5G-sikkerhet: En kvalitativ studie av sikkerhetsforståelsen ved 5G-utrullingen i Norge

Mari Moen

Masteroppgave i statsvitenskap, Institutt for statsvitenskap
UNIVERSITETET I OSLO

Høst 2020
Antall ord: 33 513

Sammendrag

Denne oppgaven analyserer hva som var den norske sikkerhetsforståelsen i 5G-debatten knyttet til valget av leverandør for 5G i Norge. For å belyse dette benyttes to teoretiske rammeverk med en sosial-konstruktivistisk tilnærming for analysering av 5G-debatten som pågikk i Norge fra ca. 2018-2020. Oppgaven synliggjører fordelen ved bruk av flere teoretiske perspektiv for å forklare dagens komplekse sikkerhetsutfordringer knyttet til staters investering i kritisk digital infrastruktur. Analysen identifiserer en risikoforståelse og en sårbarhetsforståelse knyttet til leverandørvalget for 5G, men som kombineres med en identifisering av en trusselaktør som ikke utrykkes eksistensiell men som alvorlig ved 5G-utrullingen. Videre kommer det til syne en tydelig teknisk diskurs og debatt med teknologisk ekspert som sentrale aktør, med mindre tilstedeværelse av politiske folkevalgte i spørsmålet om cybersikkerheten i 5G-utrullingen. Analysen synliggjører kompleksiteten ved både moderne elektronisk utstyr, mobilnettverket samt globale verdikjeder som inngår produsering og drift av elektroniske komponenter som inngår 5G-nettverket, og som legger føringer og utfordrer vår kunnskap om risikoer og sårbarheter i det fremtidige mobilnettverket. Videre viser analysen hvordan et sikkerhetspolitisk samarbeid i dette tilfellet legger føringer og forutsetninger for sikkerhetstiltak gjort i denne saken, og viktigheten dette har for evnen å gjenopprette 5G-nettverket ved et eventuelt tilsiktet uønsket hendelse. På bakgrunn av funn foreslår oppgaven også et mulig tredje teoretisk perspektiv som kan gi nye videre innsikt i 5G-debatten.

Forord

Etter en lang og krevende tid er man omsider i havn med et masterstudium der denne masteroppgaven avslutter det hele. Jeg vil takke veileder Niels Nagelhus Schia fra NUPI som har bistått med innsikt, råd og mange innspill til selve oppgaven, men også hvordan å arbeide med og strukturere en slik omfattende oppgave og prosess som dette er. Oppgaven hadde ikke vært mulig uten veileder Tobias Liebetrau fra Institutt for Statskundskab ved København Universitet (KU), som har bidratt med uunnværlige kompetanse, tilbakemeldinger og innspill til oppgaven. På bakgrunn av dere har jeg hatt mulighet til å skrive om et tema som ikke synes å være så skrevet så mye om, men som omhandler et viktig og aktuelt tema som omgår oss alle.

Ikke minst må jeg takke familie og venner som har støtte meg i denne prosessen, og som jeg ikke hadde klart dette her foruten.

Mari Moen
Oslo, 15. november 2020

Innholdsfortegnelse

1.0 Innledning

«Men som jeg nevnte, det er et veldig mye mer komplekst bilde … Du kan si, ja Huawei har hovedkontoret sitt i Kina og blir selvfølgelig styrt etter kinesisk lovgivning, men vi henter jo utstyr fra store deler av verden, mange underleverandører. Ericsson er i Stockholm de er svenske? Njee … hvor er det de ulike folkene i Ericsson jobber. Nokia er i Finland, er de egentlig finske? I [Selskap X] vi har 20 000 ansatte, 3000 i Norge. Vi er norske fordi vi har hovedkvarter i Norge, men jeg tror i alle fall for meg så er det viktig når du skriver den oppgava at man må tenke over at det over hundrevis om ikke tusenvis av underleverandører for å faktisk levere infrastruktur til et nett. Det er store deler av jorden befolkning som er på en eller annen måte involvert i prosessen» (Informant 7).

Når neste generasjons mobilnettverk (heretter 5G-nettverket) har det uten tvil blitt et taktskifte på nasjonalt nivå her i Norge, men også globalt når det gjelder sikkerheten rundt det kommende 5G-nettet. 5G-nettverket beskrives ikke bare en videre utvikling og forbedring av det nåværende mobilnettet 4G, men blir også tilretteleggeren for den fjerde og neste industrielle revolusjon (Center for a New American Security, 2019). Få av oss stilte nok ikke så mange spørsmål når symbolet på skjermen på våre digitale enheter endret seg fra 3G til 4G tilbake i 2012, og heller ikke at nettopp Huawei stod bak som leverandør av 4G den gang. Selskapet Huawei har til nå stått for både 2G, 3G og 4G i Norge ved at selskapet vant budrundene den gang der hele selskapets mobile nettverksinfrastruktur ble skiftet ut med Huawei-teknologi. Når 5G-nettverket nå skal bygges ut i Norge og i resten av verden, har den offentlige diskursen og den sikkerhetspolitiske oppmerksomheten rettet seg mot sikkerheten i mobilnettverket og beskyttelse kritisk digital infrastruktur med oppmerksomheten har dreiet seg hovedsakelig rundt skepsisen til selskapet Huawei.

Utrullingen av 5G blir sett på å stå sentralt i den videre digitalisering av samfunnet. Sammen med utviklingen av Internett of Things eller «tingenes internett» (heretter IoT) blir og som ikke bare legger til rette for videre effektivisering av tjenester, men der teknologien og produktene vil legge til rette for nye bruksområder i flere bransjer og sektorer fremover (Norsk Kommunikasjonsmyndighet, 201, s.22). Ved utviklingen av og økningen i anvendelse av IoT, vil IoT-applikasjoner komme til å bære viktige samfunnsverdier framover, og være kritisk innenfor liv, helse og sikkerhet, og det er blant annet her man antar at 5G vil blant

annet komme til å spille en svært viktig rolle også som en tilrettelegger for dette. I tillegg får digitale enheter utvidede og flere komplekse funksjoner og oppgaver å utføre. Det har vært en økende konvergens av digitale oppgaver der man har GPS, kamera, telefon, betalingsterminal, datamaskin og mer i en og samme digitale enhet. Dette forsterkes ytterliggere med en økende andel brukere som kobles til det mobile nettverket.

«Så vet vi at nødnettene i Norge som skal legges inn. Vi vet at sykehus, Oslo Sporveier som har sine egne nett, de ser at dette er en mulighet til å bygge, dekke det behovet i framtida innenfor kommersielle nett, men da kreves det såkalt skivedeling. Så dette er med private nett inn i kommersielle nett. Forsvaret er et annet eksempel. Det er snakk om fjernkirurgi. Det er selvfølgelig hvis du må kjøre en hasteoperasjon i Mosjøen som er veldig kritisk, så kan du ha med verdens beste kirurg fra Stanford University som kan stå med høy definisjon video og guide operasjonen» (informant 7).

Parallelt med dette legger det det norske samfunn og myndigheter vekt på digitalisering i offentlig sektor og tjenester, og som er med på å bidra til videre økt avhengighet til det mobile nettverket for realisering av disse tjenestene og teknologiske funksjonene. Dette innebærer hver for seg og kombinert, en enorm kompleksitet. Norge blir omtalt som et av de mest digitaliserte landene i verden og ligger i toppen bak de andre skandinaviske landene, og har et høyt digitaliseringstempo. Regjeringen ønsker å satse på digitalisering, og ser på dette som et viktig virkemiddel for å modernisere og effektivisere offentlig sektor, men også for å skape et bærekraftig velferdssamfunn for generasjoner i fremtiden. Men med en økende digitalisering av både private og offentlige tjenester, øker både befolkningens og de offentlige myndigheters avhengighet til det fungering av det digitale system for levering av disse tjenester, men da også sikkerheten rundt og skjerming av disse systemene og informasjon som befinner seg der (Regjeringen: 2019). Ikke bare det, men når stadig flere tester i privat og offentlig sektor baseres på teknologiske løsninger, åpner dette for en utvidet angrepsflate for cyber hendelser. Direktoratet for Samfunnssikkerhet- og Beredskap (heretter DSB) har i sin risikovurdering vurdert et cyberangrep mot norsk ekom-infrastruktur er det scenarioet som medfører de alle største kostnadene for det norske samfunnet (Direktoratet for Samfunnssikkerhet- og Beredskap, 2016, s. 10).

For det digitale domenet kan muligens ikke lengre bare sees på som et separat domene der noen deler av livets funksjoner utføres, men et sted der så og si alt nå ordnes. Det er her vi i

større grad skaper og opprettholder menneskelige relasjoner, der noen av våre mest personlige og fortrolige opplysninger og aktiviteter ligger, der vi foretar en stadig større andel av våre finansielle transaksjoner og får nyheter som vi forholder oss til. For å ikke snakke om der politisk virksomhet i større og større grad organiseres, og der internett og sosiale medier er blitt et vesentlig verktøy for myndigheter og politiske aktører for politisk kommunikasjon og informasjonspåvirkning (Greenwald, 2014, s.13-14). Med det mobile nettverket, som bærer av stadig økende samfunnsverdier og kommer til å drifte det fremtidige norske nødnettet, øker en større bevissthet på hvordan disse nettverkene opereres og hvem som drifter de. Kombinert med økende kunnskap rundt egenskapene ved mobile nettverk og ny teknologi som innføres i kritisk infrastruktur, kan nettverket sees på som å ha fått umåtelig økende verdi.

1.1 Forskningsspørsmål

For offentlige ansatte og politikere over hele verden har som oppgave og ansvaret med å håndtere dagens sikkerhetsutfordringer, samtidig som å planlegge håndteringen av en uforutsigbar fremtid. Stater må i dag i økende grad håndtere uautorisert adgang i deres datasystem med formål om sabotasje, spionasje, cyberkriminalitet og digitale påvirkningsoperasjoner mot sin befolkning. Norske sikkerhets- og etterretningstjenesters trusselvurdering peker på dette som en av de største og vedvarende truslene mot Norge (Politiets Sikkerhetstjenester, 2019, 2020). Den foreløpige teknologiske utviklingen har gitt uante muligheter, men også sårbarheter som har blitt sett på som nødvendig å håndteres. Hvordan saker blir fremstilt og snakket om legger føringer for de politiske- og sikkerhetsmessige tiltak som sees som passende (Betz og Stevens, 2013, s.147). Bruken av språk påvirker hvordan cyberspace beskrives og snakkes om og videre er med på å forme hvordan cybersikkerhet konseptualiseres (Dunn Cavelty, 2013, s.106). Videre så kan ulike oppfattelser og beskrivelser av trussel sammen med bruk av metaforer påvirker diskursen, og som har politiske konsekvenser. For det er i tillegg ikke bare den politiske og tekniske elite som er med på å forme diskursen, men også andre ikke-statlige aktører er også med på å utgjøre en substansiell del i forming av diskursen, og til sammen preger forskjellige perspektiver og forståelser cyber-diskursen (Dunn Cavelty, 2013 s.118).

For cyberangrepene opererer, hvisker ut territorielle grenser og synliggjør den komplekse konstellasjonen av ulike aktører og sektorer som inngår cybersikkerheten. Disse hendelsene,

med sine multifasetterte effekter, fører til ulik forståelse av cybersikkerhet og hvilke tiltak som kreves for å imøtekomme hendelsen. Med en vid gruppe av ulike aktører som inngår cyber-diskursen, er dette med på å gi flere ulike valgmuligheter til politiske aktører, da forskjellige aktører relateres til forskjellige perspektiv på trussel, nemlig hva er det utgjør å være en sikkerhetsutfordringer innenfor cyber-domenet. Dette inkluderer ikke vare statlige og ikke-statlige aktører, men også byråkratiske aktører, konsulenter eller tekniske eksperter har muligheten til å etablere «en sannhet» om visse trusler eller risiko, og derfor skape en akseptert presentasjon av trusselen som synlige politiske aktører nytter seg av (Cavelty, 2013 s.106-107).

Den statsvitenskapelige litteraturen innenfor cybersikkerhet sies har til nå vært hovedsakelig politisk orientert og ikke i stor grad basert seg på, eller kobler seg på andre statsvitenskapelige teorier innenfor internasjonale studier (Dunn Cavelty, 2013 s. 106). Sett bort fra at flere forskere har tatt i bruk Københavnerskolens sikkerhetiseringsteori og analysert om cyberdomenet har blitt sikkerhetisert, med et fokus på talehandling, elitediskurs, en eksistensiell trussel og en truende aktørs evne og hensikt å utføre et cyberangrep (Buzan, 1998, Cavelty 2007, 2008, 2013, Hansen og Nissenbaum, 2009).

Dette leder derfor videre til forskningsspørsmålet for denne oppgaven:

Hvilken sikkerhetsforståelse preget debatten om 5G-utbyggingen i Norge?

For å forstå dette er det ikke nok å bare se på Københavnerskolens sikkerhetiseringsteori, men man må også inkludere perspektivet risiko, nemlig riskification. For med en inkludering av bare sikkerhetiseringsteorien kan man for eksempel i ikke fange opp:

a) Sikkerhetsutfordringer som ikke sees å være preget av en eksistensiell cybertrussel og hastverk, eller kreve nødtiltak eller overskrider normale politiske prosedyrer. Men at sikkerhetsutfordringer som er preget i større grad av sikkerhetsutfordringer preget av langsiktig og kontinuerlig karakter og derfor sees mer på som den hverdagslige cybersikkerheten i 5G-nettverket.
b) I større grad gå glipp av bakenforliggende forhold, som blant annet teknologi, som ligger til grunn for muligheter for uønskede hendelser mot og i 5G-nettverket.

c) Hvordan også teknologi innebærer og skaper en viss usikkerhet som påvirker evne til å identifisere trussel, måle risiko og derfor preger evnen til å nøytralisere trussel og gjøre risiko- sårbarhetsreduserende tiltak.

Derimot kan man med sikkerhetiseringsteorien i økende grad, gjennom Hansen og Nissenbaums (2009) cyber-sikkerhetisering, et utvidet rammeverk av den opprinnelige Buzan, de Wilde og Wæver (1998), fanget opp en dynamikk som er spesiell innenfor cybersikkerhet, ved at det teknologiske i større grad inkluderes enn det teorien har opprinnelig lagt opp til, sammen med inkludering ekspertenes rolle i diskursen. Denne dynamikken kan også i større grad være med på å fange opp hvordan cybersikkerheten opererer på tvers av et samfunn og kan påvirke den nasjonale sikkerheten, men i like stor grad også individer som brukere av digitale enheter og tjenester. Begge teoriene har en sosialkonstruktivistisk tilnærming på sikkerhet og risiko, og innebærer at det i oppgaven her skilles mellom trussel og risiko innenfor cybersikkerhet, kan i tillegg være med på å belyse når et sikkerhetsspørsmål befinner innenfor eller utenfor politisk kontroll, styring og ansvarsmyndighet.

1.2 Bakgrunnen for problemstillingen

For uten tvil har det digitalisering, internett og det elektroniske kommunikasjonsnettverket (heretter ekomnettet) fått en enormt viktig rolle. Kanskje tilnærmet likt et nervesystem for dagens samfunn, og vil uten tvil fortsette å få vesentlig betydning i fremtiden for hele verden. For viktigheten av en sak kan måles utfra de konsekvenser saken har på samfunn som helhet. Debatten om 5G-utrullingen i Norge handler om i hvilken grad stater og samfunn kan stole på utenlandske leverandører av teknologiske komponenter siden Norge ikke produserer slik teknologi selv. Norge i likhet meg mange andre land trenger derfor å investere internasjonalt for å oppgradere kritisk digital infrastruktur og drive en innovativ samfunnsutvikling. I forlengelse av dette, burde man derfor reflektere kritisk over alt som kan gå feil ved en sånn investering, behøve å også tenke igjennom og ta høyde for scenarioer som internasjonale kriser og krig (Lysne, 2018 s.8). Diskusjonen rundt Huawei er et eksempel på dette, og selv om det til nå ikke eksisterer noen internasjonal enighet eller konsensus på hvordan stater skal forholde seg til utfordringer knyttet til tillit til teknologiselskap i en moderne globalisert verden, der økonomien består av globale verdikjeder med innsatsvarer fra hele verden.

Allikevel er utfordringen med utrullingen av 5G-nettverket vist seg å være så viktig at det har nådd nivået for internasjonal politikk. 5G-utrullingen har vist å ha blitt en global sikkerhetsutfordring og har vært på dagsorden til så og si alle stater, men også vært på agendaen til overnasjonale institusjoner som EU (EUs risikovurdering fra av cybersikkerheten i 5G). Utrullingen av 5G har ført til at nasjoner og EU har foretatt sikkerhetsvurderinger knyttet til å staters investering i mobilteknologi og kritisk infrastruktur. USA, som nok den mest aktive aktøren i denne saken, har oppfordret andre stater til å også ta avstand fra selskapet og at valg av leverandør vil komme til å få diplomatiske og sikkerhetsmessige konsekvenser. Videre er 5G-debatten i Norge men også globalt, et eksempel på hvordan teknologi har fått en betydning for den sikkerhetspolitikken som drives i cyberdomenet på både nasjonal og internasjonalt nivå.

Valget av forskningsspørsmål er delvis basert i den fremtredende debatten og medieoppmerksomheten knyttet til å tillate at kinesiske telekom-selskapet Huawei stå for levering av 5G-ustyr. Huawei står allerede for 90 prosent av det mobile nettverket i Norge, og nå har man disse sikkerhetsbekymringene. Dette forsterkes og kombineres med hvordan debatten synes å ha vært høyst kompleks, som «den perfekte storm», inneholdende flere dimensjoner. En økonomisk dimensjon med den mye omtalte handelskrigen mellom USA og Kina, der Huawei uttales som å være et verktøy i forhandlinger og at dette er motivet bak det amerikanske forbudet av Huawei. Saken har i forlengelse også en teknologisk dimensjon som omhandler en teknologisk konkurranse mellom statene og muligheten for at USA som et teknologisk hegemoni, har større bevissthet rundt kinesisk økende innovasjon, tekniske fremskritt og økonomiske investeringer på globalt nivå.

Til slutt har saken også en sikkerhetsdimensjon knyttet seg til sikkerheten i 5G-nettverket, og i hvilken grad det er mulighet for et cyberangrep (spionasje, tyveri og sabotasje eller påvirkning) gjennom eller ved hjelp av Huaweis teknologi. Det er klart at det er muligheter for og anklager om at disse ulike dimensjonene påvirker hverandre i denne saken, og legger føringer for den den forståelsen av den sikkerhetsutfordringen både Huawei og stater står ovenfor i denne saken, samt de avgjørelser stater og mobiloperatører har gjort i denne saken. Allikevel forsøker forskningsspørsmålet her fokusere på i sikkerhetsdimensjonen knyttet til debatten 5G-nettverket. På bakgrunn av dette mangefasetterte debatten, tenker jeg å ta den på alvor og undersøke hva som blir cybersikkerheten i det kommende og fremtidige mobilnettverket i Norge med utrullingen av 5G, og derfor hva som er den norske

sikkerhetsforståelsen i denne saken. På bakgrunn av dette vil det neste avsnittet ta for seg hva som menes med cybersikkerhet i oppgaven her, og hvordan denne forståelsen av cybersikkerheten i dette tilfellet befinner seg i en større vitenskapelig studie på cybersikkerhet og konseptet cyberspace.

1.4 Cyberspace og cybersikkerhet

Det er ulike oppfatninger og forståelser rundt hva som menes og defineres som cyberspace, og oppgavens problemstilling og omfang gir ikke rom for å gå en inngående kartlegging av alle de ulike måtene cyberspace og cybersikkerhet konseptualiseres. Det legges til grunn at ulike konseptualiseringer av cyberspace, cybersikkerhet og trussel har en effekt på aktørenes sikkerhetsforståelse og deres meninger rundt politiske tiltak og hvilke mer generelle praksiser og tiltak blir satt i verk (Dunn Cavelty, 2013 s.115). Cybersikkerhet er en type sikkerhet som utfolder seg i og gjennom cyberspace, og der utvikling og praksisen av sikkerheten blir både begrenset og muliggjort gjennom dette rommet. Derfor er det å ta utgangspunkt i hvordan 5G-utrullingen snakkes om og språket som brukes i denne saken for å snakke om dette digitale domenet, blir sett på som en nødvendig del i analysen, siden språket er med på å beskrive det digitale rommet og måten cyberspace opererer på og som har gjort at dette har blitt en del av politisk debatt og en sikkerhetsutfordring på nasjonalt og internasjonalt nivå (Dunn Cavelty, 2013 s.107). Videre blir cybersikkerhet blir i oppgaven her forstått som både diskursive og ikke-diskursive praksiser fra ulike grupper og sektorer av aktører, selv om oppgaven her, selv om oppgaven forholder seg til den diskursive delen for analysering av sikkerhetsforståelse (Dunn Cavelty, 2013 s.108). Det avvises ikke at ikke-diskursive praksiser er irrelevant forklaringsvariabler, men at dette allerede er en aktiv del å forme forståelsen, og at dette kommer også uttrykk i uttalelser i debatten og diskursen.

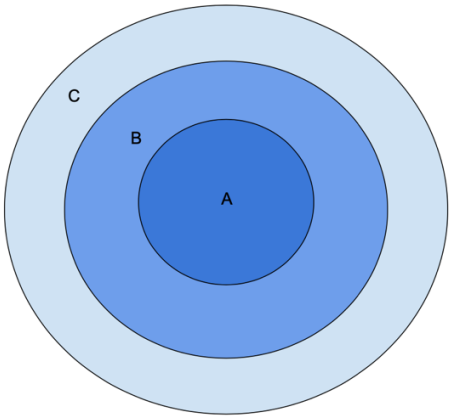
En mye brukt måte å definere cyberspace er se på den som bestående av tre lag: det fysiske laget, et syntaktisk lag over det fysiske og til slutt et semantisk lag på toppen (Libicki, 2009 s.12). Alle informasjonssystem avhenger av et fysisk lag som fysiske bokser og ledninger, og fjernes dette laget forsvinner systemet også. Det syntaktiske laget består av instruksjoner som utviklere og brukere gir maskinen og protokoller for at maskinene interagere med hverandre, som ruting, enhets gjenkjenning, pakkeinnramming, adressering etc. Det er på dette nivået hvor hacking fra utenforstående plager å foregå. Det semantiske laget inneholder ideer og informasjon som maskinen inneholder og er grunnen til at maskiner. Etter denne definisjonen

blir cyberspace sett på som bestående av både det virtuelle og det materielle, som et rom av ting, ideer, strukturer og innhold (Deibert og Rohozinski, 2010 s.16). Oppgaven her tar for seg det syntaktiske nivået innenfor cyberspace, der forskningsspørsmålet legger opp til en analyse om sikkerhetsutfordringen knyttet til 5G-nettverket, og de ulike måter dette på kan påvirkes gjennom det syntaktiske laget, gjennom kode, instruksjoner og andre verktøy for å få tilgang til det mobile nettverket og kunne påvirke det.

