular, the size of these, that should be able to act autonomously in the event that central infrastructure becomes unreachable. This decision will be related to the cost of establishing the autonomous edge infrastructure, which further begs the question of who is going to take on this cost, as remarked on by the representative of the defense sector in [Appx. O, 38]. Secondly, concerns are raised by the representative of DSB in regard to the security implications of spreading subscriber information, that would typically remain under lock and key in a centralized core network, out into regional or even local edges [Appx. M, 65].

## 4.4 Short summary of findings

In an attempt to take a step back and round out this chapter with a wider perspective on the various findings that have been presented, this section gives a short summary of the overarching themes observed in the results. First off, as has been pointed out numerous times before in this thesis, the verdict on the existing Nødnett seems to be largely positive in terms of what the TETRA network actually tries to do. Although, as pointed out by virtually every interview subject when the topic is brought up,

Nødnett lacks a bit of functionality, particularly in relation to services that require any significant amount of bandwidth. As for NGN, discussions in interviews have ranged from what kind of functionality users would like to see implemented in NGN, all the way to specific details about how the makeup of some of the alternative deployment models could potentially make the implementation of autonomous operation in the network edge quite challenging. The three deployment models proposed by the three Norwegian MNOs cover what is essentially the whole spectrum of potential approaches the Norwegian state will likely take to NGN, and aspects of these models have been discussed extensively in interviews with both commercial and state actors.

Without stealing too much of the thunder of the upcoming discussion chapter, there are some general observations that seem quite straightforward to make about the deployment models in question. For one, it seems clear that a single turnkey provider model would likely be the easiest to deploy in terms of complexity, but that it could have serious drawbacks with regard to some of the other comparison criteria. It is also worth emphasizing the negative impact a single turnkey provider model could potentially have on the commercial telecom market in Norway. It also seems likely, when considering the results, that a model involving a multitude of operators and providers, as well as a MOCN type solution with RAN sharing, are two of the most technically complex alternatives for NGN. An interesting sidenote to this, as well as to other models, is that it seems like a certain amount of the perceived complexity stems from the fact that there still exists a lot of uncertainty in regard to the implementation and function of several 5G related technologies, such as some of the VNFs. Something that does already seem to be crystal clear, however, is that there are no definitive answers to the big question of how to best deploy NGN. There are tightropes to walk and trade-offs to make the entire way. A sentiment that is reflected by many of the subjects interviewed in relation to this project.

We are of the opinion that the results presented in this chapter do well to cover the matters outlined by the research questions proposed in Section 1.5, as well as the tasks put forward in the problem description to this thesis. Multiple alternative deployment models have been the topic of conversation throughout the interviews, and the apparent benefits and drawbacks of each model have been examined in detail. Furthermore, there has been a special interest devoted to the topic of state involvement in NGN, and several suggestions have been made by interview subjects in response to questions regarding how the state could or should approach the situation in collaboration with commercial actors. This chapter has attempted to provide an unbiased selection of what we believe to be the relevant pieces of information extracted during the interviews. However, we concede that there are no truly unbiased selections, and as such we encourage curious readers to examine the transcripts of the interviews found in the appendices to this thesis themselves.

# Chapter 5
# Discussion

Now that the results have been presented it is time to delve into the discussion that was teased in Section 4.4 and examine the potential consequences of alternative deployment models in terms of the comparison criteria defined in Section 2.4. The chapter starts off by considering each criterion by itself. Relevant questions regard which aspects of the alternative deployment models affect the criterion and how one should approach the challenge of maximizing the benefit gained from the criterion without incurring too much drawback. From there we go on to evaluate the relative value of each criterion as opposed to the other criteria, before attempting to combine the best from each criterion into an abstraction of a deployment model. To round out the chapter we question the validity of the gathered results with regard to some of the concerns raised in Chapter 3, such as bias and representativeness, and then, lastly, we question the relevance of the selected comparison criteria as a way of expanding upon the justifications made in Section 2.4.

## 5.1 Considering each comparison criterion

As presented in Section 2.4, each comparison criterion represents distinct aspects of a next generation PSN deployment model. This section aims to understand how each criterion is affected by choices made in regard to various deployment models based on the results presented in Chapter 4. While there exist stronger or weaker correlations between some of the criteria, and while some of these correlations will be examined briefly in this section as specific elements of deployment models could affect multiple criteria in different ways, most of the interplay between the different comparison criteria will be covered in Section 5.2 when we attempt to weigh the criteria against each other. As it was presented in the introduction to this chapter, this section will focus on how the apparent benefit of each comparison criterion could be maximized by decision makers involved in next generation PSN processes while simultaneously attempting to mitigate potential drawbacks.

### 5.1.1 Robustness

The first considered criterion regards measures taken in a deployment model to ensure continued service to users during challenging circumstances, such as core network outages due to, for instance, errors in software or access network outages due to the fiber backhaul being disrupted by, for instance, construction work or a landslide. Looking back to the results presented in Chapter 4, a number of suggestions are made by interview subjects in regard to ensuring the robustness of NGN. While measures relating directly to the strengthening of the RAN are outside of the scope of this project, several relevant points are brought up during interviews about how to cooperate with commercial operators to ensure robustness both in the RAN and in the core network. In terms of radio networks, this entails primarily how one could achieve added robustness in the radio network by deploying a model for NGN that allows users to make use of all available radio networks.

#### Robustness in the radio network

For starters it seems obvious that NGN should incorporate all three Norwegian RANs in such a way that users of NGN have the ability to make use of an alternative radio network if the one they were originally connected to is unreachable for some reason. While there are different ways of doing this, with some being significantly more complex than others, allowing NGN users to connect to all available RANs gives you robustness in the form of redundancy and would also give you the best baseline radio network coverage. In regard to coverage it is worth noting that as the three Norwegian MNOs have, for commercial purposes, constructed their radio networks with the intent to cover as much of the Norwegian population as possible. As such, the three RANs are mostly overlapping. However, as the argument for redundancy still stands, any additional benefit you might gain in terms of coverage is a welcome addition to an otherwise already strong argument in favor of the ability to connect to all three RANs. The relatively straightforward way of ensuring this ability is to make use of traditional tried and tested national roaming techniques, and implement a model where NGN users may make use of all three radio networks in the same way as priority subscriptions facilitate today. That is to say, you have one main provider, but are allowed to roam to other RANs within range should your primary RAN for some reason become unavailable. As in a regular roaming scenario, you would still be connecting to the core network of your primary provider.

Another way of enabling the ability to make use of all three RANs is what has been discussed in conjunction with MVNO based approaches to NGN, namely a MOCN solution. In this approach an MVNO, which would presumably be the state or a service provider hired by the state to operate a state-owned core network, owns a full stack of core network functionality, and, as such, is responsible for their own AMF. As has been mentioned, and as we will also get into when considering the

criterion of security, this approach could give the state a larger degree of direct control over the NGN solution, but could potentially end up resulting in a high degree of complexity. In terms of redundancy and robustness in the RAN alone, however, a MOCN based setup gives you the same benefits as traditional roaming while also tacking on some additional benefits and drawbacks. Essentially, any approach that allows you to make use of multiple RANs will give you the same benefits in this regard. With that said, however, and although it was mentioned that the particulars regarding strengthening of radio networks is out of scope for this project, the relative robustness the ability to connect to alternative RANs would add to your NGN solution is naturally dependent on how this strengthening is done. For instance, if the state opts to only strengthen one of the radio networks in Norway, and then chooses the owner of that radio network as a single turnkey provider for NGN, then the added benefit of being able to make use of the other RANs would be smaller than if all networks were strengthened equally. This consideration relates to the preservation of competition in the Norwegian telecom market, which is something that will be covered in more detail when discussing the criterion of flexibility. However, due to the relative ease with which traditional national roaming could be implemented, it seems somewhat unlikely that even a single turnkey provider would not attempt to make use of it in an NGN delivery.

In addition to MOCN and national roaming, one final method that could perhaps be argued to be a way of making use of more than one RAN is the approach that was proposed by a representative of one of the Norwegian MNOs of using multiple operators' entire stacks, consisting of both radio networks and core networks. While the robustness argument in regard to this model was one of robustness in the core network, you would technically be making use of several radio networks as well. With that said, the same argument regarding national roaming as was presented in relation to single turnkey providers also applies here, as it would be silly to not let NGN users subscribed to one operator also use the radio networks of other operators if need be. The mentioning of this multi-operator model does, however, segue us nicely over to the topic of robustness in the core network.

#### Robustness in the core network

There are two main avenues of robustifying the core network that are directly related to how NGN is deployed. Similarly to how the radio network should be strengthened by laying redundant lines of fiber and installing backup power supplies at base stations, so too should perhaps the core network. A fundamental investment into strengthening the core network solution is, however, presumed to be necessary regardless of which deployment model is chosen, and is therefore not of particular interest when attempting to compare models against each other. In regard to deployment models, the two ways that have been proposed during interviews with

the aim of increasing the robustness of the core network are the previously mentioned multi-operator model, and the fact that DSB might be looking to cultivate some infrastructure of their own regardless of the chosen deployment model.

Firstly, the multi-operator model where NGN is served on three separate operator's full stacks and where public safety actors are spread evenly over these three networks would, naturally, mitigate the consequences of a core network failure in an NGN setting. Interview subjects have, however, raised a couple of concerns in regard to this proposed model. For instance, there is the concern that this model could introduce not insignificant levels of complexity to the NGN solution by requiring the service platforms on top of the three networks to be where the integration happens, as well as the concern that feature imparity between the three independently delivered solutions could lead to headaches for control room operators who have to decide which of the three networks to put interagency talk groups on. Additionally, concerns are raised in regard to the actual robustness benefit gained by deploying this model. While the consequence of a core network outage would only be a third of what it would be if you relied on a single core network, one has to assume that the outages will happen three times as often. In other words, if a core network experiences approximately one failure per year, an NGN solution relying on three core networks would be expected to experience three core network failures a year, although with only a third of the users being affected each time. One suggested solution to this problem, if we assume that each of the primary public safety agencies are subscribed to different providers, is that a firefighter experiencing an outage could borrow an NGN terminal from a police officer or use a police officer as a communications mediator. While this would technically be possible, it sounds operationally unwieldy, and is something that takes away from the benefit of running a multi-operator solution. As a final note in regard to this multi-operator model, however, it is worth mentioning that it was proposed with mercantile considerations in mind, and not explicitly as a way to robustify the core network. These considerations will be covered in more detail when discussing competitive aspects related to the comparison criterion of flexibility.

In regard to the comment made by a representative of DSB about how they are looking to have some infrastructure of their own regardless of the chosen deployment model, details are a bit stingy. However, it could perhaps be assumed that this is related to a concern of robustness. If one imagines a model in which a lone turnkey provider is delivering the entire NGN solution, state-owned infrastructure separated from the network infrastructure of this single provider might, for instance, function as a fallback network in the event that the core network of NGN's sole provider fails. This sort of fallback mechanism might not be as relevant in a scenario where the state is already owning and operating their own core network as an MVNO, but some contingency measures should likely still be implemented as part of the general strengthening of the core network. The big question in regard to operating additional

infrastructure as something to fall back on in the event of an outage in one's primary solution, however, is one of cost and benefit. While the cost could potentially be large, depending on how extensively one chooses to implement redundant infrastructure, the benefit is essentially dependent on how poor your primary solution is, if one assumes that the main point of the extra infrastructure is redundancy in the event of a contingency. As several interview subjects have noted that core network failures are relatively rare, in particular for the existing Nødnett core, but also somewhat for the commercial operators' cores, it may be worth considering whether or not investments made into redundant infrastructure could have provided greater benefit were they made into additionally strengthening the primary core network solution instead. Although, while experience with current mobile network infrastructure suggest that significant core network failures are few and far between, it is noted by interview subjects that one usually sees a higher frequency of failures at the start of a new generation of technology, such as 5G.

Lastly, despite the fact that it was said in the introduction to this discussion on core network robustness that there were two main ways in which the choice of deployment model could impact this part of the comparison criterion in question, there is one final note that is worth making in regard to it. While it could be argued that it teeters on the edge of what was initially dismissed as general measures to take in order to strengthen the core network, running the NGN core network on dedicated hardware could potentially help strengthen robustness in the face of regular core network outages. As it was mentioned, these sorts of core network outages are relatively rare. However, when they do happen they can often be attributed to mishaps in conjunction with software updates or maintenance work. If the NGN core network services are provided by way of dedicated network assets, it could be imagined that one could avoid some of these outages by simply being a bit more conservative and mindful when administering software updates and performing necessary maintenance. This is not to say that commercial MNOs do not take these things seriously, but the nature of a PSN is different from that of a commercial network in such a way that one could in some situations be willing to sacrifice the succulent fruits of the newest updates in favor of the assurance of unwavering stability.

#### Autonomous edge operation

Considerations regarding the network edge have been awarded their own section under the robustness umbrella, as they deal with matters that, in a way, fall in between the core and the radio network. The way we see it, there are two main scenarios in which autonomous edge operation is a relevant concept to ensuring continued service of NGN to users, the first being related to radio network robustness, and the second being related to core network robustness. As gathered from interviews, the most

common forms of outages in mobile networks today are due to disruptions to fiber access lines. While this is something that has to be addressed as part of strengthening the RAN in general, the implementation of autonomous edge operation could allow users to effectively operate in geographical areas that have otherwise been isolated from the rest of the PSN. On the other hand, in relation to core network robustness, autonomous edge operation could also allow for continuation of services in the event that the core network becomes unreachable, not due to a failure in the backhaul, but due to a failure in the core network itself. While the latter might be a less common occurrence than the former, this is something that could be seen in conjunction with the state's aforementioned desire to possess some network infrastructure of their own.

Regional data centers that facilitate the autonomous operation of base stations within their respective regions is something that could potentially help alleviate the consequences of both fiber backhaul failures and core network failures. The size of these regions is something that will have to be deliberated on by decision makers, however. Smaller regions with data centers that sit closer to the edge of the network would be more robust in the face of backhaul failures, while larger regions with data centers that sit further away from the network edge would enable a greater number of PSN users to stay connected to each other in the event of a core network failure. Additionally, the cost of the solution will probably increase the more decentralized it gets, as more infrastructure would be needed in more locations. In regard to the DSB's interest in having some infrastructure of their own, owning regional data centers such as these might be an interesting proposal. Among other things, state ownership of regional data centers could potentially address some of the security concerns related to autonomous edge operation that will be covered by the discussion on the comparison criterion of security.

### 5.1.2 Complexity

As presented in Section 2.4 when introducing the criterion of complexity, the intention behind it is to facilitate the comparison of deployment models based on their perceived technical complexity. The criterion differs somewhat from the others, as it essentially only exists as a drawback of decisions made with the intention of increasing benefits from other comparison criteria. As such, the overall goal of a deployment model would be to maximize the amount of benefit one is able to gain from other criteria, while at the same time minimizing the amount of incurred complexity. Naturally, most of the decisions made in regard to alternative deployment models have some effect on complexity. However, while the effect a modelling decision has on complexity may in some cases appear rather clear, there could be a significant amount of uncertainty attached to assessing the complexity incurred by other modelling choices. This is due to the repeatedly mentioned fact about how many aspects of 5G and related technologies are still not entirely known. Because of this the discussion concerning

the comparison criterion of complexity will in some cases need to rely on assumptions that seem reasonable, rather than cold hard facts.

The deployment model that would incur the least amount of technical complexity drawback seems likely to be the single turnkey provider one. Having a single provider be responsible for the end-to-end solution eliminates challenges related to, for instance, diffusion of responsibility and integration of separately delivered systems. In regard to the alternative deployment models mentioned when discussing robustness, both the multi-operator model and the MVNO model are associated with some complexity when you compare them to the single turnkey provider model. As noted previously, the multi-operator model requires the service platforms running on top of the three adjacent networks to be the point of integration, making sure that users subscribed to different service providers are able to communicate with each other across networks. While there seems to be some uncertainty tied to the complexity of such an integration, comments from the interviews suggest that it should be far from impossible to get this to function in a satisfactory manner. Concern for a different type of complexity is, however, raised by interview subjects in regard to this multi-operator model, related to the fact that you might get feature imparity between the services provided by the three MNOs. This is something that could potentially result in a situation where control room operators would have to make on the fly decisions about which network to employ for interagency talk groups based on an evaluation of the services that exist in each network. As an example of a worst case scenario, you could risk ending up in a situation where you would have to choose between different types of functionality implemented in different networks that are all deemed to be mission critical by their respective public safety agencies. With that said, however, the state's ability to define strict requirements that NGN providers have to comply with would perhaps make such an extreme scenario rather unlikely. Nevertheless, users of NGN are probably not particularly interested in running the risk of having to handle additional complexity on top of their already challenging day-to-day activities at all.

Compared to the multi-operator model, the MVNO model provides an entirely different set of complexity challenges. Instead of having to ensure that entirely different networks produce services that are compatible with one another, you now have to ensure that your potentially state-owned MVNO is compatible with the network of whichever host operator you select. As discovered during the interviews, the way in which MVNOs will work in 5G is something that seems to be particularly unclear. It is unclear how an MVNO will be interacting with the host operator in question, how much infrastructure it will be common for MVNOs to own and operate themselves, and what role the NEF in the 5G SBA is going to play. However, gauging by comments made by interview subjects in relation to the topic of 5G MVNOs, it seems clear that all of the aforementioned challenges are something the industry remains confident in its ability to solve in a satisfactory manner. When it comes to

MOCN, however, outlooks do not necessarily seem as promising. While it is conceded by interview subjects that a MOCN type setup is something that could probably be implemented, concerns are raised in regard to the complexity of such a solution. These concerns range from MNOs being opposed to the idea of having foreign AMFs directly connected to their radio networks, to a more NGN specific concern about how one would likely need to administer multiple AMFs as an MVNO to be able to make use of more than one radio network, as connecting the same AMF to multiple RANs could potentially result in some unwanted interconnections between different operators' networks.

In addition to potential challenges related to the integration of an MVNO with the host operator's network, some concerns have also been raised in regard to the implementation of autonomous edge operation in an MVNO based deployment model. In short, this concern has to do with the question of who is going to be responsible for the autonomous edge solution. As autonomous edge operation will require some subscriber information to be stored in the edge of the network in order to authenticate users while the edge is disconnected from the centralized core network, concerns are voiced by interview subjects in regard to how that information will be safeguarded. This will be covered in more detail when discussing the comparison criterion of security, but it is worth noting that challenges surrounding the implementation of autonomous edge operation look to have the potential to provide responsible authorities with more than their fair share of headaches. To wrap up the topic of complexity, it is something that one can not avoid entirely regardless of which deployment model one chooses. While the single turnkey provider model seems to be the least complex, it could have drawbacks in other areas. As such, the big questions relate to how much complexity one is able to stomach in the pursuit of benefiting from the qualities described by other comparison criteria.

### 5.1.3 Flexibility

When it comes to the comparison criterion of flexibility, there are two topics which concerns primarily relate to. First there is the topic of supplier lock-in effects, and then there is the topic of preserving the competitiveness in the commercial Norwegian mobile market. While concerns regarding these two topics are closely related by the way in which they are mitigated by relying on standardized solutions, the topics describe somewhat different aspects of the flexibility criterion. Concerns related to supplier lock-in have to do with the way in which NGN could potentially end up suffering from becoming technologically attached to individual suppliers. Adjacently, the discussion about competitiveness is first and foremost concerned with the side effects some deployment models could potentially have on the telecom sector in Norway at large. However, if you consider how a low degree of supplier lock-in would allow for more competitiveness by enabling NGN suppliers to be substituted for

their competitors, one can see how the two topics could in some cases be closely intertwined.

The dangers of supplier lock-in effects were covered in Section 2.1. In short, there are several ways in which one might become locked in to a supplier, but the most common one would likely be because your supplier has delivered a tailored system that makes it difficult for another supplier to take their place. The topic of being stuck with a single supplier is something that comes up several times during interviews, often in conjunction with the single turnkey provider model. In regard to this, a concern that is raised is about how being selected as the single provider for NGN on a long-term contract could disincentivize you from constantly developing and improving your delivered solution, as you can be confident that no competitors will be able to take your place regardless of the service you provide being subpar. On the other hand, however, concerns are also raised about how tailored solutions could induce supplier lock-in not only in single turnkey provider scenarios, but also in models involving several different suppliers. If, for example, two suppliers develop a tailored interface between them in order to integrate their respective NGN components with each other, you could end up equally as locked in to two suppliers as you would have been to one supplier delivering a tailored solution.

The way in which to avoid supplier lock-in by tailoring is to rely on standardized solutions as much as possible. However, this may not turn out to be as easy as it sounds for a couple of reasons, the big one being the by now often reiterated adage about how the specifics implementations of relevant 5G solutions are still not entirely known. As mentioned by several interview subjects, there will always be some aspects of implementation which standardization organizations leave to equipment providers to do as they please with, and we still do not know how specialized the NGN solution will have to be in order to provide the necessary functionality. In order to ensure the delivery of standardized solutions, the state will have to contractually obligate suppliers to this end both on entry and exit of a contract. By this we mean what is suggested in interview by a representative of DSB about how the state will have to ensure that any contract entered into will obligate suppliers to deliver standardized solutions that will still be standardized on the day the contract is terminated. Such a reliance on standardization would make it easier for competing suppliers to replace a current NGN supplier, and as such it would incentivize the current supplier to continuously improve and develop their delivered solution in fear of being substituted.

In terms of preserving the competitiveness in the commercial mobile market there is one aspect of a deployment model that is even more important than the facilitation of competition by relying on standardized solutions, and that is the balance of the involvement of Norwegian MNOs in the deployment model itself. The prominent example illustrating the concern here is the single turnkey provider model, as selecting

one of the MNOs to be this single provider and subsequently investing into that MNO's network has a real potential to end up giving that MNO a competitive advantage over the other Norwegian MNOs. The concern is that other Norwegian MNOs will not be able to compete in terms of coverage and robustness with an MNO who is subsidized by the state, as the requirements for NGN are stricter and demand more investment than what is otherwise financially reasonable to invest into a mobile network. In order to avoid this situation and preserve the competition in the commercial mobile market the multi-operator model is proposed by an interview subject as the antithesis to the single turnkey provider model in terms of competition. The multi-operator model would involve all MNOs equally in NGN, but, as we have discussed, could potentially result in a more complex overall solution.

While the multi-operator model and an MVNO model that involves all operators equally are probably the only two deployment models that can be considered to be truly fair in terms of competition, there are some other compromises that could be made in an attempt to address the issue of commercial competitiveness. The main idea is to distribute state-funded investments relatively evenly across all three operators or at the least make sure that all operators are able to take advantage of infrastructure funded by the state. For example, an approach we see taken in Britain and Sweden is that all operators will be allowed to make use of masts that the state funds in order to provide a satisfactory degree of radio network coverage to their next generation PSN. As such, even though there may be a primary radio network provider for the next generation PSN, that provider will not get an unfair advantage in terms of coverage compared to its competitors when competing for customers in the commercial market.

Before rounding out the discussion on the comparison criterion of flexibility, there are two more important things to take note of. The first is that the concept of supplier lock-in applies to vendors as well, and not just service providers. While the ways in which the state might get locked in to certain providers by them developing tailored solutions and interfaces are often the ones in focus, it is similarly important to contractually obligate any potential infrastructure equipment vendors to deliver standardized solutions. If the state is going to own and operate its own MVNO and thereby lessen its dependence on providers, there will naturally be a need to involve more vendors of equipment, which will subsequently increase the risk for vendor lock-in. The second thing to note before rounding out the discussion on flexibility is that reliance on standardized solutions have other benefits apart from the ones directly related to flexibility. The most prominent being how it allows NGN to interact with the PSNs of neighboring countries, given that they also rely on standardized solutions. The Norwegian public safety agencies will in many scenarios have to cooperate with the public safety agencies of our neighboring countries, something that is facilitated by the inter-system interfaces of today's TETRA networks. As

such, involving suppliers in NGN that guarantee the delivery of solutions that make use of standardized interfaces will likely be a minimum requirement from the state when procuring services or equipment for NGN.

### 5.1.4 Security

Lastly we come to the comparison criterion of security. As described in Section 2.4 when introducing the comparison criteria, much of the information that passes through PSNs is sensitive in nature. As such, protecting the confidentiality of this information is important to ensure effective and safe public safety communications. While the communications channels themselves are likely to be heavily encrypted, metadata regarding these communications could potentially contain information that the users of NGN do not want to be publicly known. The most straightforward example of this are police operations that rely on subterfuge to carry out their mandate and keep their personnel safe. Additionally, there will be a need to safeguard subscriber information and the key material that enables authorized NGN users to authenticate themselves and access the resources they need in order to do their jobs.

The big question related to the criterion of security is whether or not the state needs to own network assets in order to be able to ensure confidentiality of sensitive information. If this turns out to be the case, then multiple measures can be taken to increase state control over the NGN solution. Such measures include, for instance, the establishment of a state-owned MVNO that runs its own dedicated infrastructure in a MOCN setup, allowing for the highest degree of state control over the core network. As discussed previously, a MOCN setup essentially implies that the state-owned MVNO is running a complete core network themselves, and hooking this core network directly on to the radio networks of operators. Importantly, this gives the state control over the AMF, which is the network function dealing with mobility. In a deployment model where the state does not control the AMF themselves, there is a potential risk that employees working for the operator who owns and operates this AMF could potentially gain insight into the whereabouts of public safety actors that do not want their location to be known.

Despite the fact that our neighboring countries, Sweden and Finland, seem to have been quick to decide that this kind of state control is something that will be important to Rakel G2 and Virve 2.0 respectively, comments made in an interview with a representative of DSB note how the Norwegian authorities have not been able to conclusively determine state control to be paramount to the security of NGN. As proprietors of critical infrastructure, all Norwegian MNOs are already subject to strict laws regarding, for instance, security clearance of personnel. Additionally, interview subjects note how the ability to properly secure the information in question would likely require a sophisticated and mature environment of security professionals.

This is something that the MNOs already have in conjunction with their commercial offerings, but that the state would have to nurture more or less from scratch when establishing a state-owned MVNO. As such, suggestions are made during interviews regarding how it might be just as, if not more, reasonable to achieve a satisfactory level of control and security through carefully constructed contractual agreements, rather than by having the state take direct control over central functions of the networking operation themselves.

Looking outside the confines of the centralized core network for a minute, there is also a big question of security related to the implementation of autonomous base stations in the network edge. As presented when discussing the comparison criterion of robustness, the idea behind autonomous operation in the edge is that users of NGN should be able to maintain some level of service in the event that the centralized core network becomes unreachable. While there are numerous suggestions proposed for how to best implement this type of autonomous operation, users of NGN will still need to be authenticated and authorized, which means that all the solutions for autonomous edge operation involve the distribution of subscriber information out into the edge in some form or another. The security implications of such a distribution will of course vary by implementation, as there would be a difference between fully duplicating the subscriber database and distributing it out into the edge and only distributing parts of the database or relying on predetermined sets of autonomous operation key material. However, regardless of which implementation ends up being selected to provide this autonomous operation of the edge, two large and related questions remain in regard to the comparison criterion of security. In a deployment model where the core network and the radio network are controlled by different actors, who will be responsible for the autonomous edge functionality itself along with the associated challenge of securing the distributed subscriber database? And, in a model involving a state-owned MVNO, does it make sense for the state to leave the handling of this distributed subscriber database in the hands of a commercial operator given that the state may go to great lengths to safeguard this information in the centralized core network, for instance by making use of dedicated personnel and hardware? These are questions that have to be answered in regard to the security implications of implementing autonomous edge operation in NGN, in the event that the state opts for something other than a pure single turnkey provider model.

## 5.2 Weighing criteria against each other

Now that each comparison criterion has been looked at individually, it is time to start considering them in light of each other, as they will eventually all be compacted into the same deployment model. From the discussion regarding each individual criterion in turn we have seen how several of the criteria affect each other in various ways. It is, for instance, suggested that a model of low complexity might also turn out to be one of

low flexibility, and that a model of high security might turn out to be one of similarly high complexity. As noted when discussing the criterion of complexity in Section 5.1, an increasing level of complexity is often the drawback of attempting to increase any of the other comparison criteria. However, other interdependencies between comparison criteria do also exist to some degree. The added core network robustness in a multi-operator model might, for instance, come at a cost of lower security in addition to higher complexity, as spreading yourself across multiple operators could potentially make it more challenging to ensure confidentiality across the board. In any case it seems clear that the challenge of selecting the best deployment model for NGN is one of balancing trade-offs between the different comparison criteria.

In order to be able to fairly balance such trade-offs, however, there are two challenges that immediately spring to mind. The first challenge regards the way in which the consequences of deployment model related choices vary in terms of uncertainty. To give a hypothetical example, if the state selects the multi-operator model for NGN with the intention of increasing robustness in the core network, it does not seem unreasonable for them to assume with at least some certainty that this will indeed result in a more robust solution. However, as noted when discussing this topic in Section 5.1, a drawback of such a solution is that it could end up becoming quite complex, and the uncertainty related to the severity of that complexity could be significantly more difficult to judge beforehand than the uncertainty related to whether or not the solution would result in increased robustness. In other words, while it seems reasonable that a multi-operator model would help increase robustness in the core network, the relative size of the drawback in terms of complexity is difficult to predict. The uncertainty related to different aspects of deployment models in this regard seem, to a large degree, to be related to the fact that there are still many aspects of 5G and next generation PSN related technologies that are themselves uncertain. How, then, should this uncertainty be taken into account when weighing the comparison criteria against each other? Should less uncertain consequences of deployment model choices be weighed more heavily, or should we perhaps assume a sort of worst case scenario in every situation where there exists significant uncertainty? Whenever one attempts to make predictions about how things could potentially turn out in the future, one has to be prepared to do battle with uncertainty. In terms of planning a huge project such as NGN, however, we regard uncertainty in and of itself to be undesirable, especially in circumstances where it could potentially result in significant drawbacks. While this means that we may in some cases lose out on the tail end of benefits, it is our opinion that it is better to be safe than sorry in this regard.

The second challenge that needs to be addressed in order to be able to fairly balance trade-offs between the comparison criteria, is related to the fact that one might simply choose to value the criteria differently. For example, the state may

decide that establishing a system with a high degree of robustness is more important to them than establishing a system that allows for greater flexibility in terms of suppliers. As we are talking about balances and trade-offs here, differences in such valuations could easily end up favoring one particular deployment model over another. If you, for instance, decide that you for whatever reason are opposed to the thought of indebting your solution with too much complexity, that is something that could heavily impact the selection of alternative deployment models that appear relevant to you. While we can observe how our neighboring countries, Sweden and Finland, are valuing state control highly in their choice of deployment model, we are not privy to any information suggesting such valuations are being made by Norwegian authorities. As such, when we conduct our own evaluation, we make an effort to weigh the importance of each comparison criterion somewhat equally to the others, and, in doing so, attempt to outline a deployment model for NGN which provides a good balance between robustness, complexity, flexibility, and security. However, as noted previously, we do wholeheartedly concede that this egalitarian approach might not accurately reflect how the decision regarding the deployment model of NGN, or any other next generation PSN for that sake, will be made in reality.

## 5.3 Combining criteria into one model

Before we get into the details of what we envision to be the choicest deployment model for NGN based on the information collected and reviewed throughout this project, we find it useful to restate what we are, in fact, attempting to accomplish here. Restrained by the scope of this project, we will not account for the economic ramifications of alternative deployment models, nor will we take into account any possible political connotations of the decision. Instead, we focus on the qualities of the deployment models themselves, as observed through the lens of our four comparison criteria. As mentioned previously, the goal is to outline a deployment model that maximizes the amount of benefit one gets out of the comparison criteria, while simultaneously minimizing the amount of drawback one incurs. In order to help illustrate what we mean by this we present a simple graph in Figure 5.1 inspired by the concept of diminishing returns from the field of economics. In this graph the x-axis represents the amount of robustness we put into a deployment model, while the y-axis represents the benefits that this robustness adds to our model divided by the amount of drawback that it incurs, for instance in the form of added complexity. Although this is an extremely simplified depiction of this concept, the main observation to take away from Figure 5.1 is that you will eventually get to a point where the benefit you gain from adding more robustness to your solution is outweighed by the amount of drawback you incur by doing so, illustrated by the horizontal blue dotted line in the graph. This concept also applies to the other two comparison criteria that one would wish to maximize, flexibility and security, and

not just to robustness. While the adding and subtracting of robustness is not done on a continuous spectrum as is eluded to by Figure 5.1, as you would, for instance, either make use of multiple core networks or not, we believe the figure could serve as a helpful aid for understanding our intentions before embarking on outlining what we believe to be the best deployment model choice to make for NGN.

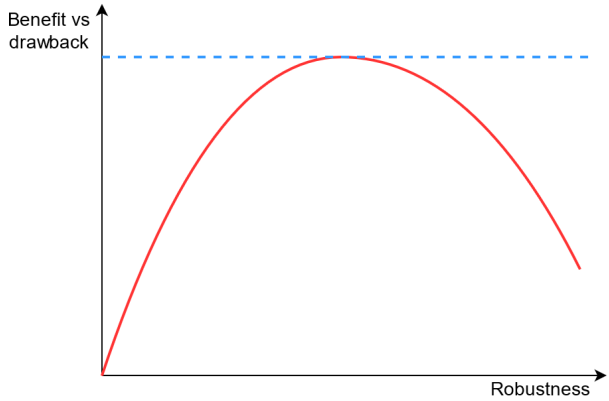


**Figure 5.1:** Illustration of diminishing returns for the criterion of robustness

### 5.3.1 The service platform and the radio network

There are, in essence, three parts to the NGN equation. From top to bottom they are the service platform, the core network, and the radio network. As the core network is the part which most decisions made about a deployment model will be made in regard to, we save that for last and attempt to get the other two out of the way first. However, it should be noted that what the radio network and service platform situations will look like in NGN could in many scenarios be influenced by decisions that are made about the core network. As for the service platform situation in particular, not much attention has been awarded to it in this project, something for which there are a couple of reasons. When introducing alternatives for the deployment of a next generation PSN in Section 2.1, the service platform is described as something that is likely to be a dedicated asset, but which ownership and operation of could be either that of the state or that of a commercial provider. However, during interviews, for instance, little interest is taken in questions regarding the service platform, while a lot of interest is taken in questions regarding the core network. The primary reason for this skewness is that questions regarding the core network are the ones most crucial to answer in order to get a grip on alternative deployment models, while questions regarding the service platform could in many cases be answered as an extension of an answer given in relation to the core network, or as a relatively inconsequential addition to an already established deployment model. If one, for

example, decides to go for a single turnkey provider model, it would make sense that that single turnkey provider would then also be responsible for the delivery of the service platform. Similarly, if one opts for a model involving a state-owned MVNO, one might imagine that the state could potentially take an interest in also being directly involved with the delivery of the service platform themselves. Either way, decisions made regarding the service platform do not overly impact the deployment model at large, and as such is considered to be of less importance than decisions made regarding the core network.

Some, although certainly not all, of the same can be said for the radio network. As it has already been established that the radio network will be commercially owned and operated, relevant deployment models differ only in how they make use of the available commercial radio networks. In the same way as for the service platform, how the radio network situation will turn out in the end is something that would also, in many cases, be affected by decisions made in regard to the core network. For instance, if one opts to go for a model based on a MOCN style state-owned MVNO setup, the way in which one interacts with the radio networks would probably look a bit different from if one opts to go for a single turnkey provider model. In either case, however, the ambition is to be able to make use of all three radio networks in order to maximize robustness and also coverage, as noted in Section 5.1 when discussing robustness in the radio network. The best way to achieve this, in our opinion, is to facilitate the use of national roaming between the radio networks of the three Norwegian MNOs. This solution could achieve a notable sense of robustness in the radio network, while simultaneously being relatively drawback-less in terms of complexity. Further reasoning for opting for this method of multi-RAN employment is provided when discussing choices made in regard to the core network.

### 5.3.2 The core network

As mentioned previously, decisions regarding how things should be handled in the core network are the essence of the deployment model itself. It must be emphasized again that the making of such decisions is no easy task. When you look outside the borders of Norway to other countries struggling with similar challenges, you can quickly observe that there are a multitude of approaches being taken to solving the problem of next generation PSNs. While all roads do not necessarily lead to Rome, it should be safe to say that there may be several ways to approach this issue that could all result in varying degrees of satisfactory results. With this consolation in mind we take on the task of outlining what we believe to be the best alternative deployment model for NGN based on the research conducted in conjunction with this project.

To start with the foundation, we will first answer the question of dedicated versus

shared assets. In order to be able to ensure that the demanding nature of mission critical services is able to be met we believe it is necessary to dedicate some assets in the core network to this purpose alone. However, on account of the uncertainties in implementation and the potentially large amount of complexity a MOCN solution could bring with it, we do not think that the whole core network necessarily needs to be dedicated. Instead we propose a model in which the upper part of the core network is dedicated and the lower part is shared, as can be seen in Figure 5.2.

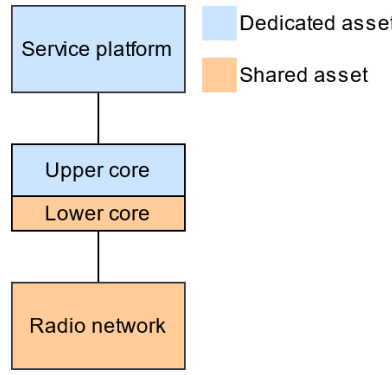


**Figure 5.2:** Distribution of shared and dedicated assets in NGN

Dedicating the upper part of the core network facilitates the use of dedicated personnel and specially designed operational procedures that could help ensure that the strict requirements of NGN are met in a satisfactory manner, both in terms of robustness and security. For robustness the dedication means that you could, for instance, instruct personnel to more carefully consider and plan for contingencies when performing maintenance or upgrade work on the NGN related part of the upper core network, and as such possibly avoid failures that could cause outages. On the other hand, in regard to security, the dedication of the upper core network could, for instance, let you keep closer tabs on the personnel who is authorized to access sensitive information regarding, among other things, subscribers, and perhaps also demand this personnel to be more carefully vetted than the personnel who works with shared assets. Regardless of how aspects regarding ownership and operation of the core network are handled, we believe this to be a good compromise between beneficial qualities and complexity.

The only other solution to this would be in relation to a single turnkey provider model where the entire core network could be dedicated without having to deal with the complexity of a MOCN solution. However, we decide against the single turnkey provider model on account of the effects it could potentially have on the criterion of flexibility and the competitive aspects of the Norwegian mobile market at large. While the supplier lock-in argument is disputed by the fact that lock-ins will happen to some degree regardless of how you approach the procurement process of NGN, and while supplier lock-in in relation to two or more providers might be comparable to single provider scenarios both in terms of likelihood and consequence, our assessment is that this is something that will need to be addressed by contractual agreements demanding standardization of solutions instead of by the deployment model itself. This could in itself perhaps be construed as an argument in favor of a

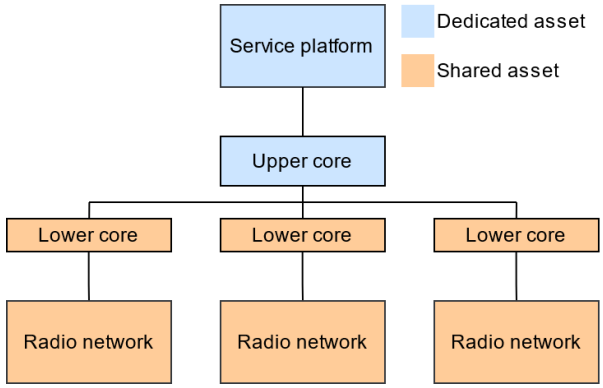


**Figure 5.3:** Utilizing the networks of several operators in NGN

single turnkey provider. However, in addition to this, based on comments made by interview subjects, we also take into account the fear that large monolithic provider arrangements could run the risk of becoming somewhat stale after a while, once the initial dust settles and the provider is left to deliver the service according to what was specified at the time the contract was entered into. As such, NGN could potentially benefit from involving more actors and being able to innovate more on smaller arenas, although with the added downside of some complexity. Adjacent to the supplier lock-in argument we additionally find the competitiveness in the commercial mobile market argument. This is one that is strongly opposed to the idea of a single turnkey provider, but that should fit well with the model that is presented here. As only the upper core is dedicated, you avoid the aforementioned MOCN related entanglement issues when attempting to involve more than one MNO in the solution. Figure 5.3 shows a scenario in which the upper core network dedicated to NGN is connected to the lower core network of all three operators. While we do not have a clear understanding of the technical feasibility of such a solution, it does not seem outright unreasonable to assume that this is somewhere NGN could potentially end up in the future should a model with a dedicated upper core separate from a shared lower core be selected. Initially, however, it would probably be a safer bet in terms of uncertainty and complexity to select a single operator to provide the lower core network, and then make use of national roaming to get access to the other two radio networks.

The scenario shown in Figure 5.3 is probably also the closest this model will get to anything like the often mentioned multi-operator model. We have decided against the full multi-operator model primarily on grounds of complexity, and on the fact that we believe core network robustness and a fair competitive environment in the commercial mobile market can be achieved through other means in other models.

Depending on how you would have chosen to implement a multi-operator model, the complexity challenges could perhaps have been overcome in a fairly satisfactory manner. However, there seems to be significant uncertainty tied to the way in which the three operators' solutions would have had to be integrated with each other, and we believe the resources that would have had to be invested into each operators' network are better employed in the improvement of a more directed and singular deployment approach.

Now that we have the general outline of the deployment model laid out, we can get into questions regarding ownership and operation of this core network. The way we see it, there are two main avenues to choose from in regard to these questions. The first is a model in which the state owns and operates the upper part of the core network itself, while the second model is one in which the state outsources the ownership and operation of the upper part of the core network to a commercial provider. If we consider ownership first, Figure 5.4 illustrates the ownership of assets in the two models in question. Remembering all the way back to the models of other countries examined in Chapter 2, one can observe that the model involving state ownership is somewhat akin to the Swedish and Finnish models, although without the MOCN setup, while the model in which a commercial operator owns the upper part of the core network is almost identical to the model of Britain's ESN. The difference in the latter case being that the lower core in our model is not dedicated. Figure 5.4 also portrays the ownership of the service platform as being in line with the ownership of the upper core network in each respective model. As mentioned when discussing the service platform previously, decision regarding it will likely be influenced by decisions made in regard to the core network. While it is certainly possible that the state could, for instance, opt to own their own service platform despite outsourcing the ownership of the upper core network to a commercial provider, we believe the decisions being made in the core network could potentially be reflecting a larger philosophical standpoint in regard to ownership. As in, if you are willing to let a commercial provider handle the responsibility of managing the upper core network, you have already let go of some of your reservations regarding commercial ownership and are more likely to also let a commercial provider own the service platform. The other way around, however, where the state owns the

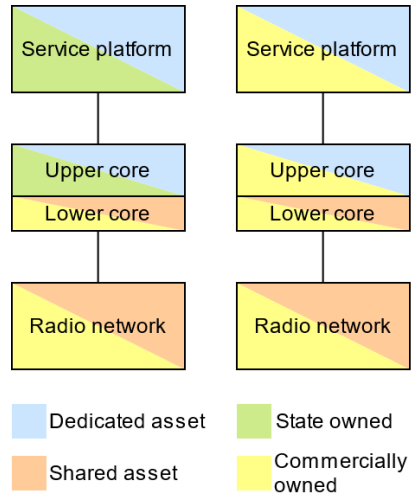


**Figure 5.4:** Ownership of network assets in NGN

upper core network but leaves the ownership of the service platform in the hands of a commercial provider, seems rather unlikely.

Whether or not the commercial provider who owns the upper core network and the service platform is the same one as the operator who provides the radio network and the lower core is something that needs to be discussed. If this should be the case, then you have essentially just taken extra steps to deploy a single turnkey provider model, which was argued against earlier in this section. As such, the reasonable conclusion seems to be that a commercial provider who is going to be responsible for the upper part of the core network and possibly also the service platform, should be a different commercial entity from the operator providing the lower core and the radio network. This being similar to how it is done in the ESN model in Britain. Before deciding whether to go for the solution in which a commercial provider owns the upper part of the model or the one in which the state owns it, we will take a moment to also look at operation of the assets. When speaking about ownership we concede that the terminology can at times get a bit ambiguous in regard to whether or not it also refers to the operation of the assets. The reason for this is that we believe it makes the most sense for state-owned assets to also be operated by the state, while commercially owned assets are operated by a commercial provider. Again, this is an argument relating to the general philosophy of the state about the involvement of commercial providers where the main idea is that if you allow the commercial operator to have a piece of the pie in any case by owning the asset, you might as well let them operate it too as they are already heavily involved. Our opinion is that there does not seem to be much to gain from adopting a half measure wherein the commercial operator owns something that the state then operates, or vice versa. Figure 5.5 shows how the two complete deployment models could look when also taking the dimension of operation into account alongside dedication and ownership of assets. As mentioned previously, some inspiration for the ownership and operation of each of the models is taken from the Finnish and British deployment model respectively.

From this point onward it should be assumed that either of these two deployment models would function in a satisfactory manner as the selected deployment model for NGN. They each exhibit the previously described qualities that facilitate robustness, flexibility, and security, without sacrificing too much in the way of complexity. Choosing between them comes down to a question of how much responsibility the state is willing to take on themselves by being directly responsible for providing the NGN service. This responsibility is something that comes up as a topic repeatedly during interviews. Out of all the difficult questions being answered here, questions regarding the state's will to take on such a responsibility might be the most difficult, as any answer would to a large extent be based on a set of decidedly intangible notions. Arguments in favor of state ownership and operation revolve around notions

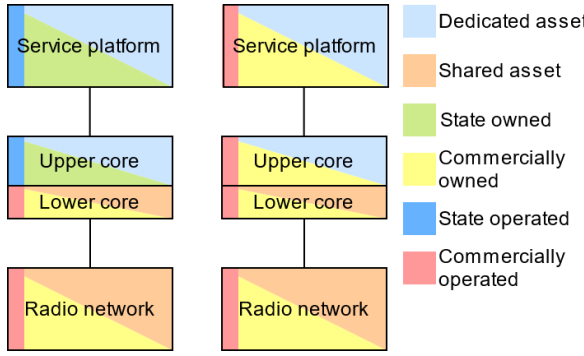


**Figure 5.5:** Deployment model alternatives for NGN

of security and state control. Looking at our neighboring countries, Sweden and Finland, who have both weighed the involvement of the state heavily in their respective PSNs, it seems clear that these are notions that can not be dismissed by the wave of a hand as being merely speculative. Despite this, representatives of DSB, the authority who is responsible for these affairs in Norway, have noted in interviews that Norwegian decision makers have not been able to reach the same categorical conclusions regarding state involvement as their Swedish and Finnish counterparts. In terms of arguments that are opposed to state involvement and that favor the involvement of a commercial provider as the owner and operator of the upper part of the core network and possibly the service platform, the most prominent is perhaps the current organizational structure of DSB, the government body who would be responsible for the core network assets and service platform in question should the state move forwards with plans of state involvement in NGN. As has been noted by interview subjects, although DSB has responsibilities in regard to the current TETRA network, they would have to undergo a serious expansion in order to become ready for the responsibilities that would fall on their shoulders as the proprietors of a state-owned MVNO in NGN. While this is by no means an impossibility, it does exemplify how NGN could perhaps stand to benefit from the involvement of an experienced commercial provider instead.

There is one last question that needs to be addressed before making a decision in favor of either alternative, however, and that is the question of autonomous edge operation. When discussing autonomous edge operation in connection with the comparison criteria of complexity and security in Section 5.1, questions were raised in regard to the implementation of autonomous edge operation in conjunction with an MVNO-centric deployment model. Related to security, the big question concerns how we would secure the subscriber information that would have to be stored in the edge in order to make the system function in the event that the centralized core

network becomes unreachable and autonomous edge operation becomes necessary. As the edge is a part of the part of the NGN stack that is otherwise controlled by one or more commercial operators on shared assets, it seems safe to say that the edge would under normal circumstances be relegated to their care. However, once you have to distribute information that would otherwise be safely stored in the dedicated upper part of your core network, the circumstances suddenly become quite different. In that scenario it would perhaps make more sense for the actor that is originally responsible for the sensitive information being distributed out into the edge to also be responsible for that information where it goes to live in the edge of the network. To put things in perspective it would not make much sense to heavily safeguard this information in your centralized core network if and adversary could easily get a hold of it by compromising one of the many lightly secured edge sites of the network where at least parts of this sensitive information is being held.

In terms of the edge in general, we propose that which was suggested when discussing autonomous edge operation in connection with the criterion of robustness in Section 5.1. Namely, that there be established regional data centers that have the ability to function autonomously to provide connectivity between NGN users within their respective regions in the event that the centralized core network becomes unreachable, due to, for instance, a backhaul failure or simply a core network outage. As a sidenote it could perhaps also be envisioned that these autonomous regions could have the ability to communicate with each other, given that the backhaul connections between them are functioning. While the size, number, and relative placement of these regions are all aspects of this that will have to be addressed before any final decisions can be made, we will, for the sake of argument, assume that a number of around twenty of these regions will be spread out across the country. We believe this number to enable a region size that strikes a good balance between accounting for failures in the fiber backhaul and letting public safety actors within a relatively large geographic area continue to communicate with each other.

With these twenty or so regional edge centers in mind, we continue the discussion on whether or not the state should own and operate their own MVNO or not. There are now two different scenarios to envision in regard to this autonomous edge solution. The first is a scenario where the state is responsible for the upper part of the core network and thereby is also responsible for at least parts of the solution in these regional edge centers. One could, for instance, picture a cooperative effort between an operator and the state-owned MVNO in which the separation between upper and lower core network components in the centralized core network is extended out into the edge cores, leaving the state to carry out a similar mandate in the edge as they are in the centralized core network. This could let the state continue to focus on the provisioning of the service and the security of sensitive information, while the operator would take care of the lower core network functions like they do in

the centralized core network. The other scenario is then, naturally, one in which the commercial provider that is responsible for the dedicated upper core network and possibly also the service platform takes care of the edge centers instead of the state, for instance by teaming up with an operator in a similar fashioned as described previously. While a commercial provider, like for instance Motorola Solutions who are heavily involved in the British solution, would certainly be capable of performing such a feat, it would likely leave them heavily intertwined with the NGN solution at large. As such, we believe that a state-owned MVNO is the way to go in order to be able to realize the suggested deployment model for NGN as can be seen in Figure 5.6.

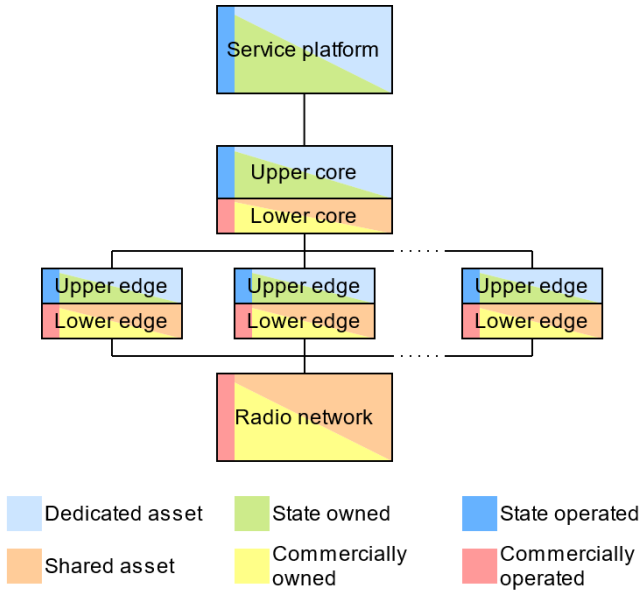


**Figure 5.6:** The suggested deployment model for NGN including the edge

While this would then require the establishment of this state-owned MVNO potentially in conjunction with a substantial expansion of DSB as an organization, several of the interview subjects respond highly positively when questioned on whether or not they believe DSB to be capable of taking on such a task. In addition it is worth taking note of a fact that has been repeatedly stated throughout this discussion. Namely, that our neighboring countries Sweden and Finland are both making use of their own state-owned MVNOs in the provisioning of their own next generation PSNs. Although they both seem to be opting for MOCN type setups, this shared reliance on state-owned MVNOs could ideally mean that there will exist significant potential for the exchange of experiences and insights in relation to challenges faced by state-owned MVNOs, which the authorities in Norway could make good use of. As for whether or not the state is actually willing to take on the responsibility of

providing the NGN service themselves, this is something that remains to be seen and that could only be speculated about at this point. The only other model we have considered that could also provide what we consider to be a satisfactory solution to the problem of autonomous edge operation is the single turnkey provider. If the state should choose not to take on any direct responsibility themselves by establishing a state-owned MVNO, we expect the single turnkey provider model to be chosen, as it has the potential to provide the state with a relatively straightforward and effective solution to the question of NGN. However, as has been covered previously in this discussion, the single turnkey provider model also comes with some drawbacks, which are the reason for it not being the one suggested by us in the end.

One concern that has been hinted to with the suggested model, however, regards the way in which the model addresses concerns of disruptions to the competition in the commercial mobile market. While it was suggested that the lower core networks of all three operators could be employed simultaneously, it was at the same time admitted that we do not have a clear understanding of the technical feasibility of such a solution, and that it thus may turn out to be a somewhat of a pipe dream, at least in the near future. This means that a cooperative agreement will potentially have to be entered into with a single operator in order to provide the NGN model with the required lower core network. Additionally, it seems likely given the circumstances that this operator will then also be the one with which the state-owned MVNO cooperates to implement the suggested autonomous edge solution. We reluctantly concede that this is something that could potentially have an impact on competitive aspects of the commercial mobile market, especially in regard to the regional edge centers. The state will have to keep an eye out for such impacts and attempt to mitigate them through, for instance, cleverly constructed contractual agreements. Another mitigating effort could be to attempt to involve multiple operators in the implementation of the regional edge centers. However, it is uncertain how this could affect the overall complexity of the solution. At the least the regional edge centers should be implemented in such a way that their existence benefits all three Norwegian MNOs, as this would shrink the competitive advantage gained by being the selected operator involved in NGN.

Lastly, a final concern may be raised in regard to the fact that the suggested deployment model differs slightly from the examined deployment models that have been selected by other countries. While this need not be of any significance in and of itself, and while the aforementioned other countries have certainly not let such concerns stop them from pursuing novel solutions, this could lead to a situation where the authorities in Norway will have to deal with challenges related to the deployment model that have yet to be solved by anyone else. This could be considered to add some uncertainty to the proposed solution, compared to an alternative deployment model that more closely mimics that which has been done before by others. We

do, however, believe that this uncertainty is not significant enough to discourage the choice of the deployment model altogether. As has been touched on previously, individual parts of the suggested deployment model are reminiscent of various other countries' solutions. The split core network can, for instance, be seen in Britain's ESN, while the state-owned MVNO is something that can be seen in Finland's Virve 2.0 and Sweden's Rakel G2. As such, we remain confident in our recommendation of the previously proposed deployment model for NGN, despite that fact that some aspects of it could be considered to be uncharted territory.

## 5.4 Regarding the validity of results

As presented in the introduction to this chapter, the purpose of this section is to examine concerns related to the validity of the findings that have been gathered throughout this project. Most prominently this means that some of the concerns raised in Chapter 3 will be reexamined in light of the information gathered through interviews and in light of how that information has been used to argue throughout this chapter. Such concerns include, for instance, the representativeness of the selected interview subjects and the way in which the results have been interpreted, as these are aspects of the research we believe could have impacted the final conclusions regarding alternative deployment models for NGN.

It is our firm belief that representatives of all major types of stakeholders in the NGN project have been interviewed in connection with this research project. As such, it seems reasonable to assume that most views on the matter have been covered to some extent. However, despite the fact that all types of stakeholders are included among the interviewed, we believe there is one point worth expanding on in relation to the way stakeholders have been given the opportunity to defend their views. This point has to do with the order in which the interviews are conducted. While it is covered somewhat in Section 3.3, we feel the need to restate the concern in conjunction with the effect it could potentially have had on the choice of deployment model. As much of the argumentation regarding various deployment models is adapted from the comments of interview subjects, the way in which these interview subjects argue in favor of their own preferences could potentially end up directly impacting the argumentation leading to this thesis' suggestion of deployment model. While we are aware of potential bias on the part of the interview subjects and believe that we manage to mitigate it to a certain degree, it may be difficult to accurately assess the inherent bias in statements regarding highly technical considerations. As we do not always possess the required technical knowledge needed to identify when a statement might be skewed towards a particular preference, we are dependent on our ability to gather other interview subjects' opinions about such statements in order to assess their validity. Where this becomes complicated is in regard to the order in which the interviews are conducted. As an example, the representative of the

MNO who favors the single turnkey provider model is the first one to get interviewed among representatives of the three MNOs. This means that that interview subject's statements are available to be run by a multitude of interview subjects holding other opinions about NGN. Conversely, the statements made in later interviews by representatives of MNOs arguing for other deployment models, such as for instance the multi-operator model, are not run past the interview subject holding the opposing view of preferring a single turnkey provider model, and may thus receive less scrutiny. While it is our belief that all deployment model alternatives have been given fair consideration in conjunction with the suggestion of a particular model, concerns such as this have to be kept in mind when reflecting on the conclusions of this project.

As for the interpretation of the results themselves it has been eluded to several times throughout this thesis that while we make an attempt at providing a fair evaluation of the gathered evidence in order to give a suggestion for how to proceed with NGN, all of that which is presented herein are products of our interpretations. Considering the fact that even the excerpts provided from interviews in Chapter 4 are subject to our own translation, as the original interviews are conducted in Norwegian, the inclusion of the transcripts as appendices to the thesis is considered to be an attempt to preserve the integrity of the researchers that make the aforementioned interpretations. As noted in Section 4.4, readers are encouraged to consult the transcripts themselves in order to form their own opinion on the topic. We do, however, believe that while others might come to different conclusions based on their own reasoning regarding deployment models, the way in which the results have been presented can be considered to be as unbiased as it would be reasonable to expect from a work like this. Nevertheless, this too is a concern that is important to keep in mind when reflecting on the conclusions of this project.

## 5.5 Regarding the relevance of criteria

This section aims to regard the question of whether or not the selection that has been made of comparison criteria can be said to be relevant, and, more interestingly, whether or not a different selection of comparison criteria could potentially have led to a different outcome in terms of suggesting a particular deployment model for NGN. We will not repeat the justifications made for selecting each of the comparison criteria, as it was covered in detail in Section 2.4. However, among other things, we find it interesting to entertain the thought of alternative comparison criteria and the effects they may potentially have had on the selection of deployment models. As most considerations made in regard to deployment models are made through a lens of one or more of the comparison criteria, taking a moment to question their relevance to the bigger picture of a next generation PSN might be a worthwhile exercise. In Section 5.2 we explored how one may decide to weigh comparison criteria unevenly in order to better reflect one's own beliefs regarding the important qualities of a PSN. While we

would be hard-pressed to imagine anyone downplaying the importance of robustness, a lesser interest might certainly be taken in the criteria of flexibility and security. In a fit of optimism one might even be inclined to disregard the apparent downsides of complexity as being something that one would expect to solve in the future without problem. In either case the lens in which one would regard arguments in favor and opposition of various alternative deployment models could change drastically without that necessarily invalidating the reasoning and conclusions that would follow from arguing through a different lens.

The most prominent example of a deployment model that could potentially end up as the chosen one by a slight change in the weighing of comparison criteria is the single turnkey provider model. The biggest drawbacks related to this model are primarily tied up in the flexibility criterion. If one decides to afford flexibility less importance, it would naturally follow that the arguments in opposition of the single turnkey provider model are significantly weakened, and as such it might suddenly rise through the ranks to become the favored alternative deployment model for NGN. As another example, one could also argue more strongly in favor of the multi-operator model in the event that the comparison criterion of complexity is awarded less agency.

In terms of alternative comparison criteria there is a single one that comes to mind as being particularly interesting and that is the aspect of state control. While it is not among the four defined comparison criteria, it is an aspect of deployment models that have nonetheless been awarded some attention throughout the discussion regarding the choice of a deployment model for NGN. The reason state control has not been considered as a comparison criterion of its own is that we consider the benefit and drawbacks associated with differing levels of state control to be too difficult to say anything certain about. For instance, opposed to something like robustness, of which it is relatively easy to argue that more is better, it is not entirely clear to us whether or not a large degree of state control can be considered to be beneficial for a PSN in and of itself. As such, state control has been argued about in conjunction with the comparison criterion of security and the criterion of flexibility. However, it is not difficult to imagine that others, possessing other preconceived notions about PSNs than us, could easily come to a different conclusion in regard to state control. Furthermore we accept the very real possibility that there might exist other alternative candidates for the position of comparison criterion that we have not considered in this thesis.

# Chapter 6
# Conclusion

As a way of rounding out the thesis, the aim of this chapter is to provide a short reflection on the findings that have been made, particularly in regard to the research questions proposed in Section 1.5 and the original problem description of this project. To reiterate, the objectives of the project have been to examine alternative deployment models for a broadband PSN, with emphasis on the way in which the state should be involved in a potential solution. The Norwegian situation is considered throughout the thesis as a prominent case study serving the purpose of a foundation on which to lay argumentation for different alternative deployment model strategies.

In Chapter 5 a suggestion is made which recommends the use of a deployment model based on a state-owned MVNO for NGN. The argumentation leading up to and culminating in this recommendation is based on various findings made throughout this research project, with particular emphasis on information gathered from interviews. In order to be able to reach a conclusive verdict on which deployment model appears to be most suited for employment in relation to NGN, a number of alternatives are considered alongside their associated benefits and drawbacks. Additionally, broadband PSN solutions deployed or planning to be deployed in other countries are examined as a way to expand our understanding of the possibility space for the next generation of public safety communications outside the borders of Norway. As such, we believe the first research question proposed in Section 1.5 regarding the identification and evaluation of alternative deployment models to have been answered in a satisfactory manner. Furthermore, through identifying and arguing in favor and opposition of a multitude of alternative deployment models including the way in which the state would be involved in each model, we believe the second research question, as well as the tasks put forward in the problem description to this project, to also have been answered. As we provide a recommended solution for the deployment of NGN, considerations regarding the proposed deployment model naturally encompass suggestions as to what we believe to be the optimal way in which to involve the state in a next generation PSN.

## 6.1 Future work

There are a couple of ways in which further research on this topic may be conducted that revolve around two distinct things. The first regards those considerations that are considered to be outside the scope of this project, such as the economical ramifications of selecting a deployment model for NGN. As is noted in Section 1.6 when discussing the scope of the project, the monetary cost of various alternative deployment models is likely something that will be able to influence the decision making process regarding the Norwegian authorities approach to NGN significantly. However, as the study of economics and finance is not our forte, we leave such analyses to be conducted by others. Although we can do nothing except speculate in regard to this, we intuitively believe that our favored model involving a state-owned MVNO could potentially lose out to a single turnkey provider model in terms of the mere price tag associated with the project.

The second avenue of research to pursue in regard to the topic in question relates to the fact that the subject matter of next generation public safety communications is being constantly developed. As an example, regards made about the way in which other countries conduct their next generation PSN related projects have had to be updated repeatedly throughout the course of this project, as new decision have been made by their respective governing authorities regarding aspects such as time frames and progress. In the case of Norway and NGN, the time is soon nigh for the Norwegian governing authorities to make a decision regarding the preferred deployment model of NGN based on suggestions they have received from DSB and Nkom, and thereby ushering in the next phase of the project. Once this decision has been reached, goal-oriented research could be conducted into discovering the true consequences of the choices made. A central topic of discussion would be the assessment of whether or not the Norwegian state seem to have made a sound decision or not, as well as discussing the trade-offs that would have had to be made in order to reach a decision. Simultaneously with this development happening in Norway, the technology and specifications of 5G and MCX will be continuously improved and refined by industry actors and standardization organizations around the world, contributing to the removal of uncertainty from the equation of next generation PSNs. While we can not know exactly what the future will bring, we believe any work such as this one, which attempts to shed light on considerations that must be made on the path to broadband public safety communications, to possess inherent value.

# References


[3GP18a] Mission Critical Data services (Release 16). TS 22.282 V16.4.0, The 3rd Generation Partnership Project (3GPP), December 2018.

[3GP18b] Mission Critical Video services (Release 16). TS 22.281 V16.0.0, The 3rd Generation Partnership Project (3GPP), September 2018.

[3GP19] Mission Critical Push To Talk (MCPTT); Stage 1 (Release 17). TS 22.179 V17.0.0, The 3rd Generation Partnership Project (3GPP), December 2019.

[3GP20a] Mission Critical Services Common Requirements (MCCoRe); Stage 1 (Release 17). TS 22.280 V17.3.0, The 3rd Generation Partnership Project (3GPP), July 2020.

[3GP20b] System architecture for the 5G System (5GS); Stage 2 (Release 16). TS 23.501 V16.7.0, The 3rd Generation Partnership Project (3GPP), December 2020.

[BAMH20] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, and Andrew Hines. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks*, 167:106984, February 2020.

[Bla21] John Black. ESN: a big picture update. Presentation at BAPCO 2021, ESN, March 2021.

[CCA18] Erillisverkot selected as the operator of the mobile broadband service for authorities in Finland. News Article, The Critical Communications Authority (TCCA), March 2018. URL: https://tcca.info/erillisverkot-selected-as-the-operator-of-the-mobile-broadband-service-for-authorities-in-finland/, Accessed: 2020-03-18.

[DSB17] Neste generasjon nødnett i kommersielle nett: Fremgangsmåte for videre arbeid. Memorandum, The Norwegian Directorate for Civil Protection (DSB) and the Norwegian Communications Authority (Nkom), October 2017.

[DSB18] Alternatives for mission-critical services in public mobile networks in Norway. Report, The Norwegian Directorate for Civil Protection (DSB), May 2018.

[DSB20] Nødnett i bruk. Report, The Norwegian Directorate for Civil Protection (DSB), June 2020. Version 1.3.

[Eri21] Virve is becoming a broad-band service – this is how the development is progressing. News Article, Erillisverkot, May 2021. URL: https://www.erillisverkot.fi/en/virve-is-becoming-a-broad-band-service-this-is-how-the-development-is-progressing/, Accessed: 2021-06-21.

[ETS20] Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design. EN 300 392-1 V1.6.1, The European Telecommunications Standards Institute (ETSI), April 2020.

[FN21] Rising to the Challenge. Fiscal Year 2020 Annual Report to Congress, First Responder Network Authority (FirstNet), February 2021.

[GGM+20] P. Grønsund, A. Gonzalez, K. Mahmood, K. Nomeland, J. Pitter, A. Dimitriadis, T. Berg, and S. Gelardi. 5G Service and Slice Implementation for a Military Use Case. In *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*, pages 1–6, June 2020. ISSN: 2474-9133.

[HC21] Home Office recall/Windrush compensation scheme, HC 174. Oral evidence given to the Public Accounts Committee, The House of Commons, June 2021.

[HLS+18] Marko Höyhtyä, Kalle Lähetkangas, Jani Suomalainen, Mika Hoppari, Kaisa Kujanpää, Kien Trung Ngo, Tero Kippola, Marjo Heikkilä, Harri Posti, Jari Mäki, Tapio Savunen, Ari Hulkkonen, and Heikki Kokkinen. Critical Communications Over Mobile Operators' Networks: 5G Use Cases Enabled by Licensed Spectrum Sharing, Network Slicing and QoS Control. *IEEE Access*, 6, December 2018.

[Jac21] Donny Jackson. Motorola Solutions CEO anticipates extension of Airwave contract in UK by end of year. News Article, IWCE's Urgent Communications, May 2021. URL: https://urgentcomm.com/2021/05/26/motorola-solutions-ceo-anticipates-extension-of-airwave-contract-in-uk-by-end-of-year/, Accessed: 2021-06-07.

[KPMP16] Panayiotis Kolios, Andreas Pitsillides, Osnat Mokryn, and Katerina Papdaki. Chapter 7 - Data Dissemination in Public Safety Networks. In Daniel Câmara and Navid Nikaein, editors, *Wireless Public Safety Networks 2*, pages 199–225. Elsevier, January 2016.

[NAO16] Upgrading emergency service communications: the Emergency services Network. Report by the Comptroller and Auditor General, The British National Audit Office (NAO), September 2016.

[NAO19] Progress delivering the Emergency Services Network. Report by the Comptroller and Auditor General, The British National Audit Office (NAO), May 2019.

[ON20] A. Othman and N. A. Nayan. Public Safety Mobile Broadband System: From Shared Network to Logically Dedicated Approach Leveraging 5G Network Slicing. *IEEE Systems Journal*, pages 1–12, 2020.

[PRVS+19] J. Pérez-Romero, I. Vilà, O. Sallent, B. Blanco, A. Sanchoyerto, R. Solozábal, and F. Liberal. Supporting Mission Critical Services through Radio Access Network Slicing. In *2019 International Conference on Information and Communication*

*Technologies for Disaster Management (ICT-DM)*, pages 1–8, December 2019. ISSN: 2643-6868.

[RM16] Colin Robson and Kieran McCartan. *Real world research: a resource for users of social research methods in applied settings*. Wiley, Hoboken, 4th edition, 2016.

[RR20] Elisa, Ericsson Win Finland's 10-Year Public-Safety Broadband Contracts. News Article, RadioResource Media Group, April 2020. URL: https://www.rrmediagroup.com/News/NewsDetails/NewsID/19535, Accessed: 2021-03-18.

[Sam17] Mer båndbredde for bedre mobile tjenester. Press Release, The Norwegian Ministry of Transport (Samferdselsdepartementet), December 2017. URL: https://www.regjeringen.no/no/aktuelt/mer-bandbredde-for-bedre-mobile-tjenester/id2581485/, Accessed: 2021-02-08.

[Sch18] Stefan Schröder. Security in 5G inter-network signalling. Presentation at ETSI security week, Telekom Security, June 2018.

[SHM21] Morten Stenstadvold, Per-Trygve Hoff, and Tom E. Markussen. Etterevaluering av TETRA Nødnettprosjektet. Report on behalf of the Concept Research Programme, Agenda Kaupang, January 2021.

[SJD20] Uppdrag till Myndigheten för samhällsskydd och beredskap att anskaffa och tillhandahålla tjänster för mobil datakommunikation till användare av Rakelsystemet. Minesterial Decree, The Swedish Justice Department (Ju), June 2020.

[SMS+17] M. Shafi, A. F. Molisch, P. J. Smith, T. Haustein, P. Zhu, P. De Silva, F. Tufvesson, A. Benjebbour, and G. Wunder. 5G: A Tutorial Overview of Standards, Trials, Challenges, Deployment, and Practice. *IEEE Journal on Selected Areas in Communications*, 35(6):1201–1221, June 2017.

[SOU18] Frekvenser i samhällets tjänst: Betänkande av Utredningen om radiospektrumanvändning i framtiden. Report, The Swedish Government Official Reports (SOU), December 2018.

[SPRS+19] M. R. Spada, J. Pérez-Romero, A. Sanchoyerto, R. Solozabal, M. A. Kourtis, and V. Riccobene. Management of Mission Critical Public Safety Applications: the 5G ESSENCE Project. In *2019 European Conference on Networks and Communications (EuCNC)*, pages 155–160, June 2019. ISSN: 2575-4912.

[SSA+18] R. Solozabal, A. Sanchoyerto, E. Atxutegi, B. Blanco, J. O. Fajardo, and F. Liberal. Exploitation of Mobile Edge Computing in 5G Distributed Mission-Critical Push-to-Talk Service Deployment. *IEEE Access*, 6:37665–37675, 2018.

[SSBL19] A. Sanchoyerto, R. Solozabal, B. Blanco, and F. Liberal. Analysis of the Impact of the Evolution Toward 5G Architectures on Mission Critical Push-to-Talk Services. *IEEE Access*, 7:115052–115061, 2019.

[Tjo20] Aksel Tjora. *Kvalitative forskningsmetoder i praksis*. Gyldendal, 3rd edition, 2020.

[Toi21] Ari Toivonen. Virve 2.0 on the path to critical broadband - the Finnish way. Presentation at BAPCO 2021, Erillisverkot, March 2021.

[USC12] Middle Class Tax Relief and Job Recovery Act of 2012. Public Law 112-96, The United States Congress, February 2012.

[VS21] Mojca Volk and Janez Sterle. 5G Experimentation for Public Safety: Technologies, Facilities and Use Cases. *IEEE Access*, 9:41184–41217, March 2021.

[Wal98] Kerry Walk. How to Write a Comparative Analysis. Writing Resource, The Writing Center at Harvard University, 1998. URL: https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis, Accessed: 2021-05-04.

[Yar20] Abdulrahman Yarali. *Public Safety Networks from LTE to 5G*. John Wiley & Sons, February 2020.

# Appendix A
# Application to NSD

The following 11 pages contain the application to the Norwegian centre for research data (NSD) regarding the handling of personal information in connection with this research project. It was approved by the NSD on the 20th of November 2020.

The application is in Norwegian and describes the need for processing background information about the interviewees and voice recordings of the interviews. It also describes measures taken in order to protect the privacy of the interviewees, as well as the rights of the interviewees in regards to this project and how the interviewees are informed of said rights.

The first 7 pages of this appendix following this preface contain the application itself as it was submitted and approved, while the last 4 pages contain the pamphlet informing the interviewees of the project and their rights should they agree to participate. As an attachment to the application as a whole, this pamphlet has also been approved by the NSD.

NSD NORSK SENTER FOR FORSKNINGSDATA

## Meldeskjema 570129

**Sist oppdatert**

20.11.2020

**Hvilke personopplysninger skal du behandle?**

---

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

**Type opplysninger**

---

**Du har svart ja til at du skal behandle bakgrunnsopplysninger, beskriv hvilke**

Stilling, eller ihvertfall rolle, og hva slags type organisasjon personen tilhører. For eksempel "systemarkitekt ved en av Norges tre kommersielle mobile nettverksoperatører." I tillegg kan personer muligens identifiseres til en viss grad baser på informasjonen de deler, ettersom det kan være et begrenset antall personer som har innsikt i temaet.

**Skal du behandle særlige kategorier personopplysninger eller personopplysninger om straffedommer eller lovovertredelser?**

Nei

**Prosjektinformasjon**

---

**Prosjekttittel**

NTNU IIK Masteroppgave: Mission Critical Services in 5G

**Prosjektbeskrivelse**

Innhente informasjon om neste generasjons Nødnett-tjenester fra relevante aktører ved bruk av intervju som metode.

**Begrunn behovet for å behandle personopplysningene**

I og med at vi skal intervjue personer direkte, er det nødvendigvis behov for å vite navnene til disse

personene. Det er ikke nødvendig å benytte navnene i oppgaven.

Lydopptak av intervjuet kan være et viktig hjelpemiddel for å kunne, så korrekt som mulig, gjengi det som blir sagt under intervjuet. Lydopptaket vil kun bli benyttet til å transkribere, og det vil ikke være aktuelt å presentere selve lydopptaket. Transkriptet vil bli delvis anonymisert for å hindre identifisering av intervjuobjektet, som beskrevet i neste avsnitt om bakgrunnsopplysninger.

Det vil være nødvendig å behandle og presentere bakgrunnsopplysninger om intervjuobjektene i oppgaven, for å tilføre kontekst til informasjonen som blir lagt frem i intervjuene. Dette vil være generaliserte opplysninger vedrørende personens relevant funksjon, som for eksempel "driftsingeniør i et kommersielt teleselskap."

**Ekstern finansiering**

**Type prosjekt**

Studentprosjekt, masterstudium

**Kontaktinformasjon, student**

Eivind Standal, eivista@stud.ntnu.no, tlf: 46433664

**Behandlingsansvar**

---

**Behandlingsansvarlig institusjon**

Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

**Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)**

Eirik Larsen Følstad, eirik.folstad@ntnu.no, tlf: 92044740

**Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?**

Nei

**Utvalg 1**

---

**Beskriv utvalget**

Representanter for brukere av Nødnett, for eksempel personer fra Nødnetts brukerorganisasjoner.

**Rekruttering eller trekking av utvalget**

Rekrutterer gjennom veileders nettverk

**Alder**

18 - 100

**Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?**

Nei

**Personopplysninger for utvalg 1**

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

**Hvordan samler du inn data fra utvalg 1?**

**Personlig intervju**

**Grunnlag for å behandle alminnelige kategorier av personopplysninger**

Samtykke (art. 6 nr. 1 bokstav a)

**Informasjon for utvalg 1**

**Informerer du utvalget om behandlingen av opplysningene?**

Ja

**Hvordan?**

Skriftlig informasjon (papir eller elektronisk)

**Utvalg 2**

---

**Beskriv utvalget**

Representanter for kommersielle mobile nettverksoperatører. Eksempler på intervjuobjekter kan være personer som har innsikt og kompetanse om de tre norske nettverksoperatørenes operasjoner og interesser.

**Rekruttering eller trekking av utvalget**

Rekrutterer gjennom veileders nettverk

**Alder**

18 - 100

**Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?**

Nei

**Personopplysninger for utvalg 2**

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

**Hvordan samler du inn data fra utvalg 2?**

**Personlig intervju**

**Grunnlag for å behandle alminnelige kategorier av personopplysninger**

Samtykke (art. 6 nr. 1 bokstav a)

**Informasjon for utvalg 2**

**Informerer du utvalget om behandlingen av opplysningene?**

Ja

**Hvordan?**

Skriftlig informasjon (papir eller elektronisk)

**Utvalg 3**

---

**Beskriv utvalget**

Representanter for statlige interesser og organisasjoner tilknyttet Nødnett. Eksempler på organisasjoner kan være DSB, Forsvarsbygg, Justisdepartementet, etc.

**Rekruttering eller trekking av utvalget**

Rekrutterer gjennom veilederes nettverk

**Alder**

18 - 100

**Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?**

Nei

**Personopplysninger for utvalg 3**

- Navn (også ved signatur/samtykke)
- Lydopptak av personer
- Bakgrunnsopplysninger som vil kunne identifisere en person

**Hvordan samler du inn data fra utvalg 3?**

**Personlig intervju**

**Grunnlag for å behandle alminnelige kategorier av personopplysninger**

Samtykke (art. 6 nr. 1 bokstav a)

**Informasjon for utvalg 3**

**Informerer du utvalget om behandlingen av opplysningene?**

Ja

**Hvordan?**

Skriftlig informasjon (papir eller elektronisk)

**Tredjepersoner**

---

**Skal du behandle personopplysninger om tredjepersoner?**

Nei

**Dokumentasjon**

---

**Hvordan dokumenteres samtykkene?**

- Elektronisk (e-post, e-skjema, digital signatur)
- Muntlig

**Beskriv**

Samtykke innhentes elektronisk på e-post ved innkallelse til intervju, og muntlig på lydopptak ved gjennomføring av intervju.

**Hvordan kan samtykket trekkes tilbake?**

Elektronisk på e-post eller muntlig under intervjuet.

**Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?**

Ved å sende en elektronisk forespørsel på e-post. Alle intervjuobjekter vil bli tilsendt transkripter fra sine respektive intervjuer, hvorpå det er mulighet for å rette eller slette opplysninger vi har samlet inn.

**Totalt antall registrerte i prosjektet**

1-99

## Tillatelser

**Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?**

## Behandling

**Hvor behandles opplysningene?**

- Maskinvare tilhørende behandlingsansvarlig institusjon

**Hvem behandler/har tilgang til opplysningene?**

- Student (studentprosjekt)
- Databehandler

**Hvilken databehandler har tilgang til opplysningene?**

Masterstudentene Eivind Standal og Lina Hexeberg Hovden. Vi benytter NTNU OneDrive for lagring av data, og programmet NVivo med NTNUs lisens for databehandling. Videointervjuene vil foregå på Zoom, som NTNU har en databehandleravtale med.

**Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?**

Nei

## Sikkerhet

**Oppbevares personopplysningene atskilt fra øvrige data (kodenøkkel)?**

Nei

**Begrunn hvorfor personopplysningene oppbevares sammen med de øvrige opplysningene**

Vi behandler ikke særlige eller strafferettslige opplysninger, og oppbevarer personopplysningene sammen med øvrige opplysninger av praktiske årsaker.

**Hvilke tekniske og fysiske tiltak sikrer personopplysningene?**

- Endringslogg
- Flerfaktorautentisering
- Adgangsbegrensning
- opplysningene krypteres under lagring

## Varighet

### Prosjektperiode

11.01.2021 - 25.06.2021

### Skal data med personopplysninger oppbevares utover prosjektperioden?

Nei, data vil bli oppbevart uten personopplysninger (anonymisering)

### Hvilke anonymiseringstiltak vil bli foretatt?

- Lyd- eller bildeopptak slettes
- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres

### Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Ja

### Begrunn

Som nevnt tidligere vil det potensielt være mulighet for å identifisere personer basert på bakgrunnsopplysninger publisert i prosjektet.

## Tilleggsopplysninger

Vi er to studenter som gjennomfører intervjuer sammne, men skriver ulike masteroppgaver. Det er levert en søknad for hvert av prosjektene, på tross av at intervjuene sammenfaller. Prosjektene har samme veileder og er ved samme institusjon.

# Vil du delta i forskningsprosjektene "Mission Critical Services in Commercial 5G Networks" og "Autonomous Operation of Mission Critical Base Stations in 5G"?

Dette er et spørsmål til deg om å delta i to forskningsprosjekt vedrørende Nødnett og 5G. Vi er to studenter med to ulike masteroppgaver som berører samme tema, og gjennomfører derfor intervjuer sammen. Den ene oppgaven har til formål å utforske problemstillinger rundt samarbeid mellom staten og kommersielle mobilnettoperatører om tilbydelse av Nødnett i 5G, og den andre vil kartlegge utfordringer knyttet til autonom operasjon av basestasjoner i Nødnett. I dette skrivet gir vi deg informasjon om prosjektenes målsetninger og hva deltakelse vil innebære for deg.

**Formål**

Begge masteroppgavene utføres av studenter ved Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK) ved NTNU. Selv om oppgavene har forskjellig formål, har begge behov for å kartlegge potensialet for utførelse av Nødnett i 5G.

Eivind sin oppgave forsøker å besvare følgende forskningsspørsmål omhandlende et eventuelt samarbeid mellom staten og en eller flere mobile nettverksoperatører om neste generasjon av Nødnett:

- Hvilke ulike alternativer finnes det for å realisere Nødnett i 5G i samarbeid med kommersielle aktører?
- Hva er fordelene og ulempene ved disse ulike alternativene?
- Hvilke sentrale vurderinger bør gjøres rundt denne problemstillingen før en eventuell avgjørelse fattes?

Lina sin oppgave bygger på følgende forskningsspørsmål relatert til autonom operasjon av basestasjoner i Nødnett i 5G:

- Hvilke tjenester blir viktigst for sluttbrukerne av autonome basestasjoner i Nødnett?
- Hva er de viktigste operasjonelle utfordringene?
- Hva er de viktigste overordnede tekniske utfordringene?

**Hvem er ansvarlig for forskningsprosjektet?**

Eivind Standal har ansvaret for sin oppgave, "Mission Critical Services in Commercial 5G Networks". Lina Hexeberg Hovden har ansvar for oppgaven "Autonomous Operation of Mission Critical Base Stations in 5G". Begge er masterstudenter ved NTNU. NTNU har hovedansvaret for prosjektet ved førsteamanuensis Eirik Larsen Følstad.

**Hvorfor får du spørsmål om å delta?**
For å forbedre vår forståelse av temaet og vårt informasjonsgrunnlag for videre diskusjon rundt potensielle løsninger, inviterer vi personer med relevant kompetanse om og tilknytning til Nødnett, 5G, og relaterte teknologier til å delta på intervju. Ambisjonen vår er å intervjue representanter for ulike organisasjoner, statlige organer og kommersielle aktører som er eller kan komme til å bli involvert i prosesser rundt etablering og bruk av en Nødnett-løsning i 5G. Kontakten med utvalgte intervjuobjekter vil kunne opprettes gjennom veileder Eirik Larsen Følstads kontaktnettverk.

**Hva innebærer det for deg å delta?**
Deltakelse innebærer et intervju med varighet på ca. 1 time, med mulighet for et oppfølgingsintervju på et senere tidspunkt om det skulle være behov for og ønske om det. Intervjuet vil foregå fysisk eller ved videokonferanse. Intervjuet vil være på ustrukturert form, med mål om å ha en flytende samtale der din rolle og kunnskap om relevante temaer vil være toneangivende for videre utspørring. På tross av intervjuets ustrukturerte natur vil det være ønskelig å geleide samtalen inn på flere kjerneområder, og få svar på sentrale spørsmål fra de to oppgavene. Det vil være noe fokus på tidsstyring for at begge oppgavene skal bli tildelt tilstrekkelig tid under intervjuet. Dersom det er løse tråder etter intervjuet og videre samtale ønskes fra både deg og oss, kan det bli aktuelt å ha et oppfølgingsintervju på et senere tidspunkt. Du vil bli forelagt et anonymisert transkript fra intervjuet, og det vil være rom for å komme med tilleggsinformasjon og tydeliggjøre eller trekke tilbake det som har blitt sagt under intervjuet. Transkriptet vil benyttes i diskusjoner i masteroppgaven. Det vil også kunne bli publisert i oppgaven (som vedlegg).

**Det er frivillig å delta**
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

**Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Kun studentene, Eivind og Lina, vil gjennomføre intervjuene og ha tilgang til dataen. Det anonymiserte transkriptet fra intervjuene vil kunne bli diskutert med veileder Eirik Larsen Følstad, førsteamanuensis ved NTNU.

Dataen vi registrerer er:
- Ditt navn
- Din stilling/rolle og organisasjon
- Lydopptak fra intervjuet
- Eventuelle notater fra intervjuet
- Anonymisert transkript

Lydopptak og eventuelle notater vil lagres og behandles konfidensielt på NTNU. Dataene lagres på NTNU sin OneDrive. Vi benytter endringslogg og adgangsbegrensning som videre sikkerhetsmekanismer. I transkriptet anonymiseres du og din tilhørighet, for eksempel som "systemarkitekt hos en norsk mobil nettverksoperatør." Vi anser det som nødvendig å gi en generalisert beskrivelse av din rolle for å sette informasjonen fra intervjuet i kontekst. Du vil bli forelagt transkriptet og vil bli gitt muligheten til å komme med revideringer av dette. Dette transkriptet er det eneste av informasjonen vi samler inn som kan komme til å bli publisert i oppgaven. Transkriptet vil brukes i diskusjoner i oppgaven, sammen med en generalisert beskrivelse av din stilling/rolle.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**
Prosjektet avsluttes etter planen innen 25. juni 2021. Lydopptakene vil permanent slettes når de er transkribert. Et anonymisert transkript vil kunne tilgjengeliggjøres som vedlegg til masteroppgavene.

**Dine rettigheter**
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

**Hva gir oss rett til å behandle personopplysninger om deg?**
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra NTNU har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

**Hvor kan jeg finne ut mer?**
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- NTNU – Institutt for informasjonssikkerhet og kommunikasjonsteknologi (IIK) ved
  - Eirik Larsen Følstad, førsteamanuensis – eirik.folstad@ntnu.no
  - Eivind Standal – eivista@stud.ntnu.no
  - Lina Hexeberg Hovden – linahh@stud.ntnu.no
  - Thomas Helgesen, personvernombud – thomas.helgesen@ntnu.no

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen prosjektansvarlige

Eirik Larsen Følstad Eivind Standal Lina Hexeberg Hovden

---

# Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektene vedrørende Nødnett og 5G, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ▢ å delta i intervju med lydopptak
- ▢ at et anonymisert transkript fra intervjuet vil legges ved og brukes i oppgavene dersom jeg godkjenner innholdet i dette transkriptet

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca 25. juni 2021.