Når det gjelder norsk cybersikkerhet og digital infrastruktur og angrep i det digitale domenet, omtales gjerne dette i norsk offentlighet som digital sikkerhet, digitale trusler og datanettverksoperasjoner. Internasjonalt brukes ofte 'cybersikkerhet' og 'cyber' som innebærer å beskytte alt som er sårbart fordi det er koblet til eller avhengig av informasjons- og kommunikasjonsteknologi (heretter IKT). I praksis blir begrepene i Norge brukt om hverandre. Lysne 1-utvalget valgte i sin utredning å benytte IKT-sikkerhet, men legger til grunn at begrepet er synonymt med cybersikkerhet (Regjeringen, 2015 s.34). På bakgrunn av at oppgaven her baserer seg på et vidt spekter av vitenskapelig litteratur knyttet til cybersikkerhet, ønskes det at oppgaven følger opp i linje med litteraturen som legges til grunn her og benytter begrepet om 'cybersikkerhet' når sikkerheten i 5G-nettet omtales.

1.3 Elektronisk kommunikasjons- og mobilnettverk

For å få et best mulig bilde over sikkerhetsforståelse rundt utrulling av 5G og debatten rundt leverandørvalget og mulige konsekvenser, krever det en kort forklaring om det norske mobile kommunikasjonsnettverket. Dette er tenkt for å øke kunnskapen rundt hva cybersikkerheten i 5G og mobilnettverket innebærer når dette skal analyseres. Nedenfor er en veldig forenklet figur og forklaring gjengitt av informant 7 som er avdelingsdirektør men har også teknisk faglig bakgrunn og kompetanse.



Figur 1: Forenklet figur av et mobilnettverk

> **A** (Kjernenettet): «Det begynner med det som er hjernen eller sånn mer sentralt, det går på intelligensen i nettet, det mobile kjernenettet. Der ligger det nøkkeldata slik at vi ruter samtalen riktig fra A til B. Det er typisk noe som er EKSTREMT kritisk hvis går ned. Så det betyr at vi bygger det med høy grad av redundans. Nå skal jeg være forsiktig med å snakke for mye om redundansen for dette er nasjonal kritisk infrastruktur. Og det blir bygd med helt spesielle type sikkerhetsløsninger rundt det, fordi det er der du virkelig kan gjøre skade».
> **B** (Transportnettet): «Dette nettet er på en måte store blodårer rundt om i kroppen som frakter. Og det og hører til Norges kritiske infrastruktur. Fordi det er 80 prosent av trafikken som går i X sitt nett. Så det er også veldig veldig høyt fokus på sikkerhetsløsninger. Typisk og at du har ulike aktører som da er inne på transportnettet versus det du har på kjernenettet» (diversitet).
> **C** (Radioaksessnettet): «Og så kommer på en måte det som er ytterst og som alle snakker om, det er dette radionettet. Men der er det mer lokalt at noe går ned lokalt. Det er allikevel typisk begrenset geografisk hvis noe går ned der. Og det er da nettverk som er 2G, 4G og 5G. Nettet vil støtte både 2, 4 og 5G og etter 2025 er det 4G og 5G. Her er basestasjonene med antenne».
> (Informant 7)

Med 5G-nettverk menes det i denne oppgaven alle relevante elementer innenfor nettverksinfrastrukturen til mobil og trådløs kommunikasjonsteknologi. Elementene som inngår menes programvare og hardvare som bestanddeler av infrastrukturen. (Europeiske Union, 2019, s.5). I oppgaven så vil betegnelsen '5G-nettverk' brukes når mobilnettverket omtales.

Norske ekom-tjenester har to kapabiliteter. For det første er det evnen til å opprettholde tilgangen til elektroniske kommunikasjonstjenester, samt evne til å raskest mulig å

gjenopprette tilgang ved en svikt. Dette omfatter både kommersielle nett og Nødnett. Sikkerhet i elektronisk kommunikasjon menes derfor evnen til å opprettholde konfidensialitet og integritet i elektronisk kommunikasjon (Direktoratet for Samfunnssikkerhet- og Beredskap, 2016 s.93-94). Oppgaven omfatter sikkerhetsforståelsen knyttet til begge delene, knyttet til å sikre tilgang (hindre nedetid), men også å sikre nettverkene og informasjonen i nettverkene fra etterretning og sabotasje som er en del av cybersikkerheten og slik argumentert og lagt ut om i forrige avsnitt.

1.5 Disposisjon for oppgaven

I kapittel 2 presenteres det teoretiske rammeverket for analysen, henholdsvis sikkerhetiseringsteori og risikoteori samt et begrepsskjema av sentrale begrep som legger til føringer for identifisering av sikkerhetsforståelsen i 5G-debatten. I kapittel 3 vil metoden for analysen gjøres rede for, og der casestudie som valgt forskningsdesign sammen med metodene dokumentanalyse og intervju blir presentert og argumenter for som passende verktøy for å besvare forskningsspørsmålet. Videre vil datainnsamlingen og framgangsmåten for datagrunnlaget for analysen gjøres rede for, og baseres på publiserte tekster og dokument når det gjelder utbygging av 5G-nett i Norge.

Oppgaven vil deretter følge opp med selve analysen i kapittel 4, og som er videre delt inn i to deler. Første delen av analysen tar for seg hvilken sikkerhetsforståelse som har preget debatten ved 5G-utbygging i valget av leverandør. Dette gjøres med å ta i bruk det teoretiske rammeverket Hansen og Nissenbaums (2009) analyse av cybersikkerhetssektoren som en egen sektor innenfor sikkerhet med grunnlag i Buzan, de Wilde og Wæver (1998) Københavnerskolens sikkerhetiseringsteori. Siste delen av analysen vil ta i bruk riskification basert på Corry (2012). Deretter gjøres det i kapittel 5 en diskusjon rundt funnene av analysen, og eventuelle sammenhenger det kan være mellom perspektivene og der det reflekteres over videre forskning innenfor temaet. Deretter følger kapittel 6 med konklusjonen i analysen. Til sist i kapittel 7 diskuteres og reflekteres det over de overordnede begrensninger og svakheter ved analysen gjort her, samt begrensninger og kritikk ved det valgte teoretiske rammeverket. Kapittel 8 vil foreslår muligheter for videre forskning innenfor dette temaet.

2. 0 Det teoretiske rammeverket

Det teoretiske rammeverket baserer seg på sosialkonstruktivistisk tilnærming på sikkerhet og risiko, der det legges til grunn en forståelse av trussel og risiko som sosial konstruert og intersubjektivistisk. Københavnerskolen legger til grunn at det er en talehandling som sikkerhetiserer, og analyserer hvordan temaer innenfor nasjonal- og internasjonal politikk har flyttet på seg til å bli en del av nasjonal sikkerhet, der andre spilleregler gjelder (Buzan de Wilde og Wæver, 1997, s.23-24). Alle først presenteres dette teoretiske perspektivet. Oppgaven her tar derimot utgangspunkt i sikkerhetiseringsteorien, men benytter det utvidede rammeverket til Hansen og Nissenbaum (2009) for hvordan sikkerhetisering innenfor cybersikkerhet (cyber-sikkerhetisering). Deretter presenteres oppgaven den andre alternativet analytiske perspektivet på cybersikkerhet med utgangspunkt i et risikoperspektiv på cybersikkerhet, riskification, for å analysere sikkerhetsforståelsen i 5G-debatten (Corry, 2012, Friis og Reichborn-Kjennerud, 2016). Begge teoretiske tilnærmingene blir i kapittelet her kategorisert til sentrale begreper som skal veilede meg i analysering av uttalelser for identifisering av den norske sikkerhetsforståelsen i 5G-denatten.

2.1 Sikkerhetiseringsteori: Cyber-sikkerhetisering

Sikkerhetiseringsteorien er også et benyttet for å undersøke hvordan og på hvilken måte digitale system og cyberspace har blitt sikkerhetisert gjennom analysering av empiriske case (Hansen og Nissenbaum:2009, Dunn Cavelty: 2007, 2008, 2013). For i tillegg så argumenterer Hansen og Niseenbaum (2009) videre fra Buzan, de Wilde og Wæver (1998) at det er individuelle referanseobjekter som oppretter flere diskurser og at disse mulitiple diskursene heller oppstår gjennom konkurrerende artikuleringer av en gruppe av flere referanseobjekter. På denne måten fanger man bedre opp den sikkerhetiserende og politiske dynamikken innenfor feltet. For om man analyserte cybersikkerheten som inneholdende av flere individuelle fragmenterte diskurser, risikerer man å tone ned de måtene cybersikkerhetsdiskursen får sin helhet gjennom koblinger mellom referanseobjekter enn å se de på som enkelte separate spor.

Spesielt ved diskursen i cybersikkerheten er koblingen mellom «nettverk» og «individ» og menneskelig kollektiv referanseobjekter, og der det «individet» i diskursen er knyttet til sosiale og politiske referanseobjekt. For det spesielle ved en sikkerhetisering av et nettverk er ikke nødvendigvis eller hovedsakelig selve nedetiden eller ødeleggelsene nettverket, men det er gjerne implikasjonene og konsekvensene ved et nettverksammenbrudd har for andre referanseobjekter «samfunnet», «regime» eller «økonomi» og hvordan dette videre er knyttet til «staten» og «samfunnet», som gjør cyber-sikkerhetisering en aktuell kandidat for politisk- og medieoppmerksomhet (Hansen og Nissenbaum, 2009, s.1163). Referanseobjektene blir heller artikulert gjennom at disse blir truet gjennom tre distinkte former for sikkerhetisering innenfor cyber-domenet som kobler referanseobjekter, trusler og sikkerhetiserende aktører sammen: hyper-sikkerhetisering, hverdagslig sikkerhetspraksiser og teknifisering. Disse er også tenkt som et verktøy i analysen for å være med på å bidra til å identifisere sikkerhetsforståelsen i debatten.

For det som blant annet skiller hyper-sikkerhetisering fra den opprinnelige sikkerhetiseringen er kombinasjonen av dens umiddelbare og spill-over eller kaskanderende effekter (følgerhendelser). For når det gjelder sikkerhetisering av selve nettverket, innebærer hyper-sikkerhetiseringen ikke bare sammenbruddet og ødeleggelser i nettverket selv men at ødeleggelser i nettverket vil skape sosiale, finansielle og militære sammenbrudd og dermed involverer alle andre referanseobjekter og sektorer i samfunnet. For eksempel påvirkning eller konsekvensen av et bortfall i mobilnettverket på andre norske samfunnsfunksjoner. Siden sikkerhetisering alltid mobiliserer fremtiden, kombineres med hvordan cyber-sikkerhetisering ikke har lik historie når det gjelder å dra historiske analogier fra tidligere katastrofale hendelser som verktøy for cyber-sikkerhetisering. Kombinasjonen av katastrofale følgerhendelser og bortfall av tidligere hendelser skaper avhengigheten på framtidsutsikter og trusselens alvorlighet, gjør diskursen utsatt for «overdrivelse» (Hansen og Nissenbaum, 2009, s. 1164).

Spesielt innenfor diskurs om cybersikkerhet kan man også finne tilfeller av en hverdagslig sikkerhetisering. Gjennom sikkerhetisering av det hverdagslige digitale livet med siner farer og trusler mot alle som enten eier en digital enhet eller er til gjenstand for digitalisering i samfunnet. Både offentlige og privat aktører mobiliserer, skaper sitt publikum som er bekymret for sin sikkerhet, og mobiliserer vanlige individers erfaringer på to måter: sikre individets partnerskap og etterlevelse av å beskytte nettverkssikkerhet, og gjøre hyper-

sikkerhetisering scenarioer mer troverdige ved å koble elementer fra katastrofescenario to erfaringer kjent fra hverdagslivet (Hansen og Nissenbaum, 2009, s.1165). Gjennom å koble hverdagslige sikkerhetspraksiser til hyper-kaskanderende scenarioer, flyttes cybersikkerhet ut av «bedriftssikkerhet» og «forbrukertillit» og til nasjonal og sosial sikkerhet. (Hansen og Nissenbaum, 2009 s.1166).

Hverdagslige sikkerhetspraksiser legger her vekt på aksept av offentlig sikkerhetsdiskurser kan skje en slik modus, gjennom publikummets opplevde erfaringer i hverdagen. Publikum her tradisjonelt definert av Buzan, de Wilde og Wæver (1998, s.41) som de den sikkerhetiserende handlingen forsøker å overbevise og suksessen av sikkerhetiseringen avhenger nettopp av den sikkerhetiserende aktørs evne til å identifisere seg med publikummets følelser, interesser og behov og at taleren behøver å justere sitt språk til publikummets erfaringer. Publikummet i henhold til Hansen og Nissenbaum (2009, s.1166), er konstituert i diskursen rundt «vi» som det menes man snakker på vegne og «du» samtidig gjennom å koble trykt og trusler til følelser, behov og interesser hos mennesker.

Cybersikkerhet og håndtering av digitale system krever en viss kunnskap om datavitenskap og datasikkerhet enn det som er tilgjengelig for den generelle befolkningen, og innenfor statsvitenskap og sikkerhetsstudier er dette med på å skape et rom for teknisk ekspertise og ekspert-kunnskap i en diskurs (Hansen og Nissenbaum, 2009, s.1166). Gjennom utviklingen av å nye teknologier og metoder for angrep, øker legitimitet til ekspert og autoriteten til tekniske eksperter gjennom kunnskap og kompetanse innenfor datavitenskap og informasjonssikkerhet, og har gitt aktørene autoritet og mulighet til å uttale seg om dette domenet og det ukjente til den generelle befolkning. På denne måten fungerer de som en sikkerhetiserende aktør for cyber-sikkerhetisering som før var tradisjonelt sett var mer forbeholdt politikere og media.

Tabell 1: Moduser (Hansen og Nissenbaum, 2009, s.1164)

Hyper-sikkerhetisering   • Multi-dimensjonale cyber-katastrofale scenarioer med alvorlige trusler i en og samme sekvens, men der ingen så langt har funnet sted.   • Planetens skjebne står på spill   • Irreversible konsekvenser   • Kaskanderende effekter (følgerhendelser) gir kraft til cyber-sikkerhetisering: hastverk og ulike former for politisk intervensjon.
Hverdagslige sikkerhetspraksiser   • Offentlige og private aktører organisasjoner og selskap mobiliserer befolkningen   • Koble hyper-sikkerhetisering til individers hverdagslige og opplevde erfaringer
Teknifisering   • Teknisk og ekspert- diskurs   • Sterk vektlegging på hypotetisk scenario   • Politisk og normativ nøytral

Teknifisering er derfor som en talehandling, som gjør noe gjennom at det konstruerer en sak som avhengig av teknisk eller ekspertkunnskap samtidig som forutsetter en politisk og normativ agenda som teknologi er. Mobilisering av teknifisering innenfor sikkerhetiseringslogikken er en som tillater en spesifikk konstruering av epistemisk autoritet og politisk legitimitet, gjennom at saken krever en viss ekspertise som offentligheten og de fleste politikere ikke har. Dette tillater til at eksperter å bli sikkerhetiserende aktører separat fra politiske aktører (Hansen og Nissenbaum, 2009, s.1167). Det tekniske og sikkerhetiserte behøver ikke å sees på som to motpoler eller to uavhengige former, men er heller arrangert i en kompleks sammenkoblende måter der teknifisering kan også spille en viktig rolle i legitimering av cyber-sikkerhetisering. Teknifisering kan operere både på egen hånd, men også ved å støtte opp under hyper-sikkerhetisering ved å tale med autoritet til offentligheten om viktigheten av hverdagslig sikkerhetspraksiser.

Tabell 1.2: Begrepsskjema over cyber-sikkerhetisering (Utvidet etter Hansen og Nissenbaum (2009))

Sentrale begrep	Beskrivelse av begrepet	Analytiske spørsmål til empirien
Sikkerhetiserende aktør	Sikkerhetiserende aktører som gjennom talehandling talesetter en eksistensiell trussel mot et referanseobjekt og krever ekstraordinære løsninger og tiltak.	Hvem snakker en eksistensiell trussel i 5G-debatten?
Referanseobjekt **Kollektivt referanseobjekt** **Individuelt referanseobjekt**	Objekter som snakkes å være eksistensielt truende og som har et kollektivt, legitimt krav for å overleve.	Hvem og hva er det i det norske samfunn som skal skjermes og bør beskyttes? Nettverket, staten? Norske individer, digitale brukere?
Eksistensiell trussel	Et emne som snakkes om å være en eksistensiell trussel mot et referanseobjekt.	Hva snakkes det om å være trusselen?
Ekstraordinære tiltak	En løsning eller tiltak mot den eksistensielle trussel som overskrider normale politiske prosedyrer og normer.	Hvilke tiltak ble satt i verk i prosessen mot valg av leverandør? Var det unntatt den normale politiske demokratiske prosessen?
Aksept fra relevant publikum	Det relevante publikum som talehandlingen vender seg til, aksepterer bruken av	Hvordan var responsen til myndighetenes tiltak blant

	ekstraordinært tiltak og dermed avgjør om emner/trusler kan sikkerhetiseres.	politiske folkevalgte og eksperter (og media?)

For å få innblikk sikkerhetsforståelsen knyttet til utrullingen av 5G-teknologiens knyttet til den norsk sikkerhetspolitiske debatten rundt leverandørvalg, benyttes Hansen og Nissenbaum (2009, s.1171) analyse av cybersikkerhet som en egen sikkerhetssektor bestående av spesifikke konstellasjoner av trusler og referanseobjekter. Ved å benytte vektlegging på den komplekse sammensetningen av individuelle og kollektive referanseobjekt, muliggjøres det for en identifisering av flere diskurser innenfor samme sektor, og potensielt kunne bidra til å fange opp den politiske dynamikken, som nettopp er kjernen innenfor cybersikkerhet.

2.1.2 Relevante cyber-sikkerhetiseringsaktører i 5G-debatten

Et viktig steg mot analysering og identifisering av sikkerhetsforståelsen mot 5G-nettet, er å avklare hvilke aktører og sektorer som er til gjenstand for analyse her. Som nevnt, så er det i tråd med Buzan, de Wilde og Wæver (1998) sikkerhetiseringsteori flere ulike aktører som forsøker gjennom talehandling å argumentere for at det er en relasjon mellom ulike emner og nasjonal sikkerhet. Her legger sikkerhetiseringsteorien vekt på politisk fremtredende talehandlinger og synlige politiske aktører, noe som førte til analyser basert på offentlige uttalelser og dokument fra statsoverhoder, regjeringsmedlemmer, høytstående embetsmenn og ledere av internasjonale organisasjoner. Hansen og Nissenbaum (2009) utvider dette på bakgrunn i teknifisering, at eksperter også kan være sikkerhetiserende aktører med hvordan cybersikkerheten avhenger av teknisk faglig kunnskap som politiske aktører og offentligheten ikke besitter. Videre hvordan denne rollen kan fungere i legitimeringen av cyber-sikkerhetisering med evnen til å snakke til offentligheten med autoritet om temaet.

I tillegg tar oppgaven her også til ordet for argumentet til Dunn Cavelty (2013, s.106), at det i tillegg er ikke-statlige aktører, spesifikke byråkratiske enheter, konsulenter eller tekniske eksperter som også har kapasitet til å etablere visse forståelser om trusler og sikkerhetsutfordringer, og ikke bare den politiske eller tekniske elite. Ved å bare inkludere de

mest synlige elite-aktørene, får man ikke inkludert de mindre synlige aktørene som også er deltakende med å forme debatten og cybersikkerheten knyttet til 5G i Norge, og kan bidra til en mer nyansert og helhetlig analyse av sikkerhetsforståelsen. På bakgrunn av dette utvides rommet for definering og inkludering av potensielle sikkerhetiserende aktører som statsminister, statsråder, embetsmenn, elitepolitikere til også gjelde eksperter og tekniske eksperter innenfor cybersikkerhet, digital infrastruktur og elektronisk kommunikasjon blant annet.

2.2 Risikoteori: Riskification

Flere argumenterer for at risiko er den nye sikkerheten, med en transformasjon fra sikkerhet til risiko eller at konseptet om sikkerhet og trussel og forsvar også inkluderer konsepter om risiko. I tillegg vises til at sikkerhetspraksiser i økende grad handler om forebygging, sannsynligheter og mulige fremtidige scenarioer og håndtere diffuse risikoer enn avskrekkelse eller forsvar seg mot identifiserbare og akutte trusler (Corry, 2012, s. 236). Det vises til at det eksisterer flere tilfeller av forsøk på sikkerhetisering, men som sjeldent har resultert i ekstraordinære mottiltak slik sikkerhetisering legger opp til. Samtidig er det empirisk bevis på den økende viktigheten av cybersikkerhet og at det praktiseres på nasjonalt nivå viser at cybersikkerheten har blitt en viktig del i det moderne samfunnet, selv om det argumenteres mot at det ikke har blitt sikkerhetisert. På bakgrunn av dette argumenteres det for riskification som en alternativ analytisk modell kan være med på å gi et mer nøyaktig bilde av cybersikkerheten og dagens sikkerhetsutfordringer enn sikkerhetisering (Friis og Reichborn-Kjennerud, 2016, s.27). Oppgaven her baserer seg på Friis og Reichborn-Kjennerud (2016) argumentering for riskification som et alternativ analyserammeverk for å forstå cybersikkerhet. Spesifikt tar oppgaven utgangspunkt i Corrys (2012, s.249) identifisering av tre sentrale begrepet og karakteristikker ved riskification: konstituerende kausalitet (heretter bakenforliggende faktorer), styresett og langsiktighet. Disse sentrale begrepene ved perspektivet benyttes i oppgaven her som del av å analysere hva som er sikkerhetsforståelsen i 5G-debatten.

Det argumenteres for dette risikoperspektivet et passende perspektiv innenfor cybersikkerhet, da faren for et cyberangrep heller burde sees på som en bakenforliggende årsak enn en direkte årsak til skade som typisk innenfor sikkerhetisering. For det er ikke bare intensjonen og

kapasitetene til aktør alene som gjør handling mulig, men hvordan bakgrunnsfaktorer som avhengighet til og mellom digitale system og teknologi, sårbarheter i teknologi og systemenes motstandsdyktighet er med på å sannsynliggjøre en uønsket hendelse (Friis og Reichborn-Kjennerud, 2016, s. 28). Dette fører til et større fokus på de materielle og diskursive former for bakgrunnsfaktorer som gjør visse uønskede hendelser sannsynlig, og gir mulighet til å inkludere mer aktivt cyberdomenet med alle sine bestanddeler i analysen (Corry, 2012, s. 246). Dette innebærer ikke en materiell determinisme, men at faktorene som utgjør en risiko for cyberangrep ikke bare bestemt ut fra en materiell dimensjon, men spiller en aktiv del i den sosiale dimensjonen som den politiske praksisen og cybersikkerheten (Friis og Reichborn-Kjennerud, 2016, s. 38).

For et cyberangrep blir oftest ikke betraktet som en umiddelbar trussel men en vedvarende risiko og et mulig scenario, da typisk at et cyberangrep vanligvis bli ikke oppdaget før etter at den har blitt lansert i systemet. Dette er ved hvordan at aktører vanligvis benytter ukjente sårbarheter som gjør at man ikke har den samme muligheten til å identifisere en trussel eller et kommende angrep. Derfor baserer cybersikkerhet seg hovedsakelig om styring og håndtering, og ikke å hindre en mulig skade. For i motsetning til sikkerhetiseringsteoriens fokus på å beskytte et referanseobjekt mot en fremtidig fare, innebærer riskification å håndtere og styre bakgrunnen for en fremtidig fare (Corry, 2012: 247). Fokuset er heller innover internt rettet mot referanseobjektet selv, imot sårbarheter og håndtere gjennom å styrke selve referanseobjektet gjennom resiliens. Videre med også å identifisere sårbarheter, beregne sannsynlighet og risiko samt oppgradering av programvare «patching» (Friis og Reichborn-Kjennerud, 2016:38)

På bakgrunn av dette fører dette til en forståelse av cybersikkerheten som innebærer et behov for langsiktig føre var-styring enn at det implementeres kortsiktige eksepsjonelle styringstiltak (Corry, 2012, s.248). Utfordringen ved trusselen om et cyberangrep er at man aldri kan være helt sikre på hvor systemet angripes eller hva man skal se etter før man oppdager tilstedeværelse av skadevare. Cybersikkerheten er i tillegg preget av et komplekst samarbeid mellom forskjellig aktører der ulike interesser, perspektiv og politiske mål som utfordrer og er preget av myke tiltak, langsiktige investeringer, forebygging for redusering av sårbarheter og risiko og ikke beskyttelse mot angrep (Friis og Reichborn-Kjennerud, 2016, s.39).

Tabell 2.0 Begrepsskjema riskification (Etter Corry, 2012, s.249 og supplert med Friis og Reichborn-Kjennerud 2016)

Sentrale begrep	Beskrivelse av begrepet	Analytiske spørsmål til empirien
Bakenforliggende forhold som sannsynligheten for angrep	Bakgrunnsfaktorer som muliggjør handling: Avhengighet av og mellom digitale system og teknologi, sårbarhet, motstandsdyktighet. Kompleksitet, Sannsynlighetskalkulering.	Snakkes det om teknologiske sårbarheter? Snakkes det om teknologi og det mobile nettverket? Avhengig av 5G-nettet? Hvor viktig blir 5G? I hvilken grad kan man beregne risiko i 5G-teknologi?
Styring	Styre og ikke forhindre skade. Styring rettet innover mot sårbarheter. Styre gjennom resiliens: Styrke referanseobjektet	Vektlegges cybersikkerheten i saken på risikoreduserende tiltak? Er det fokus på å redusere sårbarheter? Fokuseres det på 5G-nettets evne å håndtere hendelser og eller nedetid?
Langsiktighet	Forebyggende tiltak og føre-var-prinsipp: sikkerhetsmargin (Corry, 2012, s.249)	Ble det iverksatt langsiktige tiltak?

	Vektlegging av myke tiltak (Friis og Reichborn-Kjennerud, 2016, s. 39)	Legges det vekt på beste praksis, standarder, holdningsbygging.

Selv om det er tre ulike vitenskapelige tilnærminger på risikostudier, så her omfatter oppgaven her en sosiologisk- konstruktivistiske tilnærming der studier baserer hovedsakelig på to risiko-teoretikere Foucaults «Governmentality» og Ulrich Becks «Globale Risikosamfunn» (Petersen, 2011, s.699). Governmentality-tilnærmingen søker etter å hvordan avgjørelser i risikostyring og sikkerhetspolitikk innebærer enn viss politikk og politisk makt. Her er det empiriske fokuset rettet mot risikostyring i daglig praksis med kritisk fokus mot økonomi og neoliberalistisk praksis som en del av den moderne sikkerhetspolitikk (Petersen, 2011, Aradau og Van- Münster, 2007). Risiko her innebærer ulike måter den klassifisert, kvantifisert og til en viss grad forutsett. Dette innebærer derfor ulike verktøy og kunnskap myndigheter tar i bruk, i forsøk på å beregne fremtidige hendelser med mål om å kontrollere og minimere hendelsers mulige skadelige og ødeleggende konsekvenser (Aradau og Lobo-Guerrero, 2008, s.149). Her innebærer risiko en spesifikk rasjonalitet innebærende hos myndighet legitimering av visse verktøy og makter hos myndigheter av forskjellige institusjoner (Corry, 2012, s. 242-243).

Ulrich Becks risikosamfunn argumenterer for at samfunnet har beveget seg fra første modernitet til andre modernitet, og hvordan man har gått fra en persepsjon av risiko som beregnelig og håndterbar til det globale risikosamfunnet som er ukontrollerbar, ikke-beregnelig og med uintenderte konsekvenser av samfunnets stadige modernisering og tidligere beslutninger (Petersen, 2011, s.700). Samfunn må i større grad håndtere og forebygge risiko som den selv har produsert, der den teknologiske utvikling og modernisering har ført til begrenset kunnskap og vitenskap om fremtidige hendelser, og at samfunn har blitt refleksive på den måten at det moderne samfunn står selv for produsering av nye og videre risiko (Corry, 2012, s.241-242). Disse forskjellige synspunktene og perspektivene synes å kunne være viktig i denne analysen av 5G-debatten. Dette er på bakgrunn av analysens

identifisering av en risikologikk og derfor evnen til å identifisere og beregne risikoer knyttet til 5G-leverandøren og 5G-teknologien.

Ved å inkludere riskification som teoretisk rammeverk legges det inn en ekstra analytisk kategori mellom sikkerhetisering og politisering, noe som åpner opp for en mer nyansert analyse av 5G-debatten. Dette gjennom å i større grad analysere variasjonen i de ulike potensielle sikkerhetsforståelsene som måtte prege debatten, måten saken ble håndtert på men også norsk cybersikkerhetspraksis innenfor telekom og mobilnettverk (Friis og Reichborn-Kjennerud, 2016, s.39). Risikoperspektivet legge forventninger om at debatten og diskursen rundt 5G-utbygging vektlegger sikkerhetsutfordringer rundt sårbarheter i programvare og hardvare, mulighet for beregning av risiko for at disse kan utnyttes. Videre vil debatten kunne synliggjøre det komplekse offentlig-private samarbeidet mellom flere aktører innenfor cybersikkerheten.

3.0 Metode

Dette kapittelet tar for seg forskningsdesignet og den metodiske tilnærmingen for gjennomføring av analysen. For å transformere de teoretiske rammene og forventningene som er valgt for analysen her, spiller de metodiske valgene en kritisk rolle, og stiller forventninger for de muligheter og begrensninger for det som kan analyseres her. For at forskning skal reliabelt og valid, må valg av metode være konsistent og logisk med metodologien samt den ontologiske og epistemologiske antagelser. Først vil det gjøres rede for forskningsstrategien og forskningsdesignet for oppgaven. Så vil det videre argumenteres for hvorfor intervju og dokumentanalyse metoder som ble valgt for å belyse og svare på problemstillingen her. Til slutt diskuteres og reflekteres det over valideten og reliabiliteten for denne studien. Inngående og videre drøfting og kritikk av den metodiske tilnærmingen her blir gjennomgått i kapittel X i denne oppgaven.

Forskningsspørsmålet i denne oppgaven ønsker å oppnå en størst mulig inngående forståelse rundt hva som er den norske sikkerhetsforståelsen rundt 5G-debatten i Norge. På bakgrunn av dette tar oppgaven her en fortolkende forskningsvitenskapelig tilnærming på analysen. Den fortolkende tilnærming og kjennetegnes legger vekt på at nettopp søkes å forstå menneskelig atferd, som for eksempel den norske sikkerhetsforståelsen (Bryman, 2016, s.26). Tilnærmingen søker etter å forstå en sak eller ting ved å lære hva det gjør, hvordan spesifikke

mennesker bruker det, i meninger og i spesifikke kontekster, enn å generalisere denne meninger dette utover akkurat denne konteksten. Den legger vekt på hvordan bruk av ord eller annen handlinger kan potensielt fortelle eller stille spørsmål om antatte verdier, forståelse eller følelser om hva som er for eksempel er tilfredsstillende sikkerhet, sikkerhetsutfordringer mot 5G-nettet eller hva som anses som norsk kritisk infrastruktur eller grunnleggende nasjonale funksjoner. Eller enda viktigere, hva kan en sikkerhetsforståelse rundt 5G-debatten fortelle om hvordan verden og Norge har blitt og som vi nå lever og er en del av (Schartz-Shea et al., 2012, s.23). Dermed spiller aktørenes subjektive tolkninger av verden rundt oss en hovedrolle for denne analysen, i tråd med tilnærmingens ønske om avdekking av intensjoner, meninger og vektlegging av kontekst ved en spesifikk sak eller hendelse. For å være i stand til å analysere dette, sees det som nødvendig å få tilgang til relevante og deltakende aktører i debatten og sikkerheten i 5G-nettverkets subjektive forståelser og meninger knyttet til dette. For med sikkerhetiseringsteoriens og risikoteorien vektlegging på sosial-konstruktivisme og en intersubjektivitet bak forståelsen av hva som anses som et sikkerhetsproblem. Dette krever at teoriene også må analyseres i samhold med dette. Sammenlagt legger dette videre føringer for valg av forskningsdesign, metoden, validiteten og reliabilitet for studien, og som gjøres rede for videre i kapittelet her.

Analysen legger derfor opp til en kvalitativ forskningsstrategi fokuserer også på spesifikke individer, hendelser og kontekst og lener seg mot en ideografisk analysestil, i motsetning der det kvantitative fokuserer mer på funksjoner som kan generaliseres til en større populasjon (Gerring, 2017:18). Prosjektet her legger derfor også opp til en intensiv forskningsstrategi der søkes etter å gå i dybden når det gjelder informasjon ved denne enheten innenfor denne saken og legger ikke direkte opp til generalisering til flere antall enheter utover Norge (Hellevik, 2011:95). Denne strategien sees på som passende da den er kongruent med forskningsspørsmålet som søker etter en større dypgående kunnskap og viten av en hendelse (Levy, 2008: 2).

3.1 Forskningsdesignet

Studiens forskningsdesign er ett deskriptivt kvalitativ single-casestudie av den norske sikkerhetsforståelsen knyttet til debatten om 5G-utbyggingen i Norge og i valget av leverandør av denne teknologien, med Norge som eneste enhet i analysen (Gerring, 2004, s. 342). Designet her kjennetegnes som ideografisk, der problemstillingen ønsker å beskrive, forklare, tolke og forstå ett enkelt case som et mål i seg selv, enn at dette skal være et verktøy for å utvikle bredere teoretiske generaliseringer (Levy, 2008, s.4, Hellevik, 2011, s.88). Den setter for seg et element av deskriptiv analyse ved å analysere variasjon internt en enhet i form av kompleksiteten og spesielle ved akkurat dette sakskomplekset, enn å søke etter variasjon og forklaringskraft gjennom kausale sammenhenger (Gerring, 2004, s.347). Forskningsspørsmålets mål er å kunne generere kunnskap gjennom en mest mulig inngående og dypest mulig beskrivelse av den norske sikkerhetsforståelsen knyttet til 5G-debatten, enn å søke forklaringskraft gjennom variasjon mellom enheter eller generalisering til et større antall enheter (Bryman, 2016, s.60).

Designet inneholder i tillegg et deduktivt element og er teoridrevet ved at det gås deduktivt til empirien, gjennom å ta utgangspunktet i det teoretiske rammeverket der stiller spesifikke teoretiske forventninger og som strukturerer datainnsamlingen og analysen, med formål om å gi et tilfredsstillende valid funn på forskningsspørsmålet (Bryman, 2016, s.21). Gjennom å legge vekt på eksplisitt og strukturert bruk av teori for å forklare dette spesifikke case, kan dette bidra til mer valide forklaringer og forståelser for viktige og avgjørende aspekt ved dette case enn ved bruk av mindre strukturerte analyser. Det er derfor analysen her benytter seg av en metodetriangulering, for å nettopp gjøre meg i stand til å gjennomføre dette. For jo mer et case blir veiledet av teori, jo i større grad kan teorienes underliggende analytiske forutsetninger, de eventuelle normative skjevheter og kausale proposisjoner, dess færre logiske motsetninger og lettere er det å empiriske validere eller invalidere disse forutsetningene teoriene bygger på (Levy, 2008, s.5). Videre argumentering for dette gjennomgås i neste avsnitt. For ved å fokusere på ett case med Norge som eneste enhet, kan man gå mer detaljert til verks i sikkerhetslogikkenes antagelser og analytiske forutsetninger, men også dens sosial-konstruktivistiske tilnærming til cybersikkerhet, risiko i det moderne norske samfunn.

Det kan selvsagt stilles spørsmål rundt hva en deskriptiv casestudie av en enkelt enhet kan bidra til å forklare. På bakgrunn av hvordan studien omfatter et tema som ikke er så mye studert før, kan dette være en viktig første steg i videre studier som gjøres innenfor cybersikkerhet i Norge men også videre i en komparativ sammenheng på et senere tidspunkt.

3.2 Metodetriangulering

Datagrunnlaget for analysen basere seg her på et mer heterogent av kilder med mål om å kunne på en best mulig måte belyse og analysere forskjellige aspekter rundt sikkerhetsforståelsen i 5G-debatten. Det legges her opp til at analysen av sikkerhetsforståelsen studeres, gjennom å kombinere to ulike metoder og datakilder for å kunne være i stand til å gi et bredere datagrunnlag og derfor bedre og sikrere basis for å kunne identifisere sikkerhetslogikker (Jacobsen, 2007, s.29). Derfor vil ønskes det her å belyse og svare på problemformuleringen gjennom et bredere datagrunnlag ved å supplere metoden gjennom å også legge til intervjumateriale som en del av datagrunnlaget for analyse. Oppgaven kombinere derfor dokumentanalyse av tekstmateriale om denne saken, men med at dette også suppleres med empiri generert gjennom elite- og ekspertintervju som ble gjennomført i etterkant av valget av 5G-leverandør var gjort.

For med sikkerhetiseringslogikken antagelser om talehandling og metodologiske tilgang til hvordan denne talehandlingen studeres og analyseres. Den opprinnelige sikkerhetiseringsteorien har derfor betraktet offentlige uttalelser relevante datamaterialet for en analyse av sikkerhetisering. Jeg har allerede argumentert under teorikapittelet for hvordan relevante analysepersoner og sikkerhetiseringsaktører utvides for denne analysen, men det ønskes her å argumentere for hvorfor intervjudata inkluderes som datagrunnlag i oppgaven her. Intervjudata brukes her som supplerende data for å gjøre et bredere tolkningsgrunnlag på en slik måte at det støtter meg som analytiker i tolkningen av de uttalelsene som gjøres i datamaterialet og dermed bidra til å øke validiteten til den tolkningen som gjøres. For eksempel så kan det å kombinere dokumenter og intervju om det samme emnet kan være med på å vurdere kildenes, uttalelsenes og ordenes troverdighet (Repstad, 2007, s.106-107). Videre kan for eksempel kan man i større grad sammenholde det folk sier med det de gjør og faktisk mener det de sier (Repstad, 2007, s.109). Et passende eksempel hentet fra et av intervjuene med en avdelingsdirektør for et norske mobilselskap: *«Det er sensitivt fordi det er veldig*

mange meninger og oppfattelser, derfor så syns jeg det er fint at du skriver oppgaven din. Og samtidig så er (selskap X) veldig sånn tydelig på det at vi har en veldig sånn standard meldinger på alle spørsmål på dette her, så det er nesten som å trykke på knappen og så kommer den samme meldingen utover: vi leverer på lovverk og lalalala» (informant 7). Dette er et eksempel på hva det kan innebære å fokusere utelukkende på offentlige uttalelser. I prosessen med å hente ut og gått igjennom datamateriale, så ble det observert hvordan selskapets offentlige uttalelser på tvers av artikler, i all hovedsak snakker om selskapet ansvar knyttet til norsk lovverk og sikkerhetslov.

I tillegg så ønskes det å ta argumentet til Hansen og Nissenbaum (2009) på alvor, nettopp at det er innenfor cybersikkerhet ved vidt spekter av mennesker som forsøker å påvirke diskursen som føres, men at det også er flere ulike aktører i ulike posisjoner som utgjør cybersikkerheten. Ved å da inkludere innsikt fra intervju kan det gi mulighet til å få tilgang til mer inngående informasjon og forståelse om hendelsen i sin samtidig av personer som har vært involvert i prosessen, og som hadde vært utilgjengelig på andre måter og i andre datakilder (Lynch, 2013, s.32). Det er derfor informantene som ble valgt ut for intervju på en eller annen måte har vært delaktig i debatten, har ansvaret med enten sikkerheten eller teknologien knyttet til utrullingen av 5G og/eller har ansvaret for den digitale nasjonale sikkerheten. Ved å derfor triangulere med dokumenter og intervju, har man mulighet til å få mest mulig inngående og detaljert kunnskap om denne saken samtidig som å kunne støtte opp under min tolkning og funn i analysen.

Dette synes å kunne relateres til hvordan man kan komme til ha lett for å tolke tekstene ut ifra begrepsforståelser og tenkemåter som er blitt til etter at teksten har blitt laget og publisert Repstad (2007, s.105). Ved at oppgaven legger opp til en analyse av en case fra nåtid gjennom de sentrale begrep ved teoriene som ble utviklet en lengre tid tilbake. Ved å triangulere med dokumenter fra 2018-2019/2020 sammen med intervju fra 2020, tenkes det dette kan også bidra til å vise en eventuell fit eller misfit ved de teoretiske perspektivene og det caset de er satt til å forklare. Uten at dette er en del av forskningsspørsmålet, at dette kan være med på å sette lys på teoretiske rammeverk fra fortiden, kan forklare sikkerhetsutfordringer i dagens og morgendagens moderne verdenssamfunn.

3.3 Dokumentanalyse

På bakgrunn av både den vitenskapelige posisjonen oppgaven har sammen med forskningsdesignet, sees det som at en dokumentanalyse, da det sees på som mest kongruent med både det teoretiske rammeverkets sosial-konstruktivistiske og intersubjektivistiske tilnærmingen på sikkerhet (Buzan, de Wilde og Wæver, 1998, Hansen og Nissenbaum, 2009, Corry, 2012).

For i sikkerhetiseringsteorien følger med et eget analytisk rammeverk, inneholdende sentrale begrep eller komponenter for karakteriserer tilfeller av sikkerhetisering og som synes å måtte være til stede for at det skal sies å være en vellykket sikkerhetisering. Måten å studere tilfeller av sikkerhetisering er at den studeres direkte i diskursen og politiske konstellasjoner, og behøver ingen indikatorer (Buzan, de Wilde og Wæver. 1998, s.25). For tråd med sosial-konstruktivismens prinsipper kan jeg ikke bare observerer «sikkerhetsforståelse» i verden rundt meg, men at verden er grunnleggende subjektiv og avhengig av å tolkes for å forstås. Derfor er forskerens oppgave å forstå hvordan aktører forstår seg selv og den situasjonen, og hvorfor de handler som de gjør, gjennom språk (Bratberg, 2018, s.19). Det sees derfor som hensiktsmessig å henvende seg til språkuttalelser i publisert tekstmateriale og videomateriale.

I tillegg så setter forskningsspørsmålet for seg et ønske mål om å analysere sikkerhetsforståelse i lys av to sikkerhetslogikker, nemlig sikkerhetisering og riskification og gjennom deres analytiske rammeverk vil disse legges over og guide meg i analysering av tekstmaterialet. Det er sikkerhetslogikken som skal identifiseres og ikke noen kollektive virkelighetsoppfatninger eller bakenforliggende ideer bak aktørenes talehandlinger eller uttalelser som ønskes å analyseres her. Derfor sees dokumentanalyse som det mest anvendelige for det formålet her. Analysen her tar derfor ikke i bruk diskursanalyse, i tråd med for eksempel Hansen (2016), som metode for å belyse forskningsspørsmålet og blir reflektert mer under kapittel 7. Spesifikt så gjøres det en kvalitativ innholdsanalyse som setter for seg å undersøke temaer i materialet som analyseres, og hvordan disse temaene blir illustrert gjennom bruk av sitater i dokumentmaterialet eller intervju (Bryman, 2016, s.563).

Dette baseres på antagelsen om at det aktører sier eller uttaler seg om for eksempel i et intervju kan reduseres til et sett færre temaer eller kategorier (Jacobsen, 2005, s.193).

Data fra både dokumentene og intervjumaterialet i oppgaven vil derfor grupperes innenfor disse oppstilte sentrale begrep. Kategoriene i oppgavene her er deduktiv fundert i teoretiske rammeverket og begrepsskjemaet, og vil bidra til å identifisere tilfeller av sikkerhetisering og

riskification. I tillegg gjøre meg i stand til å forenkle datamaterialet men også kategorisere data som omhandler samme temaet på tvers av dokumenter og intervju.
Kategoriene vil også muliggjøre å ikke bare sammenligne det som blir sagt, men også sammenligne de teoretiske rammeverkene på en tydeligere måte. I tillegg ble det utarbeidet en beskrivelse av kategorienes innhold for å konkretisere kategoriene og begrepenes betydning og mening nærmere (Jacobsen, 2005, s.195). Avsnittet om kodingen går videre inn på hvordan tekstmaterialet ble kodet og dermed tilordnet til de ulike kategoriene i begrepsskjemaet.

3.3.1 Dokumenttyper

Derfor i tråd med den kvalitative forskningsstrategiens språkbasert tilnærming til innsamling av kvalitativ data og dokumentanalysens prinsipper som forskningsmetode, gis her tekstmaterialer (både tekst og video) status som kilde eller data for selve undersøkelsen (Repstad, 2007s. 77). I valget om hvilket tekstmateriale som var relevant for analysen, var det for det første viktig å majoriteten av tekstene ble utformet under tidsperioden analysen her er satt til å analysere, men at det også kan inkludere mer historisk materialet som omhandler nettopp det analysen setter for seg å analysere. For det andre burde datamaterialet også inkludere tekster som blir hyppig sitert til (Hansen, 2006, s.82). Det empiriske datagrunnlaget for analysen strekker seg bredt og blir grovt inndelt i ulike type dokumenter. Dette er også fordi det ønskes å undersøke 5G-debatten i en brede forstand ikke bare som politisk debatt forbeholdt den politiske elite og aktører i visse sosiale posisjoner. Analysen baseres på mer sekundær data i form av publiserte nyhetsartikler, nyhetsinnslag, kronikker, offentlig seminar/debatt og offentlige utredninger (Repstad, 2007, s.106).