---

(Signert av prosjektdeltaker, dato)

# Appendix B
# Health Services A

This interview is with an interview subject possessing substantial knowledge about Norwegian emergency health services, their use of the existing Nødnett, and the process towards NGN. The interview covers both challenges related to limitations of the existing Nødnett, as well as expectations and concerns surrounding NGN.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Og så spør jeg deg om det er greit at vi gjør opptak av intervjuet, sånn at vi kan transkribere det. |
| 2 | I | Det er greit. |
| 3 | E | Da kan jeg starte med å presentere min egen masteroppgave. For vi skriver jo to ulike masteroppgaver, men vi har samme veileder og det handler om noe av de samme tingene relatert til Nødnett og neste generasjon av Nødnett i 5G hovedsakelig. Min oppgave handler om å vurdere forhold relatert til eierskap og drift av kjernenettet med tanke på at man ikke skal ha et eget Nødnett sånn som man har i dag, men skal samarbeide med kommersielle mobiloperatører for å tilby tjenestene. Og ulike vurderinger rundt hvordan man skal fordele ansvarsoppgaver i kjernenettet. |
| 4 | I | Ja, hvis det blir den løsningen da. Det er jo ikke vedtatt hva slags modell man skal gå for enda. |
| 5 | E | Ja, ulike vurderinger som må gjøres rundt det. |
| 6 | L | Mhm, jeg ser litt mer teknisk på saken. Jeg ser på autonom operasjon av en eller flere basestasjoner i Nødnett, i caset der vi ser på 5G. Så jeg ser på tekniske og operasjonelle utfordringer og løsninger knyttet til det. Og det jeg synes er spennende nå når jeg snakker med deg er å se på hvordan behovene til helse er og hvordan dere vil prioritere løsninger eller brukertjenester i en kritisk situasjon i 5G. |
| 7 | I | Mhm, men det er bare via basestasjon? Det er ikke å se på eventuelle muligheter for at devicene kan snakke direkte med hverandre utenom basestasjon? |
| 8 | L | Jeg ser på andre muligheter også, ja. |
| 9 | I | Du ser på det, ja, men det er bra. |
| 10 | L | Mhm, vil du presentere hvem du er? |
| 11 | I | Ja, [navn] heter jeg. Jeg jobber i [arbeidsplass] og har IKT-bakgrunn, men også noe helseerfaring fra [arbeidsplass]. Jeg har erfaring fra nød og beredskap. |
| 12 | E | Vi kommer nok til å generalisere det en del, hehe. |
| 13 | L | Absolutt. |
| 14 | E | Ja, så vi kan jo begynne å snakke om hvordan Nødnett fungerer i dag i helsetjenesten - Nå høres det på en måte ut som om du har kunnskap om hvordan Nødnettet brukes i mange ulike sammenhenger, men hvis vi fokuserer på helse i denne omgang. Kan vi snakke litt om hvordan Nødnettet brukes i helse i dag, og hvilke behov og hvilke utfordringer som man har med det nåværende nettet. |
| 15 | I | Ja, nå er jeg ikke noen stor bruker av Nødnett sånn i det daglige - Jeg bruker det litt. Men jeg regner med at dere har lest, det finnes vel noen evalueringsrapporter og sånn som dere vel kanskje har tilgang til, men vårt - eller mitt - inntrykk er vel at det fungerer bra til talekommunikasjon. Altså gruppebasert talekommunikasjon, som jo selvfølgelig var primærkravet når man innførte det. Og der har jeg inntrykk av at det fungerer stort sett bra. |

| | | |
|---|---|---|
| | | Lite klager på det i utgangspunktet, mellom de tre nødetatene. Og så brukes det jo en del av andre brukere også, frivillige organisasjoner og beredskapsrelaterte organisasjoner som el-verkene og sånne ting, selv om det er litt begrenset der. Så til tale så fungerer det vel rimelig bra på talegrupper. |
| 16 | I | Så er det selvfølgelig ikke alle brukergrupper som er like komfortable med det med gruppekommunikasjon. Vi har jo for eksempel dette med legene, legevaktslegene som er ute å kjører og sånne ting. De er jo noe i talegrupper når de skal samhandle med ambulanser og sånn, men de har ofte behov for det vi kaller en-til-en samtaler. Altså mer en toveis telefonsamtale via radiosystemet. Der har systemet vist seg å ha en del begrensninger, særlig på talekvalitet. Det går litt på brukervennlighet, men mye på talekvalitet som man mener er for dårlig. Sånn at der brukes det nok mye mobiltelefon i praksis. Det er noen som bruker radio, det er fullt mulig å bruke en-til-en samtaler i Nødnett, men det er noe med kodeken og sånt som gjør at det blir dårlig. Ihvertfall hvis du har litt dårlig dekning så blir det mye dårligere talekvalitet enn det gjør på en mobiltelefon. Så det har vist seg litt begrensende. |
| 17 | I | Og det gjelder jo også ambulansetjenesten, fordi at mye av den samvirkedelen/akuttdelen skjer jo i disse talegruppene hvor man nøkler og sånt, men når ambulansen da for eksempel skal melde inn pasienten til AMK eller til sykehuset og beskrive mer hva som har skjedd i detalj, og kanskje snakke med en lege inne på sykehuset som kanskje heller ikke er bruker av Nødnett, så bruker de ofte mobiltelefon. Det går jo også an å ringe inn med Nødnett-terminalen til de som har mobiltelefon, men der blir det også litt for dårlig talekvalitet. Så man ender nok opp med veldig mange steder at de bruker mobiltelefonen til det og ikke Nødnett-terminalen. |
| 18 | L | Tror du at de bruker mobiltelefonen mest på grunn av talekvalitet, eller er det også på grunn av personvern? Siden det er pasientinformasjon som ikke skal over talegruppe. |
| 19 | I | For det første så er det ofte ikke privattelefon da, det er jo gjerne tjenestetelefon man har. Veldig mange ambulanser har jo en mobiltelefon som tilhører ambulansen. Nei, altså, de ønsker gjerne å snakke en-til-en istedenfor gruppe i visse tilfeller. Det går litt på talekvalitet, men også taushetsplikten - at det bare er én som skal høre det som sies. Og når de skal snakke med legen på sykehuset som ikke har Nødnett-terminal, så må de jo bruke en-til-en, fordi at talegruppe til telefon blir veldig dårlig. Vi har prøvd på det, men det blir helt håpløst. Men det er klart de kunne ringt med Nødnett-terminalen da, men da får de det talekvalitetsproblemet. Også er det jo det med at når du snakker med noen som ikke er så fryktelig vant med å bruke radio så er det enklere med en-til-en, der man kan snakke i munnen på hverandre på en måte da. Altså, som en vanlig telefonsamtale der samtalen flyter litt enklere. Så det er vel sånn sett flere grunner til det. |
| 20 | L | Mm, nei, men det var interessant. |
| 21 | E | Ja, da er det riktig å forstå at dette gjerne er noe man skulle ønske at man kunne tilby i Nødnett, men at man bare ikke har fått realisert det. |
| 22 | I | Jada, vi har jo prøvd det. Vi prøvde ganske mye å gjøre noe med talekvaliteten og en del sånne ting, på å ringe sånn en-til-en mellom to radioer, eller mellom en radio og en telefon. Så vi skulle gjerne hatt det, for det hadde jo gjort at man på en måte kunne slutte helt å bruke mobiltelefon da. Og det har jo vært et ønske. I tillegg til at Nødnett jo er ansett som et lukket nett da, kontra mobiltelefonen, sånn at det kanskje var hakket sikrere. Ihvertfall i forhold til gammel GSM/2G og dette her så var vel ihvertfall Nødnett ansett som noe sikrere. Om det er noe særlig sikrere enn 5G det er jo en annen sak. Men det var jo liksom det som |

| | | |
|---|---|---|
| | | var det ønskede nettet. Og så er det jo en del sånn - nå blir vi veldig detaljerte da men - ofte så er det jo sånn at man for eksempel skal melde inn en pasient tilbake til AMK, så ønsker kanskje AMK å konferansekoble, som vi kaller det, med en lege inne på sykehuset eller med en legevakt. Sånn at man har på en måte en liten telefonkonferanse med tre deltakere. Og det er da også lite egnet i praksis i Nødnett. Det har for mye begrensninger, det støtter ikke den type ting, sånn at der er det mye enklere å håndtere en telefonsamtale, som jo kan bruke systemenes innebygde funksjonalitet for telefonkonferanser og sånn. Som gjør det mye enklere, og med bedre lydkvalitet også der enn hvis man skulle brukt Nødnett. Så klart alternativet til en telefonkonferanse er jo en gruppesamtale, altså at alle kan snakke, men det krever at alle deltakerne har en Nødnett-radio, og det er det ikke alltid man har. Hvis man skal snakke med en lege inne på sykehuset er det vel få av de som går med Nødnett-terminal, og dermed så er de nødt til å bruke telefon. At alle da er på telefon gir et bedre brukergrensesnitt og kvalitet da. |
| 23 | L | Med en telefonkonferanse så mener du bare en liten samtale der det fortsatt er alle-til-alle? |
| 24 | I | Ja. Og det er ikke en stor telefonkonferanse vi snakker om, det er bare at du - Man har et betjeningssystem på AMK-sentralen som man kaller ICCS, og du kan gjøre det samme der som du kan gjøre på en mobiltelefon. At du får en samtale og så kan du koble inn en til ved hjelp av menyen på telefonen, så du får en treveissamtale for eksempel. Og det er det samme man bruker på AMK. |
| 25 | E | Så for å gå litt videre, er det på en måte, er dette i tillegg til andre ting - Vi lurer litt på hvilke forventinger man på en måte har da, til hva slags type tjenester man kan kunne komme til å ha behov for og kan kunne komme til å kunne tilby i neste generasjon av Nødnett i bredbånds-nettverk. |
| 26 | I | Jeg har jo store forventninger til at et nytt Nødnett på en måte er mer sømløst der da, med type kommunikasjon. Som gruppesamtaler og en-til-en samtaler og det man kan kalle telefonkonferanser eller virtuelle telefonkonferanser og virtuelle gruppesamtaler. Både hvor alle kan snakke i munnen på hverandre, eller hvor én kan snakke om gangen med en knapp. At dette blir på en måte, at overgangen mellom de blir sømløs. At man kanskje kan begynne samtalen med én kommunikasjonsmåte og så finner man ut at man må gå over til en annen en fordi det er mer egnet eller man skal ha inn en telefonbruker, så switcher man bare over og at det blir mer sømløst. Det har jeg forventninger til at en ny plattform vil kunne støtte. Det gjenstår jo å se selvfølgelig, om alt det vil bli tilfredsstilt. Men at man får en mer dynamisk greie der. |
| 27 | I | Og så er det en ting til som jeg ikke nevnte i sted, av mangler i Nødnett, og det er jo datakommunikasjon. Noen trodde også at det skulle kunne brukes til det, men det har det i praksis vist at det ikke kan. Det er jo fryktelig dårlig datahastighet. Og der har også det med at man har mobilnettet, med mye høyere hastighet, og at man har da på en måte - Veldig mange av ambulansene har jo mobilt bredbånd parallelt med Nødnett, og dermed så har man endt opp med å bruke det istedenfor. Fordi at det har gitt bedre funksjonalitet der, selv om selvfølgelig oppetid har vært en utfordring. Det er jo ikke det nå, men i starten var det en stor utfordring med datakommunikasjon. For eksempel på nyttårsaften i Oslo så brøt jo mobilnettet sammen en time, alltid, på grunn av overbelastning i mobilnettet. Sånn at da kunne man bare prate sammen via Nødnett, og så forsvant muligheten til å sende oppdrag ut i bilen via mobilnettet. Alle ambulansene har PC og får vanligvis oppdrag og kartinformasjon fra AMK, og AMK kan se hvor alle ambulansene er i sitt kart fordi de sender inn sin posisjon via mobilt bredbånd. Men det kuttet da gjerne rundt midnatt på nyttårsaften de første årene, på grunn av overbelastning i mobilnettet. Men det er klart, det er ikke noe stort problem nå lenger, etter at 3G og 4G kom. Dermed så lider man ikke så mye |

| | | |
|---|---|---|
| | | av det i dag da. |
| 28 | L | I min oppgave så ser jeg jo på den edge casen der én eller en gruppe av basestasjoner har mistet tilkoblingen til kjernenettet, så du har liksom et lokalt nettverk der alle som er der kan kommunisere med hverandre. Og jeg er litt interessert, i den anledning, å forstå hva slags tjenester som er bare minimum for - |
| 29 | I | Men hva tenker du, jeg fikk ikke med meg innledningen din jeg. Var det i dagens nett eller i din prosjektoppgave eller? |
| 30 | L | I min prosjektoppgave så ser jeg på 5G, eller autonome basestasjoner da. |
| 31 | I | Altså, hva slags tjenester som er viktig der? Der er jo selvfølgelig gruppesamtaler som er det aller viktigste. Og er det bare en basestasjon som er oppe, som du har kontakt med, så er det jo et begrenset antall andre du kan snakke med. Og det har jo vært en stor begrensning i Nødnett og ikke sant, for den har jo også den funksjonen - Vi kaller det for local site trunking tror jeg. Men det har det vært stor skepsis til å skru på, fordi at - Jeg vet ikke hvor inne du er i det tekniske, men du sa jo at du var teknisk så jeg regner med at du kan en del av det. Fordi at du får jo bare snakket med de som er på den basestasjonen, og hvis den basestasjonen er satt opp til å støtte det, så vil den så vidt jeg skjønner tiltrekke seg radioer i det området til den basestasjonen. Og det er litt dumt hvis nabobasestasjonen har strøm og er på nettet, så hvis bare radioen hadde valgt - Men der er Nødnett/TETRA litt dårlig, for radioterminalene er litt dårlig på å prioritere mellom basestasjoner - Sånn at da vil man jo egentlig heller at radioen skal koble seg til en av de basestasjonene som faktisk er på nett. Sånn at i de tilfellene hvor det bare er én basestasjon som detter ut, eller som mister tilkoblingen til resten av nettet, men det er andre basestasjoner i nærheten, så ønsker man jo ikke å ha skrudd på den funksjonen, local site trunking, fordi det er bedre at radioene bare kobler seg til nabostasjonen. Men har du en bygd eller en dal da, som bare har én basestasjon, og alle radioene som er i den bygda er på den basestasjonen, da er det mer relevant å la den basestasjonen stå i det moduset. Så det er viktige ting som man også håper kommer med 5G, at devicene og basestasjonene blir mer intelligente og kan styre radioene til den basestasjonen som er mest egnet. Som har kontakt med nettet. Så vi har liten erfaring sånn sett med det i Nødnett, så vidt jeg vet. |
| 32 | L | Jeg ser jo også på, i 5G så er det ihvertfall teoretisk mulighet for at en gruppe av basestasjoner som har mistet tilkoblingen kan fungere som et lite lokalt nettverk. |
| 33 | I | Da blir det jo straks mer aktuelt, hvis de kan snakke sammen i det området hvor du er. Men igjen da, det er jo da gruppekommunikasjon selvfølgelig mellom de enhetene som er der er kanskje det aller viktigste. Hvis dette går over lengre tid og litt sånt forskjellig, så vil jo også en-til-en samtaler, at man kan ringe direkte mellom radioene, også være aktuelt. |
| 34 | L | Ser du for deg at det hadde vært interessant med push-to-video samtaler og sånne ting? |
| 35 | I | Ja, hva er push-to-video? Altså, gruppebasert video? |
| 36 | L | Ja, videosamtaler på samme måte som den push-to-talk funksjonaliteten i gruppesamtaler fungerer i dag. |
| 37 | I | Vi har ikke kommet til det i intervjuet i og for seg, men det er selvfølgelig en av de funksjonalitetene som er ønsket i det nye nettet. Og det er klart, har du en større hendelse i det stedet, og det er noen enheter som filmer og andre som gjerne skulle sett det, så er jo det absolutt en tjeneste som er aktuell også i en sånn modus. Jeg må innrømme at frem til |

| | | |
|---|---|---|
| | | Gjerdrum så har jeg vært litt skeptisk til det med nytteverdien til video, og det har også veldig mange andre vært i tjenesten. De sier at "Ja, det er fint, det er en sånn kjekt å ha-greie," men vi er jo ikke kommet så langt på video i Norge enda som de er i en del andre land. Og det er de ganske tydelige på fortsatt: Det er gruppekommunikasjon, tale, som er viktigst, og som folk mener er det - |
| 38 | I | Vi har hatt en stor diskusjon i Nødnett-arbeidet det siste året om video skal defineres som kritisk eller ikke. Altså, alle er enige om at gruppesamtaler er kritisk på tale, og så er det en stor diskusjon om vi skal definere video som oppdragskritisk, altså en funksjon som du er avhengig av for å utføre oppdraget. Til nå har man på en måte ment at det er ikke kritisk for oppdraget. Det er veldig kjekt å ha, men det er liksom ikke kritisk. Men det er klart, etter Gjerdrum så har nok mange fått opp øynene for det med video. Nettopp fordi man måtte bruke video der for å guide helikoptrene ned til disse som var forulykket. Det hadde jo blant annet med at redningshelikopteret hadde ikke infrarødt videokamera som var god nok, sånn at det var politihelikoptrene som måtte filme infrarødt, og så måtte de sitte og fortelle redningshelikopteret hvor: "Ja, litt mer til venstre litt mer til høyre," den type ting da. Mens, hvis de hadde kunnet overføre video mellom politihelikopteret og redningshelikopteret i real-time, så hadde jo det på en måte gjort operasjonen enklere da. |
| 39 | I | Og det er jo en viktig ting med neste generasjons Nødnett også, det er det at man skal kunne dele, altså ha et felles mobilt bredbånd mellom nødetatene. For det har man ikke i dag. Brann, politi, helse, ihvertfall helse og politi har jo vært sitt i praksis virtuelle mobile bredbånd gjennom en av teleleverandørene, som er etatsinternt, og som man bruker til mye oppdragsinformasjon og den type ting. Man bruker det ikke nødvendigvis så mye til video i dag, men det vil jo teoretisk være mulig hvis man hadde videokamera. Men man mangler den muligheten til å gjøre det på tvers av etatene, og med Forsvaret. Og det er en stor del av det kanskje neste generasjons Nødnett-prosjektet vil kunne etablere - Altså, teknologien finnes der i dag, du kan gjøre dette over 4G hvis du vil det. Men det er klart, det koster penger, man må lage en infrastruktur, man må ha sikkerhetsbarrierer, alt dette greiene der som man håper skal bli en del av et neste generasjons Nødnett-prosjekt. |
| 40 | I | Så jeg tenker jo på en måte at det er absolutt relevant, men det er klart i det daglige så har man ofte sett på video som en greie mellom de ute og de inne. For at de skal være med og få et situasjonsbilde, at operasjonssentralen skal kunne se hva som skjer. Og da vil det jo ikke hjelpe at du har sånn local site videooverføring. Sånn at det for veldig mange av casene på video så vil det ikke være noen vits å ha støtte for det i en sånn lokal autonom greie, men sånn Gjerdrum case, hvor på en måte noen filmer noe på et svært skadested som andre på det samme skadestedet kanskje i nærheten skal se, da er det selvfølgelig relevant at det støtter video. |
| 41 | E | Du sa innledningsvis at du var involvert i på en måte den utviklingen til neste generasjons Nødnett, og at du hadde vært involvert i den prosessen. Kan du utdype litt om hva din rolle er der, er det noen spesielle behov du skal ivareta, for eksempel helsesektorens brukeres behov. |
| 42 | I | Vi driver jo med en sånn KVU. Så det er jo fortsettelsen på forprosjektstadiet, og vi har jo ikke laget noe detaljert kravspec eller noe sånt, så det er jo veldig overordnet. Med vekt på de kravene som er styrende for hvilket konsept man skal velge. Som du nevnte dette her med om man skal basere seg på et eller flere av mobilnettene og legge et virtuelt lag oppå dette, om kjernenettet skal være offentlig og bare basestasjonene skal være private, eller om man skal bygge opp et helt nytt 5G-nett som man gjorde med Nødnett. Så det er jo alle de kravene og avveiningene som styrer det valget som på en måte har vært i fokus. Disse nettene består gjerne av tre ting: Terminaler, kjernenett - Eller basestasjoner, kjernenett og |

| | | |
|---|---|---|
| | | kontrollrom. |
| 43 | L | Men fra fokus på kontrollrom, hva er liksom hovedutfordringene som dere håper å løse med en eventuell overgang til kommersielle eller til - |
| 44 | I | Ja, altså det er jo sånn sett litt forskjell. For i Nødnett-prosjektet var anskaffelse av kontrollromsløsning en del av hovedprosjektet. Det gjorde det jo fryktelig mye mer komplekst det prosjektet, så det brant man seg kanskje litt på det. Ihvertfall DSB angrer nok litt på det noen ganger, fordi det gjorde prosjektet mye mer komplekst. Vi mener at det gjorde at man faktisk fikk løsninger som spilte sammen, men som kanskje ikke var så hypermoderne som de kanskje kunne vært. For det de har gjort i andre land er å enten å bare kjøpe nettet, at det er prosjektet, og så kommer liksom terminaler og det som er i kontrollrommene, det må hver etat ordne selv. Sverige for eksempel har hatt det sånn, og det er mulig også England har gjort det på den måten. Det gjør på en måte at man kanskje kommer kjappere i gang med kjernenettet og nettet da, men at kontrollrommene henger etter. Det har vi sett i Sverige, at de har slitt med på en måte å få avanserte kontrollromsløsninger for der har etatene måtte gjøre det selv. Mens i en del andre land har man kanskje fokusert på én etat, og å innføre Nødnett og kontrollrom for én etat, og ikke at alle tre etatene skal bli enige. Det gjør jo også prosessen vanvittig mye enklere. Så sånn sett har vi i Norge i Nødnett-prosjektet hatt den mest kompliserte utgaven: Vi skal dekke alle tre nødetatene, og vi skal dekke både utstyr ute og inne. Og det har gjort det til et komplekst prosjekt, men det gjør selvfølgelig også at det er mer integrert, de løsningene som man da til slutt får. |
| 45 | I | Men i neste generasjon så ligger det vel an til at man ikke gjør det. Man anskaffer på en måte et nett og så har hver etat sine kontrollromsprosjekter. Og det har vi jo allerede, helse har jo nå tegnet kontrakt med en leverandør av en kontrollromsløsning neste generasjons Nødnett. Fordi at man trenger en ny kontrollromsløsning. Så den løsningen vil også fungere mot dagens Nødnett såvidt jeg husker. Mens politi og brann bare såvidt har kommet i gang. De har holdt litt igjen, de har ikke vært så ivrige på å bytte ut den kontrollromsløsningen som de har i dag. Så hva vi skal få ut av det? Hvilke gevinster? Vi håper jo selvfølgelig å få en mer moderne kontrollromsløsning, for det har jo gått, holdt på å si, ti år siden den ble anskaffet, den forrige. Så den begynner å bli rimelig gammeldags. |
| 46 | I | Så vi håper jo å få en mer moderne løsning, og vi kommer nok til å satse på en mer sentralisert løsning. I forrige runde var det veldig fokus på at det skulle være autonome kontrollrom, de skulle på en måte greie seg litt selv uten alt for mye sentral infrastruktur. Sånn at det ble jo kjøpt inn til helse tre hundre kontrollrom med en del utstyr lokalt. Noe av det ble sentralisert etter hvert, for det ble helt uoverkommelig med alt det lokale utstyret. Så legevaktene, de bruker jo en sentralisert løsning hvor type tolv og tolv legevakter deler en serverløsning som står i en fjellhall. Men for AMK-sentralene så har de en seks-åtte racks hver, i hver AMK-sentral, for å ha den kontrollromsløsningen. Mens nå, i neste generasjon så satser man på en sentralisert løsning hvor alle AMK-sentralene og legevaktene og akuttmottakene kobler seg bare til en løsning som står i et sett med fjellhaller rundt omkring i landet da. Det gjør at man håper at driften skal bli enklere, forvaltning skal bli enklere, og at den blir enklere å modernisere, oppgradere, at den ikke henger så etter teknologisk. Det er vel en av de største gevinstene der i tillegg til at det, som jeg nevnte i sted, å få mer sømløs betjening med litt mer moderne muligheter for å støtte flere typer kommunikasjon og den type ting. |
| 47 | L | Så det blir en liksom markant reduksjon i antall sånn, jeg er ikke så rutta på den terminologien her men, sånn kontrollromsenheter rundt om i landet? |

| | | |
|---|---|---|
| 48 | I | Ja, altså, kontrollrom eller nødsentraler, nødmeldesentraler, blir jo det samme antallet i utgangspunktet. Men servere, hvis du kan kalle det det. Serverinstallasjoner blir jo drastisk mye færre. Men de vil betjenes fra det samme antall steder da. Eller, det går jo sånn sakte nedover, vi sentraliserer jo innimellom. Hvis ikke Senterpartiet får alt for mye makt så sentraliserer vi jo fortsatt disse kontrollrommene, for det er noen av dem som er litt for små. Altså de har liksom, du kan telle på to hender hvor mange samtaler de har i døgnet, sånn at å ha døgnbemannet og all teknologi på et sånt sted er jo kanskje ikke regningssvarende alltid. Så det skjer jo en viss grad av sentralisering på disse kontrollrommene også, men ikke sånn voldsomt. Det er en prosess som går sakte. Så i utgangspunktet legger man opp til det samme antall som i dag. Men som sagt, med mye færre servere da. |
| 49 | E | Det med at serverløsning sentraliseres, er det på en måte i forlengelsen av 5G-konseptet med at man kommer til å ha store datasenter der den virtuelle infrastrukturen til 5G-nettet kjører? |
| 50 | I | Nødnettet er jo også veldig sentralisert. Det er jo noen svære servere. Selve kjernenettet i Nødnett er jo kjempesentralisert. Så det hadde ikke vært noe problem for kontrollrommene i Nødnett å være sentralisert heller. Ønsket om sentralisering nå er vel for å forenkle driften og få ned kostnadene, og også at kontrollrommene skal kunne samarbeide mer. For det er også en viktig bit her. |
| 51 | I | I dagens Nødnett så er på en måte hvert kontrollrom, hver nødsentral, er en liten øy, og de kan jo snakke sammen, de kan være i samme talegruppe, det er ikke noe problem, det er helt sømløst. Men på telefoni for eksempel, så er det ikke helt sømløst. Så det er komplisert hvis ett kontrollrom skal ta over for eller hjelpe et annet kontrollrom å svare på telefonsamtaler. For eksempel hvis det skjer en svær ulykke og det kommer masse - For det er en viktig bit av kontrollromsløsningen, det er jo ikke bare for å styre radionettet det er jo også for å ta imot alle henvendelsene fra publikum, som jo er en like stor og viktig del av det denne kontrollromsløsningen gjør. Og hvis det da kommer veldig mange samtaler inn til en nødsentral, så er det ikke så veldig lett å si det at halvpartene av de nødsamtalene skal rutes til en annen nødmeldesentral som kan hjelpe til. Både sånn teknisk med ruting og sånne ting, men også det operasjonelle med at de kanskje ikke deler, ja, de deler ikke kartsystemer de deler ikke journalsystem, så det blir vanskelig på en måte å jobbe med de samme casene da. Mens med en ny løsning som er mer virtuell, så ser man for seg at disse sentralene kan hjelpe hverandre, at det blir lettere å ta over for hverandre, lettere å hjelpe hverandre med stor belastning. Både fordi at de får en sentralisert håndteringsløsning for tale, men også fordi at de samtidig nå anskaffer nytt det vi kaller hendelseshåndteringssystem, eller oppdragshåndteringssystem, altså der hvor de sitter og legger inn alle data- Og kartsystem, hvor de har flåtestyring av alle ambulansene på kartet. Alle de tre systemene blir jo nå også sentralisert, sånn at også disse nødsentralene, ihvertfall i helse, kan på en måte samarbeide mer om oppdragene på en enkel måte. Det blir også viktig. |
| 52 | E | En ting jeg fokuserer litt på i min oppgave er det at man kommer til å ha et tettere samarbeid med kommersielle mobile nettverksoperatører i neste generasjon av Nødnett, fordi at altså, i forlengelsen av at man ikke skal ha sitt eget radionett så må man uansett samarbeide med de. Og så er liksom spørsmålet, hvor mye skal man eventuelt samarbeide i kjernenettet også. Men vi har snakket litt om at det er mye bruk av kommersielt mobilt bredbånd i dag på grunn av funksjonelle utfordringer med Nødnett. Betyr det at man ikke ser på det å samarbeide med kommersielle operatører som en utfordring i det hele tatt, eller at det ikke liksom - Hvordan er vurderingene der på en måte? |
| 53 | I | Det er helt uproblematisk, hehe, neida. Det er ikke det. Nei, altså, grunnen til at man bruker kommersielt mobilt bredbånd i dag er jo på en måte at det har vært det eneste alternativet, |

| | | |
|---|---|---|
| | | og det har gitt en mye bedre tjeneste enn det data i Nødnett har kunnet gi. Sånn sett så er det jo ikke, til nå har det ikke vært noe sånt stort problem å bruke kommersielle operatører, og det er jo flere aspekter som gjør det. Det ene er jo at man har ansett tale på gruppe som det aller viktigste, og det går jo da ikke via kommersiell leverandør. Det har vært én greie. Men nå blir man jo mer og mer avhengig av data, så de blir veldig hemmet hvis de ikke har datatrafikk med ambulansene, men de greier seg fortsatt. Det tar bare litt lenger tid. Det er litt vanskeligere for han inne å få oversikt over alle ambulansene, hvor der hen, og man må lese opp alt som de ute i ambulansene skal vite om pasienten istedenfor å bare sende det som en datamelding. Så alt blir jo mer komplisert, men du får gjort jobben din så lenge du har talesambandet og kan varsle ambulansene. Det andre aspektet er jo selvfølgelig som vi er litt bekymret over, er jo at i dag har man to helt separate nett. Altså, man har tale og så har man mobilt bredbånd og mobiltelefon. Så hvis dagens Nødnett går ned av en eller annen grunn, så har man fortsatt mobiltelefonen som backup, og man har datakommunikasjonen. Hvis man nå går over til å bruke kommersiell leverandør som er den samme som leverer mobiltelefonsystemet, og det går ned, så har man på en måte ikke noen backup. Det er jo ting vi jobber med selvfølgelig da, for å se på mulige backupløsninger. Men i utgangspunktet så legger man da mer alle eggene i én kurv, og det har da vært kanskje den største skepsisen til å gå over til en kommersiell leverandør. Det har vært at man får færre reservemuligheter da. Men så er jo det en del av avveiningen ikke sant, fordi at Nødnett bruker jo også Telenor sine fastlinjer veldig mange steder for å fremføre Nødnettet, sånn at når det graves over en kabel ut til en eller annen øy, så ryker ofte Nødnettet samtidig med mobilnettet fordi de lå i den samme grøfta eller brukte den samme fiberen. Mens noen ganger leser man at mobilnettet var nede men Nødnettet fungerte, fordi at de kanskje har en annen føringsvei eller har brukt en annen linje eller et eller annet sånt, mens mobilnettet har ikke gjort det. Så noen tenker vel det at man bruker alle pengene sine på mobilnettet da, istedenfor å bygge opp enda et nett, gjør at man kan få det mobilnettet enda sikrere da. At man bruker penger på nødstrømsaggregater, altså flere nødstrømsaggregat, istedenfor at både Telenor og Netcom og Nødnettet må ha hvert sitt nødstrømsaggregat på den samme fjelltoppen ikke sant. Man har jo noe samarbeid der i dag og, men på en måte at mobilnettene sannsynligvis vil bli sikrere og ha mer oppetid enn det et eget Nødnett som staten betaler for vil kunne ha. Fordi at det er så mye mer penger i mobilnettet. Så det er jo et av argumentene som brukes, men det er jo disse avveiningene man sitter med nå i disse dager og teller på. For det er fordeler og ulemper med begge løsninger. Men det er absolutt ankerpunkter for det å basere seg helt på et kommersielt nett, det er det. Det går på det med oppetid og tilgjengelighet, og det med sikkerhet. Ja, faren for - Ja, hybridkrig, ikke sant. Hva vil de først ta ut der? Vil de ta ut de kommersielle mobilnettene, vil et dedikert Nødnett være like utsatt, eller kanskje enda mer utsatt, altså hvem vet. Hva som er beste løsning, det er ikke så lett å vite. |
| 54 | I | Men sikkerhet, altså sånn data, altså avlyttingssikkerhet, det tenker jeg vi - Det vil jo være kryptering her og man vil vel ende med at man har et kanskje slags virtuelt nett innenfor det kommersielle som skal være rimelig sikkert. Så jeg er ikke så redd for den datasikkerheten i det daglige ihvertfall, med at pasientopplysninger skal komme på avveie og sånn. Det tenker jeg i utgangspunktet vil være like sikkert i et kommersielt mobilnett, uten at jeg er noen sikkerhetsekspert. Det jeg er bekymret for er mer den tilgjengelighetsbiten, og sabotasjebiten og det her, og hvem av konseptene som gir best løsning der da, og det er jeg faktisk litt usikker på. |
| 55 | E | Når det kommer til eventuelle ulike alternativer for ansvarsfordeling i kjernenettet, er det også der på en måte - Mitt inntrykk har kanskje vært at den beste løsningen i manges øyne er at staten eier og drifter sitt eget kjernenett, men at det kan bli ressurskrevende. |
| 56 | I | Men tenker du eget kjernenett med en kommersiell basestasjon, eller helt eget nett med |

| | | |
|---|---|---|
| | | statseid basestasjon? |
| 57 | E | Da mente jeg med kommersielle basestasjoner. |
| 58 | I | Ja, jeg husker ikke hva det heter for noe, de har et fint navn på det, det kan jo sikkert du? Eller, nei? |
| 59 | L | Haha. |
| 60 | E | Nei, jeg vet ikke helt hva du sikter til, hehe. |
| 61 | I | De har jo forskjellige grader av - Det bør du kanskje finne ut av. Jeg husker dessverre ikke navnet, men de har jo sånne grader av dette her, ikke sant. Som du sier, man kan jo bare leie seg inn og bruke det kommersielle nettet sånn som det er i dag. Det er det vi gjør med Telenor. Det er jo ett nivå hvor vi bare bruker et helt vanlig mobilt bredbåndsabonnement i Telenor. Noen av sentralene gjør det, og så er det noen av sentralene som har kjøpt seg sånn at man, jeg husker ikke helt, men sånn at man har en egen slags virtuell server hos Telenor. Det har et navn, i 4G i dag, som man gir en viss grad av høyere sikkerhet. At man lager på en måte et virtuelt IP-nett innenfor Telenors mobile bredbåndsnett. |
| 62 | E | En slice? |
| 63 | I | Nja, jeg vet ikke om det er så langt som å kalle det en slice. Det er en sånn mellomting på en måte. Dette er ikke mitt fagområde altså, men i Nødnett i 5G har man jo også det ikke sant, at man bare kan leie seg inn, bruke det helt vanlig, eller at man kan kjøpe seg et virtuelt nett, eller man kan gå enda et hakk og få leverandøren til å sette opp en helt egen slice. Og så kan du jo da, som du sier, på en måte da at man også kjøper fysiske servere og etablerer kjernenettet, og så er det bare basestasjonene og linjene man bruker ut - Dette har man noen sånne navn på - Og det har man vel ikke falt ned på enda, hva man kommer til å velge. Men det er jo noe med at ting er dyrere enn andre ting, og krever selvfølgelig drifting om man skal begynne å kjøpe sitt eget kjernenett. Sånn at det er vel på en måte ikke endelig bestemt tror jeg. |
| 64 | E | Det er jo litt den KVUen som går på det samme som jeg skal innom i min masteroppgave. |
| 65 | I | Ja, ikke sant. Det er jo noe med det. Så der diskuteres det vel fortsatt. Og jeg har ikke noe store meninger der om det, med eget kjernenett kontra å leie seg inn med virtuell slice eller hva det er for noe. Om hvem av de løsningene som er best, det er jeg usikker på. |
| 66 | E | Så lenge funksjonaliteten er ivaretatt på en måte? |
| 67 | I | Ja, så lenge funksjonaliteten er ivaretatt, og datasikkerheten og oppetiden og alt dette her blir ivaretatt. |
| 68 | E | Så er det ikke så nøye hvem som leverer tjenesten? |
| 69 | I | Jo, eller altså, jo det er det vel. Men det er ikke så - Jeg vet ikke hvem av variantene som gir best tjeneste, sånn sett. Jeg har ikke dybdekunnskap nok til å se - Jeg vet ikke fordelen og ulempene med de ulike variantene der godt nok. Så det skal jeg ikke uttale meg så mye om. |
| 70 | E | Sånn i prosessen med å utvikle neste generasjons Nødnett, samarbeider dere noe med andre land? For å lære av hverandres erfaringer og sånt? De har jo gjort det på litt ulike måter rundt omkring. |

| | | |
|---|---|---|
| 71 | L | Som du egentlig tidligere nevnte også. |
| 72 | I | Hm? |
| 73 | L | Det nevnte du vel tidligere også, at du har sett litt på Sverige og sånn. |
| 74 | I | Ja, ja. Det var jo mye med forrige Nødnett og sånt. Nei, altså, vi gjør jo - Vi har jo et visst samarbeid med andre land. Vi har jo hatt mye samarbeid med Sverige og litt med Finland nå med dagens Nødnett, for å få nettene til å snakke sammen. Sverige går vel for en annen løsning for neste generasjon. De har vel tenkt å bygge sitt eget 5G-nett såvidt jeg har skjønt. Så det gjøres jo som du sier litt forskjellig. Og så er man med i en del sånne prosjekter. Det har vært noen litt sånn utredningsprosjekter i EU, Broadway og Bridge heter vel de prosjektene. Og disse som jobber i DSB, det er jo de som er på en måte tettest på dette her, og de er jo aktive internasjonale foraer og den type ting. Vi har også vært det, men nå er det jo litt med Covid og i og for seg også nedskjæringer som har gjort at vi har ikke anledning - Vi får ikke lov til å være med på internasjonale konferanser så mye som vi var - Det er jo gjerne sånn når vi var en del av Nødnett-prosjektet så hadde vi prosjektmidler, så der var det jo anledning til å være med på internasjonale konferanser og utveksle erfaringer og den type ting. Nå er det jo ikke laget noe nytt neste generasjons Nødnett-prosjekt enda, nå er det på en måte bare den KVUen som vi må gjøre parallelt med alle andre arbeidsoppgaver. Og det er ikke finansiert det utredningsarbeidet som har vært frem til nå, sånn at der har ikke vi fra brukersiden hatt anledning til på en måte å ha så fryktelig mye dialog med andre land rundt det. Men jeg regner jo med at DSB for eksempel, Nødnett-organisasjonen i DSB, at de har noe mer dialog også med andre land. Kanskje særlig England som er de som er kommet lengst, såvidt jeg vet, på det med neste generasjon. Men de har jo møtt noen vegger de og. De skulle jo for lengst være gått over fra TETRA til 5G, men har vel måttet spise den kamelen noen ganger tror jeg. Jeg vet faktisk ikke helt hvor langt de er kommet nå. De har vel snakket om at de ihvertfall skal begynne å ta i bruk datadelen av det nye nettet, men holde igjen litt på tale. Men det er absolutt noe samarbeid - DSB har nok en del samarbeid utad. Og vi har jo en viss dialog vi også med andre land, også på brukersiden. Men det er det mye Sverige, på brukersiden der da når det gjelder Nødnett. |
| 75 | L | Ja, det har vel vært relevant nylig det også. |
| 76 | I | Hva da? |
| 77 | L | Samarbeid med Sverige var vel i bruk i Gjerdrum-saken var det ikke? |
| 78 | I | Nja, kanskje litt, men jeg vet ikke om jeg har hørt så veldig mye om det. Det kan jo ha vært en eller annen ressurs som var inne med et helikopter eller noe sånt kanskje, men jeg har ikke hørt noe særlig om det. |
| 79 | L | Det her var veldig opplysende, du! |
| 80 | I | Okay, ja. |
| 81 | E | Veldig interessant. |
| 82 | I | Det er bra. |
| 83 | I | Jeg vet ikke om du fikk alle svarene du trengte om autonome ting og tang, men det er ihvertfall noe som - Altså, som jeg sa, når vi legger alle eggene i én kurv og ikke har |

| | | |
|---|---|---|
| | | mobilnettet som backup, så er jo dette med dekning for eksempel. Frivillig redningstjeneste er veldig opptatt av dette med dekning, blant annet i nasjonalparker og sånt, hvor man frykter at 5G skal gi dårligere dekning enn Nødnett fordi rekkevidden på basestasjonene vil være mindre og hvor naturmyndighetene nekter DSB å sette opp basestasjoner. Og selvfølgelig det når en litt grisgrendt basestasjon detter ut, så har man på en måte da plutselig ikke mobilnettet som fallback, for det er jo den basestasjonen som faller ut. Så både nødetatene og resten av redningstjenesten er jo litt spent på både hvordan dekningen blir i grisgrendte strøk og hvilken fallback man har der. Og da er jo dette med DMO, altså direct mode - Det har jo vært en litt sånn uløst greie, hvor ingen egentlig har kunnet svare på om det kommer eller ikke, og når det kommer. |
| 84 | L | Er det tatt i bruk i Nødnett? |
| 85 | I | Om det er tatt i bruk? Ja, det brukes en del. Det læres ihvertfall opp i det, og det brukes absolutt en del steder. Men det er nok litt avhengig av hvor god man er, og hvor mye opplæring man har. Det ble jo snakket om for eksempel på Gjerdrum, så ble det jo en overbelastning av Nødnettet i startfasen. Der ble det for mye trafikk. Og da var det en del snakk om at man da burde gått over til DMO mellom en del av aktørene, for å avlaste basestasjonen. Men så har man litt vekslende erfaring. Den vanlige ambulansetjenesten har ikke så fryktelig mye erfaring med - Der har nok de frivillige kanskje, de som er vant til å være ute på fjellet uten særlig dekning er nok mer vant til å bruke direct mode enn det en vanlig ambulansesjåfør i byen er. Jeg er litt usikker på om de fikk gått over til å bruke det eller ikke. Og det er også et håp jeg har, det må jeg innrømme, det er håp jeg har i neste generasjon at - For nå må du jo switche radioen over fra å jobbe i nettet til å jobbe direct mode, og jeg har en forventning at disse devicene som kommer, at de kan skjønne det automatisk at "Oi, nå har jeg ikke nettdekning, kan jeg se om det er noen devicer i nærheten som har nettdekning?" Drømmen hadde jo vært mesh-funksjonalitet, hvor disse devicene snakker med hverandre, men jeg har skjønt at det bruker fryktelig mye batteri visstnok. Men at på en måte devicene gjør en del av disse tingene av seg selv da, eller at det blir veldig mye enklere enn i dag. |
| 86 | L | For det er jo masse arbeid i 5G med det her også, som jeg har sett og touchet innpå såvidt. Så det er jo absolutt noe å legge litt mer innsats i, spesielt i casene med den - Det er bra input! |
| 87 | E | Det virker som om sømløshet - |
| 88 | I | Nå faller dere ut. |
| 89 | E | Hører du oss nå? |
| 90 | I | Jada, jeg hører dere såvidt. |
| 91 | E | Jeg sa bare at det virker som om sømløshet er et nøkkelord her. |
| 92 | I | Ja. Det er veldig stor spredning i brukergruppen, med tanke på hvor mye fokus de har på teknikken og funksjonaliteten. Sånn at det er brukervennlig nok for de enkle brukerne samtidig som det er avansert nok for de avanserte brukerne. Det er absolutt et viktigt aspekt. |
| 93 | L | Nettopp, og at det ikke blir partisjonering fordi at folk har forskjellig brukererfaring. |
| 94 | I | Hva sa du nå? Om det blir? |

| | | |
|---|---|---|
| 95 | L | Liksom oppdeling av hvem som faktisk kan snakke med hverandre fordi de har forskjellig innsikt og teknisk kompetanse. |
| 96 | I | Altså, de må jo kunne snakke med hverandre uavhengig av den innsikten da. Så det er jo viktig at alle kan snakke med hverandre. Men kanskje de som har mer teknisk innsikt kan hjelpe de som har mindre teknisk innsikt. Det har vi jo. Sånn som en detalj som i Nødnettet for eksempel, at hvis en lege eller en annen som ikke bruker radioen så mye vet kanskje nesten ikke hvordan man skifter talegruppe da. Hvis dere vet hva en talegruppe er da, det er jo, ja. Der har vi jo lenge ønsket at AMK-nødsentralen på en måte kan flytte radioene - Bare tegne en ring rundt i kartet eller merke alle radioene på skjermen sin, og så bare dra dem over i en ny talegruppe. Sånn at de ute slipper å forholde seg til hvilken talegruppe det er når de har mye annet å gjøre. Men det støtter jo ikke den - Ja, altså, teknologien er jo egentlig der, men den ICCSen, som vi sier, den softwaren vi har på nødsentralene, støtter ikke den funksjonaliteten på en brukervennlig måte. Sånn at den typen ting er ting vi håper skal være mye enklere i neste generasjons Nødnett. At de inne på en måte kan hjelpe de brukerne ute med en del ting, for eksempel å flytte radioen over i en ny talegruppe. Eller gjøre andre ting med radioen. Eller at en operativ uteleder som sitter f.eks i en bil, også kan gjøre noen av disse tingene fra en liten skjerm. Ha mer funksjonalitet for å gjøre den typen ting da. Dytte folk over i de rette talegruppene der de skal være, og fasilitere det samvirket som skal være der ute. |
| 97 | L | Mhm, brukervennlighet. |
| 98 | I | Yes, jeg har et nytt møte om fire minutter. |
| 99 | E | Har du noen spørsmål til oss? |
| 100 | I | Nei, ikke sånn umiddelbart tror jeg. Jeg har jo fått stilt noen spørsmål. Det er jo ihvertfall veldig interessante aspekter dere er inne på i avhandlingen, så jeg tar gjerne en kopi eller noe sånt av det når det kommer. Eventuelt om det er noe foreløpige greier, jeg får jo sikkert en transkriptsgreie ihvertfall. Og er det noe dere lurer på så er det jo bare å spørre, enten å ringe eller sende meg en mail hvis det er noe, noe som var uklart, så er det bare å sende det. |
| 101 | E | Det setter vi pris på. |
| 102 | L | Vi gjør ferdig masterne våre i slutten av juni. Vi kan sende over masteren så fort vi, eller den publiseres jo offentlig så fort vi har fått sensur tror vi. |
| 103 | E | Ja, vi vet ikke helt hvordan det funker. |
| 104 | I | Det hadde vært interessant det altså. |
| 105 | E | Vi får se hvordan det blir. |
| 106 | L | Jeg setter veldig pris på at du tok deg tid til å snakke med oss. |
| 107 | I | Yes, det var hyggelig å prate. Det er jo gøy å prate om noe man brenner for, så det går bra. Fint det, vi snakkes. |
| 108 | E, L | Ha det bra! |

# Appendix C
# Customs Authority

This interview is conducted with a representative of the Norwegian customs authority. It concerns the customs authority's use of the existing Nødnett and touches on, for instance, Nødnett in the context of international collaboration with the customs authorities of neighboring nations, as well as the Norwegian customs authority's expectations and concerns in regard to NGN.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Da har jeg satt på opptaket, og så spør jeg deg om det er greit at vi tar lydopptak. |
| 2 | I | Det er helt greit, bare å kjøre på. |
| 3 | E | Da kan jeg sette i gang med å presentere min masteroppgave. Fokuset mitt er på samarbeid mellom staten og kommersielle aktører i tilbedelsen av neste generasjons Nødnett. Fordi man ikke skal ha sitt eget radionett, blir man avhengig av å samarbeide med de kommersielle mobiloperatørene for å få tilgang til deres radionett. Det er også vurderinger som må gjøres rundt om man skal samarbeide med kommersielle aktører i kjernenettet, og ulike fordeler og ulemper ved det. |
| 4 | L | Min oppgave går litt mer teknisk til verks. Jeg ser også på Nødnett i 5G og hvordan man kan ha en eller flere autonome basestasjoner, og hvordan det kan løses teknisk og operasjonelt. Det er kort oppsummert oss, har du lyst til å presentere deg og hva din rolle er? |
| 5 | I | Ja, det høres spennende ut. |
| 6 | I | Ja. Jeg heter [navn] og har vært ansatt i [organisasjon]. Jeg har jobbet med Nødnett siden [år]. Jeg er nå i [organisasjon]. Nå er Nødnett samlet i grensedivisjonen, som er de som bruker Nødnett mest i Tolletaten. Jeg synes dette er en interessant og veldig ålreit oppgave å jobbe med. Jeg brenner litt for Nødnett, må si det. Ja, det er vel det. |
| 7 | E | Kan du fortelle litt om hvordan man bruker Nødnett i Tolletaten, og hvordan det kanskje er ulikt fra hvordan man bruker Nødnett i andre nødetater? |
| 8 | I | Da vi kom inn i Nødnett-familien i 2014 så var det jo kun to tolldistrikter som det het den gangen, tollregioner, som hadde samband. Det var Oslo og Akershus og så var det Østfold. De andre tollregionene hadde, ja, nesten ingenting. Noen brukte mobiltelefoner, andre brukte radioer, og noen vanlige gammeldagse walkie-talkier. |
| 9 | I | Når vi da fikk Nødnett som et prøveprosjekt, vi fikk lånt noen terminaler fra politiets IKT-tjeneste på Jaren, og prøvde det ut i Oslo og Østfold, 7 terminaler i hver region. Vi fikk nesten ikke terminalene inn igjen. Det var så mye klarere lyd, og vi hadde dekning der vi overhodet ikke hadde hatt dekning før. Og det er jo noe av cluet med Nødnett, at vi har dekning over hele fjøla langs svenskegrensa og opp til Finland. |
| 10 | I | Når vi da kom inn i samarbeidet med Sverige, da med NoSe og med FiNo med Finland, så fikk vi også tilgang til basestasjoner både i Norge og Finland. |
| 11 | L | Okei! Hva kalte du det, NoSe? |
| 12 | I | NoSe, ja, Norge-Sverige. Det er et finsk-norsk, svensk-finsk talegrupper som vi har felles med svensk toll og svensk politi, og samme med norsk toll og norsk politi. Vi har egne talegrupper som vi kan bruke over grensa når vi jobber sammen. Vi har tilsvarende med Finland. Og så finnes det et norsk-svensk-finsk talegruppesamband, det har vel kommet til drift nå for ikke så veldig lenge siden. Der kan alle de tre landene snakke sammen i felles talegrupper. Spesielt er jo det viktig oppe i nord hvor du har tre grenser som møter hverandre. |
| 13 | L | Ja. |
| 14 | I | Det svenske nettet har vi visst stor hjelp av langsmed svenskegrensa, fordi der Nødnett ikke |

| | | |
|---|---|---|
| | | har dekning, der er det stort sett dekning fra Sverige. De kjører med litt hardere styrke enn hva Norge gjør. Norske og svenske tollere kan jobbe inntil 15km inn i hverandres land uten å søke om tillatelse til det. Det har vi i en grensetollsamarbeidsavtale med Sverige, og det har vi hatt siden 1958. Vi har vært tidlig ute når det kommer til samarbeid. |
| 15 | L | Hva slags tjenester er det som brukes mest? Er det gruppesamtaler? |
| 16 | I | Det er gruppesamtaler og tale 1-1. Men stort sett er det bare gruppesamtaler. |
| 17 | L | Har du noen formening om de synes 1-1-samtalene fungerer greit, brukerne? |
| 18 | I | Ja, de synes forsåvidt det, der du trenger å prate 1-1. For eksempel i et spesielt oppdrag kan du kalle opp den andre hvis du da vet ISSI-nummeret på den du skal snakke med. Ikke så veldig mye brukt, men av og til blir det brukt. Stort sett er det gruppesamtaler, så du kjører alt sammen via operasjonssentralen som vi har. Per i dag har vi en operasjonssentral og den ligger på Helsfyr i Oslo. |
| 19 | L | Okei! |
| 20 | I | Vi flytter den til Moss nå i løpet av våren, sånn at det blir operasjonssentral i Moss. Vi har en nesten-operasjonssentral, nesten ICCS, på Svinesund. De to blir slått sammen, sånn at de samarbeider. |
| 21 | L | Blir det da en felles operasjonssentral for hele landet? |
| 22 | I | Ja, det gjør det. Og det er en stor forskjell, sånn at vi kan utnytte ressursene best mulig. Og sånn som det har vært med den operasjonssentralen vi har nå, har den stort sett betjent sentrale østlandsområdet. Nå blir det jo mye bedre for de i Vest-, Midt- og Nord-Norge. Nå får de én operasjonssentral som de kan forholde seg til og få hjelp av når det gjelder oppsjekk av f.eks. bilnummer, personer, og ting som vi har i våre systemer. |
| 23 | L | Mhm. I min oppgave ser jeg på autonomi, og caset der en eller flere basestasjoner har mistet tilkoblinga til kjernenettet og fungerer som et lite lokalt nettverk. Har du en formening om hvordan det ville fungert dersom en del av landet mista tilkoblinga til denne sentralen? |
| 24 | I | Vi har faktisk vært litt på når det gjelder det å skape dekning selv. |
| 25 | L | Å? |
| 26 | I | Hvis en basestasjon faller ut, har vi gateway/repeater i alle bilene våre. |
| 27 | L | Dere har det, ja? |
| 28 | I | Slik at vi kan gå over i DMO og skape dekning der hvor vi er, altså rundt 5-6km hvis det er flatt. |
| 29 | L | Lokalt mellom dere, eller skaper dere da – |
| 30 | I | Nei, det blir lokalt mellom de som er i det området. |
| 31 | L | Ja, og det brukes faktisk, altså. |

| | | |
|---|---|---|
| 32 | I | Ja. Og vi har jo faktisk i skip, i cruiseskip og store båter, så har vi sånne gateway/repeater-kofferter hvor vi skaper innendørsdekning. |
| 33 | L | Jøss. |
| 34 | I | Hvor vi da setter opp den kofferten stort sett midtskips, og så setter vi opp antenna horisontalt sånn at den kaster strålene inn, rundt båten i stedet for gjennom og vertikalt, men horisontalt. Da har vi hatt dekning helt ned i motorrom, helt bak til propellaksler og helt foran i baugen. Vi kan skape dekning der vi er. |
| 35 | L | I DMO, er det kun talegrupper det går i? |
| 36 | I | Da er det DMO-talegrupper, ja. Når du bruker repeater og bruker gateway-funksjonen, kan tjenestemann som er inne i båten gå i DMO. Signalene går ut via kofferten eller bilradioen og ut i det vanlige Nødnettet. |
| 37 | L | Ja, ikke sant. Brukes noen datatjenester av Tolletaten? |
| 38 | I | Ikke i Nødnett. Det er for dårlig kapasitet til det. Nødnettet er et rent talesamband, og det er det det ble bygget som. Du kan sende SMS med opptil 128 tegn, og det er ikke noe særlig. |
| 39 | L | Tror du, gitt muligheten, at datatjenester hadde vært en kritisk funksjonalitet for dere? |
| 40 | I | Ja, hvis det hadde vært tilgjengelig tror jeg vi hadde brukt det i stor grad. Nå har vi jo utviklet, samme som politiet har, gateway/repeater i bil. Du kan logge på med laptopen din hvor som helst omtrent, og komme deg på nettsider og det du vil i forbindelse med repeater i bil. Og da er jo ikke Nødnett så veldig aktuelt egentlig. |
| 41 | L | For da brukes kommersielle nett? |
| 42 | I | Ja, det gjør det. Vi har to SIM-kort i de repeaterene som står i bilen, og de kan kobles opp mot [operatør] hvis det er behov for det. |
| 43 | L | Åja, så du har tilkobling kommersielt og så ut til DMO? |
| 44 | I | Nei, det er ikke koblet opp imot Nødnett. Det er kun databærere. Du kan bruke vanlig jobb-pc i bilen, men det går ikke i vanlig Nødnett nå. Det er det ikke kapasitet til i det hele tatt, og det er ikke utviklet sånn heller. |
| 45 | L | Vi ser på muligheter for det i 5G. |
| 46 | I | Det blir nok et av punktene som blir med videre, tror jeg, men så spørs det hvor aktuelt det er når alle etater har sine egne, kall det mobilnett, i bilene. |
| 47 | L | Mhm. At det kanskje blir en unødvendig kostnad, liksom? |
| 48 | I | Det kan godt tenkes, det. I og med at både Toll og f.eks. Politi har disse ruter i bil, som dem kaller det, hvor de kan koble opp PCene sine. Hvis de da har et SIM-kort som kan bruke f.eks. begge eller alle mobiltilbyderene i et område så er det ikke sikkert det er behov for det i et nytt Nødnett. |
| 49 | E | Så man tenker på en måte at behovet allerede er møtt, iallfall for Tolletaten, med den løsningen man har? |

| | | |
|---|---|---|
| 50 | I | Ja, vi ser ikke noe behov sånn som vi har det i dag. Jeg kan ta med meg PCen min, jeg, og koble meg opp via telefonen min. Såfremt jeg har dekning på telefonen kan jeg koble meg opp på Tollvesenet sitt nett uansett hvor jeg er hen. Om jeg er hjemme, eller på hytta, eller hvor som helst. Så lenge jeg har mobildekning kan jeg komme meg inn og jobbe på Tollvesenet sine systemer. |
| 51 | L | Så opplever du at dere ikke har veldig mange umøtte behov nå inn i neste generasjons Nødnett? |
| 52 | I | Jeg skal ikke si at vi ikke har noen behov, for det spørs jo liksom. Det som er litt spennende er jo om det nye 5G-nettet kommer til å få like god dekning som vi har med dagens Nødnett. Det har vi spilt inn hele veien sammen med alle de andre brukerne at vi må ha like god eller bedre dekning enn vi har i dag. Og det skal godt gjøres i et kommersielt nett. Når vi ser at de som da har vanlig 4G sliter i enkelte områder, og så skal en da klare å jobbe og bygge ut 5G-nettet like fort og like godt. Det kan bli spennende å se. |
| 53 | L | Hm. |
| 54 | I | Dekning er iallfall et av hovedpunktene i det nye Nødnettet som Tollvesenet har spilt inn. Vi må ha like god dekning langs svenskegrensa og finskegrensa som vi har i dag og ha samarbeid med svenske og finske tollere og politimyndigheter. |
| 55 | E | Det var det jeg skulle spørre om. Er det noen vurderinger om hvordan det kan bli i 5G med de internasjonale samarbeidet med svenske og finske tollmyndigheter når man går over til et kommersielt radionett? |
| 56 | I | Vi har spilt inn det som et må-punkt. Det samme har politiet, og brannvesenet har også gjort det i forhold til dekning ifm. skogbranner langs grensa og søk og redning. Så vi er ikke alene om å liksom ha spilt inn det punktet i det nye Nødnettet. Det blir jo spennende. |
| 57 | L | Ja, det blir veldig spennende. |
| 58 | E | Er det Tolletaten selv som kjøper inn Nødnett-tjenester, eller får man det som pakkeløsning fra DSB? |
| 59 | I | Vi abonnerer på brukergrupper, ut ifra hvor mye du bruker. Har vi en terminal som er lite bruk står den i beredskap, har vi en som er litt mer bruk så har vi meget lav, lav, middels og meget høy. |
| 60 | L | Ja stemmer, det har vi sett på nettsiden. |
| 61 | I | Mhm. Ja, det ligger på abonnementssidene til DSB. |
| 62 | E | Hva med teknologi i kontrollrom, f.eks.? |
| 63 | I | Der har vi såkalt ICCS, altså, samme operasjonssentralsystemer som politiet har. Vi arva en slik operasjonssentral, ICCS, fra politiet når de begynte å omorganisere og legge ned politidistrikter og slå sammen de. Da arva vi en slik sentral fra politiet. Så det er den vi har satt opp på [sted]. |
| 64 | L | Bare for å dobbeltsjekke, du kaller det ICCS? |
| 65 | I | ICCS, ja. |

| | | |
|---|---|---|
| 66 | L | Informasjons- og kontrollsystem? Eller hva – |
| 67 | I | Nå husker jeg ikke helt hva ICCS står for, men det er det nettet eller de datamaskinene som ligger i bakkant av en operasjonssentral. Det du liksom får opp på skjermen din. Da har du Nødnett på den ene siden og telefoni på den andre siden, og det styres av en ICCS som ligger i bakkant. Det er en tre-fire datamaskiner, store datamaskiner som ligger i bakkant. |
| 68 | L | Ja, som for dere da ligger på det ene sentraliserte stedet? |
| 69 | I | ICCS-en står i datasenteret til Tollvesenet. Vi har splittet den i to, så hvis den ene detter ned, tar den andre over. |
| 70 | L | Fornuftig. |
| 71 | I | Så vi har helt likt oppsett som politiet har, bare at skjermbildet er litt tilpasset Tollvesenet. All teknologien som ligger i bakkant er helt likt, og det er likt for alle. Det er DSB som eier Nødnett og det er jo Motorola som drifter det for DSB. Og så er det jo Frequentis som da har laget det du ser på skjermen og oppsettet for det. Firma som heter Frequentis og holder til i Østerrike. |
| 72 | E | Såvidt jeg har skjønt er det sånn at når man skal gå over til neste generasjons Nødnett er etatene selv ansvarlige for å skaffe kontrollromsteknologi. Er det noe man har tenkt på i Tollvesenet enda? |
| 73 | I | Nå er ikke den teknologien ferdig utviklet enda. Det går en diskusjon på om det skal kjøpes sentralt, eller om vi skal kjøpe det hver for oss. Diskusjonen går på om vi kjøper det sammen som en stor gruppe og så er det brann, politi, helse og andre som har bruk for det som går ut i et felles innkjøpsforum, antakeligvis. Uten at det er noe bestemt. Nå ble jo denne KVU-rapporten levert til justisdepartementet i fjor sommer, og den ble fort stempla unntatt offentlighet. Jeg får jo ikke referert noe til den. |
| 74 | L | Vi hadde jo håpet at den skulle bli publisert nå på nyåret, men den gang ei. |
| 75 | I | Jeg tror dem ligger litt i etterkant, fordi det ble nedsatt et utvalg, eller det ble kjøpt en tjeneste som ble utvalgt for å gå gjennom og kvalitetssikre hele den KVUen. For å si det sånn, jeg har ikke hørt noen ting siden juni i fjor. |
| 76 | L | Jaja. Vi håper jo at den ikke kommer og gjør masterne våre overflødig. |
| 77 | I | Vi venter jo på å få den frigjort så vi kan begynne å jobbe med det. Men, nei, justisdepartementet har vel kanskje hatt litt annet å stri med akkurat nå. Jeg har ikke hørt noen ting. Da jeg snakket med DSB nå før jul, så lå de etter skjema. Det er vel det jeg vet om den biten der. |
| 78 | L | Og årene går fort frem til den Motorola-avtalen går ut. |
| 79 | I | Ja, 31/12/2026. Men hvis du ser til England har de holdt på i mange år for å få dette til og brukt mange milliarder kroner. |
| 80 | L | Hehe, ja, får prøve å ikke følge det eksempelet kanskje. |
| 81 | I | Nei, det er et skrekkeksempel. Det var Motorola som eide nettet der, og så kjøpte de opp |

| | | |
|---|---|---|
| | | over det firmaet som engelskmennene skulle gå over til. Nå sitter de med bukta i begge hender og tjener store penger på det gamle nettet og det nye nettet. Vi har det som et skrekkeksempel, og regner med at vi ikke går i den fella. Men det kan se litt dårlig ut. Nå tror jeg ikke Motorola kommer til å kjøpe opp Telenor og Telia og Ice og den biten, men jeg vet ikke. Det blir spennende. |
| 82 | L | Det gjør det. |
| 83 | E | Med tanke på det forholdet dere i Tolletaten har til kommersielle aktører i dag, at dere bruker de kommersielle aktørene til de databehovene dere har. Hvordan tenker dere det kommer til å bli i NGN, når kommersielle aktører er enda mer involvert og kanskje får ansvar for talegrupper? |
| 84 | I | Nei, det.. Om de får ansvar for talegrupper, det tviler jeg på, for de tar vi hånd om selv. Vi styrer oppbygninga og hvor mange talegrupper og den biten der sånn. Men det skal jo driftes da, av noe i bakkant, og vi må stole på at det er like mye oppe som det Nødnettet er i dag. Det er jo veldig lite nedetid i dagens Nødnett. Det er jo kun hvis det blåser eller brenner opp eller på annen måte blir satt ut av spill at det ikke er dekning i det normale Nødnettet. Da får vi brukt gateway/repeater-løsninga. Vi kan i alle fall skape dekning der vi jobber. Selv om vi ikke har kontakt inn, har vi kontakt med hverandre når vi er ute. Og det må jo komme en tilsvarende løsning på NGN og, at det blir utvikla gateway/repeater-kofferter og -radioer vi kan ha i biler. Det er jo en ekstra trygghet for de tjenestemennene som er ute. |
| 85 | L | Det finnes jo en del fremgangsmåter til det i 5G. Det blir spennende å se hva som blir egnet. |
| 86 | L | Har du vært borti bruk av LST, local site trunking-modus? |
| 87 | I | Hmm, nei. |
| 88 | L | Nei. Det er løsningen for autonomi i Nødnett i dag, der en basestasjon kan fungere autonomt. Men jeg har forstått at det fungerer litt dårlig, for da mister du tilkobling til alt annet. |
| 89 | I | Nødnett er jo bygget opp i sirkler med to veier inn. Hvis begge veiene blir kuttet, fungerer jo den masta eller basestasjonen i det området den står, med de Nødnett-terminalene som er i nærheten. Den fungerer jo som en, sånn liten bærer. Men du har ingen dekning inn til en operasjonssentral. |
| 90 | L | Nettopp, det er akkurat det caset jeg ser på. |
| 91 | I | Tolletaten kjører jo det samme opplegget som politiet har med ende-til-ende-kryptering på sine radioer. |
| 92 | L | Mhm. Er dere operative selv om dere ikke har kontakt inn til operasjonssentralen? |
| 93 | I | Ja, det er vi. Nesten samtlige tolltjenestemenn er ute i felt av de som er i grensedivisjonen og de som er grenselangs. Jeg er jo ikke ute sånn operativt, jeg sitter stort sett bare inne og koser meg med kaffe og Nødnett-terminalene og oppgavene. Men vi pleier å være litt ute for å prate med de som er ute og for å finne ut av om det fungerer optimalt. |
| 94 | L | Mhm, jeg mener, de som bruker terminalene, endebrukerne av Nødnett. Hvis de mister sin tilkobling til kontrollrommet og kun kan snakke med hverandre. Kan de virke da? |

| | | |
|---|---|---|
| 95 | I | Ja, det gjør de. Selv om en patrulje eller to er ute langsmed grensa og mister kontakten med det normale nødnettet, har de kontakt seg imellom. Da går de over i DMO eller bruker gateway/repeater-funksjon på bilen. Det blir en forsterker. |
| 96 | L | Hm, det her var interessant. At det er den foretrukne formen for autonomi, virker det som. |
| 97 | E | En ting. I sånne tilfeller hvor du har dårlig dekning. Hadde det vært fordelaktig å også kunne ha dataoverføringskapasiteter, som f.eks. video, eller er det noe man ikke har så vondt for å ofre? |
| 98 | I | Hvis Nødnett detter ut er det dårlig dekning for resten og, og hvert fall mobiltelefoni. Hvis du ikke har noe bærer, f.eks. en mobiltelefon som bærer, og Nødnett detter ut, detter i hvert fall vanlig mobiltelefoni ut. Da har du ikke noe datakapasitet i det hele tatt. |
| 99 | E | Jeg tenker på i NGN der du kanskje kan ha datakapasitet i nødnettet. Da kan vi se på use caset der du kan ha dataoverføring lokalt, for eksempel. |
| 100 | I | Hvis du skal koble opp en datamaskin til NGN, så må du ha dekning og kapasitet til å hente ned de systemene som Tolletaten bruker. |
| 101 | E | Så dere bruker ikke videooverføring og sånt? |
| 102 | I | Vi har noe som heter ANPR som tar bilde av bilskilt som passerer inn over grensa, men det er jo vanlige stillbilder som blir sendt. Der bruker vi vanlige SIM-kort, mobilkort, som blir sendt inn til en sentral og så blir bilnumrene sjekket for om det er noe på dem fra før. Om vi har snakket med eieren av bilen. Det er det samme som Statens Vegvesen bruker ifm. årsavgift. Vi bruker det i forbindelse med grensepassering: Hvis en bil har vært ofte ute, kjører ut et sted og kommer inn et annet sted og varierer på det, kan vi bruke de kameraene til å sjekke om dette er en gjenganger og hvor ofte han har vært inn og ut over grensa. |
| 103 | L | Så i deres bruk av digitale kommunikasjonsløsninger generelt, hvis vi ikke bare ser på Nødnett, så har dere egentlig behov for både de klassiske Nødnett-tjenestene som gruppesamtaler og 1-1, men dere bruker også dataløsninger en del, ved bruk av kommersielle nett? |
| 104 | I | Ja, det gjør vi. |
| 105 | E | En ting vi har hørt litt om, er at mange er litt skeptisk til at i neste generasjon skal det kommersielle og Nødnettet på en måte være ett og det samme: at de skal bruke de samme basestasjonene og sånt. Da får man ikke den redundansen, som i eksempelet der vanlig Nødnett faller ut kan man bruke den vanlige telefonen sin til å kommunisere. Er det noe man tenker på i Tolletaten, eller er dekningen i det kommersielle mobilnettet generelt så dårlig at hvis Nødnett faller ut så har man ingenting allikevel? |
| 106 | I | Ja, hvis man er langt ute ved svenskegrensa og langt ute i skogen.. Vi er jo der folk ikke skal være, for å si det sånn. Vi er jo ikke der folk bor når vi er langs grensa. Og det er langt til neste bosted. Og hvis Nødnett faller ut så har du ingenting. Da må du bare kjøre til du finner dekning, eller om du får dekning via en mobiltelefon fra Sverige. Vi har sett det at når du kjører langsmed svenskegrensa og kobler opp i disse NoSe-gruppene, Sverige-Norge-talegruppene, og vi da setter Nødnett-terminalen på automatisk og kjører ut og inn over grensene flere ganger, så hekter den seg opp imot f.eks. en svensk BS hvis den er sterkere enn det norske nødnettet og motsatt. Sånn sett har vi i norsk tollvesen og svensk tollvesen god hjelp av hverandres nett. |

| | | |
|---|---|---|
| 107 | L | Dette samarbeidet mellom Norge, Sverige, Finland, gjelder det både brann og politi og toll? |
| 108 | I | Ja, det finnes avtaler innafor hver etat, men Tolletaten har sin egen avtale. Det har vi hatt, ja, siden 1958. Vi har samarbeidet i mange år, og når de koblet sammen det norske og svenske nødnettet så hadde vi avtaler som lå så langt tilbake i tid på samarbeid, så dette kom som en sånn liten pluss i tillegg på samarbeidsavtalen. |
| 109 | E | Hvordan blir det samarbeidet nå? Både Sverige og Finland går jo også nå over til nye nødnett eller har planer om det. Forventer man at samarbeidet blir det samme? |
| 110 | I | Ja, vi håper det. Vi ser ingen grunn til at det ikke skal bli det. Norske og svenske tollere, vi jobber såpass tett med hverandre. På enkelte tollstasjoner utfører vi jo enkelte oppgaver for det andre landet. Svenske tollere gjør norske oppgaver og norske tollere gjør svenske oppgaver på enkelte grensepasseringssteder. Det er ikke norske og svenske tollstasjoner på alle grensepasseringssteder. |
| 111 | E | Blir det litt sånn da at de vurderingene man gjør rundt hvordan man skal utføre det nye nødnettet i Norge, at man gjerne vil at det skal være sammenlignbart med sånn man gjør det i Sverige og Finland for å forsikre seg om at samarbeidet blir opprettholdt på en god måte? |
| 112 | I | Jeg tror nok det. For vi har jo i den prosessen som gikk mellom Norge og Sverige når vi starta å lage disse NoSe-talegruppene, så er det bygget opp på samme måten. |
| 113 | E | Mhm. |
| 114 | I | De NoSe-gruppene, de er jo landsdekkende sånn at vi kan koble opp en svensk talegruppe, norsk-svensk talegruppe på Svinesund og kjøre opp langs hele grensa og ha dekning i den ene talegruppa. Vi slipper å bytte. |
| 115 | I | Svenskene kjører mer landsdekkende talegrupper. Vi i Norge kommer nok etter, vi og, men vi har vært litt sånn at hver region har sine talegrupper. Vi har hatt en skikkelig oppvask nå da vi ble omorganisert i fjor. Vi har kuttet ganske mange talegrupper. |
| 116 | E | Fordi man hadde mange talegrupper som bare var til overs, på en måte? |
| 117 | I | Ja, vi hadde en 500-600, vel, på 900 mann. |
| 118 | E | Veldig fragmentert. |
| 119 | I | Vi har voldsomt med talegrupper. Og vi har talegrupper sammen med Forsvaret, med kystvakta, med fylkesmannen, med hovedredningssentralen. Så vi snakker med alle. |
| 120 | E | Er det noen kontrollromsfunksjonalitet man kunne tenke seg for bedre å kunne koordinere disse talegruppene, som man kanskje kan ønske seg i det nye nødnettet? |
| 121 | I | Nei, altså, vi har jo kontrollen på alle de talegruppene med det kontrollrommet vi har i dag. Det fungerer veldig bra. Og vi kan jo ikke få noe dårligere kontrollrom i det nye nødnettet enn det vi har i dag. Og vi kan ikke ha noe dårligere funksjonalitet på et kontrollrom enn det vi har i dag. I dag fungerer det helt utmerket. Vi er veldig fornøyde med det vi har i dag. |
| 122 | E | Det er jo veldig bra å høre. |

| | | |
|---|---|---|
| 123 | I | Nei, det er en liten jobb å gjøre i forbindelse med det nye nødnettet, altså, for å opprettholde den kvaliteten som vi har i dag over i et nytt et. Selv om det er private som skal drifte kjernenettet og den biten må det være like bra. Vi kan ikke ha noe som er dårligere. |
| 124 | E | Har dere tenkt på noe som å forlenge den kontrakten med Motorola for å fortsette driften i det gamle nødnettet hvis den nye løsningen virker tilfredsstillende? |
| 125 | I | Det er det DSB som bestemmer. Det er de som kjører avtalen med Motorola og det er de som eier kjernenettet. Det er det DSB eller Justisdepartementet som må ta en avgjørelse på. Jeg regner vel med at skal vi fortsette å kjøre i nåværende Nødnett blir det antakeligvis ikke gratis. Det er en utfordring der sånn, altså, for å få det her til å fungere. |
| 126 | I | Det er jo snakk om en prøveperiode mellom gammelt og nytt nett når den tida kommer. For å se om det nye fungerer like godt som det gamle, og kanskje ikke kutte det gamle før du er sikker på at det nye fungerer optimalt. Antakeligvis blir det nok et år eller to med felles drift på gammelt og nytt nett for å sjekke ut kvaliteten på det, men om vi rekker det da før 31/12/2026, det gjenstår å se. Tiden går fort. |
| 127 | L | Da må de få ut den KVUen snart! Nei, det er spennende. Vi rekker såvidt å skrive master før det er for seint! |
| 128 | I | Jeg regner med at dere blir ferdige med masterene deres lenge før Nødnett blir faset ut, hehe. |
| 129 | E | Får håpe det! Vi kan sikkert ta en doktorgrad innen den tid. |
| 130 | I | Ja ja. Bare å stå på! |
| 131 | L | Har du noe mer på lista di? |
| 132 | E | Eh, nei, det blir litt sånn... Hvis man tenker at man er veldig happy med den løsninga man har i dag, og ens største ønske er at den nye løsningen skal bli like bra, og da er man happy på en måte. Da blir det litt at, sånn... Jeg vet ikke helt hva jeg skal spørre om, når det ikke er slik at det er noe nytt en ønsker seg at den nye generasjonen. |
| 133 | I | Det kan jo godt tenkes at vi kan få ting som vi ikke visste at vi trengte, for å si det sånn. For eksempel å styre det nye nødnettet med droner eller den typen ting. Brann og politi bruker jo droner nå i søk og redning. Om det kan kunne brukes og styres via NGN, ja hvem vet, det kan godt tenkes, det. Jeg vet jo det at brannvesenet oppe i nord har en samarbeidsavtale med et firma hvor de kan kjøre opp store droner og skape dekning i fjellområder hvis det er søk eller hvis det er skogbranner. |
| 134 | L | Jøss. |
| 135 | I | Det er jo muligheter. Da er det jo bare å få med seg en repeater opp i en drone, og så vipps så har du jo dekning. |
| 136 | L | Jeg synes det her er litt interessant. Jeg har jo sett på Nødnett teoretisk ganske lenge nå, og jeg har ikke forstått før nå at repeateren er en mye mer anvendelig funksjonalitet enn den funksjonen som ligger innenfor autonomi i en enkelt basestasjon. Det var interessant å få innsikt i! |
| 137 | I | Hehe, ja, basestasjonen står jo der den står. Og med gateway/repeater så er det bare snakk |

| | | |
|---|---|---|
| | | om to knapper på en vanlig bilradio. Trykker du på den andre knappen har du en repeater som skaper dekning akkurat rundt der du er og trykker du på den andre knappen så har du en gateway hvor du da kobler opp DMO-gruppa i det vanlige nødnettet. |
| 138 | L | Jeg har sett litt på brukerevaluering av Nødnett, og det er veldig forskjellig mellom brukergrupper hvem som er brukere av DMO og gateway/repeater fordi det ikke er alle som synes det er så brukervennlig. Men det opplever ikke du? |
| 139 | I | Nei, vi satte fokus med en gang at på at dette skal vi lære oss. Fordi vi trengte dekning f.eks. inne i fjellhaller. Hvis du setter en bil, trykker den over i gateway og rygger den 10-15 meter fra åpningen på en fjellhall, så kaster den inn i tunnelåpningen og du får dekning langt innover. Og kraftverket bruker jo Nødnett 60m under bakken, inn i fjellet. Bare for å skape dekning nedover og innover. |
| 140 | L | Mhm. Veldig moro å høre at det fungerer i praksis. |
| 141 | I | Tollvesenet var jo tidlig ute med å kjøpe sånne kofferter for å ha med seg inn i båter og vi var en av de første som klarte å skape dekning i et helt cruiseskip. |
| 142 | E | Ved å plassere flere kofferter rundt omkring? |
| 143 | I | Nei, det holder med en. Kjører du flere kofferter, begynner de å sloss med hverandre. |
| 144 | L | Jeg beklager at jeg må ha det her inn med teskje, men jeg sliter med å forstå denne kofferten. Snakker den med Nødnett, eller- |
| 145 | I | Det er en bilradio som er montert i en koffert. |
| 146 | L | Ja, ok, så den snakker med Nødnett også. |
| 147 | I | Jaja. Den har kontakt med Nødnett. Helt klart. Den kan snakke med Nødnett og uten Nødnett. Er det uten Nødnett er du i DMO. Og da er du bare der. |
| 148 | L | Mhm. En liten, autonom basestasjon. |
| 149 | I | Ja, nemlig. |
| 150 | E | Mhm. Veldig flyttbar. |
| 151 | I | Ja veldig flyttbar. Jaja, altså den veier ikke mye. Omtrent som en litt stor weekendkoffert. Ikke større enn det. |
| 152 | L | Jøss. |
| 153 | I | Også er det en batteripakke i den, så hvis du ikke har strøm kan du bruke den batteripakka. Den varer vel en 5-6 timer. Og hvis ikke kan du bare koble den opp i vanlig strøm så den bare står og sender hele tiden. |
| 154 | L | Hm. Nå har jeg noe å lese på! |
| 155 | I | Ja, har du noen spørsmål til oss? Noe som – |
| 156 | I | Nei, jeg synes det var litt morsomt at dere fant fram til meg. Jeg så det var en veileder som |

| | | |
|---|---|---|
| | | jobber i DSB. |
| 157 | E | Ja, stemmer det. |
| 158 | I | Så jeg tenker at da har han nok fanga opp navnet mitt der. |
| 159 | E | Ja han har oversikt, han. |
| 160 | I | Det hadde vært artig å fått lest oppgavene deres, da, når dere er ferdige. |
| 161 | E | Ja, dette må vi finne ut av. Vi er litt usikre på når vi har lov til å sende det av gårde og når det er publisert, om det er etter sensuren har kommet eller.. |
| 162 | L | For vi leverer oppgavene våre i slutten av juni, og så vet vi ikke da når de er offentlige. |
| 163 | E | Det kan vi finne ut av. |
| 164 | I | Jeg tar gjerne imot og leser oppgavene deres, jeg, når de er offentlige. |
| 165 | L | Det er det veldig hyggelig at du sier! |
| 166 | I | Litt spennende å følge med på hva som skjer, og at dere skriver om Nødnett synes jeg er artig. |
| 167 | L | Hadde det vært aktuelt for deg å svare på eventuelle oppfølgingsspørsmål i ettertid? På telefon for eksempel? |
| 168 | I | Jaja, bare ta kontakt. Ikke noe problem. |
| 169 | E | Så hyggelig. |
| 170 | L | Det kan det hende vi tar deg opp på. |
| 171 | E | Så det som skjer nå er at vi tar det lydopptaket her og transkriberer det og så anonymiserer det og litt sånn. Og så får du se på det og så kan du komme med innspill til det. |
| 172 | I | Jaja. Ikke noe problem. Jeg synes dette er artig! |
| 173 | L | Så bra, det synes vi og. Det var veldig hyggelig å prate med deg! |
| 174 | I | Jo, i like måte! |
| 175 | E | Jeg må si, mange av de vi snakker om Nødnett med, de brenner veldig for det, og det er artig. |
| 176 | I | Ja, jeg fikk jo denne slengt i fanget i [år]. Og da var beskjeden å melde deg på i de foraene som du finner noe om Nødnett, møt på de møtene og lær deg de tinga du må lære deg. Jeg hadde da et innlegg i noe som het [konferanse] i sin tid, det er jo lagt ned nå. De hadde et møte i [sted] hvor jeg da skulle fortelle om Tollvesenet og hvilke ønsker vi hadde. Det vi ønsket var å få talegrupper og samband så vi skulle kunne snakke med tollere i hele Norge, og at vi kunne snakke med våre samarbeidspartnere. Vi hadde også et annet ønske, og det var at vi kunne snakke med kollegaer på andre siden av svenskegrensa. Da sa [navn] at det var et heftig ønske, men de skulle jo se på det. Og ja, jeg fikk oppfylt det! Vi har svenske og |

| | | |
|---|---|---|
| | | norske talegrupper nå. Veldig fornøyd med det. |
| 177 | L | Det får'n si! |
| 178 | E | Så bra. |
| 179 | E | Det hadde vært litt kjedelig hvis man fikk nytt Nødnett og så var det bare mye dårligere! |
| 180 | I | Hehehe ja, det kan du si! |
| 181 | I | Nei så hvis dere har noe mer å spørre om senere så er det bare å slå på tråden. Vi kan ta en videokonferanse senere. Får bare håpe jeg har et kamera som virker! |
| 182 | E | Men supert, takk skal du ha. |
| 183 | L | Tusen hjertelig! |
| 184 | I | Jo bare hyggelig. Ha det bra. Og lykke til! |
| 185 | E | Takk! |

# Appendix D
# Health Services B

This interview is conducted with two representatives of the Norwegian emergency health services. The topics of conversation range from the way in which the existing Nødnett is currently being employed by ambulance workers and the likes in Norway to what the limitations of the current Nødnett are, and how those limitation might be addressed by NGN.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | ... Lydopptaket, og så spør jeg om det er greit at vi gjør lydopptak. |
| 2 | I1 | Det er det for [navn]. |
| 3 | I2 | Og det går helt fint for [navn]. |
| 4 | E | Supert. |
| 5 | L | Flott. |
| 6 | E | Jeg vet ikke om du [navn] har fått sett det informasjonsskrivet, men vi kan jo presentere våre egne oppgaver litt først. Min oppgave handler om å kartlegge litt utfordringer knyttet til at man skal samarbeide med kommersielle mobiloperatører i gjennomføringen av neste generasjons Nødnett, og jeg ser på litt ulike alternativer for hvordan det kan gjennomføres på en ryddig måte. |
| 7 | L | Jeg ser på at én eller flere basestasjoner i Nødnett har mistet tilkoblingen til kjernenettet og fungerer som en autonom eller flere autonome basestasjoner. Hvordan det skal gjennomføres, både teknisk og operasjonelt. |
| 8 | I1 | I det nye Nødnettet? |
| 9 | L | I det nye Nødnettet, i 5G. Det er en viktig presisjon. |
| 10 | I2 | Jeg har forsåvidt sett, altså, jeg har lest informasjonsskrivet og det er jo kjempespennende oppgaver. Dere jobber jo sammen med Eirik og jeg kjenner han godt, så dere er råheldige som har med Eirik. |
| 11 | L | Det har vi merket. Jeg føler han kjenner hele Norge. |
| 12 | E | Ja, han kjenner veldig mange. |
| 13 | I2 | Ja, Eirik har jobbet med det her i 100 år så han kjenner alle. |
| 14 | E | Vi kan jo åpne med- Det vi lurer litt på er litt sånn bruksområder og hvilke tjenester som brukes. I hvilke scenarioer opplever man ulike typer utfordringer og sånne ting, med dagens Nødnett da, og så kan vi på en måte gå litt videre derfra til hvordan ting kanskje blir i neste generasjon. |
| 15 | I1 | Skal vi si altså, når Nødnettet ble anskaffet så var det jo krav til både talefunksjonalitet og datafunksjonalitet. Det var jo på den tiden også behov for det. Men det fantes ikke én teknologi som klarte å løse både talebehovet og data/videobehovet den gangen. Så var det mye kritikk i media når Nødnett ble bygd ut og teknologien TETRA ble valgt. Det var mye i mediedialogen om at dette her er så gammeldags, men det har vist seg at talefunksjonaliteten i TETRA er suveren. Den er nødvendig, og den er nok det viktigste for nødetatene. Men det jeg da har sett opp igjennom er at behovet for data og videotjenester øker -- At behovet og kritikaliteten for det øker. Så det er nok den største utfordringen med dagens Nødnett, basert på TETRA, at det ikke støtter data/videotjenester som tjenestene har behov for. |
| 16 | L | Ja, ikke sant. Men videotjenester, brukes det aktivt i dag? |

| | | |
|---|---|---|
| 17 | I1 | Det brukes vel ikke aktivt, men det pågår jo- Altså, covid-19 har trigget behov for en del nye funksjoner. Så i april ble det gitt et ekstra oppdrag om å implementere video inn til AMK og legevaktsentraler for å understøtte å kunne kommunisere med publikum på video. |
| 18 | L | Er det mest bruk av videotjenester ut mot innringere gjennom telenettet, eller kunne du se for deg at det er et kritisk bruksområde å ha det mellom Nødnett-operatører også? Mellom brukerne og kontrollrom. |
| 19 | I1 | Vet ikke om du skal svare på det jeg, [navn]. |
| 20 | I2 | Bare for å plukke opp det du sa først, [navn]. Altså, covid-19 har jo på en måte vært en katalysator for å faktisk muliggjøre at vi kan bruke videoløsninger i helse. Det er vel mange i helsetjenesten som har ønsket å bruke video i mange år, innenfor mange områder. Men på grunn av det lovverket som finnes og de strenge reguleringene som finnes, spesielt rundt personvern for eksempel, så har det på en måte ikke vært mulig. Altså, teknisk har det vært mulig i mange år, men det har ikke vært lov rett og slett. Men covid-19 nå gjør at, tja, nesten alt blir jo lov for å få pasientbehandling til å fungere. Så det er som sagt en veldig bra katalysator for å få ting på plass. Til spørsmålet ditt, Lina: Det foregår et helt konkret prosjekt i sykehuset Innlandet, jeg vet ikke om du har sett det, der de jobber med noen sånne videobriller fra ambulanseoperatøren, eller ambulansesjåføren typisk, inn til AMK-legen. Et helt konkret prosjekt som pågår ved sykehuset Innlandet akkurat nå, der de bruker kommersielle nett som databærer, men som helt klart kan være et område der neste generasjons Nødnett kan brukes i fremtiden for å være den sikre, stabile og trygge databæreren. |
| 21 | L | Har det prosjektet et navn jeg kan søke opp? |
| 22 | I2 | Eeh, det prosjektet klarer vi vel å finne. Du finner referanse til det blant annet i nasjonal helse og sykehusplan, og så hvis du bare søker på sykehuset Innlandet og videobrilleprosjektet så finner du blant annet en lengre video som er gjort av NRK. Så det er jo én type kommunikasjon internt i helsetjenesten der Nødnett definitivt vil være en sentral bærer. Og så har vi andre prosjekter som [navn] nevnte, typ kommunikasjon mellom innringer og helsetjenesten, og da vil det ikke være Nødnett som er involvert sånn sett. Men det kan jo være en naturlig videreføring om du sier at du for eksempel skal sette innringer på video i kontakt med brann/politi ute på skadested. Og sånn sett å koble sammen det kommersielle nettet og bruk av Nødnett som bærer. Så det er et uvant mulighetsrom, så fort vi får lov til å gjøre det. Både internt i helse, og mellom nødetater. Vi ser jo for eksempel at brann, 110-sentralen, har kommet lenger enn oss med bruk av video sånn sett. At de har et litt mindre rigid regelverk da. |
| 23 | L | Litt mindre strenge krav til personvern kanskje? |
| 24 | I1 | Det vet vi ikke kanskje, men det tvinges jo litt av sånne hendelser som for eksempel Gjerdrum. Den trigget jo veldig et behov for video, da politihelikopteret sendte video fra skadestedet ned til nødetatene i KO, slik at de kunne bruke det. Så det er jo noe sånt, ganske nylig, som viser behovet for en felles situasjonsforståelse for nødetatene. Og bruk av droner -- det er mange prosjekter i helsetjenesten som ser på bruk av droner. Det er droneprosjekter i politi, og det er droneprosjekter i brann, så jeg tror alle nødetatene har prosjekter som ser på bruk av droner, og da er det jo video som er aktuelt å overføre der. Og det å kunne ha et Nødnett som kunne være en sikker bærer for det, vil jo da være nødvendig. Så det første svaret på spørsmålet ditt om det brukes i stor grad er vel nei, men det er mange pilotprosjekter som pågår. Slik at når det nå har blitt mer akseptabelt, så tror |

| | | |
|---|---|---|
| | | jeg at det her kommer til å ta ganske av. Utfordringen er jo nå da at vi ikke har noe Nødnett som dekker det, så da blir det bruk av kommersielle nett uten robustifisering eller noen sikkerhetsløsninger som er bygd inn. Så da må man legge det på toppen, som kan utfordre- Og så er de vel ikke bygd heller for å dele nettet mellom nødetatene. |
| 25 | L | Så hvis vi da ser en 5-10 år frem i tid så er det da realistisk å tenke at det er en kritisk funksjonalitet med videosamtaler. |
| 26 | I2 | Lenge før. Covid-19 gjør at ting går så mye fortere, så jeg har vondt for å tro at vi ser så mye som 5 år frem i tid. Men det er en ganske stor jobb som må på plass, som [navn] sier, for å få standardisert dette her spesielt mellom etater. Vi så jo det på Gjerdrum, at de var helt avhengige av at operasjonsledere samlet seg i KO fordi de ikke hadde mulighet til å streame videoen som politiet tok ned fra helikopteret sitt til de andre nødetatene for eksempel. De fikk det kun ned på politiet sine enheter i KO. Det er jo en av de tingene som vi har sett så langt fra Gjerdrum. Og så var vi heldig på Gjerdrum, for mobilnettet funket jo. Det ramlet ikke ned. Det er jo hele greien med Nødnett, å faktisk sikre at vi har et sikkert og stabilt nett som klarer å overføre ikke bare tale, men og video i den type settinger/hendelser uansett. |
| 27 | L | I min oppgave så ser jeg på - Jeg bare drar den dit jeg, Eivind - Så ser jeg jo på tilfellet der en basestasjon eller en gruppe basestasjoner har blitt isolert fra resten av nettverket, typ at du har maks uflaks og begge de redundante transmisjonslinjene er nede, og kun de som er det området kan kommunisere med hverandre. Så da lurte jeg på, dere snakket om videobehov og databehov, kan dere se for dere at det er behov for video og data mellom de operatørene som er i felt hvis de har mistet kommunikasjon med kontrollrommet. |
| 28 | I1 | Altså, det er nok helt avhengig av type aksjon tror jeg. For en sånn type Gjerdrum, det de gjør der er at de setter en lokal redningsstab, og da har du lokal skadestedsansvarlig for hver av nødetatene, og så har du et KO. Og så kommuniserer du da fra KOet og ut på skadestedet som er da i nærheten. Det så vi veldig tydelig på Gjerdrum. Og i et sånt tilfelle vil det jo være veldig behov for å ha kommunikasjon lokalt. Men det er bare i de store hendelsene at det etableres et KO lokalt. I nesten alt annet styres det jo fra en av disse tre 11X-sentralene. Og da sitter lederen inne på operasjonssentralen eller AMK-sentralen eller 110-sentralen, og er helt avhengig av at kommunikasjonen fungerer ikke bare lokalt, men ut. Så derfor vil på en måte behovet være avhengig av hvilken type skadested det er. Og jeg vet at lokale siter, sånn local site trunking som det heter i TETRA, likte vi ikke noe særlig for da blir brukerne hengende på dem. Istedenfor å kanskje henge på en annen site som kanskje har litt dårligere dekning, men som kunne ringt ut. Så der var behovet egentlig å få de bort fra de lokale og heller kanskje bruke en repeater som gjør at man kan snakke via den og inn i nettet, istedenfor å snakke bare lokalt på ett skadested. |
| 29 | L | Dette er det flere som har sagt. |
| 30 | I2 | Men samtidig er det graden av det. Det 4G-nettet som vi har i dag er 110% avhengig av at Telenor sin infrastruktur i Oslo fungerer. Hvis du mister forbindelsen til Oslo i dag så ramler alt ned, da slutter alt å virke. 5G har helt andre muligheter til å la telenettet fungere til en viss grad. Enten om du går på sone controller eller om du går helt ned på én local site controller, at du faktisk kan få én site til å stå der som en slags repeater-sak. Så uansett hvordan du ser på det er det jo veldig spennende med 5G og de mulighetene for at segmenter av nettet fortsatt kan fungere, sånn som Nødnett gjør. Som [navn] sier er det ulike meninger og oppfatninger om local site trunking som vi har i Nødnett i dag. Men ihvertfall for et konsept der vi kan bryte det ned og si at en ring av basestasjoner eller et antall basestasjoner kan fungere adskilt fra resten av telenettet er definitivt spennende. Fordi dagens telenett er ekstremt sårbart. |

| | | |
|---|---|---|
| 31 | I1 | Så tenker jeg at, basert på at det er såpass forskjellige behov avhengig av skadested, så tror jeg det er viktig at det, sånn som [navn] sier, å utnytte den fleksibiliteten som 5G og det kommersielle nettet har. Si at du per tilfelle bestemmer om du skal slå av de her, eller om du skal slå på. Og sett at du kan konfigurere nettet ved en feilsituasjon slik at du får tilpasset det til behovet. Så jeg tror kanskje operativ styring, gitt at det er mulig, ville vært behov for å slå på eller av eller sammenkoble og tilpasse dette her etter kritiske behov. Men det stiller jo krav til den operatøren, hvis det skulle være sånn [vanskelig å høre], for da må man på en måte vurdere nødetatenes behov kontra det store kommersielle behovet og alle betalende abonnenter der ute. Og det vil bli en avveining som sikkert er litt tøff. Og derfor så må vi kanskje ha reguleringer for å få det til, for en operatør vil kanskje tenke på income og ikke på nødetatsbrukerne. |
| 32 | L | Her var det mange nyttige innspill synes jeg. |
| 33 | I1 | Men jeg kjenner ikke godt nok til det til at jeg kan gå inn på det. Hvordan du kan styre nettene i et sånt type 5G-nett, men jeg tror det er som du sier mer fleksibelt enn det dagens Nødnett er. |
| 34 | I2 | Ja, det har vært flere av de store nye tingene som kommer i 5G som gjør at du har en helt annen mulighet til å - jeg vet ikke om det blir riktig begrep, men - segmentere nettet litt mer som vi har i Nødnett. Som sagt, i dag er du så ekstremt avhengig av Oslo og Telenor sine lokaler på Fornebu for at nettet skal fungere. Men 5G tenker jo på en måte å legge flere ting ut på sone controllere, ut på site controllere, og ha funksjonalitet tilgjengelig selv om du bare har én basestasjon. |
| 35 | E | Er dere noe involvert i den prosessen med utviklingen av neste generasjons Nødnett? |
| 36 | I1 | Oh, yes. I helsetjenesten så har vi og [organisasjon] fått det spesifikke oppdraget om å bidra inn i den. |
| 37 | I2 | Det som vi har fått som oppdrag da: Vi sitter nå som et mellomledd mellom den samlede helsetjenesten og DSB sitt prosjekt. Oppdraget vårt er nå å dra den prosessen her både mot kommunehelsetjenesten og spesialisthelsetjenesten, alle sykehusene, alle AMK-sentralene, alle ambulansetjenestene i hele landet. Nøyaktig hvordan vi skal gjøre det vet vi ikke helt, men vi skal ta lead og samle inn krav og behov og få videreformidlet det inn i DSB sitt prosjekt og få den her dynamikken til å fungere. Så i NGN, neste generasjon Nødnett-prosjektet, vil vi sitte ekstremt sentralt. Vi driver forsåvidt også og bemanner opp for å ha flere ressurser for å drive de prosessene her for oss. Så vi jobber med veldig spennende ting sånn sett. Det finnes straks jobbmuligheter rett borti gata. |
| 38 | E | Dere nevnte tidligere at det var litt utfordringer knyttet til det å bruke kommersielle bredbånd til de datatjenestene man benytter i dag. Hvordan tror dere det kommer til å bli, har dere gjort dere noen vurderinger rundt hvordan det kommer til å bli å involvere de kommersielle aktørene mer i selve Nødnett i neste generasjon? |
| 39 | I1 | Det er jo det som er litt av hovedutfordringen i den konseptvalgutredningen som pågår. Det er å finne ut hvordan det kan gjøres. Men det er klart, det har på en måte vært litt trygt å ha et eget dedikert nett som ikke er avhengig av å bruke de samme bærerne og den samme kapasiteten som alle andre. Det å gå derifra og over til et nett som skal, hva skal man si, krangle med de andre kommersielle brukerne som er veldig mange i forhold til oss, og der vi har stilt noen vanskeligere krav som i visse tilfeller kanskje vil sparke ut kommersielle brukere fordi vi trenger nettet. Det er veldig krevende, og det må reguleres. Det kan ikke |

| | | |
|---|---|---|
| | | være økonomien som styrer det hvis det skal kunne fungere. Og det er derfor NKOM sitter inne i prosjektet. Samtidig er det det vi ser, at vi har prøvd nå å etablere et dedikert TETRA-nett som bare er laget for oss, og det som skjer er at du får et veldig dedikert nett, men du har ingen utvikling du har ingen penger. Staten har ikke penger, selv i Norge. Noen må betale for utviklingen. Vi blir stuck i et sikkert nett, men som ikke dekker behovene. Det er i den settingen vi må forstå den dreiningen fra å være et dedikert nett til å bli en del av et kommersielt nett. Staten har ikke penger til å kjøpe et dedikert kommersielt nett til nødetatene, 40 tusen brukere, og sørge for utviklingen av det som et fjerde kommersielt nett. Og vi har heller ikke råd til å betale den kostnaden det ville vært, for i Nødnettet nå som er dedikert til oss så må vi betale alle kostnadene ved driften. Så utfordringen er kost-nytte, og da må man begynne å se på det. Og vi tror at ved å regulere bruken og tilgangen i Nødnettet, i et kommersielt nett, så må vi stole på at operatørene tar ansvar for at nettet er robust nok. Og det må da reguleres. Det må gjøres noe med nettet for at det skal bli robust. Det er det ene. Det andre er at det finnes en del funksjoner i Nødnett som dere kanskje er kjent med, vi har blant annet et AGA-nett som gjør at vi kan ha kommunikasjon til helikopter, som ikke finnes i kommersielle nett. Det finnes en del sånn spesialfunksjonalitet som ikke finnes i kommersielle nett enda. Men som man tror vil kommer, og som holder på å standardiseres. Så det er jo spennende å gå over, og det er jo ikke bare vi som gjør det. Heldigvis så er det mange som ligger foran oss. Vi har fått en del erfaring fra England. Samtidig så ser vi at Sverige og Finland har en annen approach enn oss. Der vi tenker at vi skal la markedet levere tjenesten, så tenker Sverige og Finland at de skal ha et statlig overbygg som regulerer det og som kjøper tjenestene av leverandøren. Så her ser vi at vi har litt forskjellig tilnærming til det, men alle går fra dedikert TETRA-nett til bruk av kommersielle nett, men med forskjellige varianter. Så er det sikkert grunner til at Sverige, Finland og vi har litt forskjellige tilnærminger til det. Jeg vet ikke om det var et godt svar på spørsmålet ditt, men, hehe. |
| 40 | E | Veldig godt svar! |
| 41 | E | Med tanke på å lære litt av andre land og sånt - Internasjonale samarbeid. Er det noen tanker rundt hvordan samarbeidet over grensen skal fungere hvis man for eksempel har ulike modeller for NGN i Sverige og Norge? |
| 42 | I1 | Hmm, bra spørsmål. Det er akkurat det vi sitter og besvarer nå. Jeg vet ikke om du vil svare litt på den, [navn]? |
| 43 | I2 | Nei, altså, jeg har jo ikke noe godt svar på det. Det ligger som en spørsmålsstilling i konseptvalgutredningen og vil bli en problemstilling inn i forprosjektet. Det er en ting som må løses. Vi har vært heldige, hvis du kan kalle det det, at Norge, Sverige, Finland og Danmark og forsåvidt har hatt et TETRA-nett som har muligheter for å koble ting sammen. Hva slags neste generasjon nød- og beredskapsnett vi kommer til å ha i de fire landene er jo forsåvidt ukjent. Min refleksjon er at den jobben som er gjort, spesielt mellom Norge og Sverige, men og mellom Norge, Sverige og Finland, med å koble sammen nettene viser at det er et behov. Det er et behov som må løses. Nei, det er et godt spørsmål. Som sagt konkluderer jeg med at behovet finnes. Hvis ikke hadde vi ikke kommet til og gjort hele den store og relativt dyre jobben som vi har gjort i de tre TETRA-nettene som ligger i de nordiske landene. Det er ihvertfall min refleksjon. |
| 44 | I1 | Før Nødnett så var det jo lite felles funksjonalitet, så dermed var det kanskje lettere å gå over fra analoge systemer til et felles Nødnett. Mens nå er det norske Nødnettet blitt såpass godt. Det er bygd ut bra dekning og oppetid, og det er koblet sammen mellom landene, og det er bygget et dedikert AGA-nett. Når du legger sammen alt dette så blir det - Det å få til overgangen til kommersielle nett som ikke har det her, det vil kanskje bli komplekst. Litt |

| | | |
|---|---|---|
| | | vanskeligere, litt dyrere. Så jeg vil tro at man her kanskje må tenke litt stegvis, og se hvor moden teknologien blir for å gjøre det. Og den andre utfordringen er hvor standardisert grensesnittet blir. Hvis Norge, Sverige og Danmark går inn på noen grensesnitt som ikke er standardiserte, så vil utfordringen med å koble dette sammen bli mye større. Da blir det mer skreddersøm istedenfor åpne grensesnitt som kan fungere sammen. Så det kommer kanskje an på hvor langt 3GPP er kommet med å definere standarder, og hvor langt operatørene er kommet med å implementere standarden, hvor lett det faktisk blir å få til å fungere. Det er vel litt av utfordringen. Hvis vi går i dedikerte nett som ikke er standardiserte, så vil vi kanskje havne i en situasjon der det er vanskelig å komme ut av en avtale, fordi du sitter igjen med skreddersøm selv om du er inne i et kommersielt nett. Så det er en utfordring å vurdere når det er modent og når det er riktig å gjøre det. Det er ikke så lett for oss å si, det er operatører og teknologien som vet det. Det har jo vært en svøpe for Nødnett, at det heller ikke var helt standardisert da man kjøpte det. Motorola hadde sin måte å implementere det på og Nokia hadde sin måte, og derfor så ble kostnaden ved å få dette til å fungere sammen - Det var liksom ikke bare å koble sammen noen ledninger - Det kostet liksom 100 millioner. Så det kan være en utfordring, for å svare på spørsmålet ditt. Hvor modent det er, og hvordan operatørene har implementert standarden. |
| 45 | E | Med tanke på modningsgraden og når man eventuelt bestemmer seg for å kanskje skru av det gamle TETRA-nettet, har man noen sånne tydelige krav fra brukernes side på at NGN skal være - For eksempel sånn som de sier i England, at det skal være minst like bra som det gamle nødnettet før vi i det hele tatt kan tenke på å bytte over. At den kjernefunksjonaliteten som går på talegrupper og sånn er så viktig i bunn at den datafunksjonaliteten bare kommer i tillegg. At den talefunksjonaliteten må være der. |
| 46 | I1 | Ja, det kan en vel si at har vært et krav. Og det har vel DSB også kanskje like tydelig kommunisert at det er et krav fra deres side som prosjekteier, at det skal ikke være dårligere. Det var også et krav når vi gikk fra analoge systemer til Nødnett. Vi la sammen dekningen og funksjonaliteten og så ble det summen av det vi hadde, [vanskelig å høre]. Det er som du sier, vi tar med oss den talefunksjonaliteten med hurtig oppkobling og stabilitet, og dekningsgraden er såpass kritisk for den operative håndteringen. Per i dag så klarer de seg vel med talestyring av akutte situasjoner og så bruker de mobilfunksjonalitet ved siden, som ikke enda har rukket å bli virksomhetskritisk. Men jo bedre og bedre de systemene blir, og jo mer effektivt funksjoner og operasjoner vil gå med automatiserte tjenester jo vanskeligere blir det nok å gå tilbake. Så hypotesen er at om det ikke er virksomhetskritisk i dag, så blir det virksomhetskritisk. Akkurat tiden for det er ikke så godt å spå, men hvis man ser noen år frem i tid - og da se tilbake og se at vi ikke hadde video vil nok være litt rart. Vi ser det i utlandet, politi som går med video på seg. Så å ha video av en operativ situasjon, like mye for sikkerheten til den tjenestemannen selv. Så det er nok noe som kommer, også her. |
| 47 | E | Jeg bare spør, jeg. Med tanke på dekningsgraden - Den avgjørelsen som har blitt tatt om at man skal la det kommersielle ta ansvar for dekningen så bygger det også egne basestasjoner som et tillegg til den kommersielle dekningen som blir bygget ut. Har man noen tanker eller bekymringer rundt det at det er det kommersielle som skal styre dekningsgraden da, for eksempel. Spesielt med tanke på at man kanskje opererer i grisgrendte strøk der det ikke bor så mange brukere av det kommersielle nettet. |
| 48 | I1 | Det er vel derfor det koster såpass mye å gå fra dagens Nødnett til et kommersielt nett. De har sett på realdekning for Nødnett og kommersielle nett, og så har de sett på - For Nødnett er jo bygd ut i nasjonalparker og sånt - Og så har de regnet ut da hvor mange kommersielle baser må du ha for å utgi den ekstra dekningen som Nødnett har i dag. Og så er de estimatene lagt inn i det å realisere dette her i kommersielle nett. Kravene stilles til den |

| | | |
|---|---|---|
| | | kommersielle operatøren, slik at man må bygge ut den tilsvarende dekningen men at operatøren da eier de. Jeg har ikke oppfattet at staten skal eie noen basestasjoner på utsiden. Staten skal betale operatøren, slik at de skal eie de hundre sitene. Operere de og drifte de inn i nettet. Og så er det en diskusjon rundt de sitene som den operatøren da får, de vil gi en konkurransefordel i forhold til de andre operatørene. Og så er diskusjonen om de skal være tilgjengelig også for de andre operatørene sine brukere. Det er et litt sånn konkurransevridningsspørsmål. Sånn har jeg ihvertfall oppfattet i Norge at det er tenkt. |
| 49 | I2 | Og det er viktig, for vi har ikke muligheten til å ta vekk dekning i områder som Nødnett har i dag når vi skal over på det nye. Så det vil være behov for utbygging. Så blir dette en anbudskonkurranse, mest sannsynlig, der den som er villig til å ta størst kostnad på egen kjøl kanskje vinner anbudet. |
| 50 | L | Jeg er spent på å følge med på det her, altså. |
| 51 | I2 | Men har vi noe dokumentasjon vi kunne sendt over? Vi har jo gjort noen rapporter på egen kjøl som belyser en del av de tingene vi snakket om som du kanskje kunne sendt over etterpå, [navn]. |
| 52 | I1 | Vi har noen rapporter som bygger opp under - Det finnes en nasjonal helse- og sykehusplan, jeg vet ikke om du kjenner til den, men det er et dokument som sier noe om hvordan du skal løse helse- og omsorgsbehovet fremover. Og det inkluderer en mobil sikker bærer sånn som Nødnett er tenkt, og de skriver egentlig hvordan den kan bli en bærebjelke i fremtidens helse- og omsorgstjenester. Og den er ikke unntatt offentlighet, så den kan vi sende over. |
| 53 | I2 | Jeg tenker og, [navn], på den rapporten som vi har gjort knyttet til utvidet scope for neste generasjons Nødnett. Det er jo et offentlig dokument som oppsummerer veldig mye og som det står mye spennende i. |
| 54 | I1 | Det dokumentet kan vi nok sende over. Men det er viktig å forstå at det er helse sitt innspill, og at det ikke nødvendigvis er noe DSB har ivaretatt. Men det gir et perspektiv på hvor viktig fremtidens nød- og beredskapskommunikasjonsnett kan bli for samfunnet. |
| 55 | E | Grunnen til at vi intervjuer litt ulike er jo for å få litt ulike innspill fra ulike aktører i denne prosessen, så det er jo absolutt relevant selv om det ikke er satt i stein enda. |
| 56 | I1 | Det går an å sende over det her, og så ha påfølgende møter hvis dere trenger det. Her har vi folk som jobber med de rapportene. |
| 57 | E | Jeg lurer på om dere har noen spørsmål til oss, eller om det er noe vi ikke har snakket om som dere tenker at det burde vi jo ha sett på? Siden dere vet litt om hva vi holder på med på en måte. |
| 58 | I1 | Dere har vært innom veldig mye av de viktige spørsmålene. En risiko er det her med helikopternettet, eller air-ground-air. Og kanskje hvordan satellittkommunikasjon kan bidra i fremtiden. Nettene er jo ganske sårbare, og spørsmålet er hvordan nødetatene kan tilgjengeliggjøre seg også i områder der Nødnett ikke har dekning. For eksempel via satellittkommunikasjon. |
| 59 | L | Jeg har ikke satt meg inn i det i det hele tatt egentlig, det er kanskje på tide. |
| 60 | I1 | Air-ground-air er implementert i Nødnett i dag med basestasjoner som skyter oppover og gir en god dekning. Og så hvis man tenker uavhengig av infrastrukturen på bakken, hvis man |

| | | |
|---|---|---|
| | | tenker satellittkommunikasjon som gir en ganske god flatedekning, men ikke innendørsdekning. Hvordan det kunne forsterke eller komplementere et neste generasjons Nødnett. |
| 61 | E | Det er vel et veldig godt eksempel på noe som kanskje ikke nødvendigvis ville vært i en kommersiell operatørs interesse å bygge ut. |
| 62 | I1 | Ja, som kanskje må bli noe som staten må tenke på i forhold til risiko og sårbarhet, og så komplementere. Har du noe annet, [navn]? |
| 63 | I2 | Altså, det er veldig spennende ting dere holder på med å skrive om. Jeg tenker at det finnes jo masse folk i helse, både på et mer teknisk nivå og andre nivåer som det kanskje kunne vært spennende for dere å snakke med. Har dere på en måte noen innfallsvinkler til helse mot operativ tjeneste, har dere behov for noen ting der? |
| 64 | L | Vi har allerede snakket med [organisasjon]. |
| 65 | E | Vi prøver på en måte å snakke med litt forskjellige. Vi prøver å få representert de ulike nødetatene og sånn, og så skal vi snakke med de som sitter på andre enden av forhandlingsbordet da på en måte i DSB og i NKOM og sånne organisasjoner, og så er det mobiloperatørene som vi skal snakke med for å høre litt hva de har planlagt. Visjonen er liksom å sammenstille det til en eller annen - Å komme med et forslag til hvordan det kan være rimelig å gjøre ting. Sikkert litt det samme som dere har jobbet med i den KVUen, men den får vi jo ikke se, så det blir på siden av den, hehe. |
| 66 | I2 | Haha, ja, nei, dessverre så er jo den unntatt offentligheten enda. Men på et eller annet tidspunkt så håper vi at den blir frigitt. |
| 67 | L | Vi hadde håpet at den skulle komme nå på nyåret, men den gang ei, hehe. |
| 68 | I1 | Da er det liksom de operative miljøene som dere kunne ha sett på, men [vanskelig å høre]. Hvis dere vil snakke med noen på ambulansestasjonen på en AMK-sentral, så går jo det an. |
| 69 | L | Men er det greit for dere om vi tar kontakt for eventuelle oppfølgingsspørsmål? |
| 70 | I1 | Det er det. Flott, men da sender jeg over den rapporten, og så får dere ta kontakt hvis det er noe mer. |
| 71 | L | Det var veldig hyggelig å prate med dere, takk for at dere tok dere tiden! |
| 72 | I1, I2 | Takk, det samme. Ha det bra! |
| 73 | L, E | Ha det bra! |

# Appendix E
# Mobile Network Operator A

This interview is conducted with a representative of one of the three mobile network operators in Norway. A wide range of topics related to NGN are discussed, with particular emphasis being put on the single turnkey provider deployment model, as it is the one favored by the interview subject in question.