Nyhetsartikler trekkes ut gjennom søkemotorene i Retriever og Google Scholar og er hovedsakelig: NRK, Tv2, Dagbladet, Dagens Næringsliv, E24 og Tek.no. Overraskende var det mange artikler fra både tek.no og E24, noe som muligens har med at saken i stor grad omfatter teknologi og næringsliv. Likevel, så ble det oppdaget i gjennomlesningen at både E24 og tek.no refereres til og publiseres av blant annet Dagbladet og Dagens Næringsliv. Gruppe to av type tekstmateriale, også relatert til ovenfor, er transkribert film- og nyhetsklipp hovedsakelig fra NRK: Dagsrevyen, Urix og Debatten. I tillegg så ble det transkribert et

NUPI-seminar knyttet til debatten om Huawei er en risiko eller ikke og er publisert offentlig på YouTube. Til stede på seminaret var det også flere nasjonale medier.

Videre er det en gruppe med dokumenter som offentlige utredninger og rapporter, risikovurderingen og trusselvurderinger. Dette er gjerne tekster som refereres til av blant annet nyhetsmedier og andre i debatten, og kan derfor bidra til å fungere som slags noder i form av intertekstualitet i debatten og bidra til å analysere en potensiell intersubjektivitet i konstruering av en felles forståelse av en eksistensiell trussel i en eventuell sikkerhetisering. I tillegg inkluderes interne saksdokumenter jeg fikk tilsendt Kommunal- og Moderniseringsdepartementet knyttet til deres saksprosess om utbyggingen av 5G-nettet i Norge og prosessen mot at mobiloperatørene skulle velge utstyrsleverandør. Disse dokumentene strekker seg fra tidsperioden november 2018 til januar 2020, og blir brukt for å støtte opp under offentlige utsagn i debatten og i intervju. Utover dette blir det også foretatt en triangulering med egen generert empirisk materiale, som er semi-strukturert elite- og ekspertintervju. Dette blir nærmere gjennomgått under intervjukapittelet lengre ned.

I følge Hansen (2006, s.82) er en poststrukturalistisk diskursanalyse gir den en epistemologisk og metodologisk prioritet for å studere tekster som er mer offisielle, som uttalelser fra statsoverhoder, taler og intervju i forbindelse med den førende offisielle offentlig politikken. Videre er det også politiske og parlamentariske debatter, men også reportasjer, leder eller kronikk i media. Likevel presiserer hun dette ikke betyr at andre sekundær kilder ikke har plass i en diskursanalyse. Sekundære tekster kan bidra til viktig kunnskap men også stille kritiske til objektiviteten og naturligheten av hvordan saker representeres. For mer sekundære kilder kan også ende opp med å bli en slags primærkilde når det gjelder hvor hyppig teksten blir referert til av andre (Hansen, 2006, s.83). For eksempel hvordan den offentlige utredningen til Lysne 1-utvalget og Lysnes bok *The Huawei and Snowden Questions* nevnes ofte offentlig men også hos informanter.

Likevel er ikke diskursanalyse som er tenkt gjennomført her, da forskningsspørsmålet ikke er ute etter en analyse av den offentlige diskursen eller debatten etter hva som er Norges offisielle sikkerhetsforståelse som sin offisielle cyberpolitikk. Derimot søkes det her å undersøke sikkerhetsforståelsens på tvers av aktører som inngår i og har ansvar for norsk cybersikkerhet, og ønsker derfor å analysere 5G-debatten i bredere forstand. På bakgrunn av dette er det lagt til grunn et bredt definere datamaterialet her, som vil det variere det når det

kommer til meningsinnholdet i de ulike type tekstene. Det vil variere fra en kronikk, nyhetsartikkel skrevet av mediene selv men også debatter. Målet er at dette kan bidra til å få et mest mulig helt bilde av 5G-debatten, men også i større grad fange opp alle deltakende potensielle sikkerhetiseringsaktører slik Hansen og Nissenbaum (2009) legger fram som typisk for cybersikkerheten samt de ulike måtene sikkerhetsutfordringene i 5G-utbyggingen forstås.

3.3.2 Datainnsamling

Datamaterialet av både tekster og video er avgrenset innenfor en viss kontekst til valget av leverandør for 5G-nettet og diskusjonen rundt Huawei som mulig leverandør. Kilder fra fortiden kan lett bli feiltolket dersom man ikke kjenner konteksten de ble til i, og at det bør gjøres en vurdering av kildenes intensjon og funksjon i sin samtid (Repstad, 2007, s.105). Forskningsspørsmålet setter for seg en analyse av teknologi om 5G og mobilnettverk i en viss kontekst om sikkerheten og en sikkerhetsforståelse. For ved uthenting av relevant data, er man prisgitt til hvilke artikler og data som gis etter hvilke søkeord jeg velger. Det ble forsøkt med variasjon av ulike søkeord for å se hvor ulike søkeresultatene ble. Dette kan argumenteres å ha påvirkning på studiens reliabilitet, da denne analysen og funn baseres på uttalelser og forståelser gjennom et visst utvalg av artikler og nyhetsinnslag. Det ble gjort trekking av dokumentmaterialet gjennomført gjennom søkemotorer som Retriever og Google Scholar, som representerte datamaterialet basert på mine valgte søkeord. Utover det ble det også gått til de største nasjonale nyhetsmediene og gjorde søk der i tillegg på tilsvarende søkeord.

For det første ble raskt lagt merke til hvordan 5G finnes i ulike kontekster, og derfor måtte jeg legge til søkeord som «sikkerhet» og «Norge» for å spesifisere hvilken kontekst jeg ønsket at tekstene skulle omhandle. På bakgrunn av jeg ønsker å analysere den norske sikkerhetsforståelsen, valgte jeg å legge til «Norge» for å ekskludere mest mulig saker om for eksempel 5G, USA og president Donald Trump noe som forskningsspørsmålet ikke er ute etter å analysere. Ved å bare søke med ordene «5G», «Sikkerhet» og «Norge» fikk jeg presentert et veldig lite utvalg av tekstmateriale. Når jeg derimot la til søkeord som «Huawei» og «Kina» økte søkeresultatet betraktelig. I utgangspunktet så var ikke dette ønskelig, da jeg ikke ønsker et skjevt utvalg med tanke på at jeg ønsker at det teoretiske rammeverket skal identifisere i hvilken grad, når og på ulike måter Kina og Huawei eventuelt snakkes om. Så

ved tanken ved å utelate de to søkeordene, så tenktes det at man kunne favne om bredere og være åpen for at andre forståelser utover Kina og Huawei. Siden søkeresultatet ble så magert, så ble det bestemt for å bruke disse søkeordene sammen: «5G», «Sikkerhet», «Norge», «Kina» og «Huawei». Det ble også foretatt noen søk der «NSM», «PST».

Mindre regionale og lokale nyhetsartikler ble ikke inkludert i analysen. I denne gruppen er det også én kronikk som ble publisert på tv2.no, men der tv2 også publiserte samme dag en sak om samme temaet og refererte også til kronikken. Det var også publisert blogginnlegg på mer tekniske nettsteder, men disse ble ikke tatt ut for koding og analyse. For det første var det fordi det ble satt en grense at bare de større nasjonale mediene ble inkludert. Og for det andre fordi forskningsspørsmålet ønsker å fange opp sikkerhetsforståelsen hos personer som på et eller annet vis er involvert og har ansvaret for sikkerheten i mobilnettverket

3.4 Intervju: Elite- og ekspertintervju

På bakgrunn av at forskningsspørsmålet søker etter å inngående kunnskap om en «forståelse» rundt sikkerheten i 5G-utbyggingen sees det om logisk at intervju er en tilfredsstillende metode for å samle inn kunnskap den norske sikkerhetsforståelsen rundt 5G.
Dette er også i tråd med den epistemologiske posisjonen for oppgaven her, der virkeligheten kun kan forståelse gjennom aktørers subjektive oppfattelse av virkeligheten rundt dem. Jeg er her interessert i å få tilgang til aktørenes subjektive forståelse og meninger rundt denne saken, og erkjenner at det er ikke objekt sannhet, noe som hverken er formålet her eller som intervju kan sies å være en kilde til.

Jeg foretok derfor elite- og ekspertintervju, der eliten forstås i oppgaven her som personer som intervjues har ekspert-kunnskap om et emne uavhengig om personen er teknisk sett «elite» på en sosiopolitisk måte (Leech et al., 2013, s.210). Noen informanter sees også på som elite i form av deres direktør-rolle som en innflytelsesrik posisjon for den sikkerheten som føres og/eller i prosessen med leverandørvalget for 5G-nettverket. Eliteintervju sees på som passende når det handler om eksisterende spesifikke case og hendelser, men også når det skal hentes ut systematisk informasjon om aktørers faktiske handlinger i en spesifikk situasjon. Det at forskningsspørsmålet og da temaet for intervjuet omhandler en konkret case, gjør at man kan fokusere på informantenes styrke, ved at de vet hva de gjorde i et bestemt

tilfelle (Beckmann og Hall, 2013, s. 198). Ved å fokusere på en faktisk og konkret hendelse får intervjuer i større grad fanget opp respondentens hukommelse av hendelse men også personen eller organisasjonens rolle innenfor denne saken, og på den måten øke validiteten til det utrykkes fra informantene.

3.4.1 Intervjuform

Elite- og ekspertintervjuene baserer seg på semi-strukturert intervjuform der det stilles relativt åpne spørsmål, noe som åpner opp for at informantene kan svare på en utfyllende måte (Leech et al., 2013). Elite-personer og andre høyt utdannede mennesker skal tilsynelatende ikke å bli satt i bås, men heller ha mulighet til å artikulere sine perspektiv og forklare hvorfor de tenker som gjør og handlet på den måten de gjorde. Ved at det stilles noen spørsmål får jeg likevel muligheten til å få kunnskap som er relevant for forskningsspørsmålet her, samtidig som jeg og får uttalelser om deres forståelse rundt case som jeg ikke i like stor grad kunne fått tilgang til gjennom uttalelser tekstmaterialet. Dette er også fordi forskningsspørsmålet legger opp til å studere mest mulig variasjon innenfor den norske sikkerhetsforståelsen, og ønsker derfor å være mest mulig åpen for at informantene skal ha mulighet til å fortelle meg noe man ikke visste om før eller har tilgang til gjennom andre kilder. Denne typen intervjuform skal være nyttig når informantene har ekspertkunnskap om et emne (Leech et al., 2013:210).

Forskningsspørsmålet er ikke ute etter å sammenligne på tvers av informanter, men ønsker mest mulig inngående kunnskap i deres forståelse av emnet med mål om å identifisere teoretiske definerte sikkerhetsforståelse. Siden utvalget av informanter i tillegg baseres på aktører med ulik bakgrunn og roller, ble det utformet tilpasset og relevante intervjuguider til informantene. Likevel ble spørsmål som ble sett på som universelle beholdt på tvers av informanter. Intervjuguidene startet med noen generelle «ground tour» spørsmål, for å gjøre det enkelt å komme i gang, men også for å få en oversikt over enten personens rolle i saken (Leech et al., 2013: 215-216). Intervjuguidene ble strukturert på en måte som gjorde at jeg kom raskt til formålet med intervjuet og får informantenes fokus på temaets kjerne. Spørsmålene gikk derfor raskt gikk inn på konkret på prosessen mot valget av 5G-leverandør, selve debatten rundt 5G og hvilke utfordringer de ser mot 5G-nettet og oppfattelsen av 5G-debatten (Beckmann og Hall, 2013, s.204-205).

Det er en usikkerhet rundt hvilke effekter rangering av spørsmål i intervju har for de svarene som gis (Beyers et al., 2014, s.180). For det å kunne danne en god rapport og mest naturlige

svar, ble det lagt opp til å få intervjuene til å være mer som en vanlig samtale. Det innebar at ikke rekkefølgen på spørsmålene måtte leses i eksakt rekkefølge men, men at jeg stilte spørsmålene i intervjuguiden ettersom det passet inn med det informanten snakket om. Dette har noe med hvordan jeg ønsket at intervjuet i større grad reflektere genuin uttalelse mer i tråd sikkerhetiseringsteorien, og at ikke jeg som intervjuer legger opp til en viss sikkerhetsforståelse. I tillegg så kunne det innebære at spørsmål ikke ble stilt på den måten det direkte stod oppført i intervjuguiden, men tilnærmet lik og med det samme budskapet (Leech et al., 2013, s.217).

Det var en del av informantene som satte direkte i gang med å fortelle deres perspektiv og forståelse av saken, og der det var til tider utfordrende å få rom til å stille spørsmål. Samtidig så ble ikke dette alltid sett på som en ulempe å måtte få stilt alle spørsmålene, da jeg fulgte med i den aktuelle intervjuguiden, og kunne følge opp med oppfølgingsspørsmål fortløpende som informantene snakket. For det var til tider jeg erfarte at informanter var innom de fleste spørsmål som var allerede lagt opp til i intervjuguide, men da gav dette mulighet til å stille videre spørsmål og gå enda dypere inn på temaet. Det var et fåtall som var såpass snakkesalig, at det var vanskelig å komme til ordet selv om det ble forsøkt. Oppfattelsen og vurderingen som ble gjort ved disse tilfellene var at det opplevdes vanskelig å avbryte informantene som var i så dypt inne i sine resonnement. Likevel så synes jeg at dette ha en fordel ved at denne uttalelsen kommer direkte fra informantene selv og med minst mulig påvirkning fra spørsmål som intervjuer. Hvert intervju ble avsluttet med spørsmålet om informantene mente det er andre ting jeg ikke har nevnt som er aktuelt å vite og som jeg har glemt å spørre om. På denne måten kunne jeg bygge på en god rapport, samtidig som at jeg kunne få tilgang til interessant informasjon som ikke var tenkt på. Det var sjeldent det kom noe ny informasjon av det spørsmålet, men der informantene i større grad oppsummerte forståelsen sin om saken og ikke minst at de utrykte viktigheten av emnet (Leech et al., 2013, s.218).

Gjennomføring av intervjuene ble gjennomført på litt ulike måter. På bakgrunn av den pågående koronapandemien og smittevernråd om sosial distansering, lot det seg ikke å møte alle informanter ansikt til ansikt. Derfor måtte noen av intervjuene gjennomføres enten over telefon eller videomøte gjennom programmet Zoom (tjeneste anbefalt av Universitetet i Oslo). Alle intervjuene ble derfor gjort opptak av digitalt gjennom UiOs Diktafon-applikasjon, bortsett fra noen få. Ved ett tilfelle så skjedde det en feil med diktafon-appen som slettet siste delen av mitt intervju, og gjorde at jeg mistet viktig datamateriale for analyse. For en stor

utfordring ved gjennomføring av intervjuene var at en del informanter brukte ulike plattformer ved gjennomføring av videomøter. Det var derfor noen ganger man fikk problem med å få tilgang til de samme plattformene, og få teknisk til videomøtene. Derfor var eneste løsning å gjennomføre disse over telefon, noe som er litt ugunstig. Da har man ikke mulighet til å observere informantenes kroppsspråk som kan være med på å fortelle om deres respons på spørsmålene som stilles, og kan være en tilleggsinformasjon som kan fortelle noe videre om synspunktet til informanten (Bryman, 2016, s.485). I tillegg hadde jeg tekniske utfordringer å gjennomføre intervjuene på denne måten, da telefonen ikke kunne bruke diktafon-appen og ringe samtidig, noe som førte til store utfordringer, utsettelser av intervju og innkjøp av ekstern diktafon.

Siden hele deler av alle intervjuene ble transkribert, kunne dette også tenkes at man kunne ha publisert transkriberingene et sted, med mål om at andre forskere kan ettergå utdragene og sitatene i oppgaven. Derimot er dette en oppgave av en mer sensitiv karakter, omhandlende måte politiske holdninger knyttet til nasjonal sikkerhet og kritisk infrastruktur. I tillegg ville det å ha tilgang til hele transkriberingen åpne opp for en mulig identifisering av informanter i studien. Derimot legges ved intervjuguidene, og dermed er mulig å ettergå til en viss grad på den måten. Intervjuguidene er å finne som vedlegg 5.

3.4.2 Intervjupersoner

Utvalget av informanter her baserer seg på et formålsrettet utvalg, der utvalget trekkes ut etter spesifikke trekk og karakteristikker som er relevante for analysen og som er i stand til å belyse forskningsspørsmålet (Lynch, 2013, s.41). Videre kan en slik formålsrettet utvalg være et utvalg som er mer løsning representativ til den populasjonen som studeres her. Den populasjonen som kan sies å bli studert her er sikkerhetsforståelsen hos aktører som har ansvar for sikkerheten og utbyggingen av 5G-nettverket i Norge, sammen med bredere konstellasjon av aktører og personer som både er med å prege diskursen og politikkutforming i kraft av sin ekspertise om temaet.

I prosessen for å finne relevante informanter og populasjonen til intervju, var det viktig å definere forskningsformålet med intervjuene (Beyers et al., 2014, s.181). Forskningsspørsmålet har som mål å forklare mest å forklare mest mulig av variasjonen i

sikkerhetsforståelsen rundt leverandørvalget i 5G-nettverket hos aktører som er involvert og har ansvaret for mobilnettverk men også cybersikkerheten knyttet til dette. Men samtidig ønskes det også se hvordan denne forståelsen(e) kan forklare i form av effekter dette har for Norges evne til å håndtere sikkerhetsutfordringene i 5G-nettverket framover. Riktige informanter menes i dette tilfellet at de er relevante til det forskningsspørsmålet som stilles her. Nettopp at de har høy kunnskap knytte til caset for oppgaven, vært involvert i prosessen mot valget av 5G-leverandør, men også har også det daglige ansvaret for den cybersikkerheten i det norske mobilnettverket. Det vil derfor ikke legges opp til her at funn som gjøres her generaliseres utover den gruppen aktører og sektoren (telekom/mobilnettverk) som studeres her.

Det teoretiske rammeverket legger også videre viktige og nødvendige føringer for hvilke informanter som er relevante. Som argumentert for i teorikapittelet, tar oppgaven utgangspunktet i Hansen og Nissenbaum (2009) argumenter for at aktuelle sikkerhetiserende aktører bør utvides til å også gjelde eksperter. Risikoteori med sin vektlegging og fokus på teknologien og sårbarheter som en del av bakenforliggende faktor bak muliggjøring av skade, gjør at eksperter og personer med teknisk faglig bakgrunn sees på som høyst relevante informanter til å gi detaljert innsikt i sikkerheten i 5G-nettverket. På bakgrunn av dette ble det også gjennomført intervju med teknisk eksperter, men også ekspert i sikkerhets- og forsvarspolitikk. For eksempel ble det også sett på som relevant å intervjue både sikkerhetsdirektøren og teknologidirektøren for et norsk mobiloperatørselskap. Det ønskes å gjennomføre intervjuet med informanter på enten direktørnivå, men også informanter på rådgiver nivå som sitter med inngående kunnskap om saken og sektoren og. Direktører har en viss autoritet både utad men også innad i organisasjonen de jobber for og representerer og derfor kan gå ut ifra at deres uttalelser har rot i den faktiske fungeringen av sikkerheten rundt 5G-nettverket og har hatt autoritet til å påvirke de valg som ble gjort men også forståelsen rundt valg av leverandør til 5G i Norge. Samtidig så innebærer autoriteten at det er mest mulig i tråd med sikkerhetiseringsteoriens forutsetninger om hvem som er de relevante sikkerhetiserende aktører i diskursen. På denne måten så er også utvalg av informanter teoretisk motivert før det undersøkes etter relevante informanter om dette i Norge (Bleich og Pekkanen, 2013, s.90).

Siden studien som gjøres her er anonymisert, så kommer det ikke frem her hvem som var deltakende informanter. Dette kombineres med hvordan temaet også omhandler et mer

sensitivt tema om nasjonal kritisk infrastruktur, norsk sikkerhet og cybersikkerhet. Likevel så viser vedlegg 1 en anonymisert oversikt over informantene, og vedlegg 2 viser en oversikt informanter som ble kontaktet men som ikke førte fram til noe intervju.

3.5 Transkribering

Både intervju- og filmmaterialet ble transkribert i sin helhet ord for ord. Utfordringen med transkriberingen var at det var til tider vanskelig å oppfatte og høre hva et intervjuobjekt sa i det aktuelle klippet, informantene snakket lavt og diktafon-appen fanget ikke opp godt nok eller lydkvaliteten kunne variere noe som gjorde det vanskelig å transkribere helt korrekt til alle tider. I tillegg ble det synlig hvordan mennesker som snakker ikke alltid i utfyllende setninger, gjerne omformulerer seg midt i setningen eller har visse digresjoner (Bryman, 2016, s.481-482). Likevel ble alt transkribert slik det ble sagt, men der direkte sitat ble tatt ut for analyse, ble slike sitat justert i selve oppgaven for å gjøre sitatet mer leselig forståelig for andre og kortfattet men uten å reformulere sitatet. Jeg hadde alltid selve originale transkriberingen som jeg kunne sjekke opp mot, for å sjekke at det stemte med det informantene sa. I tillegg er det tydeligvis noe man kan erfare innenfor kvalitative intervju, at informanter kan snakke om emne som ikke er relevant for forskningsspørsmålet. Det var ved ett tilfelle der en liten del av intervjuet ikke ble transkribert da dette var ikke relevant for forskningsspørsmålet og som omhandlet hvordan det er mennesker som er bekymret rundt strålingen fra mobilnettverket med utrullingen av 5G (Bryman, 2016, s. 483).

3.6 Koding av datamaterialet

Som nevnt tidligere ble det først gått deduktivt til teorien og tatt ut sentrale begrep ved før innsamling av datamateriale og gjennomføring av intervju ved oppretting av analyseskjema. Selv om kvalitative studier er opptatt av å analysere helheter og ikke bare utvalgte variabler, kommer man seg ikke helt unna et systematisk arbeid med kvalitativ data med en oppdeling av materialet i form av klassifiseringer og kodinger. Viktige tema må klassifiseres og kodes og skjer ut ifra forskningsspørsmålet som stilles (Repstad, 1993, s.94). Disse teoretiske fundamenterte begrepene blir her brukt som arbeidsredskaper som skal gjøre meg mer følsom ved sider av 5G-debatten og mulige sammenhenger, men ikke minst føre frem til både gjenkjennelse og ny innsikt (Repstad, 1993, s.95).

I tillegg til fortolkende forskningstilnærmingen som ligger til grunn her, var kodingen preget av å være en slags hermeneutisk prosess. Med at det er vedkommende som utfører analysen som leser trekk og forståelse gjennom uttalelser som gjøres i tekstmaterialet og gir det mening i møte med teoretiske begrepsskjema. At enkelte utrykk tillegges en mening utover dens umiddelbare fremtreden, men at disse uttalelsene leses og tolkes på i lys av teoretiske definerte sikkerhetsforståelser (Repstad, 2007, s.121). Selv om det må sies at uttalelsene som kodes leses mer direkte og på en umiddelbar måte enn for eksempel diskursanalyse. Prosessen med koding av hele datamaterialet kan sees på som en hermeneutisk sirkel. Det ble konstant vekslet mellom å lese og forstå teksten i sin helet, men deretter gå inn og forstå de ulike delene av samme tekst før uttalelsen fikk sin kode (Repstad, 2007, s.121).

Først ble datamaterialet lest igjennom i sin helhet, før det ble gått til enkelte deler av tekster med temaer og delutsagn, og dermed igjen se de i en mer helhetlig sammenheng med andre utsagn fra samme person og teksten som helhet. Men samtidig ble tekstene og uttalelser i tekstene lest i relasjon til hverandre for å ikke bare undersøke hvordan kilden inngår i puslespillet med de andre aktuelle kildene i datamaterialet, men også hvordan tekster og utsagn kan hente noe av sin mening gjennom tilknytning til andre (intersubjektivitet) (Bratberg, 2007, s.167-168). Dette både på en implisitt og eksplisitt måte, med hvordan aktører og uttalelser i teksten henviser til andre tekster eller aktører i forståelse av sikkerhetsutfordringer i 5G-debatten, men også implisitt gjennom tilstedeværelse av felles sikkerhetsforståelse. Dette er også i tråd med sikkerhetiseringsteoriens intersubjektivistisk konstruering av en sikkerhetstrussel eller riskification legger til grunn til en forståelse av risiko som en sosial konstruksjon (Aradau og Van-Münster, 2007, s.96). Derfor ble det kontinuerlig gjennom hele kode-prosessen av data samt skriving av analysen gjort en slik lesing av enkelte tekster, men også lese gjennom hele datamaterialet for å sikre meningsinnholdet og intensjonen av uttalelsen og kodingen.

Kodingen var også preget en iterativ prosess mellom teori og empiri. Selv om det ble utarbeidet sentrale begreper på forhånd av datainnsamling og koding, ble det sett på som viktig å se tilbake til det teoretiske rammeverket og spesielt de analytiske spørsmålene som ble utledet videre av de sentrale begrepene ved teoriene. Totalt sett er denne hermeneutiske prosessen både mellom enkelte deler og helhet av en tekst, men også bevegelsen som gjøres mellom teori og empiri med på å bidra å styrke meg som analytiker i kodingsprosessen og dermed føre til en mer utdyping og styrking av meningsforståelsen i uttalelsene som hentes ut

av tekstene for koding. Koding av tekstmateriale kan også føre til utfordringer knyttet til validiteten og reliabiliteten i studien her, og vil derfor bli gjennomgått mer inngående nedenfor.

Sentrale begrep som ble identifisert i tekstmateriale ble derfor kodet med den tilhørende teoriens farge. Etter at dette ble gjort for hele datamaterialet, ble det opprettet en datamatrise (se vedlegg 4) over alle teoretiske begrep ved teoriene. Hvert kodede utsagn ble derfor plassert på tilhørende teoretisk begrep. Kodingen ble gjennomført manuelt ved at hver teoretiske perspektiv fikk sin egen farge, og det ble bestemt å ikke bruke teknologisk hjelpemiddel til dette. Dette var på bakgrunn av to ting. Med å triangulere med to ulike datakilder synes det å være mer håndterbart å plassere alle kodede uttalelser i ett og samme dokument i Word. I tillegg, ved å kode manuelt med farge opplevdes dette at det gav bedre oversikt når man bevegde seg både mellom deler av teksten og leste den som helet, samt når man vekslet mellom teori og empirien.

3.7 Reliabilitet og validitet i studien

Dette del-kapittelet tar for seg reliabiliteten og validiteten i studien. Først gjennomgås disse kriteriene for dokumentanalysen, og deretter for elite- og ekspertintervju. Det er klart at ved en fortolkende tilnærming så står validiteten og reliabiliteten i en særstilling når det gjelder å både objektivitet og etterprøvbarhet.

3.7.1 Reliabilitet og validitet ved dokumentanalyse

Når det gjelder den eksterne reliabilitet og i hvilken grad studien her kan gjennomføres på nytt og komme til tilsvarende resultat, er dette mer utfordrende for kvalitativ forskning å imøtegå i veldig stor grad (Bryman, 2016, s.383). Det er helt klart at kvalitativ forskning har sine utfordringer når det gjelder validitet og reliabilitet i studien. Siden dette er en studie av en sosial setting, kan dette være utfordrende å fryse sosiale situasjoner og hendelser, eller replisere dette identisk på et senere tidspunkt. Derimot baserer tekstmateriale seg på publiserte nyhetsartikler og nyhetsinnslag, og er større grad å finne framover i tid. For det første så ble relevante tekster funnet gjennom det ble brukt søkeord for å finne tekster til analysering. Det er mulig at søkeresultat vil kunne variere etter bruk av søkeord. I håp om

mest transparens i studien, økt ekstern reliabilitet og større sjans for replikasjon av studien, har søkeordene blitt beskrevet under.

Den interne reliabilitet betyr om den er intern konsistens innad forskningsgruppen. Siden det i dette tilfellet legges opp til at forskningsprosjektet bare utføres av én person, er det ingen utstrakt fare for inkonsistens. Derimot kan det innebære en fare for skjevhet. Siden kvalitative metoden inneholder et fortolkende og derfor et subjektivt element ved at det er forsker som tolker og henter ut elementer fra tekstmaterialet, er det en økt sannsynlighet for at resultatet kan bli farget av forskerens egne verdier og holdninger (Repstad, 1993, s. 91). En slik fortolkningsprosess som forskningsdesignet og metoden innebærer, åpner det opp for en viss subjektivitet hos forfatteren i denne studien. Blant er det elementet om i hvilken grad mine egne verdier og holdninger kan komme til å påvirke min forståelse av tekstmateriale og derfor de utsagn som kodes og analyseres (Repstad, 2007, s.122). Siden jeg er alene med å gjennomføre denne studien, har jeg ingen andre som er deltakende med å eventuell korrigere en skjevhet som følger med min rolle i fortolkningsprosessen. Derimot kan både aktivt bruk av begrepsskjema og den iterative prosessen mellom teori og empiri være nettopp en slik mekanisme for å hindre en slik skjevhet i koding, analysen og til slutt funn som gjøres der.

Dette har også sammenheng med den interne validiteten i studien. Dette menes med i hvilken grad det er korrespondanse mellom mine observasjoner som analytiker i studien og de teoretiske begrepene som brukes og utvikles (Bryman, 2016, s.384). Det sentrale teoretiske begrepene i analyseskjemaet er allerede etablert og lagt vekt på i det teoretiske rammeverket (Buzan, de Wilde og Wæver, 1998, Hansen og Nissenbaum, 2009 og Corry, 2012). Videre har jeg gjennom en iterativ prosess mellom teori og empiri, spesifisert disse gjennom formulering av analytiske spørsmål som jeg stiller til empirien ved koding og analyseringen av empirien. Målevaliditet innebærer i hvilken grad analysen klarer å observere, identifisere eller å måle det forskningsspørsmålet sier at den skal måle (Bryman, 2016, s.41).

For innenfor en fortolkningsbasert tilnærming på analysen kan det være utfordrende og vanskelig å vise til begrepsvaliditet og indre validitet og dermed kan det være en fordel å støtte seg på en bredere forståelse av validitet (Bratberg, 2007, s.63). Ved at det gjøres tydelig hvilke dokumenter som undersøkes og med hvilke analytiske verktøy. Ved oppretting og bruk analyseskjemaet over sentrale begreper ved det teoretiske rammeverket, er dette med å håndtere denne utfordringen. Ved å bistå og justere meg i tolkning av tekstmaterialet med å

bidra til at det som skiller en sikkerhetisering og riskification fra en politisering blir dratt frem i analysen. Det at det er elementene og konseptene som karakteriserer en sikkerhetisering eller riskification er det som blir identifisert, og på den måten er kan man større grad bidrar til å sikre at analysen måler og svarer på det problemstillingen legger opp til. Videre så legges det ut hvilke type dokumenter og tekster som brukes i analysen, samt det forsøkes å synliggjøre hvordan lesingen av tekstene har foregått gjennom hvordan oppgaven legger ut om kodingen av datamaterialet her.

Når det gjelder den ytre validiteten ved en dokumentanalyse, er det tydelig analysen her i liten grad gjør seg generaliserbar utover denne enheten Norge. Dokumentene som ligger til grunn er valg ut basert på en spesifikk kontekst som disse tekstene og uttalelsene befinner seg, for å kunne besvare forskningsspørsmålet. For den største utfordringen med bruk av en intensiv og beskrivende casestudie med én enhet Norge er den den eksterne validiteten. Nettopp i hvilken grad funn som gjøres her kan generaliseres utover et større antall enheter utover denne spesifikke konteksten her (Bryman, 2016, s. 42). For på bakgrunn av forskningsdesignet er funn som gjøres er i stor grad kontekstavhengig til den sosiale settingen knyttet til 5G-utbygging og debatten i Norge, og det kan ikke sies at funn her kan generaliseres automatisk utover det. Selv om det må sies at formålet med forskningsspørsmålet er nettopp ikke en slik generalisering. På bakgrunn av dette, er den eksterne validiteten begrenset knyttet til hva dette caset kan fortelle og generalisere utover akkurat denne enheten Norge og denne sosiale konteksten (Bryman, 2016, s.384).

3.7.2Validitet og reliabilitet ved elite- og ekspertintervju

Intervju ble gjennomført i studien her for å få en mer inngående kunnskap om sikkerhetsforståelsen i 5G-debatten. Ved å gjennomføre intervju kan dette gi informasjon som tidligere ikke har vært tilgjengelig gjennom en dokumentanalyse. Ikke bare dette, men gjennom at intervju benyttes som triangulering synes dette å kunne bidra til å øke validiteten i studien. For faren er om det bare hentes ut ikke reflektere informantenes fulle og hele synspunkt, men at sitatet er formulert enten på en måte som ikke reflekteres i virkeligheten i form av hos informanten, men at det velges sitat som stemmer med det spesifikke teoretiske begrepet. Ved bruk av triangulering mellom dokumenter og intervju, skal dette styrke meg i tolkning av datamaterialet og dermed kan være med på å styrke målevaliditeten. På denne måten brukes flere kilder eller metoder for å studere samme fenomenet, sikkerhetsforståelsen

i 5G-debatten, slik at funn styrkes gjennom at forståelser og uttalelser som gjøres kan kryss-sjekkes (Bryman, 2016, s.697).

Noe som også kan utfordre validiteten og bidra til en skjevhet i intervjumaterialet, er hvordan det ved ekspertintervju er en asymmetrisk balanse til fordel for informanten. Det at respondenten enten har en veldig spesialisert rolle men også høy kunnskap og erfaring innenfor sitt fagfelt og saken som intervjuet omhandler. Dette forsterkes med hvordan forskningsspørsmålet omhandler cybersikkerhet, et mer teknisk domene som innebærer et behov teknisk innsikt og kompetanse (Beyer et al., 2014, s.178). Dette kan føre til at de innholdet i uttalelsene som gitt under intervju kan i større grad stå usagt. Selv om dette har krevd at intervjuer har måttet sette seg inn i saken, kan det være vanskelig for intervjuer og evaluere det som blir sagt. Det er ikke å si at intervjuer skal utfordre informantene i en intervjusituasjon, men at dette kan spille en rolle i når jeg tar med meg dette datamaterialet i møte med teoretiske rammeverket under analysen. I hvilken grad jeg kan evaluere uttalelsene og sikkerhetsforståelsen i intervjuet i lys av de teoretiske perspektivene i oppgaven her.

Dette henger også med hvordan oppgaven handler norsk infrastruktur, og er dermed svært sensitivt da det berører deler av nasjonal sikkerhet og er hemmelig. Dette kan være med på å gjøre saken litt betent å snakke om, og der man må være mer på vakt for ord og informasjon som gis ut og at man muligens ikke snakke fullt ut om hverken hele saken og prosessen, men også det norske mobilnettverket. I tillegg så kan også informanter som er ansatte i et selskap er heller ikke nødvendigvis objektive og føler ikke at de behøver å fortelle hele sannheten eller sin personlige overbevisning. Det kan tenkes at det er viktig for informantene å utrykke seg både i tråd med organisasjonens syn og valg, og ikke utrykke en forståelse av hendelsen som strider imot. Siden intervjuet gjennomføres etter valget av 5G-leverandør er tatt så kan det tenkes at informanter vil kunne være mer tilbøyelige å svare på en måte som rettferdiggjøre valget som ble tatt. Det at det kan tenkes at man ønsker å være fornøgd med noe som har hatt (og fortsatt har) stor oppmerksomhet både nasjonalt og internasjonalt, og samtidig omhandler nasjonale (og internasjonale) sikkerhetsutfordringer. Dette omfatter også og fører videre til en annen mulig skjevhet i elite- og ekspertintervju, nemlig en slags omvendt attraktivitetsskjevhet, der informanten over- eller underestimerer sin innflytelse og makt (Beyers et al., 2014, s.178). Dette spiller inn på objektiviteten og validiteten til studien, ting blir sagt som det egentlig er, noe som er vanskelig når det er en sak som handler nasjonal sikkerhet og cybersikkerhet.

Dette henger også sammen med og fører til en annen utfordring med intervju. For når man gjør datagenering av empiri gjennom intervju kan det oppstå et problem dersom intervjuer rapporterer eller henter ut sitat og uttalelser som generer eller reflekterer en spesiell holdning eller om som bekrefter teoretiske rammeverket eller sine argument, men som ikke reflekterer informantens fulle forklaring og uttalelse (Bleich og Pekkanen, 2013, s.89). En mulig løsning, men som også har sine utfordringer, er at det gjennomføres sitatsjekk hos informantene. På den måten at informanten kan sjekke at de kan stå innenfor uttalelsen men også få avklart tolkningsforskjeller mellom intervjuer og informant. Men det som er høyst uheldig er hvordan dette kan legge til rette for at informanter ser tilbake på uttalelser som de i etterkant ikke ønsker skal publiseres og derfor endres eller fjernes fra oppgaven. Likevel var det to informanter som ønsket å gjennomføre en sitatsjekk før levering av oppgave. Ved begge tilfellene ble sitatene justert av informantene, men der budskapet og meningsinnholdet er bevart i de reviderte versjonene. Det var også noen få sitater ikke ønskes ble inkludert i den reviderte versjon og ikke ønskes brukt, så derfor ble ikke disse inkludert. Det ble vurdert til at det viktigste er at det er en felles forståelse enighet rundt sitatene som publiseres, enn at sitatene og dermed analysen skal miste sin troverdighet i etterkant. Siden meningsinnholdet ble all hovedsak bevart, oppfattes ikke dette som å avvike i stor grad fra det opprinnelige.

Når det gjelder reliabiliteten ved intervju, kan denne styrkes ved at det føres opp hvem informantene er når det gjelder bakgrunn og organisasjon de kommer fra (Bleich og Pekkanen, 2013, s.90). Når det gjelder studien her, så anonymiseres den og dermed har jeg ikke mulighet til å gi detaljert informasjon om hvem informantene her er. Likevel er det en anonymisert oversikt som vedlegg 1 der det er forsøkt å opprettholde anonymisering men å gi en viss informasjon om faglige bakgrunnen og posisjonen til informantene. Dette er også på bakgrunn av sikkerhetiseringsteoriens vektlegging på sikkerhetiseringsaktører. For på denne måten kan man sikre at undersøkelsen som gjøres her i størst mulig grad kan etterprøves av andre i ettertid. På en annen side så handler studien her om mobilnettverk og telekomsektoren i Norge. Å finne de involverte partene i denne sektoren, kan ikke synes å være den største utfordringen da sektoren er temmelig liten med få aktører. I tillegg så er informantene også delvis basert på og hentet ut ved at de i ulik grad har vært deltakende i den offentlige debatten ved og vært intervjuet eller gitt en kommentar til media. På bakgrunn av dette synes det å kunne være relativt enkelt å kunne ettergå studien ved å finne de aktuelle informantene.

3.8 Oppsummering

På bakgrunn av det teoretiske rammeverket sammen med den metodiske tilnærmingen for studien, viser tabell 3 det endelige analyseskjemaet som skal veilede meg i analysen av datamaterialet etter identifisering av hvilken sikkerhetsforståelse som karakteriseres 5G-debatten. En analyse av data sies å være prosessen der man forsøker å ordne data slik at de får struktur, og gjøres lettere tilgjengelig for tolkning, og der tolkningen av data er en begrunnet vurdering av dette datamaterialet knyttet til problemstillingen som er stilt i oppgaven (Repstad, 1993: 83). Gjennom å benytte dette analytiske begrepsskjemaet, er målet at dette guider meg på en slik måte at relevante begrep for det teoretiske rammeverket hentes ut i er i størst mulig grad svarer på forskningsspørsmålet som stilles i oppgaven her.

Tabell 3: Totale analyseskjemaet

Begrep	Beskrivelse	Analytiske spørsmål	Empiri
Cyber-sikkerhetisering Cyber-risiko			

Det komplette utfylte analyseskjemaet for identifisering av sikkerhetsforståelse er lagt som vedlegg 3 i oppgaven.

4.0 Analysen: Den norske 5G-utrullingen

Analysen baserer seg som kjent på både dokumenter og elite-intervjuer, og kombinerer disse to for å få mest mulig inngående og detaljert kunnskap om den norske sikkerhetsforståelsen knyttet til leverandørvalget for 5G-nettverket. Analysen er delt inn i to deler, der første del tar utgangspunkt i en analyse av den norske debatten og der den norske sikkerhetsforståelsen(e) identifiseres i lys av de tre teoretiske perspektivene. Den første analysedelen er strukturert slik at cyber-sikkerhetiseringsteorien benyttes først, deretter følges det opp med riskification.

4.1.0 Cyber-Sikkerhetisering

«Jeg tror .... (lang pause). Man må se ... det er ikke Huawei som er trusselen, det er Kina som er trussel aktøren. Så det er viktig å plassere» (informant 5).

Ved utrullingen av det neste generasjon mobilnettverket 5G, har det i motsetning til tidligere utrullinger kan synes å ha vært et taksskifte når det gjelder den offentlige debatten på både på nasjonalt nivå i Norge og globalt nivå knyttet til sikkerheten i telekom-utstyr og leverandør-selskap bak teknologien. Flere land tok steget og innført forbud mot at det ledende telekom-selskapet Huawei skulle levere utstyr for utbygging av 5G-nettverket. Den gangen synes det ikke å ha vært den store debatten, selv om det finnes nyhetsartikler om at både Politiets Sikkerhetstjeneste (heretter PST) og Norsk Sikkerhetsmyndighet (heretter NSM) advarer mot selskapets kinesiske tilhørighet, og risikoen ved å la selskapet levere komponenter til viktige samfunnsfunksjoner i Norge. For PST uttrykte også skepsis til Huawei da de vant anbudet for å levere hele mobilnettverket i Norge i 2014. *«Det er et problem at det selskapet er fra et land vi ikke har et sikkerhetssamarbeid med»* sa seksjonssjef Erik Haugland i PST (tv2.no, 2014). I følge sikkerhetiseringsteorien synes temaet den gang å være nærmere ikke-politisert ved mangelen av å gjøre det til en offentlig debatt og at staten den gang ikke var involvert i håndteringen og vedtaket om 4G (Hansen og Nissenbaum, 2009, s. 1158).

I programmet «Debatten» med tittelen «I lomma på Kina» på NRK, ble det stilt spørsmål rundt hvorfor den rød-grønne regjeringen tillot Huawei å bygge ut 4G-nettet dersom man er bekymret nå for Huawei, svarer stortingsrepresentant Torgeir Knag Fylkesnes: *«Det var jo på det tidspunktet ingen på Stortinget som tok til ordet mot det. Det var noen, blant annet*

eksperter rundt omkring blant annet Gisle Hannemyr (professor i informatikk) som blant anna advarte mot det. Det var ingen stor debatt da. Siden den gang så har jo nettene ikke minst 5G ... altså siden 2007-2008, fått et helt anna omfang enn det har i dag. 5G kommer til å gripe inn i omtrent alt av infrastruktur» (NRK.no, 2019e).

USAs etterretningsmyndigheter skal ha vært skeptisk i flere år, også ved utbyggingen av 4G, men det var i 2019 at president Trump signerte et forbud mot Huawei i å bygge mobilnett eller drive salg av telefoner til USA (White House, 2019). Amerikanske myndigheter og etterretningstjeneste har uttalt at den kinesiske tele-giganten er en sikkerhetsrisiko mot nasjonens sikkerhet, og advarte andre allierte nasjoner mot å tillate det kinesiske selskapet å levere telekom-utstyr til sine neste generasjon mobile nettverk. Etter den tydelige amerikanske skepsisen og påfølgende utestengingen av kinesiske Huawei, fikk dette økt oppmerksomhet i norsk presse og startet debatten rundt sikkerheten rundt å la Huawei, som allerede står bak alle G'ene i det norske mobile nettverket, også skal få muligheten til å levere 5G-utstyr. For det er gjerne hvordan andre stater som USA, Australia og New Zealand bannlyste Huawei som gjør at norske medier henvender seg til sine myndigheter med viten om at Huaweis mangeårige tilstedeværelse i det norske mobilnettet. Med hvordan nyhetsanker introduserer saken om 5G-utrbyggingen i Norge og der Huawei bannlyses i USA av frykt for spionasje, sier daværende justisminister til NRK Dagsrevyen januar 2019 slik: *«Jeg har merka meg hva USA og Storbritannia gjør. Og vi deler også den uro for etterretningsvirksomhet mot kritisk infrastruktur. Så det er uro vi har. Det e jo derfor vi også må gjøre en vurdering om hvilke krav vi skal stille* (nrk.no, 2019a). Med norske mediers nyhetsdekning om USAs uttalelser og tiltak mot Huawei samt hvordan det henvises til andre lands tiltak og sikkerhetstjenester at dette er (nrk.no, 2019b). USA synes å i alle fall være en bidragsyter til at emnet blir politisert eller være en slags «politiserende aktør» til at saken om Huawei som potensiell leverandør for 5G-nettet får den økte og tette medieoppmerksomheten i Norge i 2019, og starter en offentlig debatt om ulike politiske tilnærminger til problemstillingen om Huawei som leverandør for 5G (Hansen og Nissenbaum, 2009, s. 1159).