Parts of this interview have been redacted in keeping with the interview subjects wishes. Where an entire paragraph has been redacted it has been marked with [Fjernet]. However, where only parts of a paragraph have been redacted, no explicit remarks are made in regards to this. A side-effect of this redaction is that it may cause the flow of the conversation in some parts of the interview to appear strange or disjointed in one way or another.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, da ser det ut som lydopptaket er på. Da spør jeg deg for ordens skyld om det er greit at vi gjør lydopptak. |
| 2 | I | Det er helt i orden. |
| 3 | E | Jeg kan begynne med å presentere min egen oppgave. Jeg ser litt på utfordringer knyttet til samarbeid med kommersielle mobiloperatører i utførelsen av neste generasjons Nødnett, med spesielt fokus på 5G og hvordan ting kan bli i fremtiden. Så er det jo veldig relevant for meg å snakke med en representant for en av mobiloperatørene. |
| 4 | L | Jeg ser mer på, ja, autonome basestasjoner i NGN i 5G. Så jeg er inne og ser på IOPS og edge computing og hvordan det skal gjennomføres, kort oppsummert. Jeg skjønner at du kan ha litt innsikt i mye relevant her. |
| 5 | I | Ja, skal jeg presentere meg selv, eller er det ikke ønsket egentlig? Jeg har jobbet noen år i [mobiloperatør]. |
| 6 | E | Så jeg lurer litt på hva [operatørs] forhold til de ulike deployment-modellene er. Er det f.eks. ønske for [operatør] å være eneste turnkey provider og ha full oversikt over nettet sånn som AT&T i USA, eller vil dere være mer som EE er i Storbritannia, der man har ansvar for radionettet og lavere del av core. |
| 7 | I | Som utgangspunkt ser vi at vi ønsker å ta en turnkey-leveranse. Kall det for as-a-service, der vi leverer komplett pakke med både radioløsninger og transportnett og tjenester og core-nett f.eks. Mulig også terminalhåndtering, altså konfigurasjoner og hvem som skal være med i ulike grupper. Det har vi også et opplegg for. Det er vårt utgangspunkt, at vi ser at det er både en synergi og gir en bedre opplevelse egentlig som en pakke hvis du har en turnkey. Du vet jo sikkert også at det har vært diskusjoner i Norge på er det en operatør eller flere operatører. Vårt fortrinn, eller som vi prøvde å posisjonere opp er at det er bedre å gå til en operatør. Da blir det enklere i forhold til å sørge for interoperabilitet på ulike nivåer og roaming med full støtte for tjenester, bruker-grupper, etc. Flere operatører er ikke en umulig modell, men det gjør det vanskeligere. Så vi har nok gitt en preferanse for en en-operatør-løsning. Da må vi jobbe med de som ønsker tjenesten og hva deres krav er, hva de ønsker, både geografisk og på tjenestesiden. Det er vårt utgangspunkt. |
| 8 | E | Jeg synes det er helt supert å høre. Det er bare å prate. |
| 9 | I | Vi ser en helt klar synergi for samfunnet å kunne bruke de offentlige frekvenser og spektrum til Nødnettet så vi slipper å bygge noe ved siden av og statisk sette av kapasitet. Så får vi heller prioritere bruk av spektrum under krisesituasjoner eller hendelser slik at de etatene som har bruk for det får de tjenestene de har bruk for på de lokasjonene de er til stede på. Sånn sett så går vi litt imot modeller som har vært diskutert i noen av landene, ikke kun for Nødnett, men som i Tyskland for eksempel der man skal reservere spektrum til private nett. Vi mener at det egentlig reduserer samfunnsnytten. Du kjenner sikkert til situasjonen i Norge med NKOM, som er at man heller kommer med krav til operatører om hvordan man skal betjene samfunnet best mulig, i stedet for å drive og splitte opp naturressurser. |
| 10 | E | Tenker man da at man da skal kjøre hele Nødnett på [operatør] sin infrastruktur, f.eks. som en slice, eller skal man ha dedikert kjernenett-infrastruktur eller noen sånne typer løsninger? |
| 11 | I | Vår langsiktige preferanse er å kunne kjøre det som en integrert del av det offentlige nettet |

| | | |
|---|---|---|
| | | og så heller reservere kapasitet. Om det er behov for slice eller andre differensieringsmekanismer kan vi diskutere, men det er konkrete løsninger. Det som egentlig er behovet er å differensiere, prioritere og isolere trafikk. Om du da velger å kalle det for en slice, det er en implementasjonsform som vi ser det. Men det blir gjerne kalt for en slice. |
| 12 | L | Du må ikke beklage deg, det her er veldig interessant. |
| 13 | I | Det som er litt av diskusjonen her, og dere har sikkert diskutert med de som allerede er i Nødnett i dag om hvordan det fungerer og hva som er deres smertepunkter. En ting er jo kostnaden dagens Nødnett er estimert til å koste 26 milliarder som staten og norske innbyggere skal ut med. Det er jo horribelt synes jeg, når du ser på hva som er dekningsområdet og tjenestene som tilbys. Så kostnadsmessig så er det jo helt klart synes jeg en fordel med å kunne bruke de kommersielle nettene og heller sette krav på løsning og leveranser. Det vesentlig å dra nytte av skalafordeler, også på globalt nivå som for eksempel terminaler. Fordi dagens Nødnett er et dedikert nett, får de ikke benytte seg av den globale skalaen rundt f.eks. smartphones der du har en milliard nye enheter i året. Så å begynne å dedikere nett som f.eks. TETRA, mener jeg er feil måte å gjøre det på. |
| 14 | E | Skal man da bruke vanlige mobiltelefoner til å gjøre MCX-tjenester og sånn? Skal man ikke ha spesialdesignede ruggedized devices eller noe sånt? |
| 15 | I | Jo, du må gjerne ha en ruggedized, men hensikten er å benytte standardchipene og standardkomponentene. Du må gjerne gjøre den vanntett og gummiert innpakning. Det kommer til å være mange typer devicer, også i Nødnett. Det tror jeg er litt av problemet man sliter med i dag. Fremover så er det jo ikke bare kommunikasjon mellom personer; Det er jo like gjerne video, like gjerne å droppe ned sensorer og kunne styre droner. Det blir en helt annen måte å jobbe for nødetatene tror jeg, som ikke bare gjør det mer effektivt, men også reduserer risikoen deres med å kunne sende inn droner i stedet for å selv måtte gå inn, for eksempel, og styre dem mer fleksibelt. Så jeg tror det er mange andre måter å jobbe på hvis man får tilgang til den utviklingen som skjer på device-siden, og like gjerne drone-siden. |
| 16 | I | Vi har samarbeid med noen dronefirmaer, også i Norge, som bygger roboter som kan bevege seg og inspisere på risikoområder, for eksempel. De går jo både dag og natt og i helga også, så det er jo ikke noe arbeidstid som sådan. De driver og registrerer objekter og kartlegger osv. kontinuerlig. Det er klart man kan bruke slike droner også i en nødsituasjon. |
| 17 | E | Hvis vi går tilbake til at [operatør] vil vil tilby en hel løsning for NGN, hva er de største utfordringene? Vil det være en utfordring å få bygget ut dekning tilsvarende det eksisterende nødnettet for eksempel? |
| 18 | I | Jeg tror vi har mye bedre dekning enn det eksisterende nettet. Hvis du sammenlikner prosenter og dekning, så er det overskyggende. |
| 19 | L | Det er vel forskjell på – |
| 20 | I | Men det er sånn at Nødnett har spesielle krav til f.eks. tunneler og en del andre spesielle områder, lokasjoner, som vi må supplere med. Det er det ene, og det andre er at de har jo så langt i alle fall lagt en del krav på batterikapasitet og muligheten til å overleve uten strøm, og vi er ikke der. Det kan ikke vi forsvare rent kommersielt for kunder så langt. Det må da suppleres med den type løsninger. Altså større kapasitet på batteri, eller eventuelt sekundærkilde til energi, altså til strøm. |

| | | |
|---|---|---|
| 21 | L | Dette kan vi komme tilbake til. |
| 22 | E | Mitt neste spørsmål var dette med den kommersielle interessen, og at noen av disse tingene kanskje faller utenfor det vanlige bruksområdet til vanlige brukere av [operatør] sitt nett. Tenker man da å få støtte av staten til å bygge ut nettet på denne måten? |
| 23 | I | Vi ser jo at man kommer til å ha brukt ca. 26 mrd. kroner på TETRA i den perioden her. Vi ser for oss at Nødnett kommer til å være en anbudsrunde der det er en kommersiell diskusjon. Og der blir det også en kostnad, en pris, og en kan komme med en type krav, sånn som dette med energi eller batterikapasitet og dekningskrav osv. Og det kommer til å ha en prislapp som må finansieres. Jeg synes det er urettferdig om det skal finansieres av andre kunder. Det bør finansieres av de som har kravene og som driver de kostnadene. Nå kan jeg si at det jo i syvende og sist er vi som betaler det her over skatteseddelen uansett, men greit nok. Men jeg synes at prislappen til den kommersielle forhandlingen bør fanges av de som driver løsningene. Om det da er DSB eller andre som driver disse kravene må vi håndtere. |
| 24 | E | Tenker man da at [operatør] har noen fordeler ift. andre mobiloperatører, som også har lignende planer? |
| 25 | I | [Fjernet] |
| 26 | E | Men f.eks. dette med at [operatør] i stor grad er et statseid selskap f.eks.? |
| 27 | I | Som en norsk operatør blir data i Norge. Vi er jo også en del av såkalt kritisk infrastruktur, vi er en del av totalforsvaret. Dermed får du en del andre krav som vi må etterkomme som Nødnett typisk vil kunne ta nytte av, som vi allerede må etterkomme. Det har f.eks. med hvem som har tilgang til å gjøre hva, hvem vet hvor BS står. Det skal være sertifiserte, sikkerhetsklarerte personer som jobber i Norge. Det er jo andre aspekter som ikke har med Nødnett og kommersielle tjenester å gjøre, men det har med en del av totalforsvaret og kritisk infrastruktur-krav å gjøre. Det er jo den siden av saken, men på den andre siden har vi jo betydelig flere BS enn [operatør] i Norge, og vi har jo naturligvis mye bedre tjenester enn [operatør] og mye mer fornøyde kunder. Men hvis du holder deg til det med kritisk infrastruktur så er jo det fakta. Og så det jo fakta med antall punkter, antall BS-punkter. |
| 28 | L | Du var innom litt og snakket om at det blir et annet type krav mtp. batteritid og redundans for Nødnett og redundans for Nødnett enn for kommersielle nett. Det bringer oss litt inn på mitt tema, som ser på tilfellet der BS mister tilkoblingen til kjernenettet. Brukes IOPS eller autonom operasjon av BS i kommersielle nett i dag? Har det noen nytteverdi? |
| 29 | I | Du beskrev autonome BS, og vi kan diskutere hva det egentlig er for noe. |
| 30 | L | Ja takk, veldig gjerne. Jeg vil gjerne forstå mer her. |
| 31 | I | Det vi jobber med, la meg stille et spørsmål tilbake igjen. Har dere snakket med [person] eller 5G-VINNI-prosjektet? Der jobber vi sammen med bl.a. Forsvaret, som ser på nett som skal overleve en del uforutsette hendelser. Det er jo ikke nødvendigvis en autonom BS, men et komplett mini-mobilnett. Du må ha inn hele kjernenettet, hele HLR, HSS-siden i tillegg som da skal kunne styre brukere. Det vi ser på, for å svare på det, hvis du snakker med [person] får du en diskusjon på det. Så svaret er ja, i forbindelse med Forsvaret. Det er også et Nødnett-case, og kan sikkert gå gjennom de casene om du spør han om det. Jeg vet ikke om du kjenner til open-RAN initiativene, cloud RAN, der man typisk flytter ut mer av logikken og gjør selve BS enklere og kanskje sentraliserer noen av kontrollfunksjonene som da går på en cloud-plattform. Den cloud-plattformen kan like gjerne kjøre et fullt mobilt |

| | | |
|---|---|---|
| | | core-nett hvis du vil. Så det ser vi på. Det er ikke nødvendigvis enkelt-BS, men et cluster av BS. |
| 32 | I | Så det er en av de tingene vi ser på, men sånn som jeg forstod spørsmålet når jeg leste det før denne sesjonen her, så leste jeg det som en BS som for eksempel er på en brannbil, altså en mobil BS som også potensielt er autonom. Altså kan den styre brannmannskap i det området og da ha full kontroll over det. |
| 33 | L | Nei, jeg må jo innrømme at jeg stadig forstår mer og mer av min egen oppgave ettersom jeg snakker med deg her. |
| 34 | I | Vi har et selskap i [operatør] som heter [navn] som leverer dekning til ferger og skip. |
| 35 | L | Ja, jeg har hørt litt om de løsningene. |
| 36 | I | Det er gjerne et cluster av BS som er autonome på skipet. Det kan skaleres ned til en BS eller et antall BS, om du vil, f.eks. på en brannbil eller en flåte av kjøretøy. Politi, ambulanse og brann, f.eks., om det svarer på formålet. |
| 37 | I | Det vi ikke har sett på foreløpig, bortsett fra det som [person] ser på, er å ha en enkelt BS som har hele logikken, altså hele mobilnettet på BS. Som sådan har vi ikke sett på det, der har vi ikke sett spesiell interesse, bortsett fra det forsvarsscenarioet. |
| 38 | L | Ja, for Nødnett har en funksjonalitet for det som visstnok fungerer litt sånn medium. |
| 39 | I | Så langt har vi som sagt ikke sett på det. Det er ikke en kommersiell driver for sånne typer ting. Det vi har sett på er nedskalerte, halvprivate nett. Det vi gjør i Sverige med å levere mobilløsninger til produksjonslokaler som er autonome. Så kan du styre roboter i en produksjonsbedrift, og så scoper du litt tilsvarende her. I caset i Sverige blir det dedikert til det formålet, mens her blir det mer generelt, et generelt mobilnett. Løsninga som sådan, sånn som vi ser det, er jo veldig lik. |
| 40 | L | Jeg tenker, haha. |
| 41 | I | I det mest avanserte scenarioet så kan du ha, en BS på en av de bilene som rykker ut der, der det er et helt mobilt, kall det mobilnett, for akkurat den aksjonen der. |
| 42 | L | Ja, ikke sant. |
| 43 | E | Men det å skulle ha HLR og sånt ute i disse autonome BSene, det medfører noen utfordringer tenker jeg. |
| 44 | I | Den typen funksjoner ønsker vi å sentralisere hvis vi kan, og distribuere hvis vi må. I det tilfellet her, med autonome BS som skal være helt autonome, må du jo distribuere helt ut der. Nå er jo alle disse funksjonene cloud-basert, så de kjøres i containere med Kubernetes. Det minste core-nettet jeg har sett i fysisk størrelse er på størrelse med tre kredittkort. Legger du de på hverandre har du det du trenger for å kjøre et fullstendig core-nettverk for 10 000 brukere. Så det er ikke store tingene som skal til av fysisk hardware. Og det var utviklet for det amerikanske forsvaret, som ville ha et autonomt mobilnett så de egentlig skulle kunne kjøre core-nettet i en drone. Hele greia var i en drone som fløy over området. |
| 45 | L | Har den løsningen et navn vi kan søke oss frem til? |

| | | |
|---|---|---|
| 46 | I | Jeg må søke tilbake, jeg tror det er to år siden vi hadde en diskusjon med det firmaet. Det var en del av et NATO-prosjekt. De ville det over til case med gårder der de hadde sensorer rundt omkring i åkrene og dronen bare fløy over og samlet data fra IoT-sensorene. Da den kom tilbake til hovedgården så kunne den laste fra seg data. |
| 47 | L | Kult! Jeg trekker samtalen tilbake til de to formene, og misforståelsen rundt begrepet autonomi. For i oppgaven min så ser jeg jo i større grad på tilfellet der en normal BS som er ute og opererer for Nødnett eller NGN mister tilkoblingen til kjernenettet for en stund, og så må den eller et cluster av BS virke som et lokalt nettverk med fungerende kjerne der ute. Har du lyst til å snakke litt om dine tanker rundt det? Og mtp. gjennomførbarhet, hva er hovedutfordringene å løse for det i 5G? |
| 48 | I | Du har både den løsninga og så har du device-to-device-kommunikasjon som også kommer som en release, som dekker deler av behovet kanskje. |
| 49 | L | Ja, nettopp, men det har jeg scopet litt vekk. |
| 50 | I | Det vi ser som en utfordring er hvordan du sikrer at det ikke plutselig er en angriper eller spion eller whatever som klarer å komme seg inn på løsninga. Hvordan er det fortsatt bare de autoriserte brukerne som kan bruke det. For hvis du ikke har da full mobilkapabilitet så må du gå ned litt på sikkerhetskravet. Da må du egentlig kunne sjekke SIM-kortene, at det er autoriserte enheter og bruker, osv. Mangler dette er du åpen for angrep. Men det som naturligvis er utfordringen først er å kunne prøve å få til et fullt mobilnett der ute når du har behov for det. Og litt av problemet er at du vet jo ikke, hvis du ikke kjører det kontinuerlig så vet du jo aldri om det fungerer tilfredsstillende når situasjonen oppstår. Og vi ønsker egentlig ikke å kjøre det her kontinuerlig, vi ønsker jo å kunne sentralisere det vi kan. Da blir det et lite dilemma rundt hvordan man skal kunne imøtekomme noe sånt når behovet er der. |
| 51 | L | Nettopp. Så det er vel snakk om å ha sovende kjernefunksjonalitet ute som på en måte vekkes opp hvis det blir isolert, men det er vel et spørsmål om kostnad i stor grad da? |
| 52 | I | Ofte er det software-lisenser og drift som er primære kostnader. |
| 53 | E | Hva med utfordringer i en modell der radionettet og kjernenettet er driftet av to ulike providers? Hvem skal da ha ansvar for denne kjernen i edgen, til å gjennomføre autonom operasjon? |
| 54 | I | Ja, nå er du rett på poenget vi startet med. Vi vil egentlig foretrekke en operatør, på grunn av sånne ting. Ellers kan det blir en utfordring å finne ut av hvem som skal ta aksjon om det ikke fungerer i en nødsituasjon. |
| 55 | E | Joda, vi kan gjerne snakke litt om alternative løsninger, ikke bare [operatør] sin foretrukne. Jeg vet ikke om du er kjent med argumentasjon og resonnement for hvordan Finland har gjort det hos seg? De har en litt annerledes løsning hvor de har en statlig eid MVNO som har helt ansvar for kjernenettet, og så leier de radionettet av Elisa. |
| 56 | I | Ja, og jeg tror det var den foretrukne modellen, har jeg mistanke om da vi i fjor gjorde et prosjekt sammen med de andre operatørene og det var vel også noen andre med på vurderingene. Jeg antar at dere har tilgang på rapporten hvor de går gjennom de ulike alternativene. En av de tingene de så på var å ha et dedikert kjernenett. Og det er som sagt teknisk sett fullt mulig å få til. Spørsmålet er å klare å være veldig tydelig på hvem som har ansvar. Og da snakker vi også om kanskje litt mer avanserte ting, som det med autonome BS. |

| | | |
|---|---|---|
| | | Plutselig må du ha kjernenettet lengre ut. Hvem har ansvaret for at det støttes, og at du får mer data og kanskje mer SW der ute. Hvem skal betale for det da, og hvem skal drifte det? Da begynner kanskje driftsmodellene å bli mer kompliserte. Igjen så er vår foretrukne løsning å ha en pakke liksom. |
| 57 | E | Hm. |
| 58 | I | [Fjernet] |
| 59 | E | Jo, nei, oppgaven min er jo på en måte litt å vurdere ulike ting. Så man må tenke både pros and cons. En stor con som man ofte kommer borti med sånne turnkey provider-løsninger er jo type vendor lock-in og sånne typer utfordringer. |
| 60 | I | Ja, og det er jeg helt enig i. Så er spørsmålet om den egentlig er mindre om du er locked in på to operatører. Hvis det da begynner å bli noen spesialtilpassede løsninger mellom de to, så er det jo locked likevel. Så man kan godt diskutere at man kan balansere volumet mellom de to hvis man får det til, men man er like gjerne locked inn på to, i stedet for å være locked in på en. Er det bedre eller ikke, det kan man diskutere. |
| 61 | E | Det virker som det er tanken i alle fall i Storbritannia der de har to har hovedproviders, Motorola og EE, som har ansvar for hver sin del, der virker det som at resonnementet er litt at når man har ulike mindre deler så er det lettere å bytte ut en og en del. |
| 62 | I | Hvis du bytter ut den og går over på en en-operatør-modell så er det nok lettere. Men da ender du opp i det argumentet du prøver å gå imot i første omgang. Men det er nok lettere å bytte ut en av de to og bare gå på en. Men om du bytter ut en av de to og drar inn en tredje, så tror jeg man har en full diskusjon på nytt igjen på hvordan ansvaret da skal være. Så det er ikke lock-in nødvendigvis på ... Jeg er enig i lock-in argumentet, bare for å få sagt det. Det eksisterer. Så jeg avviser ikke det, men jeg tror det er veldig viktig å se på det argumentet i lys av hvordan dette skal håndteres over tid. Den ene tingen er jo den første installasjonen man setter opp og å få det til å funke. Og så skal det driftes og det skal rapporteres på performance og det skal rapporteres på feil osv. Og det er nok komplisert når flere skal komme med sine bidrag, for å få en totaloversikt. Det andre som kan være utfordrende i en kombinasjon av flere er, at det kommer nye releaser, nye funksjoner som også må synkroniseres. Så hvis de skal leveres ut til en sluttkunde på en konsistent måte så må oppgraderingen synkroniseres. Og det betyr at disse to kommersielle aktørene som nettopp er i konkurranse på andre områder må sette seg ned og samordne en del planer, som man ikke vil. |
| 63 | E | Nei, jeg bare grubler litt. Men jeg tenker, du nevnte jo at det virker som det har vært en preferanse for denne statlig eide MVNOen på en måte. At det virker litt sånn at i Norden så lener man litt mot det. Hva tenker du at kan være fordelene ved det? Er det snakk om statlig autonomi og sikkerhet og sånne typer ting? |
| 64 | I | Ja, har du et dedikert, eget kjernenett så kan du selv styre over både tjenester, hvem som får tilgang. Du har full innsikt i hvem som er ansatt i politiet, SIM-kort, og du har også full innsikt og kontroll over terminaler f.eks. Så det har ingen av de andre to operatørene potensielt mulighet til å kunne trikse med. Dette er ett argument for å kunne ha et corenett som er dedikert til den kundebasen. Antar drift settes ut som for TETRA-nettet. Det er jo en eller annen som får en driftsoppgave her. Et dedikert corenett kan gi full innsikt i både brukerne og den tjenestekvaliteten og du kan selv definere opp om det er dashboard, og du kan styre grupperinger og nye tjenester som kommer inn osv. Du har nok større valgfrihet på det sånn sett. Og det er en modell som fungerer og har fungert. Vi kjører den samme modellen i dag i |

| | | |
|---|---|---|
| | | [operatør] f.eks., både i Danmark og i Sverige der vi har nettverksdeling på radiosida med en annen, med et eget corenett. Det er en modell som funker, og det er på grunn av at det er standardisert mellom radiodelen og corenett-delen at det funker. Men hvis du begynner å snakke om tema nummer to, der corenett og radiodelen kommer til å flyte litt sammen, så må nok den grenseoppgangen dras på en gang til. Men det kan gjøres, det er ikke umulig å gjøre. |
| 65 | E | Hva med å for eksempel benytte seg av flere mobilnett, er det noe å tenke på? Jeg vet jo at [operatør] vil jo gjerne dekke alle kravene, men tror du at det kan bedre robustheten i nettet og dekningsgraden i nettet, uten at det blir for mye utfordringer med interoperabilitet? Eller kommer interoperabilitetsutfordringene til å trumfe hele diskusjonen? |
| 66 | I | Vi har jo et foretrukket syn at det går hos en operatør. Man må gå inn på realiteter og se på hvor det er unik dekning egentlig. Og det er veldig få plasser der [annen operatør] har dekning og ikke [operatør] for eksempel. [Operatør] driver jo også med hosting, altså at [annen operatør] plasserer sine BS f.eks. på [operatør] bygg. Det betyr at hvis strømmen blir borte så faller begge BSene ned. Vi må prøve å realitetsorientere den diskusjonen, så vi ikke tror at hvis vi har 97% populasjonsdekning hos [operatør] og 99% hos [annen operatør], betyr det at du har nesten 100%. Det er ikke det i virkeligheten. Det er som regel 99%. |
| 67 | E | Ja, at de er mer avhengige av hverandre enn man kanskje får inntrykk av, sånn rent logisk. |
| 68 | I | Ja. Og nå ser vi også på transportnettløsninger og fiber, så er det gjerne den samme fiberen som brukes til flere ting. Så det er både strøm og forsåvidt dekning. Som sagt så funker det jo i dag, det funker jo med nasjonal roaming. Det er flere som har avtaler for det. Teknisk løsning funker der, så det er jo egentlig bare å finne ut av hvordan man eventuelt skal støtte de mer avanserte tingene, sånn som autonome BS - hvordan det skal spille inn - og hvordan man skal sørge for at hvis man har en tjenesteutvikling, noe mer avansert rundt gruppe, video, med sensorer osv., og hvordan det skal funke mellom operatører der det er mindre grad av standardisering og der det gjerne er egne apper eller sånt som kommer som senere trinn som avtalen også må støtte. Så det er eventuelt en ulempe, altså kompleksiteten. |
| 69 | E | Nei, det er spennende det. |
| 70 | L | I Nødnett har de sånne transportable basestasjoner plassert rundt om i landet som de flytter inn hvis de mister dekning. Er det tilsvarende i [operatør]? |
| 71 | I | Ja, cells on wheels. Så det finnes en del av det. Første cells on wheels hadde vi for 30 år siden. Det var i Lofoten under lofotfisket. |
| 72 | L | Ja, vi har ledd godt! |
| 73 | I | [Fjernet] |
| 74 | L | Okei. Er de distribuert over hele landet? |
| 75 | I | Ja, de står på en del plasser. Og det er en del av de som faktisk står i drift. Hvis du er i Oslo for eksempel og går nedfor Skøyen her, ser du en COW stående i drift. |
| 76 | L | Jøss. Hvorfor det? |
| 77 | I | Det er billigere enn å betale husleie og komme på taket. |

| | | |
|---|---|---|
| 78 | L | Er det sant? Jøss. Men opplever du at det, hm- |
| 79 | I | Litt av utfordringen med å ha reservemateriell er at man kan bli overrasket når man har bruk for det at utstyret faktisk ikke fungerer: For eksempel, det er ikke oppdatert med ny software, vognen er punktert, whatever. Du har alle slags sånne ting. Når den ikke blir brukt regelmessig er det fare for at det ikke funker når du først har bruk for det. |
| 80 | L | Jo, det er egentlig dit jeg vil. Og så med å flytte dem, jeg regner med at de står litt rundt om i landet som er litt preget av at Norge kan være litt værhardt til tider. Er det en problematikk? |
| 81 | I | Ja, man har i beredskap en del slike som kan kjøres ut og ha dekning ved behov. Det er også en utvikling; Det ene er de tradisjonelle eller gammeldagse tilhengerne, men det vi ser på nå er det eksempelet som vi nevnte før med å heller kunne bruke en drone eller andre løsninger som kanskje er litt mer fleksible og kjappere å få til. En mulighet er løsninger som HAPS, high altitude platform station. Altså, det er fly i ca. 30 000 meters høyde som sirkler og gir et definert et dekningsområde. Det er flere initiativ her. Ett av dem hadde demo i sør-Tyskland, i Bayern-området nå nettopp som viste at det her kunne de få til. Og det er jo en type løsning som man kan ty til ved behov. Ved utfall av bakkenettet eller om det er andre områder eller ting man vil dekke. Så det er jo flere løsninger på det, egentlig, enn å ha en bakkebasert BS. |
| 82 | L | Men i dag så har dere disse COW, det er det som brukes? |
| 83 | I | I dag har vi COW, ja, som står der. |
| 84 | L | Kan du fortelle meg hvor mange dere har? |
| 85 | I | Nei, det er en del av kritisk infrastruktur. Det er en del informasjon som vi ikke har lov til å fortelle om. |
| 86 | L | Det er greit, verdt et forsøk! Vi vet at vi beveger oss igjennom hele denne oppgaven veldig nærme det folk ikke får lov til å si. |
| 87 | E | En ting som jeg har vært litt interessert i når vi først snakker med en mobiloperatør som har litt erfaring med å være en mobiloperatør. Hvis staten skal gå inn og opprette sin egen MNO, som f.eks. i et MOCN-scenario, har du noen råd til staten, eller hva tenker du kan være utfordringene med å opprette en sånn type egen løsning og operere det selv? |
| 88 | I | Det første rådet er jo å vurdere om du egentlig ønsker å foretrekke det eller kunne du vært komfortabel med å bruke et av de eksisterende. Det er klart at hvis du må gjøre det, så ville jeg brukt anerkjente standarder som 3GPP. Men så bør man tenke gjennom, hva er egentlig formålet med det og hva er det man vil oppnå? Er det for å kunne styre sin egen brukerbase f.eks., så er det jo sikkerhetsargumentet egentlig. Hvis det er for å kunne sørge for at du hele tiden har siste tjenester og støtter alle apper osv., så er det det som bør bygges opp. Man bør tenke gjennom ikke bare det første steget, men også de neste stegene og rigge en organisasjon tilsvarende. Man må også sørge for at man får disse tingene inn i avtalen rundt de andre tingene, altså det som skal leveres fra de andre operatørene. Ellers så vil man potensielt kunne få en forhandling for enhver ting som skal oppgraderes, og det funker ikke. Du må tenke gjennom et par steg frem i tid. F.eks. dette med autonome BS, er det noe vi ønsker å ha, og i så fall tenke OK, hvordan får du det til. Og det ville jeg ha forhandlet fram prinsippene på tidlig, så man slipper å komme tilbake etterpå. Da tror jeg det blir et problem. |

| | | |
|---|---|---|
| 89 | I | Når jeg har sagt det. Hvis du er inne på hvordan man skal implementere et corenett med cloud og greier, så er det en del anbefalinger på teknisk side på hvordan det skal gjøres. Det finnes jo verktøy og løsninger for å gjøre det, og mye av det her er basert på open source. Jeg ville heller ha gått den løypa, i stedet for å utvikle noe spesialtilpasset. |
| 90 | E | Et spørsmål til er på utfordringer med å skulle dele opp core-nettet. At staten f.eks. har ansvar for noe, og en operatør har ansvar for en annen del av corenettet. Det er litt det de har gjort i England, at de har delt opp ansvarsområdene i kjernenettet. Jeg har bare funnet info om lower og upper core, så jeg lurer litt på hva slags funksjonalitet det egentlig er snakk om i denne SBAen. Sånn jeg har tenkt det er at lower core har UPF, SMF og AMF, det som har med den trafikk-funksjonaliteten å gjøre. Og så er upper core alt det andre. |
| 91 | I | Ja, jeg tror jeg ville tenkt det samme som et utgangspunkt. Det vi har sett, og jeg tror AT&T har noe sånt, er at UPFen eller gatewayen er en del av kundeløsningen. Det kommer spesielt om det er noen kunder - Nødnett eller andre - som har spesielle sikkerhetskrav, om du skal kryptere all brukertrafikken og må styre krypteringsnøkler selv. Det gjøres i gateway. Da må de kunne administrere gateway selv. Så det kan være en diskusjon, men det er kanskje litt sære anvendelser, litt mer på sikkerhetssiden enn Nødnett-siden. Utgangspunktet vårt er at man egentlig eksponerer det helt på toppen, over SBAen. Det er exposure-funksjoner (SCEF, NEF) for tredjepart-tilgang. |
| 92 | E | Nei, jeg bare tenker om det er noe mer jeg har behov for å spørre om. Og så vil jeg ikke spørre om noen sånne ting som er åpenbare, som om [operatør] tror de har kapasitet og evne til å levere på denne typen tjenester, for det tenker man er åpenbart sant. Men type det å kunne gi prioritet til Nødnett-trafikk i nettet og sånne type ting hvis det går på bekostning av kommersielle interesser f.eks., og at det må noen regulatoriske krav til for at man skal ha den påliteligheten som man har behov for i nødnettet. |
| 93 | I | Ja, jeg vet ikke om det trengs regulatoriske krav. Altså, for meg er det en kommersiell diskusjon egentlig på prioritering av trafikk. Men det som da er spørsmålet, dilemmaet i diskusjonen her, er jo vår erfaring. Staten har en tendens til å komme med krav uten å ha en betalingsvilje. Og den diskusjonen er ikke enkel å være i. Så hvis man ønsker å si at min trafikk skal være prioritert, men jeg ønsker ikke å betale noen ting, så har man en litt sær diskusjon. Så de må være villig til å gå inn på en sånn dialog tror jeg. Jeg tror også andre brukere typisk vil forstå det at det er ambulanse og brann osv. som skal ha prioritet. Og det som vi ser nå og som du sikkert har diskutert med politi og andre, er at mange av de går med to eller tre devicer. De har en TETRA og så har de en offentlig telefon, og de bruker like gjerne smartphonen sin som verktøy både for navigering, kommunikasjon og bildetaking. De sliter jo i dag med at hvis det skjer noe så er det så mange andre, publikum osv., som strømmer til og de kommer ikke gjennom på det. Det ønsker vi også å nettopp kunne styre, at det ikke blir publikum som tar over situasjonen, men at det gis til de som har bruk for det. Det er mekanismer for å få støttet det, og slicing er en mulighet, som du var inne på, enn det var i tidligere generasjoner. |
| 94 | E | Tenker man at man kan tilby en helt skreddersydd slice for Nødnett type trafikk, eller- |
| 95 | I | Ja. |
| 96 | E | Som har både litt sånne URLLC-karakteristikker og broadband-karakteristikker? |
| 97 | I | Ja. Det er litt forskjellige meninger om slice, litt i det vi snakket om tidligere. I min oppfatning så er slice egentlig en måte å isolere trafikk på. Om det er for Nødnett eller for IoT-anvendelser osv. Innafor en slice, mener jeg, kan du fortsatt ha en subslice. Så du kan godt |

| | | |
|---|---|---|
| | | ha en Nødnett-slice og en egen politi og brannvesen-subslice. Du kan ha flere subelementer der. Så selv brannvesenet har jo ulikt prioritetsbehov. Så noen er mer operative enn andre som er mer back office. Samme med politiet, og for så vidt ambulansen. Det er ikke alt som er nødrelatert i en sånn aksjon. |
| 98 | E | Det som er interessant er kanskje mulighet for mer interoperabilitet mellom nødetatene også. |
| 99 | I | Ja, og hvem som får lov til å snakke sammen og hvem som ikke får lov til å snakke sammen. Da er du litt tilbake på hele UDC og styringa og hvem som skal ha lov til å lytte inn osv. Hvis du har en autonom BS, hvordan får du den logikken og den informasjonen dit? Så du unngår at noen lytter på ting som de ikke skal ha, f.eks. |
| 100 | L | Har du noen tips og råd for oss nå som skal prøve å komme frem til konklusjoner på to forskjellige ting inn mot juni, har du noen tips til hvordan vi skal gå frem der? Jeg vet at du har veiledet mange før. |
| 101 | I | Med spørsmålene som er listet her er det ganske tydelig. Det er å være tydelig på problemstillinga. Jeg forstår at dere er i en samlingsfase av synspunkter, vurderer alternativer. Alle spørsmålene er jo veldig viktige i den dialogen der, med å få opsjoner på bordet og få pros and cons. Det høres rimelig fornuftig ut det her. Så er spørsmålet om man klarer å konkludere tydelig, der konklusjonene kan godt være scenarioavhengig. Det kommer jo litt an på hvilke faktiske krav som kommer rundt Nødnett, for eksempel. Hvor kortsiktig/langsiktig er det, og hva er man egentlig ute etter å oppnå. Jeg mener også det at gitt et sånt dilemma, er det mange som tyr til å legge ansvaret over på en instans og sørge for at det er turnkey. Så får heller sette premissene riktig på den måten. Også tror jeg det er veldig viktig at man forholder seg til internasjonale standarder så man slipper å holde på med noe Nødnett Norge-spesifikke ting f.eks. Det gjelder også autonome BS, at man følger den utviklinga der. Spesielt på det siste rundt 5G så ser vi at det er andre bransjer som plukker opp 5G, ikke bare de kommersielle mobiloperatørene og heller ikke bare Nødnett, men det finnes mange andre som nettopp ser anvendelser, i forbindelser med roboter eller andre autonome nett som man godt kan lære av. |
| 102 | L | Det er hyggelig å høre. Det er en berg- og dalbane, hehe. |
| 103 | E | Det er i alle fall spennende å gjøre noe som er veldig aktuelt og der det ikke finnes noe ordentlig godt fasitsvar. Vi får mulighet til å utforske litt. |
| 104 | I | Det som vi har sett som en aktør i dette generelt, er å kunne gjenbruke disse komponentene. Og så kan vi diskutere hva en komponent er. Men å kunne gjenbruke disse komponentene mellom de ulike use casene, om det er Nødnett eller kommersielt eller private nett, det er fundamentalt. Og for å kunne gjøre det så må man standardisere. Og da er man litt tilbake på dette med SBA og hvor det er man åpner opp. Hvor er det bransjen går hen. Skal du plutselig åpne opp på et nivå som ingen andre gjør, så sitter man med skreddersøm som blir utfordrende å videreutvikle. Og det er litt tilbake til det jeg prøvde å si tidligere, at enkelte ganger har vi en tendens til å tenke for kortsiktig. Hvis du skal opprette et nett til i dag eller i morgen, og ikke tenker på hvilke behov man har om fem år, da sliter man med et TETRA-nett som er 20 år gammelt i dag og ikke klarer å holde tritt med utviklinga ellers på de andre områdene. Da er det veldig viktig å kunne holde tritt med den internasjonale standardiseringa og det volumet som er rundt det. Men nå farger jeg dere med mine perspektiver. |
| 105 | L | Vi snakker med flere operatører, så det er ikke noe problem. Det er vi forberedt på. |

| | | |
|---|---|---|
| 106 | I | Okay, det er bra. Da får du balansert inntrykket. |
| 107 | I | Snakker dere med direktoratet også, og andre der? |
| 108 | E | Ja. |
| 109 | L | Har du noen spørsmål til oss, eller noe du synes vi burde ha spurt om? |
| 110 | I | Nå er spørsmålene formulert sånn at det vanskelig å si at det ikke spørres om det, selv om det ikke står der. Men sikkerhetsproblemstillingen er en fundamental problemstilling. Det andre er, som dere kanskje er litt inne på, er de reelle brukerbehovene fra brukerne i Nødnett, altså politi og ambulanse. Og operasjon av tale, video og whatever. Hva er det man ser for seg i utviklinga der. Det kommer mange devicer, om det er droner eller IoT-devicer eller whatever. Det kommer behov som man ønsker å dra nytte av. Jeg ville supplert med den. Men det kan jo leses inn i spørsmålene, så det er nok ikke noe som er uteglemt. |
| 111 | L | Nei, vi driver og intervjuer folk fra de forskjellige brukerorganisasjonene. Folk er generelt ganske tilfreds, så det er vanskelig å finne ut av hva som faktisk kommer til å bli behov om 5-10 år. |
| 112 | I | Er de tilfreds med TETRA, er det det du sier? |
| 113 | E | Noen av dem er i alle fall det. Et av kravene til NGN er i alle fall at det skal være minst like bra som TETRA, den talefunksjonaliteten og sånt. |
| 114 | I | Åja, okay. Men er de fornøyd med TETRA, det er jeg nysgjerrig på. |
| 115 | E | Noen av de er fornøyd med TETRA. Og så er det jo noe funksjonalitet som mangler mtp. data og sånt, og så er det jo en del use cases som ikke har blitt en del av hverdagen enda, men som kanskje blir uunnværlig i fremtiden. |
| 116 | L | Jeg må nesten spørre, hva er det du reagerer mest på når vi sier dette? |
| 117 | I | Jeg så for meg at, altså, TETRA er jo egentlig sånn som 2G eller GSM om du vil. Det er på det stadiet. Vi hadde jo en vurdering da vi satte 2G i drift med hvordan dette kan sammenlignes med håndtering av Nødnett-trafikk og dimensjonering av TETRA. Og det er jo en dårlig utnyttelse av kapasitet, men greit nok. Slik av situasjonen på det tidspunktet. Det jeg stusser på er om ikke man ser behov for mer data og interaktivitet rundt data og flere ikke-person sesjoner, som droner og roboter. Hvordan TETRA burde ha fungert med slike muligheter. Hvis de er fornøyde i lys av denne utviklingen og mulighetene nødetatene kunne hatt, er jeg litt undrende. |
| 118 | L | Nei, men det er interessant, for vi har vært mye rettet på person-til-person-kommunikasjon. Så det er et godt tips videre å se på mer maskin til maskin. |
| 119 | I | Ja, jeg vil tro spesielt brann og kanskje politi bør se på robot og andre ring. Det har jo med risikoen til personell å gjøre. |
| 120 | L | Jeg synes vi har fått mye gode innspill nå, jeg! |
| 121 | I | Det er bra. Det er følelsen som teller, er det ikke det? |

| | | |
|---|---|---|
| 122 | I | Yes. Jeg kan se om jeg finner det vi snakket om med det autonome firmaet i USA. Et NATO-prosjekt de holdt på med. |
| 123 | E | Så nå kommer vi til å skrive transkript av det her, og så sender vi det over til deg så du får se hva du synes, om det anonymisert godt nok og sånt. |
| 124 | L | Tusen takk skal du ha! |
| 125 | I | Ha en god dag! |

# Appendix F
# Mobile Network Operator B

This interview is conducted with a representative of one of the three Norwegian mobile network operators. The favored deployment model of this interview subject is that of a state-owned MVNO making use of all three available radio networks. As such, considerations in regard to this model are made, in addition to general considerations regarding 5G, NGN, and public safety communications at large.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, så spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Jada, det er helt okay. |
| 3 | E | Supert, så kan jeg begynne med å presentere min egen oppgave. Jeg ser på utfordringer rundt samarbeid med kommersielle aktører om utførelsen av neste generasjons Nødnett. Nå skal man jo ikke ha noe eget radionett, og så er spørsmålet om hvordan man skal gjøre det i kjernenettet med staten og kommersielle aktører. |
| 4 | I | Forutsetningen din da er at man bruker de kommersielle nettene som finnes til å realisere neste generasjons Nødnett. |
| 5 | E | Ja, radionettene. |
| 6 | L | Jeg ser på Nødnett i 5G standalone, og så ser jeg på tilfellet der én eller flere basestasjoner mister tilkoblingen til kjernenettet og må virke autonomt som et lite lokalt nettverk. Problemstillinger både operasjonelt og teknisk rundt det. Med antagelsen om at Nødnett kjører i kommersielle radionett. |
| 7 | E | Som jeg har skjønt det på deg, så er det kjernenettet som er din hovedspesialitet. |
| 8 | I | Det stemmer. Og så har vi egne ansvarlige for radiobasestasjoner osv. som da har gode og fundamenterte meninger om hvordan et radionett bør se for Nødnett. Så vi har vært med noen runder med besvarelser til DSB der vi har gitt et innspill som er litt annerledes enn hva de andre operatørene har gitt, men de dokumentene er unntatt offentligheten så de kan jeg dessverre ikke oversende, men jeg kan snakke om innholdet. Det er en stund siden vi gikk gjennom de besvarelsene, så det er ikke alt jeg har like friskt i minnet, men gjennom diskusjon kommer det forhåpentligvis tilbake til meg. |
| 9 | E | Jeg er litt interessert i hva du mener med at dere svarer på en litt annen måte enn de andre operatørene i forbindelse med disse tingene. Handler det litt om hvordan infrastrukturen ser ut i dag? |
| 10 | I | Ja, og så har det også med maktforholdet mellom operatørene å gjøre. [Operatør] er the incumbent, det er de store. I europeisk målestokk så er det ikke mange andre land i Europa annet enn Romania som har samme struktur som Norge, der the incumbent har beholdt markedsmakten sin. Så har det vært snakk om forskjellige modeller for hvordan Nødnett skal realiseres i kommersielt mobilnett, og da er det slik at hvis en av modellene velges der én operatør hoster alle tjenestene, så er det naturlig at det faller på den som har sterkest markedsmakt. Vår modell har beskrevet en løsning der man sikrer robustheten og diversiteten gjennom å bruke alle tre radionettene samtidig, og får DSB til å ha en MVNO-funksjon bak radionettene. Slik at man får styrken av tre, og så får man interoperabiliteten bak for én. Da slipper du å tenke på type interconnect. Vi får feature parity gap og kompabilitetsgap ved at det er tre forskjellige leverandører som hoster disse nødnettstjenestene og skal sende interconnect og samtrafikk mellom hverandre. Det kan være en utfordring. I tillegg så vil det å ha en MVNO-modell bak sikre konfidensialitet ved at den trafikken som går på de tre mobilnettene, i radionettet, er kryptert og at innholdet dermed ikke er synlig for de som driver med operations innenfor operatørene. Selv mobilitet vil da være usynlig fordi man da bruker egne komponenter, hvis man tar mobilitetsfunksjonen også inn i MVNOen, altså AMF-funksjonen. I den helt rake motsetningen der man sier at the winner takes it all, sånn som modellen til AT&T i USA, så vil |

| | | |
|---|---|---|
| | | du ikke kunne sikre den samme integriteten og sikkerheten. For da sitter operatøren som hoster dette og ser alt av trafikk. |
| 11 | E | Så det blir en litt annen trust-modell på en måte? |
| 12 | I | Ja, det gjør det. |
| 13 | E | Det er interessant å høre en litt annen approach. At de ulike mobiloperatørene har ulike syn på hvordan ting burde være. At ikke alle ønsker å være den ene provideren, men at man på grunn av ulike maktforhold, som du sier, har ulike forventninger til hvordan ting - |
| 14 | I | Og så er det også det, at når det gjelder mobilnett og Nødnett, så blir det midler fra staten rundt forsterkning av nett i grisgrendte strøk. Det er midler som er konkurransevridende hvis de tildeles én. Fordi da har man en helt annen business case på å bygge ut dekning der det ellers ikke er lønnsomt. Hvis man fordeler det på tre nett, så er det ingen konkurransevridning der, og Nødnettet kan utnytte den kapasiteten fritt imellom. Og så har vi også tenkt på en modell der Nødnett vil få en egen PLMN ID, som er en operatørkode. 242 er Norge, 01 er Telenor, 02 er Telia, 14 er Ice osv. Så de kunne hatt 242-99, som hver operatør hadde definert som en unik ID i sitt eget nett. Da ville mobilen oppfattet alle basestasjoner som eget hjemmenett, og da bare tatt det sterkeste nettet den hadde funnet på det tidspunktet. Utfordringene med dette er mobilitet. Det vil si at du klarer å hande over når du mister dekning, så vil ikke Telia ha mobilitet til Telenor, for det vil du ikke kunne normalt gjøre uansett, eller andre veien, eller til Ice. Dermed vil du få brudd. Men, så lenge du har ankret deg opp på et mobilnett innenfor en slik modell, så vil du holde deg på den operatørens mobilnett så lenge du er i active mode/connected mode. I det øyeblikket du går idle, altså at du ikke har aktiv datakommunikasjon eller talekommunikasjon, så ville du gjort idle mode reselection. Da ville telefonen valgt vilkårlig ut fra de nærliggende basestasjonene avhengig av hvem som har sterkest signal. På den måten kunne du fått tre ganger basestasjonskapasiteten og dekningen og diversiteten, istedenfor å velge én av disse sine. Du får noen drawbacks på det, men vi tror at oppsiden i robusthet og diversitet vil veie opp for de drawbacksene. Det vil ligge litt mer engineering bak for å få det til, men vi mener at det absolutt er oppnåelig. Og det ville sikre mest mulig robusthet til lavest mulig kost for nasjonen Norge. Det er brukt mange nok milliarder på det Nødnettet som er der allerede uten at det kan konkurrere med kommersielle aktører. |
| 15 | E | Man sikrer seg kanskje mer mot typ vendor lock-in-effekter og sånt, enn man gjør hvis man skal velge én? |
| 16 | I | Ja, det tror jeg nok. Men i radionettet så bør man kanskje også ha diversitet i leverandør, for én bug kan slå ut alle nett. Har du nett fra forskjellige leverandører, så vil ikke de trigge de samme feilene, og da vil du ha større robusthet. Når det er sagt, så tror vi fremdeles at Nødnett bør være en egen MVNO bak de kommersielle operatørene. Og ha sin egen driftsorganisasjon for å sikre konfidensialitet og integritet, og oppetid og interoperabilitet. Ellers så kan man løse det med at one winner takes it all. Da er det ingen interoperabilitets-issues, men du har sårbarhets-issues. I forhold til den operatørens oppetid, men også den operatørens konfidensialitet. Da er det eksterne kommersielle aktører som kan ha innsyn i trafikk og mobilitet til verneverdige funksjoner, om du vil. Vi som operatører bruker selvfølgelig mye utenlandsk arbeidskraft, det er ikke til å komme unna. Sikkerhetsklareringer osv. er en tøff oppgave å få til ofte. Det kunne vært et mindre team som kunne gjort den jobben og hatt en større grad av konfidensialitet i en MVNO-setting. Og da, hvis man bare bruker operatørene som bærere, så ville man da produsere tjenestene selv på topp. Så har man sårbarhet, for da er du single vendor på topp som MVNO, og du kan få nedetid i alle nettene om du roter det til selv. Når du sitter som toppen av hierarkiet, og du får nedetid |

| | | |
|---|---|---|
| | | pga. en oppgradering, da har du ikke to andre nett som er oppe. Men hvis operatørene tar ansvar for push-to-talk-funksjoner osv. så vil de to andre fungere selv om én er nede. Så det er pros and cons hele veien her. |
| 17 | E | Da tenker du at DSB da oppretter en egen MVNO og så organiserer alt med dedikert infrastruktur og sånt selv, og drifter det selv? |
| 18 | I | Ja, det er det vi tenker. Det er en RAN sharing-funksjon, der Ice, Telenor og Telia bare er RAN providers, mens all verdiøkning foregår på innsiden, bak oss. Der DSB sitter som en aggregator og terminerer radiofunksjonene inn. Ellers så er det en hybridmodell, der du sier at AMF- eller MME-funksjonene, det tar operatørene, mens DSB tar applikasjonene. Men da gir du fra deg noe rundt konfidensialitet. Vi, operatørene, vil ikke klare å se innholdet i meldinger og taleanrop osv., men vi vil se mobiliteten. Vi vil se at bruker X var på posisjon A, B og C. |
| 19 | L | Jeg ser på tilfellet der basestasjoner mister tilkoblingen til kjernenettet, og jeg har gjort en antagelse i min oppgave om at det kun er én operatør som har radionettet, for å gjøre det enkelt for meg selv. Men i det tilfellet du ser, der DSB er en MVNO, så tenker jeg at du sikkert har noen tanker rundt å ha funksjonalitet i edge. Jeg vil jo egentlig ha hele push-to-talk-funksjonaliteten i edge, i tilfelle den må fungere autonomt. Det vil vel bli en massiv utfordring med tanke på sensitiv informasjon. |
| 20 | I | Ja, det er nok enda vanskeligere når du skal ha MEC, mobile edge core, og at den skal være fullt autonom. Å da også klare å ha RAN sharing mellom alle operatørene, det blir mye vanskeligere. Jeg kan tenke meg at disse MECene, edge corene, de vil sitte i små datasentre som vi også kombinerer med cloud RAN. Cloud RAN er når vi går fra å ha distribuerte basestasjoner med hver sin logikk, til å ha sentraliserte basestasjoner. Si at Haugesund, for eksempel, er et cloud RAN som sitter med et titalls basestasjoner innenfor sentrum. Der de bare har radioheads ute på enheten, og så har de all compute inne i cloud RAN-datasenteret. Det kan også fort være et mobile edge senter, der du har mest mulig autonomitet. Jeg tror det mest utfordrende for full autonomi er å flytte SDM, subscriber data manager, som da er HLR/HSS-funksjonen, helt ut. Det er funksjoner som typisk sentraliseres. Det skillet man ofte gjør er at man flytter ut user plane-funksjonene, der brukerdataen går, som er mye og massivt og påfører latency hvis du skal rute hjem og tilbake, og at man da kan gjøre en knappenålssving på user-planet lokalt. Kontrollplanet er ikke fullt så tidskritisk, fordi det gjør man under oppkobling og det gjør man hjemme. Så veldig mye av den subscriber data management-biten gjør man ofte sentralt, og de nodene er kanskje ikke designet enda for å være autonome. Når jeg tenker på autonomi osv. da, så er det vel kanskje for Forsvaret og politi, og da er kanskje de kravene rundt SDM-funksjonen vesentlig mindre, og da kan man kanskje få det til. Men jeg er helt enig med deg i at du bør fjerne den multippel RAN-biten fra dette for å gjøre det håndterbart. |
| 21 | E | I forlengelsen av det, hvem er det som kommer til å ha ansvaret i edgen i et sånt scenario. Er det DSB, som har ansvaret for kjernen, som også må være ute i edgen eller er det noe mobiloperatørene kan ta ansvar for? |
| 22 | I | Hmm, veldig godt spørsmål. Jeg tror ikke det er helt klart for operatørene heller hvordan edge-strategien skal være til enhver tid. Hvor mange datasentere skal vi ha? Jeg deler det opp i tre nivåer: Du har kjernenett-sitene som har all funksjonalitet. Ice har to og skal bygge tre, Telenor har fire og Telia har tre. Der skjer alt. De kan være helt autonome og tar over for hverandre med utfall på én. Så har du regionale datasentere, som vi må se for oss i 5G for å få ned latency. Der flytter du for eksempel bare user plane for pakkedata, fordi det er der volumet går i starten, mens user plane for tale kan flyttes helt hjem. For det menneskelige |

| | | |
|---|---|---|
| | | øret har du 200ms å forholde deg til før du merker en forsinkelse, mens på pakkedata har du single digit latency på millisekunder. Så på regionale datasenter kan det for eksempel bare være user plane, eller så kan du ha user plane for voice også, og så kan du ha all control plane i core. Og så har du edge-sitene som kanskje bare tar en liten funksjon av det. Men å legge opp den kabalen, det tror jeg ikke noen av operatørene, ihvertfall ikke oss, har gjort. Når det er sagt, så kommer aspektet med å få MVNOer inn i disse datasenterne. Der kan du se på DSB som en av MVNOene, for det kan være flere. Det kan være kommersielle aktører der ute også. Det kan være private 5G nett for bedrifter som for eksempel en fiskeindustri som har mærer utenfor rekkevidde av wifi fra land. Da kan det være greit å bruke en frekvens som ligger innenfor 5G som er privat, som ikke forstyrres, fordi den er licensed til operatøren og som når lenger ut. Da kan de ha en hensikt av å hoste lokalt på et edge-senter, på samme måte som DSB. Hvordan og hvem som drifter disse sitene, det henger litt på hvordan man legger opp orkestreringen. Orkestrering er også ganske fersk teknologi for operatørene. Da kan operasjonen styres som en managed service av operatøren for DSB, eller man kan legge opp til orkestreringsløsninger som gjør at DSB selv får tak i orkestreringsverktøyene. At du har en hierarkisk brukerautorisering på orkestreringsløsningen. Men det er områder som ikke er utforsket av oss enda. Eller så kan DSB gå hele veien ut og sette opp sine egne lokale datasentere for den slags skyld, og terminere radioen vår lokalt. |
| 23 | E | Du nevnte at det er ulike krav til ulike typer kommunikasjon, så går det an å tenke at man har en enklere type tjenestetilbydelse i et scenario der man er avhengig av å bruke edgen? |
| 24 | I | Ja, enig i det. Og så er det, når man tilbyr edge, pakkedata primært. Da kan man tilby voice som en over-the-top-applikasjon. 4G tale, voice-over-wifi og VoLTE er ganske komplekse verdikjeder, så det kan godt hende at det er enklere å realisere push-to-talk-tale lokalt med en over-the-top-applikasjon som ikke tilbyr den samme kompleksiteten som kommersielle tjenester må gjøre i forhold til alle mulige forhandlinger om codecer, interoperabilitet, internasjonal roaming osv. Man kan fjerne det, fordi man har en mye mindre brukergruppe med mye mer spesifikke og definerbare behov. Og da kan du forenkle autonomiteten der ute. Men hvis man skal bruke de kommersielle tjenestene som VoLTE og video over LTE osv., så krever det den fulle 3GPP-infrastrukturen. Og da vil jeg anta at SDMen, altså HLR- og HSS-funksjonen er det vanskeligste å flytte ut for å få det autonomt. Nettopp fordi de ikke er designet for det. De er designet for å være store massive databaser som går på big iron inne i kjernenettsenter på to eller tre lokasjoner, ikke på et femti-talls lokasjoner. |
| 25 | E | Hvis vi går litt på det med den hypotetiske MVNOen som DSB skal opprette. Hva tenker du kanskje kan være utfordringene for DSB, og hva innebærer det å være en MVNO i et 5G økosystem? |
| 26 | I | Det er et godt spørsmål. DSB slipper den vanskeligste utfordringen med å starte opp en mobiloperasjon, og det er å få tak i internasjonale roaming-avtaler. Så lenge man ikke tenker å roame internasjonalt med disse abonnementene. I motsetning til internett som er en hierarkisk modell med DNS, som propagerer endringer automatisk, så er ikke mobiloperatørverden slik. Det er bilaterale en-til-en-avtaler. Hver av de tre til fem hundre operatørene som du har interesse av å snakke med, de må du ha en egen avtale med, og så må operatørene bilateralt teste tjenestene. Så når det da kommer en liten aktør inn og skal ha avtale med en stor aktør som har plenty med avtaler allerede og er complacent med at de ikke trenger flere, så er det et veldig langt lerret å få til interconnect. Så hvis DSB har ambisjoner om å lage SIM-kort som vil være på de vanlige bring-your-own-devices-terminalene, altså kundenes egne telefoner, typisk en Apple eller Samsung per tidspunkt. Hvis det er policyen, at du kun skal ha et SIM som skal være et vanlig abonnement i tillegg til et nødabonnement, da må roaming tilbys og da er det en utfordring. Da bør man heller |

| | | |
|---|---|---|
| | | bruke de eksisterende operatørenes avtaler enn å begynne å gå inn på den lange tunge jobben med å tilby roaming selv. Men jeg tror at hvis det blir et krav, med BYOD osv., så løser man heller det med såkalt eSIM, som er da logiske SIM istedenfor fysiske SIM. De aller fleste high-end terminaler på det tidspunktet klarer fint å håndtere flere forskjellige SIM-kort og flere forskjellige roller. Så da har du et eSIM for nød, og et vanlig for vanlig kommunikasjon. Ellers, om det er noen andre utfordringer med å etablere MVNO, så som en oppstart så har jo DSB allerede en driftserfaring med sitt nåværende TETRA-nett. De har en operasjon, de har prosedyrer, og de har operasjonelt personell som er vant til å kjøre operasjon. Jeg tror ikke at det blir en veldig tøff oppgave for dem å komme opp på et godt nivå. Utfordringen for en operatør er alltid robusthet. Oppetid i forbindelse med oppgraderinger, nattjobber, å forstå nye endringer osv. Men jeg tror at DSB er en profesjonell organisasjon som klarer å takle det fint. |
| 27 | E | Med tanke på det du sier om robusthet og det vi tidligere var litt inne på, at hvis man velger én operatør så kan den operatøren få konkurransefremmende tilskudd fra staten for å tilfredsstille kravene til robusthet i Nødnett. Tenker man da at alle operatørene skal få det, hvis alle operatørenes nett blir brukt, eller tenker man at når man har alle operatørenes nett så blir dekningsgraden og robustheten stor nok i seg selv? |
| 28 | I | Da tenker man at hvis det skulle trengs konsesjoner for å dekke indre vidda et eller annet sted, så vil den tildeles til én operatør. Og da vil Nødnett få tilgang til det dekningsområdet. Neste gang, når du skal ta indre vidde nummer to, så vil operatør Y få det og så operatør Z få det, og sånn vil du fordele det. Eller så kan du lage en konsentrasjon som sier at alle basestasjoner som er bygget på DSB sitt budsjett, det skal alle operatører få tilgang til gjennom noe som heter MOCN, som er multiple operator core network-integrering. Det vil si at da vil de basestasjonene signalisere i luften at de er både Ice, Telenor og Telia, og eventuelt Nødnett da hvis Nødnett velger sin egen operatørkode. Nå tror jeg ikke det går den veien personlig. Jeg tror at Nødnett kommer til å velge operatørkode som tilhører en av operatørene. Men de har muligheten til å definere sin egen, og pålegge de forskjellige operatørene å stråle ut Nødnetts operatørkode, som kunne vært 242-99, for eksempel. |
| 29 | E | Hvis vi ser litt på Finland for eksempel, som har en tilnærmet lik modell der staten har sin egen MVNO. De har valgt å gå for ett mobilnett, ihvertfall fra starten av, og så har jeg hørt at de eventuelt vil vurdere å benytte flere mobilnett etter hvert som man begynner å få orden på de interoperabilitetsutfordringene. Tenker du at det kunne vært en logisk utvikling i Norge også, at man begynner med én og så heller tar flere etter hvert? |
| 30 | I | Altså, forstår jeg riktig nå, for jeg har ikke studert Finland, at Finland bygger sin egen MVNO i tillegg til at de bruker én operatør? |
| 31 | E | Ja, de har sin egen MVNO, Erillisverkot, og så bruker de Elisa sitt radionett. |
| 32 | I | Det kan være en grei start det. Så lenge de har sin egen MVNO står de sterkere enn om de bruker funksjonaliteten til den MNOen der. Og det kan man gjøre på mange måter. Man kan spinne opp nye instanser hos den MNOen som gjør at man blir en MVNO, men da er man prisgitt den MNOen sin operasjon. For da er det ofte den MNOen sitt personell som også opererer MVNOen. Bygger du opp et helt separat datasenter utenfor og så interconnecter til MNOen, så står de friere. Og da går det fint å få inn de andre radioaksessnettene etterpå. Det er flere mekanismer å gjøre det på. Den måten som vi foreslo er å hele tiden søke etter det beste nettet. Hvem som har den sterkeste radiobasestasjonen. Uavhengig av om det er Ice, Telenor eller Telia. Men en mer tradisjonell måte å gjøre det på er en SIM-kortstyring der du sier at Telenor er preferert, og så etter det er det Telia og så er det Ice. Da vil telefonen være i Telenor-nettet så lenge den finner Telenor-nett. Men, i det øyeblikket |

| | | |
|---|---|---|
| | | Telenor mister dekning, så vil den søke etter Telia og Ice som en erstatning, og det går fint. Gjør du det på den måten så bruker du 3GPP sine egne mekanismer for nettverksvalg. Det vil være som om du dro til Sverige, der du har tilgang til alle operatørenes nett, men der du - Hvis du har Telenor-abonnement, så vil Telenor bestemme hvilken operatør du skal velge først, fordi Telenor har sin egen operasjon i Sverige og vil ønske å beholde trafikken internt. |
| 33 | E | Du nevnte det litt tidligere, men det med at operatørene kanskje tar ansvar for noe kjernefunksjonaliteten, som AMFen eller SMFen eller noe sånt: Tenker du at det finnes modeller her der det gir mening å dele opp kjernenettfunksjonaliteten og fordele ansvarsområdene. For eksempel sånn de har gjort i England, der jeg tror at mobiloperatøren EE har ansvar for den nederste delen av coren med AMFen, SMFen og UPFen. |
| 34 | I | Det går helt fint, men du mister integritet på det. Fordi da gir du fra deg en funksjon der du lekker opplysninger. Hvis det ikke er sensitivt og ikke betyr noe, så er det en fin måte å gjøre det på. |
| 35 | E | Tenker du at det er en fordel å styre showet litt selv når man beveger seg fremover, for eksempel når man da skal - Nå går jeg utifra at neste generasjons Nødnett først kommer til å bli etablert i LTE, og så at man etter hvert oppgraderer til 5G etter hvert som standalone begynner å bli ferdig. Tenker du at det er enklere å få til hvis man har kontroll over tingenes tilstand selv, som en egen MVNO? |
| 36 | I | Det er nok lettere å få det til hvis man bruker mest mulig fra operatørens kjernenett. |
| 37 | E | For da henger man på en måte på når de oppgraderer sin egen? |
| 38 | I | Ja og nei. Jeg skal kanskje moderere meg. Hvis man får til en ordentlig MOCN-modell så er man helt uavhengig av operatøren. Og hvis man begynner med LTE og går over til SA uten det NSA-steget, så er du vel bare avhengig av at operatørene begynner å rulle ut 5G gNodeBene for å kunne sette i drift ditt eget 5G SA-nettverk. Jeg ser ikke noen store drawbacks med noen av modellene. Om du har AMF og SMF lokalt eller om du bruker operatøren sine. |
| 39 | E | Kanskje vi kan snakke litt om slicing. Det er på en måte et konsept som man kommer litt innom når man begynner å snakke om RAN sharing, og ihvertfall hvis det skal være et kommersielt kjernenett. Da må man kunne isolere den Nødnett-trafikken fra den kommersielle trafikken. Jeg vet ikke om du har noen tanker om det? |
| 40 | I | Slicing får du på 4G også, men det er ikke så mange som har implementert det. Det er en teknologi som er egnet for å kunne prioritere trafikk, skjerme trafikk, men også rute trafikk kanskje i sikrere datasentre, der du kan ha datasentre nede i fjellhaller istedenfor i offentlige bygninger, for eksempel. Så det tenker jeg er en naturlig utvikling av Nødnett hos kommersielle operatører. Jeg ser ikke noen større utfordringer rundt slicing heller. |
| 41 | E | Ikke noen ekstraordinære utfordringer med å få det til sånn rent praktisk? |
| 42 | I | Neh. Håndsettene kjenner vi ikke så godt til enda, men de støtter vel åtte slicer. Og så lenge man har nok slicer med de tankene som Nødnett har rundt dette, så skal det ikke være større utfordringer tror jeg. Nå vet jeg ikke hvordan slicing skal funke mellom operatører, hvis det skulle være en RAN-modell der du brukte alle tre nettverkene. Det kunne vært en utfordring kanskje, det har jeg ikke sett på. |
| 43 | E | Ja, og litt det med den logiske isolasjonen som slicing og lignende teknologier tilbyr. Vi har |

| | | |
|---|---|---|
| | | vært innom sikkerhet og integritet og sånt, så om det vil være tilstrekkelig å ha på delt infrastruktur - Om det vil være tilstrekkelig isolasjon, eller om man også burde ha egen infrastruktur i datasenterne. Egne racks. |
| 44 | I | Slicingen kan sende deg til et eget kjernenett som du kan sikre på eget vis. Jeg tror slicingen vil gi deg den robustheten som Nødnett etterspør. |
| 45 | L | Jeg synes dette var veldig oppklarende! |
| 46 | E | Ja, jeg får masse informasjon. Det er spennende å høre om den litt mer komplekse modellen og ikke bare "vi vil tilby en pakkeløsning" og så være ferdig med det. Det blir på en måte veldig enkelt, men så får man jo noen drawbacks med det og. |
| 47 | I | Ja, det gjør man. Og samtidig så tror vi at man får den største robustheten og beste dekningen [med vår løsning]. Men det er nok den løsningen som også står lengst i fra en standardimplementering. Jeg tror det hadde vært det beste for nasjonen Norge, men jeg tror ikke det er den løsningen som blir valgt. |
| 48 | E | Fordi det blir for mye kompleksitet? |
| 49 | I | Ja, og fordi Telenor står sterkt i den offentlige forvaltningen, og de har minst å vinne på en slik løsning. De vil tenke på den inntjeningen de vil kunne få ved å ha mest mulig trafikk selv. |
| 50 | L | Det er et spennende og sammensatt problem det her. |
| 51 | E | Ja, jeg prøver på en måte å forholde meg til de tekniske utfordringene og scope litt ut det som går på det økonomiske og politiske. Men det er ingen tvil om at det også er veldig viktige aspekter her. |
| 52 | I | Mainstreamløsningen er å legge alt hos én. Det vil ha den raskeste utrullingen, men med den laveste robustheten og diversiteten. Det er mainstreamløsningen, og det er vel derfor USA er oppe såpass raskt med den løsningen de har. Skal du tenke robusthet og diversitet og litt nytt, og ikke nødvendigvis bare ta den enkle veien, så vil man utforske de idéene i forhold til at nettet skal ha minst mulig svakheter og sårbarheter til lavest mulig investering. |
| 53 | E | Nå tenker jeg litt høyt, men sånn hypotetisk i Norge: Hvis vi ser på sånn de har gjort det i USA at AT&T har den offisielle nødnettstjenesten, men så finnes det også andre, for eksempel Verizon, som tilbyr egne nødnettsløsninger? Tenker du at det er noe dere kunne gjort i Norge hvis en annen operatør blir valgt som eneste operatør? |
| 54 | I | Haha, at vi er på den lokale brannstasjonen? Nei, de har jo en kommersialisering som vil bære seg i Norge. Jeg tror ikke vi er store nok til at Hallingdal brannvesen har store nok finansielle muskler til å kjøpe opp sine egne løsninger. USA er jo et kontinent i seg selv, med stater som små land, og da blir det litt annerledes. |
| 55 | L | For å spinne over på noe litt annet. Har dere flyttbare basestasjoner rundt omkring? |
| 56 | I | Ja, vi har noen. |
| 57 | L | Brukes de? |
| 58 | I | Da spør du feil person. Vi har et par stykker, og de brukes i forbindelse med festivaler og den type ting. De kunne selvfølgelig bli brukt ved brann i Årdal og militærøvelser osv., men vi er |

| | | |
|---|---|---|
| | | nok ikke de som har flest i den parken der. |
| 59 | L | Vet du om de brukes til å bygge opp igjen dekning hvis dekning faller ut? |
| 60 | I | Ikke hos oss. Det er klart, dekning faller ut i ny og ne, men vi har bygd ut vårt radionett robust, så hvis vi mister noe så mister vi sjelden lite om gangen. Hvis vi mister et område så er det fordi en av våre tre transportører har sentrale brudd inne, selv om det er redundans i deres nett også. Ellers har vi lag 3-nett til hver enkelt basestasjon. Jeg har jobbet hos andre mobiloperatører også, og der hadde vi lag 2-ringer. Da forsvant hele områder hvis du mistet én node i en ring. Så det er ikke så ofte vi har utfall i større områder, så vi har egentlig ikke hatt behov for å dekke det opp på den måten. Da hadde kanskje ikke en enkelt basestasjon vært tilstrekkelig heller. |
| 61 | L | Nei, det er liksom virkelig ytterste edge case av redundans jeg ser på i oppgaven. |
| 62 | I | Men i forbindelse med en eller annen katastrofe så kunne vi sikkert fått til noe sånt. Hvis Årdal brant ned igjen, eller slikt. |
| 63 | E | Jeg bare spør jeg: Har dere noen timeline eller noe sånt for hvordan utviklingen kommer til å bli videre nå med kjernenettet og sånt. Kommer man for eksempel til å få en dual core-type greie der man har NSA på den siden og så bygger man sakte opp SA på den andre siden, eller noe sånt? Vet du sånn ca. når ting skjer? |
| 64 | I | Ja, vi har et NSA-nettverk. Vi har ikke fryktelig mange basestasjoner på det, men kabalen legges og det er mange variabler på NSA vs SA i forhold til kapasitet, håndsettstørrelse, noe som heter dynamic spectrum sharing, band aggregation osv. som er pros and cons hele veien. Det er jo SA-nettet som til syvende og sist blir det gjeldene, men hvor mye NSA spiller inn i mellomtiden det vet jeg ikke. Hvordan komboen blir er et godt spørsmål for oss. Jeg sitter i diskusjonen, men vi legger strategien og så er det alltid sånn at det er en dynamikk i det. Så den strategien vi legger i år ikke er den samme strategien vi følger til neste år. Vi må styre etter endringer. |
| 65 | E | Men har dere noen ca. time frame på når man begynner å se SA in action? Eller er det for mye usikkerhet? |
| 66 | I | Det er lansert i T-mobile, USA. Så det er litt opp til operatører. Operatøren sitter med et sett med parametere: Hvilke frekvenser har man? Hvor tett belagt er de frekvensene? Har du frekvenser som du kan dedikere til 5G, for eksempel, så kan du kanskje gå inn på SA tidligere, gitt at du har håndsettstøtte, enn om det er spektrum du må dele mellom 4G og 5G og du ikke vet når du kan få frigjort. Det kan godt hende at mindre operatører har et fortrinn, fordi de har mer spektrum per kunde og kan frigjøre kabalen litt annerledes. Så jeg tror det er godt mulig å ha et standalone nett innen 2022, gitt at man har frekvenser dedikert på det, og gitt at noen av håndsettleverandørene har noe som vi ikke har forutsett. De håndsettleverandørene som typisk gjelder i det norske markedet er Apple og Samsung. De to står for 90% av markedet. Så SA-nett kommer nok i 2022, og så er det også sånn at Norge er et litt rart marked, fordi det er the incumbent som er innovatøren. The incumbent er da [operatør], og det er de som har mest markedsmuskler til å drive med R&D. Så jeg tipper at [operatør] har standalone nett å tilby i 2022. |
| 67 | E | Som kunde hos dere gleder jeg meg ihvertfall veldig til det, haha. |
| 68 | I | Haha, det er bra. Dere får komme og jobbe hos oss og bygge det SA-nettet. Hvor langt har dere kommet i studiet nå forresten? |

| | | |
|---|---|---|
| 69 | E | Dette er masteroppgaven da, så det er siste semester. Så er det ut i jobb i august. |
| 70 | I | Ah, men dere får ringe på da. Vi leter etter gode kandidater. Innenfor det vi snakker om nå så vil jeg si at det er arbeidssøkers marked i disse tider når vi bygger ut SA-nett, 5G-nett. Og så er det også det at det politiske bildet endrer seg. Russland og Kina blir større og større sikkerhetstrusler, og det påvirker også evnene til Ice, Telenor og Telia å ansette. Fordi vi er underlagt sikkerhetslover og det da blir større og større fordeler å være norsk, for å si det på den måten. |
| 71 | L | Jeg synes det virker som en spennende bransje! |
| 72 | E | Har du noen spørsmål til oss eller er det noen ting du kanskje tenker at vi burde spurt om som vi ikke har vært inne på? Nå vet du jo litt om hva vi er interessert i sånn generelt. |
| 73 | I | Nei, jeg synes dere har vært veldig reflekterte. Dere har tydeligvis tenkt gjennom dette. Hvis det skal være noen vanskeligheter, altså, oppgaven rundt autonome nett det er ikke lett i seg selv. Da bør man kanskje tenke litt på hvilke typer tjenester man tar. Tar man da de 3GPP-spesifiserte, eller er det over-the-top? Og i forhold til din [Eivinds] oppgave: Se på interoperabilitet hvis det skal være flere tjenestetilbydere der ute, for interoperabilitet kan være vanskelig mellom push-to-talk providere hvis du ikke har en MVNO. |
| 74 | E | Det med den felles PLMN IDen, det synes jeg var veldig interessant å høre. Det har jeg ikke sett på før. |
| 75 | I | MOCN heter den teknologien der. Den gjør at basestasjonene sier at den basestasjonen er hjemmenett. Alle operatører kan sende ut MOCN-nett, altså flere MOCN-nett, alle kan stråle DSB sin kode, og dermed så får telefonene et veldig utøket hjemmenett - Men, med mobilitetsproblematikk. Så du vinner noe og du taper noe. Men for et nett til mange milliarder kroner så kan det være verdt å "overcome some hurdles" istedenfor å gå den enkle veien. |
| 76 | E | Minste motstands vei. |
| 77 | I | Ja. Men det er ofte den som blir valgt når prosessene er komplekse. |
| 78 | L | Det som skjer nå er at vi transkriberer og så sender deg det transkriptet, så du kan se om du synes det er anonymisert nok. |
| 79 | I | Ja, det er helt fine. Jeg tror ikke jeg har problemer med det som står der. |
| 80 | E | Nei, det varierer litt hvilke behov folk har for anonymisering, men vi gir alle intervjuobjekter samme behandling. |
| 81 | I | Jeg skjønner. Nei, men veldig bra! Da får dere ha lykke til med oppgaven, så håper jeg at det går bra. Ha det bra så lenge! |
| 82 | E, L | Takk for det, ha det bra! |

# Appendix G
# Mobile Virtual Network Operator

This interview is conducted with an interview subject who is familiar with the workings of MVNOs in Norway. The conversation ranges from specific topics such as challenges the state might have to overcome should they opt to establish their own state-owned MVNO, to more general topics regarding 5G and how MVNOs will be expected to function in relation to the 5G SBA.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, opptaket er i gang. |
| 2 | I | Okei, så Nødnett og MVNO. Har dere mer spesifikke spørsmål eller skal jeg bare gå inn å forklare litt hva vi gjør og hvordan vi gjør det og sånn. |
| 3 | E | Kan godt bare høre litt om hvordan dere gjør det. |
| 4 | I | Okay. Så, jeg kan jo si hvor vi kom fra for det forklarer litt sånn DNAet. [Historisk har innovasjon innen telco vært vanskeligere enn det har behøvd å være.] |
| 5 | E | Hvordan relaterer det dere gjør til typ MVNO-virksomhet? Jeg ser at dere lister to operatører på nettsiden deres som dere har avtaler med. |
| 6 | I | Ja, så da kommer vi til at dette får du ikke til hvis du ikke har en viss mengde med kjernenettelementer. Da har vi startet med det, og sagt at det er en full MVNO. Dere vet hvor grensene går der på hva dere har i tech-stacken eller er det et litt uggent område? |
| 7 | E | Vi kan jo ta det kort. Den inndelingen jeg ofte har sett er en sånn lower og upper core type inndeling. At man har på en måte, nå har jeg sett mest på 5G da, men der har man den delen som går på UPFen, AMFen og SMFen i lower core og har direkte med trafikkflyten å gjøre, og så har man de andre tjenestene på toppen. |
| 8 | I | Ja, og det tror jeg nok er ca. riktig. I 5G så må jeg nesten ha med en av ingeniørene mine, men i 4G da, hvis du tar EPCen, så er det SGW og MME i aksessnettverket, PGW i MVNO-nettverket, MSC og VLR ligger i aksess, GMSC ligger i full MVNO. Så det som har med mobilitet å gjøre ligger definitivt i aksess, og så ligger serving-delen av det å sette opp forbindelser og å håndtere bærere også i aksess, og så ligger ruting og alt det i full MVNO. Så du har full kontroll på brukeropplevelsen som ikke er radioavhengig, grovt sett sånn jeg ser det. Vi er da full MVNO, og det er for å få nok kontroll på brukeropplevelsen til at man kan manipulere brukeropplevelsen til det man ønsker å få til. Av de teknologiene vi har, så har vi full kildekodekontroll på alt bortsett fra PGW som vi har fra Cisco. Og alt det snurrer i Amazon. Alt er i containere, alt er microservices. Det er Java- og Go- og Kotlin- og Erlang-språk, og veldig lite SIGTRAN og Diameter. Vi stopper SIGTRAN og Diameter på kanten av nettverket, og så bruker vi gRPC-baserte protokoller internt i nettverket. |
| 9 | E | Ja, for å få til interoperabiliteten mellom de tradisjonelle telekomprotokollene og Kotlin liksom? |
| 10 | I | Litt det, og litt for å få utviklereffektivitet og hastighet. Og så er det også noe med at telco-tjenester ikke er så veldig cloud native. Så når du bruker public cloud, så er ikke de gamle protokollene så veldig cloud native friendly. Så det hjelper oss å bytte over de. Det er mye IP-logikk, og det å gjøre ting horisontalt skalerbart er ganske vanskelig på de gamle protokollene, så vi prøver å abstrahere bort det i størst mulig grad. Og så er vi multi-tenant. Så hvis dere ville blitt en MVNO så kunne dere fått en tenancy av meg i morgen. Da kunne dere bare koblet på et administrativt grensesnitt og så koker vi hele kjernenettet ned til et API. Og da kan dere provisjonere brukere og provisjonere tjenester og holde på som dere vil. Så, hvis vi skal begynne å linke dette til Nødnett. Jeg har snakket litt med Nødnett-gutta på et tidspunkt. Det er veldig avhengig av hva du skal bruke det til, og veldig avhengig av settingen du ser på det i, hvor relevant det er. Det er ekstremt avhengig av det store bildet. Nødnett har gått mye ned den ruten at de skal ha en slice av MNOene sine nettverk, helt ned til radio og radioprioritet. Vi ligger på en måte et lite lag over det, selv om vi nå også er |

| | | |
|---|---|---|
| | | på vei helt ned til å ta det fulle kjernenettet inkludert aksessnett-coren. Jeg tror, jeg tenker litt sånn halvhøyt for jeg har ikke hatt så mye tid til å tenke på dette som jeg skulle ønske, men det er et par versjoner hvor vi er relevant i Nødnett-sammenheng. Den ene er hvor vi tar de siste elementene av kjernenettet, og da kan politiet eller hvem som helst komme og si "Jeg vil ha Nødnett av deg." Vi kobler oss på aksessnettene, ett eller flere, og så ser vi de som en operatør, og vi leverer et fullt kjernenett til de som de har full kontroll på. Eller, mer presist, de administrerer, mens det er vi som drifter det. |
| 11 | E | Hvis vi tar DSB som sin egen MVNO, da er de en kunde av dere på samme måte som om vi ville opprettet en MVNO? |
| 12 | I | Nei, i det scenarioet så vil det være litt mer enn en MVNO, for da er du helt nede og håndterer også mobilitet og disse tingene. Da får du et fullt kjernenett. Versjon 1, da har du den tech-stacken du har i dag, men nå bygger vi også hele 5G-coren helt ned til AMF og UPF og SMF og det greiene der, så da får de det også. Så da er du mer enn en MVNO er i dag. Det er opsjon 1, og der er det kanskje også mulig å koble det på tre forskjellige nett. Men da er du ikke avhengig av MNOen sin core. Du kobler deg på lenger nede, på gNodeBene egentlig, du går rett på radionettet. Så det er versjon 1. Versjon 2 er vel en mer klassisk MVNO, at de er en MVNO. De kan være MVNO på tvers av Ice og Telia og Telenor, og det er en ting vi er satt opp ganske bra til å gjøre, å være en multioperatør-nett MVNO. Fordelen med det er at du har en konsistent opplevelse på tvers av radionettene, det er det ene. La oss si at du har en sentralbordtjeneste eller en nødappstjeneste som ringer alle parallelt, eller whatever. Hvis du har produkter på toppen av bare data, så kan vi levere de konsistent på tvers, så du kan bytte mellom Telia og Telenor og sentralbordtjenesten din eller whatever fungerer fortsatt. Det andre er at du kanskje kan gjøre ting som Telenor og Telia ikke vil klare å gjøre på grunn av den innovasjonskraften vi har. Og det tredje er at vi kunne gitt mer kontroll til DSB. De kan ha sitt eget BSS, management, billing system, og de kan ha all sånn kundedata og sånn, og vi kunne også gitt de en stor grad av kontroll i kjernenettet selv. De hadde vært mindre avhengig av operatøren. Vi ville gitt de en større grad av kontroll. Så: Større grad av kontroll, felles brukeropplevelse på tvers av nett, og evnen til å lage produkter som er relevant for deres use case på andre måter. Og så, skulle vi ha servet noe sånt, så måtte vi ha gjort ting på - Dette ville jo vært nasjonal infrastruktur, så vi måtte ha snurret opp dette i Norge. Nå står det per i dag ikke i Norge. Det er fullt mulig, men det tar tid og krefter. Og så måtte vi sannsynligvis ha skilt dette fra alt annet. Nå kjører vi multi-tenant solutions, men de ville sikkert insistert på å ha sin egen instans, og det kunne vi fått til. Og så måtte det vært voldsom redundans og resilliency og forferdelig mange 9-tall, og der har vi også en jobb å gjøre for å få det til, men det er også fullt mulig å oppnå. Jeg tenker i en sånn fredstidsversjon, så er dette superkult, for de kunne virkelig vært sin egen operatør og gjort ting på sin måte, og hatt en fleksibel leverandør som var villig til å jobbe med dem. I krigstidssammenheng er det andre krav som slår inn, som kanskje er krevende eller ikke, det er jeg ikke helt sikker på. Det var noen høynivåtanker. |
| 13 | E | Det er supert. Det er veldig interessant å høre. Hvis du tenker i forhold til at DSB skulle opprettet sin egen MVNO og driftet sitt eget kjernenett og alt sånn der, hvordan blir det annerledes å introdusere dere? Jeg skjønner at man får den ekstra programmabiliteten med tanke på apputvikling og sånt, men da hadde dere på en måte tatt dere av det operasjonelle rundt infrastrukturen og sånt, og så hadde DSB bare hatt en portal eller noe funksjon i sitt eget datasenter, men mindre da? |
| 14 | I | Ja, stemmer. Det blir litt som om de hadde kjøpt egne bokser, bare at de boksene blir kjøpt som en tjeneste istedenfor bokser. |
| 15 | E | Hvis vi går enda et hakk tilbake da: Det er jo litt ulike modeller som kan velges for neste |

| | | |
|---|---|---|
| | | generasjons Nødnett, og én av disse er den MVNO-modellen, og så finnes det noen andre som er sånn, ja, for eksempel at man velger Telenor til å være en fullstendig provider i alle ledd. Som en som har innsikt i litt sånn MVNO-type aktiviteter, hva tenker du at kan være fordelene og ulempene ved at staten har sin egen MVNO i et neste generasjons Nødnett? |
| 16 | I | Jeg tror liksom ikke det er så mye ulemper ved det. Det handler mest om hva du prøver å oppnå. Det at staten har sin egen MVNO, det hadde vært udelt morsomt det på en måte. Du får masse fleksibilitet, du kan gjøre masse ting, du gjør deg mindre avhengig av én operatør, du kan sitte på tvers av nett. Velger du Telenor så er du på Telenor, velger du MVNO så kan du faktisk sitte på alle nettene. Så du bygger deg aksessredundans og resilliency på tvers av aksessnett. Men så blir du mer avhengig av leverandøren av kjernenettet ditt da. Hvis du tenker risiko i stacken, fra radio opp til BSS: Hvis du kan sitte på tvers av flere radionett, så er det en gevinst. Det kan du også løse på andre måter gjennom multi-IMSI-type løsninger og sånt, men da er du begrenset til minimum fellesnevnere av tjenestene. Litt avhengig av hvordan de løser det, men i verste fall så får du bare data. Avhengig av hvordan du gjør, så vil heller ikke telefonnummer fungere på tvers, men det er som sagt avhengig av hvordan du gjør det. Så hvis du skal sitte på tvers av flere nett og ha den redundansen, så er en MVNO en ganske gunstig løsning tror jeg. Da kan du ha opplevelsen lik på tvers, med telefonnummer, med data, med SMS, og med de applikasjonene de velger å bygge på toppen. Det er en stor fordel. Og så tror jeg du kan ha uavhengighet for veldig mye av brukeropplevelsen ved å være uavhengig av å finne minste felles nevner av de nettene du sitter på. La oss si at de ønsker kryptert video og krypterte samtaler fullintegrert i nettene, men også bare på telefonsamtaler på 2G. Altså, du ønsker å kunne ha en 2G-samtale, og så ønsker du å kunne ha en video på den andre siden, og alt skal liksom være på en viss måte. Det får du ikke til hvis du skal gjøre det med Telia, Telenor og Ice. Det blir for komplekst, det går ikke. Det kan vi gjøre. Veldig mange av de casene vil vi kunne ta. Da kan du gjøre det, fordi du sitter på en stor del av brukeropplevelsen, og så lenge aksessnettet gir deg CSVoice og PSVoice og data, så kan vi legge på ting på toppen. Så du får en helt annen fleksibilitet til å gjøre det som er viktig for deg. Istedenfor å være bundet av minste fellesnevner av alle operatører i verden da, i praksis. Det er kanskje den største fordelen tror jeg. Jeg tror at Nødnett hvis det kjøpes av én leverandør, så handler det veldig mye om sikkerhet, og så blir det veldig statisk. Da har du speccet det opp, og så er det det du får. Du får ikke mer eller mindre enn det. Det er ikke noe utvikling i det. Det blir så krevende å levere bare det, at da betaler man noen milliarder for det, og så er det statisk. Jeg tror med en full MVNO så kan du starte mye mindre, du kan gjøre det mye billigere og enklere, og så kan du iterere deg for å komme deg dit du vil i mye større grad. |
| 17 | E | Har du noen tanker rundt at man introduserer ekstra kompleksitet, med tanke på interoperabilitet mellom ulike providers i løsningen? |
| 18 | I | Det er noe vi tar oss av på en ganske grei måte. Så jeg vil si at den kompleksiteten er marginal i forhold til den kompleksiteten du introduserer hvis du skal gjøre det på andre måter. Altså, vi har gjort det, vi har integrert på forskjellige nett. Det er litt tid og litt krefter, men det er ikke vanskelig egentlig. Det som skjer med full MVNO er at du integrerer på disse såkalte national roaming interfacene, og de er standardiserte. Alle operatører må roame, så de interfacene er faktisk ganske standard. Så det å integrere på de for oss, i den sammenhengen her, så er det en piece of cake. Du genererer ikke kompleksitet med det, vil jeg si. Eller ihvertfall svært lite. |
| 19 | E | En ting vi ser på er også litt sånn edge-funksjonalitet i ulike sammenhenger. Hvordan blir det i et sånt type MVNO-forhold? Hvem er det som skal ha ansvar for edgen, hvis man da for eksempel sier at man er avhengig av flere ulike radionett? Hvem er det som tar seg av det som skjer i edge? |

| | | |
|---|---|---|
| 20 | I | Hm, ja, godt spørsmål. Edge blir så altomfattende, det er så mye, så jeg tror man må være litt mer spesifikk. Det jeg tror vi kan gjøre på en kul måte, eller en enkel måte. La oss si at du har Telenor, du har Telia, og du har Ice. Det vi også kan gjøre er å si at "Ja, men Forsvaret de trenger - Det er ikke noe dekning ute på fjellet på Setermoen." Det vi kan gjøre er å lage et radionett, og vi kan tilby den fulle coren. Da kan Forsvaret snurre opp en full core oppe på et fjell på Setermoen, så lenge de har backhaul. Og så vil tjenestene fortsatt fungere på tvers, så da har du et fjerde radionett som de kan legge på til enhver tid. Da har du en radio-edge. Det caset kan vi serve ganske elegant. Med det samme SIM-kortet kan du da ha dekning i radionett som snurres opp over hele Norge. Så det er edge case 1. Og så er det vel den mer tradisjonelle edgen, som du sier, som er å prøve å skille ut user plane-trafikk lokalt for latency- eller sikkerhetsformål. Når vi da bygger hele 5G-coren så er det noe vi skal enable også. Hvordan det blir med edge i et MVNO-setup, det er jeg ikke sikker på. Da skal du inn og mekke ganske kraftig nede i aksessnettet for å få den til å bli veldig edge, altså. Jeg tror at vi får det til hvis du gjør det på egen radio, det er jeg veldig komfortabel med. Hvis du har et eget radionett der du ønsker edge, da er det ganske greit. Hmm, la oss si at Forsvaret ønsker å hairpinne trafikk på en base et eller annet sted, da må de gå og be Telenor gjøre det. Og hvis Telenor kan gjøre det for de, så burde de virkelig kunne gjøre det for oss. Ah, her er jeg litt på tynn is, altså. Her må jeg ha med noen ingeniører. |
| 21 | L | Jeg spinner litt opp til min oppgave, jeg. Jeg ser på tilfellet der et cluster av basestasjoner mister backhaul connection og må virke som et autonomt nettverk. Jeg antar at vi kun har én radiooperatør for å gjøre det litt enklere for meg selv, men i tilfellet at vi har Nødnett som en MVNO: Hvordan skal vi løse disse komponentene i edge da? Har du noen tanker rundt det? Når du må ha et fullt duplisert kjernenettverk i edge. |
| 22 | I | Ja, altså, kan du gjenta spørsmålet en gang til? |
| 23 | E | En av de tingene hvis du liksom skal ha den fulle funksjonaliteten i et nettverk som er avskåret fra hovedkjernenettverket, så må man kanskje ha - I tillegg til å ha de vanlige trafikkontrollfunksjonene så må man kanskje også ha HLR-type funksjon ute i nærheten av basestasjonene. |
| 24 | I | Ja, så du ønsker å snurre opp hele kjernenettet på edge. Det finnes open source-prosjekter og prosjekter som gjør det. Som er basert på det, på en måte. Det kan være Magma, eller det kan være - Som snurrer opp hele autonome nett der ute, og det er en hel industri bygget rundt gruver og sånn som gjør det der. Men det er ofte enten eller. Enten så har du et sentralt kontrollplan eller så har du ikke det. Nå bare tenker jeg høyt, men jeg kjenner ikke til caser der du har sentralisert kontrollplan for de effektene og fordelene det gir, og så er det fullt autonomt hvis det forsvinner. Det tror jeg er en krevende case å løse, altså. |
| 25 | L | Jeg tipper det er derfor de har gjort det til en masteroppgave, hehe. Jeg har fortstått det som at det er en ganske unik case for public safety-tjenester. Et kommersielt nett vil jo ikke ha nytte av at personer i et lokalt område kan snakke med hverandre uten å ha tilgang til tjenestene. Men disse gruppesamtalene blir viktige i den lokale konteksten. |
| 26 | E | Men hva med sånn type mer regional edge. At man har infrastruktur som er nærmere basestasjonene enn kjernenettverket, men likevel også litt sentralisert. |
| 27 | I | Ja, det tror jeg skal være mulig, også etter et MVNO-setup. Jeg tror det burde være mulig å ha multiple PGW som rutes liksom nærmest. Det tror jeg skal være mulig, altså. Det er jeg ganske sikker på. Jeg tror det her helautonome, jeg bare tenker høyt nå, fordi det du sier er jo et scenario der du ikke kan nå tilbake til den sentrale HLRen og whatnot, så ønsker man |

| | | |
|---|---|---|
| | | egentlig at man oppretter en ny lokal modus, det er en måte å tenke på det, ikke sant. At du får et basissett av tjenester uansett. Jeg tror det å deploye lokale replikaer av hele coren der ute er ekstremt krevende. Men her er det igjen: Hadde DSB kommet og sagt "Kan dere løse dette for oss?" så tror jeg vi hadde klart å få til det faktisk. Det tror jeg ikke Telenor hadde klart like enkelt faktisk. Da måtte de gått til Nokia og startet et treårsprosjekt. Men det er fullt mulig at - For eksempel da, hvis vår HLR går ned, så er det jo fortsatt mye trafikk som går. Autentiseringsvektoren er sendt, så for eksempel datatrafikk som har en bærer, den fortsetter jo. Så det er nye connections som blir avvist, men eksisterende connections blir. Det å kunne skape et minimumssett av tjenester som fortsatt fungerer der ute selv om den sentraliserte funksjonaliteten er borte, det er en jobb som må gjøres og jeg tror ikke vi ville gjort det med å duplisere replikaer og sånt, men kanskje sagt noe sånt som at "Disse brukerne har en setting som tillater de å gjøre en del ting uansett om de får snakke med HLRen eller ikke," på et eller annet vis, jeg vet ikke helt. Det kunne vært en morsom ingeniørutfordring å spørre teamet om, hehe. Men jeg tror for eksempel det å ha gruppesamtaler basert på en databærer som man gir lang varighet og noe intern ruting, ja, ikke umulig, altså. Jeg har ikke noe svart-hvitt svar til deg, men jeg tror det er mulig. |
| 28 | L | Det er veldig interessant å bare sparre litt synes jeg! |
| 29 | E | Ja, for du tenker hovedutfordringen med å desentralisere HLRen og sånn: Er det synkroniseringsutfordringer eller er det sikkerhetsutfordringer? |
| 30 | I | Nei, det er vel mer det at vi ikke har gjort det. Det er sikkert mulig. Altså, på voice nå så sitter vi og ser på å bruke Kafka-teknologi på å kjøre distribuerte databaser med active-active på real-time signalisering og oppsett av voice. På tvers av Amazon-regioner. Sånn at hvis hele Irland synker i havet, så skal Stockholm og Frankfurt fortsatt kunne betjene det. Og det er jo bare en større versjon av dette. Man kan jo da i teorien putte på en Amazon outpost edge-løsning, i teorien ihvertfall, så kan du gjøre det. Og så er spørsmålet: Hvor er edgen din? For dette er jo teknologi som krever noe prosessering og lagringskapasitet, så du kan nok ikke putte det på en gNodeB sånn integrert. Det må bli noe regionalt isåfall, for hvis du skal ha public så er det såpass tung prosessering og lagring og sånn at det må du ha en viss kapasitet for å kunne kjøre. Men det å ha det på regionalt og sånt, det er nok absolutt mulig. Det er ganske dyrt, potensielt, men absolutt mulig. Det er mer det at vi ikke har gjort det, og ikke tenkt på det så veldig mye. |
| 31 | L | Det er jo standardisert for dette gjennom 3GPP - Eller, de jobber ihvertfall med det for gruppesamtaler for tale og video, og data kommer vel også. Men jeg forstår at det er utfordringer mer enn bare tekniske protokoller og [vanskelig å høre]. |
| 32 | I | Men alt det som 3GPP standardiserer det klarer vi å lage. Jeg har ennå ikke møtt veggen på det. Da har du sett mer på det enn jeg har gjort, men hvis de har et format for det så kommer vi til å måtte lage det, sånn sett. Men det er ikke noe vi har brukt mye tid på enda. |
| 33 | L | Det gir mening. |
| 34 | E | For å gå over til noe annet. Jeg forstår det slik at dere opererer mest i 4G LTE i dag, hvordan tenker dere at det blir å være en MVNO going forwards i 5G? Blir det enklere med tanke på at man får mye virtuelle nettverksfunksjoner og sånt istedenfor å ha spesialisert hardware? |
| 35 | I | Vi er jo der allerede. Vi kjører ikke på noe spesialisert hardware. Ja, PGWen kjører vi, men alt annet er som sagt ut av Amazon. Vi har liksom tatt 5G-logikken og dratt den tilbake ned til 2G, 3G og 4G, så for oss er det ikke noen forskjell egentlig. Signaleringsplanene går vel stort sett på HTTP, så vidt jeg har skjønt, så sånn sett er det nærmere den type ting som vi liker. |

| | | |
|---|---|---|
| | | Men, som sagt, det har vi allerede begynt å oversett uansett. Så for oss er 5G liksom bare å implementere noen nye protokoller, hvis man skal si det litt kult og enkelt. På signaliseringsplanene så er det mye det faktisk. Jeg tror de store utfordringene i 5G er i distribuerte nett, og med performance, latency og throughput, også i kjernen. Men sånn MVNO-aktig så tror jeg ikke det er - Det er alltid mer komplekst når det kommer en ny G, så for MVNOer så vil det nok være 5G NSA, non-standalone, ganske lenge tror jeg før MVNOer kommer på 5G SA. Det vil nok ta en god del tid, altså. Operatørene er ikke alltid incentivert for å gi MVNOene den beste brukeropplevelsen, for å si det sånn. |
| 36 | E | Jeg synes det har vært veldig informativt å få høre om - Vi snakker jo med litt ulike MNOer og sånn, så det er spennende å høre ulike perspektiver på disse tingene. |
| 37 | I | Finner dere ut av noe da? Har dere noen hypoteser eller egne meninger om hvordan dette bør gjøres? |
| 38 | E | Ja, jeg skal jo kanskje mene noe til syvende og sist. Det er mye pros and cons, og så hører man ulikt fra ulike aktører. Hvis man snakker med noen fra Telenor så vil de gjerne selge Telenors løsning på en måte. Det jeg ser på er hvordan de gjør det i andre land som har kommet lenger enn oss i prosessen, for eksempel Storbritannia, USA, og Finland spesielt. Som på en måte er litt videre i prosessen. Og så prøve å lære litt av deres feil. |
| 39 | I | Hva ser du der da? |
| 40 | E | Det er litt ulike modeller. Finland har gått for en sånn MVNO-type modell der de har et statlig selskap som er ansvarlig for en MVNO og drifter den selv, og så har de leid radionettet til Elisa, en mobiloperatør i Finland. Mens i USA for eksempel så har de tatt en sånn hel avtale med AT&T, der AT&T leverer fra ende til annen. Både radionett og kjernefunksjonalitet og sånt. Så FirstNet Authority, den statlige organisasjonen, er på en måte bare en kunde av AT&T på en veldig lang kontrakt. Der er det også litt interessant fordi det ikke er det eneste nødnettet i USA. Andre kommersielle aktører som for eksempel Verizon tilbyr også egne nødnettløsninger, så man får en annerledes kompetitiv dynamikk. I Storbritannia har de ett nett. Der er det EE som leverer radiotjenestene, og så er det Motorola som leverer den øvre delen av coren. |
| 41 | I | Det er avhengig av hva du ønsker å oppnå, men jeg tror jo at det historien viser er at det å lage egne nett er ganske dyrt, og har en tendens til å være utdatert innen du er ferdig. |
| 42 | E | Speaking of Nødnett? |
| 43 | I | Ja, det er vel det norske nødnettet, ikke sant. Jeg tror at hvis du ønsker fleksibilitet så må du ta kontroll selv. Ønsker du fleksibilitet, og ønsker å drive utvikling, så må du ta mange små steg og ikke liksom få store steg. Det er så banalt å si, men jeg tror også det er ekstremt viktig. Så jeg tror, litt den der AT&T-modellen da, å gå inn å kjøpe en kontrakt på fem milliarder dollar over 15 år eller noe sånt - Måten telco funker på er jo at du har store upfront costs, og så prøver du å monetize de. Her er det jo ikke vekst. Hvis DSB kjøper et nødnett så er det ikke sånn at du får flere brukere over tid som gir deg masse penger. Vanligvis så prøver jo telco å lage et radionett, og så prøver de å makse ARPU og antall kunder for få mest mulig utbytte av radionettet. Her er dynamikken: Da spinner jeg opp det jeg skal spinne opp, og så vil jeg bruke minst mulig penger på det. Så det blir jo et veldig statisk nett, og tar sikkert lang tid å lage. Så med noen grad av sannsynlighet så blir det stående ganske stille, tror jeg. Og det tror jeg ikke er så lurt, i mitt hode. Så jeg tror at disse organisasjonene enten burde gjøre det in-house. Rett og slett utvikle selv. For det er krevende, men det er ikke så krevende i en kontekst. Vi har Kongsberg og vi lager våpen, og |

| | | |
|---|---|---|
| | | vi gjør ting som er ufattelig my mer komplisert enn dette. Og det å ha kontroll, både sikkerhetsmessig og autonomitetsmessig, og fleksibilitetsmessig, tror jeg vil gi viktige langsiktige effekter. Og hvis du ikke gjør det selv, så ville jeg tatt kontroll selv i størst mulig grad. Jeg ville da jobbet med partnere som gir meg, om ikke kildekodekontroll, så gir de meg fleksibiliteten som om jeg hadde det. Så jeg ville hatt færrest mulige ledd mellom meg og koden. Og så fort du jobber med en operatør, de vil alltid ha et eller to eller tre ledd. Så da ville DSB være kunde, Telenor være leverandør til de, og så ville Telenor kanskje igjen ha to, tre, fire, fem, seks, syv, åtte, ni, ti leverandører som leverer inn til de igjen. Det er en veldig krevende struktur å få gjort noe i. Så enhver som har jobbet med en operatør kan fortelle deg at da får du ikke gjort mye, altså. Så jeg tror du skal ha partnere og ikke leverandører, hvis du skal gjøre noe med dette nødnettet utover bare basis. |
| 44 | E | Ja, jeg ser jo på litt sånn vendor lock-in effects og sånn. Spesielt teknisk vendor lock-in effects: At man får spesialiserte grensesnitt utviklet av den leverandøren man har til en viss tid og så setter man seg litt fast i det. Det er jo et interessant aspekt. |
| 45 | I | Men det tror jeg du gjør her uansett hvis du ikke tar kildekodekontroll. Det er en illusjon at du ikke gjør det. Den eneste måten du unngår det på er å få basis og ingenting annet av noen. Hvis du får SMS og du får VoLTE, og du skal ha data, da kan du klare deg. Men hvis du skal gjøre noe annet så blir det lock-ins i huet og ræva uansett. Det er bare graden av lock-in som varierer. Så tror jeg også - Ja, igjen, Nødnett trigger jo helt andre dimensjoner og det er jo "Hva hvis krig?" liksom. Hva hvis Nokia i Finland ikke kan hjelpe deg? Hva hvis landet er stengt ned og du ikke har internettkontakt til resten av verden, hva skjer da? Og igjen så er det litt sånn: Har du kontroll, så kan du få gjort en del, er du avhengig av for mange leverandører så blir du stående ganske fast. |
| 46 | E | Men, supert. Det har vært veldig interessant å prate med deg. Har du noen flere spørsmål til oss, eller er det noe vi kanskje burde ha spurt om som vi ikke har vært innom? Nå har du fått litt innsikt i hva vi lurer på litt generelt. |
| 47 | I | Helt generelt så hadde det vært kult om vi brukte litt mer tid på studiet deres om ikke så altfor lenge. Jeg har egentlig hatt litt dårlig samvittighet for at vi ikke har vært og snakket mer med dere. Dere er vel den linjen i Norge vi som selskap burde bruke mer tid på. Så det har ikke noe med oppgavene deres å gjøre, men vi er egentlig ganske interessert i å snakke med linjen deres. |
| 48 | L | Ja, det er bare å ta kontakt med Abakus linjeforening, eller så går det jo an å prøve seg inn på den akademiske siden med gjesteforelesninger for eksempel. Det tror jeg kunne vært spennende. |
| 49 | E | Men, ja, det har vært veldig hyggelig å snakke med deg. |
| 50 | I | I like måte. Lykke til med oppgaver og studier! |
| 51 | L | Vi sender deg transkriptet, så får du sett over det i god tid før vi skal gjøre noe med det. |
| 52 | I | Takk skal du ha, ha det godt! |
| 53 | E, L | Takk skal du ha! |

Appendix H

# Directorate for Civil Protection A

This interview is conducted with a representative of the Norwegian directorate for civil protection (DSB). It regards topics related to limitations of the existing TETRA based Nødnett and the way in which Norwegian public safety agencies make use of the capabilities that exist in this currently available PSN. A particular interest is taken in questions related to autonomous operation of base stations on the edge of the network, and reflections are made concerning the Local Site Trunking (LST) mode which exists in TETRA based PSNs today.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn! Da har jeg satt på lydopptaket, og så spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Det er helt i orden. |
| 3 | E | Jeg kan starte med å si litt om min oppgave. Min oppgave konsentrerer seg egentlig hovedsakelig om kjernenettet, og ulike modeller for hvordan vi skal gjøre NGN i forbindelse med at vi skal samarbeide litt mer med kommersielle aktører enn vi gjør i Nødnett dag. Så man skal ha et kommersielt radionett sånn jeg har forstått det, og så er det litt ulike løsninger for hvordan man skal gjøre det i kjernenettet. Sånn jeg har forstått det, så er du en radiofyr, så det kan hende at Lina sin oppgave blir litt mer relevant akkurat i dag. |
| 4 | I | Jeg tror nok det, ja. |
| 5 | L | Jeg er mer ute i radionettet. Jeg ser på hvordan man kan opprettholde funksjonaliteten til en eller et cluster av BS som har mistet tilkoblingen til kjernenettet, i scenarioet der vi ser på at Telenor drifter radionettet, og vi har en MVNO-situasjon i kjernenettet. Så jeg tenker at du sikkert har mulighet til å sparre litt med meg på hvordan det kan være mulig å realisere autonome BS i 5G? |
| 6 | I | Jeg må innrømme at jeg ikke har fulgt så innmari mye med på 5G eller 4G generelt, så jeg vet ikke mye om det. Local Site Trunking er noe jeg holder på med, og det er like frustrerende i dag som det har vært før. Det er et veldig vanskelig tema. |
| 7 | L | Vil du ta oss gjennom hva som er hovedutfordringene der? |
| 8 | I | Teknisk sett er ikke dette noe vanskelig. Du setter bare en BS til å kunne operere i LST. Så det det begynte med, default mode, det er at alle BS skal ha den muligheten. Så da vi gikk, i fase 0 som det het med det sentrale Østlandsområdet i 2009/2010, så hadde alle BS det enablet, altså LST. Så ville jo alle BS fremdeles gi samme dekning, men det ville jo være masse sånne små øyer. Og det, ja, i teorien er det kanskje bra, men det viser seg at de ikke har noen å kommunisere med, men de står på den øya alene. Og hvordan kan de kommunisere? Det som er viktig er å forstå hvordan de forskjellige enhetene og etatene kommuniserer. Politiet kommuniserer f.eks. alltid fra terminalen til operasjonssentralen. Så hvis de ikke er på samme øy som operasjonssentralen, så har de egentlig ikke noe samband. Men dette gjelder ikke alle. |
| 9 | L | Hvem er det det ikke gjelder? |
| 10 | I | Det vil jeg tro gjelder brann, i utrykning og sånt er det noen som kommuniserer fra terminal eller bil til operasjonssentral, mens akkurat når de er i brannslokkingsfasen er det mer internt. Så forståelsen av det er veldig viktig for å få det her ordentlig til. Og vi fant jo ut da, at ved å ha masse sånne små øyer, så fungerer ikke de greiene her. Brukerne visste ikke at de kunne gli inn og ut av LST, du ser ikke det. Du kan se det på displayet ved at det endrer farge, men stort sett har de ikke den terminalen foran seg. De ser ikke det, de vet ikke det her. Så når politiet da er i en farlig situasjon og de ser at det er rødt lys, men kanskje det er oransje, men akkurat i en stress-situasjon så melder de og spør om å få backup, og så er det ingen som svarer. Så for de fikk vi beskjed ganske tidlig at det er viktigere for dem å få et rødt lys, enn å være i en LST-situasjon. For da kan du se at du ikke har samband, og må agere på en helt annen måte i en farlig situasjon enn når de har samband. Og de sier at det absolutt viktigste HMS-verktøyet de har i politiet er ikke skuddsikker vest, det er samband. Så hvis de da tror de har samband, så er det en veldig farlig situasjon for dem. Jeg vet ikke, |

| | | |
|---|---|---|
| | | kanskje dere skal intervjue etatene også, det vet jeg ikke. Så jeg behøver ikke si for mye her, men det er dette jeg har fanget opp. |
| 11 | L | Ja, det skal vi. Samtidig er det interessant å få innsikt i hva du anser som behovene deres også. Det er ikke alltid så lett å stille de riktige spørsmålene selv. |
| 12 | I | Vi kan komme tilbake til det senere også. Så det vi gjorde etter hvert, var å samle de forskjellige etatene og prøve å legge en strategi for å prøve å lage disse cellene eller øyene større. Så da måtte vi velge ut enkelte BS, så det vi landet på den gangen var veldig generelt alle BS som hadde 48 timer backup, og det var den gangen ca. 15% av BS. |
| 13 | L | Det er det jeg har sett i dokumentasjonen nå og. |
| 14 | I | Og så var det alle som var tunnel-donor. Vi har dekning i ca. 400 tunneler, og de fleste av de har ikke en egen BS, så de mottar signalet fra en BS og sprer det ut i tunnelen. Så det var de donorene som mottok det signalet. Tanken der var at på den siden som de mottar signalet, kanskje det er naturlig for brann eller innsatsstyrken å ha et innsatsleder-KO. Så da vil i alle fall de og de som er inne i tunnelen kommunisere. Det var det som var tanken bak den. Selv om de ikke hadde KO, var det det at de skulle ha dekning inne i en tunnel. Noen av de er jo 24 km lange, så det er veldig viktig ville vi tro at det var dekning i de forskjellige tunnelene. Så da ble det lappet sammen på en måte, du tok 48 timers BS og tunnel-BS og så ble det et design for hele landet. Og der har det stoppet. |
| 15 | I | En av grunnene til at vi kunne gjøre det, var mulighetene til etatene selv for i terminalene å kunne slå av og på om du vil benytte deg av LST. Brukeren kan ikke gjøre det, men du kan programmere det i kodepluggen, altså i selve terminalen. Og det gjorde det enklere fra vår side, for da er det opp til brukerne om de skal forholde seg til det her. Og da var det forskjellige ting. For politiet, det de tenkte den gangen, originalt, var at de skulle ha det i de håndholdte terminalene, men ikke i bilterminalene. Tanken med bilterminalen var at du har bedre antenneforhold, og du har sterkere senderstyrke så du har kanskje større sjanse for å nå en BS som ikke er i LST. Men etter hvert gikk de vekk fra det. Det ble for forvirrende da de kjørte inn og ut av BS som var i LST. Så de skrudde det av igjen. Brann, på sin side, tenkte motsatt. For brann er det ekstremt viktig at de har en callout-funksjon som fungerer. De fleste er jo deltids-brannmenn. LST fungerer ikke i en callout. Så da var det bedre for de, igjen er tankegangen at du ser at de ikke har dekning, og å forholde seg til det. Så de slo av, nå vet jeg ikke om de har det enda, slått av for håndholdte terminaler. Mens på bilterminalene så var ønsket sentralt at det skulle være på. Men hva de har i dag, om alt er slått av, det vet jeg ikke hva de har programmert inn. Helse er jeg litt mer usikker på, jeg tror de var enige i det de hadde. Jeg tror de har slått det på. |
| 16 | I | Det var det det begynte med, men det er jo ikke noe problem du støter på her, ikke noe opplæring hos styrkene i denne bruken av LST. Det er veldig vanskelig å forstå når du er, det er vanskelig å se. Det er ikke noen sånne klare signaler. En spaner som har en skjult terminal, kan ikke se om det er annet lys, grønt eller rødt eller noen ting. De må bare stole på at de har samband eller ikke samband. Så sånn sett har det ligget der. Vi tilbyr det, det er flott for oss å si at vi har det og det er kjempeviktig og greier, men for brukerne er det greiere på mange måter å gå rett i DMO og den walkie-talkie-modusen. Det er enklere å forstå, for da er du innenfor et område du kjenner til. Så den tror jeg de klarer greit. Men det å operere og gjøre design for LST, det er fysisk mulig, som vi gjorde. Du kan designe LST, du ønsker da en BS som dekker et stort område som inkluderer de viktigste punktene du har med politistasjon, brannstasjon, samfunnshus og alle de tingene, så du lager en svær øy så alle kan kommunisere internt i den bygda eller den byen. I Ålesund hadde vi et utfall i en av de store BS som ser et kjempeområde, en fantastisk site for LST. Problemet var at det var den |

| | | |
|---|---|---|
| | | eneste BS som gikk ned. Alle andre BS som da har dekning i hele området vil fungere normalt. Den store BS sugde til seg veldig mange terminaler. De hang der, politistasjonen hadde antenne på den andre siden av bygget og hang på noe annet. Helt kaos, ingenting fungerer. Og det var ikke en BS her, det var ikke feil på strømmen, det var transmisjonslinken som var tatt av lyn. Det tar vel tre måneder å bygge den opp igjen. De endte med å sende teknikere opp for å fysisk slå av BSen. Du har ingen mulighet til å omdirigere. Så den ideelle BS, den var ikke så ideell den heller. Så du kommer i den problemstillingen der når du har en av mange som går ned. Da ønsker du kanskje den nest sterkeste. Så har du den andre siden, hvor alt går ned. Det er det letteste scenarioet, da velger du bare de som dekker det største området når alt går ned. Det har ikke skjedd enda. Det som pleier å skje er at enkeltdeler går ned. Da får du en miks av ting, og da er det veldig vanskelig, for min del i hvert fall, å designe. Skal du designe for at en går ned, skal du designe for at alt går ned? Så det er noe av problematikk-tankegangen der. Nå prater jeg bare i vei her da. Bare å stille spørsmål. |
| 17 | L | Nei, det er bra. Jeg lærer mye. |
| 18 | I | Er det klart så langt? |
| 19 | L | Ja, jeg synes det var veldig opplysende, fordi du løfter det opp til et litt mer oversiktlig nivå enn jeg har vært på hittil, og det hjelper meg veldig. Og så har jeg flere oppfølgingsspørsmål som vi kan ta etter hvert. |
| 20 | I | Bare si fra når du trenger de. Det er lett å kanskje grave seg litt ned i de tekniske, men det er ikke det som er … Nå vet jeg ikke på 5G, jeg tror det blir enda verre der. |
| 21 | L | Du tror det? |
| 22 | I | Ikke teknisk, men jeg tror operasjonelt, å få det her til. Det kan hende jeg tar feil. Forsvaret synes det er veldig positivt. Men hvordan kommuniserer de? Kommuniserer de tilbake til en operasjonssentral, eller er de en styrke som er der ute, en liten tropp som skal gå inn og gjøre ting der? Det er en helt annen måte å operere på enn som f.eks. politiet. For enkelte er det her ideelt. Røde kors, kanskje, i et søk er det helt greit. Men samtidig sitter de og leder søket fra HRS, eller i Stavanger, eller de sitter på politistasjonen og leder søket. Så plutselig så hjelper ikke det noe allikevel. Så kanskje de i Røde kors hadde klart seg med DMO, det vet jeg ikke. |
| 23 | I | Ja, hvor var vi. Når vi har laget dette designet, og det designet her er det jo ingen som vet noe om, bortsett fra enkelte folk i etatene. Det er ikke hemmelig, vi har snakket om det på konferanser og sånt, fagdager, men det er jo ikke noe en vanlig bruker tenker på i det hele tatt, vil jeg tro. Hvordan det er designet når strømmen går, ja da fungerer det sånn, det skjer ikke. Så det som var håpet var at vi går inn lokalt og sitter sammen med etatene og brukerne og setter opp en LST-plan, eller DMO eller C-plan. Altså, hvordan fungerer ting. Og det er to kommuner som har tatt kontakt for å gjøre det her. Jeg tror du må ned på kommunalt nivå, for du må vite hva som er viktig å dekke i den kommunen og hvilke områder er det de ønsker å helt sikkert ha dekning i. Tanken min der er at du finner en basestasjon som de klarer å holde i drift uansett. Du har mulighet med en generator og at noen fyller på diesel på den generatoren. Det trenger ikke å være en stor BS, det kan være en som dekker legevakt, nå har du kanskje ikke legevakt i bygder, skolen og samfunnshuset, og brannstasjonen. Sånne ting, at du får den garantert til å fungere uansett. Da har du den, og dekningsområdet til den BSen er kjent. Så når alt er gærent, kan styrkene vite at hvis de kommer seg innenfor den gata der så har de dekning. Da kan de kommunisere med hele området. |
| 24 | I | Selv om det var en tunnel der, for vi vet ikke hvilken angrepsside eller hva det heter for noe |

| | | |
|---|---|---|
| | | brann har når de går inn. Vi vet ikke hvilken vei viftene blåser. Det kan godt hende at det er der vi har donoren vår at røyken kommer ut så det må angripe brannen fra den andre siden av tunnelen. Sånne ting har ikke vi satt opp. Og flere av de store tunnelene på Vestlandet er over to kommuner, så det er to forskjellige brannvesen som går inn. Angriper de på samme måte? Aner ikke. Etter min mening bør det for hver eneste store tunnel vært satt ned en LST-plan eller DMO-plan. Det samme for byer og bygder. Lage en LST-plan som folk der lokalt kjenner til. |
| 25 | I | Stavanger har tatt kontakt med meg. Det de ønsket var å sette opp et DMO-system. Vi satt noen punkter rundt omkring på fjellene rundt Stavanger. Jeg tenkte dette er en ypperlig anledning, de har en kjempe BS midt i sentrum. Jeg ba dem vurdere det her, BSen kan gå i LST, den er lett tilgjengelig, den har store aggregater der det bare er å fylle på drivstoff. Så gjorde kommunen ved hjelp av politiet og DSB en test der vi satte denne i en egen subscriber class. Jeg vet ikke hvor kjent du er med det, men en subscriber class gir tilgang til en BS. Vi satte den i en spesial subscriber class så bare BS og terminaler som var programmert dit kunne fungere sammen. Terminalene kunne ikke bruke en annen BS. Så vi kjørte rundt, de kjørte masse tester, og denne BSen dekket hele Stavanger, men også øyer og langt ned i Sandnes. Et kjempeområde. Ikke innendørsdekning, men utendørsdekning. Så der har de en ideell kandidat som de hvis alt går ned. Jeg tror at i RoS-analysene til kommunene så skal de ha en plan for bortfall av EKOM. Og da har de tenkt på hva de kan bruke Nødnett til. Det kan hende at vi da er ute, men hvis de har laget en LST-plan tror jeg de kunne kommet veldig langt. Men fra det punktet der alle var veldig fornøyde med testen, har det ikke blitt gjort noe. Det har ikke blitt operasjonalisert, jeg vet ikke om den BSen er enablet for LST. Det er mange tunneler i Stavanger-området, og den er ikke donor til de, så hva gjør vi med dem? |
| 26 | L | Er det mangel på engasjement i kommunen for å ta tak i det, eller ...? |
| 27 | I | Nei, jeg tror vel ikke det heller. Men det å få ting videre og så skulle vi jo møtes på Nødnett-dagene i fjor og sånne ting. Alt har blitt forskjøvet, og den beredskapsavdelingen som var interessert i det her vil jeg tro har andre ting å tenke på i disse tider. Det er nok forskjøvet. Vi hadde jo håpet at vi kunne gjøre noe mer, og de var jo litt hyppe på det her også. Politiet også, at de kunne si at sånn har vi gjort det og kan vise det til andre politidistrikter. Det hadde vært veldig gunstig å få en av de store byene til å gjøre det. Men absolutt, vi også skulle nok vært mer på tilbudssiden her. |
| 28 | L | Hvis vi ser for oss at 5G kommer til å brukes til radionettet i Nødnett, så kommer vi til å ha en høyere celletetthet. Hvordan ser du for deg det her, vil du tenke litt høyt om det? |
| 29 | I | Ja, kan jeg bare ta denne tråden ferdig? |
| 30 | L | Så klart. |
| 31 | I | For det jeg ønsket meg og det jeg forhørte meg med Motorola om teknisk, var som du nevnte tidligere med clustrede sites, en eller to. Klarer kommunen å opprettholde to BS i det scenarioet, så de er sikre? Det er igjen det her at brukerne må være sikre på at de alltid er oppe. Det er det som er poenget mitt her, at de må være sikre på det. Hvis du da klarer å ha to eller tre BS som har garantert transmisjon, som er garantert at er oppe, så hadde vi hatt den bobla. Selv om det ikke er teknisk mulig, i alle fall med TETRA-systemet. Hvis det hadde vært mulig å gjøre det, og en av disse BS var veldig usikker, da tror jeg du er tilbake til usikkerhetsmomentet igjen med at noen ganger fungerer det, andre ganger fungerer det ikke. Poenget mitt var å få noen som garantert er oppe. Selvfølgelig ikke hvis de blir bombet, men alt annet. Står de der, skal de være oppe og fungere. |

| | | |
|---|---|---|
| 32 | I | Så da tilbake til 5G hvor du har mange. Da skal det fungere for dem å kommunisere med hverandre, så lenge de har transmisjon. Med den store celletettheten og strømutfall f.eks. så vil jeg tro at det vil variere veldig hvilke BS det er som kommuniserer med hvem. Denne LST-bobla kan flyte rundt. Noen ganger er de inne, noen ganger er de ute, noen ganger får de rødt lys. Det fungerer sikkert veldig bra for beredskapstroppen, Forsvaret, Røde kors, sånne ting. Men når du er avhengig av call-out, du er deltidsbrannmann, du er hjemme, du er på jobben og venter, da får du ikke noen call-out. Du sitter i en LST-boble, selv om du ikke vet det, hva skal du gjøre. Så jeg tror det der kan by på problemer sånn operasjonelt. Hele den fluksen av inn og ut. |
| 33 | I | Det var det som forvirret politiet, eller ikke forvirret. Du kjørte forbi en BS som var i LST og gikk inn dit, plutselig var du da flere minutter uten samband egentlig, for du er den eneste politibilen i området. Det er ingen som kommuniserer med deg. Så jeg vil tro at med den celletettheten så vil det her bli enda verre med det operasjonelle. Rent teknisk er det sikkert kjempeflott. |
| 34 | L | Ja, så dette med å få oversikt som bruker over hva som er tilstand for deg, det er krevende. |
| 35 | I | Det vil jeg tro. Det her er bare et verktøy for dem. Hvis du intervjuer en fagsjef samband, som det heter i politiet, det er de som bestemmer over hvordan samband skal være i politidistriktet, de har peiling. De sier at de som er ute, de vet ingenting. |
| 36 | L | Ja, vi har snakket med brukere. |
| 37 | I | Ja, vanlige brukere altså. De har ikke den kunnskapen. De får en eller to dager opplæring på politihøyskolen om samband. Det er ikke en LST-plan som står i hodet deres. Det her er bare noen som de skal ta opp og som skal fungere når de snakker. Når de tar den opp har de lys, og det er ikke rødt i alle fall, men så er det ingen som svarer, og da sliter de litt. Så kan du bare slenge inn helikopter og sånne ting i de greiene her så blir det enda mer komplisert. Helikopter, for eksempel, de har ikke LST enablet. Det er ikke noen hensikt, hvis AGA-basestasjonen går i LST, hvem skal den snakke med? De andre helikoptrene? Det fungerer bare ikke, så vi har valgt å skru det av for dem. Er nettet nede, så er det nede. |
| 38 | I | Jeg tror en bør prøve å se dette operasjonelle, hvordan kommuniserer brukerne? Finn ut av det. Er de avhengige av å kommunisere med HRS, så hjelper ikke LST. Da er det bedre å få et rødt lys, og gå på en fjelltopp for å få det grønne lyset for så å kommunisere. Det er lett for oss med mobilen å se at det ikke er dekning. Da skjønner vi at vi må gå opp et sted for å få dekning. Det er litt den samme tankegangen der tror jeg. Problemet er da at for f.eks. Røde kors som kommuniserer med operasjonssentralen for politiet i det ene øyeblikket og så lokalt i det andre, hvor LST kan være greit fordi du er i en boble hvor du f.eks. leter i den delen av fjellet hvor den LST-basestasjonen har dekning. |
| 39 | L | For du kan ha forskjellige policies for forskjellige brukergrupper, at deres terminaler kan gå i LST og de kan ikke.. |
| 40 | I | Nei, jeg tror ikke du kan sette det på talegruppenivå, du setter det på terminalnivå. Terminalen er lagt inn via software til å enten fungere med LST eller uten. For Røde kors som skal gå inn i Røde kors-gruppe som er gunstig med LST muligens og så inn i samvirkegruppe hvor det ikke er det, men du har fremdeles enablet LST i terminalen. Du får ikke skrudd av LST, det er ikke basert på talegrupper. |
| 41 | L | Det er lag på lag med utfordringer! |

| | | |
|---|---|---|
| 42 | | Det er mye. Det er greit å sitte på et kontor og planlegge det her, men å få det ut krever opplæring, forståelse, du må prøve å få solgt det her inn til brukerne på en måte som de forstår, samtidig som du tar vare på designet. Det er veldig komplisert. Teknisk ikke noe problem, men å få det her til, og at det samspiller slik at beredskapen blir bedre, er vanskelig med så mange forskjellige aktører vi har nå. |
| 43 | I | Et annet, enkelt eksempel, er for de strømselskapene vi har, de som bruker det her til arbeidstalegruppe. De bruker Nødnett når de kommuniserer ute i felt. Har strømmen gått, eller de må reparere noe, og hvis vår BS er nede i det området med LST, så skal de inn og gjøre noe, og skal de si tilbake til sin operasjonssentral at nå må de skru av strømmen. Du er i LST, det hjelper ikke, for de sitter i Trondheim eller hvor de nå sitter, og skrur av den strømmen. Så de ønsker ikke LST, for der har du ikke noe funksjon. Funksjonen kan være at du snakker med kollegaen din, men det kan du også bruke DMO til. Egentlig er det viktige her at de får noen sentralt til å skru av den delen av strømnettet de skal jobbe på. De roper inn at nå skal de skru av, og så går inn og jobbe. Det kan være farlig. Dette er kanskje den enkleste måten å se på det på, med strømmen, at det er farlig hvis du ikke får kommunisert ut. |
| 44 | I | I 5G, om man klarer å sette opp sånne store paraply-BS, kanskje? Jeg vet ikke hvordan det ville fungere. Om du tar Moholt eller en av de store BS i Trondheim som dekker et område, eller om du tar den som står oppe på St. Olavs hospital for eksempel og dekker sykehusområdet og store deler av sentrum, hvordan fungerer den med de 500 andre BS som ligger under der? Så teknisk sett kan det være et problem der. |
| 45 | I | Sånn som det er i dag med LST i TETRA, hvis du har det enablet i terminalen og hvis du kjører fra en BS til en BS i LST, og så til vanlig nett igjen, så gjør denne en handover på nesten normal måte. Den har litt andre terskelverdier for å gjøre handoveren, så hvis du kommer fra et område med dekning så venter den litt lengre enn normalt før du hopper over. På et eller annet tidspunkt hopper du over. Så kjører du inn igjen. Problemet når du er i LST er at den BS som er i LST ikke vet om naboene er i LST. Kommunikasjonen fra BS til terminal sier at dette er naboen min, den har sånn og sånn service. Det går greit når de er tilkoblet, så den BS her ute som du kommer fra vet at den du skal kjøre til ikke er på nett. Den kan si til terminalen at det skal holde så lenge som mulig før den går over. Men den BSen som er i LST kan ikke gi den beskjeden. Den gir beskjed om naboene sine og hvor den skal gjøre handover, men den vet ikke hvilken situasjon naboene er i. Så den antar at når jeg har et dårligere tjenestenivå, så har den neste BS det også. Så den sier at vi er på likt nivå, og den holder helt normalt og gjør en handover til den andre BS, som har normal service. Hvordan optimalisere det her, det er ikke veldig enkelt sånn sett. I 5G vet jeg ikke hvordan det her vil være, men med en gang du mister connection med MSOen så får du ikke en oppdatert situasjon med hva de andre er. Så jeg vil jo tro det blir lignende i 5G. |
| 46 | L | Det var veldig interessant, for du tar det opp til et annet abstraksjonsnivå. Det var nyttig, for jeg har fordypet meg i ting som kanskje ikke er det som kommer til å bli krevende. Så jeg tror det var sunt for meg å få høre det her. |
| 47 | I | Ja, jeg vet jo det selv også at det er lett å gå ned i tekniske detaljer. Du kan gjøre veldig mye fancy, men det er de store tingene du må ta tak i, og så kan du etter hvert begynne å tweake de tekniske detaljene. Det er dette å få den store greia til å fungere som er det absolutt viktigste. Det er som når du tørker et glass, så begynner du ikke med håndkleet. Du hiver ut vannet først, og så tar du håndkleet. Det er veldig lett å finne ut hvordan du skal få den dråpa ut, du vet hvordan du skal gjøre det, men det er ikke det som betyr noe. |

| | | |
|---|---|---|
| 48 | L | Ikke sant. |
| 49 | I | Jeg pleier å bruke veiterminologi når jeg er ute på foredrag og sånt. En BS er egentlig en vei, og på BSen har du busser som er talegrupper, så alle inne i en buss kan prate med hverandre. Kommer det for mange busser på veien blir det sperring, med dårlig kapasitet som du kan bygge ut. LST blir egentlig en vei som ikke er tilknyttet resten av veinettet. Du kan gjøre alt, du har like stor plass og kapasiteten er normal. Du kan fylle på med busser. På et punkt må den ene bussen vente litt før den kan komme inn på veien, men du kan vente litt og så kommer den inn og kjører. Og de som sitter i bussen, det er en talegruppe den bussen, de kan kommunisere internt i den bussen. Inne på bussen kan de ikke prate i munnen på hverandre. Der sitter de og prater og det er flott, og du kan bytte ut de som sitter i bussen. Det kan være en politibuss, og det kan også være en samvirkebuss hvor du har forskjellige folk fra mange forskjellige etater, og de sitter der inne og prater. De kjører på den samme veien. Nå går vi inn på kapasitet og sånt, men veikapasitet er en ting, altså hvor mange felt og sånt du har. Talegruppekapasiteten har ikke noe med bredden på veien å gjøre, men hvor mange som kan snakke inne på den bussen. Der er det 60 sekunder i et minutt som gjelder. Så skal du få det her til å samspille, og som sagt da, hvis du da kjører og det plutselig blir kuttet av, så er resten av bussene på samme vei, men du er på en vei som blir kuttet av av gravearbeid, da kjører du frem og tilbake på den veien i LST-modus. Det kan fungere hvis den veien går til det stedet du skal. Hvis den ikke gjør det, har du et problem. Det er sånn jeg prøver å få solgt det inn til folk som forståelig nok ikke er så interessert i de greiene her. |
| 50 | L | Den var fin! |
| 51 | I | Så det blir det her at du kjører rundt i din egen lille verden. Denne verdenen kunne du også skapt med DMO, laget din egen lille private bane og kjørt rundt der. Det er litt enklere å forholde seg til tror jeg, når du setter opp en DMO-sone. DMO er jo bare da de som er i den talegruppa, den egne bussen. Da skal den bussen inn på en privat bane og kjøre rundt der, og det er ingen andre trenger å bry seg fordi den banen ikke har noe med det offentlige veinettet å gjøre. |
| 52 | L | I 5G har jeg lest litt i spesifikasjoner om at en BS kan virke som en rele-BS til en BS som har mistet dekning. Har du noen tanker om det? |
| 53 | I | Som jeg skjønte det, hvis du har mistet transmisjon til en BS kan du opprette en kommunikasjon via den som er live, er det sånn å forstå, at en del av den kan bli brukt til å kommunisere der. Hvis det er mulig er det flott, fantastisk sånn sett. Da blir det jo ikke noen LST på den, så hvis det fungerer så er det under utvidet dekning, og da vil en bruker oppleve at hvis den ikke klarer å opprette kommunikasjon har den rødt lys, hvis den klarer det har den grønt lys og kan kommunisere. Det er lettere for en bruker, tror jeg, å se grønt og rødt. Hvis det er grønt lys kan jeg kommunisere, om det er rødt må jeg gå et annet sted. Det er nok lettere å forholde seg til, selv om det er varierende at noen ganger får du det, andre ganger får du det ikke. Det er veldig klart og tydelig, rødt og grønt. Så det er absolutt en fordel, hvis det er mulig å få til. |
| 54 | L | Hva pleier være hovedårsaken til at en BS går i LST-modus? Er det hovedsakelig at fiberkabler er kuttet av? |
| 55 | I | Det er stort sett radiolinjer vi har. Det er jo strøm og transmisjon, så strømmen går og så er det at transmisjonen går ned av en eller annen grunn. Det er sjelden at selve radiolinjen går ned, men det kan være feil på utstyr, eller at strømmen på den andre siden går ned. Da forsvinner det her. Også har vi mange såkalte leased lines, der vi leier linjer stort sett av |

| | | |
|---|---|---|
| | | Telenor, og de ruter det gjennom hva som helst, så vi har ikke kontroll der. I og med at de er bygget i en sånn ringstruktur skal du i teorien ha to brudd før det her går ned. Det skjer en del at når vi leier linjer inni en ring, så kan det hende at den ene linja har blitt rutet sammen med den ene enden av ringen. Så går den ned, eller så er det et stort fiberbrudd. Når det er et stort fiberbrudd i et område, så går masse ned. Vi har blitt reddet en del ganger ved at vi går ut på den andre siden av dalen. Som Telenor gjorde sine ting før, gikk det i ethvert dalsøkk en fiberlinje opp som stoppet på den siste gården. Det er sånn det var og det er sånn mobilnettet er bygget, så hvis du har fem BS opp der og den ene linja går, så stopper hele greia. Mens Nødnett brukte penger på å komme seg ut av dalen en annen vei. Så når det er kuttet der nede, kommer vi oss ut den andre veien. Det er ofte vi blir reddet av det, når vi ser at Nødnett ikke er nede. De andre er nede, fordi de er helt avhengige av den, mens vi har tapt redundans, men vi har fremdeles opprettholdt den. Det er ikke bestandig det fungerer, så hvis det var en fibergreie, en større, f.eks. Kongsbergsentralen går ned i Telenor, så har det store innvirkninger på store områder fordi det er veldig mye som går inn der. |
| 56 | L | Det blir et issue når de samlokaliserer radionettet til Nødnett med kommersielle radionett? |
| 57 | I | Det vil jeg tro. Det er sikkert tekniske forklaringer eller gode grunner hele veien her for å velge en kommersiell aktør, men det er jo et tankekors at ingen andre land gjør det her. Hvorfor tør vi å satse på hvem nå det blir? Personlig så hadde ikke jeg turt det. I dag har vi et talenettverk som jeg tror det blir veldig vanskelig å forbedre. Du kan forbedre innendørsdekning og sånne ting, men den hurtigheten og robustheten som er bygget inn i TETRA tror jeg blir veldig vanskelig å slå. Selvfølgelig er data noe helt annet, vi har jo ikke det, så der er det jo store muligheter for å hente gevinster. |
| 58 | I | Jeg pratet med noen som har vært på den litt mer stressa treningen til beredskapstroppen og sånt. Jo mer aktiv, jo mer stresset du er i en situasjon, etterhvert begynner sansene dine å forsvinne. Du står hvertfall ikke med en smarttelefon og ser på et kart, du skal inn i et rom hvor fienden ligger med skytevåpen. Da står du ikke der og trykker på... Kanskje før du går inn at du har droner og sånt som ser det her, greit, men når du er i en stressa situasjon. Først forsvinner alle eksterne ting, PCer og sånt, du klarer ikke konsentrere deg, og etterhvert forsvinner også sambandet. Altså, radiosambandet klarer du ikke få med deg. Det eneste som fungerer på slutten er at folk står og roper til deg. Og så når du er inne i rommet er all energien på den fienden eller hva det er. Du får ikke med deg andre ting, det eneste som fungerer er rett og slett roping. Tenk litt på det her sånn. Hvor er vi, vi er i alle fall leddet rett etter med TETRA. Det er noe som fungerer og er robust. 5G-fordelen her er litt lengre tilbake. En brannmann som står på en stige med en brannslange ser ikke på en skjerm. De har noe på øret muligens, og så er de der. Det er litt den tankegangen der, tror jeg, som er viktig å få med seg. Det er flott hvis du spør innsatsledere, og for de som sitter i ko. For dem så er det her fantastisk, å få dronebilder og alt det her inn, og det er fint. Og så skal det formidles ut til de der ute, og de tror jeg ikke nødvendigvis har det store behovet for noe fancy greier. Du går opp til en person, kan kanskje sitte i bilen og sjekke ut på en pad med bilskilter, men når du går opp på siden av bilen, da må du ha fullt fokus på personen og det du har på øret. Så det å putte alle egg inn en sånn greie. |
| 59 | I | TETRA, terminalene i TETRA, alt, altså standarden og opp, har blitt bygget opp med tanke på beredskapsstyrker. Det har vært tanken. Oppsetningstid fra under 250ms fra Kirkenes til Lindesnes, du kommer inn med en gang, og at det er robust, og at det fungerer. Tankegangen har vært fra beredskap og opp. Det du opplever nå i 5G, vil jeg tro, er at du har noe fancy, noe som har blitt designet for en helt annen brukergruppe, og du skal konvertere det til noe som beredskap skal gjøre. Du kan tweake det, sånn som de holder på med i England der de holder på å pakke inn en Galaxy S5, de holdt på i fire-fem år etter den har gått ut, med å gjøre den robust. Det er bare en enkel liten del. Det kan hende de får opp |

| | | |
|---|---|---|
| | | noen terminaler, det er vel 0,5% av markedet eller noe sånt de snakker om her. Jeg tror mye av tankesettet her er at vi bare kan slice der, vi gir det en slice og så går det her i orden. Det er det vi har hørt på presentasjoner om hvor fantastisk 5G er. Vi bare slicer den, så får dere eget. Så jeg vet ikke om å dele transmisjonsnettverket, er tankegangen der fra MSOen, sånn som [person] jobber mye med, alle de her redundante komponentene som er i dag i MSOen, både fysisk og software-messig skal det fungere hvis det går ned. Har vi noe kontroll på det med [operatør]? Ja, dere har to slicer dere. Nei, det kan godt hende det fungerer veldig bra og alt sånt, men jeg er litt tvilende. Jeg tror det er litt vanskeligere å gjøre det her med å konvertere den veien enn når det er bygget opp fra bunnen av. Og så er det noen som sa i gamle DNK, der Nødnett var før, at de skulle likt å se den justisministeren som slår av Nødnett. Med tankegang på da de slo av FM, hvor mye baluba det var. Når de går inn og sier at nå slår vi av Nødnett for alle brukere, for de får så mye fancy. |
| 60 | I | Folk blir ekstremt fascinert av, de som var ute på Gjerdrum og sånt, det var disse dronebildene. Å, det må vi få inn! Som de sier, noen som har fulgt med sånne hjelmkamera inn i en øvelse, de fulgte omtrent siktet på beredskapstroppen. Hele operasjonssentralen satt og fulgte med på den skjermen. Det er operasjonssentralen som skal ha oversikten, de skal få med seg alt rundt. Med en gang det blir visuelt så strupet de inn, helt tunnelsyn. De fikk ikke med seg meldinger, ingenting som gikk rundt. Så hva var det var viktig for den personen? Det var sånn. Mange av de i operasjonssentralen bare kastet ut det visuelle. De bare hører for å få et balansert inntrykk av hva som skjer der ute, hva det store bildet er. Den lille biten, det er de på taktisk nivå og de på lavt nivå som må håndtere. De har sagt det at hvordan stanse hele operasjonssentralen i Oslo er å sette på en biljakt på TV. Da følger alle med på biljakten, ingenting annet. |
| 61 | L | Nei, det er mye gode innspill du kommer med her. Det er jo en trend til at alle vi snakker med har ganske mye meninger, og det er fryktelig morsomt å høre forskjellige synspunkter. |
| 62 | E | Jeg synes det var veldig forfriskende å høre et litt mer nøkternt syn på hvor fantastisk 5G er. At man tenker litt mer på de faktiske scenarioene der man skal bruke dette nettet. |
| 63 | I | Jada, så alt mulig, med hacking og alt mulig rart er det andre ting. Selv om det kanskje er mer robust. Om du får [operatør] til å knele da, har du plutselig fått hele samfunnet til å knele. Så det som er nå, er å få folk til å prate. Det er ingen som vil høre på oss ingeniører normalt, så vi er bare glade når noen vil høre etter. Det kommer igjen helt an på hvem dere spør, jeg vet ikke hvem dere skal snakke med bortsett fra [person] som jobber med noe helt annet egentlig, som er på teknologi-greiene, mens jeg ser på det på den gammeldagse måten. Jeg har syntes det her har vært ekstremt interessant, for jeg har aldri visst hvordan etatene kommuniserer, hvordan det fungerer der ute, hva det er som er viktig for de før jeg fikk denne jobben her. |
| 64 | L | Mhm. Jeg må si det er et morsomt case å se på for masteren, jeg føler at vi lærer om noe som er samfunnsnyttig og frempå teknologisk samtidig, så det er virkelig morsomt. Er det noe du føler vi burde ha spurt deg om nå, som vi ikke har spurt? |
| 65 | I | Neida, egentlig ikke. Jeg vet ikke helt hvor dere tar denne oppgaven hen. Som sagt er det bare å ringe eller sende mail om det er små spørsmål eller hva som helst, så er det bare å gjøre det. |
| 66 | L | Det er veldig hyggelig, det kan det hende vi tar deg opp på. |
| 67 | I | Det trenger ikke være noe videogreier eller hva som helst, det er bare å slenge ut spørsmål. |

| | | |
|---|---|---|
| 68 | L | Nei, tusen takk for tiden. Det var veldig spennende. Jeg gleder meg til å prosessere dette her. Vi sender deg transkriptet og så får du gå gjennom og se på anonymiseringen vår. |
| 69 | E | Ja, og så får du anledning til å gi innspill om du har sagt noe du gjerne vil trekke tilbake, for eksempel. Takk skal du ha! |
| 70 | I | Den er grei, ha det godt. |

# Appendix I
# Mobile Network Operator C

This interview is conducted with a representative of one of the three Norwegian mobile network operators. Contrary to most of the other conducted interviews which length of conversation spans approximately one hour, this interview spans closer to two. The deployment model favored by the interview subject in this interview is one which involves the utilization of multiple operators' full stacks of services, referred to throughout the thesis as the multi-operator model. In addition to considerations regarding this model in particular, topics of conversation range from general observations about the deployment of commercial 5G networks to concerns regarding the way in which certain deployment models for NGN could risk disrupting competition in the commercial telecom market in Norway at large.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | ... og så spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Ja, det er det. |
| 3 | E | Jeg kan begynne med å introdusere min egen oppgave. Hovedfokuset er på neste generasjons Nødnett og kjernenettet. Hvordan vi skal samarbeide med kommersielle aktører. Med tanke på at vi ikke skal ha et eget radionett sånn som vi har i dag, i Nødnett, så kommer man til å måtte samarbeide med kommersielle operatører om det, og så er spørsmål om hvordan man eventuelt skal gjøre det i kjernenettet. Skal man involvere kommersielle aktører mye der, eller skal man for eksempel ha en statlig MVNO eller noe sånt? Så det er litt ulike vurderinger som gjøres rundt det. Jeg tenker ihvertfall vi kan snakke litt om det i dag, hehe. |
| 4 | L | Hehe, og så ser vi an litt på oppgaven min. Jeg ser mer på den tekniske biten ute i radionettet, der én eller flere basestasjoner mister tilkoblingen til kjernenettet og må fungere autonomt som et cluster av basestasjoner der. Og så ser jeg på det i caset at radionettet kjører hos én av teleoperatørene for å gjøre det litt enklere. Og så både operasjonelle og tekniske utfordringer rundt det, i 5G da. |
| 5 | E | Så vi kan starte litt med deg. Sånn jeg har forstått det så jobber du med deres forslag til hvordan dette kan gjøres i neste generasjons Nødnett? |
| 6 | I | Ja, jeg har vært med på hele løpet der vi har svart på hvordan Nødnett kan løses i kommersielle nett. Det begynner å bli en stund siden, så nå venter vi i spenning på hva DSB og KVUen innstiller på, for det er fortsatt ukjent for oss. Men jeg har vært med på hele den prosessen. På det tidspunktet vi leverte det svaret så anbefalte vi å ikke benytte 5G for Nødnett. Litt fordi det ikke er nødvendig funksjonsmessig, og litt fordi det på det tidspunktet når 5G-nettet ville være tilgjengelig i forhold til tidsfristen, 2025-2026, for å ha et operativt Nødnett. Nå har ting heldigvis skjedd raskere enn det vi fryktet når det gjelder 5G-utrulling. Så vi vil vel være ferdig med en landsdekkende utrulling innen utgangen av 2023, radionettmessig. Det som er spennende da er hvor langt vi har kommet i forhold til å modnes med å bruke network slicing som metodikk, og hvor modne vi er for å eksponere nettverk over mot andre aktører via den her network exposure function som er definert i standarden. Men jeg tror det er viktig å begynne med at det strengt tatt ikke er nødvendig å bruke 5G for å løse Nødnett-behovet. All teknikken finnes ferdigdefinert for 4G, med unntak av den autonome operasjonen og håndsett-til-håndsett-kommunikasjonen. Altså, det finnes som konsept, men det hjelper veldig lite så lenge ingen har tatt seg bryet til å utvikle støtte for det, i verken nett eller håndsett. Det er nok kanskje den største trusselen. At leverandører må utvikle det som trengs. |
| 7 | L | Ja, og der er det kanskje ikke like stor kommersiell interesse? |
| 8 | I | Nei, siden Nødnett i kommersielle nett ikke har vært noen hit så langt. Men vi ser at det ligger foran oss. Det kommer. Flere og flere land antar jeg vil benytte det samme. Korea har gjort det, England har tatt den beslutningen, USA har sitt FirstNet, men alle har en litt annen variant enn det som kanskje er løsningen i Norge da. Det positive er at det ligger noen foran oss. Om ikke så fryktelig langt foran oss, så ihvertfall foran oss i å dytte på de standardene. Jeg kan si litt om det forslaget vi la frem som løsning. Det baserte seg på å for Guds skyld bruke alle radionett, altså nasjonal roaming, men ta ikke på dere som stat å drifte kjernenett. Så kjøp tjenesten hos operatøren. Og det er en litt sånn modell som ligner på den som er gjort i USA. Heller kravstill funksjonalitet og tjenester, SLA-krav, og dra nytte av |

| | | |
|---|---|---|
| | | det utviklingsarbeidet som operatørene gjør hele tiden fremover, fremfor å ende opp i samme situasjon som Nødnett er i nå, at det er utdatert før det er ferdigbygd. Så det er vel litt sånn grunninnstillingen vi har foreslått. Og så er det vanskelig. Det vanskeligste med det er ikke nødvendigvis teknikken, men det å ikke ødelegge mobilmarkedet i Norge for evig og alltid. Det går på at hvis staten går inn og kjøper tjenesten, og da også investerer i spesielt det å bygge dekning der det ikke finnes dekning i dag, og det å robustifisere ett radionett med økt batteritid og økt robusthet for å kunne betjene et Nødnett, så har du for evig og alltid ødelagt konkurransen i spesielt bedriftssegmentet. Ingen vil velge et av de nettene som ikke er benyttet til Nødnett. Så den kommersielle trusselen er nok kanskje den største i forhold til hvilken modell man velger. Ikke nødvendigvis det tekniske. Teknisk sett så er både et MVNO-oppsett der du har et eget kjernenett, eller å kjøpe full stack fra hver operatør, fullt mulig å gjennomføre fra staten sin side. Og da ser vi egentlig varianter helt fra at DSB kun sitter med ansvar for Nødnett-påbygget på toppen, og kjøper hele stacken hos hver operatør, eller at de har sin egen kjernenett-stack, og bare kjøper radionett, da fra enten én eller alle aktører. Så det er egentlig de variantene vi har sett. Og utifra den RFIen som ble besvart for et par år siden, så kom det vel inn svar fra de tre operatørene som dekte alt. Fra at én operatør skulle ta alt, til en MVNO, til vår variant. Så det vanskelige er nok å balansere dette, men det er ikke teknisk. Det vanskeligste er merkantilt, vil jeg vel nesten si, sånn jeg ser på det. Jeg har tidligere sagt, og til DSB, at det vil være tilnærmet galskap å ikke legge til rette for at du skal kunne bruke hvilket som helst radionett som måtte være tilgjengelig på det stedet du er. Vi har allerede i Norge i dag, og det er dere kanskje klar over, prioritetsabonnement for tale. Det er regulert i Norge i dag. Du får SIM-kort som kan benytte alle nett. Men du er selvfølgelig betjent av ett kjernenett, hos den operatøren du abonnerer hos. Men du bruker alle radionettene. Og det er enkelt å få til. Standard roaming-grensesnitt. Det er komplett galskap å ikke legge til rett for det for et Nødnett, som bør ha den beste tilgjengeligheten i landet. Så finnes det et radionett, så bør du kunne bruke det, for å si det litt enkelt. Det er det som har vært, kall det, grunninnstillingen vår. Og det er veldig enkelt å få til. Altså, roaming er man god på. |
| 9 | E | Er det sånn at man har et hovednett som man helst vil koble seg til, og så har man de andre radionettene som fallback? Eller har man en sånn felles PLMN ID eller noe sånt på en måte? |
| 10 | I | Nei, det de har gjort i dag er at du holder deg til det nettet som er hjemmenettet ditt frem til det ikke eksisterer lenger, og så roamer du over på andre nett. Det er med brudd. For det å sette opp nettene slik at du har gjensidig handover, eventuelt samme PLMN-kode, er mye tyngre vedlikeholdsmessig, og gevinsten er veldig liten. Men det er eventuelt varianten. At du er en egen MVNO og har din egen PLMN ID, som da er tilgjengelig i alle tre nett. Men du får litt problemer der du har overlappende dekning. Altså, i veldig stor grad så bygger vi jo nett med basestasjoner på samme sted. Og da må du velge: Hvilket nett og frekvens skal du benytte for din PLMN ID på det stedet? For alle tre vil ha like god dekning. Så hvis du har samme PLMN ID i alle tre nett på forskjellig frekvenslag, så får du et ganske utfordrende trafikkstyringsoppsett for å være sikker på at du faktisk holder deg i det nettet du først har knyttet deg til, og ikke hele tiden hopper mellom nett. Og da begynner det kanskje å koste mer enn det smaker. En av tingene som er viktig for et Nødnett er jo nettopp sikker transmisjon frem til basestasjonspunktet, og ikke minst sikker strømforsyning, slik at du kan holde den operativ selv om strømmen går i lang tid. Det er et av grunnkravene som ligger inne. Overlappende dekning kan selvfølgelig dekke noe. |
| 11 | E | Men den modellen som dere har sett for dere for neste generasjons Nødnett, baserer den seg også på de eksisterende nasjonal roaming-mulighetene? Med kanskje med dere som hovednett for eksempel? |
| 12 | I | Ja, vårt forslag går kort ut på at vi vil at hver operatør skal ha full stack med tjenester. Så la |

| | | |
|---|---|---|
| | | oss ta Oslo som et eksempel da. Da kunne brannvesenet kjøpe tjenesten i fra Telia, og så kunne sykehus og helse kjøpe i fra Telenor, og så kunne politi kjøpe fra Ice. Full stack, men operasjonssentralene på toppen skal snakke sammen. Der er det definerte samhandlingsgrensesnitt, men det er ikke definert at ett Nødnett-system skal håndtere mer enn ett nett i slengen, hvis man tenker sørover med integrasjon mot nettet. Det skal ikke så mye til i standarden for at du skal støtte å bruke mer enn ett nett, men i dag ligger det ikke der. Dette var selvfølgelig det som var spesifisert på det tidspunktet for 4G. 5G er ikke ferdig standardisert i forhold til talebærere enda, og i forhold til det med 5QIer for mission critical-tjenester. Alt dette finnes i 4G-standarden allerede. Så der har du liksom det at det er tilstrekkelig det som er av funksjonalitet i 4G, men vi forutsetter jo at dette vil komme på plass i 5G også, og da kunne du i teorien benyttet deg av slicing som teknologi for å gjøre et ytterligere skille. Men det er strengt tatt ikke nødvendig, fordi det en trenger i radionettet det er prioritet, både til å bli hørt i en celle som er mettet av trafikk, spesielt opplink, og å få brøyte seg vei og kaste ut andre når du har blitt hørt. I mobilnettene i dag så er den vanskeligste situasjonen når håndsettet prøver å ta kontakt, men ikke blir hørt. Altså, når du har opplinksperr og støyen i cellen er så høy at basestasjonen ikke hører deg. Der er det samme mekanisme i 5G som det er i 4G, for å komme seg ut av den situasjonen, og det er access class barring. Hvert SIM-kort tilhører en aksessklasse, og så kan du på et predefinert lastnivå begynne å stenge ute aksessklasser for å begynne å ta ned opplinkklassen. Da får håndsettene beskjed om at nå skal aksessklasse 0, 1 og 2 være stille i 40 sekund, for eksempel. Ingen får gjøre random access. Og på det viset tar du ned opplinkklassen, sånn at prioriterte som tilhører en aksessklasse som ikke får beskjed om å gjøre dette, aksessklasse 11 til 15, de kan sende hele tiden, de blir hørt, og da kan nettet foreta prioritering. Dette er den aller viktigste funksjonaliteten. Det andre er selvfølgelig at når du har blitt hørt, så må du ha prioritetsmekanismer som gjør at du kan bryte andre sine pågående forbindelser og få den kapasiteten du trenger. Alle de mekanismene har du i 4G, og så har du slicing i tillegg i 5G. Det er egentlig, for dette bruksområdet, unødvendig. |
| 13 | E | Fordi man har allerede den nødvendige isolasjonen? |
| 14 | I | Ja, og du har den prioriteten du trenger for å brøyte deg vei. Isolasjonen oppnår du enkelt ved å - Hvis du er redd for integriteten til trafikken din, så er APN-konseptet like sikkert som slice-konseptet. På radio så er slice-konseptet kun et parameter i tillegg til alle de andre QoS-parameterne, så det er ikke noe større skille enn det. Og så kan du selvfølgelig gjøre et mye mer strengt skille når du kommer til kjernenettet, basert på dem, men du er tross alt alltid betjent av det samme, i din slice, AMF for eksempel. Men med slice så kan du da velge kjernenettskomponenter som skal betjene deg for den slicen, og det gir deg en mulighet for eksempel til å kjøpe en slice hos en operatør for ditt formål. Og gjennom det ha dedikerte nettverkselementer. Det kan gjøre sikkerheten rundt drift, tilgang på data, og den type ting bedre. Kanskje spesielt viktig for politi, som ikke vil at andre skal vite hvor de er, og den type ting. Altså, konfidensialitetsdelen av det er lettere å sikkerstille, fordi da kan du ha dedikert driftspersonell som har tilgang til den nettverksslicen sine data og nettverksfunksjonene. Så det er en enklere måte å gjøre et administrativt skille på for å tilfredsstille den typen krav. |
| 15 | E | Kan det tenkes at man skal ha fysiske skiller i datasenter og sånt for eksempel? |
| 16 | I | Ja, det er tenkbart. Men det som er litt kinkig nå er at 5G forutsetter en fullvirtualisert struktur. Så om du kjører funksjonen din på et sett med servere som står innenfor et gittergjerde eller utenfor gittergjerdet, er kanskje ikke det som er det store og hele. For de som kommer seg inn i datahallen må du ha kontroll på uansett. Så sikkerhetskravet til oss som operatører, som er underlagt sikkerhetsloven, er ikke noe mindre strengt for den normale driften. Men det er fullt mulig å gjøre det, å sette opp egne virtualiseringsmiljø for de kjernenettskomponentene som tilhører en spesifikk slice. Men det er klart, alt dette her |

| | | |
|---|---|---|
| | | kommuniserer inn og ut gjennom felles transmisjonsløsninger. IP-nettene er ikke adskilt, fiberne er ikke adskilt. Så det er et spørsmål om hvor nyttig det er, og hvilke trusselaktører du ser for deg og hvilke kapabiliteter de har. Så det er nok mest den digitale sikkerheten som kanskje er den skumleste eller den vanskeligste å holde rede på, mer enn den fysiske. Elektroniske innbrudd er lettere å kamuflere, rett og slett. Men nå har nå jeg bare begynt å bable i vei, jeg advarte dere jo, men dere skal jo få lov til å spørre og om det dere egentlig lurer på, haha! |
| 17 | E | Haha, ja. Jeg har kanskje fått høre noe annet enn det jeg forventet med tanke på fokus på 4G og sånn. Men jeg har et par oppfølgingsspørsmål til det vi har snakket om nå. Blant annet det du nevner at man skal bruke alle tre operatører i kjernenettet. Jeg vil bare se om jeg har forstått det rett. Det høres ganske likt ut som sånn man bruker nettet til kommersiell trafikk til vanlig på en måte, og så får man denne prioritetsmekanismen på toppen. Men ja, la oss si at helse har Telenor og at brann har Telia, og så snakker de med hverandre sånn som en vanlig kunde som har et abonnement hos Telia ville ringe til en kunde som har abonnement hos Telenor. Er det riktig å forstå? |
| 18 | I | Nei, for hvis du ser på push-to-talk-systemet som ligger på toppen, så har det definerte grensesnitt mellom operasjonssentraler, mellom system. Og det som er veldig viktig er selvfølgelig at når man er i samme region, igjen Oslo for eksempel, så skal selvfølgelig brann, helse og politi kunne snakke sammen i samme talegrupper. Og der er det definert sånn at det er én operasjonssentral som har kontroll på én spesifikk talegruppe. Men den kan inkludere brukere fra andre system, som er autorisert for tilgang. Og det er det og definert grensesnitt for: Hvordan du autoriserer inn og ut i grupper, men det vil da bestandig være styrt av ett push-to-talk-senter for å si det litt enkelt. Så for eksempel i Oslo da, så kan du ha brann, politi og helse med deltakere i samme talegruppe. Men da er det styrt av enten brann, politi eller helse. Så vi ser det at dette er, for å være helt ærlig, en mer kompleks struktur. Samtidig, tre uavhengige system gir en totalt sett mye bedre oppetid enn ett system. For det er en av de tingene som er svakheten med det vi har av prioritetsabonnement i dag: Du er fortsatt avhengig av ett kjernenett. Blir det kjernenettet du hører hjemme i borte, da har du ikke tjeneste. Hvis Nødnett legges til én aktør, og den aktøren svikter, så er det ikke noe Nødnett. Hvis det er flere aktører som har full stack med funksjonalitet, så er ihvertfall deler av abonnentbasen oppe. Det betyr at hvis politi mister sin tjeneste, så kan de enten låne en enhet fra brann, eller de kan bruke en brannmann som kommunikasjonsmedarbeider og likevel styre situasjonen. Så det er redundans på et helt annet nivå. Men det kan godt være at den operasjonelle ulempen, kompleksiteten, er så stor at det ikke er verdt det. |
| 19 | E | Og det handler om interoperabiliteten mellom de ulike kjernenettverkene da? |
| 20 | I | Ja, fordi du kommer til å få en avhengighet. Støtter du samme type funksjonalitet? Støtter du det og det? Hva skjer når ett nett har mer funksjonalitet enn det andre? Og likedan, hvis du ser på de større operasjonssentralene som koordinerer alle innenfor et område: Hvilket system skal de bruke? Så vi får være ærlige nok til å si at å faktisk gå full stack hele veien overlater en del kompleksitet til nødetatene som de kanskje ikke ønsker. Og det er nok mer en konstruksjon av hva som vil gi størst mulig konkurranse i dette markedet, om Nødnett-brukere, enn det er DSB sin ønskedrøm om one-stop shopping. Altså det ble vel sagt tidligere: "One throat to choke." Som kan være vel så viktig. Men det er litt sånn: Hvordan sikrer du at nødetatene over tid har det beste tjenestetilbudet? Hvorfor skal man ikke konkurrere om tjenestetilbud? Dette var en av de tingene som FirstNet i USA hadde gjort. De konkurranseutsatte tjenesten. De sa ikke hvordan den skulle produseres. De hadde tolv hovedområder med krav, som operatørene konkurrerte på. Inklusiv det å ha service-punkt for hvor du får nye håndsett, reparerer dem når de er ødelagt, osv. Så det er mer den |

| | | |
|---|---|---|
| | | merkantile kommersielle betraktningen enn den tekniske. |
| 21 | E | Men i en sånn type der man har flere ulike kjernenett, hvem er det som skal ha ansvaret for interoperabiliteten og utvikle de løsningene for det? Er det MNOene som har ansvar seg imellom eller er det noe som DSB skal ta ansvar for, for eksempel? |
| 22 | I | Nei, i vår modell så er det operatørene som er ansvarlig for at dette fungerer. Vi opererte med en term som vi kalte sertifisert operatør. Altså, at du må støtte minimum dette for å kunne være med i konkurransen, og deriblant sette krav til interoperabilitet. Men jeg skal vel innrømme at teknisk sett, så er det enklere å benytte ett push-to-talk-system, kontrollsystem, på toppen, og så bruke nettene under. Det er det strengt tatt ikke støtte for i standarden, men det er en liten tilpasning. Personlig tror jeg at det er veldig lett å få operatører - Altså, her har jeg snakket med ikke så mange leverandører, og dagens leverandør, Motorola, er i stand til å gjøre dette. |
| 23 | E | Så da har på en måte en ekstra entitet helt i den øverste delen av coren, eller er det på applikasjonsnivå? |
| 24 | I | Det er applikasjonen. Jeg kaller det push-to-talk-tjenesten, det er ikke bare push-to-talk, det er video og alt sånt. Det systemet kan håndtere tre nett såfremt de underliggende kjernenettene har støtte for det som trengs. En av de tingene som mangler i dag er multicast/broadcast-støtte i mobilnettet, eMBMS. Det er det ingen som har i Norge i dag. Det er nødvendig for å kunne sette opp store talegrupper raskt og effektivt i nettet, og ikke forbruke for mye kapasitet. Et av kravene, hvis man ser på det, var at talegrupper på hundre pluss abonnenter skulle settes opp innenfor en forsinkelse på 400ms i én celle. Det klarer du ikke hvis du skal signalere opp unicast, altså én-til-én. Det finnes ikke nok tid, det går ikke. |
| 25 | E | Så man kan ha PTT-grupper i liten skala uten MBMS, men for å ha det i stor skala så må man ha MBMS i nettverket? |
| 26 | I | Ja. Hvis du har ulykkessted eller hendelsessted der du har mange first responders, som nettopp dette scenarioet som jeg pekte på, så må du ha det. Du må ta opp en felleskanal, for du rekker det ikke. Og så vet jeg at DSB håpte på at 5G skulle løse det. Jada, man klarer å sette opp flere, fordi du har gått fra scheduling på 10ms til 1ms. Men du har fortsatt ikke nok tid, hehe. Så du rekker det ikke, rett og slett. Og det er en enorm sløsing av radiokapasitet. Helt unødvendig stor sløsing av radiokapasitet. Fordi det som da skjer er at du fortrenger alle andre brukere i cellen. Sett opp en nedlink talekanal som alle skal høre på, istedenfor å sette opp én-til-én. Så det er vesentlig enklere og billigere å implementere eMBMS enn det er å kjøre det sånn. En av de tingene som er kostbart med eMBMS i 4G-nett, det er det strenge kravet til tidssynkronitet mellom basestasjoner. Du sender det tross alt samtidig. I 5G så er det et grunnleggende krav med tids- og fasesynk som langt overgår det som er nødvendig for broadcast. |
| 27 | E | Så terskelen for å innføre MBMS blir kanskje lavere da i 5G, er det det du mener? |
| 28 | I | Ja, for vi må uansett ha på plass den strenge tids- og fasesynken, så den kosten er allerede tatt. For det har vært det store for 4G. At du i teorien måtte ut med en GPS-antenne på hver basestasjon. Det er dyrt, det er det ingen som tar seg råd til. Når du har den tids- og fasesynken som nå blir spredt gjennom de faste transmisjonsnettene ut til basestasjonene, så er det kostelementet borte. Og da snakker du om en relativt beskjeden investering i funksjonalitet i radionettet, som allerede er der, og en eMBMS-server, en sentral funksjon. Så da er det plutselig enklere. Men jeg vet at dette er veldig forskjellig utifra modenheten på 5G. Hos oss for eksempel, i Norge, vi skal være fullmodernisert innen utgangen av 2023, |

| | | |
|---|---|---|
| | | nobrainer. Sverige vil ikke være fullmodernisert. Finland? Kanskje. Altså, Sverige ser på eMBMS som en kjempekostnad fordi de fortsatt vil ha en del basestasjoner som ikke har 5G, som ikke har den synkroniteten som skal til for å kunne støtte broadcast. Så det er sånne tekniske ting da, som endrer seg til Nødnettets fordel kan man kalle det da. |
| 29 | E | Nå var liksom utgangspunktet at man skulle opprette NGN i 4G, er det med å få til eMBMS en kost som operatørene må ta på seg eller er det noe man tenker at man kan få statlig støtte til på lik linje med robustifisering av nettene? |
| 30 | I | Altså i vår modell, det vi kalte å være kvalifisert tilbyder, så er det noe som tilbyderne måtte ta selv. Både det og det å tilstedebringe et push-to-talk-system, og så full stack. Vi så på en kost i størrelsesorden 100 millioner for å bli Nødnett-ready, uten å ha fått en kontrakt enda. Så det er ticket to play da. Men det er basert på at du må tilrettelegge for en del funksjonalitet i nettet for at det skal fungere. Men, jeg skal vel innrømme at jeg er særdeles usikker på om dette er en modell som vil bli valgt. Jeg tror at teknisk sett, så er det mer sannsynlig at det velges en løsning med bruk av tre nett og en eller annen form for - Enten å bruke tre kjernenett med ett tjenestelag på toppen, som er det mest robuste du kan gjøre, for da er du ikke avhengig av ett kjernenett. Eller at DSB velger å kjøre et MVNO-oppsett, men da har du innført en sårbarhet med at du har ett kjernenett. Det spiller liten rolle om det er huset hos en operatør eller kjørt separat. Svakheten er den samme. Du har ett kjernenett. Når det kjernenettet svikter, for det skjer, så er nødnettet ute. Hvis du har tre kjernenett, altså tre fulle mobil-stacker, og har tilgang til det - Du kan godt velge deg ett primærnett per region, og så kan du diskutere hvor stor en region skal være. Og her er det selvfølgelig operatøren som prater igjen, for de er livredd, det må jeg si, for at det skal velges en én-operatør-løsning. Selv om den operatøren kan være oss, så mener vi at det ikke er bra for konkurransen i Norge. Det er ikke bra for markedet om det velges én operatør. Spesielt de store pengene som må sprøytes inn for å få et robust radionett, og ikke minst bygge dekning der det ikke er dekning i dag. Den vil forskyve bedriftsmarkedet for evig og alltid, og det er ikke bra. Selv om vi skulle få avtalen, så er det ikke bra for markedet. |
| 31 | E | Kan det tenkes at man får en sånn modell som - Nå må du bare korrigere meg hvis jeg tar feil, men i Sverige bygger de ut ekstra dekning med forbehold om at den ekstra dekningen som blir bygget, selv om man holder seg til ett radionett, så kan også de andre operatørene benytte seg av de nye mastene. |
| 32 | I | Ja, det er en variant som tar ned forskjellen. Det fikser litt på dekningen, for å si det sånn. Det kan du gjøre med et multi-operator core network-opsett, et MOCN-oppsett der alle får tildelt sin del og bruker sine frekvenser. Men det er fremdeles sånn at du må komme deg til punktet med en transmisjonsløsning. Det er dyrt. Det er en grunn til at det ikke er dekning der, for å si det sånn. Det å grave fiber ut til sånne lokasjoner er kjempedyrt. Og så er det robust fremføring av fiber, altså to veier. Eller at du har to basestasjoner som dekker samme område, for å ikke måtte ha to veier. Da er det plutselig sånn at hvis én aktør har bygget det, skal man da leie av den aktøren, og hvordan får man en fair pris på det? Det er ikke ukjente problemstillinger i dag heller. Men det er en mulig mitigering av den dekningsforskjellen, men det er én del av robusthetsspillet da. Hvis du blir valgt som hovedleverandør til Nødnett i et helt land, så har du forskjøvet konkurransefordelen. Det går på kjernenettrobustheten, det går på driftsrobustheten og oppetidskravene for hele nettet. Som vil være en sånn forrykkende konkurransefordel. Og den er langvarig, for hvis du går på bare én operatør så har du ikke et fungerende marked for nødkommunikasjon. Da har du bundet deg til masten de neste 20 årene, ikke sant. |
| 33 | E | Du tenker at man får en veldig tydelig teknisk lock-in effekt? |

| | | |
|---|---|---|
| 34 | I | Ja, fordi det er én aktør som har tiltrukket seg alle pengene til å robustifisere og tilrettelegge og lage løsninger. Og når du er der, så blir det gjerne i lange kontrakter. Jeg kan eksemplifisere det med å si at vi har vunnet en kontrakt for å kjøre t-banen i Oslo, der signalnettet skal erstattes med mobilnettet. Relativt høye oppetidskrav, og en kontrakt som går frem til 2052. Sant? Så det er ikke konkurranse, etterpå. Og det er nok ikke sånn at når staten skal ut å kjøpe Nødnett, at de signerer en femårsavtale, hehe. Men alt dette har veldig lite med teknikken å gjøre, men alt med konkurransesituasjonen å gjøre. Så vårt hovedargument har egentlig vært å finne løsninger der du kan ivareta statens behov for Nødnett i de kommersielle nettene, samtidig som du ikke ødelegger mobilkonkurransen for evig og alltid. Så våre tekniske svar er innrettet mot det, for å si det sånn. |
| 35 | E | Men som vi nevnte tidligere: Hvis vi ser litt på andre land som har kommet lenger i prosessen enn oss, så er det ofte én operatør eller - For eksempel i Storbritannia så har du EE som leverer nettet og nedre del av coren, i Finland så har de Elisa, og i USA så har de AT&T, selv om det også finnes andre nødnettilbydere enn AT&T i USA. Hva tenker du om - |
| 36 | I | Ja, responsen i USA var ganske interessant. For når FirstNet fikk avtalen der, så gikk de nest største ut og sa "Neinei, selvfølgelig skal vi bygge nødnett. Vi trenger bare ikke statlige penger." Det er fordi det er umulig å ikke tilby det. Fordi da har de tapt konkurransen for evig og alltid. Og det er nettopp den typen dynamikk - Altså, for å si det sånn: Hvis Telia skulle få en avtale på Nødnett i Norge, så er helt utenkelig at Telenor ikke ville svare på det. |
| 37 | E | Ja, med sin egen type løsning på en måte? |
| 38 | I | Jepp. Helt utenkelig. Fordi det ville rykket balansen i bedriftsmarkedet, særlig, så hardt over i Telias hjørne at de ville være nødt til å foreta robusthetsinvesteringer i sitt nett. For å kunne si at de har det samme. |
| 39 | E | Så ikke for å tiltrekke seg Nødnett-type kunder, men for de andre kvalitetene som det å være Nødnett-tilbyder gir til nettet? |
| 40 | I | Ja, for at ikke Telia skal si "Jamen, herregud du kan jo ikke bruke Telenor! Vi kjører Nødnettet, det er det mest robuste som finnes. Kom til oss!" I tillegg har de fått milliardsubsidier for å bygge det nettet, ergo skal de konkurrere hardere på pris. Dette er å forrykke markedet med statlige midler noe helt enormt. Derfor mener vi at det er helt feil. Selv om det skulle tilfalle oss, hehe. Altså, det er ikke bra for markedet. Og etter det hadde vært gjort, så ville DSB vært hos Telia de neste 20 årene. Psh, hvor interessert trenger de å være i videreutvikling? Nyte god tjeneste? Hele tiden forbedre produktet? De kan ikke skiftes ut. Det er ingen tilstedeværende konkurranse. Så det er den største trusselen, og det vanskeligste området å løse i forhold til neste generasjons Nødnett. Teknikken er ikke vanskelig. Noen områder av teknikken er vanskelig fordi leverandøren ikke ser ut til å utvikle løsninger som er standardiserte, men det er en annen sak. Det å tilstedebringe en erstatning til dagens Nødnett, bortsett ifra ProSe-funksjonaliteten, den håndsett-til-håndsett- og den autonome basestasjonfunksjonaliteten, det finnes det allerede teknologi og mekanismer for. Vi kan gjøre det i 4G, vi kan også gjøre det i 5G. Den der ProSe, den er ikke der, rett og slett. Det er den største utfordringen. Ikke det at den ikke finnes spesifisert, men den finnes ikke implementert. |
| 41 | L | Men har dere satt dere inn i og sett på autonome basestasjoner? Har du noen tanker knyttet til autonom operasjon av basestasjoner fremover? |
| 42 | I | Ja, den største utfordringen er nettopp dette med at det baserer seg på en del funksjonalitet, som ligger i den ProSe-standarden også, spesielt rundt autentisering og |

| | | |
|---|---|---|
| | | kryptering og håndtering av nøkler. Det å holde på konfidensialiteten, og ikke minst det å være sikker på at den du prater med er den du tror det er. |
| 43 | L | Bare for å være tydelig nå. Snakker vi om device-to-device eller snakker vi om - |
| 44 | I | Begge deler. Fordi i det øyeblikket en basestasjon mister kontakt med omverdenen, så har den ikke tilgang på fornying av nøkler eller å sjekke at den nøkkelen du kommer med er gyldig. At du er den du utgir deg for å være. |
| 45 | L | Ja, så det er synkronisering av typ autentisering mellom kjernenettet og edge-siten som er hovedutfordringen? |
| 46 | I | Ja, så hvordan skal du sikre det. Du kan alltids si at de som allerede er oppe å kjøre på basestasjonen har autentisert seg, har hatt kontakt med det sentrale autentiseringssenteret, har fått nøklene verifisert. Der er du relativt sikker på, selv om du bruker nøkkelen over lengre tid, at det fortsatt er den samme brukeren. Men hva skjer når det kommer én brannmann til inn og skal på nettet? Hvordan vet du at dette er riktig nøkkel? Hvordan vet du hvilke talegrupper han har tilgang til? Hvordan vet du hvilke autorisasjoner han har til å kommunisere med alle andre? Hvordan vet du at det ikke er en som er ute etter å ødelegge alt? Ikke sant? Hvordan gjør du det? Og du kan ikke ha all den type data lagret på en basestasjon til enhver tid. Det går ikke. Du vet aldri når bruddet kommer. Derfor så er dette vanskelig. |
| 47 | L | Så vi ser på i 5G - for i Nødnett i dag så er det autonom operasjon på enkeltbasestasjoner, sånn 15% av dem eller noe sånt. Men i 5G så blir celletettheten så mye større at vi ser på å ha autonom funksjonalitet for et område, et subsett av basestasjoner, så da blir det å kjøre - |
| 48 | I | Ja, men da tror jeg dere skal tenke over én ting. 5G kommer til å være utbygd i Norge uten at det er bygget en eneste ny basestasjon omtrent. Celletettheten i Norge går ikke opp. |
| 49 | L | Hva mener du nå? |
| 50 | I | Altså, hvis du ser på sånn vi bygger nett. Frekvensene vi bygger nett på i dag, der er den høyeste 3,7 GHz. Der bygger vi ut på eksisterende stasjonspunkt i by. Det site-griddet er tett nok. Neste hakk ut, suburban, altså nær by, der bruker vi og 3,7. Da begynner det å skorte litt på rekkevidde, så det vi gjør da er at vi kombinerer det med 5G i 700 MHz for opplink. For det er opplink rekkevidden som bestandig er begrensende. Så da bruker vi 700 opplink, og så bruker vi 3,7 nedlink. Plutselig har vi et dekningsområde som ligner på det du har på 1800 MHz igjen. Da har du nådd suburban. Og så skal vi ut i rural, ut på bygda, der vi kun har lavbånd: 700, 800, 900 MHz. Det vi gjør da: 5G på 700. Etter hvert: 5G på tilleggsfrekvenser, men ikke på millimeterbånd. Det har ingen hensikt. Så der du vil se en økt celletetthet på 5G er innomhus først. Industrielle applikasjoner som trenger voldsomt med kapasitet. De løsningene som er skissert bruker blant annet Nokia, som har konsept for at du kan sette 5G i 26 gig på lyktestolper og den slags og bruke det som aksess inn i hus. De aller fleste plassene i Norge der det vil være aktuelt å gjøre det, i avstand, har fiber. Der dette blir for langt, altså litt over 300-400 meter, da kan du ikke sett opp én sånn basestasjon for hvert hus. Du må frem til fiber til det punktet uansett. Det man bruker da? 3,7 GHz. Pluss alle andre frekvensressurser under 6 GHz som vil komme. Og mekanismen som vil bli brukt, spesielt i begynnelsen, er dynamisk spektrumsdeling, som gjør at man kan kjøre 4G og 5G i samme frekvens samtidig. |
| 51 | E | Det blir en sånn god balanse mellom rekkevidde og kapasitet da? |

| | | |
|---|---|---|
| 52 | I | Ja, altså i begynnelsen så har du ikke så stor penetrasjon av 5G-håndsett. Så det er ikke så mange som trenger kapasitet. Men du har veldig mange på 4G, så vi har ikke råd til å ta et helt frekvensbånd og gjøre det om til 5G. Og da er det den dynamiske spektrumsdelingsmekanikken som gjør at du kan kjøre - For rammestrukturen er veldig lik mellom 4G og 5G, og det er standardisert slik at 5G-håndsettet ser 4G og 5G, mens 4G-håndsettet bare ser 4G. Og her er det faktisk broadcast-mekanikken som brukes til å skjule 5G fra 4G-brukerne. For på radiogrensesnittet har du muligheten til å si til 4G-håndsettet at "Ikke lytt på disse kanalene her, for de er satt av til broadcast, altså eMBMS." Men vi bruker de ikke til eMBMS, vi bruker de til 5G. Det er mekanismen som DSS benytter seg av for å stacke 5G inn i 4G-dekning. Og da har du 4G og 5G i samme frekvensbånd samtidig, og den er dynamisk. Så den er ikke statisk avsatt, men er avhengig av hvor mange 5G-brukere du har i cellen og hvor stor etterspørsel du har etter 5G, og gjerne ressursfordeling. Men den er selvfølgelig saktere enn om du har en ren 5G-bærer. Så det er nok det vi kommer til å se, jeg tenker i det tidsrommet her, der vi ser at Nødnett må være ferdig og satt opp til testing og sånt i 2025. På det tidspunktet tviler jeg på at Norge har bygget veldig mye småceller. |
| 53 | L | Ihvertfall i min oppgave så scoper jeg det frem til at vi ser på 5G standalone, så det er jo på et større tidsperspektiv. |
| 54 | I | 5G standalone kommer nå. Vi vil ha 5G i standalone i 2022. En av grunnene til det er nettopp å kunne gi 5G til hele landet. Som nevnt har vi en del siter som vi kjører kun lavbånd på, altså 7-, 8- og 900 MHz-frekvenser. Og da er det dessverre sånn at du ikke klarer non-standalone. Håndsettene klarer ikke å ankre for eksempel i 900 og kjøre 5G i 700, eller motsatt. Det er for tett i frekvens. Og så har du intermodulasjonsprodukt. Så det som er i bruk i dag i non-standalone er gjerne at du ankrer i 1800 MHz, og så bruker 3,4 til 3,8 til 5G. Eller, du kan bruke for eksempel 1800/700, altså andre frekvenser. Så det er visse frekvenskombinasjoner som er støttet i begynnelsen, og så blir det flere og flere av dem. Men det betyr at hvis vi i Norge skal ha et landsdekkende 5G-nett, så må vi faktisk ha standalone. Fordi vi må være i stand til å kjøre 5G i et område som bare har 7-, 8- og 900 MHz-dekning. |
| 55 | E | Så da er det enklere å ha en sånn dual core-løsning der man har 4G og 5G hver for seg? |
| 56 | I | Ja, og da er det sånn at hvis du blir 5G standalone-kunde, da er du 5G standalone-kunde, men du får selvfølgelig tilgang på 4G radioaksess. Og derfor så kommer det tidlig. Og du ser at pushet er stort. Finland, for eksempel, de har startet med 5G SA allerede, Elisa. Så er det ikke så utbygget enda, det er mest for å kunne skrive i avisen at du har det. Men det kommer, og det kommer raskt. Det kommer raskere enn vi trodde bare for et år siden, for å si det sånn. |
| 57 | L | La oss gå tilbake til disse basestasjonene. Så ihvertfall i første omgang så kommer ikke cellestrukturen til å endre seg så mye, så du tenker at det fortsatt kommer til å være en verdi av å ha autonom funksjonalitet i enkeltbasestasjoner, kanskje de med større range i urbane strøk ihvertfall? |
| 58 | I | Ja, du kan velge ut noen, siden det er ganske mye overlappende dekning. |
| 59 | L | Men hva tenker du ellers er de hovedutfordringene som må løses på veien mot å implementere det for dere? |
| 60 | I | Det er tilgjengeligheten av funksjonalitet. |
| 61 | L | Ja, hva legger du i det? |

| | | |
|---|---|---|
| 62 | I | Det er kun det. Og så er det sånn at det kanskje ikke er i byene du vil se størst nytte av autonom operasjon. For i byene så er det så stor grad av overlappende dekning mellom basestasjoner. |
| 63 | L | Men se for deg at Ålesund by blir kuttet av fra omverden for eksempel. |
| 64 | I | Ja, du tenker at hele byen blir isolert? Ja, absolutt. Da har du i teorien mulighet til, i mangel av full autonom operasjon, å på forhånd bestemme regioner som skal klare seg autonomt, gjennom å dytte ut nettverksfunksjoner til regionen. Altså, nærmere brukerne. Det er en mulighet som finnes i 5G. |
| 65 | L | Ja, og da blir hovedutfordringen å holde autentiseringen oppdatert. |
| 66 | I | Å holde det synkront. Rett og slett. Sånn at alle brukerne innenfor det geografiske området faktisk har sine data lokalt. En kopi av dem. Og så er det bestandig sånn at når du skal begynne å spre informasjon der du har hemmeligheter, altså autentiseringssenterne, utover, så øker risikoen for, kall det, lekkasje. |
| 67 | L | Ja, overflaten blir større liksom. |
| 68 | I | Ja. Men når du går autonomt trenger du ikke nødvendigvis å bruke dine vanlige nøkler. Så du trenger ikke å eksponere dine dypeste hemmeligheter. Så hvis man har muligheten til å predefinere områder, så kan man gjøre ting med kjernenettet, som gjør at du ikke trenger den autonome basestasjonfunksjonen, for da har du et kjernenett. Men vi er helt avhengig av at hvis dette skal kunne fly ute på basestasjonsnivå, så må leverandørene ta det frem først. Det har vært noen år nå der ProSe har vært spesifisert, men det er null interesse for å ta det frem. |
| 69 | L | For kommersielle bruk så har det vel ikke så stor nytteverdi. |
| 70 | I | Nei. Det er ingen som er villig til å betale for noe sånt. |
| 71 | L | Men det kommer vel frem nå da? Ihvertfall så vet jeg at tilsvarende ProSe i Nødnett er kjempemye brukt, så det vil bli behov for det i en kommersiell løsning. |
| 72 | I | Ja, men det er nok mest i en Nødnett-setting. Det kommersielle tilsvaret er gjerne at bedrifter setter mer av sin bedriftskritiske kommunikasjon over på 5G, og løsningen på det er at du får lokale kjernenett. |
| 73 | E | Ja, private 5G-nett da? |
| 74 | I | Ikke nødvendigvis private, men lokale kjernenett. Vi gjør det, vi tilbyr private kjernenett som vi drifter. |
| 75 | L | Blir det i praksis egentlig samme grunntanke som å kjøre et kjernenett som kan fungere autonomt? |
| 76 | I | Ja, det fungerer helt autonomt. Så vi kjører allerede nå for gruvedrift i Sverige, men og satt opp i Norge, der de kjører dumpere og gravemaskiner og bruker 5G og 4G med lokalt kjernenett, fordi du må ha veldig lav latency. Og så sitter de utenfor og styrer, det er med kameraer altså. Den typen bruksområder krever lokale kjernenett. Vi ser også på når industrien skal ta i bruk 5G som bærer istedenfor kablet infrastruktur, så vil du trenge det lokale kjernenettet. Både for kapasitet, og ikke minst for driftssikkerheten. De må tåle å bli |

| | | |
|---|---|---|
| | | isolert uten å måtte legge ned produksjonen. |
| 77 | L | Så sånn sett blir det litt kommersielle behov for å utvikle den teknologien her da? |
| 78 | I | Ja, men da bryr du deg ikke så mye om autonome basestasjoner og håndsett-til-håndsett-kommunikasjon. Det bryr du deg ikke om. Du bygger robust dekning med overlappende basestasjoner, så du løser radiosårbarheten på det viset. Og så løser du kjernesårbarheten med å bygge kjernenettet veldig nærme der du trenger det. Og så vil vi se med 5G, en kombinasjon av at der du trenger lav latency men det ikke er så nøye med - Så får du edge computing. Så akkurat den kommersielle bruken av håndsett-til-håndsett-kommunikasjon har vi ikke noe etterspørsel etter, ikke engang i sykehussetting. Vi har hatt mye diskusjon med Norsk Helsenett og sånn, og Sykehuspartner, og det som vil løse behovet deres er lokale kjernenett. Fordi du trenger å kommunisere med flere som ikke nødvendigvis er innenfor din basestasjon sin dekning. Ergo så trenger du et eller annet sentralsystem, og du trenger noen som kan kontakte alle. Meldingssystem eller tale. |
| 79 | L | Use caset du tenker på nå er redundans i et sykehusområde? |
| 80 | I | Ja, på et sykehus for eksempel. |
| 81 | E | Men da har man ikke noe sånn sentral kjerne et annet sted som man liksom må synkronisere med? |
| 82 | I | Jo, det finnes begge varianter. Ta for eksempel Oslo som et godt eksempel. Sykehusene i Oslo har vel tre hovedlokasjoner, og 72 andre lokasjoner i Oslo. Du kommer ikke til å installere lokalt kjernenett på 72, men på de store sykehusene så kan du gjøre det. Og det betyr at det vil være et samspill, og det er da kanskje slicing er et godt konsept. Da kan du si at "Ja, vi har slice nummer 8. Den eksisterer på Ullevål. Og hvis du har et SIM-kort som er provisjonert med slice 8 så tilhører du kjernenettet der når du er der." Og det kjernenettet kan og betjene de 72 andre lokasjonene. Eller, du kan ha samme type funksjonalitet i makronettet i de 72 andre lokasjonene. På sine egne slicer i det store nettet. Så det er mange måter å sy sammen dette på i et 5G-system. Krukset er bestandig: Hvilke tjenester er du dønn avhengig av i krisesituasjon? Og jeg ble overrasket selv da jeg hadde den diskusjonen med sykehus. Paging. Det er det viktigste. Få tak i legen. "Dr. Johnsen til operasjonsstue 4, takk!" Det er det viktigste. |
| 83 | L | Vi har vært i tilsvarende dialog med nødetatene for å prøve å finne ut av: I den isolerte konteksten, hva er det som er tjenestene de trenger der ute. Så det er interessant å høre at det er samme problemstillinger som er i litt forskjellige caser. |
| 84 | I | Ja, men det er et veldig interessant spørsmål å stille. Hvilken kommunikasjon trenger du i den ytterste krise. Hva er det minste du kan klare deg med? Så jeg ble overrasket over svaret. Jeg hadde aldri tenkt på at det var paging, haha. Men det er klart, for en brannmann som er inne i et brennende hus, så er det helt andre kommunikasjonsbehov, han må snakke med de på utsiden. Men det kan være at andre - I en mer kommersiell setting så trenger du å nå en større del av verden. På en byggeplass trenger du kanskje å nå kranen, så det kan være interessant. Å kunne operere i walkie-talkie-modus. Så jeg sier ikke at det ikke finnes i det hele tatt, altså, bruks-case der autonome basestasjoner eller håndsett-til-håndsett kan ha nytte, men vi har ikke sett noen stor etterspørsel etter det. |
| 85 | L | Mm, nei, men det gir mening. |
| 86 | E | Hvis vi tar det sykehuseksempelet og overfører det til en Nødnett-sammenheng: Vil det |