(Eksistensielle) trusselen: Tilknytning mellom Huawei og Kina

Selv om det er nettopp PSTs oppgaveå skaffe frem kunnskap og identifisere hvilke trusler Norge står ovenfor til enhver tid og derfor ikke i seg selv overraskende at de peker mot Kina.

Det som peker seg ut med 5G-debatten i motsetning til tidligere utbygginger av det norske mobilnettverket er hvordan selskaper Huawei utrykkes eksplisitt offentlig av PST-sjefen selv, og i tillegg synes å ha fått en økende oppmerksomhet gjennom å ha blitt gjengitt hos norsk media, norske stortingspolitikere og akademikere i større grad enn tidligere. Da gikk PST-sjefen Benedicte Bjørnland ut og advarte mot Huawei: *«Vi har sagt at man bør være oppmerksom på Huawei som aktør i forbindelse med 5G-nettet som skal bygges ut. Ikke fordi det er noe galt med Huawei og menneskene som jobber i Norge, men Huawei som selskap har antagelig ganske tette bånd til kinesiske myndigheter»* (nrk.no, 2019c). Denne påståtte tilknytningen mellom Huawei og Kina, forsterkes gjennom en endring i den kinesiske sikkerhetsloven i 2017. For PST-sjefen sier i intervju med NRK Dagsrevyen i forbindelsen med deres åpne trusselvurderingen at: *«Og Kina har en etterretningslov som pålegger både private virksomheter og enkeltpersoner å samarbeide med kinesiske myndigheter»* (nrk.no, 2019d).

Når det gjelder om PSTs offentlige uttalelse om Huawei artikuleres gjennom de spesifikke sikkerhetsmodusene som viser seg typisk innenfor cybersikkerhet. PSTs uttalelser beskriver ikke scenarioer om katastrofale cyberhendelser av en flerdimensjonal karakter som innebærer flere hypotetiske alvorlige trusler og hvordan en cyberhendelser mot et nettverk har umiddelbar og domino-effekt som videre påvirker andre sektorer, institusjoner og aktører og dermed drar med seg andre referanseobjekt og sektorer i Norge (Hansen og Nissenbaum, 2009: 1164). Det utrykkes ikke at denne trusselen er eksistensiell etter den opprinnelige sikkerhetiseringen heller og argumenterer for løsninger og tiltak som overskrider normale politiske prosedyrer, men PST maner til «oppmerksomhet». Kriteriet som ligger bak en eksistensiell trussel innenfor sikkerhetiseringsteorien er temaet blir *presentert* som en eksistensiell trussel på en slik måte at det saken blir argumentert for å overgå vanlig politikk (Buzan, de Wilde og Wæver, 1998, s.24). Det argumenteres ikke for at dersom dette ikke håndteres, så blir alt annet irrelevant og et spørsmål om overlevelse, noe som innebærer denne saken er mer viktig enn andre ting og derfor krever den det absolutte prioritet.

PSTs uttalte bekymringen rundt Huaweis baseres hovedsakelig på staten Kina, en av de statene som sikkerhetstjenesten har vurdert i flere av sine åpne trusselvurderinger til å være en av de største trusselaktørene mot Norge i det digitale domene (pst.no, 2019, pst.no, 2020). I den åpne trusselvurdering for 2020 nevnes 5G spesifikt når det kommer til statlig etterretningsvirksomhet. Uten at konkrete land eller selskap nevnes, vil 5G-utbyggingen:

«innebære en ytterligere forskyvning i maktbalansen mellom offentlige myndigheter og kommersielle virksomheter» (Politiets Sikkerhetstjeneste, 2020). I følge sikkerhetstjenesten vil en 5G-utbygging innebære en videre utvikling der både norske mobiloperatører og utenlandske leverandører får mer makt ved at de har kontroll og tilgang til økende mengde informasjon som ligger i mobilnettene, men også hvordan dette nettverket forvalter stadig flere samfunnsfunksjoner men også kritiske samfunnsfunksjoner: «*For en fremmed stat med særlig interesse for Norge og norske forhold vil eksempelvis eierskap i slike virksomheter kunne gi store muligheter for etterretnings og påvirkningsvirksomhet»* (Politiets Sikkerhetstjeneste, 2020).

Uten å nevne hverken Huawei og Kina spesifikt, kan det tolkes som at utenlandsk eierskap i norsk ekom oppfattes av PST som potensielt truende i form av å utfordre den norske autonomien. For med privat eierskap over kritisk infrastruktur kombinert med økt avhengighet til digitale løsninger slik som 5G forventes til å spille, forventer PST at aktøren som kontrollerer norsk ekom har *«svært stor makt over samfunnet»* (pst.no, 2020). Dette utrykkes også offentlig til NRK i PSTs kommentar til det kinesiske tilbudet om en «no-spy-agreement: *«Det er problematisk om Huawei får bygge ut 5G-nett i Norge. Vi er bekymret for at det kan medføre at vi ikke har full kontroll på norske e-komnett som er kritisk infrastruktur»* (nrk.no, 2019h). På bakgrunn av PST offentlige uttalelser og i sine åpne trusselvurderinger kommer det til utrykk at informasjonen som er i mobilnettverket og det økende antallet samfunnsfunksjoner og kritiske samfunnsfunksjoner sees på som kollektive referanseobjekt norsk, i likhet med at kontroll over ekom som PST uttaler som å være kritisk infrastruktur.

Sikkerhetsutfordringen som PST utrykker, deles også av den norske Etterretningstjenesten (E-tjenesten). E-tjenesten legger også frem i sin åpne trusselvurdering for 2020 hvordan 5G ble en del av geopolitikken som følge av debattene rundt Huawei, og erkjenner at Kina er ledende når det gjelder 5G-teknologi og at: *«Den sentrale rollen 5G vil spille i all kommunikasjon vil samtidig utfordre tradisjonelle forestillinger om territoriell integritet og nasjonal råderett»* (Etterretningstjenesten, 2020, s.62). 5G vil i følge E-tjenesten føre til at *«Dette vil kunne påvirke hvor godt nettverksoperatørene evner å sikre kommunikasjon. Neste generasjons kommunikasjonsnett vil være kritisk for å opprettholde sentrale samfunnsfunksjoner. Dette betyr at kontroll over informasjonsnoder vil kunne brukes til politisk, økonomisk og militær etterretning og legge til rett for nettverksoperasjoner og sabotasjeformål»*

(Etterretningstjenesten, 2020: 73-74). Kinas kapasiteter og motivasjon trekkes også fram av Etterretningstjenesten (E-tjenesten). *«For det tredje gir Silkeveienstrategien Kina styrket etterretningskapasitet. 5G-nettverket, fiberkabler og smartbysystemer vil kunne brukes til å samle inn sensitiv informasjon. De gir også tilgang til massedata som er verdifullt for Kinas satsing på kunstig intelligens»* (Etterretningstjenesten, 2020, s.55)

Derimot vektlegger sikkerhetstjenestenes en presentasjon av farene ved 5G-utbygging er preges her av et trussel perspektiv, der en aktør utrykkes som ha vilje, motivasjon og kapasiteter, slik som Kina identifiseres (Reichborn-Kjennerud, 2016, s.33). Lysne 1-utvalget definerer i sin offentlige utredning: «at en trussel blir estimert basert på trusselaktørens kapasitet, evne og vilje til å påføre skade og det er denne måten som brukes mot tilsiktede uønskede handlinger der man må forholde seg til en strategisk og kalkulerende trusselaktør» (NOU:13, 2015, s.32). Sikkerhetstjenesten la derfor vekt på tilbake i januar 2019 på den direkte trusselen og faren for direkte skade, nemlig aktøren Kinas og muligheten for at den gjennomføre uønskede handlinger mot 5G-nettverket. En seniorforsker innenfor forsvar og sikkerhet uttrykte i intervju på spørsmål om den norske debatten og hvorfor den fikk så stor oppmerksomhet i motsetning til 4G: *«Og så kan man mene at hvis det bare skyldes handelskrigen og sånn, da mener jeg det er feil fordi jeg mener det at gitt utviklingen i Kina så er det bekymring rundt den autoritære retningen i Kina. Med masseovervåkning og alt det her, så vil jeg mene at det ville være uansvarlig å være IKKE bekymret for Kina. Når det gjelder at de kan misbruke dette her. Men at det har bidratt til at resten av Europa har våknet opp litt og har et litt annet syn på Kina, det tror jeg nok. Og så kunne man si at det burde man gjort før eller, men uansett så mener jeg at det er alvorlige ting ved Kina, at det er grunn til å være bekymret»* (informant 2).

For følge Buzan, de Wilde og Wæver (1998, s.33) så er det noen faktorer som er til stede som bidrar til at en talehandling fungerer og som øker sjansen for at forsøket på sikkerhetisering fungerer. Utover det viktigste med interne elementet med at språket og uttalelsene utrykker en tilstedeværelse en eksistensiell trussel så avhenger det av det eksterne elementet ved talehandlingen. Det betyr den sosiale posisjonen og autoriteten til den sikkerhetiserende aktøren som bidrar til at publikum aksepterer talehandlingen og innholdet i den, nettopp at det er en eksistensiell trussel mot et referanseobjekt som derfor legitimt krever ekstraordinære tiltak for sikre overlevelse. For det som også skiller seg fra tidligere er hvordan PSTs advarsel og uttalelse om Huawei i etterkant av pressekonferansen, har fått en økende oppmerksomhet

etter hvordan uttalelsen hos flere og kommenteres av flere deltakende aktører i debatten. På denne måten kan PST kan sees på som en form for sikkerhetiserende aktør, som har en viss autoritet i form av posisjon i det norske samfunnet, og som bidrar til at deres uttalelser får en viss legitimitet og fasiliterer til at det bør gjøres tiltak knyttet til valget om hvilket selskap som skal stå som utstyrsleverandør for 5G i Norge. For tråd med den opprinnelige sikkerhetiseringsteorien, er det eksakte kriteriet på en sikkerhetisering gjennom hvordan det intersubjektivt etableres en eksistensiell trussel med en såpass vekt at det får substansiell politisk effekt (Buzan, de Wilde og Wæver, 1998, s. 25).

Det synes ikke å være stor motstand til både norske myndigheters og sikkerhetstjenestes uttalelser i 5G-debatten knyttet til hverken Huawei eller Kina, og det synes som PSTs uttalelser har en legitimitet hos noen politikere i opposisjonen. For derimot etterspørres det etter tiltak fra justisministeren i lys av PSTs uttalelser. Under NRK «Debatten» uttrykket stortingspolitiker Torgeir Knag Fylkesnes fra Sosialistisk Venstreparti (SV) bekymring for Huawei og det kommende 5G-nettet: *«Vi står nå i fare for å slippe inn reven til å designe hønsehuset igjen. Og dette på et nett som er såpass omfangsrikt og kommer til å styre så store prosesser i vårt samfunn, der vi ikke har kontroll på om sikkerheten er ivaretatt. Og derfor mener jeg at det er all grunn til å advare mot å gå videre. Jeg mener at Astrup rett og slett bør gå inn i dette her. Ta bekymringa fra PST på alvor og aldri tillate at vi får inn i en avtaler som dette her hvis vi fortsatt har en usikkerhet knytta til Huawei»* (nrk.no, 2019e). For måten å studere et tilfelle av sikkerhetisering er å se etter når og om et argument med en viss type formulering får tilstrekkelig effekt til å få publikum til å tolerere at vanlige normale politiske prosedyrer brytes og saken håndteres gjennom ekstraordinære tiltak. Det er ikke tilstrekkelig nok bryte vanlige politiske prosedyrer brytes, men at denne presentering av eksistensielle trusselen legitimerer at vanlige normale prosedyrer brytes (Buzan, de Wilde og Wæver, 1998, s.25). For det er andre stortingspolitikere som også synes offentlig å ta PST-sjefens uttalelser på alvor. Når stortingsrepresentant Vågslid fra Arbeiderpartiet (Ap) får spørsmålet om hvilke tiltak Arbeiderpartiet ønsker, svares det: *«Vi tar ikke til orde for å stenge noen ute, det må ansvarlige myndigheter vurdere og de bør også lytte til PSTs vurderinger. Vi må selvsagt velge et alternativ som er teknisk på høyde og godt på pris»* (dagbladet.no, 2019)

PSTs uttalelser om Huawei ble også gjengitt med en bekymring rundt å la Huawei levere 5G-teknologi. Oberstløytnant Vågan Karlsen ved Forsvarets høyskole uttalte bekymring rundt Huawei og dens betydning for norsk sikkerhet. Han peker ut at *«Kina oppfattes som en*

betydelig sikkerhetstrussel av alle vestlige hemmelige tjenester. For det andre, 5G-nettet er kanskje den mest kritiske delen av fremtidig norsk kritisk infrastruktur. Til sist, trusselen om cyberangrep er økende og griper inn på alle andre områder». (tv2.no, 2019a). Her identifiseres staten Kina som trussel aktøren og det fremheves av vestlige sikkerhetstjenester og trusselen om cyberangrep som etterretning, påvirkning og sabotasje som foregår i økende grad og hvordan slike angrep skjer og påvirker på alle områder. Uttalelsen kan tyde på et forsøk på å mobilisere vanlige mennesker, spesielt her gjennom å bygge opp under hyper-sikkerhetiseringens troverdighet ved å koble elementer ved et katastrofe-scenario til vanlige menneskers erfaringer i hverdagen. I tillegg til at dette fasiliteres gjennom å appellere til nordmenns følelser og interesser, ved at digitale tjenester bør opprettholdes til enhver tid og konsekvensene ved at nettverket brytes eller får nedetid (Hansen og Nissenbaum, 2009, s.1165).

Videre får uttalelsen fram nettverks-egenskapen og karakteren ved et cyberangrep i og mot mobilnettverket med 5G-teknologi. Nettopp ved hvordan 5G-teknologi vil komme til å fungere som et nettverk som binder digitale tjenester i flere sektorer på tvers av det norske samfunnet, helt fra meg og deg som digital bruker og helt opp til norske myndigheters handlingsrom og suverenitet. Dette forsterkes ytterligere etter hvordan han mener at 5G-nettet vil komme til å bli en av de mest kritiske delene av norske kritisk infrastruktur. I tillegg til hvordan han legger vekt på karakteristikkene ved et cyberangrep, som har en altomfattende påvirkning og påvirker alle områder, og hvordan cyberangrep er en økende aktivitet og virkemiddel hos andre stater. For han avslutter med *«digital sikkerhet er nasjonal sikkerhet, og 5G-nettet vil i fremtiden knytte alt sammen. Vi må være sikker på at det er trygt»*. På en annen side uttrykkes det ikke ekstraordinære tiltak eller at Norge, norske myndigheter eller norske samfunn er eksistensielt truet utover at Norge vil settes under ekstremt press og at dette vil påvirke det norske samfunnet. Derimot på et spørsmål i et eget intervju med Tv2 knyttet til saken, og om det er grunn til å advare mot Huawei, svarer Hågen Karlsen «*Jeg skal være tilbakeholden med å konkludere siden jeg kan for lite om det tekniske. Det jeg kan si med sikkerhet, er at Kina er en betydelig etterretningstrussel»*. Der han henviser til amerikanske datakyndige og etterretningstjenesters vurderinger (tv2.no, 2019b).

Når det gjelder konsekvensene ved et angrep i mobilnettet, sier Hågen Karlsen i sin kronikk: *«Hva skjer hvis strøm eller mobilnett blir bort i dager og uker nå i februar? Hva skjer med norsk økonomi og tyske kunder hvis gasseksporten stanser? Hvor mye kontanter har du hvis*

kort og Vipps ikke virker? DSB-direktør Cecilie Daae har påpekt legemiddel som en av de største truslene, og en studie viser at vi i verste fall kan få 2500 dødsfall. Også næringslivet er utsatt, og Visma skal nettopp ha blitt utsatt for et potensielt katastrofalt angrep fra Kina» (tv2.no, 2019a). Selv om han ikke nevner noen referanseobjekt eller noe som må beskyttes, drar han frem hvordan dette vil få konsekvenser for «norsk økonomi», «du» som bruker av digitale løsninger og «næringslivet» men også «norske myndigheter» og dermed kobler sammen «staten» og «samfunnet» legger det trykk på graden av alvorlighet som en slik hendelse (Hansen og Nissenbaum, 2009:1169). Videre sier han: «*Men konsekvensene er alvorlige, svært alvorlige. I en konflikt kan en troverdig trussel om bare noen av slike angrep sette norske myndigheter under ekstremt press»* (tv2.no, 2019a).

For å forstå rekkevidden av cyber trusler kan ha, så må man også forstå nettverksstrukturen til datasystem (Hansen og Nissenbaum, 2009: 1161). Dette kan sammenlignes med mobilnettverket sin nettverksstruktur med sine sammenkoblede basestasjoner, men også nettverkslignende strukturer med de mange digitale verdikjedene som støtter opp under alle digitale tjenester som det norske samfunnet i økende grad er avhengige av. Betydningen mobilnettene har i dag med 4G synes å allerede å være veldig viktig for det norske samfunnet, og legges tydelig merke til når mobilnettet er nede: *«For da fungerer ikke BankID og alle tingene som folkene er vant til å bruke i hverdagen, fungerer ikke. Så selv ved kortere avbrudd så ser man at det går inn i så mange verdikjeder at det er veldig mange ting ved samfunnet som ikke fungerer. Men ved lengre utfall så blir det det alvorlig for liv og helse. Spesielt i utkant-Norge hvor man ikke har så mange alternativ, så er mobilnettene kjempe alvorlig hvis de faller ut. Så den betydning er allerede mye større enn det mange tenker på. Så for samfunnssikkerhet er allerede 4G og mobilnettene kjempe viktige»* (informant 6).

På denne måten kan det tolkes at nedetid i det allerede 4G-nettverket vil innebære multi-dimensjonalt scenario, slik hyper-sikkerhetiseringen legger opp til, med kaskanderende effekter som spiller videre på flere sektorer i det norske samfunnet (Hansen og Nissenbaun, 2009, s.1164). *«Men ved lengre utfall så blir det alvorlig for liv og helse. Så jeg tror nesten det ikke går ann å overvurderes. Det vil gå inn i alle sektorer. Vil være nesten som en grunnmur som den digitaliseringen og automatiseringen som skjer vil være avhengig av. Så hvis den faller bort så vil det være veldig ødeleggende for samfunnet»* (informant 6). For denne nettverksstrukturen mobilnettverket har spiller også en rolle i rekkevidden og spennet mellom samfunnssikkerhet og nasjonal sikkerhet i følge informant 6: *«For at det skal ha en*

nasjonal betydning, altså sikkerhetsbetydning, så må det være en viss andel. Ved at det må være en ganske stor del av et mobilnett som blir satt ut av spill før nasjonens sikkerhet er truet. Det er ikke sånn at hvis man har ti basestasjoner i en bygd eller dalføre som er satt ut av spill, så er ikke nasjonens sikkerhet truet. Men mobilnettet som helhet? Ja. Og de tyngste delene av et mobilnett». Utsagnene viser hvordan cyber hendelse mot 5G-nettverket vil få disse multi-dimensjonale effektene som spenner seg på tvers av sektorer og styringsnivå fra lokalt til nasjonalt nivå avhengig av hvilken del av nettverket tas ned, hvor stor andel og hvor lenge nedtid det er snakk om (Hansen og Nissenbaum, 2009, s.1165). En informant med teknisk kompetanse innenfor informasjonssikkerhet i utrykker i intervju hvordan komponenter i norsk kjernenettverk bør kjøpes fra land Norge har et sikkerhetspolitisk samarbeid med: *«For hvis vi da har utstyr fra Huawei og vi har en konflikt med Kina, da mister vi vårt handlingsrom. Da har de nærmest brakt armen bak ryggen vår og vi har ikke noe handlingsrom rett og slett. For vi vet at plutselig, av mystiske årsaker, så kan telenettet feile ikke sant. Så da har de makt over oss da»* (informant 1).

(Hyper)-sikkerhetisering og hverdagslige sikkerhetspraksiser

Under «Debatten» «I lomma på Kina» starter programleder Fredrik Solvang programmet med å si: *«Ja hvis du har brukt mobilen din i dag, så er det stor sannsynlighet for at det du gjorde på telefonen ble sendt gjennom et nett som er levert av Huawei for Telenor og Telia»* (nrk.no, 2019e). Her utrykkes det ikke om katastrofale og multi-dimensjonale cyberhendelser slik hyper-sikkerhetiseringen legger opp til, men heller cyber hendelser som «digital overvåkning». Selv om NRK er statseid mediekanal, innebærer hverdagslige sikkerhetspraksis hvordan private organisasjoner og bedrifter er sikkerhetiserende aktør som forsøker å mobilisere vanlige mennesker, og er med på å gjøre hyper-sikkerhetiseringen mer plausibel gjennom å koble katastrofer innenfor cyberdomenet til vanlige menneskers rutiner i hverdagen (Hansen og Nissenbaum, 2009, s.1165). Videre legger programlederen ut om Kinas styringsregime som verdens største diktator, har henrettet flere mennesker, har ingen ytrings- eller religionsfrihet og er i økende grad mer autoritær og kommunistisk stat: *«Så et av spørsmålene vi MÅ stille oss er om at det er lurt å la et kinesisk selskap levere nesten hele mobilnettet vårt og det nye superraske 5G-nettet. Vi skal først ta et blikk på hvor langt kinesiske myndighetene går for å kontrollere EGNE innbyggere med teknologi»* (nrk.no, 2019e).

På denne måten kan det synes som det gjøres kobling mellom mobiltelefonen «din» i Norge, selskapet Huawei og Kina og digital overvåking. Med å invitere i studio en forfatter og journalist som har skrevet om Kinas president Xi Jinping, snakker de om hvordan Kina bruker teknologi til å støtte opp under det stadig økene autoritære regime: *«Han slår veldig ned på alt som handler om ytringsfrihet, frie medier, folk som tenker annerledes og han gjør dette sammen med et utstrakt overvåkningsapparat»* og hvordan Kina bruker teknologi i blant annet infrastruktur i noe hun omtaler som *«en digital gapestokk»* (nrk.no, 2019e). Selv om det ikke snakkes om multi-dimensjonale cyberhendelser og de konsekvenser det får, så er det som nevnt viktig for en vellykket sikkerhetisering at sikkerhetiseringsaktøren gjennom sine uttalelser, evner å identifisere seg med publikums behov, følelser, interesser og erfaringer. For gjennom å koble katastrofale scenarioer med erfaringer i menneskers vanlige liv, kan dette være med på å bidra til å gjøre en hyper-sikkerhetisering mer plausibel. Dette er med hvordan en slik kobling også i større grad er med på å fasilitere aksepten hos relevante publikum, gjennom at programlederen henviser seg til norske seere gjennom å henvise til deres smart-telefon, noe som alle nordmenn har, bruker mye og har blitt en nødvendighet og på denne måten kan appellere til nordmenns hverdagsliv og behov (Hansen og Nissenbaum, 2009, s. 1165). Istedenfor å knytte dette til mer katastrofale og multi-dimensjonale cyberhendelser, gjøres det heller koblinger til Kina som trusselaktør gjennom uønskede cyber hendelser som for eksempel digital overvåkning av et autoritært regime.