| | | |
|---|---|---|
| | | være for ressurskrevende å bygge ut regionale kjernenettverk? Ikke lokale, men at man kan få på en måte regioner der man har egne kjernenettverk? Vi var litt inne på i sted at du får synkroniseringsproblemer, men det vil jo være det samme som i et sånt sykehus da, eller? |
| 87 | I | Ja, det spørs litt på hvilket du nivå du tenker. Hvis du tenker på oss som kommersiell aktør for alle kundene våre, å sikre en region, for å si det litt enkelt. Det er mulig. Men igjen, hvis du ser på hva 5G muliggjør i konsept utifra standardiseringen, så er det mulig. Men, noen må implementere løsningen. Hvis man ser på de mest sentrale komponentene da: Autentisering og UDR/UDM, altså abonnentdataene dine, samt en ofte oversett funksjon: Dagens PCRF, morgendagens PCF/CHF, altså policy-kontroll. Det å sette opp bærere, nettverksinitierte bærere, er PCFen nødvendig for. Det vi ser er at leverandøren ikke enda har klart å ta frem løsninger for hvordan man skal klare å synkronisere nødvendige data mellom mange siter. Vi har i dag løsninger for tilsvarende, altså HSS/HLR, felles nettverksdatabaser og PCRF i 4G-nettet. Det leverandøren klarer er tre-sites-løsninger. Skal du skalere noe mer enn det, så går det ikke. Da må du begynne å splitte opp. Det betyr at du aldri kan tilhøre mer enn et cluster på tre noder. |
| 88 | E | Og da er det sånn at man har tre noder på hele landet, for eksempel, eller? |
| 89 | I | Ja, og dette er noder som er på hele landet. Og da kan du selvfølgelig si at "Ja, da kan vi jo plassere ut sånne da." Rundt omkring. Men, folk holder seg nå ikke i ro. Så når du flytter deg fra Oslo til Trondheim, og du har ett kjernenett i Oslo og ett i Trondheim. Hvordan flytter du denne dataen med deg? Hvis ikke er det ikke autonomt. |
| 90 | E | Når du sier leverandør er det Ericsson, Nokia, den typen leverandører? At det er deres oppgave å løse dette problemet isåfall? |
| 91 | I | Ja, for dette er et grunnleggende systemarkitekturproblem. Og du har flere: Oracle, ja, alle som er i denne leverandørsfæren og som prøver å løse disse problemene. Ingen synes å ha løst - For det som er vanskelig er det store behovet for synkronitet i normaldrift, samt å være sikker på at du har dataen på riktig sted når det går galt. Og da må de i utgangspunktet synkronisere alt overalt hele tiden, eller å være smart med å detektere hvem som flytter seg til hvor, og på et visst tidspunkt migrere data over. Men hver gang du legger til rette for den mekanismen, så har du ett grunnleggende problem. Fordi de sentrale databasene som dette egentlig er. HSS for eksempel i 4G, UDM i 5G, den er der for at nettet skal klare å finne deg. Det er ett sted å spørre: Hvor er denne enheten? Men hvis du i utgangspunktet må vite hvor enheten er for å spørre hvor den er, da har du tapt litt. Og så har jeg vært med i dette gamet så lenge at vi har vært i en situasjon at vi hadde ikke mindre enn 9 forskjellige HLRer, der kunden tilhørte kun en av dem. Hver gang kunden skulle nås måtte du finne ut hvilken HLR de lå i. Da får du igjen et sentralt nettverkssted som kan vite dette og rute det til riktig sted. Da har du en ny sårbarhet. Dette er det som er vanskelig med distribuerte data. Vi har noen nettverksløsninger som er nærmere å kunne løse det. Vi bruker Nokia. De har en databaseløsning som de kaller One-NDS, som er en veldig skalerbar løsning. 100 millioner kunder inn der, det spiller ingen rolle. Hele tiden faste byggeblokker. Men de har bestandig en ruting-instans. "Ja, du kan spørre meg, så vet jeg hvem du skal spørre, og så vet han hvem du skal spørre og så -" Altså, du får det er treet for å skalere. Samtidig så må du bestandig ha et første punkt å gå til. Og dette er vanskelig i fulldistribuert arkitektur. Når noen data, av natur, er - Du må spørre i kartoteket, hvis ikke vet du ikke hvor det er. Det kommer sikkert løsninger på det, men i dag er det ikke mulig å bygge nett sånn. Ikke effektivt. |
| 92 | E | Hmm, jeg tenker litt sånn at hvis man har en sånn autonom situasjon der man tenker at det å ha distribuerte data blir for vanskelig. Går det an å tenke seg at man har noen predefinerte autentiseringsklasser, for eksempel basert på håndsettene - At dette håndsettet har, hvis det |

| | | |
|---|---|---|
| | | ikke har tilgang til HLRen, så har dette håndsettet likevel noen predefinerte klasser som det har mulighet til å være med i disse talegruppene for eksempel. Er det noe som går an? |
| 93 | I | Ja, men talegruppen blir borte da. |
| 94 | E | Ja, men at man har den PTT-funksjonaliteten og alt det der finnes jo der på en måte fremdeles. Det kan man ha selv om man ikke har tilgang til dataene tenker jeg. |
| 95 | I | Ja, men push-to-talk baserer seg på én ting. Du trykker du prater, data sendes ett sted og så distribueres. Når du er isolert. Du kan trykke, du kan prate, men det sentrale stedet er der ikke lenger. |
| 96 | E | Nei, men da vil det sentrale stedet på en måte være basestasjonen da tenker jeg. |
| 97 | I | Ja, da må den ha den funksjonaliteten implementert på det stedet. |
| 98 | E | Men kan man ikke ha den funksjonaliteten implementert uten å ha tilgang til subscriber-informasjonen? |
| 99 | I | Jo, for subscriber-informasjonen går litt på talegruppen du skal tilhøre, men som sagt, du kan predefinere. Så lenge du har kontroll på håndsettene. Men, det vanskelige er å kryptere radiogrensesnittet. Fordi det forutsetter at du har en delt hemmelighet. Og at du kan gjøre gjensidig autentisering. Du autentiserer nettet, nettet autentiserer deg. Så bestandig når du går over i sånne situasjoner, så går du over i en økt risiko for at noen ikke er den de utgir seg for å være. Tenk over i dagens situasjon: Falske basestasjoner. Så i den grad du tillater autonom funksjonalitet i nettet, så må du være klar over at det er en angrepsvektor. For eksempel kan jeg da som fremmed stat sette opp en autonom basestasjon utenfor Stortinget, og utgi meg for å være Telia sitt nett og tiltrekke meg kunder. Hvis det da er mekanismer for å etablere den kommunikasjonen med kjente parameter, så har du en risiko fordi du avlytter all tale som går, fordi du kan videreformidle den. Den eneste beskyttelsen man har mot dette i dag er den delte hemmeligheten som aldri kommuniseres. Som er ukjent. |
| 100 | E | Som man får sentralt? |
| 101 | I | Ja, den ligger lagret to plasser: På SIM-kortet og i vårt autentiseringssenter. Og den går det ikke an å hente ut i klartekst. |
| 102 | E | Og det å skulle distribuere den hemmeligheten utover, det blir en sikkerhetsrisiko? |
| 103 | I | Det er en sikkerhetsrisiko i seg selv. Men ikke umulig. Men da er det litt sånn, hehehe. Og så kan du ikke ha alle på hver basestasjon, så hvordan bestemmer du hvilke du skal ha på basestasjonen til enhver tid? Men dette finnes det løsninger på innenfor denne her proximity services-delen av standarden. Hvordan du skal løse midlertidig autentisering, kryptering, osv. Men det er ingen som har giddet og gjort det enda, hehe. |
| 104 | E | Hvis vi da drar det litt tilbake til den modellen der man skal bruke alle tre operatørene. Er det sånn å tenke at det å implementere dette er et åpenbart konkurransefortrinn med tanke på å tiltrekke seg Nødnett-kunder? |
| 105 | I | I vår modell, så er det det. For da skal man by på å bygge et robust nett i et område. Men adskilt i fra å by til kunden. Vi skal konkurrere om kunden på funksjonalitet, pris, osv. Og så skal vi konkurrere på nettverksutbygging på hvor lite penger vi skal ha for å lage dette |

| | | |
|---|---|---|
| | | området robust innenfor de kravene som finnes. Det var liksom hovedbyggesteinen i konseptet, hvis en skal forenkle det da. Men det er basert på at du ikke skal ødelegge konkurransen, men for å si det sånn, det er et fullt mulig konsept, det du nevner for Sverige. Altså, at staten fortsatt kan utlyse "Ja, vi skal ha white spot-dekning utbedret her og her og her." Og så kan operatørene by "Ja, vi skal ha 500 tusen for å gjøre det, de skal ha 300 tusen for å gjøre det," "Ja, da får de bygge." Da er det det som er egg-siten, og så er det krav om at de andre enten skal få innplassere seg. Altså, at vi får sette vårt aktive utstyr der ved vanlige kommersielle betingelser. Eller at det er et krav om at det skal skje etter et nullspill eller - Her finnes det mulighet for å lage kommersielle modeller. Den største faren kommersielt er det som jeg nevnte med at hvis én aktør tar hele landet og får alle tilskudd. Det er det vi ser på som verst, men det har ikke noe med teknikken å gjøre. Det å kunne tilby Nødnett i tre nett, om du så velger én hovedleverandør, mener jeg bør gjøres uansett. Det krever så lite. Det krever, i dagens oppsett, et S8-oppsett for roaming, og så krever det at vi har en enighet om hvilke prioritetsklasser man skal ha på trafikken og hvilke aksessklasser man skal bruke. Og så at vi mellom operatører, vi må stole på - At det er lov fra de andre operatørene å be om den kvaliteten i vårt nett. Easy peasy. Dette er det vi gjør med VoLTE-roaming i dag. Vi gjør policing av hvilke QCIer du får lov til å spørre om, hvilke hastighetsklasser du får lov til å sette osv. på nettverkstjenestene. Aksessklasse er predefinert. Noen gjelder i land, noen gjelder kun i eget nett, osv. Og da er det bare radionettstøtte - Og det har vi. I Norge har vi tross alt prioritets-SIM. Dette har vi gjort allerede. Du bruker samme aksessklasse på tvers av nettene. Det gir prioritet i hvert enkelt nett, med utvekslet MLPP-informasjon om prioritet, gir brukerprioritet mot B-abonnent i terminerende nett. Så lenge du holder deg til 2G og 3G, men ikke i 4G. For det er ikke regulert. Det kan gjøres i 4G, men det er ikke gjort. Samme mekanisme, litt annen variant, videreføres i 5G. Så dette er bread and butter, dette er enkelt. Så derfor er det nesten en tjenesteforsømmelse om DSB ikke ender opp med å kreve det, og at NKOM som regulatør ikke regulerer det. Jeg forutsetter at det kommer. Tilgang til alle nett. Men det gir ikke full funksjonalitet. Støtte for MBMS for eksempel, må forfinnes i hvert enkelt nett hvis du skal bruke det. Men det er ikke nødvendig i et konsept der du har én hovedleverandør. Den kan måtte støtte eMBMS, og så kan du godt ha unicast ut til de andre nettene i tilfelle ditt nett ikke fungerer i det området. |
| 106 | E | Ja, man kan akseptere på en måte en litt dårligere service i noen tilfeller, når uhellet er ute. |
| 107 | I | Ja. Alternativt kan en eventuelt kreve, og derunder også bekoste, implementasjon av eMBMS i hvert enkelt nett, og kreve en samhandling om broadcast-grupper. Da går du hakket mer avansert til verks, og da begynner du å nærme deg at push-to-talk-systemet på toppen faktisk må greie å forholde seg til tre ulike broadcast-senter. For du må bruke broadcast-senteret til det nettet kunden befinner seg i. Så den kompleksiteten øker plutselig, bare ved å legge på en liten ting. |
| 108 | E | Men det er noe som må komme fra toppen av, sånn top-down? |
| 109 | I | Ja. Så for å være ærlig så har jeg vel kanskje mest troen på en modell der det finnes ett overordnet push-to-talk-system som har kontakt med tre nett, der det defineres et minimumssett av funksjonalitet som operatørene skal støtte. Det er nok det enkleste. Da har du funksjonell støtte i tre nett for å gjøre nødnettsfunksjonalitet i sin enkleste form. Ikke autonom operasjon og ProSe, men alt annet. Men det er litt jobb med det for du må bli enig om prioritetsklasser, hvilken parameterisering skal du gjøre osv. Vi brukte vel et års tid på å bli enige operatørene og NKOM imellom når vi gjorde prioritetsabonnement for tale for noen år tilbake, men det er bare en jobb du må gjøre, det er ikke vanskelig. Så når du er enig om det så implementeres det i nettene likt, og da kan du kjøre på så lenge systemet på toppen kan forholde seg til tre nett. Det er nok den enkleste trenettsløsningen du kan få til. Da kan du også konkurrere på å selge aksess til Nødnett operatørene imellom. Ergo kan DSB |

| | | |
|---|---|---|
| | | ha et fungerende marked. Ikke for push-to-talk-tjenesten - |
| 110 | E | Ja, er det DSB som skal være kunden her eller skal de individuelle nødetatene inngå egne avtaler med mobiloperatører? |
| 111 | I | Det vet vi ikke enda, for det er en del av det som KVUen skal gi svar på. Men det gir mulighet til å konkurranseutsette. Og sågar å konkurranseutsette aksessen til det enkelte politidistrikt om det var så, men det er ikke sånn de kjøper inn. De kjøper gjerne inn regionalt gjennom statens innkjøpsfellesskap og den typen ting. Så du kjøper gjerne på kommunenivå. Politiet kjøper for eksempel en kontrakt for hele politiet i dag, så da kan du for eksempel tenke deg at du kan vinne kontrakten for hele politiet i Norge. Men det betyr ikke nødvendigvis at du vinner kontrakten for helse eller brann. Kanskje de vil ha regionale avtaler, fordi du kan bundle det med andre produkt i porteføljen til tjenesteoperatøren som gir deg billigere aksess. Det er et konstrukt du kan tenke deg for å få et fungerende marked. Men du sitter fortsatt igjen med den vanskelige delen, for det blir vanskeligere jo mer penger det er snakk om, og det er hvordan du løser den nødvendige robustifiseringen av nettverket i hver region, i hvert område. Du trenger ikke tre like robuste nett. Det er mye bortkastede penger hvis tre operatører bygger like sterke nett i hver region. Du trenger ett sterkt nett i hver region. Så kan man diskutere hvor stor en region skal være. Er det en kommune? Er det et fylke? Eller er det mindre eller større. Men det er da du står i fare for å forrykke balansen, fordi det er snakk om milliardbeløp. Det å kunne tilby en push-to-talk-tjeneste er billig. En fullverdig push-to-talk-tjeneste som kan gi mission critical-tjenester, om vi klarer å bruke 30 millioner. Og da tenker jeg ikke på operasjonssentralen hos politiet, men nettverksstøtten for det. Så det er ikke der pengene går. Men det koster et par milliarder å robustifisere radionettet, minst. Og så skal vi bygge dekning i tillegg, så det er der de store pengene ryker. Men det er ikke teknisk vanskelig. |
| 112 | E | Hmm, ja. Men hvis vi tar den modellen der DSB har sin egen MVNO da, for det er jeg litt interessert i å høre fra en som har innsikt i hvordan det er å være en MNO. Utenom det at man mangler den redundansen man får ved å ha tre kjernenett, hva tenker du at er utfordringene for DSB med å skulle drifte sin egen MVNO? |
| 113 | I | Hvis de skal drifte sin egen MVNO så har de den som felles sårbarhet. |
| 114 | E | Ja, men om det er noen tekniske utfordringer med tanke på å bygge ut en MVNO og operasjonalisere det, eller om det er trivielt i forhold til andre utfordringer. |
| 115 | I | Nei, altså, vi har allerede MVNOer kjørende for eksempel i vårt nett som kjører med sitt eget full-stack kjernenett, og som bare bruker radionettet vårt, nesten. De bruker SGW i pakkekjernenettet vårt, det må de, det er den som styrer opp radionettet. Så det har vi konsept for, så det er ikke sånn teknisk vanskelig. Men det endrer seg vesentlig i 5G. 4G er lett. |
| 116 | E | Det endrer seg fordi kjernenettarkitekturen blir annerledes, eller hva tenker du? |
| 117 | I | Ja, fordi kjernenettet ikke lenger ser ut som vi er vant til, hehe. Så det gjør det komplisert. For hva er en MVNO i 5G? |
| 118 | E | Mhm, ja, det er et av de spørsmålene jeg har prøvd å stille meg selv. Men ta for eksempel den oppdelingen de har i Storbritannia. Der har EE ansvar for radionettet, og så har de ansvar for den nedre delen av kjernen, og så har Motorola ansvar for resten av kjernen. Det jeg har fått inntrykk av at det handler om i 5G er kanskje at du har UPFen, SMFen og AMFen, det er forlengelsen av radionettet. Og så har du alle de andre tjenestene på toppen av det |

| | | |
|---|---|---|
| | | som den øvre delen av kjernen. |
| 119 | I | Ja, hadde det enda vært så clean cut. Så clean cut er det ikke. Det er sånn da, at et håndsett kan være del av mange slicer samtidig. Og et håndsett vil forespørre en AMF i slengen, så hva gjør du når du har noen slicer som vi må tilby som operatør, og noen som en MVNO må tilby. Hvilken AMF bruker du? Tenkbart, men hvis du ser på 5G som konsept, så er det spesielt den network exposure function som det er meningen man skal bruke for å få satt opp dine egne dedikerte ressurser i gjesteoperatørens infrastruktur som er dedikert til deg. Om det er det vi skal kalle service provider-oppsett.. |
| 120 | E | Det blir nesten som et API inn mot deres kjernenett da. |
| 121 | I | Ja, men om det er det som er morgendagens MVNO, eller om det er den tradisjonelle måten vi er vant til å tenke på det der en MVNO er en som sitter på kjernenettinfrastrukturen selv, der er jeg sannelig ikke sikker. Det er litt avhengig av både hvilken funksjonalitet vi klare å tilstedebringe i en network exposure function, og i hvilken grad vi er villig til å eksponere de egenskapene. Fordi, i det du begynner å eksponere slice-styring og QoS-parameter så har du en enorm risiko. Da risikerer du at en tredjepart gjør noe som de ikke burde og tar ned hele nettet. Jeg ser ihvertfall en umiddelbar risiko opp mot sikkerhetsloven, der vi skal være sikre på hvem det er som er inne og klår i vårt nett til enhver tid. De skal være klarerte osv. Så jeg har egentlig ikke noen klar oppfatning av hvordan dette kommer til å bli, for å være ærlig. |
| 122 | E | Man må vente å se litt hvordan implementasjonene blir rundt omkring? |
| 123 | I | Ja, og hvordan markedet beveger seg. For hvis det er sånn at de tradisjonelle MVNOene ikke lenger er interessert i å huse sin egen maskinpark, men heller vil leie kapasitet fordi det er enklere. Så vil jo det bli MVNO-løsningen. At de slicer kapasitet i vårt nett. Men det er fullt tenkbart at de fremdeles ønsker å ha større kontroll på egne kjernenett. Men du kan ikke plassere dine egne nettverksfunksjoner der du måtte ønske, fordi du er avhengig av kommunikasjon til radiobasestasjonene. Den kommunikasjonen skjer i gjesteoperatørens IP-nett. Det gjør at du fortsatt er like avhengig av exit-punkt i det IP-nettet. Om vi får på plass segment routing, så kan vi rute deres segment dit de måtte ønske på den funksjonen de måtte ønske det, forutsatt at det finnes et NNI der. Og NNI-punkt, altså tilknytningspunkt mellom forskjellige nett, er tradisjonelt sett ganske sentralisert. Så hva er gevinsten? Og det går litt på hvor stor bruk av utskutte UPFer og sånn. Altså, hvor langt ut i nettet vil kjernenettskomponentene komme? Hvilke bruks-caser? Er du en MVNO som skal tilby internettaksess eller narrowband IoT-tjenster, så er det kanskje greit å ha overleveringspunkt sentralt, og bruke slicene til nettverksoperatøren. Du trenger ikke å gå mer på toppen enn det. For å eksemplifisere så har vi Com4 for eksempel i vårt nett. De er en MVNO, har full stack hos seg selv, og tilbyr M2M IoT-tjenester. For de vil det nok være helt unødvendig å tilstedebringe den funksjonaliteten selv. Det er ikke der de har verdiøkningen sin. Men de vil ha SIM-kortet. Så de vil ha sin egen UDM/UDR. Men resten? Hvem vet, kanskje de vil ha det, men da i ett sentralisert overleveringspunkt, så de har sine egne UPFer men bruker vår AMF, for eksempel. Så det er vanskelig å spå. Konseptet har liksom ikke modnes. |
| 124 | E | Så det å si at DSB skal opprette sin egen MVNO, det blir på en måte sånn - Det er veldig utydelig hva det egentlig betyr da, fremdeles? |
| 125 | I | Ja, det kan bety litt forskjellige ting. Men det å bygge sitt eget kjernenett, det kan man gjøre. Men det er ikke gitt at vi vil akseptere at noen andre sin AMF står i vårt nett og snakker med vår basestasjon. |

| | | |
|---|---|---|
| 126 | E | Ja, DSB sin AMF på en måte? |
| 127 | I | Ja, det er ikke gitt. Det går litt på hvor sikkert det blir, og hvor godt de klarer å styre det opp. Og så er det sånn: Er det formålstjenlig? For en av de tingene som er helt nødvendig dersom 5G skal bli en suksess i forhold til å lage mange slicer, kundetilpassede nettverksdeler, det er at du klarer å orkestrere nettet ditt. Du kan ikke sitte sånn som vi gjør i dag og konfigurerer. Det går ikke. Noen få, en håndfull, går bra. Sånn vi holder på i dag med store operatører og en service provider her og en service provider der, liksom 10-12, det går greit. 300? Det tror jeg ikke altså. Så når bedrifter begynner å ha det samme behovet. Som vi ser at de har. Autonome nett, spesialtilpassede nett, sin egen edge-compute kanskje. Så blir volumet stort. Ergo må vi automatisere og kunne orkestrere. Hvis du skal orkestrere, så må du faktisk ha kontroll på alle ressursene. Da kan ikke noen andre drive å klå inn fra siden og ta ressursene dine. Det funker ikke. |
| 128 | E | At det blir vanskelig å skulle ha spesialløsninger for noen av kundene hvis man har et litt mer sånt automatisert økosystem? |
| 129 | I | Det er mulig. For du kan si det at "Ok, vi genererer en slice, og innenfor den slicen er du kongen." Vi setter opp infrastrukturen i vårt orkestreringssystem som overleverer trafikken dit den skal, og så tar du deg av resten. Da har du de kjernekomponentene hos deg, kjære DSB. Dette er Nødnettet. Konseptuelt, fullt mulig. Det går. Alt jeg sier er egentlig at vi enda er tidlig på den reisen, så det er vanskelig å spå hvor vi ender opp. Om det blir den foretrukne, eller om det blir foretrukket å bruke network exposure function eller en variant av det til å sette opp og styre nettverksdeler mer dynamisk for kunden, det være seg store eller små. Men absolutt, fullt mulig. Altså, Nødnett er helt spesielt. Det er stort, viktig for landet, osv. Der vil du kunne gjøre mye, kall det, spesialsøm for én kunde i et nett. Det vil du kunne gjøre. Så det er fullt mulig å tenke på det i nærheten av sånn vi er vant til å tenke på MVNO-oppsett. Altså, bruke minimalt med komponenter i gjesteoperatørens nett, bortsett fra radionettet. Det er også tenkbart, som jeg tror er på linje med det som er det offentlige svaret til en av de andre operatørene, at du bruker et multi-operatør-oppsett, men da er det som sagt litt vanskelig å bruke samme operatørkode i tre nett. Det gir egne utfordringer, men det er fullt mulig å tenke at du bruker ett hovednett som du er multi-operatør inn i, og at du roamer på de andre. Og at du med et MOCN-oppsett er ditt eget kjernenett og er din egen MVNO, med egenstyrte radiodeler i ett nett og roamer på de andre. Jeg er ikke sikker på om jeg ville gjort det, men det er en helt annen sak, hehe. Men det går mer på at da er du igjen avhengig av ett kjernenett. Og det spiller liten rolle om det er huset hos en operatør eller en uavhengig tredjepart. Det nettet kommer til å svikte. |
| 130 | L | Ligger svarene på den RFIen, fra operatørene, ute? |
| 131 | E | Hmm, ja, man har jo det alternatives for mission-critical-dokumentet, men jeg tror ikke de faktiske svarene ligger ute. Men den rapporten til DSB finnes jo der. |
| 132 | I | Ja, DSB lagde en rapport. Og så tror jeg det skal finnes noen offisielle versjoner, som er såkalt redacted da, eller tilpasset. Vi har ihvertfall forberedt sånne versjoner som vi har gitt til DSB. |
| 133 | L | Ok, da skal vi forhøre oss om det. Jeg tar en liten avsporing jeg. Jeg vet at Nødnett har og andre kommersielle operatører har sånne transportable basestasjoner som de flytter ut hvis dekning faller ut et sted eller - Ja, hvordan er situasjonen for det hos dere? |
| 134 | I | Jo, mobile basestasjoner har vi. |

| | | |
|---|---|---|
| 135 | L | Ja, sånn distribuert rundtom i landet for å kunne flytte ut ved behov? |
| 136 | I | Vi har to varianter. Vi har våre egne mobile basestasjoner, som rett og slett er hengere. De har fullt oppsett med antenne på taket, stolpe vi kan sette opp, radiolinje så vi kan få kommunikasjon, og mulighet for å ta inn fiber. Og da finnes det et antall vogner som er beredskapsvogner, og som DSB har bekostet. Og de finnes utplassert på forskjellige plasser i Norge, sammen med mobile nødaggregat for strøm, for å kunne brukes i krise på DSB sin forespørsel. Og så har vi et antall vogner som vi bruker selv for å dekke evenement. For eksempel Øya-festivalen, da kommer vi og setter opp mobile vogner. Store sånne konserter eller ting som skjer sporadisk, der du trenger punktvis økt kapasitet. Da kjører vi ut det. Ved krise så kjører vi også ut. Hvis en basestasjon hos oss brenner opp eller noe sånt, så kjører vi ut. Skal vi rive en basestasjon og flytte den, som skjer alt for ofte synes jeg, hehe. Så vi har en del sånne basestasjoner på hengere som vi kan kjøre rundt og plassere. |
| 137 | L | Hva er hovedutfordringen med dem? Synes du det går på skinner eller er det begrenset av typ hvordan Norge er med vær og vind og stengte veier? |
| 138 | I | Nei, for oss tar det en dag eller to å få de operative. For det du må skaffe er transmisjonslinjer, kommunikasjon til basestasjonen. Alt annet har man med seg, inklusiv strøm, men du må ha kommunikasjon med basestasjonen, og så må vi planlegge basestasjonen inn i det området den skal stå, frekvensmessig. Det er veldig sjelden at de står i helt komplett døde områder, så man må gjøre en grunnleggende radioplanlegging. Og vi gjør det raskere når ting virkelig går åt skogen, hvis vi kan. Men som en normal prosedyre så tar det et par dager. |
| 139 | L | Men de dere har på DSBs forespørsel, hva er use caset der? |
| 140 | I | Si det skulle skjedd et jordskred. En bygd blir isolert. Den typen ting, der nødetater må inn. Det er rett og slett en ressurs som er tilgjengelig for oss som DSB har vært med å betale for, fordi det øker beredskapen i Norge. Det finnes også en annen kategori som kanskje ikke er så kjent, noe som heter forsterket EKOM, der staten har betalt for økt tilgjengelighet i kommunesentre. Da er det gjerne sånn at de kan kjøre 72 timer på batteri, aggregattilknytning, forsterket transmisjon. Men det er typisk kommunesenter, så hvis et større område skal bli rammet av et større utfall, så kan ihvertfall kommunikasjon opprettholdes fra sentrale punkter. I mangel av telefonkiosker, hehe. Og de basestasjonene vil fungere helt som vanlig uten noen begrensninger. |
| 141 | L | Nemlig. Jeg prøver å inkorporere det litt med oppgaven min, og se på fra en basestasjon mister tilkobling til vi er oppe og går igjen med en transportabel basestasjon som midlertidig løsning. |
| 142 | I | Det finnes nå veldig mange spennende konsept som ikke er tatt i bruk i Norge enda da. Hvis du ser på andre nødnett, så har du f.eks. droneløsninger for å generere dekning der dekning er borte. Altså, du kan ha satellitt-link tilbake til kjernenettet. Kjører drone opp. Den får strøm fra bakken, og er en basestasjon. Genererer dekning. Den typen løsninger finnes for eksempel. Og det er mange andre konsepter. Du kan ha fastmontert i biler. Det være seg kommandobiler eller den slags, som kan idriftsettes. Alt du trenger er kommunikasjon bakover, som du kan kjøre på satellitt-link hvis det du trenger å gjøre i tale. |
| 143 | L | Ja, det finnes jo i Nødnett med den type gateway/repeater-funksjonaliteten. |
| 144 | I | Ja, så den typen ting kan du gjøre. Og den blir mer og mer interessant med lavbanesatellitter med lavere delay. Uten å si alt for mye, så er dette konsepter som vi diskuterer blant annet |

| | | |
|---|---|---|
| | | med Forsvaret. Men de har veldig likt behov som det man vil se i Nødnett, det er bare at de ligger et par år foran. |
| 145 | L | Ja, ikke sant. Vi har sett litt på det arbeidet Forsvaret har gjort gjennom 5G-VINNI-prosjektet. Det er mye spennende som rører seg der. Men, ja. Nå har du på en måte fått litt innsyn i hva vi er på jakt etter. Er det noe du føler at vi burde spurt om eller se på? |
| 146 | I | Nei, altså, det jeg ikke vet er hvor mye dere skal kikke på det som jeg kanskje har brukt litt mye tid på, nemlig konkurransesituasjonen og påvirkningen på det. |
| 147 | E | Jeg kommer ikke til å se så mye på det økonomiske og det politiske sånn sett, men det å se på teknisk vendor lock-in og sånne typer aspekter det blir nok veldig aktuelt. Det blir på en måte i forlengelsen av det konkurranseproblemet da, at man får én leverandør som man har investert i og som ligger annerledes til enn de andre leverandørene da gjør, og at man da kan få problemer med eventuelt velge en annen leverandør. En av de tingene du nevnte tidligere var at hvis man da inngår en 25-års kontrakt med DSB, så har man ikke så mye incentiv til å kanskje produsere den beste løsningen til enhver tid. |
| 148 | I | Ja. Samtidig så kan det ikke være for kort, ikke sant. For da blir investeringsviljen lav, fordi kontraktsverdien ikke er høy nok. Så dette er det som er kjempevanskelig. Men jeg hadde kanskje ville kikket på dette jeg snakket om innledningsvis med timingen og modenheten på 5G som teknologi og bærer for Nødnett, opp mot det som er tilstrekkelig teknologinivå for å løse nødnettsoppgaven. Og som jeg sa, vi anbefaler å ikke satse på 5G i første omgang, fordi vi trodde at det ville være umodent i forhold til 4G på det tidspunktet, men at 4G ville ha tilstrekkelig funksjonalitet til å løse oppgaven. Men så er det jo, ja, er det to år siden vi skrev dette, og ting skjer nå. Så om du vurderer inn det, så skal ihvertfall jeg lese det, for å si det sånn, haha. |
| 149 | E | Jeg ser ikke så mye på akkurat den overgangsfasen, men det er ikke til å komme utenom at det virker som om oppfatningen til de fleste er at 5G-nettet ikke kommer til å være modent nok i 2025 allerede, sånn at det blir en sånn - I fremtiden tenker man jo at da skal man selvfølgelig over på 5G, og så når 6G kommer så skal man sikkert over dit også. Men ihvertfall i første omgang, så får man en overgangsfase der man må støtte seg på 4G fordi det er det som finnes. Som er utbygd og som er modent av teknologi. |
| 150 | I | Ja, men bare for å si det, så har jeg vært med en stund. Og hastigheten med modningen på Gene har speedet opp. Og 5G modnes raskere enn noen annen G jeg har vært med på, det må sies. Men så langt så har modningen kanskje skjedd mest rundt radioteknologien. Og i og med at radioteknologien ikke er vesensforskjellig fra 4G, så er det kanskje ikke så merkelig. Mens kjernenettdelen tror jeg blir en mer bumpy ride. Det er den første store kjernenettendringen på snart 20 år. Den forrige store kjernenettendringen skjedde med innføringen av GPRS i 2001 eller hva det nå var. Og siden da så har kjernenettet vært mer eller mindre stabilt. Man har hatt noen små utviklingstrinn, men i prinsippet fungert ganske likt. Det endres fullstendig med 5G. Mye kan du kjenne igjen med mekanismer, men distribusjonen av det og bruken av protokoller. Den her flate arkitekturen, og forutsetningen om å kunne skille hvilke kjernenettkomponenter du bruker per bruker, og det at du skal kunne flytte kjernenettkomponenter mye nærmere sluttbruker, det er game changer. Og dette med at du i en og samme sesjon skal kunne bruke mer enn én kjernenettnode på brukerdatatrafikken din. Det faktum at du i en og samme sesjon skal kunne bruke to UPFer, avhengig av hvor endepunktet ditt er. Den tror jeg kommer til å ta lenger tid. Så det med edge compute, med de store skyaktørene inne, tror jeg kan ta litt lenger tid å få på plass. At den jevne forbruker får nytte av edge compute ved at Google sine servere plutselig står rett oppi høgget, eller bruker kapasitet på servere som står rett oppi høgget. Samtidig, når det |

| | | |
|---|---|---|
| | | først løsner så tror jeg det kommer til å gå fort. Så det er spennende. Og det kan godt hende at vi har tippet helt feil når vi tror at 5G ikke er modent nok i 2025. Men det er mye mekanikk i 5G, så det spørs hva du regner inn. For det å levere på den 5G-hypen, det kommer til å ta noen år. |
| 151 | E | Gigabithastigheter og sånn? |
| 152 | I | Nei, gigabithastigheter har vi forsåvidt allerede. Hastighet er enkelt. Ultra-low latency derimot. Millisekund og at du skal kunne bruke det til noe fornuftig. En ting er at du får millisekunds forsinkelse på radionettet. Fine, det. Men hvis serveren du skal nå fortsatt ligger på vestkysten av USA, så går det ikke noe fortere dit. Det er fortsatt sånn at i Norge, hvis du sitter i Tromsø og skal ha en server i Oslo, så tar det deg 34 millisekund. Lyset går ikke fortere gitt. Nå er det ikke bare lys, for det er i 4G-nettet som har mye høyere forsinkelse enn i 5G, så du får nok noe forbedring på det. Men forventningen til det 5G skal løse, både i enormt båndbreddetilfang og ekstremt lave forsinkelser, samt kanskje den mest oversette svakheten per i dag: Enorme opplinkhastigheter. Det eksisterer ikke. Nedlink? 1,4 gigabit i sekundet. Opplink? 90. 90?! Kombinert med 4G: 150. Det rokker ingen båt. Det er den store asymmetrien som finnes i 3,7 GHz-båndet, som er det eneste ferske frekvensbåndet som er tilgjengelig for 5G i dag. Det er at vi bruker 3 kanaler ned, men bare 1 kanal opp. Det gjelder for nasjonen Norge og Europa som kontinent, og det kan ikke én operatør gjøre noe med uten å sette inn gigantiske guard bands på hver side, og da kaste vekk like mye kapasitet som man kunne brukt til opplink. Så den er låst. Men det vil løse seg når frekvensmengden kommer. Når vi begynner å bruke - Altså, vi har 90 MHz til sammen av andre frekvensressurser per i dag, vi får se hvordan auksjonen går, hehe, og så har vi 100 MHz i 3,7. Så det gir seg selv at vi trenger mer frekvenser om 5G skal innfri kapasitetsløftet. Det holder ikke å bare bruke de 90 megahertzene vi har, selv om det er sammenlignbart til 180 fordi det er 90 ned og 90 opp fordi det er FDD-bånd. Men tilfanget av nye frekvenser for bruk i 5G kommer til å bestemme når du får enorme hastigheter både opp og ned. Og så vil vi se en bedring i opplinkhastighet de kommende årene fordi vi tar i bruk flere frekvenser av de vi allerede har, pluss littegrann til. Samt at det er FDD-frekvenser, så du får like mye opp som ned. Så det vil hjelpe på opplink. Men det er fremdeles ikke sånn wow i forhold til det du får i dag. Med en iPhone i et område der du har godt utbygd 4G i dag så kan du få 600 Mbit i sekundet i dag på 4G. Alt handler om hvor mye frekvenser du har. 5G i dag, du kan se 1,4 hvis du er heldig, og det er nice det, men hva du skal bruke det til det må gudene vite. Men systemkapasiteten øker, og det er viktig, for da kan du tilby høyere hastighet til flere samtidig. Men vi trenger flere frekvenser, og det må med i 5G, kall det, regnestykket hvis 5G skal levere på lovnaden. Det jeg tror vil skje er det samme som skjedde med en tidligere G. 4G innfridde det 3G skulle innfri, hype-messig. Og så, 4G+ innfridde det 4G skulle innfri hype-messig. Så du må liksom en halv generasjon videre for å få det. I 5G så må vi nok ha flere frekvenser for at 5G skal innfri. Samt at vi selvfølgelig må over på ny kjernenettarkitektur, men den har jeg nesten i beltet allerede for den kommer nå. Men den må selvfølgelig bygge på seg, for den første versjonen av 5G SA kommer ikke til å innfri alt det 5G SA skal løse, for alt er ikke klart enda. Så akkurat den timingen, den er kjempespennende. Men det går fort. |
| 153 | L | Nei, nå har jeg lært mye. Veldig mye artige innspill, og gøy å få det fra et nytt perspektiv. Så vi sender deg transkriptet fra dette om en stund, og så får du se gjennom det. |
| 154 | I | Haha, jeg står for det jeg har sagt uansett om det er feil! Så det er nå greit, haha. Men hvis det skulle være noe dere kommer på i etterkant som dere kommer på, så er det bare å ta kontakt. |
| 155 | L | Det setter vi pris på! Supert, takk for tiden din. |

| | | |
|---|---|---|
| 156 | I | Bare hyggelig. |
| 157 | E, L | Alright, ha det godt! |
| 158 | I | Ha det! |

# Appendix J
# Fire and Rescue Services

This interview is conducted with a representative of the Norwegian fire brigade. The interview subject possesses a thorough understanding of how the fire brigade employs Nødnett in their daily activities, what challenges firefighters are faced with in regards to using the existing Nødnett, and what the fire brigade expects of NGN. During the conversation we discuss, for instance, how the fire brigade deals with the eventuality of Nødnett being unavailable, as well as in what types of scenarios video and data communications may prove invaluable to the firefighter of the future.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, da er lydopptaket i gang. Da spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Det er helt greit. |
| 3 | E | Supert. Jeg kan begynne å presentere min egen oppgave litt. Jeg ser på NGN i 5G og utfordringer knyttet til samarbeid med kommersielle aktører. Siden man ikke skal ha sitt eget radionett i 4G/5G for Nødnett må man samarbeide med kommersielle aktører der, og så blir spørsmålet hvordan man skal gjøre det i 5G. Utfordringer rundt det med samarbeid med kommersielle aktører. |
| 4 | L | Jeg ser på tilfellet der en BS eller en gruppe av BS mister tilkoblingen til kjernenettet og virker som en autonom gruppe. Da ser jeg på operasjonelle utfordringer spesielt, med hvordan det fungerer for brukerne av Nødnett. Så jeg er veldig spent på å høre hvilke brukerbehov brann har, hvordan det fungerer når dere mister tilkoblingen til kontrollrommet og sånne ting. |
| 5 | E | Sånn vi har forstått det har du [rolle]. |
| 6 | I | Ja, stemmer. Vi er 110-sentralen for [område]. Samme som politidistriktet. |
| 7 | L | Nemlig. Stort område. |
| 8 | I | Jada, absolutt. Det er mye forskjellige typer brannvesen, fra et fullverdig profesjonelt heltidsbrannvesen til mye deltid, men det er det som er gjennomgående i hele landet med et stort geografisk område. |
| 9 | L | Har du lyst til å starte med å fortelle litt om deg og ditt forhold til Nødnett? |
| 10 | I | Jeg kommer opprinnelig fra beredskap og har vært der i mange år, drevet med opplæring. Etter hvert har jeg fått gå over til roller innenfor [tema]. Og så har jeg en bred bakgrunn både fra aktiv tjeneste ute i beredskap til administrative oppgaver. Jeg har vært med fra vi ble samlokalisert, først da vi flyttet til ny stasjon og så har vi gjennomført en samlokalisering da først helse og så politi flyttet inn her. Så vi er en litt spesiell 110-sentral som er samlokalisert både med helse og politi. En god stund var vi alene. Drammen begynte med det, men er nå flyttet til Tønsberg. Vi var en god stund de eneste som var samlokalisert med både helse og politi. Det er kjempespennende. Det er også mange andre nye prosjekter her som er kjempespennende. Det skjer mye og vi har hatt mye besøk av justisministere. Så det er interesse rundt det vi gjør her oppe og måten vi er organisert. |
| 11 | I | På Nødnett, litt gjennom den rollen jeg har hatt som er litt spredt og forskjellig, så har jeg vært valgt inn i en gruppe. Jeg har vært med i en del av KVUen med Nødnett, og KVUen med nytt oppdragshåndteringsverktøy, etter hvert som de dukker opp, felles ressursregister og sånne ting. Så er ganske med på mange av de prosjektene som er gjort. Så jeg kjenner godt til hva tanken bak nytt Nødnett har vært, og har vært med på utvikling fra utviklingen av det Nødnettet vi bruker i dag ble etablert, og hvordan det har utviklet seg. Så vi har veldig mye tanker rundt hva vi ønsker oss og hva vi trenger, det blir litt sånn, hvor skal man begynne hen? Jeg vet ikke hvordan dere vil ha det sortert, med det vi synes er feil med det gamle nødnettet først, eller..? |
| 12 | L | Kan du starte med å fortelle litt om hva slags tjenester brukerne av Nødnett hos dere bruker? Er det gruppesamtaler det går i? Jeg har forstått det som at brann har en litt annen |

| | | |
|---|---|---|
| | | organisering ved en hendelse enn de andre gruppene, ved at dere tar med en leder ut til hendelsesstedet. |
| 13 | I | Ja, ledelse til hendelsesstedet gjør politiet også, forsåvidt, for de er innsatsledere, som regel ved skadestedet. Nå er det litt spesielt med brann, for de har politimyndighet frem til politiet kommer til skadestedet. I distriktet er det ofte brann som fungerer som politi den første tiden, for vi har større grad av nærhet, ofte, til ulykken. Det er jo et av problemene, kanskje, at vi skal ikke drive og fungere som politi og dekke det behovet. Det har du jo fått noen saker med, sånn som den bussulykken med øksedrap der brannvesenet er først på stedet. Så politiet har ledelse og vi har ledelse på stedet. Helse kan også ha ledelse på stedet gjennom lege og sånne ting. Så alle tre etater kan stille med ledelse. Vi er jo de som har tydelige hierarkiske oppsett blant flere mennesker når vi rykker ut. Politiet rykker gjerne ut med to mann i en bil, ikke sant, og da blir de innsatsleder. Er det storby har de egen operasjonsleder eller operativ leder som kjører rundt i en egen bil. Så det er litt hvor du er i landet. |
| 14 | I | Det som kanskje er litt spesielt på utkalling er at for politiet, så velger de en ressurs som er nærme. Den kjører til stedet, så lenge de ikke vet at det er en etterforskningssak eller lignende. Helse velger den ambulansen eller det helikopteret som er mest mulig egnet til å kjøre til stedet eller fly til stedet. Brannvesenet gjør forsåvidt det nærme, men vi har på en måte en flåtestyring i bakkant som velger den mest egnede ressursen i tillegg. Det kan være at det ikke er den bilen som burde kjøre, men at vi burde ha en tankbil til det. Og da kan det hende at den velger det, og den velger på tross. Det som er spesielt for oss i motsetning til politi og helse, er at vi ikke har operativ myndighet over brannvesen som ikke tilhører vår region. Det som er spesielt med hvordan 110-sentralen i [område] er organisert, er at vi er en av de sentralene som ikke er en avdeling under et eksisterende brannvesen. Hvordan det blir i framtiden, får vi se. [Lokalt brannvesen] drifter 110-sentralen, så vi har eierkommuner og deltakerkommuner. Det er [antall] kommuner totalt inn i samarbeidet, hvor [antall] av disse kommunene eier sentralen og drifter den for de andre. Det gjør det litt spesielt, men sånn er det for alle sentraler nå. De har bare operativ myndighet over [antall] kommuner. Brannsjefen kan gå inn at jeg velger å bruke bilen i en helt annen kommune. |
| 15 | L | Den tildelingen der, når kontrollrommet tar tak i en ressurs og sier at du skal til det skadestedet. Brukes Nødnett? |
| 16 | I | Ja. Det er en bakgrunnsprogramvare som kalles Vision. Det er end-of-life, det har vært et stort prosjekt og vi har nå valgt ny leverandør av oppdragshåndteringsverktøy, og det er [verktøy], som også leverer kartverket til politiet og en del av utstyret til helse. Vi har også brukt det før som alarmmottak, vi kjenner godt til de som leverandør. Nå vet vi at det blir de og det er avklart. |
| 17 | L | Hva var det du sa de skulle levere? |
| 18 | I | Nytt oppdragshåndteringsverktøy. Vi har et flåtestyringsverktøy, det vil si at når vi setter et skadested i kartet, så kommer det med ferdigoppsatte premisser for hvilke ressurser som er mest egnet for å reise til det stedet eller for å agere på den hendelsen. Da forflytter det seg ressurser, kanskje over kommunegrensa. Det har sentralen lov til å gjøre. Når du får et eksempel på et ressursoppsett for den hendelsen i Vision-systemet, og så velger du å kalle det ut. Da agerer de på det. Da går det en call-out på håndholdte radioer og på bilradioer som gir et oppdrag i radioen. I displayet på både håndholdte radioer i bilen så kommer oppdraget opp som en tekstmelding i tillegg. |
| 19 | L | Ok, så en callout er en tekstmelding? |

| | | |
|---|---|---|
| 20 | I | Det er en sånn lydbølge, på lik linje med gamle VHF-radioer der det kommer et tåkesignal som varsler deg om at den er aktivert. Den ser sånn her ut, en vanlig håndholdt terminal. Det er som en gammel Nokia-telefon, det er old-tech deluxe det her. Da bekrefter du mottatt varsel, og så slutter den å pipe. Da går signalet tilbake til sentralen som får beskjed om at han [person], han kan møte på denne aksjonen. |
| 21 | L | Okei, så den eneste dataen som sendes er et lydsignal og en enkel bekreftelse, du sender ikke mer data frem og tilbake enn det? |
| 22 | I | Det er svært lite data som går, og det er en av begrensningene med det gamle nødnettet. Det er ikke en høy grad av datatrafikk mellom radioene. Det er maksimalt en SMS-type melding som kommer opp i displayet som sendes ut fra det styringssystemet på sentralen. |
| 23 | L | Føler du det er et udekket behov der med datatjenester? |
| 24 | I | Brannvesenet er nok en av de etatene som mest på egenhånd har utviklet teknologien. Vi har jo sørget for det på andre måten. Vi har pad'er i bilen som via Locus Emergency-systemet, som vi i flere år har hatt som alarmmottak. Så vi har knyttet disse og jukset disse opp mot hverandre sånn at når den radioen trigges, kan vi også sende objektplaner, kartreferanser, kjørerute og alt mulig til bilene. |
| 25 | L | Kommer det systemet kommersielle nett, eller bruker det også Nødnett med de databegrensningene? |
| 26 | I | Det er rett og slett en mobilbrikke i det Locus-systemet på den paden som gjør at den er på nettet og som får de opplysningene som vi kan sende frem og tilbake. De kan sende bilder og filmer til oss og vi kan sende bilder tilbake til dem fra f.eks. streaming, kartreferanser, objektplaner til huset som brenner, osv. Så det har vært sånn passe utviklet. Det er hver enkelt stasjon og 110-sentral og brannvesen som kan velge det. Jeg tror det er 10 eller 11 av de 14 sentralene som bruker dette Locus-systemet i tillegg. Det har vært på eget initiativ. |
| 27 | L | Så det er da mellom en lokal 110-sentral som bruker kommersielle nett ut til de ute for å dele informasjon? |
| 28 | I | Ja. Og så kobler vi disse. De godtar egentlig ingen form for det, og det har vært hele problemet. Det har vært helt nedstengt for å hente opp og kjøre data mellom Vision og andre systemer. Så det har vært ganske gammeldags type drift av dette systemet fra det offentlige. Det har vært ganske vanskelig å få. Vi har juksa det til så det står en sender oppe som trigges av det som sendes til radioene, så den vet at den skal gjøre det samme til bilene. Det er juksa til i systemet. |
| 29 | L | Okei, så det er en slags samhandling mellom Nødnett og det kommersielle nettet der? |
| 30 | I | Ja. Det er klart at den eneste måten å få gjennomført kryptert tale og lignende er med radioen. Vi er ganske aktive på radio, alt etter hvor erfaren de føler seg, de som er ute på stedet. Heltidsbrannvesen er ganske aktiv på radio med rapportering til 110 under innsats i forhold til f.eks. når det er igangsetting av røykdykker-innsats med alt som er alt som er pliktig med lov å loggføres. Så det er aktiv kommunikasjon mellom innsatsleder brann på stedet som kanskje har et ønske om et økt ressursbehov, eller flere tankbiler, eller veihjelp for å komme og hente en bil som har vært med i en trafikkulykke, osv. Så alle disse ressursene er i kommunikasjon mellom 110-sentralen og brannvesenet. |
| 31 | L | Ja, i en gruppesamtaler som regel, eller er det mye en-til-en? |

| | | |
|---|---|---|
| 32 | I | Det kan være talegrupper. Vi har gjerne flere talegrupper oppe på hendelser. Da har du en talegruppe som bare er mellom de som er på skadestedet, en type enklere arbeidskanal. Og så kan du ha en kanal som kun er mellom innsatsleder brann og 110-sentralen. Og så har du f.eks. en SAR-kanal hvis det er en redningsaksjon eller bare en politi-helse-brann, en BAPS-kanal som vi kaller det. Det er politiet som styrer det, og det brukes gjerne i starten av hendelsen, på vei ut til skadestedet så alle får en felles forståelse av situasjonen på vei ut dit. Med det nye Nødnettet så kom dette talegruppesystemet inn, og kallesignaler og styringssystemet. Tanken er veldig god, og den blir nok adoptert over til det nye oppdragshåndteringsverktøyet. Dette med å bruke talegrupper, alt etter hvilken situasjon det er du er i, men der stopper nok det man tar med seg videre fra Nødnettet, for det har veldig klare begrensninger med tanke på datatrafikk. |
| 33 | L | Du nevnte tidligere at dere har en del deltidsbrannmenn også. Med opplæring og bruk av Nødnett, er det forskjell i hva slags kompleksitet de forskjellige brukerne håndterer? |
| 34 | I | Ja, det er kanskje en av de store utfordringene. Brann-Norge består hovedsakelig av deltidskorps. Du har noen brannområder helt sør, rundt om Osloområdet hvor det er veldig mye heltid. Men generelt sett, uansett hvor du er i landet så er det ekstremt mye deltidskorps. Det er folk som vanligvis har andre jobber, er lærere og alt mulig på fritiden eller ellers, og er 1-2-3% stilling i brannvesenet der de får øvd litt innimellom. Det er gjerne at de er entusiastiske lokalbygdinger som gjør at det blir bra. Problemet er at dette er veldig lite brukervennlig. Det er utrolig enkelt, men likevel utrolig komplisert. Det gjør veldig lite, men det er veldig vanskelig å orientere seg. Du må inn og ut av menyer, trykke på tastene for å bevege seg. Det er veldig mange valgmuligheter for en deltidsmann. Så det som gjerne skjer, er de har slitt. Erfaring over tid har slitt med bruken, for de får brukt det for sjelden. Det beste hadde vært hvis den her hadde vært litt lik en smarttelefon i brukervennlighet. Da hadde ekstremt mange skjønt og fått det til. Vi kjører kurs og opplæring på de her, men det er en utfordring. En annen funksjonalitet som er på disse radioene, er statusmeldinger. Det vil si at de kjører status når de kjører ut, når de kommer frem og når de er ferdige med hendelsen og er tilbake på stasjonen. |
| 35 | L | Hva legger du i å kjøre status? |
| 36 | I | Det vil si at de kjører statusmeldinger som gjør at det kommer et pling inn i Vision som sier f.eks. at klokken 12:03 kjørte Bil 1 ut. Da kommer det direkte inn i loggen. Og nå logger vi inn i Locus og så forskyves det over. Det er et loggesystem der hver operatør får sin signatur og så logges det inn i det systemet. Det er ingen andre som kan logge inn, det er bare politisentralen som kan logge inn i det systemet. Hvis du går over i Locus så går det an å dele logger og skrive sammen og gjøre det på en helt annen måte. Så vi blander disse to funksjonalitetene for å få mest mulig ut av det. |
| 37 | L | Mhm. Jeg har forstått det som at, eller jeg kan gi litt kontekst først. Jeg ser som jeg nevnte på at basestasjoner mister tilkoblinga til kjernenettet. I Nødnett i dag er det noe som heter LST-modus, kjenner du til det? At en BS kan virke selv om den ikke har tilkobling til kjernenettet, så det blir som en isolert øy med dekning. |
| 38 | I | Å, heter det LST? Jeg trodde kanskje det het noe annet. Men ja, de kan fungere som BS selv om, og vi har også muligheten til å kjøre ut en egen henger som fungerer som en egen repeater. Så det er jo noen muligheter. Men det som vanligvis skjer.. Vi har vanligvis ganske god kontroll over den, men i det øyeblikket vi har dårlig vær eller ekstremvær så fyrer vi gjerne opp et kart som gir oss oversikt inn i systemet på hvilken tilstand BS har. Når det er ekstremvær vil vi da se at BS begynner å dette ned, og går over på batteridrift. Og så går det |

| | | |
|---|---|---|
| | | jo da et par timer kanskje, alt etter hvordan BS det er og hvor bra nødstrømmen er, så begynner de å dette ned og så mister vi kontakt. Så vi har opplevd både at vi faktisk har telefonisk kontakt, men ikke kontakt med nødnettet og motsatt, og begge deler. Vi har også opplevd at en hel telestasjon ramler ned, og da ramler et helt område ut. Vi har opplevd at en av de store hubene detter ut, og da fungerer ikke det systemet som du tenker på. Så erfaringen er at på ekstremvær så detter BS ned og de har ikke noen funksjonalitet til å fungere likevel. Mister de hovedkontakten mot Telenor sine største stasjoner så blir det krise. Da er det ingenting som fungerer. |
| 39 | L | Sånn jeg har forstått det så er det mulig for dere å programmere deres devicer med hvorvidt de skal koble seg til de basestasjonene som er sånne isolerte øyer eller ikke. Så dere kan programmere i de håndholdte devicene og bilene hvorvidt de skal hekte seg på. |
| 40 | I | Nei, vi kan velge to moduser. At de går fra radio til radio, eller fra radio til BS. Så det er de to formatene vi kan velge, og så kan vi gjennom f.eks. egne repeatere forlenge denne distansen hvis det er fra radio til radio. Av og til er det egnet for radio-til-radio hvis de er i et område og de ønsker å snakke med hverandre inne på et større skadested så er det radio til radio som kan være ønskelig. Da okkuperer de heller ikke en BS og ressursene som er på den. Men sånn i utgangspunktet så holder de seg mot basestasjonen og bruker faktisk den båndbredden som er der. Det er det som er vanlig kultur. Problemet vårt da Nødnettradioen kom var at de også skulle erstatte røykdykkersambandet, men det var problemer med at hjelmgarnityret som ble levert med disse radioene var for dårlig. Så det vil si at det ikke var høyt nok lydvolum for dem til å høre radioen. Så den ble avskaffet som røykdykkersamband i veldig mange brannvesen. I vårt brannvesen brukes UHF fortsatt som røykdykkersamband. Så det er også en av beskaffenhetene som ikke har vist seg å bli sånn som det var tenkt. |
| 41 | I | Og så er det klare begrensninger med radio til basestasjon på samme måte som det er f.eks. mobiltelefoner i konstruksjonsbygg og en del andre typer bygg der vi rett og slett ikke har dekning. Så langt nede og inne i bygg så er ikke Nødnett sånn som det er gira opp i dag så veldig egnet. Det er en del bygg som har valgt å ha ekstra forsterkninger i bygget, men det går tregt. De har satt opp ekstra antenner og sånt. |
| 42 | L | Bruker dere av og til gateway/repeater inn i byggene? |
| 43 | I | Veldig sjelden. Det er altfor vanskelig. Det er ganske omfattende, det må være en mann som driver og holder på med det her og setter det opp. Så det er ekstremt sjelden at vi setter opp gateway, igjen fordi det er veldig lite brukervennlig å gjøre det. Kanskje de på heltid har en anelse om hvordan du gjør det, men de på deltid har ikke peiling. |
| 44 | L | Hva med å svitsje over til device til device, DMO-operasjon? Det synes brukerne er greit, og det er brukervennlig? |
| 45 | I | Det går ganske greit, det er ganske lett på radioen. Men det kan også være en terskel. Vi har også fordelt en arbeidskanal til hver enkelt stasjon vi har i [område] f.eks., sånn at den arbeidskanalen trenger du ikke gå over i DMO for å bruke. Det er det de fleste gjør. Her i [by] f.eks. er kanal 22 lokal arbeidskanal. Det er ingen andre som er inni der, det er bare den stasjonen som er her som har den. Og så har f.eks. [by] 21. |
| 46 | L | Mhm. Jeg trekker det litt tilbake igjen. La oss si at du er i et område der du mister total kontakt med de som er innenfor den radiusen du er i. La oss si du har en radius på 6km i et område, der alle som er der kan snakke med hverandre gjennom en BS, men du kan ikke snakke med kontrollrommet. Det er det jeg anser som en autonom BS som kun virker med seg selv. Hvilke tjenester er det du hadde savnet mest i brannvesenet hvis du kun kan |

| | | |
|---|---|---|
| | | kommunisere i det området? Kan du fortsatt virke, selv om du ikke har kontakt med kontrollrommet? |
| 47 | I | Jada. I utgangspunktet er det sånn at 110-sentralen ikke har operasjonsmyndighet over det kommunale brannvesenet. De er en utalarmeringssentral og en ressurshåndteringssentral. Vi vet hvilke ressurser som er tilgjengelige og vi kan kalle ut brannvesen, osv. Det er en støttefunksjon for de der ute, men den reelle kommandomuligheten for brannvesenet er på stedet, eller inn f.eks. til en stasjon der kanskje det sitter en stab eller lignende. |
| 48 | L | Ja, er det et lite backup-kontrollrom på de lokale stasjonene? |
| 49 | I | Ja, det kommer an på størrelsen på området. Her er det det, i [by] er det det, men i [annen by] er det ikke det. Det kommer an på størrelsen. Er det et bittelite deltidskorps er de mer villige til at vi tar over aksjonen, de vil ha hjelp. Er det heltid er de mer sånn, la oss ordne opp i det her selv. De vil jo ikke slutte å gjøre den gode jobben på stedet selv om de mister omverdenen. De fortsetter etter beste evne, men de mister all kontakt og evnen til å hente inn mer ressurser som ikke er tilgjengelige innenfor det spennet de har. For av og til så setter vi biler på hjul, eller pga. f.eks. situasjonen nå med covid så velger vi å hente inn den tankbilen som er to timer unna fordi at det her ble en langvarig aksjon. De der ressursene får ikke de nødvendigvis tak i. Men de har med seg mobiltelefon, og hvis det fortsatt er kontakt med mobiltelefonen kan de ringe etter veihjelp og sånne ting. Men brann på stedet, politi på stedet og helse på stedet vil jo fortsatt gjøre den gode jobben, men de kan gå glipp av en del viktig informasjon og andre ting. |
| 50 | L | Ja, så det de mister er muligheten til å hente ressurser og muligheten til å koordinere, men de er fullt i stand til å virke som en autonom lokal enhet. |
| 51 | I | Ja. De vil ikke slutte å jobbe om de mister kontakten. Det eneste i vårt brannvesen som fungerer på den måten, det er hvis vi er i en røykdykkerinnsats så skal røykdykkerne trekke seg ut hvis de mister kommunikasjonen. |
| 52 | L | Okei. |
| 53 | I | Da trekker de seg ut. Fordi da vet ikke de hva som foregår. Huset kan ha tatt fyr, de utenfor kan se at huset i hele andre etasjen har tatt fullstendig overtenning. Hvis de er nede i første etasje og huset er på vei til å rase sammen, da vet de ikke om de kommer seg ut. Så mister du radiokontakten så trekker du deg ut. Da kan det hende at du mister makkeren din og andre ting i tillegg, så da trekker du deg ut. Og så er det større aksjoner, hvis vi flys ut til brann i båt og vi mister all kontakt med omverdenen, da ønsker vi antakeligvis etter hvert å trekke oss ut. Vi ønsker ikke å være i et brennende skip midt til havs hvis ikke vi har kontakt med omverdenen. Da er det å komme seg av bord eller et eller annet. Men det er liksom de små hendelsene der vi trekker oss ut hvis vi mangler radiokommunikasjon. Ellers vil en innsats på et sted på et sted gå helt som normalt. Og som sagt så bruker vi jo ikke nødnett for røykdykkerkommunikasjon. Da vil det jo være batteristans på en UHF-radio eller et eller annet. |
| 54 | L | Når du skal kalle inn deltidsbrannmenn til en hendelse, har de da en Nødnett-terminal hjemme hos seg som du varsler til, eller bruker du kommersielle nett når du når ut til dem? |
| 55 | I | Sånn som vi er, det er litt forskjellig hvordan de har gjort det. Måten det var før i gamle dager, da hadde vi personsøkere til de ansatte. De som er heltidsbrannvesen der det en vakt du møter opp til som i Oslo, der har de ikke det konseptet med deltid. De har ikke radio hjemme. Vi er avhengige av å kalle dem opp, og vi er pliktige til å få tak i mannskapet. Det er |

| | | |
|---|---|---|
| | | det beredskapen er basert på. I vårt distrikt er beredskapen basert på deltidsmannskap, men i Oslo så er det vaktordning der det er folk på vakt. De har ikke radio med seg hjem og bemanner brannordningen i den kommunen. Så vi hadde personsøkere. Da Nødnettradioen kom, så måtte du ha den i tillegg til en personsøker, for personsøkeren snakket med radioen din og så med en BS. Så da var det bare å kassere denne personsøkertjenesten som vi brukte før som gikk over VHF. Da fikk alle de ansatte i beredskapen i Salten en radio. Vi kjøpte jo, jeg vet ikke hvor mange Nødnettradioer, men det var i hvert fall over 500 i det her tildelte området vi har her. Så det er en ekstrem kostnad. |
| 56 | L | Ja, det tror jeg på. |
| 57 | I | Så hjemme på nattbordet til disse brannfolkene står det en radio. Når det er behov for de i en innsats blir de kalt opp, drar til stasjonen, kler på seg klærne og blir med ut i den bilen som er på den stasjonen f.eks. |
| 58 | L | Så en potensiell sterk konsekvens for dere av en sånn isolering, partisjonering av nettverket, er at du ikke får tak i disse deltidsbrannmennene. Hvis du ser for deg at dere er på forskjellige øyer. |
| 59 | I | Ja, hvis den senderen som gjør at vi får kontakt fra 110 og ut til de der de er, er brutt, så får ikke de utkallet. Nå er det sånn at hvis det er ekstremvær, f.eks... De overlapper hverandre, ikke sant, en del. Hvis det er meldt ekstremvær, så ser vi etter hvert at disse begynner å dette ned eller gå over til batteridrift. Da begynner vi å varsle. Gjerne sender vi ut tekstmelding til de ansatte: nå må dere være obs, det kommer ekstremvær og det kan se ut til at dere kommer til å miste dekning om en liten stund. Da er de jo klar over det, da blir det nesten litt sånn at da får dere gå opp i tårnet og speide. Da må man bare gå tilbake til steinalderteknologi og omtrent være obs og se hvor på veien... Eventuelt at de møter på kommunehuset der krisestaben hos kommunen er etablert for ekstremvær. Da etablerer de seg der og man prøver å samle de. Alternativet er også da å kontakte den huben med f.eks. satellitt-telefon. |
| 60 | L | Ja. Så i tilfelle ekstremvær opplever du at dere er forberedt på en sånn partisjonering. |
| 61 | I | Ja, jeg vil jo egentlig si at vi er vant til at de detter ned. Vi gjør fortløpende vurderinger på hvor vi skal dra det her. Det er klart, blir de helt tause og vi har null kontakt imellom så er det en utfordring. |
| 62 | L | Mhm. Jeg kan se for meg også at det er en utfordring hvis de går ned på grunn av teknisk svikt, eller hvis en gravemaskin har brutt en fiberkabel så det ikke er noen grunn til å forvente at det ryker. Det vil jeg tippe er en ny utfordring? |
| 63 | I | Ja, det har skjedd noen plutselige kutt og da er det brutt en periode. Det er et problem. Men av en eller grunn er det ofte, kan enten være nå vi er over på GSM eller, satellitt-telefon eller en eller annen måte. Til syvende og sist, i ytterste konsekvens må man begynne med en eller annen form for ordinans. Gå tilbake til det gamle, omtrent begynne å tenne bål på haugene. Man må til syvende og sist finne en løsning som gjør at man får tak i hverandre. Men det begrenser jo smidigheten ekstremt når man går over til de verktøyene som ikke er egnet til å ha kontakt med hverandre. |
| 64 | L | Jeg har lyst til å bytte tema helt igjen, jeg. Jeg har forstått at dere bruker en større grad av maskin-til-maskin i brannvesenet. Stemmer det? Jeg vet at det er noen avdelinger som bruker drone. |

| | | |
|---|---|---|
| 65 | I | Hva tenker du på med maskin-til-maskin? |
| 66 | L | At Nødnett brukes ikke bare mellom personer som prater med hverandre, men for å synkronisere eller koordinere mellom, eh, vil du hjelpe meg? |
| 67 | E | Ja, sensorer og systemer. Bruker dere drone f.eks. til å få oversiktsbilder f.eks. ved skogbranner og sånne typer hendelser? |
| 68 | I | Ja, ja. Vi er ganske langt frempå med det her i [område]. Vi er et av de brannvesenene som både har dronekapasitet hos oss selv, og vi har lagt til rette i 110-sentralen for å motta dronekapasitet både for å bruke som en ressurs og til å motta bildefeed fra. Vi var før helse, det blir ikke sagt i nyhetene, men vi var et år før helse på bruken av innringerfunksjon der vi tar over telefonen og streamer fra innringer. Det kjører vi i egne systemer. Vi bruker Incendium, som det heter, fra Danmark. Flere av bilene våre er utstyrt med kamera som streamer direkte inn i 110, så enten 110-sentralen eller staben kan hente ut den bildefeeden når som helst og bruke den til å lage et felles situasjonsbilde. Så det er ofte sånn at politiet kommer inn til oss for å se på den feeden som vi har fra skadestedet. Men det har ingenting what so ever å gjøre med Nødnett. |
| 69 | L | Nei, ikke sant. Men det er i dag da. Spørsmålet er da om det er noe som kan tilbys av Nødnett i fremtiden. |
| 70 | I | Ja, sånn ja. Det har vi spilt inn. Jeg har faktisk spilt inn sånn at jeg mener på mange måter at nesten er viktigere enn tale. Tale blir veldig fort sånn at du hele tiden skal si status og du skal ditt og datt. Det er kanskje ikke egnet for mottakelse. Det må være noe i begge ender. Det er nå vi skal skape plattformen med det nye oppdragshåndteringsverktøyet. Det er spilt inn at helst skal det være slik at han som er ute på stedet, han logger i et system. I det samme systemet som de på 110-sentralen og på staben er. Så det kommer flere typer logger samtidig. Det blir naturligvis være en del dialog, spesielt i startfasen på et oppdrag. Jeg tror vi har vel så mye nytte i stab og 110 av å se hva som foregår på stedet, fordi at man da kan støtte de, ift. f.eks. at det er superfare for spredning og han som er innsatsleder står midt i det og det er lite mannskap. Da kan vi gå inn og bidra med en gang. Trenger du mer folk, ja jeg trenger mer folk. Vi ser at du har behov for mer kjøretøy, ja kom med flere kjøretøy. Da kan man bidra inn i det spillet og man forstår. Eller man kan få motsatt, at innringer sier at det er totalt kaos, og man ser på bildet at det er ingenting det her, helt uproblematisk og vi sender en bitteliten bil med 2-3 mann bortover til å hjelpe. Det kan gå begge veier. Så det å få den streamen fra enten innringer eller fra noen av de andre verktøyene våre er ekstremt nyttig. |
| 71 | L | Så du vil ha en videostrøm mellom operatører som er ute i felt og kontrollrom. |
| 72 | I | Ja. Og vi ser også på at de har en modul på vesten sin, alle mannskaper skal ha det sånn som en del av politiet i USA også har prøvd, der det er en kamerafunksjon. Det må være enkelt, det må ikke være at du må logge deg på eller starte opp. Du må vri på en bryter og så kobler den seg direkte til systemet. Da går den av seg selv. Så kan vi gå inn, du kan velge på kartet hvilken av disse personene du vil lytte til eller se på. Ser du innsatsleder gå bort til politiet så aktiverer du det kameraet på den skjermen. Vi har bl.a. både på operasjonsrommet og på 110-sentralen så er det svære videovegger der vi kan veldig enkelt vise områder der vi vil vise forskjellige streamer. |
| 73 | L | Så du sier at det er mest behov for mer datakrevende kommunikasjon mellom operatør som er ute og de som er på kontrollrom. |

| | | |
|---|---|---|
| 74 | I | Ja. |
| 75 | L | Så blant de som er ute.. Igjen trekker jeg det tilbake til scenarioet jeg ser på, der du er på en isolert liten øy av folk som kan kommunisere med hverandre. Blant de som er ute, så vil det fortsatt være talekommunikasjon som er viktigst, eller mener du at det også vil være behov for video for de som er ute i felt? Det kan f.eks. være han innsatslederen som står et lite stykke unna og de som faktisk er inne og opererer. |
| 76 | I | Det vil være veldig nyttig for innsatsleder som er i ko f.eks. Vi har jo startet at vi har sånne biler der vi åpner bakdeler der det er skjermer og tavler som også skal streames inn til politi. Det vil vi også se for oss hvert fall med tanke på utrykning så er det veldig interessant å se hva. Med røykdykkerne, om du ikke ser så mye så ser du at de beveger seg. Og når de snakker så ser du at de snakker med normal tale, eller forholdsvis normal tale, det er aldri normalt sånn sett. Men du hører at de går og beveger seg og prater sammen, og kanskje plutselig ser ting. I tillegg er det ønskelig å se lokasjon i 3D i bygget. Vi holder på nå med smart arkitektur både for å hente inn data på bygget i 3D og hva som er begrensninger og muligheter i det bygget mtp. barrierer og brannskille, om farlig gass er oppbevart der osv. Det ønskelig å både se bilder fra personen og hvordan den bever seg i et hus. Vi har enkle systemer som ivaretar det fra gammelt av. Vi har røykdykkerapparat som er slik at hvis en person legger seg ned og blir liggende i ro i et visst antall sekunder, ikke beveger seg, så begynner alarmen å pulse mer og mer, til slutt slår den seg ikke av. Det å se at de beveger seg betyr på mange måter at de er ok. Da kan vi jo se om vi til og med kanskje hvis det ikke er for ille miljø inne i brannrommet, kan vi se om de er på vei til å dra ut et offer eller andre ting. Så generelt er det med å kunne streame og selektere den streamen. Etter hvert som du får veldig mange kanaler som streamer inn så er det viktig at du velger riktig, hvilken stream er det vi ønsker å se. Så du får den viktigste informasjonen. |
| 77 | I | Så er det veldig mange som sier det, og politiet har vært restriktive mot det, at du i stab og strategisk og operativ så blir du nedlesset av informasjon. Hvordan håndterer du dette, for det kommer til å forstyrre deg i de strategiske avgjørelsene. Det er det de nye personene i stab og operativ ledelse må lære seg, å sjonglere mellom mange informasjonskilder og koke ut den essensielle informasjonen til enhver tid. Det er det som blir det nye stabsarbeidet, å både kunne jobbe i det strategiske og operative perspektivet, men samtidig tåle å få mye informasjonsflyt inn og sortere denne. Og så er det hvordan du velger verktøy som automatiserer dette for deg ved at når kameraet til en røykdykker inne er på, sånn og sånn, så streames det inn. Når han ikke gjør noen ting eller er sånn og sånn, hvis han tar av seg maska og er ute, så shuttes feeden ned. Automatisere. Hvis det er sånn at en innringer er på videofeeden så får den første pri i feeden og sånne ting. Det er ikke sikkert at de reglene jeg lager nå er aktuelle, men hvis du lager visse kriterier til å si hvordan de automatisert blir satt i rekkefølge på prioritet, så kan du klare å håndtere større mengder av informasjon da. |
| 78 | L | Mhm. Så for å ta et steg mer overordnet igjen. Av det du forteller nå, for å trekke de store linjene, så forstår jeg det som at blant dere som er ute i felt så er det to ting som er hovedbehov. Det er egentlig video primært som blir hovedbehov i fremtiden, men det er kanskje fra operatør til innsatsleder, og så er det fortsatt behov for tale blant de som er ute. Mens mellom de som er ute og operasjonssentralen, når den er operativ, så har du behov for både data med de systemene du snakket om, og video og tale og hele spekteret. I det begrensede scenarioet så er det video og tale. |
| 79 | I | Jada, jeg tenker det. Og så er det det å åpne for datatrafikk for alle mulige former. Sensortrafikk er f.eks. 110-sentralen veldig opptatt av. Ikke bare i forhold til kamera. F.eks. sånn som det er nå så monitorerer vi sensorer på temperaturen på kjelene på Alcoa i Mosjøen. Hvis den går over et visst nivå så går alarmen her. Og da varsler vi. Det har vi gjort |

| | | |
|---|---|---|
| | | fordi Alcoa i Mosjøen er nesten en milliardbedrift. Faller den ned så er jo hele Mosjøen over. Så det er så kritisk. Hvis de kjelene detter ned så kan de ikke startes opp igjen. Det er en hjørnesteinsbedrift der, og vi har valgt at det er så viktig at vi har godtatt å ha en alarm. |
| 80 | I | Poenget er, i dag er det video og andre former for data som skal sendes. Poenget er at du skal kunne sende nesten ubegrensede mengder med data i det her løpet. Det er det jeg tenker. Jeg tenker data skal være tilgjengelig på alle feltene fordi man ikke skal begrense. Det er det som har vært problemet med Nødnett. Det ligger jo helt åpenbare begrensninger i Nødnett som det er i dag. Det er det vi vil få bort. Vi hadde et møte ganske tidlig i KVUen, og da var politiet ganske tydelige på at det er tale de vil ha. Og det er greit, men jeg tenker at det som er viktig hvis man skal møte framtiden og mulighetsrommet som er der, så må man være åpen for hva som kan ligge i alle kanalene, liksom. |
| 81 | E | Et kjapt spørsmål bare nå når vi går mot slutten her. Det du nevner med at dere benytter dere av kommersielle nett i dag, har dere egne avtaler med de kommersielle aktørene som går på prioriterte abonnement for eksempel? |
| 82 | I | Vi har prioriterte linjer på alt som går inn til sentralen. Det er sånne gullavtaler på alt av linjer, både datalinjer og telefonlinjer. Noe av det er gjennom dette nasjonale systemet gjennom DSB og BDO. Alt det andre vi også kjører som er opp mot Locus som omtrent bare er oss, er også av den karakteren. Men mobiltelefonene der ute har ingen har ikke noen annen prioritet enn at de er del av en prioritert kunde hos Telenor bedrift. Så vi får ikke noe... Men det vi har gjort f.eks. på Incendium er at vi har en sånn Incendium Pack, den som kjører med dronestreamingen. Så de dronepilotene har en egen ryggsekk som det ligger en ruter i, som har tre eller fire eller fem forskjellige SIM-kort fra forskjellige leverandører. |
| 83 | L | Mhm. For maksimum redundans? |
| 84 | I | Ja. Så den kan bruke alle hver for seg etter som de detter ut, og den kan også koordinere de sammen og bruke dem felles for datatrafikk for å overføre. Så du har ganske bra båndbredde, i tillegg til at du har bra redundans. Så det er en måte å gjøre det på. Det her er sånn som flere av de store brannvesenene har gjort i mange år, at de driver og utvikler på egen hånd. Nå er det bare at det burde bli en nasjonal prosess rundt det og ta en felles utvikling mot det. Men det er det som er fint med det kommunale brannvesenet, det at det er ingen som dikterer hva vi skal ha fokus på, ut over de faste, formelle, lovmessige kravene vi skal ha for å ha en brannberedskap. Så når vi utvikler så står vi ganske fritt. Politiet er jo en mye sterkere organisasjon, og det samme med helse, men de er hele tiden låst av de ideene som skjer ute blant mannskapene som har en veldig lang vei for å komme seg opp i systemet. Vi kan bare si at vi setter av noen penger, og så kjøper vi denne videoveggen hvis det er penger til det. Så det gjør at vi er de som er drivere av den teknologien her. Men jeg synes ikke det heller er rett, det er jo ikke kommunene som skal stå for nasjonal utvikling på det her området. Det blir kjempespennende. |
| 85 | I | Jeg tror 5G er løsninga, og jeg tror det at en app i mobilen, en app-lignende løsning er mer egnet enn å lage enn ny telefon. Som har et sikkerhetsnivå i seg, og som sier hvilket sikkerhetsnivå som er oppe. Er du grønn, rød eller oransje mtp. sikkerhetsnivå. Hva kan du prate om, hva kan du gjøre. Da kjenner du til det, det er den telefonen du er kjent med. Det tror jeg er en base som heller ville fungert. Men det er min personlige mening. Men det er det som går igjen. Lager du en egen enhet blir den kjempedyr, kjempevanskelig å få tak i, må bestilles, må ha egen, spesiell opplæring. Det er sikkert noen brukergreier der du må ha en sånn spesiell radio fordi sikkerheten må være så og så høy, men generelt sett for deltidsmannskap går det ikke sånn tale over denne her uansett. |

| | | |
|---|---|---|
| 86 | L | Ja, så for dere så er det fryktelig viktig dette her med brukervennlighet, med andre ord. At det skal være lett å lære opp. |
| 87 | I | Ja, ekstremt viktig. At det skal være lav brukerterskel, hva enn det medfører. Jeg tror også at det å kunne bruke private, sivile verktøy gjør det både billigere og mer rimelig. For det er klart at et sånt garnityr til den her typen radio er sånn 6000 kroner. Kjøper du garnityr til en iPhone til 6000kr så har du det råeste på markedet. Så det gjør at vi blir veldig spesielle og det er aldri bra. |
| 88 | L | Jeg tror vi får begynne å runde av her, men vi fikk utrolig mye gode innspill av deg her nå. |
| 89 | I | Så bra, takk. |
| 90 | L | Er det noe du føler vi burde ha spurt om, når du har hørt litt om temaene? |
| 91 | I | Nei, det spørs hvor bredt dere går. Jeg tror det er veldig at denne utbyggingen av 5G blir dimensjonert på en sånn måte at man bruker nytten som er i privat næringsliv og at det er statlig drift. At man får full utnyttelse. Men det er de på tråden på, hvordan det skal driftes. |
| 92 | L | Det fikser Eivind, hehe. |
| 93 | I | Det er kjempespennende. Det er gode muligheter. |
| 94 | L | Ja, supert. Vi kommer til å skrive transkript intervjuet og sende det til deg så du kan se om det er greit. |
| 95 | I | Det er helt sikkert greit. |
| 96 | L | Håper det er greit at vi eventuelt følger opp tråden på noen ting her hvis det blir behov? |
| 97 | I | Det skal du bare gjøre. |
| 98 | E | Takk skal du ha! |
| 99 | | Ha det godt! |

# Appendix K
# Police Services

In this interview we speak to two representatives of the Norwegian police force who are knowledgeable about how the Norwegian police uses Nødnett today. Topics of conversation include how officers of the police handle limitations of the current Nødnett, such as limited data transfer capabilities, how they plan for and deal with the eventuality of losing reception in critical moments, and what expectations and concerns the police force have in regards to NGN.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, da er opptaket på, og så spør jeg om det er greit at jeg gjør lydopptak. |
| 2 | I1 | Det er greit for meg i hvert fall. |
| 3 | I2 | Det er greit. |
| 4 | E | Supert. Jeg kan begynne med å presentere min egen oppgave. Dere har kanskje sett i informasjonsskrivet, men fokuset er på utfordringer knyttet til samarbeid med kommersielle operatører i utførelsen av NGN. Spesielt da i kjernenettet, med tanke på at man uansett skal samarbeide med kommersielle operatører i radionettet så er spørsmålet om hvordan man skal gjøre det i kjernenettet. Pros and cons med ulike modeller for det. |
| 5 | L | Jeg ser på en litt mer teknisk oppgave. Jeg ser på tilfellet der en eller flere BS i Nødnett mister tilkoblingen til kjernenettet må virke som en isolert øy. Jeg ser på det i 5G, sånn som Eivind gjør. Kort forklart. Så jeg er spent på å høre hva slags behov politiet har. Hva er det som skiller deres bruk av Nødnett fra de andre etatene og hvordan dere ser på disse forskjellige problemstillingene. |
| 6 | I1 | Ja, det er kjempespennende oppgaver, og vi vil jo gjerne bidra til at dere får både god informasjon og at dere får det dere trenger, men så er det det at i og med at vi er i en prosess med å anskaffe det nye. Eller, vi har jo ikke kommet dit en gang egentlig, vi vet ikke helt hva vi skal gå videre med, men nettopp derfor så kan det være noen ting vi ikke kan si. Men det har dere forståelse for såvidt jeg har skjønt, så det får vi i så fall bare ta underveis. |
| 7 | E | Ja. Og hvis det er noe man sier som man kanskje ikke burde ha sagt, så er det også mulighet for å redigere det transkriptet i etterkant. |
| 8 | I1 | Ja, ellers må vi ta beslag i lydopptaket ditt, hehe. Nei, det tenker jeg vi skal klare å få til. Så det skal gå bra. |
| 9 | L | Det er bra. Har dere lyst til å starte med å fortelle litt om hvem dere er, og hva slags rolle dere har opp mot Nødnett? |
| 10 | I1 | Det kan vi gjøre, vet du. Jeg kan starte, og så kan du ta etterpå, [I2]. [Introduksjon]. Å ha ansvar for det betyr ikke at jeg har inngående fagkunnskap om det, og derfor synes jeg det var ålreit å ta med [I2] fordi han har mye mer erfaring med den faktiske bruken av Nødnett, langt mer faglig kunnskap om det tekniske. Og så kan jeg estimere om behov og brukeropplevelser, og samhandlingsbiten med de andre nødetatene, tenker jeg sånn i utgangspunktet. |
| 11 | I2 | Ja. [Introduksjon]. Også har jeg vært med på brukersiden på disse brukersamlingene i KVUen som er gjort nå i forbindelse med det nye, fremtidige Nødnettet, og prøvd å mene noe der på vegne av etaten sammen med flere andre. Jeg har ikke inngående teknisk kunnskap, og vet kanskje enda mindre om 5G sånn sett. Så ut over det jeg har hørt og fanget opp i diskusjoner så har jeg ikke så mye å bidra med sånn teknisk på deres nivå, men vi har nå noen oppfatninger om hvordan det burde være. |
| 12 | L | Nei, det er bra. Det er jo primært synspunktet deres som politi som vi er mest interessert i her nå, så det her tror jeg blir veldig bra. Vi kan kanskje starte med å snakke litt om brukertjenestene dere bruker i Nødnett i politiet. Vi driver og snakker med de forskjellige brukerorganisasjonene om dagen, og er litt interessert i hva slags tjenester som brukes og |

| | | |
|---|---|---|
| | | mellom hvem i vanlig bruk av Nødnett. Eksempelvis, brukes primært gruppesamtaler mellom operasjonssentral og folk i felt? |
| 13 | I1 | Jeg tror det er det som er hovedbruken av det. [I2] fyll gjerne på, men det er i hvert fall det som er rutinene sånn i utgangspunktet. Og hvis du tenker på dette med 1-1-samtale i tillegg så vil det være behov for det innimellom ut ifra en konkret situasjon kanskje. I hovedsak er det de definerte gruppene som er per distrikt. |
| 14 | I2 | Ja, det er riktig det. Politiet sin bruk er jo... Det er vi som bruker det mest, snakker mest, i dagens Nødnett. Vi bruker i svært stor grad talegrupper og ikke 1-1-samtaler. Det er vel mønsteret i vår bruk. Antall klikk er ganske høye hos oss, sammenlignet med de andre. Både mellom enhetene våre, men veldig ofte går kommunikasjonen vår via operasjonssentralen. |
| 15 | L | Mhm. Jeg har fått med at flere andre brukerorganisasjoner bruker en device i tillegg som bruker kommersielle nett til datatjenester. Brukes det i politiet også? Som ikke bruker Nødnett? |
| 16 | I2 | Nei, eller vi har en eller to piloter hvor vi tester ut det her. Den jeg vet om, det er jo politiets utlendingsenhet som bruker den når de er utenfor Nødnettdekning så de har en bærer via mobilnettet til en Nødnett talegruppe. Det er stort sett når de er utenlands at de tester det ut. Jeg vet veldig lite om den testingen, uten at den pågår. |
| 17 | L | Så det er ikke så stort behov for datatjenester, eller stor bruk av datatjenester? |
| 18 | I2 | Jo, men vi bruker ikke Nødnett til det. Vi bruker datatjenester ellers, men da er vi per i dag avhengig av de kommersielle aktørene og bruker vanlig 4G med de begrensningene det har. Derfor har vi heller ikke gjort oss kritisk avhengige av datatjenester, fordi at det er andre krav til de kommersielle nettet enn vi vil stille til et nød- og beredskapsnett. |
| 19 | L | Ser du for deg at det vil stilles kritiske krav til datatjenester i NGN, hvis det er mulig? |
| 20 | I2 | Ja, det må det jo gjøre. Vi er veldig opptatt av tilgjengeligheten til tjenestene våre, og når vi gjør oss avhengige av noe ut ifra arbeidsmetodikk og hvordan vi jobber, hva vi må ha for å løse oppdraget, så vil vår arbeidsmetodikk begrense seg hvis vi ikke er sikre på at løsningen har hvert fall en viss tilgang. Sånn som i Nødnett er det jo 99.95% som er kravet som vi forholder oss til. Vi skulle gjerne hatt bedre, men det er en balanse ift. økonomi og kostnader for å få til de siste desimalene. |
| 21 | L | Nå snakker du om befolkningsdekning? |
| 22 | I2 | Nei, oppetid, altså tilgjengelighet av tjenestene. |
| 23 | I1 | Også blir det jo viktig for oss, kanskje et av de viktigste momentene for oss inn i NGN, den sikkerheten i det kommersielle nettet, i den delen som vi skal bruke til nødkommunikasjon. Fordi vi håndterer personvernopplysninger, vi håndterer sensitive opplysninger om helsetilstanden til folk, vi håndterer informasjon om folks kriminelle historikk. det kan ikke være utad, det kan ikke falle inn i feil hender, det kan ikke være mulig å lytte på det, ikke sant. Der har jo Nødnett hjulpet oss veldig i forhold til hva vi hadde før med det gamle sambandet som alle sammen lyttet inn på. Den situasjonen kan vi jo ikke ha i det nye kommersielle nettet. Der vil vi være ganske tydelige på en del krav. Selvfølgelig sammen med helse og brann, men det er kanskje helse og vi som er mest opptatt av sensitive opplysninger og riktig håndtering av det. |

| | | |
|---|---|---|
| 24 | E | Når du sier... Er det først og fremst konfidensialiteten på innholdet i kommunikasjonen som er viktig, eller er det også f.eks. informasjon om mobilitet i mobilnettet også? F.eks. informasjon om hvor enheter befinner seg til enhver tid. |
| 25 | I1 | Begge deler. Det vil helt klart være informasjon som er unntatt offentlighet, og til tider også gradert informasjon som da rammes inn av sikkerhetsloven. Og da er vi jo over på en helt annen teknisk innretning av et kommunikasjonssystem. |
| 26 | L | Så med den løsningen som er i dag, deler dere sånn informasjon kun gjennom talegrupper for å ha det på den krypterte standarden som Nødnett tilbyr? |
| 27 | I1 | I dag brukes Nødnett til å dele informasjon som er opp til gradert. Vi kan ikke dele begrenset informasjon der, så det gjøres ikke. Da må vi inn på graderte systemer som vi har på stasjonen for å dele det. |
| 28 | L | Nemlig, hm. Så dette er en måte dere skiller dere litt i hvert fall fra brann, sannsynligvis, med at dere har såpass sensitiv informasjon. |
| 29 | I1 | Ja, nå får brann si noe om hvilken informasjon de har å dele på Nødnett, men de har ikke nødvendigvis det samme ansvaret hverken for helseopplysningene til folk, eller informasjon som går inn på folks personvern, som vi gjerne håndterer. Enten ved å identifisere folk, eller ved å dele informasjon ut til våre mannskaper fra operasjonssentralen som går på f.eks. historikk, som gir patruljen en mulighet til å danne seg et situasjonsbilde av hva de går inn i. Da kan det ligge informasjon der som er sensitive opplysninger. I den grad brann har, ikke tror jeg de har så mye av det, og ikke tror jeg de deler så mye av det heller, for de er mer på håndteringsbiten knyttet til sitt mandat. Men de må de si noe om. Jeg vet ikke om du, [I2], har noe mer på det? |
| 30 | I2 | Nei, vi jobber jo litt på ulike måter, også under ulikt regelverk. Utover vanlig offentlighetslov så har vi også andre. Og som du sier mye oftere bruk av opplysninger som er sensitive. Og så er operasjonssentralen og taletrafikken vår, den er nok hyppigere mellom operasjonssentral og patruljer enn et brannvesen. De har veldig ofte statiske oppdrag som de blir utalarmert til, og når de er framme så deles informasjonen på stedet uten at deres 110-sentraler er like involverte i det oppdraget som våre sentraler er. Det er litt ulik metodikk. Vi har ofte dynamiske eller mobile oppdrag, mens de møtes gjerne lettere fysisk og slokker en brann eller bidrar på en trafikkulykke. Da er de på stedet sammen og deler informasjon der. |
| 31 | L | Nemlig. I oppgaven min ser jeg på tilfellet der et område blir isolert fra kjernenettet. Da kan vi se på kanskje to forskjellige scenarioer. Et der vi har et område som er isolert, som ikke innebærer et kontrollrom, så operatørene som er i et område kun kan kommunisere med andre der, og ikke med kontrollrommet. Kanskje vi kan starte der, for jeg forstår det som at det blir ganske kritisk for politi hvis de ikke når sin kontrollsentral? |
| 32 | I1 | Ja, det vil det jo bli. Men så har man jo da, nå får du korrigere meg hvis jeg sier feil [I2], men da har man muligheten til enten å bruke 1-1-samtale der og da hvis det er veldig akutt, men det tar veldig mye kapasitet. Ellers har man også benyttet at man kjører ut sånne mobile stasjoner, men det tar tid. Det er viktig at vi har planer for en sånn type situasjon. |
| 33 | I2 | Vi er jo sårbare for at nettverket ikke henger sammen. Det er funksjonalitet i dagens Nødnett som gjør at en BS kan stå alene og dele dekning med de som er innenfor dekningsområdet. I statiske hendelser gir jo det tilstrekkelig mulighet for oss til å jobbe ut oppdraget normalt sett. Våre patruljer kan også være ganske autonome, og er forberedt på å ende opp uten kommunikasjon. Men det er klart, det blir ikke noe mindre kritisk når vi |

| | | |
|---|---|---|
| | | etter hvert etablerer et behov og en avhengighet til flere digitale tjenester og flere datatjenester. Da kan man risikere at støtteverktøy og sånt ikke er tilgjengelig for å innhente informasjon eller dele informasjon når det er behov for det. Og så er det sånn at vi har i dagens Nødnett så kan man ha en sånn walkie-talkie-funksjon, radio til radio, i sånn direktemodus som jo hjelper så lenge man er innenfor en viss rekkevidde av hverandre, selv om oppdraget er i bevegelse. Der kjenner ikke jeg til at 5G har en løsning som erstatter det enda, ift. sånn kommunikasjon uten et nettverk. |
| 34 | L | Det finnes i standardene til 3GPP, men noen implementasjon kjenner jeg ikke til enda. Det er litt interessant, det at det isolerte scenarioet begrenser deg til bruk i en statisk operasjon, mens direktemodus kan være en løsning når det er dynamisk og ikke bare innenfor det lokale området. Har du noen tanker om hvilke brukertjenester som kan være nødvendige da, hvis kun operatørene kan snakke med hverandre og ikke kontrollrom? Er det da noe vits med video- eller datatjenester? |
| 35 | I1 | Ja, jeg tenker jo det. Dekning for oss blir jo ekstremt viktig for å få gitt et bilde tilbake til operasjonssentralen om hva vi står ovenfor. Jeg mener i fremtiden at en ting er tale, det er bra det, men hvis du ikke har mulighet til å gi tale og gi uttrykk for hva du står i, er kanskje bilde eller film en bedre måte å overføre informasjon på, sånn at man i større grad får en forståelse av situasjonen. Det kan f.eks. være så mye støy der at man ikke klarer å høre hva som blir sagt på stedet, mange mulige situasjoner der. For vår del vil det være ekstremt viktig med dataoverføring i fremtiden, fordi at det er færre og færre som bare driver med tale i kommunikasjon. Man driver ofte med både video og bilde nå, kanskje mer enn man driver med. Hvis det var det du spurte om. |
| 36 | L | Nødvendigheten for det, blir det mellom operatør og kontrollrom, ikke mellom operatørene hvis du ser på dem isolert fra kontrollrommet? |
| 37 | I1 | Jeg tenker det blir mellom alle operatørene som er både i patruljen ute på stedet, men også i kontrollrommet, sånn at man har det felles bildet da. |
| 38 | I2 | Hvis man ser for seg at scenarioet der man ikke har mulighet til å sende disse dataene via nettverket til noen som er utenfor dekningen av en bestemt BS, vil fortsatt det i svært mange tilfeller være nyttig, så lenge man drifter et oppdrag i en hendelse. Når det er koordineringsbehov, hvis politiet har mer enn et par patruljer på plass eller det er flere etater, så har vi ansvar for innsatsledelse på stedet. Denne stedlige innsatslederen har jo da behov for denne muligheten til å dele. Vi snakker veldig mye om muligheter for å dele video, altså push-to-video som er nærliggende og som vi antar at vil bidra veldig mye i forhold til det å få raskere etablert et felles situasjonsbilde og felles forståelse etter hvert, med at man tolker bilder og raskt kan f.eks. se omfanget av noe eller få et inntrykk av forholdene på stedet. Innsatslederen vil jo være i nærheten av de patruljene som jobber på oppdraget og vil dra nytte av det, uavhengig av om også operasjonssentralen også har mulighet til å se det samme. Så ledelseselementet vårt ut taktisk, som vi sier, det vil uansett ha nytte av datadeling. |
| 39 | L | Mhm. Det gir mening. |
| 40 | I1 | Mens vi er inne på temaet. Det kan være greit for dere å vite. Det er ikke vi som har ansvaret for det, men det juridiske omkring deling av data, det er ikke på plass. Det er noe vi har etterlyst overfor justisdepartementet. Deling av informasjon, altså regelverket rundt hvordan vi har samlet inn informasjon og deler den videre, det er ikke tilstrekkelig på plass mener vi. Det er noe som hører med inn i videre utvikling. Hvis vi skal gjøre det på riktig måte, og lovmessig måte ikke minst, så må det på en måte sees litt på regelverket rundt det. |

| | | |
|---|---|---|
| 41 | L | Vil du utdype litt på hva slags data du mener og hva slags innhenting og deling du snakker om? |
| 42 | I1 | Et eksempel kan være data som vi samler inn f.eks. ved bruk av sensorer. Vi har noen biler i politiet som automatisk tar inn trafikkskilt, altså bilskiltkontroll. Den informasjon kan vi per i dag ikke dele med andre etater. Den må vi kun bruke hos oss selv, innenfor en veldig begrenset bruk. Det kan være et eksempel på noe sånt. |
| 43 | L | Mhm. I dag brukes sannsynligvis ikke Nødnett til den typen dataoverføring, gjør det det? |
| 44 | I1 | Nei, det er ikke mulighet for det. Annet enn tale, selvfølgelig. Hvis man deler informasjon i talenettet i en pågående sak, så er ikke det noe problem. Men innhenting via sensorer automatisk, så du får den stordata-delen av det, da blir det et problem. |
| 45 | L | Så hvis dere vil tenke litt visjonært på NGN, så er det et ønske å ha maskin-til-maskin-kommunikasjon og sensordata over et trygt Nødnett? |
| 46 | I1 | Det kommer litt an på, tror jeg. Men poenget er at vi i alle fall må ha muligheten til å overføre mer enn tale. Vi må kunne bruke data på en annen måte i fremtiden for å dele et situasjonsbilde i nødkommunikasjonskanalene våre. |
| 47 | E | Hvis vi går litt mer på de kommersielle tjenestene som brukes i dag. Er det noen begrensninger med tanke på at man benytter seg av kommersielle nett, f.eks. sikkerhetsmessig eller personvernhensyn som gjør at man holder litt igjen med tanke på hvilke tjenester man benytter i de kommersielle nettene? |
| 48 | I1 | Ja, jeg kan begynne litt jeg. Per i dag, f.eks. når vi bruker mobiltelefon så kan vi ikke si noe informasjon over mobilnettet som spesielt ikke er gradert. Det er rett og slett ikke sikkert nok. Men i tillegg så skal vi jo ikke bruke det helst til informasjon som er unntatt offentlighet heller, for det er jo faktisk et offentlig nett, men vi kan jo ikke tenke at alle sammen avlytter mobiltelefonene til politiet. Så vi må finne en balanse, må være pragmatiske på det. Noen ganger er det mobiltelefoner man har for å dele informasjon, og f.eks. i en akutt situasjon så må man dele det som er nødvendig, men man må gjøre en vurdering hvis du ikke har Nødnett tilgjengelig. For Nødnett er jo sikrere enn det kommersielle mobilnettet til sånne typer opplysninger. Sånn umiddelbart så er jeg skeptisk til bruken av det mobile nettet per i dag, for det en telefon for oss som vi bruker til å avklare praktiske ting, og litt som andre folk bruker en telefon. Men med deling av informasjon, der man skal man være forsiktig. Hvis det var svar på spørsmålet. |
| 49 | E | Ja, jeg synes det er interessant å høre. Du nevnte også at dere har egne graderte systemer for informasjon som er for hemmelig for Nødnett. Kan du utdype litt om det? |
| 50 | I1 | Nei, ikke hemmelig på Nødnett. Sikkerhetsloven gir rammer for hvordan gradert informasjon kan deles enten internt i politiet eller mellom etater. Da har vi kun noen få, godkjente systemer på data, men det er de faste PCene inne på stasjonene som er godkjent for sånn type kommunikasjon. Nødnett er ikke godkjent for å dele gradert informasjon. |
| 51 | E | Nei. Og det er noe man tenker at heller ikke kommer til å bli aktuelt i fremtiden? |
| 52 | I1 | Nei, jeg vet ikke [I2], om vi skal bruke noe tid på det de siste årene vi har Nødnett. Vi har jo jobbet littegrann med det, men.. |