Cybersikkerheten peker seg ut i motsetning til andre sektorer, ettersom det innebærer teknisk et behov kunnskap og kompetanse innenfor datavitenskap for å forstå blant annet digitale system og elektronisk utstyr som ikke alle i offentligheten har. Alle mennesker i har i dag i mer eller mindre grad flere enheter av elektronisk utstyr, men alle har ikke innsikt bak teknologien bak dens funksjon. Derfor skiller cyber-sikkerhetisering seg litte mer ved måten legges rom for mer teknisk ekspert diskurs (Hansen og Nissenbaum, 2009, s.1166). Viktigheten av det tekniske kommer til utrykk blant annet i intervjuet med avdelingsdirektørens i departementet tekniske bakgrunn: *«Så det har vært en nyttig bakgrunn i det arbeidet her å ha vært på den siden som da er veldig teknisk. For du må komme litt inn på det i den diskusjonen. For du må kunne spesielt kunne den teknologiske siden, har vært viktig å forstå, for å kunne gjøre en reell sårbarhetsvurdering»* (informant 6). For teknifisering innenfor sikkerhetiseringslogikken, åpner opp for at det tekniske og ekspertkunnskapen får en spesiell autoritet og politisk legitimitet på bakgrunn av at resten av samfunnet og politikere ikke har (Hansen og Nissenbaum, 2009, s.1167). For det teknologiske

ved 5G-nettverket har sin veldig sentrale rolle i denne debatten. Utover at den forrige gjesten som var forfatter og hadde skrevet bok om Kina, uttaler også den teknologiske eksperten Olav Lysne seg i programmet om kinesernes evne til å stjele data fra norske mobilkunder: *«Dersom de ønsker det, så vil jeg si at svaret på det er JA. Og så er det litt teknaliteter knyttet til hvor mye data de vil klare å lekke ut at vi oppdager at det skjer. Men utgangspunktet er svaret ja. Det kan de»* (nrk.no, 2019e).

Teknifisering er som sikkerhetisering, en talehandling som gjør noe ved konstruere en sak som avhengig av teknisk ekspertkunnskap samtidig som at den er politisk nøytral og dermed skiller seg fra politiske aktører (Hansen og Nissenbaun, 2009, s.1166). Som Lysne velger starte med i NUPI-debatten å dra fram en historie om et israelsk flyangrep på en kjernefysisk installasjon i Syria i 2007, hvor de syriske radarene sluttet å fungere to minutter før angrepet, og førte til spekulasjoner rundt at det var teknologiske muligheter som gjorde at noen på avstand hadde skrudd av eller ødelagt radarene: *«Det mest interessante med den historien er at dette fant vi aldri noe ut av. Det lot seg altså ikke sjekke disse chipene, sjekke dette utstyret. Hva var det som egentlig hadde skjedd her, det lot seg da altså ikke gjøre»* (youtube.com, 2019). Teknifisering spiller viktig rolle i å legitimere cyber-sikkerhetisering på egen hånd, men også som å støtte opp hunder hyper-sikkerhetisering (Nissen og Hansenbaum, 2009: 1168). Dette er et nærmere eksemplene på en tett dynamikk der teknifisering i kan tolkes som som å støtte opp under hyper-sikkerhetisering. Selv om det også her ikke beskrives mer katastrofale cyber-hendelsers med sine karakteristikker som domino-effekter og mer hypotetisk. Likevel kan dette sees på som et utsagn om et faktisk katastrofalt scenario som er kombinert med teknologisk kunnskap om hvordan dette elektroniske utstyret ikke lot seg verifiserer, noe som kan forsterke hyper-sikkerhetiseringen fordi man aldri får kunnskap om dette hverken var en tilsiktet eller utilsiktet hendelse eller mulighet for attribusjon.

For teknifisering av en diskurs kan bidra til at vise at det tekniske er et domene som krever en viss ekspertise som både offentlighetene og de fleste politikere ikke har. Dette igjen bidrar til at tekniske eksperter også kan bli sikkerhetiserende aktører, samtidig som at de skiller seg selv fra mer politiske aktører ved å betrakte seg selv som politiske nøytrale og ser saken ut ifra et teknologisk perspektiv (Hansen og Nissenbaum, 2009, s.1167). Lysne er totalt sett, på tvers av det offentlige publiserte datamaterialet og intervju som ble gjennomført, den personen som blir oftest omtalt. Ikke bare har han skrevet bok som omhandler spørsmålet om Huawei, men har ledet flere offentlige utvalgsarbeid knyttet til digital sikkerhet i Norge.

Lysne henvises også til i intervju med avdelingsdirektør i departementet: *«Men så tenkte vi på software-messig, så kan man legge inn skjult software som ikke trengs å brukes til vanlig men som da kunne gjøre en eller annen operasjon som også ødela basestasjonene men da fra innsiden. Og det var kanskje spesielt den faktoren. Du har sikkert lest Olav Lysnes bok? Jeg syns han får det frem på en veldig og fin måte den rest-risikoen der»* (informant 6).

4.1.1 Oppsummering av første analysedel

Sett i lys av teorien om cyber-sikkerhetisering, legges det i hovedsak vekt på hvordan aktøren Kina er en trussel mot Norge og 5G-nettverket, på bakgrunn den påståtte relasjonen mellom kinesiske myndigheter og Huawei. I tillegg påvirkes dette av at Kina er Huaweis opprinnelsesland, og at derfor at hele selskapet globalt er underlagt den relative nye sikkerhetsloven som krever at alle innbyggere og selskap samarbeider med etterretningsvirksomhet om det etterspør. Offentlig så utrykkes dette som å ha sammenheng med de norske sikkerhetstjenestenes identifisering av Kina som en av de største trusselaktørene i det digitale rom. Selv om debatten ikke avslører at det har vært en sikkerhetiserende aktør i tråd med hvordan hverken Hansen og Nissenbaum (2009) eller Buazan, de Wilde og Wæver (1998) legger til grunn, synliggjøres analysen PST som en sikkerhetiserende aktør, når det gjelder aktørens rolle innflytelse og legitimeringen rundt bekymringen av Huawei.

Derimot viser analysen så langt hvordan cyber-sikkerhetiseringen gjennom de typiske moduser, dynamikken mellom sikkerhet og det tekniske, og hvordan eksperter i økende grad blir deltakende og definerende «sikkerhetiseringsaktører» i en sak knyttet til cybersikkerhet i det kommende 5G-nettet. Dette vises med den fremtredende og tydelige rollen til den teknologiske eksperten Lysne i 5G-debatten, kombinert med hans offentlige utvalgsarbeid om digital sikkerhet og sårbarheter, har han vært en tydelig stemme. I lys av cyber-sikkerhetsteorien artikuleres det referanseobjektene debatten å være både individuelle referanseobjekt som «du» som individ som digital bruker av mobilnettverket og digitale tjenester.

Som kollektive referanseobjekt legges det vekt på norsk suverenitet gjennom at det snakkes om «nasjonal råderett» og «nasjonal kontroll» over kritisk infrastruktur. På denne måten så dras nasjonal sikkerhet inn i 5G-debatten. Men det snakkes også om andre kollektive

referanseobjekt som «samfunnet», «norske økonomien» som omfatter mer knyttet til samfunnssikkerhet. Det som er eget med cybersikkerheten og som 5G-debatten gir et eksempel på, er hvordan cybersikkerheten nettopp kobler sammen individuelle og kollektive referanseobjekt gjennom hvordan en cyber hendelses multi-dimensjonale effekter kan påvirke på tvers av individ, samfunnet og Norge som stat. Det sentrale innenfor cybersikkerheten er nettopp denne dynamikken og måten referanseobjekt som «nettverket» her sett på som 5G-nettet, «individet» er knyttet til nasjonal- og statssikkerhet (Hansen og Nissenbaum, 2009: 1171).

Utover dette, blir det ikke utstrakt grad uttalt noe som peker mot en katastrofal cyber hendelse med sine kaskanderende effekter i tråd med Hansen og Nissenbaums (2009) hyper-sikkerhetisering. Det eneste er Tv2-kronikken til Hågen Karlsen fra Forsvaret, der bekymringen om 5G-nettet og Huaweis rolle artikuleres gjennom både hyper-sikkerhetisering, hverdagslige sikkerhetspraksiser og teknifisering. Tendenser til hverdagslige sikkerhetspraksiser vises også i NRK «Debatten». Dette etter hvordan det artikuleres gjennom denne modusen, gjøres en kobling mellom det autoritære regimet Kina og teknologi som for eksempel digital overvåkning av befolkningen og norske befolkningens mobiltelefoner.

4.2.0 Riskification

«Intervjuer: Kan du si noe om hvordan du syns den norske sikkerhetsforståelsen har vært i denne prosessen?
Informant: Den er under … den blir bedre og bedre. Jeg tror jeg skal si det sånn. Og jeg trur at kanskje sårbarhetsforståelsen har modnet seg» (informant 4).

Sikkerhetsutfordringer knyttet til bakenforliggende faktorer: Sårbarheter

Selv om PST gikk ut offentlig og uttrykte bekymring rundt Huawei og tilknytning til kinesiske myndigheter, sa PST-sjef Bjørndal dette til NRK etter pressekonferansen om den åpne trusselvurdering for 2019: *«Vi har ikke noe grunn til å tro at personer som jobber for Huawei i Norge at de bedriver ulovligheter eller løper den kinesiske stats ærend. Men vi gjør oppmerksom på en betydelig sårbarhet som følger med Huawei som selskap»* (nrk.no, 2019c). PSTs uttalelse, basert på den allerede påståtte relasjonen mellom Kina og Huawei, innebærer tilstedeværelse av tredjepart-risiko. At Kina, et av de største trussel aktørene mot Norge

innenfor etterretningsvirksomhet og datanettverksoperasjoner, kan benytte utstyrsleverandøren Huawei med formålet om å forstyrre eller ta ned det mobile nettverket i Norge om ønskelig (Corry, 2012, s. 246). Hvordan det er en sårbarhetsforståelse knyttet til private selskap som i økende grad blir verktøy for å utøve makt av en tredjepart ved hvordan en statlig aktør kan drive etterretning/spionasje gjennom selskapet Huawei (Lysne, Elmokashfi, Gjesvik og Friis, 2019: 15).

Etter at det ble offentlig kjent at USAs president bannlyste selskapet Huawei ble oppmerksomheten rettet mot Norge der Huawei er tilstede 90 prosent i mobilnettverket. Settestatsråd i samferdselsdepartementet Harald T. Nesvik sa til e24 knyttet til hva norske myndigheter vil gjøre med Huawei: «*Vi ser at ekomnettene er avhengig av et fåtall leverandører, og at en høy andel av særlig basestasjonsutstyret leveres av utstyrsleverandører fra land Norge ikke har sikkerhetspolitisk samarbeid med, og dermed potensielt kan rammes av en og samme sårbarhet*» (e24.no, 2018). Slik DSB skriver i sin risikovurdering, så påvirker sårbarheten ekom-sektoren både sannsynligheten for en uønsket hendelse men også konsekvensene av hendelsen som inntreffer (Direktoratet for Samfunnssikkerhet- og Beredskap, 2014, s.7).

Sårbarhet: Digital avhengighet

I intervju med seniorrådgiver innenfor telekom hos NSM, spørsmålet om hva som blir de største utfordringene med 5G i Norge svarer han: *«Det vil bare gjøre at man blir mer og mer avhengig, og mer og mer sårbar. Så det som er veldig viktig er at operatørene bygger nettet såpass robust, med så mye redundans og så mye alternativer sånn at du ikke er sårbar på grunn av én leverandør, én forsyningskjede som leveranse. Det er kanskje den største bekymringen vi har da»* (informant 4).

Risikologikken innebærer at oppmerksomheten rettes mer mot bakenforliggende faktorer og årsaker som gjør mulig for at faren får mulighet til å materialisere seg. For det gir lite mening å fokusere på direkte årsaker til skade (trusler) med fokus på spesifikke aktører som har ondsinnet motivasjoner og kapasiteter for å utføre skade (Friis og Reichborn-Kjennerud, 2016: 36). Dette er typisk for cybersikkerhet, der Norges høye digitaliseringstempo kan sees på som en bakenforliggende faktor og en som gjør mulig fare. Nettopp at stadig store deler av

tjenestene i offentlige sektor er digital og derfor avhengig av teknologien fungering og stabilitet for at tjenestene kan tilbys og opprettholdes. Dette strekker seg videre med hvordan 5G spiller i større deler av samfunnet, både kritiske og mindre kritiske infrastruktur og tjenester. Dette åpner angrepsflaten for at trussel aktører kan utnytte seg for å forstyrre eller ta ned 5G-nettet, men der konsekvensene ved nedetid er det som gjør oss sårbar: *«Ikke utover at du vil bruke tjenestene mer og mer. For hvis du går fra nitti-tallet med 2G til nå, så har avhengigheten bare økt. Det brukes i dag av alle samfunnets kritiske funksjoner. Når avhengigheten øker blir samfunnet og individet også mer sårbar»* (informant 7).

Deibert og Rohozinski (2010, s.15) med grunnlag i tilnærmingen til Becks risikosamfunn, argumenterer hvordan det er både en «risiko til» cyberspace i form av risiko mot kritisk digital infrastruktur og mobilnettverket og «risiko gjennom» som genereres og fasiliteres av cyberspace selv gjennom sin teknologi. Med hvordan globaliseringen fører med seg nye sikkerhetsutfordringer, og der cyberspace kan sees på som en spesiell kategori av risiko som et menneskeskapt domene som eksisterer på grunn av konsekvensene av teknologisk utvikling og en sammenkoblet og gjensidig avhengighet av globale kommunikasjons- og informasjons infrastruktur (Deibert og Rohozinski, 2010, s.16).

NSMs risikorapport for 2020 identifiserer tre risikofaktorer for nasjonal sikkerhet, som nettopp peker på dette her. Det er samfunnets økende avhengighet av blant annet elektronisk kommunikasjon, en økende avhengighet av digitale infrastruktur og verdikjeder som strekker seg utover norske grenser samt at det er en virkemiddelbruk i form av strategiske oppkjøp, investeringer og påvirkning (Norsk Sikkerhetsmyndighet, 2020, s.5). Direktoratet for Samfunnssikkerhet- og Beredskap peker på hvordan sårbarheten i et system har en sammenheng med grad av avhengighet mellom de ulike leddene i en verdikjede som systemet bygger på (Direktoratet for Samfunnssikkerhet- og Beredskap, 2020, s. 12). Ved at en hendelse skjer, vil dette føre til umiddelbare følgehendelser og er noe som gjør det vanskelig eller umulig å stoppe denne typen hendelsesforløp.

For om noe kan indikeres som et tilfelle at *riskification* og dermed talesetter en fare som risiko så må risikoaktøren i følge Friis og Reichborn-Kjennerud (2016, s. 37) legge vekt på tilstedeværelse av nye avhengigheter av og mellom digitale system. Forståelsen om utfordring med hvordan den økte digitaliseringen i Norge øker sårbarheter deles også av daværende justisminister Wara. På et spørsmål fra NRK på hvorfor 5G-utbyggingen har blitt viktigere

enn den gangen man bygget 4G-nettet, svarer han: «*Nei altså, 5G-nettet vil ha en rekke andre både kvaliteter og sårbarheter i seg. I tillegg så e det nok sånn at man blitt mer bevisst i større grad det digitale samfunnet, den sårbarheten som ligger der. Så fordelen av at vi har et flott digitalt samfunn, åpner også en del sårbarheter. Det må vi tenke ekstra nøye gjennom*» (nrk.no, 2019). EUs koordinerende risikovurdering av cybersikkerhet i 5G-nettverket peker på hvordan staters og samfunns allerede store avhengighet av både sosiale og økonomiske funksjoner har til 5G-nettverket, vil bidra signifikant til en potensiell forverring av konsekvensene en ved tidligere nettverk (EU, 2019:12). For digitaliseringsminister Nikolai Astrup nevner også at ha bare et fokus på aktøren løser ikke sikkerhetsutfordringer i 5G-nettet: *«Og derfor er det blindspor å fokusere kun på én enkeltleverandør. For det er jo ikke slik at selv om vi skulle utelukke ett enkelt selskap etter ønske fra Knag Fylkesnes så ville det betyr at vi har god sikkerhet i nettet»* (nrk.no, 2019d).

Når den ene mobiloperatøren Telenor valgte i desember 2019 den svenske Ericsson som leverandør til sitt 5G-nettverk i Norge, sier digitaliseringsminister Nikolai Astrup: *«5G-nettet kommer til å bære langt høyere verdier for det norske samfunnet enn det 4G-nettene gjør, og derfor så har jo også norske myndigheter opptatt av sikkerhet*. (nrk.no, 2019g). NSM beskriver i sin risikovurdering hvordan disse verdiene er i stadig endring på bakgrunn av den raske teknologi- og samfunnsutvikling, og påvirkes også av stadig sterkere avhengigheter mellom samfunnsfunksjoner (Norsk Sikkerhetsmyndighet, 2020, s.10). Det er derfor et dilemma eller tveegget sverd, ved at det ønskes digitalisering for å øke effektivitet og for rå bedre tjenester til det norske samfunnet, men disse avhengighetene øker også sårbarheter gjennom at dersom en uønsket hendelse eller feil skulle oppstå i en verdikjede, så forplanter den seg. Nettopp at et utfall av ekom vil ha umiddelbar konsekvens for mobiltjenester, nettilgang, informasjons- og nyhetsformidling og digital samhandling over nettverket. Dette synliggjøre også hvordan disse sårbarhetene og digitale avhengighetene gjør mulig et multi-dimensjonale cyber scenario som Hansen og Nissenbaums (2009) hyper-sikkerhetisering innebærer.

Verifisere teknologisk utstyr: Fokus innover på hardvare og programvare

I den offentlige 5G-debatten ble det fokusert på og uttalt i stor grad om ikke bare sårbarheter i hardvare og programvare i elektronisk utstyr som 5G-teknologien, men også hvordan dette utstyret ikke fullt ut lar seg undersøke om det finnes bakdører (implementert med vilje eller

ikke) eller funksjonalitet som kan utføre handlinger imot norske mobiloperatører ønsker og sette mobilnettverket ut av spill. For risikoteoretikeren Beck argumenterer hvordan moderne samfunn har kommet i en anerkjennelse om begrenset kunnskap og vitenskap, og er noe som fører til og innebærer et føre-var-holdning til risikohåndtering i moderne samfunn, enn en forebyggende holdning (Petersen, 2011: 700). En del av kjerne i Becks risikoteori er at forståelsen av at visse risikoer i verden i dag har blitt så enorme at de skaper sosiale og politiske dynamikker som går imot tanken om kontroll som var typisk for industrielle samfunn. Den teknologiske og industrielle utviklingen som skjer i verden har ført til at risiko ikke lengre forstås som håndterbare sideeffekter av vekst i verdenn (Aradau og Van Münster, 2007, s.92).

I tråd med risikologikken må en risikoaktør peke på at det er til stede en sannsynlighet for fremtidige skadelige hendelser, enn at det foreligger direkte grunner til skade eller en spesifikk trussel. For risiko er ikke så umiddelbar i tid og er mer fremtidsrettet enn trussel. Dette gjør at det innenfor risikologikken har et fokus på eller bakenforliggende faktorer, både materielle eller diskursive, som er det som legger til rette visse type handlinger eller skadelige situasjoner (Corry, 2012:246). Daværende sikkerhetssjef i Huawei var opptatt av sårbarheter og derfor er et fokus på aktør Huawei som trussel feil: «*Fordi de fleste angrepene i dag, de kommer ikke gjennom en hardware-del som vi leverer, det kommer gjennom sosial manipulering, sårbarheter i mange typer programmer, det er der angrepene og de kriminelle og fremmed etterretning kommer seg inn, gjerne gjennom alle de verktøyene som ble lekket av NSA, de ble jo brukt i stor grad for å drive angrep og de brukes da av alle mulige etterretningstjenester»* (youtube.com, 2019). Risikologikken handler om *hva* som skaper nødvendige betingelser for at noe skal skje. Med å ha oppmerksomheten og fokuset rettet mot teknologien, hardvare og programvare, evne til å legge inn bakdører og uønsket funksjonalitet men også kjøperens evne til å sjekke dette utstyret og oppdage dette. For med disse sårbarhetene kan sees på som en bakgrunnsfaktor som muliggjør en trussel aktør å gjøre en uønsket villet handling i og mot norsk 5G-nettverk. Dette kommenteres også i intervju, der informanten sier: *«Når man ser på årsakene til feil i nettene i Europa, så er det hovedsakelig hardware og software. Den neste faktoren er strømforsyning, vær og vind. Trusselaktørenes bidrag er beskjedent. Tjenestenektangrep og fysisk sabotasje representerer en veldig begrenset trussel i den større sammenheng. Så det er klart at mens man bekymrer seg for at denne «ringe på og stikke av»-kategorien av trusler som DDoS er skal utvikle seg til noe farligere, så må man holde ting i perspektiv*" (informant 3).

Som allerede nevnt analysedelen knyttet til cyber-sikkerhetiseringen, preget 5G-debatten i stor grad av vår manglede evne i dag til å verifisere teknologi, og derfor oppdage alle sårbarheter, uønsket funksjonalitet. Dette er knyttet til rundt muligheten om Huawei selv, eller gjennom sin påståtte tette relasjon til kinesiske myndigheter, har mulighet til å legge inn funksjonalitet som for eksempel om ruter tilbake informasjon fra norske brukere tilbake til Huawei og Kina eller kan ta ned delene i 5G-nettet som de har levert utstyr til. Teknologen Olav Lysne, som har vært leder Sårbarhetsutvalget nedsatt av norske myndigheter og står bak flere viktige offentlige utredninger knyttet til digital sikkerhet, er fremtredende i 5G-debatten og fokuserer hovedsakelig på denne sikkerhetsutfordringen: *«Hvis noen hadde spurt meg om en enhet er helt sikker, og jeg hadde fått uendelig med penger og uendelig med tid for å verifisere det, hadde jeg måttet si: beklager, det kan jeg ikke, for det går rett og slett ikke an. Dette er en helt ny situasjon i verden vi lever i i dag, hvor teknologi rett og slett ikke kan etterprøves»* (tek.no, 2019). I forskningslitteraturen om risikologikk, så er det som nevnt en problemstilling og diskusjon rundt evnen til å beregne sannsynlighet og risiko fullt ut. Becks overgang fra første til andre modernitet, og hvordan det moderne kapitalistiske samfunnet i dag i økende grad dreier seg om ukontrollerbare og ikke evne til å beregne farer som påvirker mennesker og teknologi (Petersen, 2011, s.700).