| | | |
|---|---|---|
| 53 | E | Jeg tenker med det nye Nødnettet? |
| 54 | I1 | Det er jo NSM som bestemmer det, så det må nesten de si noe om. Det er de som godkjenner sånn type bruk i så fall, og hvilke endringer man må gjøre for å få til det. |
| 55 | I2 | Jeg kan komme til litt på det, for det er klart at vi skulle ønske, det hadde vært veldig praktisk om det nye nettet kunne håndtert gradert informasjon. Nå er det sånn at rent teknisk, nå er det sånn at i politiet sin del av Nødnett der vi har ende-til-ende-kryptering av talegrupper, så teknisk er det sikkert nok til å ha noe gradert informasjon der. Men den store utfordringen er administrasjonen og forvaltingen av radioterminaler og sånne ting. Det ville vært et helt annet regime. Det er fortsatt ikke sånn at tjenestemenn tar med seg radioer hjem hvis ikke det er tjenestelig behov for det, men dette med å holde de innelåst og sånt, det ville vi måtte hatt et annet regime på. Så jeg tror nok det er en del praktiske ting som kreves, som vil være den største bøygen for å gjøre det. Og så kan man se for seg at man kan få et eget lag i et nytt nett med et fåtall terminaler med tilgjengelighet, som man kan ha et sånt regime på. Men for at vi skal ha 17 000 brukere som skal ha hver sin radio og ha kontroll på den, så det antakeligvis ikke være praktisk og hensiktsmessig å ha et nett som ivaretar sikkerhetsloven sånn. Men det er klart at vi ønsker oss noe enklere for å kunne også dele gradert informasjon, for det blir innimellom litt mer klønete for oss. Og så er det sånn at når krisen står på, helt inn i initialfasen så deler vi det som trengs for å redde liv eller andre viktige oppgaver. Da er det andre ting som teller mest, men det er klart at det er begrensende for oss at vi må ta hensyn til hvordan informasjonen vi deler er beskyttet. |
| 56 | L | Er det systemet i dag da mellom kontrollrommene? Det er der dere kan dele? |
| 57 | I2 | Ja, mellom kontrollrommene blant annet kan vi dele. Vi har ikke noe mobile enheter som er tilgjengelige for patruljene, sånn at de kan få gradert informasjon ut uten å dra tilbake eller å få det på annet vis. |
| 58 | E | Med disse kommersielle tjenestene, er det noen integrasjon mellom de kommersielle tjenestene som benyttes og Nødnett? Jeg vet f.eks. at brann har en egen løsning der de har noen oppdragstjenester på det kommersielle nettet, og så kan folk page inn på Nødnett og si at dette oppdraget tar vi og sånne typer ting. |
| 59 | I2 | Vi har vel ikke noe kommersielt inn på Nødnett for politiet, annet enn dette pilotprosjektet som DSB kjører og som politiets utledningsenhet er med på, som vi nevnte tidligere, Motorola-løsningen som bruker en kommersiell bærer inn i Nødnett. Vi har ikke noen andre gatewayer inn, eller andre ting fra vår side. Så da går det parallelt. |
| 60 | E | De kommersielle tjenestene, er det karttjenester og flåtestyring og sånne typer tjenester, eller hva er det egentlig snakk om? |
| 61 | I2 | Det er datainformasjon ut til mobilapplikasjoner, eller applikasjoner på en PC som heter informasjon, eller hvor informasjon sendes fra politiet sine systemer og via mobilnettet. Såvidt jeg har skjønt, så er det en sånn sandkasseløsning i dem.. Det godkjente brukerutstyret som er der ute, det er både nettbrett og PCer og mobiler, men da i en sandkasse der de kan logge seg på og hente ut opplysninger. Da er det oppdragsinformasjon, lokasjon, kart som viser hvor enheter er og sånt. |
| 62 | L | Jeg vet ikke med deg, Eivind, men jeg har ikke helt klart for meg oppe i hodet mitt hvordan operasjonssentralene er distribuert ut over landet i politiet. For å få litt oversikt over hvor langt det er fra en operasjonssentral til et hendelsessted. For min oppgave er det relevant å se på når regioner blir avkuttet. |

| | | |
|---|---|---|
| 63 | I1 | Ja, det kan vi egentlig sende deg en oversikt over på en enkel måte, som et kart, som kanskje er det mest visuelle hvis du skal ha det i en oppgave. Etter reformen i 2016 så gikk vi fra 27 til 12 politidistrikt, det er du sikkert kjent med. Da gikk vi også ned til 12 operasjonssentraler, så det er bare en sentral per distrikt. Den har sitt hovedsete bare ett sted i distriktet. F.eks. sånn som Nordland, som er et distrikt som har ekstreme avstander og er et ganske spesielt distrikt, fordi E6 går gjennom hele Nordland, men det er over 80 mil fra sør til nord i distriktet, og i tillegg har du småveier som går ut fra E6 ut mot kysten. De har kystlinje langs hele distriktet. De har fem hoved-politisoner som det heter, men operasjonssentralen ligger i Bodø. Fra Bodø ned til Mosjøen er det over 30 mil, kanskje mer. Så operasjonssentralen er ikke i umiddelbar nærhet til der politipatruljen der. Så det er ekstremt viktig for oss at de som sitter på operasjonssentralen har god kunnskap om distriktet, forståelse for de minste tettstedene, ressursene som er få og langt ut. Det var en diskusjon da vi gikk over til bare 12 distrikter selvfølgelig, at de som tidligere hadde jobbet på de minste operasjonssentralene, de syntes det ble veldig problematisk at de nå skulle være så langt unna patruljene sine og så langt unna der det skjedde og man hadde ikke lokalkunnskapen. Men jeg tror jo det, [I2], at hvis du spør dem i dag vil de se annerledes på det. Nå er de mer robust i selve samhandlingen på sentralen, de er flere på jobb samtidig, og med litt sånn at hver har sin kunnskap fra hele distriktet. Totalt sett tror jeg nok at de i dag vil si at de er bedre stilt til å gjøre jobben på en operasjonssentral. Men ja, de er jo langt unna den enkelte. I Finnmark, for eksempel, sitter operasjonssentralen i Kirkenes, det er jo helt øst i distriktet og ganske mange mil, en hel flyreise, fra andre siden av distriktet. Det er store avstander. |
| 64 | L | Kan du si noe om konsekvensen hvis, si at hele denne operasjonssentralen blir frakoblet resten av distriktet. Hvordan fungerer resten av distriktet da? |
| 65 | I1 | Da må det være at operasjonssentralen får tekniske problemer så man ikke har kontakt. Vi kan ikke gå inn på detaljene for det, men vi har planer for hvem som tar over distriktet, hvem som kommuniserer med patruljen og sørger for at de både får informasjonen de trenger og får gitt informasjonen de trenger og får den videre, også til andre nødetater. |
| 66 | L | Ja, og dette er distribuert utover? |
| 67 | I1 | Ja. |
| 68 | E | Jeg tenker litt sånn at nå som vi skal over til NGN etter hvert, så er noen av modellene som har blitt foreslått og som er alternativer, at man involverer kommersielle operatører veldig mye i utførelsen av hele nettet. At DSB kjøper en tjeneste av Telenor f.eks., og at Telenor leverer hele stacken med tjenester. Fra radionett til tjenestelaget, omtrent. Er det noe dere i politiet tenker er en utfordring, sikkerhetsmessig og personvernmessig? Skulle man heller sett at det var en statlig organisasjon som hadde ansvar for det som f.eks. DSB, eller holder det at mobiloperatørene er underlagt sikkerhetsloven? |
| 69 | I1 | Jeg tror ikke nødvendigvis at vi må ha en statlig organisasjon som håndterer det, men det skal jeg ikke ha sagt, hva som er fasiten på det. Uavhengig av om det er en statlig eller en kommersiell aktør som skal drifte det, må lovverket være på plass, det sikkerhetsmessige og tekniske må være på plass, og det må være en avtale som både sikrer at du har nødvendig tilgjengelighet, nødvendig dekning, og ikke minst så må det være nødvendig robusthet i nettet sånn at det ikke ramler ut plutselig, eller at noen har gravet opp en kabel og så er hele distriktet uten kommunikasjon, naturlig nok. Du må ha redundante løsninger. Det spiller ingen rolle om det er en kommersiell aktør eller en statlig organisasjon. De samme reglene gjelder for begge. Men det er klart at hvis du skal ha en kommersiell leverandør, så må du i utformingen av det regelverket og den avtalen, så er det klart at de må ha nødvendig |

| | | |
|---|---|---|
| | | forståelse av både lovverket og behovet som aktørene har. Ikke bare politiet, men de andre nødetatene også. Og forplikte seg til at det må være noe eget. Det er greit at det er det kommersielle nettet, men det må likevel være, som [I2] sa i sta, kanskje et eget lag i nettet. Nå kjenner ikke jeg til tekniske ting, men det må være en egen del av det som er spesifikt bygget opp for å dekke de behovene som nødkommunikasjon krever. Jeg vet ikke om du har noen andre tanker, [I2]? Kanskje [I2] er helt uenig, og vil ha en statlig aktør! |
| 70 | I2 | Det er kanskje det som er det store spørsmålet knyttet til denne KVUen også, at man må velge hvor på skalaen, hvor mye skal staten ha. Ytterpunktene er jo at man overlater alt til de kommersielle aktørene, til at staten.. Nå er det ikke lenger aktuelt at staten bygger et eget nett som bærer radionettet også da, det er bestemt at de kommersielle skal ha radionettet. Vi merker oss jo at mange europeiske land har valgt å ha et statlig, eller et offentlig eid kjernenett, mer eller mindre, som de kontrollerer. Jeg tror det blir en sånn, det spørs hvor tett man klarer å følge opp de kommersielle, hvor interessant det er kommersielt å utvikle tjenester og bygge robusthet for nødetatene. Vi er vel 1% av brukerne eller noe sånt i et kommersielt nett, så det er en samfunnsøkonomisk balanse. I en ideell verden for politiet, så ville vi kjent en trygghet i at staten eide alt, kanskje. Men vi ser jo hvor dyrt det er, og ikke minst at kommersielle aktører vil ha en raskere utvikling av tjenester enn det man klarer, kanskje, ved å følge opp fra det offentlige. Så vi er jo spente på i hvilken grad staten kommer til å eie noe som helst i nettet. Men det viktigste er jo hvilke avtaler vi gjør og hvilke risiko vi løper for å bytte leverandører osv., hvordan dette blir spredd og hvordan ansvar ivaretas. |
| 71 | E | Det er ikke noen umiddelbare varsellamper som begynner å blinke hvis man tenker på at f.eks. en kommersiell aktør kommer til å ha oversikt over mobiliteten i nettverket da? For eksempel: Jeg går ut ifra at ting fremdeles kommer til å være ende til ende-kryptert. |
| 72 | I2 | Ja, det vil politiet i hvert fall gå inn for for vår del. Vi har sett, vi har eksempler også i Nødnett da man oppdaget at det ble servet fra India en periode så var vi fornøyde med at vår informasjon var kryptert. Det er klart at man løper en risiko for dette. Det ender vel opp med databehandler og sånt som skal ivareta det og at risikoene er kalkulert. Politiet driver jo ikke med noe som trenger beskyttelse i det daglige i stor grad. Vi har enkelte enheter i politiet som vi er svært opptatt av å passe på, beskytte og holde hemmelig. Men de fleste driver jo med en tjeneste som er ganske åpen og som ikke vi har noe problem med at er åpen. Jeg vet ikke hvor stor andel, men det meste av det vi kommuniserer i dag går jo via ugraderte plattformer. Så vi er ikke så redd for det, men det er klart at noen miljøer som er opptatt av å skjerme seg, de er skeptiske til at metadata finnes, hvis det ikke er kryptert og ivaretatt. |
| 73 | I1 | Og så må vi jo på en måte sikre at det ikke skal være mulighet for å kunne ta ut hvor politiet har vært hen, på hvilke adresser i løpet av dagen ned på et sånt detaljnivå at vi plutselig får problemer både personvernet til folk, og ikke minst at man kan benytte det i kriminelt øyemed. Enten for befolkningen, eller å benytte informasjon om politiet og våre kapasiteter. Sånne ting må vi sikre oss at blir ivaretatt hvis det er en kommersiell aktør som skal håndtere det for oss. |
| 74 | L | Jeg trekker den litt tilbake til tjenestene som du snakket om i sta. Vi snakket litt om at dere så på det som sannsynligvis kritisk i fremtiden med videotjenester både ute i felt og i vanlig operasjon. Jeg lurte på om dere vil diskutere litt hvordan, sett at vi har et isolert scenario enten med eller uten kontrollrom, hvordan ville dere prioritert løsningene? Er det tale som kommer til å være viktigst også i fremtiden, eller ville dere satt eksempelvis videokommunikasjon over, sånn som vi snakket om i stad? |
| 75 | I1 | Ja, vanskelig å prioritere kanskje. Jeg tror det kanskje blir litt situasjonsbetinget, i forhold til |

| | | |
|---|---|---|
| | | at det alltid vil være viktig å ha tale, for det er da du kan være presis med ord og gi kanskje en avgrensning. Et bilde kan være feil bilde, det gir ikke noe særlig informasjon hvis det er et stillbilde f.eks. Men video kan også gi veldig mye mer enn tale på kortere tid, men det kan også gi et mer dramatisk blikk på en situasjon enn det faktisk er. Så de er vanskelige å sette opp mot hverandre tenker jeg. Jeg vet ikke, [I2], hva du tenker? |
| 76 | I2 | Det er et tilbakevendende spørsmål og diskusjon som man har hatt, for vi har jo frem til nå og for så vidt fortsatt understreket at vi har kritisk behov for tale, fordi det er det lettest tilgjengelige og mest universelle som vi har. I en ekstrem situasjon, eller i sånne hendelser hvor ting skjer veldig fort, så er det med tale man kanskje opptrer mest naturlig og klarer å formidle fortest noe uten å ha tilgjengelig spesielle devicer eller noe for å formidle noe, annet enn et sambandssett. Samtidig så er vi litt sånn, vi er jo oppmerksomme på at vi er bundet av den arbeidsmetodikken vi har i dag og de erfaringene vi har nå, og at vi ikke har tatt i bruk nye tjenester. Det er vanskelig å si hvor avhengige vi kommer til å bli av de i fremtiden, for vi kjenner ikke den hverdagen så godt. Vi ser at ellers i samfunnet og hvis du ser på den yngre delen av befolkningen, så kommuniserer man mindre muntlig og mye mer med tekst. Så det er litt sånn vanskelig å si, men per i dag er vi fortsatt der at vi må ha tale og at det vil trumfe alt. Det kan hende det ser helt annerledes ut om ti år. |
| 77 | L | Det er spennende tanker, synes jeg. Og i hvert fall sånn jeg har forstått 5G-oppbyggingen hittil, er det slik at taleteknologien danner minimumskravet som alt annet bygger oppå. Så jeg ser ikke på det som en mulighet per sånn jeg har forstått det nå at du mister tale, men fortsatt har video. Men det er interessant å høre refleksjonene, synes jeg. |
| 78 | E | Litt avslutningsvis er jeg nysgjerrig på hva man tenker om sånne alternative, f.eks. video fra drone eller fra kroppskamera på folk som er ute i felt, for å gi et mer omfattende situasjonsbilde. Er det noen prosjekter på gang med det? |
| 79 | I1 | Vi har jo innført droner i politiet. I 2019/2020 hadde vi et pilotprosjekt i fire politidistrikt. Det var såpass gode erfaringer og såpass positivt, at vi har tatt en beslutning på at vi skal innføre det i alle politidistrikter. Så den jobben går i år. Både med å utdanne dronepiloter, det vil si de som styrer droner, de er faktisk piloter per definisjonen fra luftfartstilsynet sine regelverk, og der har vi også satt på kamera på noen av de dronene. Eller, vi har kamera på alle dronene, men vi har litt forskjellige typer kamera. På de store dronene så har vi kamera som er varmesøkende f.eks., brukes mye i redningsoppdrag. På de mindre har vi kamera som kan overføre bilder og video nettopp for å gi et situasjonsbilde i en situasjon, enten for å ta bilder i forbindelse med en trafikkulykke, eller for å overføre f.eks. store områder, typisk en demonstrasjon som går over et stort område med veldig mye folk så kan du overføre bildene inn til operasjonssentralen for å vise litt mer hva som rører seg. Igjen er vi tilbake på regelverket rundt dette. Det er ganske begrenset per nå hvordan vi kan bruke den typen informasjon og det vi henter inn gjennom de sensorene. Det er og veldig begrenset hvordan vi kan dele den informasjonen og bruke den, ikke minst, som politi per i dag. Men sånne kroppskamera, det har vi prøvd ut i Oslo politistrikt for noen år siden, men det er ikke tatt noen beslutning på om vi skal fortsette. Igjen vil det være det samme regelverket, for det er jo en sensor som henter inn informasjon, og muligheten til å ta opp informasjonen. Per definisjon er det jo ikke noen forskjell på politimannen eller damens øyne som ser ting, eller om det er et kamera som ser det samme. Men i det øyeblikket du kan begynne å ta det opp og ta det frem senere, da kan du begynne å se etter flere ting enn det polititjenestemannen fikk med seg i utgangspunktet. Da går du ut over det som er vanlig informasjonsinnhenting. Da må man bevege seg litt forsiktig og riktig med tanke på hvordan du bruker den informasjonen. |
| 80 | E | F.eks. i redningsaksjoner har jeg fått inntrykk av at det i mange situasjoner kan være aktuelt |

| | | |
|---|---|---|
| | | å dele videofeed på tvers av etater, f.eks. til brann eller helse. Om det er noe som er vanskelig med den måten de kommersielle løsningene funker på i dag, og så tenker man at det blir lettere om man får videoen inn i Nødnett i NGN? At man kan ha disse felles gruppene på tvers av etater der man også kan dele video f.eks.? |
| 81 | I1 | Det tror jeg hadde lettet situasjonen i enkelte sånne hendelser betraktelig, enten om du har Nødnett eller andre kartfunksjoner som alle etatene bruker enten på operasjonssentralen eller ut på mobile enheter. Det er klart at det vil være til hjelp, men det kommer litt an på hvor du er hen i håndteringa tror jeg. I startfasen, kjempefint å få et oversiktsbilde kanskje for å orientere seg om situasjonen. Lengre ut i så er det kanskje for dem som er på stedet i hvert fall viktig å ha den tetteste samhandlinga fysisk på stedet og direkte kommunikasjon og hvordan du håndterer det. Nå snakker vi på taktisk nivå, altså innsatslederne og de som står med hendene midt i og håndterer. Mens for operasjonssentralen eller de andre som bidrar litt lengre ut i systemet, så vil sånne typer bilder og kart være behjelpelig for å kunne estimere hvilke ressurser trenger vi på sikt, hva må vi planlegge med fremover, hvordan kan det her utvikle seg. Så vil det være en annen type bruk for sånne verktøy. Jeg vet ikke hva du tenker, [I2]? |
| 82 | I2 | Dette er en veldig aktuell problemstilling for oss. Vi har behov for å dele. Utfordringen er at vi gjerne ikke har de samme applikasjonene i etatene, og det kan være både proprietære løsninger og løsninger som ikke er kompatible med hverandre. Det naturlige i et nytt Nødnett på 5G vil være at man samarbeider og har noen standarder som sikrer at det man kobler inn der, det kan man dele mellom alle aktørene som bruker det nettet. Der har vi en stor utfordring i dag, og som vi også tror vil få drahjelp av at vi får et felles nett. Vi har sagt det at gevinsten med et nytt nett ikke vil være at vi får en ny plattform vi kan snakke sammen på, men at vi får applikasjoner som er felles og som bidrar til at vi kan dele informasjon effektivt på tvers. Det er ikke noe tvil om at samhandling mellom alle aktørene som driver med beredskap er viktig, og det viser seg stadig at det er sammen vi klarer å løse oppdrag best. |
| 83 | I1 | Absolutt, og jeg tenker jo at det absolutt viktigste for oss i NGN, det er å opprettholde de veldig gode erfaringene og den samhandlingsplattformen vi fikk gjennom dagens Nødnett med de andre aktørene. Ikke bare de andre nødetatene, men det er også mange andre vi samhandler med, som for eksempel frivillige og andre som bruker det nå. At ikke vi kommer i en situasjon hvor vi får noe som er dårligere i verste fall, fordi vi velger forskjellige, eller at de ikke klarer å sette såpass krav at de kommer opp med den samme muligheten, men har verre. Sånne typer ting. Det er kanskje noe av det viktigste fremover nå, å sikre sånne type ting og samhandlingen. For det er ikke noe tvil om at hvis ikke vi klarer det, så tar vi noen steg tilbake i forhold til hva vi har hatt frem til nå. Det blir for dumt, tenker jeg. Så det blir viktig. Men i forhold til det med det vi snakket om med deling av kart og informasjon, nå kan jeg ikke si detaljert hva som kommer frem i evalueringen etter raset på Gjerdrum, men den rapporten kommer før sommeren. Den tenker jeg kan være aktuell for dere, for der tror jeg det temaet blir berørt. Jeg vet ikke hva som står der, men det får dere se da. Den tror jeg kommer før sommeren. |
| 84 | E | Det er bra tips! |
| 85 | L | Vi begynner å tom for tid her. Er det noe dere vi føler vi burde ha vært innom i løpet av samtalen her, som vi ikke har vært borti? |
| 86 | I1 | Nei, jeg tror det var det som jeg har tenkt i utgangspunktet. Men det er bare å ringe eller sende epost, hvis det er noe dere lurer på eller var uklart som dere kommer på i ettertid og. |
| 87 | L | Det setter vi pris på. Jeg synes det var veldig oversiktlig og fint, det her. |

| | | |
|---|---|---|
| 88 | E | Så det som skjer nå, er at vi transkriberer lydopptaket, og så anonymiserer vi det, og så sender vi det over. Da kan dere se over om det er noe dere vil presisere eller trekke tilbake, og om dere synes den anonymiseringen som er gjort er ok. Så samarbeider vi om å sørge for at det blir et ok produkt til slutt som alle kan være fornøyd med. |
| 89 | I1 | Det høres veldig greit ut. Når skal dere levere? |
| 90 | E | Det er tredje uken i juni, så det er enda en stund til. |
| 91 | I1 | Ok. Jeg lurer på om det er mulig å lese over før dere leverer, så vi har muligheten for å se hvordan det blir i konteksten og hele oppgaven. Ikke for at vi skal sette noen begrensninger på den, men det handler litt om at vi vil være sikre på at informasjonen om politiet er riktig og ikke går inn på noe som vi ikke kan gi ut offentlig. Det vil i så fall ødelegge for dere, det er ment som en hjelp til dere. |
| 92 | E | Jeg tror ikke at det burde være noe problem. Jeg tror vi har lov til å sende til dem vi vil. |
| 93 | L | Det setter en liten frist til oss, at vi må være ferdige med skrivingen på et tidspunkt så dere rekker å se, og det fikser vi. Det er bra. |
| 94 | I1 | Nå går vi også gjennom transkriberingen, så der vil vi få luket ut om det skal være noe sånt, men så er det noe med å se det i kontekst som kan være nyttig. Men vi kan bare ha dialogen om det, kanskje. |
| 95 | L | Absolutt. Det er ikke noe problem. |
| 96 | I1 | [I2], hadde du noe du tenkte burde komme frem? |
| 97 | I2 | Nei, jeg håper dere har fått svar som ligner på noe dere trengte. Det er ikke så lett, og dette kunne vi snakket i timesvis om. Jeg tenker også at dere må komme tilbake med spørsmål hvis det er noe som dere trenger noe mer på. |
| 98 | E | Det setter vi pris på. Nå nærmer vi oss slutten på intervjuene, og så blir det et helt eget maratonløp å skulle prosessere alt og trekke ut noen konklusjoner. |
| 99 | I2 | Ja, ikke sant. Det er spennende oppgaver, i hvert fall. |
| 100 | I1 | Veldig. Det blir spennende å lese. |
| 101 | L | Tusen takk for at dere tok dere tiden! |
| 102 | I1 | Bare hyggelig, takk skal dere ha! |
| 103 | E | Ha det godt! |

# Appendix L
# Mobile Network Operator D

This interview is conducted with a representative of one of the three mobile network operators in Norway. By the pigeonhole principle it could easily be deducted that this interview subject has to be representing one of the same mobile network operators as at least one of the three previously presented representatives of mobile network operators. The figuring out of which one that might be, however, is left as an exercise to the reader. The topics of conversation in this interview range from general considerations of 5G and related technologies, to more specific considerations regarding alternative deployment models of NGN.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Så da har jeg satt på lydopptaket, og så spør jeg om det er greit at vi gjør lydopptak. |
| 2 | I | Ja, det er greit. |
| 3 | E | Så, min oppgave konsentrerer seg om kjernenettet i neste generasjons Nødnett. Spesifikt ser jeg på 5G-mulighetene og utfordringer rundt samarbeid med kommersielle Nødnett, og alternative måter for å realisere neste generasjons Nødnett i kjernenettet da. |
| 4 | L | Ja, jeg er litt mer ute i radionettet. Jeg ser på hvordan man kan ha autonome basestasjoner, eller en gruppe av autonome basestasjoner, i 5G for neste generasjons Nødnett. Og for deg da, så er det kanskje interessant å snakke om hvordan man kan realisere og kjøre et parallelt kjernenettverk ute i edge. Det kan vi ta litt når det passer seg. |
| 5 | I | Jeg vet ikke så mye om autonome basestasjoner og hva det innebærer, men det er interessant å vite hva det har å si for kjernenettet. |
| 6 | E | Så, nå har vi jo hørt litt om deres foretrukne metoder, og det involverer ganske tydelig den DSB-eide MVNOen, som er front and center der sånn jeg har forstått det. Noe som er litt forskjellig fra de andre operatørenes forslag. Så jeg har et par spørsmål rundt ulike måter man kan realisere en sånn MVNO-løsning i 5G, med tanke på den arkitekturen man får i 5G-nettet som kanskje er litt annerledes enn sånn det fungerer i dag. Og så har jeg noen spørsmål også om noen av de andre operatørenes forslag. Spesielt det som går på det med å bruke flere kjernenett for å få den ekstra redundansen og robustheten, og da på en måte ha Nødnett-tjenesten som et tjenestelag på toppen. At man har en push-to-talk-tjeneste for eksempel som kan kommunisere med alle de tre nettene, og at man bruker vanlige funksjoner for nasjonal roaming og sånt for å kommunisere på tvers av nettene. Men, ja, en av de tingene jeg er litt interessert i er på en måte det med hvordan en MVNO kommer til å se ut i 5G, eller hva man tenker om det. Spesielt med tanke på om man skal ha hele stacken med kjernenettkomponenter, og hvordan man skal gjøre det i forhold til for eksempel AMF og sånt. Om en MVNO vil ha sin egen AMF som de kobler direkte på basestasjonene, eller om man må bruke gjesteoperatøren sin AMF. |
| 7 | I | Ja, jeg har tenkt litt på det. Det er litt forskjellige muligheter, men ihvertfall i det oppsettet hvor Nødnett har sin egen AMF, så kaller du det ikke lenger MVNO sånn som jeg kjenner det. Da har du mer det du kaller MOCN, hvor du deler radionett. Det er brukt av noen operatører i Danmark, Sverige og Finland blant annet, hvor de går sammen om å bygge felles radionett, og så har de egne kjernenett. Så det er ikke et typisk MVNO-oppsett. En typisk MVNO er ala det samme som du har når du roamer, hvor den som eier radionettet også har AMFen, men der du har din egen kundedatabase, UDM tror jeg det er i 5G, og sånn gateway for pakkedata, UPF på 5G-coret. Så det er ihvertfall to forskjellige oppsett, om du har et sånt MOCN-oppsett eller om du har MVNO. Jeg har blant annet sett at de i Finland kjører det MOCN-oppsettet. De har en egen nødnettintegrasjon hvor de leier radionettet fra Elisa, og så har fullt kjernenett hos seg. Jeg vet ikke om de er på 5G forsåvidt, men de har ihvertfall tilsvarende på 4G. |
| 8 | E | De skal vel sikkert over på 5G uansett etter hvert. |
| 9 | I | Sikkert det, ja. |
| 10 | E | Så da tenker jeg litt sånn i den norske konteksten da. Argumentene for at DSB skal ha sin egen MVNO - Da tenker jeg at man fort kommer inn på at tjeneste og data skal være sikkert, |

| | | |
|---|---|---|
| | | og at man skal beholde integriteten i nettet og sånn. Men når man da er avhengig av gjesteoperatørens AMF, så vil man jo da for eksempel kunne ende opp med å lekke mobilitet til gjesteoperatøren, som kanskje kan være bekymringsverdig for politiet for eksempel. |
| 11 | I | Ja, som et sikkerhetsaspekt, ja. Det er klart at operatøren har mer innsikt i hvor du er, typ lokasjon og andre ting, enn om du hoster den AMFen i eget nett, det er sant. Så det er noe man må avklare eventuelt. |
| 12 | E | Mm, og hvis man da skal ha et MVNO-oppsett der man ikke har sin egen AMF og sånt - Jeg er litt nysgjerrig på hvordan det fungerer - Jeg har skjønt at man fort begynner å involvere network exposure function? |
| 13 | I | Ja, akkurat det er på en måte et eget kapittel for seg selv den der network exposure functionen. Kanskje et litt ubeskrevet kapittel egentlig. Du må ikke bruke den, men det er på en måte en mulighet for å kunne eksponere nettverket til Nødnett. Sånn at Nødnett kan se typ status på terminaler, om de er koblet på eller ikke, kanskje provisjonere ut data for abonnenter ... Så jeg tror egentlig det med network exposure det er en sånn egen greie egentlig. Det er ikke noe du nødvendigvis må bruke, slik jeg ser det, men det er et tillegg for å øke styringen for Nødnett selv om du har satt bort mye av kjernenettkomponentene til en operatør. |
| 14 | E | For hvordan er det det funker når de kjernenettfunksjonene på en måte blir eksponert ved hjelp av NEFen. Er det sånn at den MVNOen da vil kunne administrere de kjernenettkomponentene direkte? |
| 15 | I | Nei, altså, jeg må si at det er litt tidlig. Jeg har ikke satt meg sånn veldig inn i den NEFen, og hva du faktisk kan utrette med den. Min forståelse er at du kan eksponere informasjon, eller at du kan styre ting. Men det er selvfølgelig en begrensning på hva du kan gjøre. Det jeg typisk har sett er at du kanskje kan monitorere dine egne kunder da, og se om de er koblet på eller ikke. Kanskje endre abonnementsinformasjon via denne network exposure functionen. For meg er det litt tidlig å vite alt du kan gjøre med den. Det er kanskje også litt opp til produsentene av mobilutstyr - Hva de tar i bruk av funksjoner. |
| 16 | E | En av de tingene som ble nevnt i forbindelse med et sånt MOCN-oppsett da vi snakket med en av de andre operatørene var at det ikke nødvendigvis var gitt at man ville tillate en MVNO å koble sin egen AMF rett på radionettet. Er det en problemstilling du kjenner til? |
| 17 | I | Det kommer nok sikkert bare an på avtaler. Du får en mye tettere integrasjon, fordi du har en direktekobling fra radionettet til egen AMF. Så det krever mye mer koordinering. Hvis du vil gjøre endringer eller legge til ny funksjon i radionettet, så må du ha støtte for disse funksjonene i begges kjernenett. Og du har også sikkerhetsaspektet ved det, når du får en direkte tilgang inn i radionettet. Men jeg tror det nok kommer an på avtalen mellom Nødnett og en eventuell operatør. Og så må du ha god nok sikkerhet på det i tillegg. |
| 18 | E | Så du tenker at det blir en sikkerhetsrisiko for den gjesteoperatøren, fordi de får en ekstern organisasjon tett inn i sitt radionett? |
| 19 | I | Ja, det er litt det. At du får noe som kommer tett inn på infrastrukturen. Kanskje mye tettere enn du gjør med et sånt MVNO-oppsett. Og du har disse avhengighetene - Typisk hvis Nødnett gjør noe som operatøren ikke er klar over, eller hvis operatøren gjør noe som Nødnett ikke er klar over. Det krever en tettere koordinering. Men sånn teknisk sett, så er det ikke noe problem egentlig. Jeg tror det er mer på avtaler mellom operatør og Nødnett som må regulere det litt. |

| | | |
|---|---|---|
| 20 | E | Og hvis vi da tar den ett hakk videre, hvis jeg har forstått den modellen som dere har foreslått, som er at man bruker en DSB-MVNO med eget kjernenett, og så at man bruker alle tre radionett. Vil det da være nødvendig å ha sånne typer samarbeidsavtaler med alle operatørene? |
| 21 | I | Jeg er litt usikker på hva som er vår offisielle løsning. Men, ihvertfall sånn jeg husker, så var det snakk om et sånt MVNO-oppsett hvor Nødnett ikke har sin egen AMF. Altså, standard MVNO er at du ikke har egen AMF - Da kaller du det heller MOCN istedenfor. |
| 22 | E | Det som ble nevnt var å ha en sånn felles operatørkode som gjør at alle radionettene kunne oppfattes som hjemmenett av brukerutstyret, og så rute det til DSBs kjernenett. |
| 23 | I | Ja, ok, sånn sett. Da blir det et slags MOCN-oppsett. |
| 24 | E | I et sånt scenario der man benytter seg av alle tre radionett. Tror du det vil være enklere om man ikke har egen AMF, slik at man ikke må ha disse avtalene med hver, og at man istedenfor kan bruke operatørene sine AMFer, og så få det rett inn i den øvre delen av kjernenettet som man har for seg selv? |
| 25 | I | Ja, det er betydelig lettere. Jeg mener at det er det som også er forslaget fra oss. At i det tilfellet så bruker alle operatørene sin egen AMF, men at de kringkaster denne felles nettverkskoden eller PLMN-koden. Et oppsett der Nødnett har sin egen AMF, det er på en måte det mest komplekse. Da krever det så mye mobilkompetanse hos Nødnett kanskje da. Mye mer enn det gjør med et typisk MVNO-oppsett. |
| 26 | E | Og hvis vi tenker litt på den andre modellen som har blitt foreslått av en av de andre operatørene, med at man bruker alle tre kjernenett. Har du noen umiddelbare tanker om hva som kan være utfordringene der, med tanke på for eksempel interoperabilitet og sånt? |
| 27 | I | Jeg er litt usikker på hva forslaget går ut på. Har du noen tegning å vise til? |
| 28 | E | Uh, nei jeg har ikke noen tegning å vise til, men jeg kan prøve å begi meg ut på en slags forklaring. Det er da liksom at man har kjernenettet til alle de tre operatørene, og så har man en sånn type mission critical-tjeneste på toppen som kan snakke med alle nettene. Sånn at man på en måte dytter DSBs rolle helt opp til toppen av stacken. |
| 29 | I | Men det innebærer da at du også må ha tre SIM-kort i telefonen da eller er det tenkt at du har SIM-kort fra kun én operatør? |
| 30 | E | Det er jeg litt usikker på akkurat hvordan det vil fungere, men det er kanskje tenkt at man for eksempel har ett hovednett for hver device. Sånn som typ prioritetsabonnement som finnes i telefonnettet i dag. |
| 31 | I | Ja, men da er det nok tenkt at du kanskje kan ha Telenor-SIM-kort, men at du fortsatt kan bruke alle de tre nettene. Men om du har Telenor-SIM-kort så vil du fortsatt gå til kundedatabasen i Telenor, så ... Nei, det er litt vanskelig å svare på akkurat hva som menes med det oppsettet. Skal du bruke tre separate kjernenett, så må du også ha tre SIM-kort. Ett fra hver operatør. Og det blir kanskje litt uhensiktsmessig for en bruker. |
| 32 | E | Det er tydelig at det fremdeles er mye rundt disse modellene som er veldig usikkert, og det er jo en del av utfordringen her. Både det at det er mye med 5G man fremdeles er usikker på hvordan kommer til å bli gjort i praksis, for selv om mye er standardisert så er det lite som er |

| | | |
|---|---|---|
| | | implementert. Og nå er det jo den KVUen som er unntatt offentlighet, men man er i en litt sånn "vent og se"-type fase føler jeg. |
| 33 | I | Men det er ihvertfall litt vanskelig å svare på noen av disse spørsmålene hvis du ikke har tegninger som viser det litt mer i detalj. Fordi det kan være nyanser her som gjør det litt forskjellig. |
| 34 | E | En annen ting jeg lurte på er litt sånn: Når det er snakk om at man skal ha et Nødnett-kjernenett, så må det skje en slags robustifisering av kjernenettet. I tillegg til at man robustifiserer radionettet ved å bygge ut batterikapasitet og ekstra dekning og sånt. Hvis man skal bruke et kommersielt kjernenett, så må det også skje en robustifisering der tenker jeg. Jeg lurer på hva du tenker at en sånn robustifisering av kjernenettet kan innebære? |
| 35 | I | Ja, i 5G så er det jo naturlig at du oppretter en egen slice for Nødnett. At du kanskje har et eget dedikert kjernenett som kun er for Nødnett sine brukere. Og så blir det litt spekulering, men da kan jo det for eksempel stå på sin egen fysiske infrastruktur. Om man vil, så kan man låse den infrastrukturen inn i egne datasentre eller egne bur, så du får typ både en fysisk sikring og en logisk sikring. Men du kan ihvertfall separere trafikken logisk fra all annen trafikk, det er naturlig. Ellers vil jeg si at du har ganske gode sikkerhetsmekanismer i mobilnettet, med tanke på at det er beskyttet utenfra, fra internett. Du kan kanskje til og med ha Nødnett-infrastruktur som ikke har noen kobling mot internett. Det er også en mulighet. En annen mulighet er at du kan ha servere som er plassert hos Nødnett, selv om en mobiloperatør drifter infrastrukturen. Så du plasserer infrastruktur som står fysisk hos Nødnett. Det er også en mulighet egentlig. Ja, og så er det kanskje på det med hvem som skal ha tilgang til utstyr. Det er kanskje regulert allerede, men det typiske er at disse operatørene, sånn type Nokia, de har folk som sitter over hele verden, som er fra Russland og kobler seg på og alt det. Det må selvfølgelig også kontrolleres, men det tror jeg kanskje man har kontroll på allerede. |
| 36 | E | Ja, man har vel ihvertfall kanskje sikkerhetsloven som går litt på sånne typer ting. Med tanke på det du sier om slicing. Jeg er litt uklar på hvordan det skal fungere i praksis. Er det for eksempel sånn at DSB da i samarbeid med en operatør utvikler en skreddersydd slice med egne Nødnett-type krav, eller hvordan er det det fungerer? |
| 37 | I | Ja, du kan etablere liksom et parallelt kjernenett da, som er kun for én gruppe brukere. Da ser jeg ihvertfall for meg at Nødnett kan komme med visse krav. For eksempel om hvor mye redundans man skal ha, altså typ holder det med to elementer eller må du ha tre eller fire? Hvor mye kapasitet skal du ha? Skal du ha dedikert og reservert kapasitet? Hvor skal det plasseres, det kan det kommer krav om. At det plasseres på visse lokasjoner i landet, kanskje i nærheten av Nødnett sine egne datasentre. Og så er det også muligheter i en sånn slice å komme med egne krav til funksjonalitet. At du kan ha egne funksjoner som du ikke har påslått i det vanlige kjernenettet. |
| 38 | E | Kan det være funksjoner som for eksempel MBMS? Broadcast typ for å ha gruppesamtaler. |
| 39 | I | Ja, det kan være alt mulig på en måte. Ting som du kanskje ikke ønsker å ha på i det vanlige nettet, men som du kan skreddersy litt for Nødnett. |
| 40 | E | Det jeg lurer på i forbindelse med slicing er hvordan en slice som for eksempel fokuserer på ultra-low latency og reliability er forskjellig fra en slice som fokuserer på høy båndbredde. |
| 41 | I | Ja, det er et interessant spørsmål, men mye av det er uklart. Det jeg vet er at om du har en sånn type ultra-realiable low latency slice, så har du funksjoner som gjør at du kan ha |

| | | |
|---|---|---|
| | | devicer som kobler seg opp til to basestasjoner samtidig. Sånn at hvis én går ned, så har du fortsatt en kobling. Og du kan også ha koblinger inn til to separate kjernenett. På en måte to slicer, hvor én er active og én er standby. Så da har du på en måte to separate veier, og ved det minste utfall så er det noe som tar over. Ihvertfall sånn jeg ser det så er det ikke sånn at slicet har helt andre egenskaper, men du kan ha mekanismer som gjør at du sikrer bedre oppetid. Og så er det også naturlig at for å skaffe low latency, så må du plassere kjernenettet så nærme kunden som mulig, kanskje helt ute i radionettet. At du terminerer trafikken og taletjenesten så nærme radionettet som mulig. Så det er kanskje den største forskjellen på selve slicet. At du plasserer for eksempel UPFen helt ute i radionettet, kontra eMBB hvor du har de på sentrale lokasjoner i landet. |
| 42 | E | En av de tingene vi ser litt på - Ja, det kommer litt i forlengelsen av å ha redundans i kjernenettet. Men det å ha på en måte flere kjernenett på flere fysiske lokasjoner. Sånn jeg har forstått det så er det typ tre eller fire sånne hele kjernenett som man har rundt omkring i Norge, slik at de to andre kan ta over hvis den ene faller ut. Stemmer det? |
| 43 | I | Ja, det er litt forskjellig fra operatør til operatør, men man har alltid redundans på kjernenettet. Gjerne georgafisk, slik at man for eksempel ikke blir rammet av samme strømbrudd eller andre lokale hendelser. |
| 44 | L | Og de synkroniseres kontinuerlig? |
| 45 | I | Nei, det er ikke noe - Eller, det kommer an på utstyret. Men du har type sånn som kundedatabaser som synkroniseres, men for en del av de andre elementene så velger du bare hvor du vil koble deg opp. Du kobler deg kanskje opp på den som er nærmest geografisk sett, eller så er det tilfeldig hvor du kobler deg opp. Men la oss si at den kjernelokasjonen faller ut, da må du koble deg opp på nytt et annet sted. Du tar ikke med deg oppkoblingen uten brudd. |
| 46 | E | Det jeg har skjønt som utfordringen med å ha kjernenett på mange lokasjoner er nettopp denne synkroniseringen av subscriber-databasen, og at det kanskje er en begrensning av den teknologien man bruker til det. At de leverandørene som leverer den teknologien - At det er en begrensning der. For en av de tingene vi kikker på er litt sånn regional edge, for å ha redundans i tilfelle regioner av Nødnettet blir isolert fra det sentrale kjernenettet. Hva tenker du om sånne typer regionale kjernenettløsninger? Mangler man implementert teknologi for å kunne gjennomføre regionale edger som kan operere autonomt, der man har en egen subscriber-database ute nærmere radionettet? |
| 47 | I | Jeg har egentlig ikke så mye erfaring med den kundedatabasen og den synkroniseringen. Hva som er kravene der. Men jeg vil tro at i teorien, så vil det fungere. Det er kanskje ikke så ofte du trenger å oppdatere disse dataene for en kunde, og i teorien så skal det jo fungere separat. Har du tre kjernenett og to av de faller ut, så skal det tredje fungere uavhengig av de andre. I teorien, riktignok, hvis det er satt opp riktig. Det er ihvertfall sånn vi bygger nett nå. Man har flere lokasjoner og man skal tåle at en hel lokasjon faller ut. Det samme vil gjelde hvis man får flere lokasjoner. |
| 48 | L | Vi ser nok på det i litt mindre skala når vi ser på regional edge. Tanken, ihvertfall i min oppgave, er at typ kritiske steder i kommuner og sånt har muligheten til å fungere autonomt når de mister tilkoblingen til resten av kjernen. Så da blir det vel kanskje en annen størrelsesorden og kompleksitet på det lokale/regionale kjernenettet? |
| 49 | I | Ja, det er mulig. Men det du snakker om er det på en måte at de skal sette opp et eget kjernenett i en kommune, enten permanent eller midlertidig? |

| | | |
|---|---|---|
| 50 | L | Tanken er på en måte det. At du har sovende kjernenettfunksjonalitet i edge som kan kicke inn dersom all redundans faller og du har den lokale øyen din som er isolert da. Som er en grad av redundans som ikke ville vært nødvendig for kommersielle aktører, men som kan være kritisk for Nødnett. |
| 51 | I | Det er en interessant tankegang. Jeg har tenkt litt på det, for jeg vet at blant annet Forsvaret har tenkt litt på å komme med egne basestasjoner og lage sitt eget mobilnett. Å bare ha en ryggsekk med et mobilnett liksom, som fungerer helt alene. Men det er klart: La oss si at man har datasentre spredt rundt i hele Norge, så er det jo lettere nå som alt er virtualisert - Før måtte man jo inn med svære servere og racks med utstyr, men nå kan man, hvis man har datasenter etablert på en del steder som noen operatører sikkert kommer til å ha, så kan man enkelt bare pushe ut et kjernenett da. Eller trykke på en knapp - En eller annen forbindelse må du kanskje ha for å aktivere det, men det er helt klart en del muligheter som åpner seg når ting er virtualisert og du har automatiserte prosesser for å pushe ut et nytt kjernenett i en region. |
| 52 | L | Det er kanskje å utnytte typ infrastruktur som blir bygget ut for å realisere ultra-low latency? |
| 53 | I | Ja, jeg tror absolutt det er en god tanke. Sånn at du kan øke redundansen midlertidig og få dekket det området som er isolert. |
| 54 | L | Utfordringen blir vel at det ikke er noe du kan gjøre etter hendelsen har skjedd. Det er liksom noe som må være der. |
| 55 | I | Ja, det er kanskje utfordringen. Hvordan skal du løse det hvis du mister all kontakt med omverden. Det er klart. Det vet jeg ikke hvordan man skal løse egentlig. |
| 56 | L | Ja, men det er interessant å sparre om det uansett. |
| 57 | I | Ihvertfall det jeg tenkte var som en idé at Nødnett kunne kommet med sitt eget sånt 5G-nett i en trailer eller ryggsekk. Kanskje med satellittkommunikasjon til sentrale elementer, eller som et helt standalone nett. |
| 58 | L | Ja, det finnes jo i dag, så det bør finnes for 5G-løsninger. |
| 59 | E | Sånne lavbanesatellitter er veldig interessant ny funksjonalitet. |
| 60 | I | Ja, absolutt. Nå har du jo det nettverket til SpaceX, hva heter det for noe, Starlink eller noe, som sikkert åpner en del nye muligheter. Du får mye lavere forsinkelser enn du har hatt tidligere med geostasjonære satellitter. Jeg vet at man på 5G også har begynt å snakke en del om å bruke satellitt som backhaul, altså forbindelsen fra basestasjonene til kjernenettet. Så det er noe som kanskje kan være aktuelt i et sånt Nødnett-samarbeid, at du har satellitt som backup kanskje. Det er ikke helt mitt område. |
| 61 | L | Det brukes i dag med de transportable basestasjonene, at du flytter inn en med satellittkommunikasjon midlertidig, men jeg tror det er en enormt stor kostnad å ha det permanent installert som backup. |
| 62 | I | Ja, da er det sikkert en mer sånn midlertidig løsning. |
| 63 | L | Men det er jo en bunnsolid backup, og ganske nyttig i områder der du ikke kan bygge ut infrastruktur så lett. |

| | | |
|---|---|---|
| 64 | I | Jeg vet jo at alle operatørene har mobile basestasjoner som de triller ut på festivaler og sånne ting. Så det blir kanskje en variant av det, men at du kanskje kan slenge på et kjernenett i tillegg, i samme trailer eller tilhenger. |
| 65 | L | Ja, litt sånn du nevnte at Forsvaret holder på? |
| 66 | I | Ja. Men det er kun noe jeg har hørt om for mange år siden, jeg vet ikke om Forsvaret har tatt det i bruk eller ikke. |
| 67 | E | Du nevnte tidligere at du har sett litt på Finland, eller at du har litt erfaring med hvordan de har gjort ting i Finland? |
| 68 | I | Ja, altså, det jeg har mest er faring med er etableringen av et delt radionett i Finland. Og så har jeg lest om den løsningen de har med Nødnett i forkant av dette møtet. |
| 69 | E | Ja, fordi i Finland så har de jo valgt Elisa som tilbyder av radionettet. En av de tingene som ofte blir trukket frem som en sånn åpenbar downside med å velge én tilbyder av radionett er at det radionettet må investeres i og robustifiseres, og at det kan være konkurransevridende i mobilmarkedet. |
| 70 | I | Ja, det er jo helt klart et problem. Det går kanskje mer på det kommersielle, men jeg tror, tilsvarende for Norge da, så ville myndighetene helt klart valgt Telia eller Telenor. De ville antageligvis ikke vurdert Ice, fordi Ice har dårligere dekning enn de to første. Og det igjen ville vært konkurransedrivende og gjort det vanskelig for Ice. Så jeg tror nok at sånn kommersielt, så er det en del ulemper med et sånt forslag. I tillegg har du ikke muligheten til å koble deg på to radionett, og får da ikke den redundansen. |
| 71 | E | Og litt det med den redundansen. Sånn jeg har forstått det så er det mye overlappende dekning. At de områdene som er uten dekning kanskje er uten dekning for alle, fordi det er såpass langt unna at - For når man bygger kommersielle nett så fokuserer man jo gjerne på befolkningsdekning istedenfor geografisk dekning. Men en ting jeg lurer litt på, jeg vet ikke om du kan noe om det men, er hvor avhengig de ulike radionettene er av hverandre sånn infrastrukturmessig. Sånn jeg har forstått det så er det ofte at man har flere basestasjoner og sånt på samme mast. |
| 72 | I | Ja, det er som sagt utenfor det jeg jobber med, men jeg vet at en stor del av kosten ved en basestasjon er tårnet og bygningen og kanskje fiber inn og sånne ting. Så det er veldig mye bruk av samlokalisering. Telenor og Telia er for eksempel pålagt å tilby plass til Ice i sine tårn. Så skal Ice etablere ny basestasjon så er det mer naturlig at de forsøker å finne innpass i eksisterende mobiltårn, enn at de skal bygge sitt eget tårn hundre meter unna. Så det er nok mye samlokalisering, selv om det ikke er det jeg jobber med. |
| 73 | E | Men kan det tenkes da at det å argumentere for redundans og robusthet i nettet ved bruk av flere radionett kan gi en falsk trygghet? Fordi hvis fiber inn til en samlokalisert basestasjon ryker, så ryker dekningen i alle tre nett? |
| 74 | I | Ja, det er klart at det kan være tilfeller hvor - Altså, jeg vet at både Telia og Ice leier en del samband av Telenor for eksempel da, så du kan kanskje ha tilfeller hvor alle tre operatører bruker Telenor-fiber. Men jeg tror det er kanskje noe som du må regulere i en avtale. At du ikke har samme fysiske fiber inn og ut av en basestasjon. Og så kan du også ha områder hvor du har overlappende dekning fra to basestasjoner. Da vil du omgå det problemet. |

| | | |
|---|---|---|
| 75 | E | Innledningsvis nevnte du at du hadde noen tegninger eller noe sånt? Jeg er litt nysgjerrig på det. |
| 76 | I | Ja, jeg ta å gå kjapt gjennom det hvis vi har tid. [Deler skjerm] Det var egentlig bare for å ha noe å snakke rundt, jeg visste ikke hva dere hadde av spørsmål. Ja, bare litt sånn avklarende på 5G da, så har vi non-standalone og standalone, men jeg antar at dere hovedsakelig snakker om standalone hvor du har et 5G-core. Bare for å avklare det. Og så satt jeg opp litt bare for å tenke selv. Vi har jo kommet med et svar til Nødnett for et år eller to siden, som jeg antar er det min kollega presenterte for dere, men nå bare lister jeg litt ut ifra egen tenking - Forskjellige muligheter for samarbeid. Jeg har en slide for hver, så jeg kan bare gå gjennom dem. Den første er det som er MOCN, hvor Nødnett har sin egen AMF. Det krever mer kompetanse hos Nødnett på mobilnett, og, som sagt, vesentlig mer koordinering med operatøren. Du kan ikke enkelt kombinere dette med en operatør Y da, hvis du vil ha det for eksempel. Det er nok mulig, men da må du kanskje ha en type ny AMF hos Nødnett. Ihvertfall litt separat så du ikke blander operatør X og Y. Men det er en interessant løsning som sikrer Nødnett full kontroll over tjenesten. |
| 77 | E | For det blir kluss hvis man skal ha samme AMF på ulike nett? |
| 78 | I | Ja, du vil ihvertfall få en sikkerhets - Altså, du vil få en kobling mellom operatørene som jeg vet at operatørene ikke er så veldig glad for. Så du bør ha det en del adskilt, hvis du skal ha to operatører. |
| 79 | E | Så det er lettere å gjøre den sammenkoblingen av trafikk hakket over AMFen da? |
| 80 | I | Ja, hvis du har AMF i eget nett, som er MVNO-oppsettet, som er neste slide her, og som er et typisk roaming-oppsett. Du kan for eksempel roame over hele verden, og reiser du til Spania så kan du velge selv hvilken operatør du vil koble deg opp på. Så dette er et typisk roaming-oppsett hvor Nødnett kan ha avtaler med alle tre operatører i Norge, og så velger man selv ut ifra dekning hvilken man kobler seg opp på. |
| 81 | E | Og da velger man bare den med best dekning? |
| 82 | I | Ja, det er en sånn prioriteringsmekanisme. Normalt velger du den med sterkest signal. Ja, så det er vel dette som min kollega har presentert for dere, er det ikke det? |
| 83 | E | Eh, jo, men jeg tror kanskje vi var litt uklare på akkurat det med hvordan AMFen skulle være. Jeg vet ikke om vi kom inn på det. Ja, det var egne SIM-kort for Nødnett, det stemmer. |
| 84 | I | Ja, så dette er et klassisk MVNO-oppsett da. Du har noen operatører i Norge som også har dette oppsettet, typ Com4 er det en som heter, som har et sånt oppsett hvor de ikke har eget radionett. |
| 85 | L | Det var en ryddig fremstilling. |
| 86 | I | Ja, takk. Det er litt sånn på høynivå, veldig generelt da. Og så har du alternativet, som vi også snakket om, med en egen slice hos en operatør, med litt sånn skreddersydd løsning. Da kan du få dedikerte ressurser, og du kan velge plassering av noder. Typisk nærme Nødnett, så du får lav forsinkelse. Og så nevnte jeg også dette med network exposure, som du spurte om. Akkurat hva du skal få tilgang til det er et ubeskrevet kapittel, slik jeg ser det. |
| 87 | E | Det gjenstår å se litt? |

| | | |
|---|---|---|
| 88 | I | Ja. Hva er det behov for å ha tilgang til og hva kan du ha tilgang til. Ja, i et sånt oppsett kan du også ha tilgang til - Du kan ha tilgang til taletjenester i Nødnett, men skal du bare ut på internett for å surfe på Netflix for eksempel, så kan du gå ut fra operatørens IT-nett forbindelse. Det er bare en detalj egentlig. Og så er det et alternativ å bare være som en vanlig kunde, og bare bruke den infrastrukturen som eksisterer. Det tror jeg nok også er et antageligvis er et bra nok alternativ da. |
| 89 | E | Ja, dette var litt det vi var inne på når vi snakket om å bruke hele stacken til alle tre operatører. Sånn jeg på en måte forstod det litt på han andre vi intervjuet, var at det var litt som å være en vanlig kunde hos alle de tre operatørene. |
| 90 | I | Ja, du kan absolutt være det. Men da er det igjen: Skal du ha det helt separat, så må du ha tre forskjellige SIM-kort som du sjonglerer mellom. Har du kun SIM-kort fra la oss si Telenor, så vil du fortsatt gå mot kundedatabasen hos Telenor selv om du roamer hos Ice. Så du vil fortsatt ha et sånt svakt fellesledd, hvis du har kun Telenor-SIM-kort. Så det må man spesifisere da. |
| 91 | E | Men sånn som de prioritetsabonnementene som eksisterer i dag, der man har ett hovednett, og at man kan benytte seg av de andre nettene hvis det hovednettet faller ut. |
| 92 | I | Ja, det er tilsvarende. Så der kan du ha prioritets-SIM fra Telenor, men da er du likevel sårbar for at sentrale nettelementer hos Telenor faller ut. For du vil uansett gå mot Telenor sin kundedatabase eller taletjenester. |
| 93 | E | Så da må du eventuelt også ha et annet SIM-kort som du kan bruke hos for eksempel Telia istedenfor, når Telenor sitt nett ikke fungerer lenger? |
| 94 | I | Ja, og så har du - Og det tror jeg alle operatørene gjør. At de som for eksempel er kritiske funksjoner hos Ice har både et Ice-SIM-kort og et Telenor-SIM-kort i telefonen. Eller to forskjellige telefoner da. Så skal du ha full redundans, så må du ha ihvertfall to SIM-kort. Disse prio-SIMene ville for eksempel ikke fungert hvis hele Telenor-nettet faller ut da, så du har egentlig bare redundansen på radionettet. |
| 95 | E | Er dette noe som blir enklere å løse når man introduserer for eksempel eSIM og sånt? |
| 96 | I | Ja, da skal det være lettere å bytte operatør. Men jeg tror likevel du må ha - Nå vet jeg ikke akkurat hvordan operatørbytte på eSIM fungerer, men du må likevel ha tilgang til en sentral server hvor det byttet kan gjøres. Så hvis den står hos Telenor, som kanskje er hovedoperatøren din, så vil du kanskje ha et svakt ledd der. Men det er i teorien enklere. Men som sagt har jeg ikke noe særlig erfaring med eSIM og hvordan det operatørbyttet gjøres i praksis, men det åpner muligheter som sagt. Du slipper å ha det fysiske byttet av SIM-kort. Kanskje du til og med kan ha type elektroniske SIM-kort hvor du kanskje har alle tre SIM-kortene i en sånn slags eSIM-løsning, og kan automatisk bytte - Jeg vet ikke hva som er teknisk mulig. Men det er litt spekulasjon, altså. Og så tenkte jeg også muligheten som en sånn, det er kanskje ikke helt realistisk, men det er også mulig at Nødnett har lisens på sine egne 5G-frekvenser og bygger sitt eget 5G-radionett, men bruker kjernenett fra operatøren. De kan selvfølgelig også ha sitt eget 5G-kjernenett, men da er det jo på en måte helt fristilt fra kommersielle operatører. Det blir den nederste figuren her, hvor de bygger et parallelt Nødnett-radionett, men er koblet mot en slice hos operatøren. Og så har de kanskje naturlig nok tjenestene hos seg, fortsatt. Og så, det som jeg har tatt som siste slide her, det var litt det dere var inne på med autonome nett. At du setter opp kanskje et sånt standalone 5G-nett i en nødsituasjon med satellittkommunikasjon, eller som fungerer helt isolert. Men det blir isåfall et sånt supplement til et av de andre alternativene. Og så hadde jeg, ja, så tok jeg |

| | | |
|---|---|---|
| | | bare litt om prioriteringsmekanismer. |
| 97 | E | Ja, dette er jo absolutt interessant. |
| 98 | I | Ja, det er ihvertfall de vi har sett på som også brukes for sånne prioritets-SIM, hvor du har noe som heter preemption. Hvis en celle er overbelastet sånn at ingen nye brukere kommer til, så kan du ha en sånn preemption hvor du kan kaste ut pågående brukersesjoner for å få tilgang til radionettet. |
| 99 | E | Er dette noe man for eksempel kan få innbakt i en slice? |
| 100 | I | Du trenger ikke nødvendigvis en slice for å få det til. Det er bare en parameter som du har per bruker, på hvilken prioritet du skal ha. Du er ikke avhengig av å ha en egen slice. Du kan bruke samme slice som andre brukere, men fortsatt ha disse prioritetsmekanismene for å få førsterett i - Ja, det er først og fremst radionettet det er snakk om, fordi det er der man har en begrenset ressurs. Og så har du andre sånne quality of service-mekanismer som gjør at du kan sikre deg en båndbredde. Altså, preemption er for å sikre deg tilgang til radionettet, og så har du det som heter 5QI, som er en sånn quality of service characteristic. Da kan du ha en garantert båndbredde for samtalen, og sikre god kvalitet. Har du en dataoverføring, så kan du ha prioritet overfor andre datastrømmer, foran de som er vanlige kunder i mobilnettet. Så kommer det litt an på oppsettet, men har du et sånt MVNO-oppsett så må du koordinere disse verdiene med de kommersielle operatørene som du har avtaler med. |
| 101 | L | Det var en veldig ryddig fremstilling, takk for det. |
| 102 | I | Ja, men det var en grei øvelse. |
| 103 | E | Jeg ser vi nærmer oss tiden. Jeg vet ikke om du har et nytt møte å løpe til, men jeg tenkte bare litt sånn - Nå har du jo åpenbart satt deg litt inn i det vi lurer på, så jeg lurer på om det er noen ting vi ikke har nevnt som du kanskje tenker at vi burde ha sett på? |
| 104 | I | Nei, ikke noe jeg kommer på sånn umiddelbart egentlig. Jeg er kanskje ikke helt sikker på hva dere er ute etter annet enn det som stod i arket dere sendte. |
| 105 | E | Nei, det er kanskje litt av det vi prøver å finne ut av selv også. Hva er det egentlig vi er ute etter? Hehe. Så det som skjer nå er at vi tar lydopptaket og transkriberer det, og så sender vi det til deg, og blir enige om hva som skal stå der. Om det er noe du ønsker å presisere eller trekke tilbake, hvis du har sagt noe som burde være hemmelig, og å se litt på den anonymiseringen som vi gjør. Det varierer litt hvor mye intervjuobjektene har for å være anonyme, men vi gir alle samme behandling. |
| 106 | I | Ja, men det høres greit ut det. Jeg tenker at hvis dere har andre spørsmål så er det bare å sende mail eller sette opp et nytt møte. |
| 107 | E | Det setter vi pris på! |
| 108 | L | Tusen takk for at du ville være med! |
| 109 | I | Ja, bare hyggelig å kunne hjelpe. Så får dere ha lykke til med oppgaven. Ha det godt! |
| 110 | E, L | Tusen takk, ha det godt! |

Appendix M

# Directorate for Civil Protection B

This interview is conducted with a representative of the Norwegian directorate for civil protection (DSB) who possesses significant knowledge regarding the NGN process and the challenges faced by the state in terms of collaborating with commercial operators. A number of relevant topics are covered in this interview, pertaining to specific concerns regarding various aspects of different alternative deployment models, as well as more general considerations made in regard to the development of 5G and related technologies at large.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Da har jeg satt opp lydopptaket, og så spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Det er greit at du gjør lydopptak av dette møtet den neste timen. |
| 3 | E | Supert, takk skal du ha. Så, min oppgave går mer på kjernenettet og hvordan vi eventuelt skal samarbeide med kommersielle aktører om å realisere NGN i kjernenettet i 5G. Med tanke på at man skal samarbeide med kommersielle aktører om radionett, så er spørsmålet på hvordan man skal gjøre det i kjernenettet og litt vurderinger på det. |
| 4 | L | Jeg er mer ute i radionettet og ser på hvordan man kan realisere en eller en gruppe av BS som fungerer autonomt uten tilkobling til kjernenettet. Caset mitt er at vi kjører hele radionettet på Telenor sitt nett, og at DSB er en MVNO i kjernenettet, kort oppsummert. |
| 5 | E | Vi er ikke helt sikre på hva dine spesialiteter er? |
| 6 | I | [Introduksjon]. Og så vet dere at denne KVUen som vi har laget, den er skrevet for at vi skal kunne gå inn i de kommersielle mobilnettene. Alt dette vet dere, ikke sant? Jeg vet ikke helt hva jeg skal si og hva jeg skal fortelle, ellers blir det bare repeat for dere. Dere har jo 5G som bakteppe her, og vi har laget dette slik at når vi går over i 3GPP type teknologi, så er vi på en måte på det utviklingssporet. Så om vi kommer oss inn og starter med 4G, vi får se hvordan timingen blir da, ikke sant. Hvor langt 5G har kommet, om 5G SA eksisterer og hvordan vi skal gripe det fatt, men på et nivå går vi inn. Da er vi i denne utviklingen, slik at etter hvert som utviklingen skjer, det kommer nye muligheter, så vil vi være en del av det toget. TETRA-teknologien er jo en moden teknologi, og litt frossen. Det skjer ikke egentlig noen nyutvikling der, det er lite nyutvikling der. Det er lite ny funksjonalitet som brukerne merker. Når vi oppgraderer TETRA-nettet nå, og det skal vi også, så er det mer sånne ting som man merker på drift og størrelsen på sentralen går ned. Den har gått ned fra fotballbane til basketballbane og snart er det bare et rack. Det var litt overdrevet, men det er sånne typen ting, besparelser der. Legger over til IP på måten nettet er bygget opp på, men brukerne merker ikke så mye fordi TETRA er TETRA. Radiogrensesnittet er det radiogrensesnittet, og det skjer ikke så veldig mye med TETRA-terminalene. Så det er fastfrosset teknologi. |
| 7 | I | Når det gjelder 4G og 5G så vil vi være med på den utviklingen og dra nytte av det som er relevant for våre brukere, nød- og beredskapsbrukerne, som den teknologien gir. Og det er så utrolig mye, det er veldig bredt og vidt hva som er standardisert og hva som er laget og hva som leveres. Nå er det ikke slik at alt som standardiseres nødvendigvis blir implementert og solgt og gjort tilgjengelig, eller tilgjengelig i Norge, men det er veldig rikt tilgang. 4G gir jo bredbåndskommunikasjonen til brukerne våre og gjør det mulig å rett og slett benytte mobilradionettene for disse gruppetjenestene med rask trykk og snakk som er helt essensiell for våre brukere. MCPTT, altså trykk og snakk-tjenestene er helt sentrale, og TETRA-nettet er jo nærmest bygget opp for at det skal kunne fungere med en del tilleggstjenester rundt. Det er liksom kjernen, det i gruppestrukturer. Nå blir det mulig. Med 2G og 3G så var ikke det mulig på en god måte. Man har jo hatt noen sånne OTT og sånne trykk og snakk-løsninger som har fungert til og med GPRS, men det har ikke vært med en oppkoblingstid og kapasitet og tjeneste som vi kan stole på for våre brukere, som må ha det til å fungere når det står om livet. Fra 4G så er dette her mulig og i 3GPP er det standardisert. Dere vet sikkert også med de tjenestene som er tatt frem i 3GPP-arbeidet siden omtrent ... Det er vel 6 år siden det begynte tror jeg, jeg tror det var i 2015 at en komite ble laget for spesielt å se på disse tjenestene. Og nå blir det mulig, fra 4G. Nå blir det mulig, og da er vi på, og da er vi en del av utviklingen inn i 5G. Og flere og flere begynner å snakke om 6G, og det blir sikkert noe for oss også en gang i tiden. Det kommer gjerne en G hvert tiende år. Det er min erfaring, jeg |

| | | |
|---|---|---|
| | | har jobbet siden 1G så jeg kan bekrefte det. |
| 8 | I | Når vi nå kommer på det her så kommer 5G-mulighetene til oss. Og så får vi se på timingen vår, hvordan vi bygger denne løsningen. Det kan jo hende at 5G har kommet ganske langt i Norge når vi skal lansere. Dere vet jo at Nødnett-kontrakten vår med Motorola, den løper til slutten av 2026 og kan eventuelt utvides, selv om det er litt i ukjent farvann. Det er ikke sikkert at det er noe vi har lyst til å gjøre så veldig lenge. Men når vi kommer til 2026/2027 så tror jeg nok mobilnettene er litt annerledes i Telenor/Telia/Ice enn de er i dag. De har sikkert fått på noe 5G SA, men det kan også hende at noe henger igjen i mer legacy på 4G-kjernenett, at de har begge deler, men når de da har SA 5G så åpner den muligheten seg for oss. |
| 9 | I | Men samtidig må vi ta hensyn til andre land, våre brukere skal ha interaksjon mot Sverige, Finland og forhåpentligvis en del andre land. Vi har noe mot Sverige og Finland i dag med TETRA-nettet, men det har kostet en god del innsats og nybrottsarbeid å få det til. Vi hadde jo håpet at flere land skulle etablere det, men det har egentlig ikke skjedd i praksis. Så vi har dratt det lasset, og da stopper det mot de to viktigste landene for oss. Og vi tre landene er på en måte en sånn landeklynge. Sverige henger såvidt sammen med Danmark nede i syd, men det er fremdeles litt sjø mellom der og det har ikke vært viktig nok til at de har gått løs på det. Østover er det land som jobber på andre måter, og vestover er det bare hav. Så der har vi tre landene løst det. Men når vi går over i 3GPP type løsninger, så håper vi og regner med at det åpner seg opp for samhandling med andre land nedover i Europa. Og da er det også noe vi må ta hensyn til når vi bygger opp nettet vårt. Hvis vi sier at vi bare skal ha 5G SA og rene 5G-terminaler, så er det mulig vi står der da, hvis ikke de andre landene også gjør det samme. Så det må vi også se på. |
| 10 | I | Og så må vi da se hvilke fordeler det gir oss å gjøre å gå over til 5G SA. Hvis vi skal bygge, og det vet vi ikke enda, om vi skal bygge et eget kjernenett eller ikke. Den avgjørelsen er ikke tatt. Vi har flere konsepter, jeg vet ikke om [veilederne deres] har røpet noe på høynivå for dere i det hele tatt? Vi har i hvert fall flere konsepter som åpner opp både for å ha noe eget og ikke ha noe eget. Skal det være noe kjernenett, eller hvor mye kjernenett og tjenestenoder hos kommersielle aktører det skal være, eller om vi skal bygge eget MVNO-nett hvor vi har et helt kjernenett og tjenesteproduksjonen selv. Det er ikke avgjort. Vi har skissert alt det her i KVUen med plusser og minuser og regnet på det og kommet frem til noen anbefalinger, men kan jeg ikke si, da. Så der er det flere muligheter, og etter hvert som tiden går nå så er teknologien med oss. Og så tenker dere primært 5G i det arbeidet dere jobber med? |
| 11 | E | Ja. |
| 12 | I | Jeg kan mer om 4G enn om 5G, men vi ser litt inn mot 5G også. Det vi vet, er at det arbeides i 3GPP for at disse MCX-tjenestene, MCPTT, MCVideo og MCData også skal støttes i 5G og SA, men det arbeidet er ikke ferdig i standardiseringen enda. Det er tilpasninger som gjøres, og det er løsninger vi trygge på at kommer til å bli støttet også fra leverandørsiden. Noe annet ville vært veldig rart. |
| 13 | L | Vi har vært og dykket inn i de standardene til 3GPP, de spyttes jo ut om dagen. |
| 14 | I | Ja, det gjøres jo stadig vekk. Det er veldig stort arbeid. 3GPP er kanskje verdens største, mest vellykkede dugnad. Det er jo en stor dugnad, ikke sant, egentlig er det frivillig arbeid. Men det er en nødvendighet for bransjen, både leverandørene og operatørene. Operatørene på alle felter, både for terminaler og nett og tjenesteløsninger og sånt. Så det er et stort arbeid som går. Som et indisium her, så tok jo 3GPP for to eller tre år siden og rensket ut mission |

| | | |
|---|---|---|
| | | critical for LTE. Det sto en sånn formulering på forsiden av alle disse tekniske spesifikasjonene for MC-tjenester. Der tok de og ryddet, slik at det ikke skulle være bundet til 4G, men for å forberede dokumentene også for at de skal kunne gjelde 5G. Tjenestene skal tas videre der, og det betyr sånne ting som at kravspesifikasjonene som kalles Stage 1-beskrivelser i 3GPP-verden, de blir gjort om slik at de også skal være gyldige i et 5G-nett. |
| 15 | I | Og så har dere kanskje sett nå, for de siste dagene så har jo FirstNet lansert MCPTT for et år siden der og tatt ombord brukere på det, og også har over 2 millioner brukere hvor de aller fleste bruker datakommunikasjon med prioritet. For FirstNet-løsningen som AT&T bruker for FirstNet, så har de jo nå satt i gang 5G faktisk med FirstNet-brukere på 5G. Hvor mange av de som har 5G-terminaler ... Det må nok være noen som har det, for de bruker en del vanlige terminaler der også, ikke bare ruggedized. Ruggedized-terminaler henger gjerne litt lett etter i utviklingen med å få nyeste teknologi. En del brukere der bruker jo normale terminaler som har 5G, og de har nå 5G inn mot FirstNet-løsningen. Jeg er ikke sikker på om de har satt på prioritet enda på lufta, men det kan i prinsippet gjøres. Da er det NSA, at de har 5G inn mot 4G-kjernenettet. Det betyr at 5G nå kommer som aksess, og det byr på fordeler med mulig høyere datarater og er interessant. Så det toget har startet allerede faktisk, at det finnes MC bruk av 5G, men NSA. Det er i gang! Amerikanske operatører er jo bebudet til å være tidlig ute med å bygge ut SA-løsninger. Jeg tror T-Mobile i USA, det er jo ikke de som jobber med FirstNet da, men de har kommet ganske langt. Konkurransen er sterk mellom de amerikanske operatørene, så der skjer det nok ting. De ligger litt foran Norge, de er store og toneangivende. Det er bra de går foran. |
| 16 | E | Mhm. |
| 17 | I | Veldig glad for at land går foran. Også ESN i Storbritannia, som dere sikkert også har fått med dere, som sliter litt med å komme ordentlig opp og kjøre, men de har gjort veldig mye bra arbeid. Og så er det Live Net i Korea også. Jeg snakker kanskje bare rundt grøten for dere. Bare å spørre. |
| 18 | E | Nei, jeg synes det er veldig interessant å høre. En av de tingene som jeg lurer litt på i forbindelse med at et av alternativene er at Nødnett skal være sin egen MVNO i NGN, er litt om hvilke driftsoppgaver har i dag. Du nevner det med at dere driver og oppgraderer kjernenettet og sånt, men sånn jeg har forstått det så driftes det av Motorola. |
| 19 | I | Ja. Du lurer på når vi skal gå inn og være en MVNO hvordan det blir? |
| 20 | E | Ja, hva slags driftserfaring har dere i DSB, og hvilke kapasiteter har man til å være sin egen MVNO? Det er litt det du nevner som dere har sagt i KVUen om disse plussene og minusene for de ulike alternativene er på en måte det jeg er nysgjerrig på. |
| 21 | I | Ja, det er klart at dette har blitt vektet. Det å skulle ta igjen driften over og stå og drifte selv. Hvis vi skal ha mye infrastruktur selv, så har vi hvert fall ansvar for driften, men så er det flere løsninger. Det går an å sette den ut med avtaler, så vi må ikke nødvendigvis ha statsansatte som gjør det. Så det blir jo da en vurdering med hensyn til kvalitet og kostnad. Det kan også hende at etter 2026, hvis vi skal forlenge TETRA-nettet at vi tar inn driften nærmere staten. Nå er det jo Motorola som gjør det for oss. Vi kan ta over den, det er den norske staten som eier TETRA-nettet. Så når den avtalen ikke er lenger etter 2026, den kan vel for så vidt sies opp nå også, så det er i prinsippet mulig å ta inn driften nå om et år hvis folk ville, så er det mulig. Da er det vurderinger, og da må staten vippe opp et driftsmiljø, hvis vi skal ha egne folk til å gjøre det. Greier vi da å få inn riktig kompetanse, blir det et bredt nok miljø, osv... Det er ikke sikkert at det er den beste løsningen, men det er noe som vurderes og det er også vurdert i KVUen. |

| | | |
|---|---|---|
| 22 | E | Det du nevner med at man kan ha sitt eget kjernenett og sette ut driften, er det til et selskap som Motorola f.eks. i NGN? |
| 23 | I | Ja, det kan være en mobiloperatør eller en annen type selskap avhengig av hvilket konsept som blir valgt. Du har de ulike konseptene i KVUen. Men det er klart at vi ser på å ha noe egen infrastruktur uansett hvem det er som drifter og eier det. Det må være en sterk grad av statlig kontroll uansett også. Vi må ivareta sikkerheten, det er viktig. Og at det er en løsning som er god og stabil. Og så har vi noen sikkerhetskrav på nasjonal autonomi, slik at det skal kunne driftes inne i Norge uten at utlandet må være involvert i en vanlig driftssituasjon. Man kommer aldri utenom utenlandske eksperter når det gjelder å levere ting og kanskje være med på design, men selve driften og sånt skal kunne gjøres uavhengig av utlandet. |
| 24 | E | Og de kravene til autonomi og statlig kontroll er noe man opplever at man har i Nødnett i dag og gjerne vil overføre videre til neste generasjon? |
| 25 | I | Ja, nettopp. Det følger av sikkerhetsloven også, du er nødt til å gjøre det. |
| 26 | E | En ting jeg er litt interessert i med tanke på den MVNO-løsningen, er om man skal ha et MOCN-oppsett eller et MVNO-oppsett og ulike tekniske utfordringer rundt det. Sånn jeg har forstått det f.eks. for politiet så kan det være interessant for brukerne å skjule mobilitetsinformasjon som vil være tilgjengelig i AMFen i et gjesteoperatørnett hvis man benytter seg av et typisk MVNO-oppsett der man ikke har sin egen AMF i 5G. Så jeg lurer på om du har noen tanker om de tekniske utfordringene med å ha et MOCN-oppsett versus et MVNO-oppsett for å skulle drifte den fulle stacken med kjernenett. |
| 27 | I | Ja, da får vi ansvar for flere noder og en større del av nettet, så det krever enda mer på driften. Du kan jo si at hvis vi har et MOCN-oppsett, dette gjelder både 4G og 5G, der er det litt parallelle problemstillinger tror jeg. Jeg vet ikke om noen har laget et MOCN-nett i verden i 5G enda, det er kanskje litt tidlig. Men altså, det er teknisk og operasjonelt mer krevende med MOCN enn med mer tradisjonell roaming som man gjerne kaller S8. S8 er det man bruker mot utlandet og som er mer gjengs, det vi er mer vant til. Hvis man skal ha MOCN så integrerer man seg tettere mot radionettet for man må dele informasjon om radionettet tett med den operatøren som man velger å samarbeide med. Det blir ganske tett samarbeid, kanskje litt vanskelig å bytte radionettoperatøren også fordi samarbeidet blir tett, og det vil være en større jobb å integrere seg mot et annet radionett. En littegrann større grad av lock-in, kanskje. Men samtidig finnes det en god del MOCN-løsninger rundt omkring i verden, og det er flere innen nød og beredskap som har gjort det. De har MOCN både i USA og England, så de som går foran oss der har hatt den typen løsninger. De har vel faktisk nå satt i drift den første datakommunikasjonen, den har vel allerede foregått i Finland for en måneds tid siden. De har etablert det på ganske kort tid, dette MOCN-nettet. De har vært flinke, men de har nok lent seg ganske tett på leverandører og operatører. Så Ericsson og Elisa har nok gjort en god del av jobben tenker jeg, der borte i Finland. Men ja, MOCN-løsning er nok en fordel sånn med hensyn til mulighet for større grad av statlig kontroll. Det kan nok også være at det kan være enklere å bygge opp sikre løsninger, for det er færre parter involvert, uten at jeg tror det er så avgjørende. Jeg vet ikke om jeg svart på spørsmålet ditt, jeg? |
| 28 | E | Joda, interessant det. Det eneste er det sikkerhetsaspektet med tanke på hva slags informasjon den gjesteoperatøren får tilgang på, f.eks. mobilitetsinformasjon i AMF. I MOCN-oppsettet vil man ha en egen AMF. |
| 29 | I | Ja, ikke sant. Det blir som i MMEen i 4G. Da ligger det jo noe informasjon der. Det er noe |

| | | |
|---|---|---|
| | | som må sees på. Da må det i så fall dekkes opp gjennom avtaleverk og rutiner og personell som får tilgang og slikt. Det må settes krav om det. |
| 30 | E | I forbindelse med det, det er kanskje litt vanskelig å finne ut av hvordan man stoler på disse mobiloperatørene i denne sammenhengen? For alle er jo underlagt sikkerhetsloven, og det er strenge regler for hvem som skal ha tilgang og sånt. Tenker man likevel at det er fordelaktig at staten har den fulle kontrollen og oversikten, at det er et statlig organ som sitter med nøklene her, i stedet for at man leier det ut til mobiloperatører? Med tanke på integritet og sikkerhet i nettet? |
| 31 | I | Vi tror ikke det er avgjørende sikkerhetsmessig at staten sitter og eier komponentene selv og har alt sammen innad. Vi mener at mye av dette kan løses med avtaler med de partnerne som vi velger å knytte oss til. Vi ser også at sikkerhet har blitt tatt ordentlig på alvor i mange år i mobilverdenen, og operatørene har bygget opp veldig kompetente miljøer for å sørge for nettopp sikkerheten. Der er jo et komplekst område, et ganske nytt område, og det er et område som krever mye ekspertise som det ikke er så lett å få tak i. Det er ikke staten er de flinkeste til å knytte til seg akkurat eksperter og få til dette her, selv om vi sikkert klarer å få til noe. Det er ikke sikkert at vi blir like gode som de kommersielle operatørene. Når du tenker på det, er det ingen garantier for at det at staten bygger opp bare fordi staten har egne bokser i nettløsningen her gir den beste sikkerheten. Det er ikke sikkert de er de beste til å ivareta den. Der tenker vi kanskje at Finland og Sverige kanskje har trukket litt for raskt til konklusjonen. Så at sikkerheten kan ivaretas med riktige avtaler og organisasjonsmessige oppsett, selv om vi er parten som har ansvar for en større bit. Sikkerhetsvurderinger gir ingen fasit for hvilken løsning som er best. Du kan ikke si at du må ha en MVNO fordi det er sikrest, vi tenker at den konklusjonen kan vi ikke trekke. |
| 32 | E | Jeg tenker også på det med utfordringer i dagens Nødnett. Den ene operatørens forslag til modell, er at man skal bruke flere kjernenett for å få ekstra redundans i den enden av nettet også. Jeg er litt nysgjerrig på, hvis du har noe innsikt i det, hvordan man tenker på utfordringer med oppetiden i kjernenettet i Nødnett i dag. |
| 33 | I | Oppetiden i kjernenettet i dagens Nødnett er veldig god. Jeg tror vi har hatt ett delvis kjernenettutfall på alle de ... Faktisk har vi vel hatt tjeneste nå i over 10 år, hvis du tenker fra den såkalte fase 0-utbyggingen rundt hele Oslofjorden, i Sør-Øst-Norge, så tror jeg ikke det var noe kjernenettutfall før det var et mindre utfall for et års tid siden. Så vi må si at det har vært veldig stabilt. Det er kjernenettutfall hos de kommersielle aktørene iblant, de ser ut til kanskje å kunne skje en gang i året eller noe mindre for hver av operatørene. Det finnes statistikk på det. Det er ganske sjelden og de varer nødvendigvis ikke så lenge hver gang, men det er klart at hvis kjernenettet faller ut så går det ut over store grupper, noen ganger alle de som bruker det kjernenettet. Eller at en god del av tjenestene, kanskje ikke alle, faller ut. Det har store konsekvenser. Hvis det da f.eks. gjør at hele MCX-tjenesten blir utilgjengelig i 12 timer i hele Norge, vil det være veldig dumt. Men altså, her må det kompenseres opp. |
| 34 | I | Spør du da om det vil bli bedre med flere kjernenett. Det er ikke sikkert, da vil kanskje utfallene skje tre ganger så ofte. Da faller jo altså en tredjedel av brukerne ut, hvis du tenker at de er likt fordelt tvers over. Da får du ikke samarbeidet på samme måten, samhandlingseffekten. Så du løser det på en måte ikke, du sprer problemet ut, så en del faller ut og det skjer litt oftere, men det blir kanskje veldig sjeldent at alle mister tjenesten. Det er ikke sikkert at det helt er løsningen. Lurer du litt på vurderinger rundt det å ha flere kjernenett i hele løsningen her? Det gjør løsningen veldig stor og spagetti. Det er veldig, veldig mye å ta hensyn til. Det er mye som skal driftes og passes på. Mye flere avtaler, mange flere grensesnitt. Det er flere ting som kan gå galt, ikke bare i kjernenettet. Det er mer som kan gå galt. Så det kan være at det er bedre å putte ressursene på å styrke den |

| | | |
|---|---|---|
| | | løsningen vi faktisk bygger. Med både buksesele og belte, med mer grad av redundans. |
| 35 | I | Hvis det da bygges opp et eget kjernenett som ikke er det samme som det kommersielle kjernenettet hos en kommersiell mobiloperatør, hvis det er en slik løsning vi ser. Da kan et slikt kjernenett hos en kommersiell mobiloperatør som ikke er det samme som det kommersielle kjernenettet, være mer vernet mot oppgraderinger og arbeid. Det er da veldig sannsynlig at hvis en operatør skal bygge et kjernenett for oss som er i parallell, men som ikke er det samme som det kommersielle kjernenettet, at de kan ha samme leverandør. Og da kan det kommersielle kjernenettet oppgraderes og endres og gjøres ting på, før de får lov til å gjøre noe med nød- og beredskapskjernenettet. Slik at du har erfaringene både fra leverandøren i utstyret, og også i organisasjonen og hvordan det gjøres. At du da føler en enda større trygghet i at det faktisk går bra. For en del av kjernenettutfallene har vært relatert til at det har vært arbeid i nettet, ikke sant. Planlagt arbeid, det kan gjøre at nød- og beredskapskjernenettet kan bli enda mer stabilt enn det vi ser på de kommersielle kjernenettene. Og så kan vi være litt mer på vakt når det kommer en teknologi inn, for erfaringen også på statistikken som Nkom har, den viser at det er flere store utfall i mobilnettene når en G er ny, enn når en G er moden. Så det var flere store utfall i 2011/2012 da LTE var nytt, 4G var nytt, enn det er nå når det er modent. Kanskje være litt på vakt på den effekten også for 5G. Så jeg tror ikke det er en quick fix å ha flere kjernenett. |
| 36 | I | Hvis du lurer på backup-løsninger så kan du se nærmere på det å kanskje la noen bruker ha kanskje et alternativt SIM-kort eller noe sånt, slik at du kan bruke et annet kjernenett. Men det er radionettet som feiler i praksis. Utfall på enkelte BS eller grupper av BS, sikkert noe som Lina ser på. Og det merker brukerne veldig, når dekningen forsvinner så er tjenesten borte vekk, den. Jeg bryr meg ikke om det er kjernenett eller radionett, dekningen er borte og jeg får ikke gjort det jeg skal på ulykkesstedet. Da kan nasjonal gjesting være et bra tiltak, at man har tilgang til de andre radionettene. Det er noe vi ser på, å innføre nasjonal gjesting. |
| 37 | E | Da er det sånn at man kan roame med et prioritetsabonnement, uten nødvendigvis ha flere SIM-kort for å koble seg til flere kjernenett? |
| 38 | I | Ja. Tenker at det blir enklere, hvert fall for brukerne. Det er litt mer transparent for brukerne og stiller ikke krav om to SIM i terminalen. Og hvis man skal ha to SIM så blir det jo dyrt. Brukerne våre klager over at det er dyrt med Nødnett. De har jo sine driftsbudsjetter, og skal de ha flere SIM, to stykker, på terminalene, så ... Selv om mange moderne terminaler i dag støtter to SIM. Det er forholdsvis vanlig, ikke alle, men en del gjør det, så det går kanskje an å stille krav til terminalene at de skal ha to SIM, men da må de betale for abonnementet på en eller annen måte. Og så snakker dere om sikkerhet. Når du sprer deg i flere nett, så blir det vanskeligere å ivareta den og. |
| 39 | E | Ja, det er litt en avveing med redundans og robusthet, og tekniske utfordringer og sånt. Det er mange nyanser her. I forbindelse med det med redundans og robusthet i radionettet. Mange av løsningene er litt på om man skal benytte seg av flere radionett. Jeg vet ikke om du har oversikt over det, men et spørsmål jeg har hatt og som har vært litt ubesvart, er det med den reelle redundansen i radionettet hvis man benytter seg i av flere radionett. Med tanke på at mange av mange av BS er samlokaliserte og på samme master, har man noen gode oversikter over, ja hvis denne fiberen faller ut så hjelper det ikke å redundans i flere radionett, fordi alle radionettene faller ut f.eks. |
| 40 | I | Ja, det er en del delt infrastruktur. Noen steder er det det, noen steder er det ikke det. Den effekten er nok størst i grisgrendte strøk, hvor det er vanskelig å få frem infrastruktur. Da er det flere som henger på det samme og mer ko-lokalisering. Da er det også mindre grad av overlapp mellom cellene. Overlapp mellom cellene gir redundans i seg selv, det. I Oslo har vi |

| | | |
|---|---|---|
| | | jo så mange TETRA-BS at hvis det detter ned 3-4 stykker så merker sannsynligvis ikke brukerne det, i alle fall ikke utendørs. Kanskje nedi en kjeller. Sånn er det også i mobilnettene. De har større grad av overlapp og mindre avhengigheter i tettbygde strøk, men jo lengre ut på landet du drar, jo verre er den effekten. Der er jo djevelen i detaljene, for det er forskjellig hele veien. Noen steder har de fått til å lage det uavhengig, andre steder ikke. Det er klart noe som man kan gjøre er å se på akkurat de sårbarhetene. Men der nok noe som er viktig for oss, men som blir viktig for landet generelt, at nettene er robuste og gode og fungerer hele tiden. Det er en av de tingene som understrekes fra myndighetene. Det kom en stortingsmelding om ekom nå på fredag, jeg vet ikke om dere har sett den. |
| 41 | E | Jeg så den kom, men har ikke sett på innholdet. |
| 42 | I | Det kan være ålreit for dere å skumme gjennom og se. Den kom nå på fredag, og der står det at å ha tilgjengelige tjenester, både god dekning, men også at det er robust, er viktig. Da må man robustifisere, gjerne med flere føringsveier, osv. Og å identifisere hvor det er svake løsninger, og samtidig er det veldig viktig at kommunikasjonen fungerer. Derfor har myndighetene nå som håndtert av Nkom et program som heter forsterket ekom. Dere har kanskje hørt om det? |
| 43 | L | Ja. |
| 44 | I | Ja, akkurat. Og det programmet har blitt trappet opp en del. Det har blitt tilført en god del flere millioner kroner per år, og det er veldig bra. For hver nye doble fremføring på transmisjon, og hver time med batteri-backup, hver kvadratmeter med dekning, det er flott. For oss også. Så det går i riktig retning, men det er klart det med felles avhengigheter og at alle tre nettene kan gå ned på en del steder samtidig, det er reelt, det. Da hjelper ikke den nasjonale gjestingen, når det ikke er noe overlapp. Si at alle tre operatørene er i det samme tårnet og det er det eneste der. Hvis strømmen går og batteriet er brukt opp, så forsvant den dekningen. Det er nok del av det puslespillarbeidet som må gjøres etter hvert. Men nå er det slik at vi skal ikke vente med å gå over til kommersielle nett til alt er tipp topp og bra. Vi må finne ut når det er bra nok, men så stopper ikke arbeidet der. Da må vi regne med at det fortsetter å forbedres og bli enda bedre. Men det må være på godt nok nivå. |
| 45 | E | Det å skulle vurdere når det er bra nok, handler det om å skulle se det i forhold til nåværende Nødnett, at det skal være minst like bra som det nåværende Nødnettet? |
| 46 | I | Det er en bra målestokk. |
| 47 | E | F.eks. sånn de har gjort det i ESN ift. AirWave i England, såvidt jeg har forstått. |
| 48 | I | Ja, de driver og bygger og forbedrer nettet der også. Og bygger tunneldekning i tuben i London, stor innsats. Hvis du tenker på dekning i grisgrendte strøk i Storbritannia, så er det program for det nå, for å legge til rette for det. At alle aktørene får muligheten til å etablere seg der det ikke har vært dekning før. De kaller det for not-spots. Der er det et spleiselag. Det er ganske stort, men det er ti ganger så mange mennesker der borte, så da blir kanskje ting ti ganger så stort, selv om vi er kanskje litt rikere per person. Der er det et stort spleiselag hvor det er vel 1 mrd. pund ca. som er budsjettet, der myndighetene putter inn halvparten og så tar de kommersielle aktørene den andre halvparten. Da blir det insentiv nok til å bygge dekning der det ikke var egnet før. Det er viktig for sikkerheten og folk som faktisk bor der. Det finnes grisgrendte strøk i Storbritannia også, selv om man ikke tror det når man er i London. |
| 49 | E | Man har ikke noen helt konkrete krav til hvilke tjenester og hvilke krav til funksjonaliteten i |

| | | |
|---|---|---|
| | | nettet når man skal gå over? |
| 50 | I | Tjenestene kommer på en måte på fordi det da bygges 4G- og 5G-dekning. Så jeg vet ikke om det er satt noen spesielle krav, du legger vel bare til rette at det kommer dekning og så vil det være godt nok for tjenestene. Da kan man lure på om det legges opp 5G-messig, med det å kunne ha veldig lav forsinkelse og ha selvkjørende biler langt ute osv., den typen krav. Det har jeg ikke sett noe til, faktisk. Jeg har ikke gått noe inn i de detaljene. Når bygger dekning, blir det bra nok for alle de fremtidige tjenestene vi ser for oss. Du får ikke millimeterbånd-dekning i 5G over hele landet ut over hele periferien fordi du bruker 1 mrd. pund. Det ville kostet mye mer. |
| 51 | L | Jeg vet at du har litt peiling på og har gjort litt peiling på datatjenester i Nødnett og i fremtidens Nødnett. Jeg har sett noen presentasjoner du har holdt for lenge siden. I min oppgave har jeg også scopet inn å prøve å få litt overblikk av hva som kommer til å være bare minimum behov for tjenester i det isolerte scenarioet. F.eks. når du er i frakoblet fra kontrollrom, er det kun behov for PTT, eller vil det i fremtiden være behov for videotjenester og dermed tilhørende kompleksitet? |
| 52 | I | Det er et veldig godt spørsmål. Det har vi ikke sett så mye i detalj på, men jeg kan tenke meg at brukerne kanskje kan akseptere at det da er et lavere tjenestenivå. Det er vel alt jeg kan si der. Men altså, PTT er den viktigste tjenesten. Den skal kunne fungere ute i et sånt tilfelle hvor BSen eller et sett med BS er avskåret fra kjernenettet. Det er vel det du ser på, Lina? |
| 53 | L | Det stemmer. |
| 54 | I | Ikke sant. Så da har du studert IOPS, da, sikkert for 4G? |
| 55 | L | Ja. |
| 56 | I | Ikke sant. Nå er det ikke igangsatt et arbeid for å videreføre IOPS inn i 5G, men det kan jo være at det kommer. Det jeg lurer på er om det kan bli en del av edge-konseptet. Der er det mulig at dere kan mer enn mer allerede. Der drar man jo prosessering lenger ut mot BSene. |
| 57 | L | Nettopp, det her kan bli en vinn-vinn-situasjon. |
| 58 | I | Ja, ikke sant. Nemlig. Men det arbeidet tror jeg ikke helt har gått opp. Jeg har stilt det spørsmålet internasjonalt, når jeg er i internasjonale møter og sånt om det er aktuelt. Jeg spurte spørsmålet til de mest sentrale chairmennene i 3GPP på tjenester og radio og core, men de hadde ikke et godt svar. Men det er jo igjen en dugnad ikke sant, så det må komme fra medlemmer. Så jeg lurer på om edge, om det er en vei å gå der. Men altså, hvilke tjenester, jeg tror at tale kommer til å være det viktigste for brukerne våre i lang tid. Men det er et bakteppe her at de får nye tjenester. Det vil jo etter hvert endre måten de jobber på, tenker jeg. Men det er jo en utvikling som kommer til å gå og sikkert ta en del år. Så det kan godt hende at det er et annet svar på det spørsmålet om en 10-15 år, Lina. |
| 59 | L | Disse tjenestene bygger jo på hverandre, så kanskje det blir logisk å legge fram at hvis du bygger ut funksjonalitet for PTT så blir det lettere å bygge på push-to-video og alle mulige ting oppå det. |
| 60 | I | Ja, men så spørs det hva du mener med videotjenester. Push-to-video, som FaceTime, blir veldig lignende PTT at du gjør det mellom gruppen fra terminalene. Men mye av de videotjenestene vi kommer til å se, de kommer til å komme fra kontrollrommet, kanskje video fra andre kilder. Og da er det kuttet av. Så om du har kontakt med kontrollrommet, |

| | | |
|---|---|---|
| | | hvert fall ikke sentralt, da må det være noe utskutt noe som er der det fremdeles er kommunikasjon. I en sånn løsning, Lina, så tror jeg ikke det er slik at det blir mye vanskeligere å opprettholde en videotjeneste. Det blir mer på use casene. Hvis du først har en sånn nedskalert type MCX-funksjonalitet ute i den isolerte delen av radionettet, så ser jeg ikke noe i veien for at det også skal kunne håndtere andre MCX-tjenester enn bare MCPTT. |
| 61 | L | Ja, spørsmålet er heller hvem du kan snakke med? |
| 62 | I | Ja, ikke sant. Er det noen å snakke med, er det noe interessant igjen. |
| 63 | L | Ja, jeg tror det er det vi har diskutert oss frem til i stor grad i det siste, at kompleksiteten i min oppgave ikke ligger på teknisk gjennomførbarhet, men heller logisk gjennomførbarhet med. |
| 64 | E | Jeg tenker litt høyt, men det vi har sett som hovedutfordringen med autonom edge er å skulle synkronisere den HLR/HSS-funksjonaliteten ut til edgen. Hvis man allerede får til det da, så er kanskje ikke den funksjonaliteten ... Hvis man først har fått til MCPTT kan man også få til MCVideo, for da har man subscriber-informasjonen ute i edge. |
| 65 | I | Ja. Det er egentlig to hovedutfordringer her, så lenge det er tekniske løsninger. Den ene er vel på kostnaden, for det må investeres ut og du må definere disse øyene, hvor mange skal du ha i Norge, og det må bygges og investeres i. Og så er det et sikkerhetsaspekt, for når du begynner å dra et aspekt av HSS og brukerinformasjon ut til flere geografiske plasser, så eksponerer du deg for et angrep flere steder. Du blir mer sårbar, det er flere lokasjoner som kanskje må sikres på noen måte. Det må også kunne løses. Det er gjort en del tenking på det på IOPS-arbeidet. Hvis dere snakker med leverandører så tror jeg det er Ericsson som har kommet lengst på det. Jeg er ikke sikker på at det er levert noe, men jeg tror de har kommet så langt at de har bygget og testet noe IOPS. Så jeg tror at hvis dere snakker med noen eksperter hos Ericsson … Dere har fått tilgang til litt leverandører og sånt eller? |
| 66 | E | Vi har fått noe kontaktinformasjon, men vi har ikke vært i kontakt med noen leverandører. |
| 67 | I | Hvis dere graver opp noe hos Ericsson så ville jeg hørt litt der om IOPS. |
| 68 | L | Ok, kult. Takk! |
| 69 | I | Det er nok de som har kommet lengst i den tenkingen. Det kan være at de til og med har bygget det noen steder. |
| 70 | E | En ting som jeg kom på i forbindelse med autonom edge. Et spørsmål vi har stilt i flere intervjuer, men som er vanskelig for flere å svare på. Hvis vi ser på et MVNO-oppsett der man har DSB som MVNO eller med et eget kjernenett, og så har man en kommersiell operatør ute i radionettet, hvem skal ha ansvar for edgen? Er det DSB som skal flytte kjernenettet helt ut i edge, eller er det noe man overlater til operatøren eventuelt? |
| 71 | I | Det er et godt spørsmål, men jeg har ikke det svaret. Jeg må innrømme at jeg kjenner ikke 5G godt nok enda, så jeg har ikke svarene innenfor 5G på alt det. Men det er slik at skivene, de går ut også gjennom edgen, gjør de ikke det da? Slik at man kan tenke seg en nød- og beredskapsskive som er beskyttet der ute som en del av arkitekturen. Er det ikke sånn? |
| 72 | E | Jo, jeg tror kanskje det, men det blir jo den samme sikkerhetsutfordringen med at man kanskje må ha ekstra sikkerhetstiltak ute i edgen for å sikre den hardwaren og sånt som den informasjonen skal være på. Og hvis man har en kommersiell aktør som er der ute i |

| | | |
|---|---|---|
| | | radionettet, om de skal ha ansvar også for edgen, så får de en helt annen sikkerhetsprofil når de også har den HLRen å ta seg av. |
| 73 | I | Nei, jeg hører spørsmålene dine, jeg synes det er gode spørsmål, men de har ikke jeg svar på dessverre. |
| 74 | E | Er det sånn å forstå at 5G er såpass nytt fremdeles at hovedfokuset er på 4G? |
| 75 | I | Jeg tror det er mye som ikke er avklart i 5G, nei. Jeg vet ikke om det f.eks. er en sånn fullgod MVNO-modell som er meisla helt ut i 5G. Det jeg hører er at en MVNO sikkert bare kan få seg en egen slice og et eget SIM-kort, men jeg tror ikke det der er ferdig tenkt. Tradisjonelt har vi sett MVNOer som har en del fysisk kjernenett selv, og så kobler de seg på radionettet som oftest med sånn S8 vanlig roaming-grensesnitt. Og så bruker de en del av coren i det nettet de har som partner. Så er det Ventelo/Phonero og danske TDC, de var også MVNO på det nivået i Norge. Da var det avklart at man hadde de nodene og så koblet man seg på. Det lignet på utenlandsroaming. I 5G ser jeg at det blir annerledes. Jeg tror ikke den er gått opp enda, MVNO-modellen. Antakelig så blir det vel at du får avtale om å disponere en skive og så leier du deg inn der, og så er du en virtuell operatør og så kan du kanskje bygge tjenester innenfor den skiven. Men jeg vet ikke helt. |
| 76 | E | Vi har fått høre ulike ting, bl.a. om denne NEF som finnes i 5G-arkitekuren, som gjør at man kan eksponere 5G-funksjoner ut eksternt. Det er veldig mange ulike måter å gjøre ting på, høres det ut som. |
| 77 | I | Der har jeg ikke så mange svar. Jeg skal nok jobbe mer med 5G etter hvert, jeg og. |
| 78 | E | I arbeidet med den KVUen, der er det 4G som er fokuset? |
| 79 | I | Vi har jo utgangspunkt i 4G, men i visshet om at det finnes løsninger for 5G. Finnene sier de skal ha 5G. De bygger opp en MVNO og skal ha 5G-utstyr i sin MVNO. Men jeg vet ikke om det er ferdig gått opp, vi får se. |
| 80 | E | Vi begynner å nærme oss tiden her. |
| 81 | I | Har du fått svar på spørsmålene dine? |
| 82 | L | Jeg har lært masse jeg, jeg tenker hardt! |
| 83 | E | Jeg synes det har vært veldig informativt. Du har vært flink til å svare på spørsmålene. Så det har vært veldig informativt. |
| 84 | I | Jeg synes det er bra spørsmål fra dere, og stilig at dere har tatt de oppgavene her. Det er gøy. Vi gleder oss til å se på hva dere lager etter hvert. Det blir spennende, det. |
| 85 | E | Det blir interessant å se. Nå skal vi prosessere disse resultatene og diskutere og kanskje konkludere litt. Jeg tror det blir vanskelig å konkludere, det vet du sikkert alt om fra KVU-arbeidet, at det er pros and cons over hele linja. Det er vanskelig å konkludere med en ting. En ting jeg også ser på er jo, jeg skal jo ikke gå så mye inn på de politiske og økonomiske aspektene ved denne avgjørelsen, men det er vanskelig å komme utenom de konkurransevridende aspektene ved f.eks. å velge en hovedoperatør i radionettet. Se på utfordringer rundt vendor lock-in og sånt. |
| 86 | I | Ser du på det i din oppgave, Eivind? |

| | | |
|---|---|---|
| 87 | E | Ja. |
| 88 | I | Ja, du gjør det ja. Når du leser den ekommeldingen som kom på fredag ... Dere har funnet den skjønner jeg, ellers kan jeg sende dere en link. Der ser du også at myndighetene er opptatt av at det skal være konkurranse i mobilmarkedet. De sier minst tre operatører, det er forhåpentligvis i hvert fall tre. Så de legger til rette for det, og det er viktig at konkurransen styrkes for å få ned prisene, for de har nettopp gjort noen analyser av prisnivået i Norge sammenlignet med nabolandene våre, og vi er jo kjempedyre. Og så ser du at sånn som operatørene har jo kjempestore marginer. Det må da være noe å gå på. Så det konkurranseaspektet, det har myndighetene også fokus på. Og det påvirker valget. Det er en viktig parameter. |
| 89 | E | Mhm. Ja det er både det konkurranseaspektet i seg selv, mobiloperatørene imellom, men også det å skulle låse seg til en operatør. Jeg har lest den etterevalueringen av Nødnettprosjektet, rapporten som kom ut i januar i år. Der er det jo litt vurderinger også rundt utfordringer med turnkey-kontrakter som er litt interessant synes jeg. |
| 90 | I | Ja, nei, det vi gjør, vi er jo en stor og viktig aktør. Hvis det gjøres feil, så kan jo en operatør få store fordeler. Så det må gjøres riktig. Hvis f.eks. staten skulle bruke flere mrd. kroner på å styrke et radionett så ville jo det vært veldig rart, så det må gjøres på den riktige måten. Samtidig ønsker jo ikke vi å stille opp med trillebårlass fulle av penger, vi må se hva operatørene er villige til å bidra med selv. Vi må få operatørene til å bygge det beste nettet, staten skal ikke bygge det for dem. Vi må prøve å være gode innkjøpere her og fiske ut mest mulig etter hvor operatørene er villige til å strekke seg for å få den store brukeren. Vi er ganske store, litt avhengig av hvordan du regner, men vi har rundt 60 000 abonnementer i TETRA-nettet nå nylig. Så vi ser kanskje på rundt 75 000 tilsvarende brukere, og så kommer IoT i tillegg med sensorer og der kan det bli veldig mange, men samtidig er det lavere volumer. Men det er klart at en kunde med 75 000 brukere som betaler forholdsvis godt per bruker, det er jo interessant. Men det finnes andre forretningskontrakter i Norge som er i størrelsesnivå. Vi snur ikke nødvendigvis opp ned på televerden med at vi kommer inn. |
| 91 | L | Det er vel en viss tyngde i å levere tjenester til de mest kritiske brukerne i landet også. |
| 92 | I | Ja, så lenge det går bra. Hvis en operatør skal levere en hovedleveranse her så får de pepper så det holder hvis det går ut over samfunnssikkerheten og konkrete aksjoner. Kommer det en stor ny 22. juli-lignende sak og det ikke funket, så er det ikke sikkert at den effekten er positiv. Men går det bra, kan det være en fjær i hatten. Vi er det nettet som er godt nok for nød og beredskap. Kan skryte på seg god dekning, masse robusthet, stabilitet, god nok oppetid, best for deg. Så det er en effekt. Men det er et tveegget sverd. |
| 93 | L | Vi går tomme for tid her. Er det noe du føler vi burde spurt deg om, som vi ikke har vært innom? |
| 94 | I | Det er vanskelig å si. Vi har vært innom mye nå, altså. Så har vi jo fått luftet ganske mye. Det er mye vi ikke har snakket om også, som device-to-device-kommunikasjon, trenger vi multicast og broadcast i nettet og sånne ting. Så det er jo mange andre temaer, og alt er ikke så godt løst og sånt. Dere er jo velkommen til å bare ta kontakt igjen utover våren igjen om dere skulle lure på noe. |
| 95 | E | Det setter vi pris på. |
| 96 | L | Det som skjer nå, er at vi transkriberer og sender deg transkriptet så du kan se over om det |

| | | |
|---|---|---|
| | | er tilstrekkelig anonymisert og det ser greit ut. |
| 97 | I | Lykke til med skrivingen! Så høres vi. |
| 98 | E | Det gjør vi. Takk skal du ha. Ha det godt! |

Appendix N

# Directorate for Civil Protection C

This interview is conducted with a representative of the Norwegian directorate for civil protection (DSB) who is familiar with the processes surrounding the establishment of the existing TETRA based Nødnett, as well as the challenges faced by the state when moving towards the next generation of public safety communications. Topics of conversation range from considerations regarding the successes and failures of Nødnett to considerations regarding the way forwards in terms of alternative deployment models and the ways in which the state could attempt to manage their relationships with commercial providers by defining clear requirements and drafting comprehensive contractual agreements.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | ... Sånn, og så spør jeg om det er greit at vi gjør lydopptak. |
| 2 | I | Ja, det er greit. |
| 3 | E | Supert, takk skal du ha. Jeg kan begynne med min egen oppgave. Jeg ser litt på kjernenettet, og hvordan man skal gjøre det i samarbeid med kommersielle mobiloperatører og aktører, siden man skal samarbeide med kommersielle aktører i radionettet. Ulike alternativer for hvordan man skal løse utfordringer i kjernenettet, med fokus på 5G da. |
| 4 | L | Jeg er ute i radionettet, og ser på caset der én eller en gruppe av basestasjoner har mistet tilkoblingen til kjernenettet og må virke som en isolert øy. Utfordringer det medbringer, både teknisk og operasjonelt med de forskjellige brukergruppene og sånt noe. |
| 5 | I | Mhm, spennende! |
| 6 | E | Sånn vi har forstått det, så har du en del kunnskap om etableringen av det eksisterende Nødnettet? |
| 7 | I | Ja, det har vært en etablering av et nett, men også etablering av en organisasjon og etablering av en tjeneste. Så det har vært en interessant reise, fordi det alltid har vært nye faser med nye problemstillinger, der man ikke har kunnet snu seg rundt og bare kopiere noen. Nå er vi jo der at den kontrakten som ble inngått i 2006, som var en to-trinns beslutning, så det tok ca. 10 år før vi var ferdig utbygd, den går ut i 2026, og det er det som er triggeren for at vi har begynt å se på hva vi skal gjøre etterpå. Og, parallelt med at vi må bestemme oss for hva vi skal gjøre med TETRA-nettet, så har det kommet nye behov, blant annet for data og sånt. Det man gjerne har sagt helt siden starten i denne bransjen også internasjonalt, er at tale det er mission critical, det er man helt avhengige av. Det er det eneste som er mission critical i dag, det sa man den gangen. Men, på et eller annet tidspunkt så visste man at data kom til å bli mission critical, men man visste ikke helt når det kom til å skje, eller hvilke tjenester som ville bli mission critical. Mission critical betyr at du ikke klarer å løse oppdraget ditt på en god måte uten. Så nå har vel det kanskje inntruffet, uten at vi har et system til å håndtere de dataene. Det er vel kanskje litt sånn teknologiutviklingen treffer denne bransjen. |
| 8 | E | En av de tingene som jeg er litt interessert i med tanke på at man nå ser på ulike modeller for hvordan man skal gjøre ting i neste generasjons Nødnett, er vurderingene som ble gjort rundt det eksisterende nødnettet da det ble opprettet, og man gikk for en sånn turnkey-kontrakt med originalt Siemens. |
| 9 | I | Mhm, det var en lang beslutningsprosess før man fikk de endelige beslutningene der. Behovene kom fra helsesektoren, der de tenkte at man hadde behov for et nytt landsdekkende nett. De hadde et gammelt nett før det, noe som het Helseradionettet. Politiet hadde sine analoge nett, som var stort sett ett og ett politidistrikt. I brannvesenet hadde de mange forskjellige analoge nett, mindre nett som dekket sine områder, kanskje med en basestasjon her og der. Sånne analoge systemer som ble driftet av dem selv. I helse hadde de faktisk et landsdekkende nett, og det var det nettet som Telenor hadde før de bygde NMT. Dere kan kanskje den historien om NMT og GSM og de ulike G'ene oppover, men dette var altså det som var før NMT, som helse hadde overtatt og som de holdt i live. Men det ble gammelt, og det var et behov for å bytte det ut. Da så man at man burde gjøre det felles, så da jobbet man for å få et felles digitalt nett. Og dette skjedde i parallell med at TETRA-standarden utviklet seg og ble rullet ut, og den TETRA-standarden ble jo til nettopp |

for å dekke dette behovet til nødetatene. Politiet først og fremst. Men det var lenge usikkert om staten skulle eie nettet, eller om de skulle kjøpe tjenestene. Det var to ting, og det gikk på selve nettet. Dette er litt sånn politisk, hvilken vei man vil gå, men når vi begynte med dette så trodde vi at det kom til å bli tjenestekjøp. Vi trodde at det skulle være en sånn OPS-modell, et sånt public-private partnership, offentlig-privat samarbeid. På den tiden var det kanskje litt moderne. Man brukte det på et par veiprosjekter, og man brukte det til å bygge noen skoler og sånn. I England, der hadde de gått for en sånn modell, og i vår bransje så lærer man mye av hverandre ved å dele informasjon. Så vi hadde dialog med dem. For det vi gjorde parallelt med at man jobbet for å få beslutningen, var at man jobbet for å få et konkurransegrunnlag. Man hadde jobbet med kravene, behovene, og så skulle vi gjøre det om til et konkurransegrunnlag, en RFP, som vi da sender ut til markedet og som de leverer tilbud på. Det var det første vi gjorde, og vi begynte å skrive den som om vi skulle kjøpe en tjeneste. Og det er jo mentalt litt forskjellig fra når du skal kjøpe noe du skal eie selv, men uansett så er man bundet av anskaffelsesregelverk, og man må skrive kravene funksjonelt. Så vi gjorde det. Men så, ganske sent i beslutningsløpet, bestemte man seg da for at staten skulle eie. Nå vil jeg ikke spekulere for mye, men man kan jo tenke seg flere grunner til det. Det ene er ønsket om nasjonal kontroll, og det andre er at OPS ofte ble brukt i situasjoner der staten ikke selv kan fullfinansiere, så det er på en måte en sånn finansieringsmodell. Men her hadde ikke staten noe problem med å finansiere. Så jeg tror kanskje at det var de to tingene i sum. Samtidig er det klart at dette med verdien eller viktigheten av Nødnett - Altså, vi visste at det kom til å bli kritisk infrastruktur, men det vi erstattet var jo mange analoge helt åpne nett. Så fokuset var å erstatte det som var den gangen. Og da tok vi det vi hadde jobbet med som et tjenestekjøp, og gjorde det om. Men det var veldig nyttig å ha jobbet gjennom det som et tjenestekjøp, for da hadde vi en funksjonell beskrivelse av kravene for det vi skulle kjøpe. Og så måtte det selvfølgelig utarbeides en del andre ting. Så det med turnkey på nettverket, det tror jeg faktisk kom litt naturlig som følge av at vi hadde vært i den modusen der vi skulle kjøpe en tjeneste. For når du skal kjøpe en tjeneste, da vet du at alt ansvaret går på én. Men det som var det aller viktigste var nok alltid risiko. Altså, hvem er best til å håndtere risiko, hvem er best til å håndtere helheten. Hvis du for eksempel ser på nettverkskontrakten - Man kunne for eksempel gjort sånn at man kjøpte nærmest én og én basestasjon, og så bygde opp delene selv. Man kunne tenke seg for eksempel at staten tok ansvar for radioplan. I Sverige hadde man en litt mer sånn tilnærming. Men jeg tror det med ansvarsdelingen, og det at staten ikke skulle påta seg for mye risiko i forhold til å være en integrator, det var viktig. Vi ville ha én å peke på som hadde ansvar ende-til-ende for tjenestene. Det gjaldt utrullingen, men det gjaldt også driften. Så det er grunnen til at driftsavtalen er med det som var Siemens den gangen. Det vi også vurderte som en del av anskaffelsen var om man skulle ha en lang eller kort driftsavtale. Man kunne jo tenke seg at man hadde en 6-årig driftsavtale, som så måtte lyses ut på nytt. Så det valget tok vi som en del av anskaffelsen, etter å ha undersøkt markedet for begge deler. Så det tror jeg var en naturlig beslutning å ta. I den beslutningen til Stortinget var det jo og sagt at staten ikke skulle etablere et nytt televerk, men man skulle eie. Det er noe med å ha én som er ansvarlig for sluttjenesten. Og så valgte vi også å inkludere kontrollrommene. Først fikk man da finansiert utstyr til kontrollrommene på alle 110, alle 112, alle AMKer, alle legevakter og noen til. Det gjorde man fordi for å få tatt i bruk TETRA-nettet, så måtte man ha utstyr der. For at det ikke skulle bli en forsinkelse der vi bygde ut et nett som ikke ble tatt i bruk som følge av en mangel på utstyr, så valgte man å finansiere det i samme pakke. Den samme logikken gjaldt for radioterminalene. Vi gjør en førstegangsanskaffelse av det nødvendige utstyret, sånn at vi kan ta i bruk nettet så fort som mulig. Og dette var ting vi hadde hørt fra andre land at man hadde problemer med, så man forstod da at det var lurt. Men det at leverandøren av nettet skulle være ansvarlig for kontrollrommene, det var et valg som vi tok. Og det var igjen for å sikre grensesnittene, og sikre at det var én som hadde ansvar for at dette faktisk fungerte sammen. Vi gjorde det sånn at den som leverte tilbud på nettjenestene måtte ha med en underleverandør på kontrollrom. Men vi kjørte samtidig, i

| | | |
|---|---|---|
| | | parallell, en egen konkurranse på kontrollrom. Den kontrollromsleverandøren som var best ble valgt, og hvis det ikke var den samme som den nettverksleverandøren hadde med seg, så hadde de allerede forpliktet seg til å bytte ut, sånn at vi tiltransporterte. Så det var en del av den pakken, der hovedargumentet var at staten ikke skulle sitte igjen med et integratoransvar. Men det ble et veldig ambisiøst prosjekt når vi gjorde det sånn, så det er jo - Har dere sett den evalueringsrapporten som er kommet? |
| 10 | E | Ja. Den er litt interessant. Det står blant annet noen kommentarer der om vurderinger som er gjort rundt det å ha turnkey-kontrakter. At det på den ene siden har vært stor forutsigbarhet, med tanke på kostnader og sånt, men at det på den andre siden kanskje har gått litt tregere, og at det har vært mye arbeid med å følge opp den ene leverandøren for å passe på at leveransene blir skikkelige. For når de har fått den kontrakten så legger de seg gjerne litt bakpå og vil minimere egne kostnader, var sånn jeg tolket det da. |
| 11 | I | Mhm, ja. Vi har sagt offentlig at det var en god kontrakt for staten. Det er sånn med sånne anskaffelser, at det er viktig å få ned prisen. Om det var fordi det var en turnkey-anskaffelse eller en fastpriskontrakt, det er jo - Vi kaller det en fastpriskontrakt, og så var det en turnkey. Om det ikke var en turnkey, så kunne det sikkert fortsatt vært fastpris på elementer, men dette var altså begge deler. Man får jo en slags monopolsituasjon i den perioden dette systemet er i bruk, men alt dette var vi opptatt av å kompensere for i kontrakten. Så tenker jeg at det faktum at vi hadde med disse kommunikasjonssentralene, det gav en voldsom kompleksitet, som vi kanskje ikke var helt forberedt på, og som vi kanskje tok litt for lett på. Det var jo egentlig et stort IT-prosjekt, der vi hadde tre etater, og alle etatene skulle levere til alle sine i hele landet. Samtidig så var kostnaden og de store pengene på nettverkssiden. Så det er to veldig komplekse og store prosjekter som er knyttet sammen. Og det var ikke bare knyttet sammen som i at leverandøren hadde ansvar for å levere det, men altså ferieplanene til legevaktsentralen et eller annet sted var plutselig en avhengighet som vi måtte ta hensyn til. Så det er klart at når man plutselig må snu helt om på utbyggingen av radionettet - Altså, det kan jo skje, og det er ikke nødvendigvis noe unormalt for en som skulle bygge radionett å snu seg rundt. Kanskje hvis det går veldig treigt her, så kan man fokusere der. Men det er klart at når du har et helt følgeprosjekt som henger på deg med sluttbrukere, så kan det skape litt friksjon. Og det gjorde det nok. Jeg tror fortsatt at vi hadde en veldig kjapp utrulling når ting først var klart. Når nettet var klart i et område så kom etatene på bang, bang, bang, altså. Så jeg tror det som var mest skadelig for tiden var den pausen. Det har jo vært sagt at kontrakten var god for staten, og det er også kjent at Siemens, som ikke var Siemens - Det ble jo Nokia Siemens Networks, fordi Nokia og Siemens slo sammen sine telekomenheter. Og det visste vi om før vi sluttforhandlet at skulle skje 1. april 2007, og da tenkte vi at det var positivt. Istedenfor én telekomaktør så har du plutselig to telekomaktører bak der. Det som skjedde forholdsvis fort etterpå, var at når dette nye selskapet ransaket seg selv og laget en ny strategi, så bestemte de seg for at den typen leveranser som de hadde til oss ikke var innenfor deres kjernevirksomhet. For det var jo Motorola som hele tiden var systemleverandøren, det var Motorola som leverte liksom Nødnettet, kjernenettet og ja, teknologien. Siemens hadde integratorrollen, som Nokia Siemens Networks da fikk. Vi fikk beslutningen fra Stortinget om landsdekkende utbygging i juni 2011, og så allerede tidlig i 2012, så overtok Motorola hovedansvar for kontrakten. Det som er kjent er at Nokia Siemens Networks som hadde den jobben, de betalte Motorola nesten 1 milliard for å gjøre den jobben. |
| 12 | E | Men hvis vi tenker på den turnkey-kontrakten da. For sånn jeg har forstått det, så var en av hovedgrunnene til at man ville bygge sitt eget dedikerte radionett at man ville benytte seg av TETRA-teknologien, og at den samme typen muligheter ikke fantes i de kommersielle nettene? |

| | | |
|---|---|---|
| 13 | I | Nei, det er egentlig ikke sant. Da vi gjennomførte anskaffelsen, var vi teknologinøytrale. Vi hadde de frekvensene som var dedikerte til nød- og beredskapskommunikasjon i hele Europa. I anskaffelsen var vi teknologinøytrale. Men det var en prekvalifisering først, og en av de som leverte tilbud der var en såkalt CMDA-teknologi. Jeg husker rett og slett ikke om det var regulert hvor mye staten skulle eie i den anskaffelsen, men det var en kjøpsanskaffelse. Så de var med i prekvalifiseringen. Og så var det en leverandør som leverte et tilbud på en TETRAPOL-teknologi, som er en mer proprietær - Det ligner litt på TETRA, men ikke, ja. Men den som leverte den CDMA-teknologien, de ble ikke med videre. Men det var ikke på grunn av teknologien. Vi var egentlig litt lei oss for at vi ikke fikk evaluert den, men det var andre forhold som gjorde at de måtte avvises. Så da hadde vi to TETRA-tilbud og ett TETRAPOL-tilbud inne i forhandlingene, som vi evaluerte. Og den TETRAPOL-løsningen ble ikke med i sluttforhandlingene, fordi det var en del funksjonalitet de ikke hadde. Men det var jo det som var den teknologien - Det fantes ingen andre teknologier, eller ihvertfall ikke noe annet marked. |
| 14 | E | Nei, for det jeg ville litt frem til var på en måte om det var mer naturlig å gå for en sånn turnkey-kontrakt fordi prosjektet var litt mer på siden av de eksisterende mobilnettene. Og at nå som vi skal til neste generasjon, der den teknologien som man skal bruke til neste generasjons Nødnett kanskje ligner mer på de kommersielle interessene til teleoperatørene, at det da vil være mulighet for større fleksibilitet. At man da ikke lener like hardt mot en turnkey-type kontrakt, men at det kan være et større marked for å utvikle tjenester som kan være mindre deler av systemet da, fordi teknologien ligner mer på den kommersielle teknologien. |
| 15 | I | Ja, altså det er en ting man har trukket litt frem. Altså, det man ønsker å oppnå ved å bruke mer kommersiell teknologi - At det finnes et marked, at det skjer en utvikling, og at man ikke blir så avhengig av de man velger. Så det kan kanskje være en hypotese. Kanskje det er en riktig antagelse at det var en såpass spesiell teknologi. Men det har jo skjedd en teknologiutvikling også, og jeg tror kanskje det nesten er like viktig. Det var sånn den teknologien var på den tiden, mens teknologien i dag er mye mer modulær. I dag er det mye mer åpne grensesnitt, og det mangfoldet som du snakket om. Men jeg tror det er den generelle teknologiutviklingen som har vært sånn. Og vi håper jo nå at vi kommer inn i en verden som er standardisert, og der det er litt mer mangfold. Men så er ikke det noe sånt med to streker under svaret, for vi vet ikke enda. Vi vet ikke enda hvor forskjellig dette blir fra det som de leverer til massemarkedet, fordi vi er fortsatt 1% av mengden. Og om den ene prosenten i alle land forener seg, som vi pleier å gjøre, eller prøver å gjøre, så er det likevel - Og man har jo oppnådd mye med den standardiseringen i 3GPP og fått på plass funksjonaliteten, men den er ikke industrialisert enda. Så vi vet ikke hvordan det markedet kommer til å konsolidere seg. Men de eventuelle endringene i markedet som vil skje, vil sannsynligvis skje på lik linje med utviklingen i det kommersielle markedet. Jeg vet ikke om dere skjønner helt hva jeg mener, men det skjer jo hele tiden at ett selskap går under og et annet dukker opp, eller de slår seg sammen, og så deler de ut og de selger ut, og det skjedde jo på begynnelsen av 2000-tallet akkurat det samme. Når TETRA kom så leverte Nokia både GSM og TETRA. Motorola leverte både GSM og TETRA. Men Nokia fant ut at det ikke var likt nok, så de sluttet med TETRA, og solgte den biten til det som etter hvert ble Airbus. Mens Motorola gjorde det omvendt, de solgte det kommersielle og satt igjen med sikkerhetsmarkedet vårt. Og alt dette skjedde jo mens vi holdt på med anskaffelsen, og det kommer til å fortsette å skje. At selskap slår seg sammen, etc. Og det må man bare ta høyde for. |
| 16 | E | Jeg synes det er litt interessant det du sier med tanke på den teknologiske utviklingen, og at ting kanskje blir mer standardiserte og modulære, kanskje spesielt nå når man beveger seg inn mot 5G. Jeg lurer på om en naturlig utvikling da, eller et resonnement ut ifra det, kan |

| | | |
|---|---|---|
| | | være at det gir mer mening å inngå kortere og mindre kontrakter med flere samarbeidspartnere, enn det gir å inngå en sånn stor turnkey-kontrakt? |
| 17 | I | Ja, det er et utrolig godt spørsmål, og egentlig veldig vanskelig å svare på. Jeg er veldig usikker. Nå er det gjort en KVU, og det er gjort noen analyser, men hvis jeg skal tenke litt på utsiden av det og tenke litt sammen med dere på det, så tror jeg det er viktig å komme i gang. Jeg tror det er viktig å komme i gang. Det er ikke sånn at man kan sitte å vente litt på at det kommer noe enda bedre. Her kommer liksom 5G, og så kommer 6G. Men jeg tror det er kjempeviktig å komme i gang. Og å komme i gang på en sånn måte at det finnes et utviklingsløp. At man ikke stagnerer i det ene eller det andre. Men akkurat hva som er den beste måten å få det til, det er jeg ikke helt sikker på, for hva slags miljø trenger du egentlig for å greie å følge med på den utviklingen? Jeg tror det er mange hos oss som synes det ville vært gøy å ha mange kontrakter og ha et stort ansvar, men er staten egentlig satt opp til - Altså, hva slags organisasjon trenger staten for å håndtere det? Det tror jeg de må se på for å stille de spørsmålene. |
| 18 | E | Ja, den ene modellen er jo det å skulle ha en egen statlig MVNO eller noe lignende. Men sånn jeg har forstått det så må man i så fall tiltrekke seg litt mer fagkunnskap og personell for å gjennomføre noe sånt i forhold til det man har i dag. |
| 19 | I | Ja, og det tenker jeg at det i seg selv er ikke en issue. Når vi startet med Nødnett så hadde vi ingenting. Så det å bygge en organisasjon, det er mulig hvis man vil. Spørsmålet er om staten er villig til å påta seg det ansvaret. Det tenker jeg er det viktigste spørsmålet. Staten må uansett styre noen kontrakter, kan man si. Om det skal være én eller to eller flere er jo litt det - Og hva slags rolle skal man ha? Hvis man er en MVNO, så har man jo ansvar for sluttbrukertjenesten, litt sånn som man er i dag. Men det i seg selv er heller ingen garanti for at man får rammer og bevilgninger til å være med på det utviklingsløpet da. |
| 20 | E | Men du tenker ikke umiddelbart at det er noen fordeler ved at staten gjør det på egenhånd egentlig? |
| 21 | I | Nei, altså, jeg tror at hvis det skal være noen fordel med det, så må det være - Det er jo noen plusser ved det. Det er kanskje noe med kontroll og sånt. Vi vet at man alltid kan skrive kontroll inn i kontrakten, men det er forskjell på å ha det der og å faktisk ha kontroll. Spesielt det med sikkerhet og sånn. Det er noe staten er opptatt av å ha kontroll på. Samtidig er det mange andre faktorer som spiller inn. For å ha ordentlig kontroll, så må du for eksempel ha et veldig stort og profesjonelt sikkerhetsmiljø. Og så kan selvfølgelig alt dette her kjøpes i enkeltkontrakter og sånt, så... Jeg tror ikke egentlig jeg har lyst til å være så mye for og imot, for det er noe med det vi har diskutert i den KVUen, men det hadde vært interessant å se hvilke plusser og minuser dere ser i deres oppgaver. Det er vi veldig interessert i. Men, det man ikke kommer unna da, det er de behovene man har som er litt spesielle. Disse kravene om det vi kaller mission critical. Så lenge de kravene og behovene er reelle, og det må vi jo ta utgangspunkt i at de er, så vil det sannsynligvis være et gap mellom det og det en leverandør synes er godt nok til å levere til massemarkedet og kanskje og til det business critical-markedet. Så, det tenker jeg er det viktige spørsmålet kanskje. Hva betyr dette for viljen og lysten til å levere sånne tjenester? For til syvende og sist så er det det som betyr noe. At du har et marked som faktisk ønsker å levere noe til dette. At du har leverandører. Om det er en stor med turnkey eller om det er mange små. Men hvis de ikke har dette som sitt forretningsområde, så er det vanskelig. |
| 22 | E | Nå har vi snakket litt med operatørene og sånt, og jeg får inntrykk av at det finnes en vilje der for å tilby denne typen tjenester. Og jeg lurer litt på om det kanskje da kan være - At hvis man i den modellen som blir valgt tilrettelegger for at operatørene kan konkurrere med |

| | | |
|---|---|---|
| | | hverandre på en annen måte enn man ville gjort om man valgte én operatør som en sånn turnkey provider. Om tjenesten da vil nytte av at man tilrettelegger for en viss konkurranse. |
| 23 | I | Ja, det er lett - Hvis man bare ser på tjenesten som en boks. At dette bare er noe som finnes automatisk. Så er det lett å tenke seg det. Men hvis det som trengs for å levere en sikker tjeneste ikke er som man tenkte seg, så ville ihvertfall ikke jeg personlig overvurdere den lysten da. Det leverandørene til syvende og sist, når alt kommer til alt, vil ha. Men det er veldig mye usikkerhet, i og med at vi ikke har prøvd dette her i Norge. Så spørsmålet er om man skal ta høyde for alt nå den første gangen, eller skal man komme i gang, og så heller sørge for at man kommer inn på et spor der det er en naturlig utvikling. Nei, det er jo - Og så er det interessant, kanskje i forhold til sånn, man ønsker jo ikke en sånn innlåsning. Men det er alltid litt innlåsning når man velger en leverandør. Uansett om du kjøper deg nye sko, eller hva det nå er for noe, ikke sant. Men det er også noe man må ta høyde for når man skriver disse kontraktene. |
| 24 | E | Ja, det vil kanskje være ulike grader av innlåsning ihvertfall. |
| 25 | I | Ja, og så må man ha mekanismer. Man må for eksempel være veldig tydelig på at ting skal være standardisert, og at det skal være internasjonale standarder. Og det skal det være når du går inn i kontrakten, men det må det også være når du går ut av kontrakten, ikke sant. Det er en del ting man kan gjøre. Man må sørge for å være tydelig på eierskap til data, for eksempel, tenker jeg. Man må etablere mekanismer som gjør at man kommer seg inn i kontrakten, og kommer seg ut av kontrakten. Og det tror jeg til syvende og sist er det viktigste. |
| 26 | E | Tenker du at det på en måte å planlegge for at man skal ut av kontrakten er enda viktigere enn det var da man inngikk kontrakten for det nåværende Nødnettet? Fordi den teknologiske utviklingen går såpass raskt nå? |
| 27 | I | Ja, det tenker jeg kanskje. Og så tenkte vi jo på det da vi kjøpte Nødnett. Vi tenkte for eksempel på det i tilknytning til den lange operatørkontrakten, at det var mekanismer der hvis det gikk skeis. Så man har jo tenkt på det. Men det er klart, det var en 20-årskontrakt, så det er litt lenger horisont. Vi kommer ikke til å inngå en 20-årskontrakt tror jeg. Selv om i USA, så har de jo gjort det, men de hadde frekvensene. Så det er egentlig frekvensene de har leid ut i den perioden. |
| 28 | L | Jeg synes du får frem veldig mange oversiktlige synspunkter her, jeg lærer veldig mye. |
| 29 | I | Ja, dette her er jo noe jeg har vært midt oppi. Og det var jo sånn den gangen at vi ikke visste alt, men bare måtte prøve å ta de beste valgene. Og sånn må det være her og. Det er vel enda viktigere nå, tror jeg, at man ikke tenker sånn fossefall og liksom skal kalkulere seg langt frem i tid. Men at man sørger for å komme i gang på et spor som går rett vei. Nei, jeg vet ikke, dere har jo sikkert snakket med mange, så dere vet at det finnes mange ulike ønsker og syn på dette. Jeg tenker at det er mye som gjenstår å se. Det er den veien alle går, men det er fortsatt ingen som har gått helt ut. |
| 30 | E | Ja, og så er det jo - Mange går på veldig ulike måter mot samme mål, men med veldig ulike metoder. |
| 31 | I | Ja, og så tror jeg at man ikke kan se bort fra at man - Altså, når det gjaldt det som stort sett var TETRA i Europa, så etablerte det seg en to-tre ulike modeller, der vi snakket om GOGO, GOCO, COGO, ja, litt sånt. Company owned, company operated; government owned, company operated; government owned, government operated. Det blir jo fire ulike modeller |

| | | |
|---|---|---|
| | | hvis du snur på det. Og det er på en måte de modellene du kunne putte det inn i. Det hadde vært veldig fint om vi kunne få det samme i fremtiden. TCCA har blant annet etablert en working group som skal se på - Ja, legal and regulatory working group heter det. En av de tingene de skal se på er om det etter hvert vil bli noen best practices for hvordan man skal gjøre dette. Jeg håper jo at man kommer dit. Sånn at det ikke finnes 10 ulike måte å gjøre det på, men kanskje 3-4, og at vi vet hva som er viktig å tenke på for hver modell. Men det jeg skulle si: Man kommer jo fra en kultur der man har eid disse nettene, så det er det lett å ta med seg videre. Det er nok lett for de organisasjonene som har eid et TETRA-nett å tenke at de skal eie et eller annet i neste generasjon også. |
| 32 | E | Det er interessant at man ser mot en fremtid der man kanskje har blitt enig om en beste måte å gjøre det på, fordi det impliserer jo på en måte, med tanke på at mange ulike land gjør det veldig ulikt i dag, så impliserer det da at mange har endt opp med å velge en ikke-optimal løsning. |
| 33 | I | Ja, det er mange som ikke har valgt enda. Det er mange som er der som oss, at de tenker å velge eller at de ønsker å - For det er en annen ting, nå ser jeg at tiden går ut her, men det er tre ting som driver dette markedet. Det ene er at det er 1% av det totale kommersielle markedet. Det andre er at man har noen krav, som fra utsiden kanskje ser ut som vanlig telekommunikasjon, men som fra innsiden, hvis du står i skredet i Gjerdrum for eksempel, så skal det virke, og du skal ikke være i tvil om det virker, om at du i den gruppen får kommunisert med de du skal kommunisere med. Det tredje er at pengene kommer via offentlige statlige budsjetter, og det tar lang tid. Så det som er i de kommersielle markedene, at det er utvikling og kjøp og utvikling og kjøp, de mekanismene finnes ikke. Og dette er likt i alle land. Så spørsmålet er hvor tålmodige de kommersielle aktørene er. Fordi én ting er at ting blir standardisert og tilgjengelig, men hvis det ikke blir kjøpt, så blir det ikke industrialisert. |
| 34 | E | Nei, det er et godt poeng. |
| 35 | I | Så kjempe - Dette er tema jeg er ganske glad i å prate om, haha! |
| 36 | L | Det er fryktelig spennende. |
| 37 | E | Nei, men det har vært veldig interessant å prate med deg og høre litt om hvordan prosessene har vært. |
| 38 | I | Ja, jeg håper dere har fått noe fornuftig ut av det. |
| 39 | L | Det har vi absolutt. Vi kommer til å transkribere intervjuet utover nå, og så sender vi transkriptet, så du kan se over om alt kan stå der eller ikke. |
| 40 | I | Nei, men jeg tror det er bra. Jeg tror jeg har holdt meg noenlunde innenfor hva jeg kan stå for ihvertfall, hehe. Yes, dere får ha lykke til da! |
| 41 | L | Takk for at du tok deg tiden! |
| 42 | I | Ja, ha det. |
| 43 | E, L | Ha det godt! |

# Appendix O
# Defense Sector

This interview is conducted with a representative of the Norwegian defense sector. While the interview subject is not a member of the Norwegian armed forces per se, they are intimately familiar with the armed forces needs and desires when it comes to mission critical communications systems. Topics range from the way in which the armed forces intend to procure their own broadband communications solution based on commercial networks to considerations regarding autonomous operation of base stations on the edge of the network, as well as more general considerations in regard to the developments of 5G and related technologies. For the sake of clarity it is worth noting that the first half or so of this interview is done with the interview subject presenting the interviewers with a slideshow presentation, and that this interview, in a similar fashion to the interview presented in Appendix I, spans two hours instead of just one.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Da spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Det er greit, bare kjør på med lydopptak. |
| 3 | E | Min oppgave går litt på kjernenettet og hvordan man skal samarbeide med kommersielle aktører om å gjennomføre NGN i samarbeid med dem, mtp. at man ikke skal ha sitt eget dedikerte radionett. Så blir det jo en evaluering av kommersielle aktører der, og så er spørsmålet hvordan man skal gjøre dette i kjernenettet. |
| 4 | I | Vil du at jeg skal komme inn på dette med MCX-tjenester og den typen ting også, eller...? |
| 5 | E | Gjerne det. |
| 6 | L | Du har kanskje lest det, men jeg ser på autonome BS i edge, både i tilfellet der en BS har mistet tilkoblingen til kjernenettet og virker autonomt, og tilfellet der et cluster av BS har gjort det, og alle mulige problemstillinger rundt det, hvordan man skal definere områder, teknisk gjennomførbarhet til en viss grad. Jeg har sett at dere og Vinni-prosjektet har sett på en del på det, så jeg har en del temaer jeg gjerne vil innom her. |
| 7 | I | Kjempeflott, det høres ut som det her kan gå litt ut over en time, men det kan vi ta. Jeg var faktisk nede på Rygge i går, der vi driver og tester akkurat disse tingene for øyeblikket. La meg bare begynne å si litt først at hvis du skal sammenligne Forsvaret og nødetatene. Nødetatene har en arv i dag igjennom TETRA-nettet. Vi har ca. 1000 brukere i dag, i HV spesielt, som har en TETRA-radio som de har med seg i tillegg til sin radio. Så de har mange radioer hvor de skal samhandle. I vårt hode, så må vi få til bedre løsninger når alle skal over på 5G etter hvert. Og så er det også slik i dag at MCX, det er definert i 4G og foreløpig så er det ingen MCX-standardisering på plass i 5G. Husk også på det, at når jeg snakker om 5G-piloter så har det ikke vært mulig å teste MCX-tjenester, for det finnes verken standarder eller utstyr. I MCX-standardene så er det bl.a. definert dette med multicast/broadcast, det er noe som heter QCIer, som er en prioriteringsmekanisme der bl.a. MCPTT har en høyere prioritering enn tale eller data generelt, og du har dette på video og disse tingene som også har sine dedikerte QCIer. Det betyr at du må ha spesialiserte håndsett med dedikerte knapper. Så når jeg trykker på en PTT-knapp så må jeg ha et chipset som faktisk påtrykker den QCIen og sier at nå skal jeg ha QCI 65, og det må være provisjonert i nettet. Dette finnes ikke i dag i 5G. Bare vi er klar over litt hvor Forsvaret står hen nå, vi er i 5G-piloter. Og hvor er nødetater i dag, og hvorfor har de egentlig fokusert på det som egentlig er 4G, og så skal jeg komme litt inn på den biten der. |
| 8 | I | Når jeg i dag f.eks. gjør testing med en vanlig caterpillar-telefon som har en dedikert PTT-knapp, så har den altså ikke QCI 65 og disse her spesielle chipsettene for det, den bruker vanlig internett APN. Så den har en best-effort tjeneste, og den konkurrerer på lik linje med alle andre, Snapchat og Instagram og whatever. Litt av problemet i dag med MCX er at det finnes en veldig smal nisje med produsenter av håndsett. Og bl.a. dette med multicast/broadcast er noe som meg bekjent det bare er en eller to produsenter som har det. Litt tingen jeg frykter her, er at hvis vi er 1% som skal ha veldig spesialiserte ting, så kan vi ende opp med at det bare er en eller to leverandører i verden. Så vi håper på nå at det blir et større økosystem rundt disse tingene. For øyeblikket, sånn som Forsvaret driver, så prøver vi å løse det på andre metoder med 5G. F.eks. for å unngå dette med multicast/broadcast i nettet, så ser vi at det er flere metoder å gjøre det på. F.eks. har vi for 5G beamforming-egenskaper som gjør at vi får ufattelig mye mer kapasitet, vi har edge computing som gjør at vi får low latency, og vi har også slicing-muligheter for å prioritere forskjellige typer trafikk. |

| | | |
|---|---|---|
| | | Så det er andre måter å gjøre det på, vi gjør det på standardhåndsett. |
| 9 | I | Okei, men nå er det dermed sagt at nødetatene IKKE kan gjøre det likt, for de har en arv. De skal ha en gateway mot 4G, og i MCX-standarden så ligger det mye mer enn multicast/broadcast og QCI-et. Det ligger også man-down, barge-in, panic, videooverføring som vi ser i USA, det er ikke ting som vi har hatt fokus på fra Forsvaret sin side. Samhandle skal vi gjøre uansett, jeg skal komme litt inn på det. Litt av utfordringen for Nødnett er at de har i dag faktisk mobiltelefonen sin, og et TETRA-håndsett. I fremtiden så skal de altså legge ned TETRA-nettet på litt lengre sikt, og da kun basere seg på mobilnettene. Det er en utfordring. Forsvaret vil aldri legge alle eggene i en kurv, vi vil alltid ha flere bein å stå på. Vi kaller det for et PACE-konsept. PACE står for Primary, Alternate, Backup and Emergency plan. Det vil si at vi har alltid flere måter å løse oppdraget på. Vi har grønne radioer, og det vil vi også ha i fremtiden, kanskje i et mindre opplag. De er robuste for f.eks. elektronisk krigføring. Satkom er viktig for oss. Når vi er i Afghanistan må vi også operere der vi ikke har mobildekning, og f.eks. fra en fregatt midt ute i Stillehavet så er det satellitt-kommunikasjon som gjelder i hovedsak, og HF-radio, altså militær radio, som vil fungere. Men det vi ser, det er at 5G blir viktigere og viktigere. Det er mange grunner til det, ikke mist at vårt spektrum nå går til den kommersielle industrien. Det kan kanskje høres rart ut, men veldig mye av frekvensspektrumet i verden går nå til den kommersielle industrien. Og det tas faktisk fra forsvarssektoren. Vi har nå mistet mange GHz på satkomsiden og på radiolinjesiden, så vi får faktisk i militære operasjoner ikke lenger utnyttet de kapasitetene som vi hadde før. |
| 10 | I | Så, if you can't beat them, join them. Og det er det vi gjør, vi har faktisk tatt i bruk disse tingene her, og så ser vi heller på prioriteringsmekanismer (i kommersielle nett), hvordan vi kan lage det autonomt og resistent mot elektronisk krigføring. Det er vårt fokus nå. Det vi også ser nå i 5G, er at sky- og datasenterindustrien smelter tett sammen med 5G- og telekomsiden. Alle 5G-kjernene som settes opp nå er såkalt cloud native, at de er basert på Docker-konteinere, Kubernetes og de tingene der. Er dere kjent med de begrepene? |
| 11 | E | Ja. |
| 12 | I | Kjempeflott. Vi vil også alltid ende-til-ende-kryptere våre data. Vi har høygradert krypto som ivaretar det. Det vi ikke får tatt med krypto, selv om vi ruter trafikken via sånne multikanalsrutere over de kommersielle nettene, så har vi fortsatt en del metadata-lekkasje. Hvor opererer vi hen, hvem snakker med hvem og den typen ting. Det er det vi jobber med med slicing. Hvordan vi kan separere den kommersielle trafikken fra forsvarstrafikken. Vi har laget en egen såkalt defense-slice for å separere ut trafikken her. Disse multikanalsruterne jobber vi også med, vi har et produkt som heter Hermod, har en del ingeniører som driver og skriver en smart kode for det her. Vi har mange forskjellige scenarioer vi opererer i, og du kan si i fredstid f.eks. der du har behov for å overføre videokapasitet, selvfølgelig er mobilnett ekstremt viktige. Men i en situasjon der du blir utsatt for elektronisk krigføring og jamming, da kan det hende at det vi kaller for combat-nett-radioen er mer robust overfor støy. |
| 13 | I | Det vi også ser i trusselbildet vårt de siste årene, spesielt etter 2014 og invasjonen av Krim og Donetsk, er at vi har et helt annet trusselbilde i dag enn for en del år siden. Behovet for samhandling i dag i totalforsvaret er større enn noen gang. Det gjelder både global oppvarming, noe vi ser i form av skogbranner og alt mulig, Forsvaret og spesielt HV er veldig tett integrerte. Redningsaksjoner, nå f.eks. i Gjerdrum, brannen i Lærdal, alt mulig du kan tenke deg. Flyktningstrømmer, og vi vil bare se mer og mer av disse tingene. I tillegg, ikke minst, terrorisme og det vi kaller hybrid krigføring. Det er ikke lenger en kinetisk krig. Jeg kan ikke dimensjonere vår kommunikasjonsteknologi utelukkende ved å fokusere kun på atomkrig. Vi er nødt til å være teknologisk relevant, og vi har faktisk ikke vært i krig i Norge |

| | | |
|---|---|---|
| | | siden 1945. Så vi er nødt til å ha noe som fungerer i hverdagen, og ikke minst med tanke på samhandling. Og der kommer 5G inn som denne fellesnevneren på teknologi. Vi nå skal fra TETRA til 5G og vi skal gå fra masse proprietære systemer til 5G for Forsvaret så blir samhandling mye enklere på applikasjonslaget. Og så skal jeg komme tilbake til MCX, for vi ønsker ikke knytte oss for tett opp mot MCX. Vi ser at nødetatene har behov for MCX med for det er snakk om man-down, panic og alle disse greiene, altså TETRA-arven om du vil. Vi kan ikke ende opp i en situasjon der vi skal være avhengige av at vi skal være i den samme mobilkontrakten og at vi kommer på samme tidspunkt inn i den samme mobilkontrakten og sånt. Vi vil ha den fleksibiliteten her. |
| 14 | I | For å ta et eksempel fra i går, det var Norsk Luftambulanse og Røde Kors som var til stede på Gjerdrum, der fikk jeg demonstrert en flott og fin tjeneste der når jeg ringer 113, så kan operatøren på 113 sende ut en SMS-link, en webRTC-link. Når jeg trykker på den, kan operatøren på 113 ta over kameraet mitt og se hva jeg ser der ute. Enormt bra informasjon, og det brukte de ute i Gjerdrum med en 4G-telefon på området. De fløy over området og dette bildet fikk de inn i operasjonssentralen på Gjerdrum. Det som var problemet på Gjerdrum var at de ønsket å videredistribuere denne videostrømmen til alle. De som var med hundeekvipasje, til HV. Det bildet fikk de kun i operasjonssentralen. Vi jobber nå med å løse dette her med forskjellige ting, hvordan vi kan distribuere denne linken til flere. Det vi ser på er bl.a. å sende opp en drone som vi kan fjernstyre med f.eks. UV-kamera som ser varme fra et skred, og så ser vi på forskjellige metoder for enten at alle har en app uavhengig av operatør, uavhengig av MCX-tjenester. At HV, Røde Kors, Sivilforsvaret, politi, hjelpemannskaper har en app som faktisk kan motta denne videostrømmen. Der blir også 5G viktig med tanke på kapasitet. Så dette var igjen et godt eksempel på en tjeneste som er helt uavhengig av MCX. Den kan selvfølgelig bruke MCX data, men vi vil ikke ha det slik at alle, Røde Kors eller Norske Redningshunder eller Forsvaret må være på samme MCX-plattform. |
| 15 | I | Og dere vet i dag at er det slik at MCX blir provisjonert (i HLR/HSS). Hvis [operatør] skal f.eks. ha MCX-tjenester for Nødnett og gitt den til Nødetatene, blir det også provisjonert inn i det som i 4G heter HSS. I 5G heter det vel UDM eller noe sånt. Altså databasene. For da blir det provisjonert inn en såkalt QCI og kanskje nettet ditt må ha multicast/broadcast. Nå kan MCX også fungere over unicast, men vi kan ikke komme i en situasjon der du må være om bord på det samme nettet for å få lov til å samhandle. Dette bildet blir så komplekst. Og vi kan samhandle på et applikasjonslag uavhengig av MCX. Det er viktig for oss. |
| 16 | I | Okei. Nå skal jeg si fire egenskaper, egentlig fem. La meg si fem, men la meg begynne med dette med åpne standarder og interoperabilitet, og ikke minst som jeg sa, at nå skal nødetatene inn i dette her og Forsvaret inn. Samhandling, det er et av de viktigste argumentene. Endelig finner vi en felles arena. Jernbaneverket går fra GSMR til 5G. Forsvaret skal ta i bruk 5G. Nødetatene skal ta i bruk 5G. Man sier 5G fordi de er på 4G i dag, men det blir 5G fram til 2026. Så det med at vi er inne på samme teknologiske plattform er viktig for oss. Og det er i mitt ståsted inn mot NATO ekstremt viktig, for der sliter vi faktisk med at hver nasjon har sine proprietære systemer. I Norge, for eksempel, har vi militære radioer som heter MRR som lages av Kongsberg. Nederland har sin Thales-radio, danskene har sin Harris-radio. Så der er det mange forskjellige dialekter og det er vanskelig å finne fellesnevneren. 5G blir også sett på som en collaboration wayform, en mulighet for å samhandle mye bedre. |
| 17 | I | Så er den nye radioen, og i all hovedsak med 5G NR så er det jo antenneegenskapene vi er interessert i fra vårt ståsted. Det er snakk om 10 til 100 ganger mer kapasitet, selvfølgelig på grunn av mer spektrum, men i all hovedsak på grunn av helt andre antenneegenskaper. I dag på en 4G-sektor-antenne på la oss si 110 grader som er sektoren på den, har du en |

| | | |
|---|---|---|
| | | 2*10MHz-blokk med 2x2 MIMO, så får du 73 Mbit/s eller noe sånt på deling på alle brukere. I samme sektoren på 5G på de antennene vi bruker, så har vi 64*64 beams, og hver beam er på ca. 13 grader. Innenfor den 13-graders-loben, så kan du gjenbruke hele spektrumspakka di. Alle 73 Mbit. Selvfølgelig har du også mye mer spektrum. Og det er interessant. Denne beamformingen er interessant, både for kapasitet, men for vår del også for skjerming. Det er litt utenfor scopet deres, men dette med signatur og dette å være synlig for satellitter og hvor du opererer hen er interessant for oss, denne beamformingen. Er dere kjent med beamforming? |
| 18 | E | Sånn halvveis. |
| 19 | I | Ja, okei. Det går egentlig ut på akkurat som i vann, hvis du har to oscillatorer som lager bølger får du doble bølgetopper en plass og de nuller hverandre ut en annen plass, det er egentlig det du gjør med fasene. Du styrer fasene for å ri på bølgetoppene, om du vil. Innenfor en bølgetopp, som er en lobe, så er det tusenvis av brukere innenfor den ene loben, og som jeg sa kan du gjenbruke hele spektrumspakka, men i tillegg så bruker du andre typer tid og frekvenser for å dele ressursene innenfor den loben. Tidsmultipleksing og frekvensmultipleksing. Det var på radio. Interessant på grunn av kapasitet, men aller mest på grunn av beamforming for vår del. |
| 20 | I | Så har du slicingen, det med å utnytte det jeg kaller den nye delingsøkonomien som 5G er et godt eksempel på og slicing er et godt eksempel på. Med denne ultradyre infrastrukturen som koster mange milliarder, med i Norge etter hvert 20 000 basestasjoner, så kan du lage egne dedikerte nett. Og dette med slicing tror jeg blir litt viktig for dere. For hva er egentlig slicing? Altså, slicing er ikke som vanlig VPN. Det kan være et vanlig VPN som har et lukket univers der. Men slicing kan være noe mye mer. Slicing kan gå helt ut på radiogrensesnittet. Du kan allokere spektrum til forskjellige brukere. |
| 21 | I | Det vi også gjør i vår slice, i vår defense-slice som vi har opprettet så har vi faktisk en egen kopi av kjernen. Så la oss si at det var Ericsson som leverte din 5G SA kjerne i det vi kaller en eMBB-slice som er til vanlige brukere. Så kan du også si at du tar en kopi av den, da er det samme driftspersonale, men du har din egen slice med en hel separasjon for å ha metadataseparasjon. Så du kan ha kontroll på egen metadata i mye større grad. Du kan også i slicen, som kjører i en skyinfrastruktur, gå så langt og si at hos Telenor skal du kjøpe egne blades, fysiske kort, og egne NIC, altså nettverksinterface. Men skal du gå så langt, hele hensikten med skyteknologi er å bedre utnytte ressurser på tvers i et datasenter. Men du kan gå så langt ned at en slice er så mye mer enn faktisk bare virtuell separasjon, du kan også si at du skal kjøpe eget jern, du kan til og med sette serverne i et annet rom, men det er samme servicepersonale som har ansvaret for å drifte begge to, og kanskje det er Ericsson på begge to. Så i vår slice, har vi total separasjon fra internettet, og vi har også ikke signaleringslink imot 900-operatører som de har i den kommersielle verden. Vi stoler kun på nasjonale nett. Det er også viktig for sikkerhet. Så er det selvfølgelig edge computing, som jeg kaller extended cloud. Folk har jo bare tenkt på edge computing som low latency, vi er kanskje mer kanskje mer interessert i edge for muligheten for å kjøre autonomt lengre ut i nettet. |
| 22 | L | Kan jeg stille et spørsmål her? Jeg har sett litt på Vinni sin bruk av autonomi-begrepet. Har du lyst til å forklare kort hva du mener med det? |
| 23 | I | I vårt tilfelle går det ut på at du kan kappe backhaul-forbindelsen inn mot datasenteret. Typisk vil teleoperatørene ha tre kjernelokasjoner. Ute på Rygge har vi en egen edge som kun supporter edge-slicen vår med egen kjerne, men den kjører bare på en 3U-server, altså tre units. Men når vi kapper fiberen og satellittforbindelsen, så kan den kjøre med full 5G- |

| | | |
|---|---|---|
| | | funksjonalitet ut i edgen. Tildeling av IP-adresser, og vi kan kjøre alle mulige tjenester. Vi kjører også en del tjenester rett i 5G-nettet som kalles Application Functions, som jeg kan komme tilbake til også, men det blir på en måte vårt private datasenter i vår defense-slice, og så har vi per i dag tre norske leverandører som har kjørt opp tjenester for oss, vi har en PTT-tjeneste fra Thales, så har vi gunshot detection system, altså skuddeteksjonssystem (fra Triangula) + en tjeneste som heter HERMOD. Så er det slik at sikring av 5G, det er vanvittig komplekst. Vi har bred kompetanse for å bruke det til et militært formål. |
| 24 | I | Vi har inngått et strategisk samarbeid med teleoperatørene på infrastruktursiden og på kjernesiden. Vi har tenkt å kjøpe en defense-slice as-a-service. Vi har ikke tenkt å drive en MVNO, det har vi faktisk fått beskjed om fra forsvarsdepartementet at strategisk samarbeid er veien å gå. Men vi skal kanskje operere private nettverk, og jeg kommer litt tilbake igjen til det. Det er slik at vi skal downsize i forsvarssektoren på driftssiden. Og det er slik at vi er flinke på nisjeting i toppen. Vår kjernevirksomhet er krig, vår kjernevirksomhet er ikke drift av 5G eller drift av datasentre. Det kan andre mye bedre enn oss, de er også nå underlagt den nye sikkerhetsloven, de vil også være sikkerhetsklarert. Når nødetatene snakker om MCX, så er det veldig knyttet inn mot mobilkjernen. Da er det viktig å se for seg at MCX er veldig knyttet mot 3GPP, mot HSS og mot den provisjoneringen med QCI og de tingene der. Vi ser på applikasjonene. Vi kan fortsatt få, det har jeg forresten ikke så mye tro på, for å si det rett ut, multicast/broadcast. Jeg tror at med 5G nå blir det behovet langt, langt mindre. Det blir snakk om i hvert fall ti til hundre ganger kapasiteten, i tillegg har vi ofte adaptive kodek som tilpasser seg miljøet vi opererer i. Når det gjelder QCI og prioriteringsmekanismer, for våre tjenester kan vi oppnå det uavhengig av MCX. Teleoperatørene vil tilby noe som kalles et NEF-grensesnitt og Rx-grensesnitt som gjør det mulig for oss å prioritere opp den trafikken hvis vi måtte ønske det. |
| 25 | I | Så skal det også sies, en forskjell fra oss til andre. Når Forsvaret skal gå i krig, så vil det ikke skje sånn. Vi vil få en warning i lang tid om at noe er på ferde, og det er ingenting i veien for at de applikasjonene våre, hvis vi hadde f.eks. definert og brukt en QCI 7, så kan vi rampe opp prioriteringen på den. Så vi ser for oss mer en dynamisk prioritering ved behov. Vi vil ha grensesnitt mot teleoperatørene som sier at nå brygger det mot krig, disse 1000 enhetene er så viktige for oss at de vil vi sette på høyere prioritering. I motsetning til nødetatene som ikke vet når det blir brann på Ullevål stadion, er det litt annerledes. Så de er veldig fokusert på prioritering, vi er ikke det i fredstid og treningsøyemed. Det er egentlig svært sjelden av vi har behov for prioritering der Forsvaret opererer også i fremtiden. Men latent så ønsker vi å se på de APIene for å få det til for sanntidskritisk kommunikasjon. |
| 26 | I | Så skal jeg si litt om at vi jobbet også iterativt. Staten generelt, og det her er litt generelt, har ofte dummet seg ut for å si det rett ut, med å kravstille 10 000 krav. Og før de er ferdig med kravspeken og KVUen sin, så har verden endret seg. Det er akkurat som når vi begynner med våre helikoptre eller våre fregatter eller hva det er for noe, så har jo verden endret seg før vi er ferdige. Vi må jobbe for en ny tankegang om iterativ utvikling og kall det en DevOps-tankegang. Vi fokuserer veldig mye i vår sektor nå på å få det til. Litt av problemet vårt i staten i dag, er at det ikke er sånn vi er rigget. Vi er rigget til en CapEx-drevet organisasjon. Vi får 10 mrd. til å sette opp en ting, og så er det nesten null kroner i linja for OpEx, altså operational expenses, for å drive kontinuerlig utvikling. Og det er en kjempeutfordring i staten i dag. F.eks. for en del år siden brukte vi milliarder av kroner, Forsvaret brukte det, for å bygge et fibernett. Når vi var ferdige med det prosjektet, prosjektet var lukket igjen, og vi har brukt 10 år på å finansiere det opp med prosjektledere og ressurser og opp i Stortinget og sånt, ekstern kvalitetssikring. Men så plutselig var det en leir som skulle legges ned eller vi hadde en ny lokasjon, og plutselig var det ikke penger i linja til å fikse det. Det viser hvor rigid og låst staten ofte kan være. Det vi prøver nå på våre piloter, det er å tenke annerledes med at vi har ingen kravspec på 5G. Vi jobber tett sammen spredt med akademia, med |

| | | |
|---|---|---|
| | | Sintef, med FFI, med Telenor Research, med NSM, på hva får vi til. Og så skal vi begynne å avtale ting underveis for å få det her til. Selvfølgelig blir det også business etter hvert på en del ting, men jeg ønsker å fortsette med dette innovasjonshjulet langt inn i fremtiden. |
| 27 | I | Jeg skal si litt spesielt om 5G-Vinni og nå Fudge-5G, to søknader jeg har vært med å skrive på, og vi har fått begge to. Telenor Research er inne i fire av dem, men totalt har vi fått 300 millioner kroner av EU-kommisjonen, noen og sytti millioner for Fudge, private nett, og ca. 20 millioner euro på 5G-Vinni. Med oss på laget har vi FFI som er spesielt gode på elektronisk krigføring og radiopropagering, bølgefrekvenser og hvordan ting går i skog og sånt; NSM, som er flinke på sikkerhet og ikke minst skytankegang og skyteknologi, det er de også flinke på. |
| 28 | I | Jeg skal begynne litt med 4G, om det er interessant. Vi begynte med 4G og jobbet iterativt. Vi hadde ingen kravspec, men vi hadde en del behov. Vi hadde behov for å ha kontroll på tale og data, og det vi gjorde med [operatørTelia] var at de bygget et eget SIM-kort til oss med to partisjoner. Så når jeg starter opp det SIM-kortet så velger jeg om jeg skal gå inn i en militær partisjon som tvangsstyrte all trafikk inn til oss, vi var ikke på internett, vi hadde kontroll på taletrafikken vår. Vi fikk ikke telefonsalg fra Nigeria eller Microsoft-support fra Uganda. Vi testet også ut mini-BS som vi kunne tatt med oss til Kabul, hengt på internett faktisk, men du har dobbelt kryptert tunnel, og du bruker ikke WiFi, men du bruker mobilfrekvenser. Så i Kabul satte vi opp disse, det som er litt spesielt er at vi brukte noe som heter access class barring. Jeg vet ikke om dere er kjent med det, men vi la inn spesielle aksessklasser som gjorde at det kun var våre SIM som så denne i Kabul. Den var usynlig for alle andre, altså usynlig ikke på en spektrumanalysator, men telefonen fant den ikke. Det betyr at du trenger ikke noen roamingavtale, du kan ta den med til utlandet, telefonen hektet seg på den og du kommuniserte via en satkom-forbindelse eller via en ISP. Ingen metadata-lekkasje, dataen er kryptert. Det var en vannfast ISP-avtale på fiber. |
| 29 | I | Vi kan og gå litt inn på 5G-piloten vår. Jeg var der nede i går, faktisk, der har det skjedd mye kult. Vi har brukt masse penger på å bygge 5G-infrastruktur på Rygge militærflyplass. Vi har faktisk 890 MHz tilgjengelig spektrum, og det er veldig mye. Norske teleoperatører hadde før 5G ca. 300 MHz på deling. Vi har 90 MHz i C-bånd, altså 3,6 GHz, og 800 på millimeterbånd. Vi er en av de få i Norge som har mm-bånd BS. Dette satte vi opp i fjor, og vi bygget opp en såkalt enterprise edge der nede. Denne edgen kjører altså kun vår defense-slice. Så du kan si at eMBB, de kommersielle, de har dekning. Men vi har altså en egen defense-slice som gjør at vi kan få autonomi på 5G med vår egen kjerne som kjører i edgen, og vi har våre AF, disse militære tjenestene som også blir tilgjengelig på flyplassen. Så selv om de kapper forbindelsen her, så har vi også satellitt-backhaul, i vårt tilfelle fra Thor 7, og så skal vi etter hvert ut og eksperimentere med OneWeb og SpaceX. Vi har bestilt utstyr fra de også. I vinter har vi vært her nede og målt spesielt rekkevidde og kapasitetstester på de forskjellige båndene for å finne ut hvor de er egnet i militær bruk. Vi skal altså se hvor sårbart 5G er. Vi har fått lov til å jamme på dette her, det ikke så ofte en får lov til det. I og med at vi har 890 MHz med spektrum så er vi i en unik posisjon. Det kommer ut en rapport på det her som er ugradert, som dere kan få lest om dere er interessert. |
| 30 | I | Neste pilot, Fudge-5G, fikk vi tilslag på i sommer og vi hadde kickoff før jul. Vi skal bygge opp en Tysse-tilhenger, et autonomt nettverk. Det blir interessant for deg, Lina. Vi bygger det opp på en Tysse-tilhenger. Det er Hærens combat lab på Elverum som bygger det opp. I første omgang nå skal vi ut med en Athonet, 5G SA-kjerne, og vi har en egen edge som skal kjøre massevis av tjenester. Det er et norsk selskap som heter Praetexo som skal bygge edgen for oss. Med de antennene våre skal vi teste noe som heter IAB for å skyte fra Vinni til denne mobile greia (FUDGE). Vi må definere en donorcelle (i VINNI) og en IAB-node (i FUDGE). |

| | | |
|---|---|---|
| 31 | L | Ja, for det gjør at du får tilkobling fra den BSen til resten, ikke sant? |
| 32 | I | Ja. Jeg skal komme litt tilbake til det. Det kommer ikke før til neste år. Release 16 er ferdig i speccen, men det kommer ikke før i Q2 neste år. Så det ligger litt frem i tid, men vi tar høyde for den. Det vi også skal ha ut i neste fase, når vi er ferdige med Athonet, da er det Microsoft som står for tur med et selskap som heter Metaswitch som er kjøpt opp nå, og så tenker vi å prøve ut en israelsk leverandør av Cloud RAN, Open RAN. Da skal vi prøve NATO-båndet, n79, og det er igjen Open RAN. Det som er interessant med Open RAN er at vi plutselig kan kjøre disse tradisjonelle BBU, og CU, DU, den splittingen kan vi kjøre inn som software in en Azure-stack edge. Så vi får mye mindre HW av det, og du kan kjøre det på vanlig HW. Det er litt av det kule her med Open RAN, at du trenger ikke ha Ericsson eller Nokia all the way, du kan faktisk ha bare en som produserer antenner som er flink på det, og så har du SW som du kjører i en vanlig edge. |
| 33 | I | Det som er viktig med denne tilhengeren her, er at vi skal utnytte både public og private networks. Så nede på Rygge vil vi ha dette fastboltede 5G-nettet med enterprise edge. 800MHz mm-bånd og C-bånd. For øyeblikket kjører vi NSA, så vi har et ankerbånd i LTE, men vi kan kjøre parallell SA også. Det kommer nå i løpet av en uke eller to, så skal vi opp med en SA-arkitektur. På Rikshospitalet hvor vi har en annen testlokasjon har vi også testet SA. De kan kjøre i parallell. Så har vi med oss dette private nettet som vi kan kjøre på hjul, og så har vi den med oss rundt omkring. Fullt autonomt, men den kan også fungere i nettverket. Det vi har fokusert på i våre piloter, er det som tradisjonelt i 4G har vært vondt og vanskelig. Elektronisk krigføring, det er liksom sagt at MIMO beamforming gir oss bedre robusthet mot elektronisk krigføring, og ikke minst signaturen som jeg snakket om er interessant. Og så er det dette med SUCI-support, subscription concealed identifier, det med analyse av nettet som var problemet i 4G, det trenger vi ikke for 5G. Og så er det noen forutsetninger her. Vi har testet nå sammen med NSM, vi har bygget en IMSI-catcher og hvis du låser telefonen til 5G SA og du har SUCI-SIM-kort og SUCI-support, så utleverer den aldri IMSI i klartekst. Den vil først sette opp en Diffie Hellman-kryptering, og så sender den dette kryptering. Men det forutsetter altså at du låser telefonen i SA. Men det er interessant for oss, og det er sånn vi kan gjøre i slicing, hvis vi sier at vi skal kun ha 5G SA. Og 5G SA blir jo først mulig når du får det som heter dynamic spectrum sharing, at du kan tilby 5G i alle frekvensbånd i landet. Det vil skje i Telia sitt nett i utgangen av 2023, og Telenor sitt nett i utgangen av 2024. Det er det som er interessant for oss, 5G SA med SUCI-support. Så er det dette med mangelen på autonomi, og muligheten du har i 5G for å få edge-autonomi. Igjen, jeg er ikke fokusert på low latency, men autonomi-biten av det. |
| 34 | I | Vi skal ha en klar separasjon til defense-slicen vår. Som sagt har vi en egen kjerne. Den kan driftes av det samme Telenor eller Telia-folket, vi skal kun ha 5G, vi skal ikke ha legacy, vi har fjernet angrepsvektorer som internett f.eks. og signaleringslinker mot 900-operatører. Vi skal fjerne metadata i form av at vi har en egen kjerne, og vi har også dette med edge-noder tilkoblet vår defense-slice, og f.eks. private nett som vi kan opprette ad hoc. Dette blir vårt økosystem, og jeg tenker typisk Nødnett også i den verdenen der. Hvordan det skillet mellom de to skal foregå, det vet ikke jeg. På min telefon kan jeg veksle mellom to partisjoner. Så kan du si at, ja, vil du ikke ha mer separasjon mellom de to verdenene? Det er jo one size does not fit all. For rene militære modem og sånt, nei. Da er det kun dedikerte SIM-kort og ingen sånn type ting. Men for en politimann kan det tenkes at han ... Det er litt avhengig av hva slags utstyr du bruker. Bruker du den typen utstyr så gidder du ikke bruke den på privatlivet heller. Men det finnes i hvert fall muligheter for å bevege seg mellom de to domenene. |
| 35 | I | Så har jeg prøvd å illustrere litt her også hvordan dette kan se ut i fremtiden. Vi har altså |

| | | |
|---|---|---|
| | | denne isolasjonen i vår defense-slice med egen kjerne. Vi har egen firewall, vi har våre militære skyer. Så litt tilbake til dette med MCX som altså skal kjøre inne i kjernen til teleoperatøren. Vi er veldig på at vi skal kjøre egne tjenester på utsiden og ha kontroll på tjenesteutvikling, og drive med DevOps eller det vi kaller for DevSecOps, basert på cloud native-prinsippet. Vi kan oppnå autonomi med private nett, og også i viktige områder som en flyplass f.eks. ved hjelp av enterprise edge. Vi har vår egen firewall i vår egen slice. Det er også litt viktig. Det er også en mulighet med slicing, det er så mye mer enn bare et VPN eller et APN. Du har masse muligheter her for å kjøre SD-LAN eller 5G-LAN, alt mulig. |
| 36 | I | Så litt om autonomi. Som sagt, vi har på Rygge en egen edge logisk tilknyttet BS. Også er det sånn, Lina, at i dette tilfellet har vi bare et par BS. I teorien kunne vi hatt en edge i Bardufoss som var tilknyttet 1000 BS i Nord-Norge. Så hvis russerne kappet fiberforbindelsen fra Saltfjellet, kunne fortsatt vi i vår defense-slice fungert i landsdelen. Så hvor du setter autonomi hen, det avhenger av hvor operatøren har transmisjon og hvor vi vil ha det hen. Kanskje edgen vår står i Telenor sin lokasjon, eller i vår leir. Litt avhengig av hvor vi kan knytte oss og rute trafikken hen. I vårt tilfelle på Rygge, nå har vi i 5G-Vinni bare Oslo og Kongsberg og Rygge. Så der nede var det nesten bare disse to stasjonene som var fysisk i nærheten av et fiberknutepunkt der vi altså kunne rute trafikken lokalt. Så selv om vi har et fiberbrudd her oppe, og satkom-brudd for så vidt, vi har også satkom-backhaul, så vil den linken gi dekning og tjeneste via den 5G-kjernen som kjører her. Men det kunne gjerne vært 1000 BS. Det er ikke noe i veien for at enterprise edge settes opp i samarbeid med teleoperatøren. Et sykehus kan f.eks. ha egen enterprise edge og være helt autonom. Telia vil nå tilby det som heter EMN, enterprise mobility network, private nett som de setter opp i samarbeid med dem, med Telia sine frekvenser. Så dette kan også nødetatene sette opp i viktige områder for dem. Jeg er nå veldig fokusert på krig. |
| 37 | I | I vårt tilfelle på Rygge så er det jo viktig, for det er noe som ikke vil flytte seg i en krig. Et datasenter, en marinebase eller en flyplass, den er vi nødvendigvis avhengige av også i en krisekrig. Der kan vi altså forsterke dette med en enterprise edge, men noe som settes opp i samarbeid med teleoperatørene. Det er ikke vår eiendom, men en forlengelse av telenettet til teleoperatøren. Den defense-slicen er for så vidt noe de drifter for oss, i dette tilfellet i deres frekvenser. Det kunne selvfølgelig vært våre frekvenser, men det er deres frekvenser. Det er et strategisk samarbeid med dem, der vi forsterker områder som er viktige for oss. Jeg har også tenkt mye og skrevet et paper om det også som er publisert. |
| 38 | I | Jeg tenker også på kommune-Norge, så kunne også dette tenkes at hvem skal ta regningen for denne typen regional edge i fremtiden? Er det teleoperatørene som utelukkende skal gjøre det selv, eller kan det tenkes at det skal reguleres? At regjeringen sier f.eks. at hvert fylke skal ha sin egen edge og den skal bekostes av staten, f.eks. Sånn at du faktisk får regional autonomi. Dette er jo også relevant for Nødnett. Det jeg vet altså, nå er jeg veldig fokusert på krig, men la oss se på en hybridkrig der noen av de første målene som hadde gått, det er å ta ned 5G-nettet og internettet. Det er det første de ville forsøkt på i et angrep mot Norge. |
| 39 | I | La oss si noe så banalt som at Norge er smalt på det smaleste. Hvis noen kapper fiberforbindelsene på Saltfjellet, eller langs E6 og jernbanelinjene der oppe, hvordan skal Nord-Norge fungere hvis kjernene fungerer i Oslo? Det er mulig at det går noe transmisjon via Sverige, men en kunne også tenke seg en modell der staten var med og bekostet regionale edger. Eller at det måtte reguleres at teleoperatørene setter opp egne edger, men jeg tenker at noen må ta den regninga her. Men dette er ting som jeg jobber med, som vi må se i et litt videre perspektiv. Ja, Forsvaret kan gjøre dette her, men bør ikke hele nasjonen og Nødnett og andre tenke disse tankene? Hvordan kan vi f.eks. få regional autonomi i større grad, slik at vi ikke er avhengig av oppetid i Oslo for å si det sånn. |

| | | |
|---|---|---|
| 40 | I | Så var det dette med private nett igjen, og hvordan vi ser på det. Dette private nettet som jeg kalte for Fudge tidligere. Jeg har i dag faktisk fått 50 SIM-kort på vårt nye private nett. Jeg kan ha så mange SIM-profiler jeg vil. Jeg har plass til to fysiske, men jeg kan også ha hundre e-SIM på telefonen min. Mitt hjemmenett kan være mitt private nett på denne tilhengeren. Og der kan jeg tilby masse tjenester. Men hvis jeg beveger meg ut av bobla, da har jeg fortsatt dette nasjonale Telenor, Telia, Ice sitt nasjonale nett og vår forsvarsslice som er tilgjengelig i hele landet. Så fra et telekomperspektiv ønsker vi å utnytte begge deler, og det er både og. Fra et tjenesteperspektiv, og nå kommer dette med skyteknologi inn som er interessant, og disse cloud native-prinsippene. Tradisjonelt er vi vant til at vi produserer tjenester, type Office 365, på sentraliserte datasentre. Med 5G og orkestreringsmuligheter nå, så er det fullstendig mulig å spinne opp tjenester lengre ut i nettet for å skape autonomi. Det vi har gjort nå i våre piloter i 5G-Vinni, det er tre norske firma som spinner opp såkalte AF rett i vår defense-slice på Fornebu og på Rygge. Og selv om i fremtiden kan du også tenke deg at enkelte av disse tjenestene kjøres rett fra teleoperatørene. Igjen snakker dere om MCX, de vil nødvendigvis kjøre det, men jeg er også på disse andre tjenestene jeg snakket om i sta som ikke er knyttet opp mot MCX. Så selv om sentrale datasentre går ned, så har du har fortsatt hele mobilnettet som tjenestene vil fungere i. Og sånn kan du gå utover, til Rygge, og fortsatt fungerer Rygge på denne regionale edgen, og til og med vårt private nett vil fungere hvis all fast infrastruktur er borte. Igjen, jeg er veldig fokusert på krig, men det er sånn vi tenker. Hvordan vi kan få både bedre og mer robuste tjenester hvis vi utnytter disse skyprinsippene på tvers. |
| 41 | I | Nå skal det sies, i dette regnestykket for vår del, så er det ting som graderingsnivå, krigens folkerett og fleksibilitet. Den metoden med å legge ting inn her, og det er kanskje litt kritikk også til Nødnett med MCX-tjenester, hvordan skal du skifte operatør hvis du blir så knyttet til de her? Så vi skal teste ut dette konseptet. Men spørsmålet er da dette med krigens folkerett, Genèvekonvensjonene og graderingsnivå. Er det slik vi ønsker det, og ikke minst med tanke på fleksibilitet. Hvor gift blir du med teleoperatøren hvis du legger det inn sånn? Ja, det er cloud native-applikasjon og Docker-containere og det kan orkestreres, men det er ganske mye håndarbeid i dag fortsatt. Så det blir kanskje denne metoden som blir mer aktuelt, at du har militære skyer, eller Nødnett-skyer for den saks skyld, distribuert rundt i landet, i kombinasjon med private nett, og så bruker vi i vårt tilfelle denne slicen som en sikker og robust måte å knytte sammen disse tjenestene. Ja du kan tenke at du kan tilby tjenesten bare sentralisert, men i kombinasjon med autonome tjenester ute i private greier så får du også den robustheten vi er interessert i. |
| 42 | I | Nå ble sikkert dette litt komplekst. Men poenget mitt er at det Forsvaret har sagt, er at vi tror ikke vi vil legge tjenestene rett i teleoperatørene sitt nett, type MCX som teleoperatørene (DSB tenker å gjøre?) gjør, men de gjør det fordi de kanskje må fordi det er knyttet mot HSS og den typen ting og det er mye gateway-funksjonalitet. Men jeg ville nok foretrukket egentlig at det kanskje var Motorola eller andre som driftet det, slik at det var helt uavhengig av teleoperatør. Nå beveger jeg meg veldig ned i detaljer på releaser og hva som blir mulig i fremtiden på det her med MCX roaming og sånt, men jeg er ikke så fokusert på MCX-tjenester. Jeg vil at vi skal samhandle uavhengig av MCX. Jeg kommer litt tilbake igjen til det også. |
| 43 | I | Jeg skal gi et eksempel på hvordan tjenester blir både bedre og mer robust med skytjenester. Her har vi et norsk firma som kort fortalt, hver soldat eller HV-soldat eller politimann blir en sensor. Tenk dere 17. mai, du har tusen politifolk eller HV som går rundt i byen. De har en app ombord med et gunshot detection system. Appen kjenner igjen at det er et skudd, den sampler 1,5 sek, den gjør om et akustisk signal til et grafisk bilde og tagger det med nøyaktig tid. GNSS-satellittgreier. De laster det opp med 5G-hastigheten, f.eks. til |

| | | |
|---|---|---|
| | | sentralisert sky hvis den forbindelsen er oppe. Den gjør to ting, den korrelerer tid og sted, og returnerer i et kartverk nøyaktig posisjon på skytteren, pipevinkel og avstand. Den bruker også maskinlæringsalgoritmer for å gjenkjenne fra et bibliotek med millionvis av skudd hva slags våpentype det er som skytes. Vi ser også på hvordan vi kan integrere med det vi kaller for et battle managment system, så du kan se f.eks. grønn blink for at det var ditt våpen, rødt blink for fiendtlig våpen etc. Dette er en tjeneste som HV ønsker seg hos oss, og politiet og andre. Dette er igjen en tjeneste som ikke har noe med MCX å gjøre. Det er viktig å skille med MCX og det enorme andre tjenesteutvalget. Det er ingenting i veien for at dette var en HV-soldat og dette var en politimann på 17. mai. Alle kan fungere som sensorer, alle har den samme appen om bord. Vi kan aggregere, vi trenger ikke sende tilbake til kartverket, vi kan til og med sende det til kommandosentralen til Forsvaret, til politiet sitt senter. Så det gir rett og slett bare en sensor ute i her. Jeg nevnte Gjerdrum-scenarioet til dere med denne web-RTC-linken. Helt uavhengig av MCX som lar folk på et skadested som Gjerdrum få sendt ut en link, trykker på den og gir video og du får samme situasjonsforståelse. Så det var et eksempel på hvordan tjenesten blir bedre med sky når vi kan forbedre algoritmene til enhver tid med disse bibliotekene. De har sensorer satt ut nå rundt omkring hele verden som lytter til skudd, og de plukker ut såkalte falske positive. |
| 44 | I | Skal vi se, jeg vet ikke hvor mye jeg skal si her om våre use caser med private nett og IAB. Jeg kan vise litt kjapt. Vi ønsker å ha med oss ut edge i felt og etablere egne private nett med våre frekvenser, gjerne i samarbeid med nødetatene. De har også de samme behovene. Kanskje vi kan bruke IAB til å forlenge til ny, fremskutt kommandopost. Du kan tenke, i et voldsomt område, kanskje politiet holder til her og HV holder til her, eller i vårt tilfelle jobber vi for å ikke bli tatt ut av bomber, rett og slett, vi kan spre oss ut i teigen med smale beamer. Disse lobene kan gå ned på 13 grader. For å knytte oss opp mot, kall det de sentrale skyene våre, som f.eks. var en PTT-tjeneste, så er det greit at vi har en felles plass å provisjonere nye talegrupper på, og så kan de heller provisjoneres ut i backend ute i felten. Her er en ny talegruppe, nå skal disse være ombord på samme talegruppe f.eks. Her kommer også denne slicingen inn i dette nasjonale nettet. Også skal vi også teste med OneWeb og SpaceX hvis vi ikke har dekning en plass. Det kan være en fregatt, eller det kan være i Kabul, for den saks skyld. |
| 45 | I | Så, kjapt, vi jobber med cloud native-prinsipper og skyteknologi, men vi ser stor sammenheng med 5G-infrastruktur og det strategiske samarbeidet. Vi kan robustifisere viktige fysiske plasser som f.eks. en flyplass i form av enterprise edges som settes opp i samarbeid med kommersielle aktører, og vi ser på dette med private 5G-nett ute i felt med forskjellige backhaul-løsninger, evt. også til havs med ship-to-ship, ship-to-shore. Antakeligvis vil vi også se 5G med satellittforbindelse. Jeg har masse use cases på IoT og AR/VR og den typen ting, jeg tror ikke jeg skal si noe om det. Jeg kan nevne at også NATO ser på dette med slicing og end-to-end slicing som en stor mulighet for å lage lukkede nett med den samme sikkerhetspolicyen. La oss si i tilfellet Norge nå, så kan vi si at Norge godkjenner og definerer en NATO-slice i Telia og Telenor sitt nett f.eks. og det samme gjør alle NATO-nasjonene. Da kan vi knytte disse sammen. Det gjør vi nå i Vinni med British Telecom og den 5G-Vinni-installasjonen der borte. Vi setter samme sikkerhetspolicy og definerer QCI 7 med en høyere prioritering på data. Og så skal vi teste med HoloLens, vi skal teste telemedisin, skal gå rundt med 5G-Hololense en plass i London og så skal det være enkelt å overføre med garantert QoS og skjerming av pasientdata til en professor på Rikshospitalet f.eks. som kan fjerndiagnostisere en pasient. Dette var egentlig bare et symbol for oss på hvordan vi kan knytte sammen flere slicer med samme sikkerhetspolicy, med samme QCI og QoS-policy, og også tilby tjenester, hvis du er tilknyttet den slicen f.eks. med en eSIM-profil, så får du tilgang til disse tjenestene, som gunshot detection. Det kan vi gjøre med disse slicene. |
| 46 | I | Ja, that's it! Som jeg sa, jeg kunne fortsatt i dagevis om disse tingene, om radio og |

| | | |
|---|---|---|
| | | Kubernetes og disse tingene i det hele tatt. Jeg tenker dere får fyre litt løs! |
| 47 | L | Ja, takk for den forklaringen der. Det var veldig fint å få litt innblikk i hva dere tenker og hvordan dere tenker. Mye god innsikt. Jeg gleder meg til å prosessere det litt etterpå. |
| 48 | I | Det blir mye data på en gang. Selv om dere er masterstudenter, så har vi andre jobbet med det her i mange år. Vi vet at dette er ganske gresk for veldig mange, egentlig. Så dere er flinke hvis dere klarte å henge med. |
| 49 | L | Jeg kan kanskje ta det til der jeg begynte å bli forvirret. Fordi du snakket om disse regionale edgene som jeg tenker på som en fin måte å skape redundans primært da mot angrep, vil jeg tro, for hvis flere fiberkabler ryker samtidig ... Det skal litt til for at det skjer tilfeldig. Men jeg har også sett på, som du kom inn på, men der jeg falt litt ut, å flytte redundansen helt ut til enkelt-BS og clustere av BS. Vil du snakke litt mer om den løsningen deres overfor det? |
| 50 | I | Ja, vi er jo midt inni ganske ... Nå skal jeg vise. Tok jeg hele skjermen nå? |
| 51 | E | Ja, vi ser presentasjonen. |
| 52 | I | Ok. La oss gå tilbake til de forskjellige formene for edge du har. Denne edgen som også kjører en 5G-kjerne, den er vår eiendom. Det er Forsvarets eiendom. Det er våre frekvenser, det er vårt utstyr som vi har med oss ut, for et områdedekkende behov i skogen f.eks., eller på et skip eller den typen ting. Typisk sammen med Nødnett, så vil dette være en felles ressurs som jeg ser for meg at her kan både teleoperatører, egentlig, Forsvaret og nødetatene samarbeide om denne typen ressurser. Det er helt naturlig. Frekvenser er en sårbar ressurs, det kan godt tenkes og være helt lurt, det er en av de tingene jeg har foreslått, at her bør vi samarbeide med denne typen ting. Det her er helt spesielle scenarioer, det er sånne typer Lærdal-scenarioer, eller Flatanger eller type Gjerdrum-scenarioer. Når det gjelder den faste infrastrukturen som ligger i hele landet, det er den som 99,9% av tiden nødetatene vil bruke, så er det slik at da vil enterprise edge-biten være et samarbeid med teleoperatøren. Teleoperatørene ser også for seg å utvide med regionale edger. Så er jeg litt usikker på hva som er driverne for det. Grunnen til at de skal ut dit kan godt være gaming og low latency, at det blir et konkurransefortrinn. Hvis du blir kunde i Telenor sitt nett, så har du mye kjappere respons på spillet ditt. Så det kan være en driver, det kan være Netflix som vil ut med 8K-video og ha noe edge-kapasitet for å ha topp 1000-lista ute i edge. Det kan være reguleringer, så myndighetene sier at vi skal faktisk ha mer geografisk spredning. Men edgen til teleoperatøren, den er ikke autonom. Det er kun dataplanet, den har ikke signaleringskapasiteten. Så det som er spesielt med vår enterprise edge, er at den har en full 5G-kjerne kjørende der ute. Så for low latency-biten, har du kun dataplanet der ute, men ikke signaleringsplanet. |
| 53 | L | Har du da full synkronisering av all subscriber-informasjon på alle stedene? |
| 54 | I | Ja, vi har det. Så det er en del om Kubernetes som styrer det. Det er vel akkurat som du i dag har, la oss si, 3 kjernelokasjoner. Da vil teleoperatørene når du provisjonerer inn en, ha full synkronisering mellom disse. Sånn kan du også tenke ut mot vår enterprise edge. I normalt tilfelle når linken er oppe, så er du online hele tiden med synkronisering. Brytes du, ja vel, hvis det er en endring i provisjonering så er de selvfølgelig ute av synk, men de synkroniseres så fort den er oppe igjen. |
| 55 | L | For den problemstillingen er ganske key inn i min oppgave når vi ser på enda mer lokal edge igjen. Hvis du ser kun på en by, for eksempel, som har lokal edge. Hvilken subscriber-informasjon skal være der og være synkronisert til enhver tid, og utfordringer du får rundt |

| | | |
|---|---|---|
| | | sikkerheten da, hvis det er i Telenor sitt radionett f.eks.? |
| 56 | I | Ja, det kan du si. I en vanlig edge så finnes ikke den UDMen. Det er ikke slik i utgangspunktet i 3GPP-designede edge-konseptet for low latency. Det er egentlig vi som har dratt frem at vi vil også kjøre frem disse komponentene der ute. Men igjen må du huske på at den edgen vår, den er bare 3U, og den supporter bare 50 000 kunder. Så den er ganske billig, jeg betalte 30 000 euro for å få satt opp den edgen vår der ute. Så det er for oss i viktige strategiske områder, f.eks. Bardufoss eller Haakonsvern, så kan vi typisk si at vår defense-slice ved Saltfjellet eller nord for Saltfjellet, så vil fortsatt hele Nord-Norge sine BSer virke, men det er kun Forsvaret sine brukere som vil ha nytte av det. Det en kan tenke seg, er at f.eks. departementet pålegger teleoperatørene mer regional autonomi med full signaleringsplanfunksjonalitet der ute, altså full autonomi. |
| 57 | L | Det ser jo sånn ut fra den stortingsmeldingen fra forrige uke, at det kan bli krav om det. |
| 58 | I | For å si det sånn, jeg har vært på de som en klegg. Jeg sitter i et forum, sikkerhet og sårbarhet i norske ekomnett, der vi skriver til ministeren hvert år om ting vi vil ta opp på agendaen på disse tingene. Og om det er tilfeldig eller ikke, men i hvert fall blir faktisk veldig mye av det vi tar opp i disse foraene tatt til følge. Så i Sverige, blant annet, har de sett på ISP-trafikk, at der skal de ha regional autonomi. De skal ikke være avhengige av Stockholmsdistriktet for å fungere. Og så er det jo mange måter å få autonomi på. Du kan jo tenke at traseer går gjennom Sverige og Finland og greier, men at vi får satt fokus på det er ekstremt viktig. Så kan du si, hvorfor er dette så viktig for nødetatene? Nei kanskje ikke, men hva er en krig i fremtiden? I mitt hode så er det ikke lenger bare en kinetisk krig, i mitt hode så er det en hybridkrig der noen går til angrep på oss, og da vil de faktisk slå ut hele samfunnet. Det er jo det vi ser i et sett nå. Noen sier jo som så at tredje verdenskrig har startet. Det er tusenvis av angrep hver eneste dag på norsk infrastruktur, og hvis de hadde hatt muligheten så ville de tatt ned mobilnettet. Og det vil de forsøke på, garantert. Så det med å få fokus på regional autonomi er jo typisk viktig for vår del i en sånn type hybridkrig, krise-krig. I hverdagen til nødetatene så er nok ikke det fokuset (krig altså), det er mer vårt fokus. Vi går litt lengre i krisespekteret enn brann på Ullevål og 22. juli. Vi går enda lengre ut der andre nasjoner vil oss vondt, og kanskje har egne spesialsoldater som kapper fibere eller gjennomfører koordinerte cyberangrep for å slå ut landet. |
| 59 | I | Den biten som nødetatene nok vil ha noe behov for, det er mer denne lokale nett som du kan sette opp ad hoc med fleksible backhaul-løsninger. Type satkom, eller kanskje IAB for den saks skyld hvis det blir dugandes. Det blir nok litt begrensninger på rekkevidden på det, men satkom ser ut til å bli en veldig fin mulighet. Så du kan altså helt ut til BS få full autonomi, men husk på at det ikke er for eMBB-slicen, ikke for 3 millioner kunder. I vårt tilfelle er det for våre brukere, la oss si at vi er 50 000 brukere, og nødetatene kanskje tilsvarende. Du kan også tillate roaming, f.eks., men i utgangspunktet snakker vi om langt færre dimensjoneringer. Ikke for 3 millioner kunder, men langt færre for vår slice og vår vertikal. Sånn ser vi på det. Så vi ønsker nok å se på en kombinasjon av robustifisering av viktige områder, f.eks. en flybase, i kombinasjon med taktisk 5G og ha det med ut i felt. Så med både telekom-redundans om du vil, altså autonomi, men også dette tjenesteperspektivet som kommer på toppen av 5G networking, altså disse 5G-komponentene, så har vi også disse tredjepartsapplikasjonene. |
| 60 | L | Jeg har lyst til å gå litt inn i flisespikking på Vinni. Jeg har vært litt inne i dokumentasjonen de siste dagene, og jeg har funnet frem til en modell av hvordan de ser for seg autonom edge med hvordan man skal distribuere nettverksfunksjoner i SBAen i 5G. Og en rent praktisk ting jeg lurer på der, er at det blir mye sensitiv informasjon i UDM, som vi var innom. Vinni-prosjektet virker det som ser for seg å ha en slags cachet løsning for den |

| | | |
|---|---|---|
| | | personinformasjonen for å ikke ha den permanent ute på edge-sitene. Kan det stemme? |
| 61 | I | Nei, husk på at edge-sitene i vårt tilfelle er en leir med bevæpnede vakter. For det er et viktig poeng du snakker om her med nøkler, masternøkler. Kompromitterer du masternøkkelen din så er UDMen din blåst. Det er to mekanismer vi kan se på her. Det ene er en tamper-mekanisme, som litt som et SIM-kort utsletter seg selv hvis den blir kompromittert eller åpnet på noe vis. Det andre er at vi har den i et kontrollert område. Det er en forutsetning for oss, at f.eks. våre leirer skal den stå innenfor gjerdet, bevæpnet og låst ned. Vi har væpnede vakter på Rygge, f.eks., den er godt bemannet og låst ned. Det samme gjelder ute i felten, så er det jo typisk i militære plasser. |
| 62 | E | Hvis du ser for deg at du er politiet, ville du vært skeptisk til å ha denne typen info ute i Telenor sin edge f.eks.? |
| 63 | I | Tenker du på HSS? |
| 64 | E | Ja, du snakker om at du har væpnede vakter og alle mulige sikkerhetsmekanismer. I en kommersiell edge som Nødnett kanskje skal benytte seg av, så vil man kanskje ikke ha de samme sikkerhetsmekanismene. |
| 65 | I | Du kan si at dette er bare ett av flere sikkerhetslag for oss. Det som er farlig for oss, er vel egentlig at vi må provisjonere alle SIM-kortene på nytt, men de får fortsatt ikke tak i våre hemmeligheter. Det er viktig for oss å si. Det er alltid slik at alle applikasjoner har egen type TLS-kryptering. Telekom-biten for oss, autentisering i telenettet, det er bare for å få tilgang til et nett og tilgang til en slice. Men vi har multiple lag av sikkerhet her for autentisering på tjenestenivå, så selv om du får tilgang på den lukkende slicen, så må du fortsatt autentisere inn på tjenesten. I en smarttelefon har du mulighet for what you are, med face-ID og fingerprint, what you have, med Forsvarets ID-kort, det er jo NFC4-støtte i vanlige smarttelefoner i dag (FIDO), og what you know. SIMen er bare en vanlig nettverksdel. Hvis du tenker på SIMen i seg selv, vi ser bort fra det laget i dag. Når vi snakker om sikkerhetshåndtering så er SIMen out of scope. Det er noe som tilhører teleoperatøren, den terminerer kryptoen i nettet, og er for så vidt ikke så interessant for oss. Men når vi får en egen slice, om vi får denne 5G SA-securityen og en egen kjerne, så begynner det plutselig å bli et av de sikkerhetslagene. Det er fordelen. Og så oppnår du høyere graderingsnivå eller tillitsnivå med multiple lag med krypto som terminere på forskjellige plasser. De må ikke terminere i samme utstyr og være samme leverandør. |
| 66 | I | GSMA har noe som heter SIM-safe. De har to kryptolag på sine SIM-kort. SIM-kort er bare for en ting. Det er en godt bevart tamper-mekanisme som aldri er kompromittert. Det vi nå ser på, er kan vi også legge ett ekstra lag med krypto inn på SIM-kortet, slik at du har applikasjonskryptoen din på tjenesten din, så har du SIM-kortet som puttes inn, og den har et lag som er ende til ende. Det kalles SIM applet for secure end-to-end communication. SIM-safe heter det, det er noe dere må se på. Den er interessant. I tillegg har du telekom-nøklene som terminerer i slicen din. Mens den andre nøkkelen på SIMen går helt igjennom. Så da terminerer de på to forskjellige plasser. I tillegg har vi per-app VPN-muligheter fra MDM-en. Så det er ikke slik at selv om noen kompromitterer vår UDM eller masternøkkelen eller nøkkelen, så er på ingen måte hemmelighetene våre blåst. |
| 67 | I | Vi vil ha to til tre lag med kryptering. Applikasjonsnivå, telekomlag osv. Det vi faktisk ser på, er mulighet for en MDM-løsningen, og fjerne alle andre radioer. Sant, vi kan si at vi skal skru av WiFi, Bluetooth og USB. Nå kommer neste versjon til og med kanskje uten USB. Hvis jeg kun lader via den trådløse ladingen og jeg stoler kun på min 5G SA-security, selv om den har en app som er godkjent og selv om jeg skulle ha SW som er full av virus, så får den ikke ringt |

| | | |
|---|---|---|
| | | hjem. Vi er i isolasjon fra internett, vi får ikke ringt hjem til Kina eller Russland. Vi har kontroll på intrusion detection, ID-scanning og disse tingene kjører vi rett i vår slice og vi kjører deep packet på hele greia, alt mulig. Så multiple lag med krypto som terminerer på forskjellige plasser, gjerne fra forskjellige produsenter. Det er det som ligger i margen til forsvarsfolk. Jeg vet ikke om det var svar på det du spør om, egentlig? |
| 68 | E | Det er interessant å høre om disse ekstra sikkerhetsmekanismene og kryptering som man kan ha selv om hele edge siten f.eks. er sårbar. For tanken er jo at det kommer til å være denne typen edge-autonomi i hele landet, liksom, med regionale edge-sentere i større eller mindre grad. Men f.eks. hvis DSB kjører sin egen MVNO og så provisjonerer nett fra f.eks. Telia eller Telenor, så er det et spørsmål om hvem som skal ha ansvar for det som skjer i edge, og hvordan man kan gjøre det sikkert. Spesielt når man skal synkronisere denne subscriber-databasen ut til edgen, hvordan kan man sikre at den informasjonen ikke havner på avveie, selv om det ikke nødvendigvis er DSB som har full kontroll over det som skjer på den edge siten. |
| 69 | I | Ja, altså, i normale tilfeller så er det jo for det første dedikerte fiberlinker. Det er nett som man må ha H-klarert personell, og lokasjonen er hemmelig. Det går via fiber og det er ikke på internett sånn sett, det er et lukket nett. Og det er satt opp kryptering i IPSec og alt mulig på forbindelsene ut til utstyret i BSene. I vårt tilfelle vil vi ha både tamper-sikring, det blir standard, og så blir det fysisk sikring av leiren som det er i dag, eller ute i felt typisk. Men du tenker på med at du skulle miste data underveis, altså MitM type ting. Men det er altså en IPSec-forbindelse som er viktig for oss. Når det gjelder disse private nettene som vi snakket såvidt om, de som er ute i felt her, hvordan vi provisjonerer de. De er flyttbare, så det kan vi gjøre inne i basen og synkronisere opp vårt eget private nett. Så dette private nettet har ingenting med det kablede nettet. Så edgen er typisk Telenor sin edge, de kalles enterprise edge, men det er typisk vår eiendom her ute. Og det blir kanskje 50 000 abonnementer maks med antall abonnenter. Vi har ikke konkludert nøyaktig med dette med om vi skal se på forskjellige metoder på å provisjonere det, annet enn at det er på blokka, og se på den typen kompromittering og eventuelt reprovisjonering. Så er det ikke slik at vi har skrevet en kravspec, det kommer nye ting hele tiden. Nye trusler, og det gjelder å få på plass en arkitektur på dette med isolasjon, det tror jeg er ekstremt viktig at vi lukker oss inn der, og dette med autonomi er jo et grunnprinsipp hos oss. Det vi kaller for et PACE-konsept med å ha multiple bærere blir en viktig ting for oss, og det med ende-til-ende-kryptering, multiple lagre og terminering på forskjellige plasser. |
| 70 | I | Jeg vet ikke om dere har fått svar på det dere lurer på, jeg? |
| 71 | L | Jeg har fått masse ny innsikt i hvert fall. |
| 72 | E | Ja, mye informasjon. |
| 73 | L | Og så er det noen overordnede konsepter som jeg tror blir veldig fine å putte inn i det vi ser på. Og så er det helt tydelig at det er litt forskjell i use caset deres og use caset vi ser på, men det er jo overlapp. |
| 74 | I | Det er forskjeller. Og igjen tilbake til at Nødnett har tatt utgangspunkt i å ta dagens TETRA-funksjonalitet med alle de TETRA-tingene og å komme fra en taleverden, og hatt fokus på å portere det videre i NGN. Vi har ikke hatt fokus på det i det hele tatt, vi har ingen arv. Vi kan tenke helt fritt, og vi tenker på helt andre ting enn tale. Tale er bare, jeg vet ikke om jeg en gang gidder å snakke om tale på en mobil. Det er jo maskinlæring og AI og analytics, det er det som blir viktig for oss. F.eks. spør du meg nå i dag om det er viktig for oss å få en stridsvogn i fremtiden som har talekapasitet, nei. Vi skal ikke ha folk i stridsvogner i |

| | | |
|---|---|---|
| | | fremtiden. Det blir autonomi som blir viktig, og det blir databæreren. Vi skal jo ikke bare slippe den helt bananas fritt utpå der, vi må faktisk også kunne se hva den ser, og det må være en man-in-the-loop for å ta beslutninger. Men der har ikke Nødnett vært i dag. De har selvfølgelig fått et oppdrag, et mandat om hvordan vi skal gå fra dagens TETRA-nett over til nye Nødnett. Der har selvfølgelig TETRA-funksjonalitet vært det primære fokuset. |
| 75 | I | Og det jeg også sier, at det som er viktig for oss, jeg har skrevet ned noen punkter om det også, skal vi se her da. Jeg deler ikke skjerm nå, gjør jeg? Skal vi se. Kort fortalt, vi må samhandle. Samhandling med nødetatene blir viktigere enn noen gang. Vi ser at de skal på MCX, Forsvaret har ikke fokus på MCX. |
| 76 | L | Blir det en utfordring? |
| 77 | I | I mitt hode så må det bli en forutsetning for dem at ... Vi kan ikke si at alle våre soldater og HV, 45 000 stykk, må ha abonnement fra Nødnett for å samhandle. Det blir å gå baklengs inn i fremtiden. Det som blir viktig for den kontrakten med MCX-tilbyderen, den må være agnostisk i forhold til hvilken operatør vi befinner oss i. Jeg tok det eksempelet på gunshot detection og Gjerdrum-scenarioet med web-RTC videostrømmer, helt uavhengig av MCX. Hvis vi ender opp i en sånn låst situasjon ... I dag er de låst med at de har en TETRA-telefon, de har en DMR-mobil og de har en smart mobil. HV har tre radioer, og det er for meg å gå baklengs inn i fremtiden. De skal samhandle i en 5G-verden, men vi må ikke være avhengige av en spesialtelefon og være abonnent hos Telenor (som et eksempel), fordi at for ikke å ødelegge konkurransen i markedet her nå. Det blir ekstremt viktig. Vi skal ha tre aktører, tre mobile aktører i Norge. Det at Nødnett kommer med sin kontrakt, Forsvaret kommer med sin kontrakt på forskjellige tidspunkt med forskjellige behov, det er veldig bra for konkurransen i telemarkedet. Hvis vi alle går sammen, hele staten inn på samme greia, har vi blåst konkurransen i markedet. Da er det kanskje den ene leverandøren som får en enorm konkurransefordel med at de får penger til å robustifisere strøm og transmisjon, mens de andre får ingenting. Vi vil ha en jevn fordeling av disse pengene slik at vi får tre robuste nett. Vi skal bruke, alle nett. Det har vi sagt. Vi kan gjerne ha en primærleverandør, men hvis ikke den er tilgjengelig så skal vi bruke disse sekundærleverandørene. |
| 78 | I | Så vi skal samhandle, og vi ser at vi må samhandle mot MCX-tjenestene, men vi må kunne gjøre det mot en annen operatør også. Det må de sette som krav. Det ligger også i standarden tror jeg fremover, f.eks. dette med multicast broadcast, men det er de ikke avhengig av. De kan gjøre på unicast. Når det gjelder QCIene må vi kunne samhandle uavhengig av QCI 65. Ja vel, vi får ikke samme prioriteringer og kanskje 10ms mer forsinkelse, men det må gå an. Sikkerheten kan vi bare ta uansett med ende-til-ende kryptering og disse tingene. Så vi vil ikke være avhengige av spesielle håndsett og være i samme kontakten, det er kanskje det viktige. Men vi ser at MCX blir viktig for nødetatene, for det er en standard som de har jobbet med i mange år. Der ligger man-down og panic og barge-in, TETRA-tingene som ikke vi har så mye forhold til. Men samhandling blir viktig. Var det forståelig, det? |
| 79 | E | Jeg synes det var veldig forståelig. |
| 80 | I | Når det gjelder de ulike alternativene for å realisere Nødnett i 5G, er dere kjent med den KVUen? Har dere fått sett den? |
| 81 | E | Nei, vi har ikke sett den, men vi er kjent med den. |
| 82 | I | Okei, men det er klart at dagens modell er jo at Motorola drifter ting. I fremtiden har du selvfølgelig for at teleoperatøren, the winner takes it all, og drifter både MCX og 5G- |

| | | |
|---|---|---|
| | | tjenesten. Men du kan også tenke deg at en tredjepart drifter MCX-plattformen. Det som er viktig for oss, er at vi skal kunne samhandle uavhengig av operatør. Det er også viktig for oss å påpeke at MCX er en ting, men det kommer til å være et hav av andre tjenester, som jeg nevnte. Og så vet jeg ikke, når du snakker om MCX så snakker du om MCData. Det kan godt være at de bare kobler disse tjenestene på toppen av MCX-platformen og sier at gunshot detection eller hva det er for noe også bare bruker QCIen der. Prioritering er også dyrt, og derfor er Forsvaret obs på at vi heller ønsker en dynamisk tilnærming og ha en knapp å trykke på i et API som sier at nå blir det krig, nå trykker jeg på knappen, taksameteret går, I don't care. Men å ha den knappen på hele tiden, teleoperatørene er heller ikke interessert i å ødelegge for de kommersielle kundene. |
| 83 | I | Men igjen blir jeg usikker på hvor viktig prioritering blir i fremtiden. Det var viktig i en 4G-verden. Hvis vi snakker om tale, som er en 12 kbit eller 30 kbit/s eller noe sånt, dynamiske kodeker. Det er jo med video at det typisk kan bli et problem. På tale med dynamiske kodeker ... Personlig har jeg litt lite troa på at det blir multicast/broadcast i mobilnettene i Norge. Det er mange grunner til det. Er behovet der i det hele tatt eller klarer vi oss med unicast? I England har de sagt at de skal klare seg med unicast. Jeg har enda ikke hørt om noen mobilnett som har innført multicast/broadcast, det går liksom andre veien. For driveren for multicast/broadcast var jo TV. Det var TV-industrien. Men nå i dag er jo alle bort sett fra lineær TV på streaming. Sånn går det for oss også. Vi er individualister hele gjengen. Vi er ikke vant til å se Dagsrevyen kl. 18 lengre, jeg ser den kl. 21:15 for da passer det for meg, som en unicast-strøm. En personlig strøm til meg. Det blir masse kapasitet og mindre latency. Jeg skjønner jo for dem at de er fokusert på prioritering. Jeg skal ikke si hva som blir viktig eller ikke, jeg ser bare at det blir allokert så mye spektrum, det skjer så mye på antennesiden, så det er uhyre sjelden at det blir sperr. Jeg husker jo enda, dere er ikke så gamle, men i gamle dager var det slik at vi faktisk gikk i sperr på nyttårsaften. Og så begynte vi å dimensjonere til nyttårsaften, og det blir jo dyrt. Men de siste årene kan jeg aldri huske å ha vært i sperr på noe som helst. Og det har vært i virkelige kriser, 17. mai og alt mulig. Så er spørsmålet når vi får 10 til 100 ganger mer kapasitet, blir det egentlig en issue? Jeg skal ikke konkludere med det annet enn å si at mekanismene ligger der, det vil koste penger. Forsvaret er ikke interessert i å betale det her i det daglige, men jeg skulle gjerne hatt en knapp og skrudd det på hvis det blir krig. Og på unicast det samme, jeg tror det blir viktig å lage f.eks. videoapplikasjonen dynamisk, slik at den faktisk hvertfall kan slippe igjennom. |
| 84 | L | Vi har ønsket oss litt å ha en diskusjon på den argumentasjonen her, så det var interessant å få innspill på. Det gir mening, det du sier. |
| 85 | I | Dere kan tenke litt på det. Det er et ganske enkelt regnestykke på dette med spektrumet. Vi har ofte en beregning på det der du ser hvor mye spektrum du har, hvilken avstand du har, hvor mange brukere du har i cella, hvilken båndbredde du har på talekodeken din f.eks. Da kan du lett beregne antall folk i cella på samtidig bruk, når du går i sperr og sånt. I hvert fall i England, som er på 4G og har mye mindre spektrum og en millionby som London, de har gått bort fra det. Nå går vi til 5G, you do the math. Og så skjønner jeg at MCX-standarden og speccen opprinnelig er basert på det, og dette ble skrevet tilbake i 2012, og så har det skjedd så mye. Opprinnelig for noen år siden, hadde teleoperatørene 300 MHz på deling av spektrum, ca. 100 MHz hver. EU-kommisjonen har beregnet at før vi er ferdig med 5G, så er det 65 (56 GHz) GHz med spektrum som er allokert til den spektrum. Allerede nå har vi allokert 1,2 GHz til dette, og bare nede på Rygge bruker vi 890 MHz, altså tre ganger det alle de tre norske operatørene hadde til sammen før. Jeg husker ikke da jeg regnet på dette, men de har ikke mer enn 115-120MHz i dag heller. Nå har de fått 5G-spektrum, da, så da har de 90 MHz på C-båndet tror jeg. Alle tre. Har dere noen flere spørsmål da? |
| 86 | E | Jeg har et lite spørsmål, jeg vet ikke om det vil gi et langt svar eller ikke, men jeg lurer litt på |

| | | |
|---|---|---|
| | | denne lekkasjen av metadata og hvordan slicing beskytter mot det. Slik jeg har forstått det, siden Forsvaret ikke skal ha en egen MVNO fra det du sa, så er det operatøren som skal ha ansvaret for det dedikerte kjernenettet dere kjører sånn jeg forstår det. |
| 87 | I | Det er et flerdelt svar, la meg si det slik. De som får kontrakten av Forsvaret og nødetatene, litt som i FirstNet i USA som AT&T vant, de har en egen government-organisasjon som er autorisert for jobben. Og så må vi skille litt mellom OSS-data og BSS-data. Hvis de nå først begynner med at i vår slice har vi en egen 5G kjerne, men det er fortsatt noen radiokomponenter her. Fortsatt må vi ha et personell som har tilgang til såkalt OSS-data. Vi må ha tillit til teleoperatøren. Poenget mitt i dag er ... Det er også en organisasjonsting dette her. Det er ikke bare en teknologisk reise. Ja, vi kan separere mye av dataen, men vi må ha tillit til teleoperatøren. Og derfor er de nå underlagt sikkerhetsloven, disse tre det er snakk om. Organisatorisk kontroll, organisering av personellet er viktig. Og så kan vi separere noen ting når det gjelder OSS- og BSS-data. OSS-data er operation support system. Et mobilnett vil alltid ha greie på hvor du befinner deg, det kommer du ikke unna. Det er hele fundamentet i hvordan handover og sånt fungerer. I vår slice så kan det godt tenkes at vi ønsker en fast pris og ikke ha BSS-data. Vi vil ikke ha billing-data som flyter rundt. Det vi også har sagt i vår slice, er at vi ikke skal ha roaming. I utgangspunktet skal vi ikke tillate roaming til utlandet. Og hvis du ikke har CPer, content providere, hvilken risiko har egentlig teleoperatøren ved å si at 30 000 kunder i den slicen der, de har ikke roaming til utlandet, de bruker bare eget spektrum og eget nett, og de bruker ikke tilholdstjenester. Det er ganske enkelt å si at dette kan vi gi en fastpris på. Det er ganske mulig at vi kjøper en telekomtjeneste for de neste 8 årene, eller betaler årlig en 2+1+1+1 rammeavtale, og så betaler vi en fastpris på det. Så det var et litt flerdelt svar. BSS-data, bort med det. Organisatorisk autorisering av personell, og slicing for å separere ut og skjerme det fra andre, f.eks. andre kommersielle, der andre har tilgang på kundeservice hos Telia og Telenor f.eks. Men det er en utfordring med metadata. Det vi så i krigen fra Krim og Donetsk var at russerne brukte metadata for å finne ut hvor soldatene var hen, for så å bombe de. De brukte også sosiale media for å hente ut en del ting og spre fake news. Så det er ekstremt viktig å ha kontroll på metadata. Det har vi jo sett helt bort fra i sikkerhet i dag. Kartlegging av det her er ekstremt viktig, men det er ting som ikke har vært sett på så mye i sikkerhetsgodkjenningsprosesser i dag. Så slicing er på en måte en bedring der, og så har vi fortsatt disse kryptomekanismene med multiple lag som jeg snakket om, men slicing gir et ekstra lag med SUCI-support der vi ser på SIMen som en del av sikkerhetskonseptet og godkjenningsprosessen. |
| 88 | L | Du kommer med gode innspill til oss, vi setter skikkelig pris på at du tok deg tiden. Det var en grundig gjennomgang, det var artig. |
| 89 | E | Jeg synes det var interessant for meg som vurderer den løsningen med at DSB skal ha egen MVNO, å høre at Forsvaret har valgt å ikke gjøre det på den måten. |
| 90 | I | Vi sier at de kan dette bedre enn oss. Og bare for å si det også, det som er problemet vårt i staten er at vi ikke klarer å henge med i denne teknologiske utviklingen. Det er for mye red tape, for mye byråkrati. Og så enkle ting som at vi er CapEx-finansiert, vi kan ikke drive DevOps. Finansdepartementet vil det annerledes, regjeringen vil det annerledes, slik at her skal vi kjøpe de tingene som jeg kaller melk og brød, datasenter og 5G, fra de som er mye mer profesjonelle, og som har for eksempel lov om offentlig anskaffelse, for oss som jobber i det offentlige, en enorm hemsko. Hvis jeg skulle ut og drive innovasjon og kjøpe en skrue, så må jeg ut på en Doffin-portal, og så må jeg vente i tre måneder på konkurranse og sånne greier. Det slipper de private. De har et helt annet forhold til det, derfor setter vi ut den biten der, og så skal vi fortsatt drive med kjernevirksomheten som er krig og sånt. Og den typen applikasjoner som er litt mer sære og som kanskje til og med er helnorske på grunn av klimaet vårt eller språket vårt, eller sikkerhetslovene våre, eller datalagringsdirektiver eller |

| | | |
|---|---|---|
| | | den typen ting. |
| 91 | E | Så det som skjer nå er at vi tar det lydopptaket som vi har tatt nå, og så skal vi transkribere det, og da tar vi og anonymiserer litt og prøver å ta vekk det som er hemmelig, men så vil vi gjerne at du ser over at det ikke er noe som har blitt sagt som ikke burde blitt sagt og sånt. Så vi sender det over til deg når det er klart. |
| 92 | I | Hvordan er det dere gjør det, er det en datamaskin som gjør det eller? |
| 93 | E | Nei, vi gjør det manuelt. |
| 94 | I | Stakkars folk. |
| 95 | E | Vi prøvde med noen datagreier, men det fungerte så dårlig at du måtte gå over med kam etterpå uansett. |
| 96 | L | Takk skal du ha, god helg! |
| 97 | I | God helg! |

# Appendix P
# Communications Authority

This interview is conducted with a representative of the Norwegian telecommunications authority (Nkom). The topics of conversation range from considerations regarding the developments of standards related to 5G and mission critical services all the way to considerations regarding the most common causes of outages in modern telecommunications networks, seasoned lightly with some reflections relating to alternative deployment models. As the interview subject is familiar with many details regarding the NGN process that are not yet public knowledge, caution is taken to avoid revealing any information that could impact the state's negotiation position in regard to the procurement of NGN. As such, parts of the transcript from this interview has been redacted in keeping with the wishes of the interview subject. Where an entire paragraph has been redacted, it has been replaced with the indicator [Fjernet]. However, where only parts of a paragraph has been removed, no explicit remarks are made in regard to this.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | ... Lydopptaket, og så spør jeg om det er greit at vi gjør lydopptak. |
| 2 | I | Ja, det er helt i orden. |
| 3 | E | Supert, takk skal du ha. Jeg kan presentere min egen oppgave litt. Det går mest på kjernenettet egentlig. Med tanke på at man ikke skal ha sitt eget dedikerte radionett, men skal samarbeide med kommersielle aktører om radionettet, så er spørsmålet om hvordan man da eventuelt skal gjøre det i kjernenettet. Skal DSB for eksempel være sin egen MVNO, eller skal man kjøpe en full stack fra en av teleoperatørene? Og fokuset er hovedsakelig på 5G, selv om det blir litt lenger frem i tid. |
| 4 | L | Jeg er ute i radionettet og ser på lokal og regional autonomi. At én eller en gruppe av basestasjoner, eller et område, mister tilkoblingen til kjernenettet. Hvordan man skal gjennomføre det i kommersielle radionett i neste generasjons Nødnett, i 5G. |
| 5 | I | Ja, det er spennende. |
| 6 | E | Jeg tenker, vi vil gjerne snakke litt om disse standardene og spesifikasjonene og sånt, for det er jo noe vi sitter med nesen ganske langt nedi for tiden. Men først er jeg litt nysgjerrig på Nkoms rolle i sammenheng med Nødnett. Litt generelt kanskje, siden vi ikke skal diskutere det som står i KVUen, men jeg er både interessert i Nkoms rolle som tilsynsmyndighet for mobiloperatørene, med tanke på at man kanskje blir avhengig av å kunne stole på kommersielle mobiloperatører i en enda større grad enn man gjør i dag, siden de skal involveres i neste generasjons Nødnett, som er det aller mest kritiske vi har av telekommunikasjon, og Nkoms rolle som regulator av mobilmarkedet, med tanke på at noen av modellene kanskje kan komme til å være konkurransevridende. Litt generelt rundt Nkoms rolle. |
| 7 | I | Ja, som du sier så har Nkom ansvaret for det vi kaller ekomsektoren i Norge, altså de som styrer med elektronisk kommunikasjon. Og det er jo et stort spekter etter hvert. Det er alt fra en liten lokal internettleverandør, til de virkelig store aktørene som Telenor. Nkoms formål er å legge til rette for robuste og fremtidsrettede ekomtjenester, med høy kvalitet og til rimelige priser. I det formålet ligger det ganske mye. Det betyr at vi skal følge opp og ivareta alt ifra en konkurransesituasjon, som du nevnte i sted, til sikkerhet og robusthet i ekomnettene. Blant annet i mobilnettene da. Så der har vi et ganske stort område der vi er inne og påvirker. Vi kommer med både regler og utspill på hvordan aktørene skal forholde seg til en del av de områdene som innbefattes der. Og det er ganske store forskjeller på det å drive med konkurranseregulering og det å sitte og beregne hvilke spektrumbånd og frekvenser som skal brukes mellom de ulike aktørene, og gjøre radioplanlegging mellom ulike radiosystemer. Så det er ganske mye Nkom er involvert i der, det er det. Derfor har vi og en del ulike typer folk. Vi har både samfunnsvitere, økonomer, jurister og ingeniører. Vi prøver å sette sammen team som kan løse disse oppgavene på en så god måte som mulig, rett og slett. Hvert eneste år får også Nkom noe som kalles for et tildelingsbrev, som er en slags hjemmelekse fra regjeringen som de vil at vi skal jobbe med det kommende året. I disse tildelingsbrevene står det typisk nevnt en del prosjekter, som for eksempel neste generasjon Nødnett. Så det vil typisk være ett sånt oppdrag som Nkom får. Å jobbe med det og bistå DSB, og passe på at man ivaretar det vi tenker er viktige forhold i ekomsektoren i sånne typer prosjekter som neste generasjons Nødnett. Da vil det med konkurranse være et av de elementene. Og så vil sikkerhet og robusthet og herding av mobilnett og radioaksessnett være andre elementer som vi har ansvar for å følge med på der. |

| | | |
|---|---|---|
| 8 | E | Med tanke på det med sikkerhet. Noen av modellene er jo for eksempel at man skal kjøpe hele leveransen fra en teleoperatør, da en teleoperatør da får ansvar for, og kanskje også innsyn i, hele løsningen. Vi har snakket med Forsvaret blant annet, og de har sagt at de ikke skal være sin egen MVNO, men de innrømmer da at man i stor grad stoler på teleoperatørene. Jeg lurer på, for eksempel det med dynamikken rundt den nye sikkerhetsloven, og hvordan den spiller inn på - Ja, litt sånn sikkerhet med tanke på om det er sikrere for DSB å ha sin egen MVNO, eller er det ett fett? Hvis du skjønner litt hva jeg mener? |
| 9 | I | Ja, når er jeg ikke jurist, så jeg tør ikke si så mye om de vurderingene som blir gjort rundt sånt som sikkerhetsloven. Men det er klart dette prosjektet med neste generasjons Nødnett, det spenner opp en mengde med sånne typer problemstillinger som staten må ta stilling til. Det gjør det. Ett av de er det du var inne på: Er dette noe som er så viktig for staten at vi skal ha full kontroll selv og bare kjøpe radioaksess, eller tenker vi på den andre siden at en eller flere av mobiloperatørene sannsynligvis kan gjøre dette like effektivt, like billig, og like trygt og sikkert som det staten selv kan få til? Så det er noe av det som selvfølgelig må vurderes, og som vi da har vurdert i selve KVU-leveransen vår. |
| 10 | E | I et scenario der man for eksempel går for å involvere de kommersielle mobiloperatørene i enda større grad, vil det være Nkoms rolle som tilsynsmyndighet å skulle følge opp at de sikkerhetskravene og alt sånt som det blir stilt krav til i kontrakten blir overholdt? |
| 11 | I | Ja, jeg antar ihvertfall at Nkom vil være påkoblet i den prosessen. Nkom har allerede den rollen når det gjelder de som tilbyr elektroniske kommunikasjonstjenester, og som da utpekes som å skulle ha særskilte krav på seg i forhold til sikkerhetslov. Så der er vi allerede. Nkom gjør tilsyn, og følger med på hvordan disse aktørene planlegger og driver nettene sine. Og da er det nok ganske naturlig at den rollen der er noe som Nkom må bruke ressurser på i forbindelse med neste generasjons Nødnett. Så det er på en måte ikke noe nytt som dukker opp, sånn sett, det er noe vi allerede holder på med å passe på. Nkom forvalter statlige midler som går med til å robustifisere og gjøre sikkerhetstiltak i de norske ekomnettene. For eksempel for å styrke fysisk sikkerhet ved fjellanlegg, for å etablere redundante transmisjonslinjer til utsatte punkter i ekomnettene, for å øke batteritiden på basestasjoner, eller lignende. Så det må man nok fortsette med, også når man får Nødnett som en kunde oppi de kommersielle løsningene. Det kommer helt klart fortsatt til å være viktig. |
| 12 | E | Er dette det vi hører om som heter forsterket ekom? |
| 13 | I | Ja, det er en del av det, det stemmer. Nkom analyserer da hendelser som skjer i de norske nettene, og ser på hva som ligger til grunn for forskjellige hendelser. Hva som for eksempel gjør at det blir bortfall av tjeneste i kort eller lenger tid. Basert på den kartleggingen bestemmer man at det på ulike lokasjoner kan være behov for styrking av ekomnettene. Det er da særlig mobilnettene som har fått sånne midler de siste årene. De er bindeleddet for, for eksempel, små samfunn på kysten av Nordland som ligger utsatt til for vær og vind, der det gjerne er mobilnettene som er livslinjen de bruker til å kontakte ressurser de måtte ha bruk for. Så det forsterket ekom-programmet er et av de virkemidlene som benyttes der. |
| 14 | L | Jeg så i stortingsmeldingen som kom ut nå nylig at det stod at regjeringen ville kartlegge hvilke muligheter det finnes nå og fremover for å innføre lokal og regional autonomi i mobilnettene. Har du noen kjennskap til bakgrunnen for det, og hva formålet der er? |
| 15 | I | Det kan nok være flere ting. Det ene kan nok være å legge opp til mer regional autonomi for å sitte litt tryggere i det hvis man skulle få store problemer i sentrale kjernenett og transmisjonsnett i Norge. En annen faktor er det med tjenesteproduksjon over 5G, som |

| | | |
|---|---|---|
| | | kanskje særlig vil kreve korte avstander mellom applikasjon og bruker, og server-side. Da skjønner man kanskje at det med lokale datasentre og edge computing, det vil kunne bli viktig for en del brukere. Da kan man kanskje da oppnå to effekter ved å se slike ting sammen. Så det er nok noe av det som Nkom skal kikke litt nærmere på i tiden fremover, og som det da gis litt hint om i den stortingsmeldingen som du refererer til. |
| 16 | L | Jeg forstår veldig bruken for regional autonomi for kommersiell bruk, når du ser på å flytte tjenester ut i edge og alt det som kommer ut av det, men jeg sliter med å forstå kommersiell bruk av lokal autonomi. Kan du si noe om det? |
| 17 | I | [Fjernet] |
| 18 | L | Det er en gullfugl for min oppgave hvis det kommer til å stilles krav om dette i kommersielle nett. |
| 19 | I | [Fjernet] |
| 20 | L | Spennende. Jeg gleder meg til å se den KVUen. |
| 21 | E | Du tenker at den teknologien som blir utviklet for Nødnett sklir litt over i det kommersielle bruksmarkedet også? |
| 22 | I | Ja, vi ser jo allerede eksempler for eksempel fra havbruksindustrien. Der bruker man bildegjenkjenning av den enkelte fisk i en oppdrettsmerd, med høydefinisjonskamera som kjenner igjen den enkelte fisk. Disse dataene behandles i et datasenter, og da vil det typisk være interessant å ha sånne datasentre og prosesseringsmuligheter tett på, ved produksjonsanlegget, for å få de prosessene til å flyte effektivt, og å slippe å flytte veldig store mengder data fra én landsdel til en annen. Så det skjer ting både med kommersiell bakgrunn, som kanskje gjør at lokal autonomi og lokal databehandling blir noe som blir interessant å se på i den tiden som kommer. |
| 23 | E | I forbindelse med neste generasjons Nødnett da, så kommer det til å kreve, som du nevnte, en robustifisering, og kanskje ekstra redundans, spesielt i radionettet, men kanskje også - Eller, det spekuleres også i om det kan være nødvendig å bruke flere kjernenett, og mulighetene for det. Jeg vet at dere fører statistikk på hendelser og feil i mobiloperatørenes nett og sånt, og jeg lurer på om - For det kommer ut en sånn årlig rapport på det? |
| 24 | I | Det stemmer det. Nkom utgir en rapport som heter EkomROS. Den kommer én gang i året, og den ligger på hjemmesiden vår. Det er på en måte en offentlig rapport som viser hendelser som blir meldt inn til Nkom, og som Nkom registrerer. Der ser man på hva de typiske feilkategoriene er i moderne nett, og de største er typisk at det er et brudd på fiber. At det bare finnes én fiberaksess som mater et spesielt område, som så blir gravd over eller tatt av steinras eller noe sånt, og at man da får tjenesteutfall. Så fiberbrudd, og feil ved programvareoppdateringer, og og det at maskinvare feiler, at komponenter går i stykker, det er veldig ofte de store årsakene til at man har utfall på ekomsiden. Og så er dette med strømtilførsel og veldig viktig. Det er en gjensidig avhengighet mellom ekom og strøm. Begge trenger gjerne hverandre for å kunne fungere, og være fit for fight. Så når strømmen forsvinner går det ofte dårlig for ekomnettene. Da er det ofte bare et tidsspørsmål før man begynner å merke konsekvensene av det. |
| 25 | E | Jeg lurer på litt - For det jeg har fått inntrykk av da, er at det meste av feil skjer ute i radionettet. Som du sier, for eksempel fiberbrudd og sånt. Men opplever man også kjernenettutfall, med tanke på softwareoppdateringer og sånt som skjer i kjernenettet? |

| | | |
|---|---|---|
| 26 | I | Ja, man gjør faktisk det. Nå er det vår sikkerhetsavdeling som er opptatt av dette, så jeg kjenner ikke alle detaljer, men jeg vet at det fortsatt er ting som skjer ved at det er menneskelig aktivitet involvert. Kanskje man har litt pølsefingre og trykker feil på en kommando på tastaturet sitt som ikke burde vært eksekvert, og sånne ting, som kan gjøre at nettverksfunksjoner får trøbbel. Da er det spørsmål om hvilke rutiner netteieren, eller den som gjør dette, har for å sikre seg mot at det ikke skal få store konsekvenser når man holder på å jobbe med det. Hvor flinke har man vært til å øve på dette i en type staging-miljø, før man går til produksjonsmiljøet, for eksempel? Hvilke rutiner har man for å rulle tilbake hvis man oppdager at det er en feil i en programvareoppdatering fra leverandøren? Så det har helt klart vært årsaker til tjenesteutfall, og vi må være så realistiske at vi forventer at det skjer også i tiden fremover. Også i 5G vil man få sånne typer feil. Selv om man kanskje vil kunne få mer effektiv støtte fra AI og lignende, så vil det fortsatt være menneskeinitierte ting som vil gjøre at man kan få trøbbel i kjernenettet. |
| 27 | E | Men for Nødnett i kommersielle nett. Hvis man for eksempel har dedikert kjernenettinfrastruktur, går det an å kontraktsfeste strengere rutiner på denne typen oppgraderinger og sånt, som kan gjøre at dette skjer sjeldnere i en eventuell Nødnett-kjerne? |
| 28 | I | Jada, det kan man jo. Så det er sånne ting som staten må tenke gjennom i forprosjektfasen. |
| 29 | E | Sånn jeg har forstått det så er det også krav om at man skal kunne, ved sånne feil som skjer ved software-oppdateringer da, så finnes det krav om at man skal kunne rulle tilbake nettet. Stemmer det? |
| 30 | I | Ja, det vil jo ofte - Hvis man kjøper en tjeneste så vil det være opp til tjenesteleverandøren å beskrive rutiner for hvordan man kan unngå å havne i sånne situasjoner. Så vil kunden som kjøper den tjenesten gjøre en gjennomgang av beskrivelsen, og se om det er bra nok eller ikke. Hvis det ikke er bra nok, så vil man da melde tilbake og si noe sånt som "Ja, vi ser at du tar en del hensyn her, men vi tenker at det kanskje ikke er godt nok. Her ønsker vi at du også skal gjøre sånn og sånn og sånn." Så det med å ha et bra system for å begynne tilbakerulling av programvare, for eksempel hvis man dytter ut oppdateringer til alt av optiske switcher i et transmisjonsnett, da vil det være viktig å sjekke at tjenesteleverandøren har orden i sysakene, og hvilke rutiner de har for å håndtere situasjoner der ting går galt. |
| 31 | E | Ja. Grunnen til at jeg spør er at jeg er litt nysgjerrig på sånn ca. hvor lenge nettet vil være nede hvis man får en sånn type sentral feil som slår ut hele nettet. Jeg vet at det har vært hendelser der det har gått ganske mange timer. |
| 32 | I | Ja, det var et par ganske alvorlige hendelser i både 2011 og 2014, som medførte at veldig mange kunder ble berørte i flere timer om gangen. Det er klart, det er svært uheldig. Og med en sånn type kunde som nødetatene, og brukerne av dagens Nødnett, så vil det kunne være ekstra uheldig om det sammenfaller med andre typer hendelser som skjer. Hvis det for eksempel er ekstremvær eller andre ting. Da er vi jo veldig opptatt av at Nødnett-brukerne og nødetatene fortsatt skal ha et verktøy for å kunne kommunisere. Så det er ingen tvil om at dette stiller enda strengere krav til de norske ekomleverandørene enn det man kanskje ser fra de brukerne de har per i dag. Men vi oppfatter at de er forberedte på dette, og at skjønner alvoret rundt det å ta på seg et ansvar for å håndtere denne brukergruppen. |
| 33 | E | Nå som vi er litt inne på robusthet og sånn. Det er snakk om også å benytte seg av flere av radionettene, for å øke redundansen der. Da får du både dette konkurranseaspektet, og dette med redundansen og robustheten, hvis vi tar det først. En ting jeg har lurt litt på er |

| | | |
|---|---|---|
| | | hvor stor den reelle redundansen er med tanke på at nettene ofte er samlokaliserte på master og sånne typer ting, så hvis du får ett fiberbrudd, så kan det hende at alle de tre nettene faller ut. |
| 34 | I | Ja, det kan helt klart skje det. Det som kanskje er ekstra utfordrende er hvis strømleveransen forsvinner. Da blir det gjerne stopp, også på de samlokaliserte sitene. Hvis det skjer typ programvarefeil i et radioaksessnett, så vil man kunne ha god effekt av å kunne flytte seg til et annet nett, og derfra kanskje kunne nå sin egen kjerne, der viktig tjenesteproduksjon foregår. Så vi har nok tenkt det, med det vi kaller for nasjonal gjesting, at du da er i stand til å bruke mer enn ditt hjemmeradionett, det kan være en smart ting å se på for Nødnett-brukerne. Det tror vi nok. Og så ser vi særlig at dette vil være aktuelt og relevant på steder der det er lite overlappende dekning fra før. Hvis du har god overlappende dekning, så er det ikke så veldig kritisk om én enkelt basestasjon detter ut. Da vil gjerne terminalen connecte til basestasjoner som er i nærheten og som den kan få tak i, selv om radioforholdene ikke er optimale, og da er det god sjanse for at brukeren kan videreføre sine tjenester uten for mye klabb og babb. |
| 35 | E | Men det å frigjøre seg litt fra sånne mer fysiske avhengigheter, er det noe man kan stille krav til for eksempel når man investerer i å robustifisere nettet? |
| 36 | I | Ja, det kan man jo. På dette programmet for forsterket ekom som Nkom forvalter, så er det jo sånn at alle de tre mobilnetteierne inviteres med i de prosjektene. Så alle vil få de samme mulighetene til å sette ut utstyret sitt på disse lokasjonene, og alle vil nytte godt av den utvidede robustheten i form av større batteribanker eller hydrogenaggregater eller hva det måtte være, og alle vil nyte godt av de dublerte fiberfremføringene som det legges opp til. Da vil det jo for staten være ønskelig at alle de tre operatørene får de samme fordelene, når staten går inn med den typen penger, det vil det jo. Så dette programmet ruller og går det. Det har kjørt i flere år allerede, og etter hvert har man kanskje fått lukket de mest kritiske lokasjonene og de kritiske stedene. Så går programmet videre, og man får på en måte robustifisert steg for steg de ulike delene av de norske ekomnettene. Særlig mobilnettene da. Så det tror jeg er positivt, og det kan og kanskje klaffe godt inn når vi vet at dagens Nødnett - Den kontrakten med Motorola, den går jo ut i 2026, og sånn sett er det jo gunstig at det er noen år frem i tid. Da får for eksempel dette programmet tid til å virke, og ha effekt på enda flere lokasjoner frem til den datoen da Nødnett-brukerne skal inn i kommersielle nett. |
| 37 | E | Det er nesten som om forsterket ekom blir et lite forprosjekt til den store utfordringen kommer med Nødnett, kanskje? |
| 38 | I | Det fine med forsterket ekom-programmet er at alle de tre netteierne får muligheten til å være med, og det betyr at kundene til alle de tre netteierne vil oppnå fordeler med dette programmet. Det er ikke sånn at det bare er kundene til Telia, for eksempel, som vil få en tilgjengelighet på 72 timer, mens alle andre bare hadde 10 timer på den lokasjonen. Man passer på at alle brukerne av de tre nettene har en mer identisk type fordel da. |
| 39 | E | Uten å si for mye om hva som står i KVUen da, men er det også på en måte en mentalitet som man tar med seg videre inn i neste generasjons Nødnett-prosjektet? Her kommer vi jo inn på det som går på konkurranse i forbindelse med robustifisering av nett. |
| 40 | I | Ja, hva kan jeg si om det da? Jeg kan ihvertfall kanskje si at det kan være gunstig at Nkom fortsetter med dette arbeidet sitt sånn helt i parallell, helt uavhengig av hva som skjer med dagens Nødnett og overgangen til neste generasjons Nødnett. Uansett om du er brannmann eller om du er hjemmeværende pensjonist, eller hva du er, så skal du vite at det er gjort ting |

| | | |
|---|---|---|
| | | som gjør at din mobilleveranse er så god som vi kan prøve å få til med de midlene som finnes. |
| 41 | E | Hvis vi ser litt til andre land da, så vet jeg for eksempel at i Sverige og i Storbritannia, tror jeg, så har de bestemt at den ekstra dekningen de bygger i forbindelse med sitt neste generasjons Nødnett, også skal kunne benyttes av andre mobiloperatører enn den hovedoperatøren som de har valgt. Det vil jo kanskje være en liten mekanisme for å mitigere de konkurransevridende aspektene ved dette. |
| 42 | I | Ja, det tror jeg nok. Så der må staten på en måte balansere den typen krav, når man går ut og lager konkurransen, opp mot hvor store kostnader det blir for de som ønsker å gi tilbud på dette. Men vi er ganske godt orientert om hva myndighetene i andre land har gjort, så vi ser selvfølgelig godt hen til det, og tar sånne ting inn i vurderingen når vi jobber med vårt prosjekt her i Norge. |
| 43 | E | Ja, for det er ikke sånn at Nkom på en måte kan pålegge mobiloperatørene å skulle tilby disse tjenestene liksom? Det må komme fra egen kommersiell interesse? |
| 44 | I | Jeg tror nok det da blir den beste kvaliteten. Når man selv har en motivasjon, så blir det gjerne et bedre resultat enn om man bruker tvangsmidler ved å si at du skal gjøre det, eller du skal fikse sånn. Så vi tror nok det er bedre om tilbyderne ser at her finnes det kommersielle muligheter, og at de da ønsker gjøre en god jobb og selv ta en del av de kostnadene som er nødvendig. Fordi de da tenker at dette over tid vil være god butikk for dem. |
| 45 | E | Hvis vi tenker litt mer hypotetisk kanskje, fordi det er litt hemmelig sikkert. Hvis man skal benytte seg av alle de tre nettene - For det vi har snakket litt med de andre mobiloperatørene om, er at om man skal benytte seg av alle de tre nettene, så er det for eksempel sånn at man rullerer litt på hvem som skal bygge ut dekning i grisgrendte strøk, på en måte. At man ikke nødvendigvis har tre robuste nett alle steder, men at man har varierende robuste nett rundt omkring, og så kan benytte seg av de nettene som er der. Jeg lurer på om du tenker - De tekniske utfordringene ved å benytte flere nett. Gir det mest mening at man har én hovedleverandør, og så kan bruke den nasjonale roamingen til de andre nettene i tilfelle der den hovedleverandøren ikke er tilgjengelig, eller kan man ha en løsning der man for eksempel har en felles operatørkode for Nødnett, og så bruker alle de tre nettene som sitt hjemmenett. Jeg vet ikke hva du tenker om de tekniske utfordringene rundt det? |
| 46 | I | Hmm, nei, da er det litt tett innpå en del av vurderingene som blir gjort i KVUen. Som det er viktig for oss å ikke være alt for åpne om nå. Før det går ut til konkurransegrunnlag og sånne ting. |
| 47 | E | Hvis jeg kan stille spørsmålet på en litt annen måte da. Tror du det hadde vært fordelaktig om den løsningen man velger på en måte er så standard som mulig, eller så nært det kommersielle som mulig, med tanke på tjenesteutvikling og sånt. At det ikke blir en sånn veldig skreddersydd Nødnett-løsning, hvis du skjønner hva jeg mener? |
| 48 | I | Ja, og svaret på det er ja, sånn som jeg oppfatter det. Det blir viktig å benytte seg av de verktøyene som allerede står på hyllen, og ikke spesialbestille alt for mange verktøy. Det har blitt gjort i andre sammenhenger, og det har vist seg at det fort kan bli et løp som blir ganske dårlig og dyrt etter hvert. Og der man og veldig fort blir låst til en leverandør, for eksempel. Så det å bruke standardiserte løsninger, som finnes i speccene fra 3GPP, det tror jeg personlig er litt av nøkkelen til god kvalitet og suksess. |

| | | |
|---|---|---|
| 49 | E | Med tanke på standardiseringer da. En ting vi hører mye om er at det er forskjeller på standardisering og implementering. Er det Nkoms rolle da - For eksempel i en sånn Nødnett-kontrakt, hadde det vært Nkoms rolle å passe på at leverandøren leverer en løsning som er tilstrekkelig standardisert, for å unngå typ vendor lock-in? |
| 50 | I | Ja, da vil staten være veldig påpasselig med at leveransen bygger på standardiserte løsninger. Det er nettopp for at staten ikke da skal havne i en sånn silo som det er vanskelig å komme ut av. Som innkjøper da, som kunde, så vil man gjerne kunne ha muligheten til å kunne skifte leverandør fra tid til annen. Man tror det er viktig for konkurransen, det holder alle på tå hev, og det skjerper som regel kvaliteten når leverandørene vet at kundene kan finne på å gå til en konkurrent. Hvis leverandøren ikke er flink nok, så risikerer de å miste kunden. Det er et perspektiv som jeg tror blir viktig for staten også. Og der vil Nkom og DSB typisk samarbeide om å definere den typen krav, og også å følge opp den typen krav. Det vil de. Nkom samarbeider mye internasjonalt med land som USA, England, Nederland, Finland, Korea, osv. i internasjonale fora, der vi prøver å snakke med litt samlet stemme. Om det er en politimann i Seoul i Korea, eller om du er politimann på Otta, så vil du sannsynligvis ha bruk for ganske mange av de samme funksjonene for å kommunisere og bruke kommersielle mobilnett som din plattform for å holde kontakten med kollegaer og overordnede. Så da prøver vi å spille inn litt i fellesskap for myndighetene, og ivareta at fornuftige løsninger blir standardiserte. Sånn at mobiloperatørene kan gå til sin leverandør, om det skulle være Nokia eller Ericsson eller hvem det måtte være, og si at de trenger tjenester sånn og sånn og har tenkt å implementere det så tett opp til spesifikasjonene som det er praktisk mulig å få til. Men så vet vi også det, at det alltid vil være litt avstand fra en papirspesifikasjon til en implementasjon. Det skal jo programmeres og kompileres og kodes og alt mulig rart, og dyttes inn i utstyr og databaser og nettverksnoder, og der vil ofte leverandørene måtte ta noen valg. Spesifikasjonene gir ikke nødvendigvis alle detaljene som trengs, men de sier litt om retninger og metoder og funksjonelle meldinger som skal utveksles og APIer og sånt, men man må likevel ta noen valg som produsent. |
| 51 | E | Altså, ref. det med - En ting vi lurer litt på er det med mission critical services og de specsene som finnes for spesifikke mission critical services, i motsetning til mer sånne over-the-top-type tjenester. Med tanke på tjenestetilbydelsen da. Vi snakket med Forsvaret, og de var litt mer interessert i de generelle over-the-top-type tjenestene enn MCPTT for eksempel. |
| 52 | I | Ja, det stemmer nok det. Og det har nok litt å gjøre med at Forsvaret ikke vil basere seg på gruppekommunikasjon levert i kommersielle mobilnett i sine skarpe situasjoner, fordi de har en del andre krav til hva slags informasjon som skal utveksles og sånne ting. De har sine egne radiosambandsløsninger som de bruker i det de kaller for stridsnære situasjoner. De øver på det, men det er jo ikke så ofte de er i krig. Mens en politimann og en brannmann og en ambulansearbeider, de er på en måte i krig hver eneste dag. Og de vet at de skal benytte kommersielle mobilnett. Det er det verktøyet de har å støtte seg på. Og da blir det veldig viktig at man velger en tjenestefunksjonalitetspakke som på en måte har et rikt spekter av muligheter, som er standardisert, som blir videreutviklet, som har mange brukere sånn at kostnadene holdes nede, etc. Det er sånne vurderinger som blir gjort. Og i den sammenheng er det ingen andre teknologiske løsninger som kan levere dette utenom mission critical services per nå. Det er vanskelig å si hva som kommer etter hvert, men per nå, og gitt det tidsperspektivet som staten Norge har for utgangen av dagens Nødnett og overgangen til et annet et, så er det ihvertfall etter mitt syn ingenting annet enn MCX som vil være relevant. Det har også å gjøre med at de viktigste nabolandene til Norge gjør det samme valget. De går også til en sånn MCX-plattform-virkelighet. Det gjøres i litt ulikt tempo, og Finland og Sverige har litt ulik strategi for å komme dit, men både Finland og Sverige og Norge vil ende opp med MCX når man ser noen år frem i tid, det er jeg ganske trygg på. |

| | | |
|---|---|---|
| 53 | L | Det er interessant å høre. |
| 54 | E | Jeg ser vi begynner å få litt dårlig tid, men apropos det med internasjonalt samarbeid, spesielt med Sverige og Finland. Tenker du at ulike valg av strategier for gjennomførelsen av neste generasjons Nødnett kan ha en innvirkning på det internasjonale samarbeidet? |
| 55 | I | Det er nok DSB som kan svare best på akkurat det tror jeg, men vi må ihvertfall være så realistiske og si at disse tre landene ikke vil ha MCX tilgjengelig på den samme datoen på det samme klokkeslettet. Noen vil være på typ TETRA-teknologi, mens andre har flyttet seg over til 3GPP-type teknologi. Så det betyr ihvertfall at man må få til en del sånne overgangsfunksjoner som gjør at man fortsatt kan samhandle på tvers av de tre landegrensene. Så etter hvert må man nok se en del på sånne typ interworking functions, som også allerede er definerte mellom for eksempel 3GPP og TETRA-teknologien. Det blir viktig for disse tre landene å videreføre det gode samarbeidet de allerede har, og å tenke ut hvordan man på en smart måte kan bygge videre på det. |
| 56 | E | Men når man da er over på 3GPP-spesifiserte tjenester, så burde det ikke ha noe å si om man har valgt en ulik deployment model i Norge og i Sverige, for eksempel? |
| 57 | I | Det skal ikke ha noe å si for samhandlingsfunksjonen. Da må man bare passe på at man stiller krav til leverandøren om at de skal støtte standardiserte løsninger, og hvis de gjør det, så bør det være rimelig god mulighet for å få dette til på en bra måte. |
| 58 | E | Ja, en av de tingene vi også har lurt litt på er det med MBMS, og eventuelt behovet for det for å få til en sånn MCPTT-løsning. Om på en måte kapasiteten i 5G blir så stor at man ikke trenger broadcast for å gjennomføre MCPTT. Jeg vet ikke om du har noen tanker om det? |
| 59 | I | [Fjernet] |
| 60 | L | Jeg synes du forklarer på en veldig fin og oversiktlig måte. |
| 61 | I | Ja, så bra. |
| 62 | E | Jeg tror vi snart har gått gjennom alt. Det eneste jeg var litt sånn - For jeg går jo ut ifra, med tanke på det man ser i andre land, at hovedfokuset nå er på LTE når man skal over på neste generasjons Nødnett. Med tanke på da modenheten av 5G-teknologi. Og det jeg har skjønt er at de behovene man har i stor grad kan bli dekket av LTE, ihvertfall sånn det ser ut i dag, og at man heller da er interessert i en litt mer moden teknologi for å kjøre neste generasjons Nødnett på, ihvertfall i starten. Men jeg lurer litt på: Modenheten av 5G-teknologi og modenheten av norske teleoperatørers evne til å drifte denne teknologien. Når man da eventuelt skal over på 5G-teknologi er det Nkom som liksom skal sitte å se på om operatørene er gode nok til at vi kan flytte NGN over dit? |
| 63 | I | Det er nok ikke Nkom som skal gi tommel opp eller ned på akkurat det tror jeg. Det må nok mobiloperatørene selv gjøre en vurdering på. Men det kan godt hende at DSB eller staten vil være litt interessert i de vurderingene som eventuelt blir gjort på det tidspunktet man tenker seg å flytte tjenesteproduksjonen fra 4G til 5G-core. Da er det naturlig at staten som kunde spør litt rundt det. Litt av grunnen til at vi følger en del med på standardiseringen, er sånn at vi vet hvor langt nødnettfunksjonaliteten har kommet med tanke på å skulle benyttes i et rent 5G-core, i forhold til det som er utviklet for 4G. Da vil det være viktig for oss som kunde å kjenne til det. Å vite hvor langt man har kommet, hva det er som gjenstår, hvor det er uenighet mellom produsenter, hvor det er uenighet mellom mobiloperatører, og |

| | | |
|---|---|---|
| | | å holde seg litt oppdatert på disse tingene. |
| 64 | E | Jeg har skjønt at man ofte ser en liten økning i hyppigheten av hendelser når man skal over til en ny G. |
| 65 | I | Ja, det er gjerne nye funksjoner og ny teknologi og kanskje nye management-muligheter som mobiloperatøren må sette seg inn i. Og etter hvert som man får erfaring med å drifte et mobilnett, å drifte en teknologi, så klarer man gjerne å pusse vekk en del sånne skarpe kanter som gjør at det kan hikke og bli brudd. Så det er alltid spennende å gå til ny teknologi i mobilnettene. Det er litt det samme som man ser i samferdsel. De første elbilene var gjerne litt begrenset i muligheter, og det kunne skje en del feil der de ble stående langs veiene og laderne virket ikke og litt sånne ting. Så går tiden litt, og man finner litt ut av det. Man blir kjent med teknologien, man gjør seg erfaringer, man ser at produsentene blir flinkere og kommer med nye software releaser som fjerner feil og usikkerhet, og så går det seg gjerne til med tiden. Det er nok mye av det samme man vil se i transisjonen fra 4G til 5G, det er det nok. |
| 66 | E | Mm, det har vært veldig interessant å prate med deg! |
| 67 | I | Så bra! Jeg hadde ikke forberedt meg kjempemye, så det blir litt sånn på sparket det jeg sier nå, men jeg håper at dere fikk et lite innblikk i hva vi i Nkom holder på med, og litt hva som er vår rolle inn i dette prosjektet. |
| 68 | E | Jeg synes det var veldig informativt. Da skal vi transkribere dette og få sendt det over. |
| 69 | L | Da får du muligheten til å se gjennom det transkriptet, og passe på at alt det som står der er greit. |
| 70 | E | Så hvis du har sagt noe som burde vært holdt hemmelig får du heller trekke det tilbake. |
| 71 | I | Haha, ja, jeg får gjøre det. |
| 72 | L | Nei, men tusen takk for at du tok deg tiden, det har vært hyggelig. Tusen takk! |
| 73 | I | Helt i orden, ha det så lenge! |

Appendix Q

# Infrastructure Equipment Provider

This interview is conducted with a representative of a major telecom infrastructure equipment provider. Topics of conversation range from considerations in regard to alternative deployment models for NGN and their technological feasibility, with perhaps a particular interest taken in a MOCN based model, all the way to detailed considerations regarding autonomous operation of base stations on the edge of the network.

| ID | Speaker | Content |
|---|---|---|
| 1 | E | Sånn, da er lydopptaket på, og så spør jeg deg om det er greit at vi gjør lydopptak. |
| 2 | I | Ja, det er greit. |
| 3 | E | Supert, takk skal du ha. Jeg kan begynne å si litt om min egen oppgave. Det går mer på kjernenettet egentlig, og litt på hvordan man skal samarbeide med de kommersielle aktørene om å gjennomføre det, med tanke på at man ikke skal ha sitt eget dedikerte radionett. Så det er litt ulike deployment models for å gjøre det i NGN. |
| 4 | L | Jess, min oppgave har du hørt litt om allerede. Jeg ser på hvordan man kan få en BS til å være autonom for Nødnett i 5G, og en gruppe av BS. Enten med IOPS eller med edgefunksjonalitet og den typen ting. Jeg har masse spørsmål i hodet rundt hvordan det skal være gjennomførbart, så jeg håper du kan sparre litt med oss der. |
| 5 | I | Ja, jeg skal gjøre mitt beste. Det er en stund siden jeg jobbet med det, det er et par år siden jeg var inne på temaet. Men det har ikke skjedd veldig mye på de to årene heller, så jeg skal prøve å grave opp det jeg husker. [Introduksjon]. |
| 6 | L | Så hva er det du jobber med nå? |
| 7 | I | Nå jobber jeg med radioteknologi. Det er faktisk 2G, 3G, lite 3G, 4G og mest 5G. [Introduksjon]. |
| 8 | L | Stilig. Så da kjenner du litt til denne IOPS-standarden? |
| 9 | I | Littegrann. Sist jeg jobbet med dette så var jo ikke dette standardisert, hva som skulle skje når du mistet forbindelsen mellom kjernenettet og edge. En utfordring har vært dette med autentiseringsnøkler og kryptering. For det er jo en viss fare for at noen kan knabbe et helt kjernenett. De er jo så små og kompakte, vi har nok løsninger i en ryggsekk. Og da vil du jo helst at alt dette slettes. |
| 10 | L | Ja, nemlig. Og da har dere jobbet med en slags tampermekanisme der? |
| 11 | I | Ja. Vi har gjort det sånn at vi konfigurerer forskjellige løsninger. Enten at du sletter alt, eller at du har et lite subsett av nøkler kun, slik at du klarer ikke å komme tilbake til hele settet av nøkler. |
| 12 | L | Nemlig. Men tenker du på da i en enkelt BS av gangen, at disse er... |
| 13 | I | Ikke i selve BSen, men du har BSen, den lager vi som standalone. Vi attacher en liten core, en kompakt core-modul som har dette i seg. |
| 14 | L | Ja, på hver enkelt site? Ikke for flere? |
| 15 | I | På en enkelt site eller på en gruppe av siter. Typisk hvis du har denne løsningen med at du f.eks. har en ryggsekk der du har dette med deg, og så hopper du ut fra et helikopter og etablerer noen siter eller en site. Ofte holder det med en site, du trenger ikke å ha så veldig mye effekt for å ta et område der det har skjedd en katastrofe. Hvis du ser på sånn som Lærdal, der klarer du deg fint med en site med noen få watt. |
| 16 | L | Ja, ikke sant. Du snakket om et subsett med nøkler, hvordan velger dere hva som skal inngå i |

| | | |
|---|---|---|
| | | det subsettet da? |
| 17 | I | Nei, det gjør nok ikke vi. Det må operatørene gjøre. De må si at vi skal ha 50 nøkler, så produserer vi 50 nøkler og så har du de liggende i dette systemet, og hvis det skjer noe kan du da bruke de igjen. |
| 18 | L | Blir det da til 50 forskjellige brukere da? |
| 19 | I | Til 50 brukere ja. |
| 20 | L | Så da må du ha predefinert et sett med brukere som skal kunne operere innenfor det området? |
| 21 | I | Ja, du tillater 50 brukere for eksempel. Du har kunnskap om hvilke SIM-kort dette gjelder, og så er det forhåndsdefinert at disse 50 SIM-kortene kan få nøkler og koble seg på. |
| 22 | E | Da er dette et helt eget nett der de bare kan ringe til hverandre, eller? |
| 23 | I | Ja. Hvis du mister forbindelsen, så lenge du har forbindelse mot kjernenettet så bruker du jo den. Men du bruker de i det tilfellet der du mister forbindelse mot kjernenettet dit. Da kan de kun snakke med hverandre. |
| 24 | L | Så med tale da? |
| 25 | I | Ja. Tale, og pakke også. Det er helt avhengig av den distribuerte coren, det med hvilke tjenester du har med det. F.eks. hvis du ser på TETRA, så er PTT en HW-løsning i hele TETRA-systemet. Men 4G og 5G vil gjøre det på samme måten, der er det på en måte som en app OTT på systemet. Du forhåndsdefinerer noen QCIer, det heter jo 5GQCI i 5G, men det er akkurat det samme i 4G og 5G. For de sikrer deg prioritet i radionettet og i aksessen. Men selve PTT-funksjonalitet og å koble det sammen i grupper, det gjør du i SW i kjernenettet ditt som en app, rett og slett. |
| 26 | L | Så du ser for deg at det her er noe som ... Fordi, i min oppgave så ser jeg på hele skalaen fra at du har en enkelt BS som har blitt frakoblet, og så ser jeg egentlig for meg hele spekteret til at du har en hel kommune eller et fylke som har blitt frakoblet. Ser du da for deg at det er snakk om å predefinere grupper for alle mulige scenarioer? |
| 27 | I | Nja. Jeg ville heller sagt at, for det er og lettere her. Det er fryktelig komplekst i TETRA, for der har du definert gruppene i terminalen og du må lage såkalte fleetmaps eller hva det heter, der du har gruppene definert. Du trenger ikke gjøre det her, her kan du predefinere grupper, men du gjør det mye enklere. Og du kan gjøre det on the fly hvis en person har tilgang til det kjernenettet. Så setter du opp det som vi i gamle dager kalte et gruppekallsregister. Altså et register over hvem som har lov til å snakke med hvem. Og ofte lager du dette hierarkisk, at du har flere grupper. At du har flere grupper, at du kan snakke på tvers av grupper fra et visst nivå, eller at et nivå har lov til å sette en gruppe, at en gruppe får lov til å snakke med en annen gruppe for eksempel. Også må du også definere disse gruppene, kanskje fra gang til gang. |
| 28 | I | Hvis du tar politiet, for eksempel, har de et hierarki over hvem som er leder og hvem som har forskjellige funksjoner. Men på et skadested så trenger det ikke være lederen som har kommandoen. Det kan være en helt annen person i politiet med mye lavere grad som er skadestedsleder, og da må vedkommende også ha kontroll og kommando for det teamet som er ute. For disse har jo mye mer ... Hvis du ser jo har de ofte ledelse og ofte |

| | | |
|---|---|---|
| | | administrativ leder også, sånn at de kanskje ikke er operative ledere på samme måte. Derfor definerer du at nå er jeg skadestedsleder og tar den rollen, og da er det jeg som har kommando eller kontroll over hvem som får lov til å snakke når og hvem som skal få lov til å snakke med hverandre. Men det kan du definere opp. Du kan definere det som en funksjon, skadestedsleder, og da sette en av brukerne sitt SIM-kort til å være skadestedsleder f.eks. |
| 29 | L | Mhm. Men det gjøres da tradisjonelt mot en sentralisert MCX-tjeneste? |
| 30 | I | Ja, du gjør det faktisk, enten setter du det i HSSen eller i det appen som kjører det. I TETRA setter du faktisk dette i terminalen din. |
| 31 | L | Ja, nemlig. |
| 32 | I | Men her så har du en service som kjører på en server som du har i kjernenettet ditt. Men det kjernenettet her, det er jo ofte ikke særlig større enn en BS. Det kan være en liten server som kjører. |
| 33 | L | Så hvis vi ser på dette her med at områder kan bli isolerte, om det er et lite område eller et stort område. Synkronisering av det her og hvor tjenesten skal være distribuert ... Det er en utfordring. |
| 34 | I | Det er en utfordring, absolutt. Eller si at du mister forbindelsen, så har du flere muligheter. Det ene er at det som er tilkoblet, det fortsetter. De har fått autentisering og alt og kan kommunisere, men ingen nye kommer på. Eller du definerer at de og de SIM-kortene får lov til å komme ombord, og da er det forhåndsdefinert. Da er det også greit. Problemet er jo i det tilfellet at det kommer nye brukere som ikke er forhåndsdefinert. Da må de enten få et SIM-kort som er forhåndsdefinert, eller de kommer ikke på, eller de må samarbeide, rett og slett, med en annen som har en gyldig terminal. Men hvis du da har med et kjernenett, så kan du jo logge deg på det og legge inn nye SIM-kort. |
| 35 | L | Mhm. Så hvis vi ser for oss at det blir liksom et stort skadested, en stor hendelse innenfor et isolert område, så går det å ta med seg transportabel infrastruktur sammen med styrker for å gjøre det mulig? |
| 36 | I | Jaja. Typisk vil du ta med deg et lite kjernenett som også inneholder HSSen. Ofte når du holder på å administrere f.eks. SIM-kort, så lager du noen såkalte templater, alle parametere forhåndsdefinerte, kanskje utenom IMSI-nummeret. Så bare legger du inn IMSI-nummeret og så er du på nett, og så får du dine rettigheter enten ved å ha de definert rett i HSS-profilen, eller at de blir mappet i den som setter opp gruppekallet og gruppekallsrettighet. Det kan du gjøre f.eks. ved å ha en PC som du kobler rett på dette nettet og setter det opp. Men da må du ha en som er autorisert til å modifisere den HSSen. |
| 37 | I | Så har vi også ... Jeg tror ikke det er noe særlig behov for det, men du kan tenke det at du gjør endringer som skal tilbakesynkroniseres når du får forbindelse med kjernenettet igjen. Men det kan også være utfordrende prosessmessig, fordi ting skjer veldig fort i sånne situasjoner, og da er det kanskje like greit å ta den jobben på ny i ettertid, etter det har vært en eller annen katastrofe. |
| 38 | L | Ja, så en måte å se på det er å i normal operasjon ha forhåndsprogrammert inn de brukerne som vanligvis er i et område, og så hvis det skjer noe ekstraordinært flytte inn ressurser med autorisasjon og med mulighet til å konfigurere kjernenettet der ute. |
| 39 | I | Ja, ofte vil du ha en såkalt superbruker som kan gjøre det. |

| | | |
|---|---|---|
| 40 | L | Hm. Det var en nyttig tanke. |
| 41 | I | Du har egne superbrukere som er i det sentrale kjernenettet. |
| 42 | I | Og du har også en annen ... Alternativet er jo ha med en liten satellitt-terminal.<br>ToP/PTP eller IEE1588v2 fungerer over satellitt, videre vil en jo alltid kunne ta ned GPS eller GLONAS for synkronisering. |
| 43 | L | Jeg har lest litt om.. Det er mye hype i 5G om lavbanesatellitter og høytflygende fly som leverer dekning og sånne ting. |
| 44 | I | Vi har levert BS til Google Loon-prosjektet med luftskip. Jeg tror faktisk Google kommer til å legge ned det prosjektet. |
| 45 | L | Tenk deg det å fly inn en sånn en i stormen i Norge ... Hehe. |
| 46 | I | Nei, men satellitter er greit. Du kan ta med GPS for synk. Så lenge du ikke kjører TDD så trenger du ikke så veldig nøyaktig synk på radio. |
| 47 | E | Da er tanken at disse predefinerte settene med brukere og sånt kan snakke sammen i et lokalt nett, at det er en ganske statisk masse? |
| 48 | I | Det trenger ikke være det, fordi du kan gå inn og redigere på disse gruppene dine. Du kan ha to brukergrensesnitt. Enten har du at en sitter med PC og går inn og redigerer i dette oppsettet, eller at en supervisor gjør det fra telefonen sin. Nå er det ikke så lett å lage et bra brukergrensesnitt for å redigere rett i ... Stresset vil nok gjerne at du i alle fall har en lignende tablet. |
| 49 | L | Ja, det er jo mange av nødetatene, eller i alle fall brann og politi, som tar med seg et lite lokalt kontrollrom ut. |
| 50 | I | Ja, det gjør de. Og da kan du konfigurere og si at de og de gruppene ... Sånn som TETRA, som ofte er referanse, så har du en knapp på toppen av terminalen som du vrir rundt, og så har du definert 12 eller 24 talegrupper du kan koble det inn på. Men i praksis går ofte politiet med to terminaler. Du har sikkert sett det når de intervjuer dem på TV, at de har en på hver side. Så det er en på hver sin talegruppe. |
| 51 | L | Så hvis vi ser for oss at ... Det blir litt forskjell fra Nødnett som det er i dag til 5G-løsningen. I Nødnett kan en og en BS gå ned og virke autonomt, men i 5G så ser vi jo for oss at hvis du plutselig har et område som mister dekning, litt uavhengig av hva slags infrastruktur som er der, så kan det gjerne fungere som et litt større autonomt område. Hvis det da går f.eks. på tvers av kommunegrenser, så du ikke har samme brukere definert der som der, vil du snakke litt om hvordan det kan gjennomføres? |
| 52 | I | Ja, disse må jo ha et kjernenett for å snakke sammen. Og da må du definere ... Det blir ofte behov for å definere på tvers av kommuner. Brannvesen er ofte kommunale eller interkommunale, og politiet er jo enda større grupper. De må jo kunne snakke med disse over talegruppene. Da må du konfigurere det i det lokale nettet når ting skjer, eller at du har forhåndsdefinert. For politiet sier at de og de medarbeiderne hos oss kommer til å dekke det og det området. Og da må du legge det inn sånn, sånn at det er klart på forhånd. Og samme med brannvesen. I kommunen vår så har vi de og de medarbeiderne i brann, i nabokommunen så er det de og de. Og da kan du enten legge alle inn som en stor gruppe, eller legge de inn per kommune og så kobler du de gruppene sammen. Så det er ulike |

| | | |
|---|---|---|
| | | muligheter der også for å gjøre det sånn. Det er ofte lurt å ha tenkt igjennom og ha de klart definert, sånn at du bare kobler de sammen om noe skjer. |
| 53 | L | Ja, nettopp. Igjen tilbake til at et sånt basescenario kan være å ha det per fylke eller per kommune, og så hvis behov kan man gå inn der og konfigurere. |
| 54 | I | Ja. Ofte så skjer dessverre det uventede. Hvor skal du sette grensa hvor mye du skal gruppere det sammen. Det kan være litt vanskelig å vite. La oss si at regn fører til at du plutselig får et område ... Jeg bor jo her på Østlandet, og det er værmessig veldig snilt i forhold til Vestlandet. Det er omtrent aldri uvær her, men plutselig får du litt regn og så får du et jordskred i stedet som drar med seg infrastruktur. Da skjer plutselig det uventede. |
| 55 | L | I Nødnett så er det vel sånn, de ser for seg at det blir kanskje 65 000 brukere eller noe sånt på et tidspunkt. Hva er realistisk å se for seg av kapasitet på et lite lokalt kjernenett hvis vi en perfekt verden ser for oss at vi har det deployert på hver eneste lille BS? |
| 56 | I | Tja, 10 000 er ingen problem. Det har ofte vært et problem for oss som jobber i Norden at startpunkt på kjernenett begynner på 1 eller 10 millioner brukere. Så det kan være en utfordring å få til kommersielt når du tilbyr det. Så en 10 000 brukere, det er nok normalt ikke noe problem. Ofte vil du dimensjonere det til kanskje noen hundre, typisk. Og du vil også, når vi kommer tilbake til det vi diskuterte tidligere, når du har autentiseringsvektorer og slike ting liggende på dette kjernenettet, så vil du ikke ha så mange liggende hvis noen skulle prøve seg og du velger å ikke slette alt innholdet hvis noe skjer. |
| 57 | I | En annen ting også, det vet jeg ikke om kommer til å skje, men du har en annen ting som går på autonomi, dette med side-link. At telefoner skal kunne snakke med hverandre direkte uten å via nettet. Du tar litt av opplinken og bruker den. |
| 58 | L | Ja, det er proximity services i 5G? |
| 59 | I | Korrekt. Ja. Men dessverre så har jeg ikke sett at det har kommet noe i 4G og 5G. Jeg tror en av utfordringene der blir at de som lager terminalene, de vil selvfølgelig bruke standard chipsett til standard telefoner som går i store volum, og alt dette som går på Nødnett-tjenester, det vil du realisere i programvare. For chipset er fryktelig dyre å utvikle, og de koster en del, og da tar du heller og bruker standardiserte mekanismer sånn som disse QCIene. Det er forholdsvis enkle ting, fordi de følger standardoppsett i 4G og 5G. Det er et enkelt tillegg. Når du legger dette PTT, push-to-video-tjenestene i en server bak kjernenettet, så er det ikke noe spesielt som kreves av telefonen. For telefonen er ofte den mest kritiske tingen når vi innfører nye ting i mobilnettet. Det er det som som regel ligger etter. Du kan se at ganske mye kreves av en ganske liten enhet, både på radiosiden er det vanskelig, og funksjonssiden. Det er ikke plass til så mange komponenter i en telefon, og ikke har du strøm til det å kunne få prosessere alt som skal prosesseres, og sendeeffekt. Derfor legges veldig mye funksjonalitet til nettverket. Så jeg tror ikke proximity services kommer noensinne, for å være ærlig. |
| 60 | L | Du tror ikke det, nei? Vi har to stykker i klassen vår som skriver master om å ha device til device gjennom WiFi, - |
| 61 | E | Ja, WiFi direct, WiFi aware. |
| 62 | I | Ja, det er litt enklere å realisere fordi telefonen trenger bare å opptre som en server. Den trenger ikke alle disse 3GPP-meldingene som går frem og tilbake. Så den WiFi-chipen gjør det, med WiFi kan du realisere det. Absolutt. |

| | | |
|---|---|---|
| 63 | L | Det er interessant å høre. Jeg har ikke gått veldig inn i device-til-device-kommunikasjon, men jeg har liksom tatt for gitt at det kommer jo. Det er interessant å høre at det kanskje ikke gjør det. |
| 64 | I | Nei, jeg tror ikke det. Fordi at da må noen utvikle et eget chipset til public safety. Hvis du ser på standard telefoner så selges de jo ... Hver modell eller hvert chipset er jo nesten 1 mrd. i antall. Mens en sånn Nødnett-telefon, det er globalt kanskje en million. Sant, så det er så lite antall og de går over mange år. Også dette med funksjonalitet, hvis du lager et eget chipset så vil det nesten alltid henge etter i funksjonalitet, for det blir for dyrt å oppdatere det. |
| 65 | L | Det her er et godt argument for å implementere autonome BS da, hvis man plutselig mister evnen til å snakke device til device. |
| 66 | I | Ja, jeg tror ikke den kommer. Den fantes i TETRA, men jeg tror ikke den kommer verken i 4G eller 5G. Det er enklere å lage autonome BS, sannsynligvis, enn å lage dette. For med autonome BS kan du tross alt realisere mesteparten av dette med programvare. |
| 67 | L | Hvis du skulle sett for deg hva som hadde vært veien å gå i NGN for å maksimere evnen til å kommunisere. Ser du for deg å ha et lite lokalt kjernenett på hver enkelt BS, eller regionale punkter? |
| 68 | I | Dette er litt avhengig av geografien. Jeg tror nok at regionale punkter ville vært en fordel. Så jeg ville lagt et regionalt punkt f.eks. i kommunesenteret. Da har du også en annen ting, med det som jeg foreslo til DNK, var å bruke MOCN-funksjonaliteten og så ha aksess hos alle radiooperatørene, Telenor, Telia og Ice. Og så har DSB sitt eget kjernenett der det ligger veldig mye av kritisk kommunikasjon. For da får du tre ganger tilgjengeligheten på en måte. Og så har du ulike leverandører av utstyr, så hvis det er en bug hos den andre, så er det kanskje ikke en bug hos den andre. |
| 69 | L | Likevel må jo da kjernenettfunksjonalitet kjøre distribuert. |
| 70 | I | Den kjører distribuert, ja. |
| 71 | L | Ser du for deg at det da blir DSB likevel som eier disse distribuerte sentrene? |
| 72 | I | Ja. Det tror jeg jeg ville gjort, hadde jeg vært DSB. Men det er klart, dette er jo politikk. Men du kan si, jeg husker iallfall da jeg jobbet med Nødnett at det var ekstreme krav til sikkerhet. Blant annet når politiet er på skarpe oppdrag er det ingen andre som skal vite det. Det skal ikke komme lyd fra telefon. Jeg vet at de kommersielle operatørene har veldig streng sikkerhet. Sånn som vi får ikke lov til å jobbe hos bl.a. [operatør] uten at vi har klarert medarbeidere til å jobbe med det. Men likevel er det åpne standarder og åpne produkter. Om ikke leverandøren kommer inn så kan det være enten en som har sluttet hos en leverandør, en som har sluttet hos operatøren, eller noen som ikke har noe med det å gjøre, men har veldig god kompetanse på dette og kan bryte seg inn på en eller annen måte. Det er veldig godt sikret med brannmurer og mange lag med sikkerhet, men det er alltid en eller annen. Det er alltid en endelig måte for risiko. |
| 73 | I | Det andre er at det er veldig godt sikret utstyr hos operatørene, men det er klart at det kan være en katastrofe som skjer. Jordskred som drar med seg strøm og fiber, eller et eller annet som skjer. Og rent kommersielt, de har jo veldig strenge krav. Vil det være fornuftig av en kommersiell operatør å tilby tjenester med så høy grad av sikkerhet og tilgjengelighet? Det kan hende at det blir for dyrt for en kommersiell operatør, rett og slett. Jeg er ikke sikker på |

| | | |
|---|---|---|
| | | om alle har tenkt igjennom alt som kreves, for å være helt ærlig. |
| 74 | E | Det må jo eventuelt komme noen reguleringer på det, og så blir det en balanse på å ha det sikkert og robust nok, og likevel få tilbud fra de kommersielle operatørene. |
| 75 | I | Jada. Du har jo dette med skivedeling, eller slicing. Så da kan du tilby QoS og alt dette som behøves. Men så hvis du da begynner å snakke om, som du nevnte, distribuerte siter. Hvem skal da eie de? Det er jo ingen som kan drifte dette bedre enn kommersielle aktører. Det er de som har absolutt høyest effektivitet, og har folk som er veldig dyktige og driver dette 24t i døgnet, og som administrerer SIM-kort og sånt. Dette har de prosesser for, alt dette. Så hvis du ser på kostmessig og samfunnsmessig kost, så er det sannsynligvis ingen som kan gjøre det bedre enn operatørene. De skalerer og alt. Så da er det mer en sikkerhetsmessig og politisk avgjørelse. |
| 76 | E | Ja, for det ene er jo at, den kommunikasjonen går jeg ut ifra at i de fleste tilfeller vil være ende-til-ende-kryptert. Men hvis man da har DSB som en MVNO, eller har et sånt type MOCN-oppsett, så er det kanskje ikke gitt at de vil kjøre sin egen AMF, for eksempel, og hvis operatørene eier AMFen og den distribuerte funksjonaliteten. Da kan det vel hende at det vil lekke f.eks. mobilitetsdata om politiets skarpe operasjoner. |
| 77 | I | Det kan skje. Selv om det ikke skulle skjedd. Fordi du krypterer jo innholdet, men du kan ikke kryptere all lokaliseringsdata heller. Da må du gå og lage noe nytt igjen, som ikke er standardisert. |
| 78 | E | Ja. Sånn jeg har forstått det er det litt usikkerhet knyttet til om operatørene vil la en typ MVNO kjøre sin egen AMF knyttet direkte opp mot deres radionett. Har du noen tanker rundt de tekniske utfordringene med et sånt type oppsett? |
| 79 | I | Det skal jo være mulig å kjøre egne AMFer på den cloud-baserte infrastrukturen og sånt. Vi har jo laget cloud-basert infrastruktur til [kunder]. Det er sikkert at det er en del utfordringer praktisk. Hvem har ansvaret for at den VNFen fungerer til enhver tid, og oppfører seg som den skal i de omgivelsene. Og igjen, hvis vi begynner å lage spesielle AMFer, så kommer det ny utgave av 3GPP, så må du kanskje gjøre noen oppdateringer. Som regel er jo ting bakoverkompatible, men det kan være en funksjon du ønsker. Hvis du ser en kommersiell VNF, la oss si hvis du ikke er den første som implementerer, så er den kanskje testet hos hundre operatører før den blir implementert for en Nødnett-tjeneste, for eksempel. Vi har jo et eksempel i Finland, Elisa, jeg vet ikke om du kjenner den operatøren? |
| 80 | E | Jo. |
| 81 | I | Der leverer de jo med nettverket, og de skal Nødnett for, de skal overta, Virve-funksjonaliteten har jeg forstått. Der har de delt BS i to logiske stasjoner, slik at du kan oppgradere den ene delen av BSen, la oss si fra 2G til 4G, uten å røre 5G. Og så tar du 5G for seg. Hvis du da tar ned 5G for oppgradering, så vil terminalen velge 4G, og så har du full funksjonalitet på 4G mens det foregår. |
| 82 | L | Vi fikk litt nyss om gjennom stortingsmeldingen for noen uker siden, at det virker som det kommer til å stilles krav til at kommersielle nett har en viss autonom funksjonalitet i fremtiden. |
| 83 | I | Ja. |
| 84 | L | Du kan gjerne snakke litt om det om du vil, først og fremst, hvis du har noe... |

| | | |
|---|---|---|
| 85 | I | Ja, jeg har ikke lest stortingsmeldingen. Men det var jo ett av ... Du har sikkert lest den rapporten som gikk på evaluering av hvordan 700-frekvensen skal brukes. Der var argumentene med å legge fremtidige Nødnett til kommersielle nett, at det er bedre å investere i redundans i de kommersielle nettene, for da får alle glede av det. Og klart, autonomitet i kommersielle nett er jo selvfølgelig en stor fordel. Men du har disse utfordringene med, ja ... Jeg tror nok HSS-delen kanskje er den største utfordringen. Fordi at med en gang du begynner å distribuere HSSer rundt om så får du utfordringer med sikring av siten. Hvis du ser på [operatør] for eksempel, så har de sånn som jeg har forstått det, kjernenettene sine hos spesielle leverandører, i fjellhaller sannsynligvis og godt sikrede steder. Hvis du da begynner å distribuere dette, så har du den at folk kan bryte seg fysisk inn og stjele krypteringsenheter og ta det. |
| 86 | I | Men det er klart, hvis du kan ha et subsett i den lokale HSSen basert på hvem som er i det lokale området og hele tiden holder det oppdatert, så vil det jo kunne gå rundt igjen. Men ulempen er jo hvis det kommer nye inn og du ikke får oppdatert, da kommer ikke de seg på nett. Eller så må du ha full HSS distribuert, og da må du se på noen måter å sikre det rent fysisk. Ellers er jo det en bra ide, og det er sånn de kommer til å bygge operatørnett etter hvert også. For de skal tilby tjenester med veldig korte svartider. Da må du ha både server og kjernenett lokalt. |
| 87 | L | Det kan kanskje være en binding da for Nødnett å plasseres i regionale edger i samme fysiske sikring som kommersielle. |
| 88 | I | Ja, det bør de nok. Jeg tror at mange av de lokale edgene kommer til å kjøre signalering og HSS sentralt. For du har rikelig med tid, hvis du ser på ms-nivå så er det rikelig med tid om du setter HSSen ... La oss si du har et par HSSer i Norge som er sikret veldig godt. |
| 89 | L | Ja, ikke sant. Så likevel så vil det stilles ytterlige krav til å kjøre hele det delvis dupliserte kjernenettet ute for Nødnett. |
| 90 | I | Ja. Da kan også Nødnett legge seg på å kjøre ... Ofte vil jo disse distribuerte edgene bestå av flere servere, og de kan faktisk ha sin egen server som er allokert til Nødnett, men kjører i serveromgivelsene til operatøren. Fordi edge som de lager, de har samme spesifikasjon som en innendørs BS. For de må tåle mye større temperaturområde. De kan ikke støye så mye som en sånn sentral server som står i egne datarom, og en del slike ting. Men ofte har du plug-in servere i dem. Ofte som ligner på disse Open-rack som dere kanskje har sett, disse firkantede serverne. Vi bruker en standard som heter Sledge, der du kan plugge kanskje fire-fem servere i en større som er basebandet på en BS. |
| 91 | L | Ja, nemlig. |
| 92 | I | Da kan du ta en server og si at den kjører Nødnett-funksjonalitet. Som et eksempel er det slicer. Sånn som jeg ser det, er HSSen den vanskeligste delen. Det er ikke tekniske ting, det er rett og slett sikkerhetsmessige ting som, ja. |
| 93 | L | Ja, ikke sant. Så da er det både sikkerhetsbiten og brukervennlighet, med at du må ha mulighet til å komme deg inn på nett. |
| 94 | I | Ja, du må komme deg på nett, og da må du ha nøkler. Du kan si at i en total katastrofe så kan du akseptere at du går ukryptert inn. Det er også et alternativ. Det er bedre enn at du ikke får kommet på og gjort jobben din. |

| | | |
|---|---|---|
| 95 | L | Men det er da tilgang til nettverket, hva blir tilgangsstyring til MCX-tjenestene? Vil det også ligge i ... Hvordan vil det foregå? |
| 96 | I | Tilgang til tjenestene? Hvis du kommer med et IMSI-nummer som er autentisert av brukertjenestene, så blir det sjekket. Du kan enten bruke en PCRF, eller ha en enklere PCRF-funksjon i den applikasjonsserveren som kjører dette. Så når den ser at du har gyldig IMSI, eller etter hvert vil du bruke et TMSI-nummer, eller et temporært nummer som er kortere og litt lettere å håndtere. Men prinsippet er det samme, du må ha et IMSI som er autorisert. MME gir ut TMSI som temporær identifikator som systemet bruker også for mapping av tjenester. |
| 97 | L | Mhm. Så sånn du ser det, så er det ikke så stor forskjell teknisk på å kjøre opp autonom funksjonalitet i et veldig lokalt område eller et ganske stort et, det handler bare om skalering og håndtering av [vanskelig å høre]. |
| 98 | I | Ja. Det handler kun om skalering og håndtering. Så det er noe en må ta. Du kan jo ha det per BS, det kan fort bli litt kostbart, men i noen tilfeller så kan det være. La oss si at de kommersielle aktørene, hvis du kjører aksessen hos en kommersiell aktør og du likevel har noe der, så er det ikke så stor tilleggskost. |
| 99 | L | Det vil vel kanskje også avhenge av hvor tett infrastruktur det er i et område. I grisgrendte strøk er det mer nyttig å ha det på en BS. |
| 100 | I | Ja, absolutt. |
| 101 | L | Jøss, det her ga god innsikt synes jeg. Det var veldig deilig. |
| 102 | I | Jeg håper det! Du ser jo det at det er lett å overse ting. Langs jernbanen ligger mye fiber, og den kuttes nok hvis du har en avsporing. Og det er da du trenger den. Eller du trenger den jo utenom og, men du trenger den ofte for nødnett og kommunikasjon. GSMR har prøvd å unngå bruk av de som går langs skinnegangen. |
| 103 | L | Det er et godt eksempel på når det plutselig blir veldig kritisk å ha den funksjonaliteten der. |
| 104 | I | Ja. Det er jo ting jeg husker fra vi holdt på med Nødnett. Du bestilte en redundant forbindelse. Så den leverandøren av fiberen gikk til en konkurrent og bestilte en redundant forbindelse. Den så at de ikke hadde fiber selv der, men den leverandøren som bestilte hadde jo fiber. Så han sendte videre til sin innkjøpsansvarlig som kjøpte en redundant forbindelse. Så da var begge i samme fiber. Det ble jo oppdaget, selvfølgelig, men det kan veldig lett skje. |
| 105 | E | En av de tingene jeg bl.a. har sett på, vi kom jo litt inn på det tidligere, om det blir mer redundant når man bruker alle tre radioaksessnett. I mange tilfeller er kanskje alle tre BS koblet opp på samme lokasjon og er avhengige av samme fiber. |
| 106 | I | De skal jo helst bruke samme site, fordi samfunnet vil ikke ha så mange siter og tårn og greier. Så det er en utfordring. Ofte er de koblet på samme lokasjon, og de deler transmisjon, som ofte er det svakeste leddet faktisk. Hvis du ser på feil i mobilnettet så er det ofte transmisjonen som står for 80-90% av feil i nettet under drift. Så det var jo også tatt opp i den Menon-rapporten, at de kanskje skulle investere litt i redundante backhaul. Og da kan en jo tenke, for Nødnett trenger jo ikke veldig mye båndbredde, selv om det kommer inn noe video. Det er fortsatt ganske overkommelig. Så en kunne jo vurdert om en skulle satt opp radiolinjer som skulle virke som en sånn redusert kapasitet i tillegg til fiber, for |

| | | |
|---|---|---|
| | | eksempel. |
| 107 | L | Har du vært noe inni dette med self-organizing networks? |
| 108 | I | Ja, det er noe vi har i dette radionettverket. Det organiserer seg selv. Hvis en site detter ut, så tilter man opp antennen på nabositen for å få en større celle, for eksempel. |
| 109 | L | Ja, nemlig. Er det strevsomt eller krevende å få til å... |
| 110 | I | Nei, ikke nå, for nå har du elektriske RETmotorer (remote electrical tilt), og denne motoren kan tippe opp antennene til nabo-BTSer slik at de kan dekke området eller deler av området til en BTS som faller ut. Når du kommer med massiv MIMO så ligger det i antennen i seg selv. Da tilter du opp motoren. Vi gjør det av og til for store arrangement. Da regner vi om nettet og omdimensjonerer det, så tilter vi litt, forandrer litt på antennetilten. Så det er en mulighet å gjøre. Omkonfigurere parametre. Nå ser vi også at de nye radiolinjene kommer. Vi er oppe i 10Gbit radiolinjer i E-bånd. Har du 10Gbit har du god nok kommunikasjon på en site, selv om du har flere BSer der. |
| 111 | L | Ja, så man kan nesten kompensere for en BS som har falt ut med å ruse opp en annen? |
| 112 | I | Det kan du i en del tilfeller, i alle fall ta en del og lage større celler. Du kan ha alternative parametersett, sånn at du kan øke celleradiusen. I noen tilfeller kan du powere de opp også. Det er ofte at du får mye mer interferens hvis du øker powernivået. Men SOen skal hjelpe til med det også. Du får jo rapportert interferensnivå fra terminalen, så da kan du steppe det ned igjen. Du har ikke powerkontroll i 5G og 4G på nedlinken, men du har det i opplinken. |
| 113 | L | Nemlig. Hm. Jeg kjente ikke egentlig til hvordan det fungerte, så det var artig å høre. Du, bare fordi jeg blir litt forvirret av det, på et helt annet tema. Hva er egentlig den kommersielle interessen i edge? Hva er det som krever så ekstremt low latency og som gjør at du vil ha tjenestene distribuert? |
| 114 | I | Det var et godt spørsmål. Det er klart, det diskuteres mye om trenger vi 5G, trenger vi ekstra low latency. Det er en tjeneste som er litt sånn, det er dette med selvkjørende biler som har vært diskutert. Det tar litt tid før det kommer i alle fall i vårt land med glatt føre og så-som-så med veldig god dekning overalt. Men disse som holder på med droner, dronepiloter, at du kan styre droner over mobilnettet. Det kan du, det gjør du med 4G i dag. Så du trenger ikke den veldig korte. Så har du kanskje andre tjenester. Styring av strømnettet, der du kanskje ønsker å komme ned i noen millisekunder hvis du skal slå ut noe last, eller fasekompensasjon, eller et eller annet. Det har også vært noe med disse tjenester med fjernoperasjon, der det sitter en kirurg et sted og opererer en pasient som er et annet sted. Du kan også kjøre noe over fastnettet. I dag gjøres det heller på en sånn måte at kirurgen opererer på vanlig måte, så sitter en annen kirurg et annet sted et stykke unna og følger med og gir anbefalinger på hva som skal sys, eller han som opererer hva han ser. Også for undervisning. Det har også vært fjernstyring i fabrikker, for eksempel, med styring av roboter. Vi har roboter i fabrikken vår i [sted] som blir styrt av 5G-nett. De kjører av gårde med komponenter og kretskort. Og på sykehus ser de for seg å bruke det. På sykehus er det veldig mye som transporteres rundt om. Da er det greit med veldig kort svartid, som hvis en server skal hjelpe en robot med å finne frem, hvis ikke den har full autonomi. Et annet marked vi ser som faktisk skjer en del, er spill. Fordi at det er mange i denne verdenen som har en mobiltelefon. Faktisk så har flesteparten av befolkningen det. Selv i fattige land, så er folk villige til å bruke veldig mye penger, forholdsvis mye penger, på mobil. Så å slippe å kjøpe egen spillkonsoll, de koster ganske mye. Hvis du kan gjøre all den prosesseringen i en sentral server, så får du bare presentasjonslaget på mobilen din, og der kreves jo ekstremt |

| | | |
|---|---|---|
| | | kort svartid. I dag, vet du hvem som krever kortest svartid av alle apper i dag? |
| 115 | L | Nei. |
| 116 | I | Det er børsmeglere. Det er helt vilt, de bruker faktisk hule fibere. Fordi brytningsindeksen i glasset er jo 1,5. Og det bremser jo hastigheten på lyset til 2*10^8 m/s i [vanskelig å høre]. Tar du vekk innmaten i fiberen og har luft der, så går den 50% kjappere. Det er såkalt hollow fiber. |
| 117 | L | Jøss. Nei, det synes jeg var et solid svar. |
| 118 | I | Dette er veldig odde ting. Men det kommer sikkert andre ting også der du har mer industriell og fjernstyringsapplikasjoner der du trenger at ting skjer umiddelbart. |
| 119 | L | Absolutt. Jeg kan tenke meg at det her fremmer innovasjon. |
| 120 | I | Ja. Og så vender vi oss til ting, at det skal gå fort. Og så har du også det som er content distribution. Det finnes jo i dag, selvfølgelig. Det krever ikke så veldig korte svartider, men det kan hjelpe på trege servere, sånn som VGnett og Adressa.no, at de laster inn innholdet til disse distribuerte serverne og så får du det derfra. Og så kommer det helt sikkert nye tjenester som vi ikke tenker på eller vet finnes i dag. Det gjør det nok. |
| 121 | L | Det gir mening. Det kommer til å bli brukt. Har du noe mer på lista di, Eivind? |
| 122 | E | Nei. Jeg tror vi har vært innom en god del. |
| 123 | L | Er det noe du føler vi burde ha snakket om nå, som vi ikke har touchet borti? Nå som du kjenner litt til hva vi ser på? |
| 124 | I | Nei, jeg tror vi har touchet inn på det meste. Jeg tror at det som skjer mer i 4G/5G ... Jeg sier 4G/5G, fordi jeg har snakket litt med trafikkverket i Sverige, de kjører både veier og tog. De sier at de vil ikke spesifisere teknologi, de vil spesifisere tjenester. Om det går på 4G eller 5G spiller ingen rolle. Så jeg tror nok at en skal ikke fokusere for mye på teknologien. Og det som blir begrensende her, det kommer til å være tilgang på gode terminaler, altså telefoner som har disse tjenestene som behøves, fysisk brukerinterface og alt dette. Og før ting var programmert mer HW-messig, det var selvfølgelig SW og switcher, men i TETRA var ting satt veldig fysisk i nettet. Så vi kommer til å se det at ting her kommer til å være OTT med spesiell støtte i radionettet. Med prioritering og slike ting, men selve gruppehåndteringen og alt dette skjer OTT. |
| 125 | E | Ja, så du tenker ikke at man trenger å implementere MBMS eller noe sånt? |
| 126 | I | Jo, det blir nok en del av nettet for å få kringkasting. Men du trenger egentlig ikke det i de fleste skadested. For hvis du ser på kapasiteten på et nettverk, så.. Om den raser ut for 50 stykker i gruppekall, serielt, så går dette så fort at det blir oppfattet som sanntid. |
| 127 | L | Men du ser for deg at langsiktig blir det faktisk behov for det? |
| 128 | I | Ja, hvis det blir mange. Hvis du tenker på en av disse jordskjelvfilmene, med at du drar inn alle nødetater fra alle fylker fra Østlandet i Oslo så vil det kanskje være det. Men hvis du ser på.. La oss si at du har 20MHz båndbredde, og du trenger kanskje et par PRBer per bruker, du sier hele tiden vil du bruke til VoLTE-gruppekall. Men du har jo mange frekvenser og, så da kan du jo fort kjøre 40-50 brukere i parallell på en bærer, sant. En annen ting du må |

| | | |
|---|---|---|
| | | huske på er at MBMS krever veldig nøyaktig synk. +/- 1 µs som er veldig strengt og krever satellitt eller transmisjonsnett med boundary clocks og eventuelt veldig høy båndbredde for timing-pakker. I prinsippet må du ha en GPS eller satellitt inn. Du kan jo ha en veldig nøyaktig oscillator, selvfølgelig. BSen vår kan gå en 24t nøyaktig hvis du mister, eller du kan få den over backhaul hvis du mister. Men du må ha en veldig bra backhaul da. Jeg tror nok i Norge med frekvensressursene vi har og en skikkelig disaster om du kjører eventuelt over flere operatører, så er jeg usikker på om MBMS egentlig trengs. |
| 129 | L | Ja, det er vel det vi har hørt fra andre også. |
| 130 | E | At kapasitetene blir såpass store, i hvert fall i 5G, at man kanskje ikke har behov for det. |
| 131 | I | MBMS, ja. |
| 132 | L | Ja, sett det relativt lave brukertallet. |
| 133 | E | Ja, det er ikke en by i Kina, på en måte. |
| 134 | I | Nei, det er ikke det. Og dette med video, og hvis du skulle sendt video ut... Hvor mange er det egentlig behov for å sende video til. Det vil du kanskje definere at er en mindre brukergruppe. En mindre gruppe i brann, en eller to på helse og en eller to hos politiet trenger å se den videoen, kanskje. Ofte er det jo at man må være flink til å beskrive det du ser. En røykdykker, det hjelper han ingenting å få en video når han er ute på oppdrag. Da kan man få en beskrivelse av bygningen og alt dette. |
| 135 | L | Vi går tom for tid her vi, men det her var en veldig informativ og god time, synes jeg. |
| 136 | I | Ja, det var hyggelig. |
| 137 | L | Så det som skjer nå er at vi skriver transkript av dette her sikkert i løpet av de neste par dagene, og så sender vi over til deg så du kan se at alt er som det skal være. |
| 138 | I | Jada, jeg skal ta og sjekke det. |
| 139 | E | Da tar vi og anonymiserer litt. Dere blir jo en infrastructure equipment provider, litt mer generelt. |
| 140 | I | Det er bra. Da får dere ha lykke til videre med masteroppgaver. |
| 141 | L | Tusen takk, ha en fin dag videre! |
| 142 | E | Takk skal du ha! |
| 143 | I | I like måte, ha det godt! |

Eivind Standal

# Mission critical services in commercial 5G networks

NTNU
Norwegian University of
Science and Technology