I følge den offentlige utredningen fra Lysne 1-utvalget, står det norske samfunnet ovenfor to typer sårbarheter. Den ene sårbarhetstypen er den som er kjent og akseptert på bakgrunn av at kostnadene ved de tiltak som er aktuelle ikke står i forhold til skadepotensialet, verdien som er tenkt beskyttes eller trusselen. Den andre er den type sårbarheter som ikke blir til gjenstand for tiltak fordi sårbarheten er ukjent, feilvurdert, ikke forstått eller mangelfullt kommunisert. Utvalget peker derfor ut denne ukjente sårbarheten er det som utfordrer oss som enkeltmennesker men også som samfunn, og det er nettopp dette er et spesielt omfattende problem når det gjelder digitale sårbarheter som økes med den stadige digitaliseringen (Regjeringen.no, 2015). En risikoaktør vil derfor fokusere på utviklingen innenfor cyberspace, det digitale domenet, teknologi og hvordan det syntaktiske nivået som er i konstant endring.

For dersom en forståelse av en farene ved det kommende 5G-nettet og i valget om 5G-levernadør skal kunne sies å karakteriseres en risikologikk, så innebærer dette et fokus som går innover mot sårbarheter i egne system (Friis og Reichborn-Kjennerud, 2016, s.37). I spørsmål om hvor reell faren er for at Huawei spionerer for kinesiske myndigheter, sier Olav

Lysne: *«Ja, det er litt vanskelig å si, men det ... det er ett teknologisk faktum som det er viktig å få fram her, og det er at når vi nå er i en verden hvor alle kritiske infrastrukturer er bygget opp av elektronikk, så er det altså sånn at det å undersøke hva elektronikk gjør, eller er i stand til å gjøre, det er ufattelig vanskelig. For alle praktiske formål – umulig»* (nrk.no, 2019a). Dette peker også mot kombinasjonen av hvordan samfunnet i dag, på bakgrunn av digitaliseringen, så består store deler av både kritisk og mindre kritisk infrastruktur av elektronikk og derfor bidrar dette til økt avhengighet til at disse digitale systemene fungerer, og cybersikkerheten i og mot systemene. Samtidig så synes dette å påvirkes i en enda mer kritisk retning, med hvordan man ikke har mulighet til å undersøke og teste elektronikken.

For et fokus på bakenforliggende forhold slik som risikologikken legger opp til, innebærer dette at oppmerksomheten rette som både diskursive og materielle bakgrunnsfaktorer enn direkte fare (Corry, 2012, s.246). Hvordan materielle sider ved cyberspace eller det digitale domenet, slik som teknologien i seg selv er en muliggjør for en trussel aktør å gjennomføre en uønsket handling i og mot digitale system. Derfor synes det at et fokus på aktør som Kina eller Huawei som en trussel mot 5G-nettverket, ikke løser fremtidige sikkerhetsutfordringer på bakgrunn av teknologiske sårbarheter elektronisk utstyr. For på spørsmålet om hvordan informanten opplevde den norske offentlige debatten knyttet til 5G og Huawei som potensiell leverandør, svarer han: *«Hvis du ser ... glemmer politikken. Så har alt som har software eller hardware komponenter i seg, det kan alltid manipuleres hvis det er noen utro tjenere som ønsker å gjøre det, så lar det seg gjøre uavhengig av hvem som er fabrikanter eller hvor de kommer fra. Så du har mulighet til å bruke det både for et sabotasjeformål og for manipulering, avlytting, etterretning sånn rent teknologisk»* (informant 4).

For dette med verifisering og testing av teknisk utstyr nevnes også PST i sin trusselvurdering for 2020, der 5G nevnes for første gang eksplisitt i en trusselvurdering. For med flere enheter som kobles til nettet, øker angrepsflaten for påvirkning gjennom det digitale domenet, og: *«For de fleste av oss vil det også være umulig å avdekke om de teknologiske komponentene og programvarene som styrer dem inneholder skjulte, ondsinnede funksjonaliteter som muliggjør spionasje, manipulasjon og sabotasje»* (pst.no, 2020). E-tjenesten nevner også dette med testing av elektronisk utstyr for funn av sårbarheter relatert til 5G i sin åpne trusselvurdering for 2020: *«Stadig økende kompleksitet i våde fysiske komponenter og tilhørende programvare gjør det vanskelig å avdekke sårbarhet ved testing. Norsk næringsliv er derfor avhengig av full tillit til utviklere og leverandører, uten praktisk mulighet til å verifisere sikkerheten fullt*

ut» (Etterretningstjenesten, 2020: 74). I følge Lysne 1-utvalget er det umulig å teste utstyret for om det ligger både alvorlige intenderte eller ikke-intenderte logiske (programvare) sårbarheter, og derfor må relasjonen mellom leverandør og kunde bygges og baseres på tillit (NOU:13, 2015, s.112).

Forståelsen av at elektronisk utstyr ikke kan testes og verifiseres fullt ut deles også av en professor i informasjonssikkerhet i intervju: *«I Storbritannia så kjøpe disse Huawei-utstyr, og så sier myndighetene: jo vi har en test-lab som tester om det er noen spionvare. Og alle bare ler av dem egentlig. For det er teknisk sett umulig å teste og undersøke så kompliserte og store systemer. Det går ikke ann. Hvis de ville, så kunne de lett skjule spionvare i disse systemene. Så det er et uløselig problem dette her. Så den strategien som brukes i Storbritannia med sånn test-lab for å verifisere utstyr, det er en logisk brist i den logikken. Rett og slett. Men det gjør jo det likevel da. Jeg vet ikke hvorfor de gjør det. Men det er sånn det er»* (informant 1). I en risikoanalyse av digitale system og for eksempel digital infrastruktur, innebærer at utviklingen innenfor tekniske og materielle i cyberspace og det digitale domenet blir en iboende del av alle risikoanalyser. Det at det materielle kan sies å spille en aktiv materiell dimensjon som konstant spiller en del av den sosiale dimensjonen, og som til sammen utgjør faktorer utgjør risiko for et cyberangrep (Friis og Reichborn-Kjennerud, 2016, s.37).

For mobilnettetneverk er et eksempel på en digital infrastruktur kjennetegnes ved at den består av hardware og software og utfører en eller flere tjenester som telefoni, meldingstjenester og tilkobling til internett. Denne digitale infrastrukturen består derfor av flere deler som eies, vedlikeholdes av forskjellige organisasjoner på et transnasjonalt nivå og som leverer disse digitale tjenestene til den digitale infrastrukturen slik at den leverer tjenesten den er satt til. En digital verdikjede sees derfor en struktur av leveranser mellom virksomheter, der hver leveranse enten er en digital tjeneste, programvare eller hardvare (Direktoratet for Samfunnssikkerhet- og Beredskap, 2020, s. 9). Når det skal håndteres sårbarheter og redusering av risikoer i en slik digital infrastruktur og digital verdikjede som innebærer et mobilnettverk er, betyr det at kreves en oversikt over hvem som eier, vedlikeholder de forskjellige delene, noe som påvirker den allerede påståtte umuligheten av å undersøke en enkelt elektronisk komponent i seg selv. For under «Debatten» på NRK, legger Astrup vekt på: *«Men det er viktig å få fram en del andre aspekter her og, og den globale verdikjeden vi har i dag. Om det er telekom eller annen type industri. Våre mobiltelefoner, de*

består av 60 til 70 prosent av andre lands komponenter. Vi har et operativsystem fra USA, vi har sikkerhetsløsning fra Finland, vi har antenne-teknologi fra Sverige. Og det gjelder alle komponentene våre. Og konkurrentene våre har og fabrikker i Kina. Det er ikke slik at hvis du plukker ut én leverandør med bakgrunn i hva han kommer ifra, så vil ikke risikoen reduseres. Trussel aktørene vil fortsatt være der» (nrk.no, 2019e).

Lysne 1-utvalget kommenterte også dette i sin første offentlige utredning, og identifiserte i sin offentlige utredning på sårbarheter knytte til drift og styring av ekomnett i Norge, og problemstillinger knyttet til et elektronisk utstyrs opprinnelsesland og Huawei-debatten. Utvalget poengterer hvordan både IKT- og ekomsektoren består av leverandører som globale aktører, og som videre har underleverandører fra ulike land. Utvalget avslutter dermed med å si *«Å avgjøre hvilket land utstyret «kommer fra», vil dermed i en del tilfeller bare ha verdi som en teoretisk øvelse»* (NOU:13, 2015, s.111). Siden de digitale verdikjedene som et mobilnettverk innebærer er transnasjonale betyr dette at deler av verdikjeden er underlagt ulik jurisdiksjon, har norske myndigheter begrenset grad av mulighet for å ha kontroll over sikkerheten i leveringen av kritiske varer og tjenester (Direktoratet for Samfunnssikkerhet- og Beredskap, 2020, s.12). Argumentet rundt og fokuset på kompleksiteten rundt globale verdikjedene i teknologi- og vareproduksjon i det moderne samfunnet i dag, får også stor oppmerksomhet på NUPI-debatten om Huawei, sier daværende sikkerhetssjef i Huawei Tore Orderløkken: *«For hvis vi tenker oss en verdikjede i dag så består den av leverandører og komponenter fra forskjellige land i forskjellig deler av verden. Og så setter vi det er sammen og så leverer man, enten om det er en Apple Iphone eller om det er Nokia-utstyr eller Ericsson-del, så har alle de her komponenter fra Kina eller fra andre land. Det å trekke ut Huawei som den store stygge mener jeg da ikke vil redusere risikoen for hendelser»* (youtube.com, 2019).

I intervju med seniorrådgiver for telekom i NSM, utrykker han noe av det samme: *«For det er klart at selv om vi sier at det er Ericsson og Nokia, så er flere av komponentene i utstyret de benytter produsert i andre land enn Sverige og Finland. De benytter seg av mange underleverandører. Hvis noen av underleverandørene får utfordringer vil det påvirke de selskapene de har leveranseavtaler med. Mange av komponentene produseres jo i det landet du snakker om, noe som er interessant. Vil Nokia og Ericsson ha mulighet til å avdekke manipulasjon av disse komponentene? Sannsynligvis ikke så godt, og det vil i så fall være*

krevende» (informant 4). Fokuset på denne sikkerhetsutfordringen i form av usikkerhet i 5G-debatten, fører videre til et annet sentralt element ved risikologikken, nemlig styring. Risiko kan ikke bli fjernet helt, kan bare bli håndtert (Corry, 2012, s.247). Dette gjør at det innenfor riskification, er et fokus på sikkerheten og sårbarheten til referanseobjektet og som videre bidrar til et fokus innover rettet på kontroll. Det er dette som kommer tydelig til syne i 5G-debatten, gjennom det teoretiske rammeverkets riskification sitt fokus på bakenforliggende faktorer som årsaker bak farer knyttet til 5G-nettet. For alle de ulike momentene som nevnes frem til nå har til felles med det at det legges vekt på bakenforliggende faktorer eller indirekte årsaker bak fare, og at fokus på aktøren leverandøren, ikke løser sikkerhetsutfordringen. Som digitaliseringsministeren Astrup uttalte i «Debatten» på NRK: *«Jeg mener at JEG er nødt til å ha en prinsipiell tilnærming til nettet og det betyr at å fokusere alt på ÉN enkelt leverandør det blir et galt utgangspunkt fordi det vil ikke nødvendigvis tilsi at vi har god sikkerhet i nettet, det å følge den linjen som Knag Fylkesnes her gjør»* (nrk.no, 2019e).

Sikkerhetsutfordringen som synes å få stor oppmerksomhet i 5G-debatten er nettopp mangelen på full kunnskap om det elektroniske utstyret som kommer til å inngå i 5G-nettet. Risikoanalyse og risikostyring, slik DSB legger det opp i sin rapport, innebærer først et behov for å få oversikt over verdikjedene og deretter gjøre en informasjons- og kunnskapsinnhenting for å kunne identifisere risiko (Direktoratet for Samfunnssikkerhet- og Beredskap, 2020, s.21). Likevel peker rapporten på hvordan kompleksiteten ved en verdikjede, gjør det umulig å kunne skaffe en sånn full oversikt. Dette i tillegg til hvordan det snakkes om umuligheten for å verifisere elektronisk utstyr i seg selv, bidrar til en mangel kunnskap om sårbarheter (både intenderte og ikke-intenderte) i elektroniske komponenter i 5G-nettverket. Olav Lysne var tydelig å dette i NUPI-debatten: *«Og så vil jeg være.. har jeg lyst til å si at dette problemet her er ikke bare ... bare et Huawei-problem, jeg mener dette er et globalt problem. Altså jeg vil også være helt enig med Orderløkken i at det i og for seg pussig at all ... all diskurs rundt dette dreier seg om Huawei, fordi dette problemet gjelder uansett hvilken leverandør vi skulle velge. Vi ville nødt til å like blind tillit uavhengig av hvem vi velger»* (youtube.com, 2019).

Alle punktene til nå peker på det samme sentrale begrepet innenfor riskification, ulike bakenforliggende faktorer som det snakkes om i 5G-debatten (Corry, 2012, s.247). Poenget og viktigheten med å dra frem alle disse er hvordan flere ulike sider ved 5G-debatten som uttales som utfordringen med 5G-utrullingen og valget av 5G-leverandør. I tillegg hvordan

disse ulike sidene også henger sammen, påvirker hverandre og skaper en kompleksitet som også snakkes om i 5G-debatten. Disse ulike bakenforliggende faktorene synliggjører også de to risikotilnærmingene til Beck og Foucault der begge synes å til en viss grad kunne gjenspeiles i 5G-debatten.

Becks syn på moderne refleksivitet peker på hvordan teknologi, modernisering og digitalisering skaper stadig nye og irreversible risikoer som må håndteres etterhvert som man tilegner kunnskap om teknologiens muligheter og potensial fortløpende (Petersen, 2011, s.700). Det at moderne samfunnet i dag legger vekt på utvikling av ny teknologi som 5G, sammen med en økende kompleksitet gjennom større gjensidig avhengighet i digitale nettverk (digitale verdikjeder) kombinert slutt samfunnets og myndigheters avhengighet av denne teknologien, gjør at samfunnet selv genererer nye og økende risiko for cyber hendelser mot et 5G-nettverk. Derfor utrykkes det i debatten spesielt ved Lysne men støttes også av informant fra departementet, at det ligger en rest-risiko eller usikkerhet i elektronisk komponenter uavhengig av leverandøren. Derfor baseres kjøp av komponenter av kritisk digital infrastruktur må baseres på full tillit (Lysne, 2018).

Men på en annen side har Becks refleksive modernitet blitt kritisert for denne skarpe delingen mellom beregnelige og ikke beregnelige risikoer, og at samfunnet har generert risikoer som ikke lengre er mulig å beregne. Aradau og Van Munster (2007, s.101) argumenterer med bakgrunn i governmentality-tilnæring, at uavhengig av muligheten for å beregne fremtidige risikoer og scenarioer, så viser deg seg at dette ikke nødvendigvis hindrer myndigheter fra å forsøke å implementere tiltak for å håndtere en usikker fremtid: *«Tillit er en viktig del av ethvert samarbeid uavhengig av leverandør, men tillit betyr ikke at man kan utelukke risikoreduserende tiltak. Telenor Norge baserer risikostyring på kunnskap om vår egen infrastruktur, sårbarheter og et løpende arbeid med trusselbildet. Det er Telenor Norge som drifter mobilnettet og som dermed reduserer risiko»,* sa Telenor Norges kommunikasjonssjef Caroline Lunde (tek.no, 2019).

Styring gjennom håndtering av risiko: Resiliens

På bakgrunn av dette søkes det derfor mer mot å forberede seg, og forsøke å endre og styre risiko, og derfor er fokuset innenfor denne forståelsen av cybersikkerhet rette seg innover mot sårbarheter i egne system og objekter eller i referanseobjektet selv (Friis og Reichborn-Kjennerud, 2016: 38). For innenfor risikologikken gir det derfor lite mening med å forsvare seg selv og kjempe imot bakenforliggende forhold for skade, som for eksempel sårbarheter til elektronisk utstyr. Man kjemper men kommer aldri i mål med å undersøke og finne alle sårbarheter i elektronisk utstyr slik Lysne og andre legger vekt på 5G-debatten. Begrepet sårbarhet definerer Lysne 1-utvalget som: *«Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet»* (NOU:13, 2015, s. 31).

For oftest så skjer cyber hendelser gjennom slike ukjente sårbarheter, eller såkalte «zero-day» angrep (Friis og Reichborn-Kjennerud, 2016, s.38). Derfor gir beskyttelsestiltak lite nytte, da ofte hendelser oppdages etter at angrepet eller hendelsen har startet. Perspektivet legger mer vekt på hvordan fremtidige farer ikke forstås som noe som må hindres, da trusselens form og tidspunktet for når en cyber hendelse skjer er i større grad ukjent når det gjelder den vanlige praksisen innenfor cybersikkerhet Corry (2012, s.247).

Det er på bakgrunn av dette at det heller bør fokuseres på å øke resiliens hos referanseobjektet (5G-nettet) for å kunne håndtere hendelser, i motsetning å fokusere på å beskytte seg imot med beskyttelsesmekanismer som et føre-var tiltak. Lysne argumenterte derfor både offentlig i den norske media og i sitt arbeid knyttet til dette, med å håndtere hendelser i 5G-netteverket: *«Både i Lysne I-utvalget og i den boken jeg har skrevet, har jeg argumentert for å håndtere dette problemet gjennom diversitet, slik at ingen enkeltleverandører alene er avgjørende for at vi har en infrastruktur som er trygg»* (dn.no, 2019). Dette betyr at gjennom diversitet, så legges det opp alternativer dersom en leverandør skulle bli forstyrret eller tatt ned gjennom en cyber hendelse, så er det andre leverandører som fortsatt fungerer og dermed hindres hele 5G-nettet (radioaksessdelen) fra å ha nedetid som har videre konsekvenser for individer, samfunn samt viktige og kritiske samfunnsfunksjoner.

Norske myndigheter gjorde nettopp dette, men forbeholdt denne diversiteten til å kunne omfatte selskapet Huawei: *«Rent konkret har vi stilt krav om at leverandører fra land vi ikke*

har sikkerhetspolitisk samarbeid med, ikke kan stå for mer enn 50 prosent av basestasjonene» (e24.no, 2019). Det betyr at dersom Huawei velges av norske mobiloperatører, og selskapet blir rammet av en cyber hendelse eller annen feil, så vil ikke dette før til at hele radioaksessnettet tas ned men at halvparten av 5G-nettet vil fungere. På spørsmål i intervju med avdelingsdirektøren i departementet om hvorfor sikkerhetskravet bare ble stilt til land Norge ikke har et sikkerhetspolitisk samarbeid med, sier hun: *«At dersom at det hadde vært en krise, at vi hadde fått et angrep som satte hele basestasjon-basen da fra Huawei ute av spill, så er vurderingen vår at det ville tatt lengre tid å gjenopprette skaden enn om det hadde vært tilsvarende hendelse og vi kunne stolt på sikkerhetsarbeidet med Sverige»* (informant 6). Dette viser en risikologikk, med hvordan norske myndigheter ikke utelukker en potensiell cyber hendelse i det kommende 5G-nettet, og i tillegg (med samme forståelse rundt verifiseringen av elektroniske utstyr slik som Lysne) ikke har mulighet til å oppdage alle sårbarheter eller implementert funksjonalitet før en eventuell hendelse og dermed hindre et cyberangrep fra å skje.

Føre-var-prinsipp og langsiktig perspektiv på 5G-sikkerheten

Aradau og Van-Münster (2007) argumenterer derfor hvordan slik mangelfull kunnskap om fremtidige hendelser og beregning av risikoer fører med seg en føre-var-logikk. Beck og Foucault har likhetstrekk når det gjelder at det er mindre og større risikoer har blitt vanskelig å beregne på bakgrunn av vitenskapelig usikkerhet, men Foucault ser ikke på hvordan beregnelige og uberegnelige risikoer, men tilsynelatende hvordan uberegnelige risikoer *blir* håndtert. I intervju med avdelingsdirektøren i departementet, synes å synliggjøre dette. I forlengelse av hvordan avdelingsdirektøren henviser avdelingsdirektøren i det ansvarlige departementet til Lysnes teknologiske synspunkt rundt mangelen på verifisering av elektronisk utstyr fortsetter hun med:

«Og når du tar det perspektivet inn over deg at det er teknisk mulig, så må du også forholde deg til at kanskje sannsynligheten er veldig lav, for konsekvensene ville bli veldig store hvis man ville gjøre det. Men da ville mobilnettene og disse 90 prosentene ville kunne være nede faktisk i flere år fordi det tar jo opp til to år hvis man skulle ut på hver eneste site og bygge de på nytt igjen. Og spesielt hvis man skulle ta hensyn til at det var, at da var man kanskje i en alvorlig krise også når dette skjedde. Så hvordan skulle man fått på plass dette nye utstyret

også. Så det er klart at for et samfunn å leve uten mobilnett i ett år eller to, det ville vært ødeleggende sånn virkelig. Så det er den type sårbarhet som vi tenkte da at vi må redusere. Egentlig en sånn konsekvens av en sånn sårbarhet. Og da er det mange som har tatt ordet for at det alltid er bra å ha diversitet og ha flere utstyrsleverandører, det er alltid bra, men det som er viktig er at man har en terskel på også utstyrsleverandøren fra land som man har et sikkerhetspolitisk samarbeid med, så hvis det skulle være en alvorlig hendelse og en krise-situasjon så kan vi jo mer legge til at vi vil kunne raskere løse og få opp igjen disse mobilnettene» (informant 6).

Utsagnet til avdelingsdirektøren er langt, men gjenspeiler i noen grad Aradau og Van-Münster (2007, s.101) argument med hvordan tilsynelatende mer katastrofale uberegnelige risikoer likevel lar seg beregne og håndtert av norske myndigheter gjennom en føre-var-logikk. At det på bakgrunn av presentering av mer katastrofale risikoer gjør risikotiltak ikke gjøres på bakgrunn av det vi vet, men det vi kanskje ikke vet eller ikke har kunnskap om (Aradau og Van-Münster, 2007, s.103). Hvordan risikoer derfor presenteres som worstcase-scenario og/eller irreversible ødeleggelse fører til en forståelse om at alle risikoer sees på som uakseptable og må unngås på alle bekostninger. Derfor utgår ekspert-kunnskap om disse risikoene, da det sees på som utilstrekkelig for politisk håndtering, og risikoredusering og spredning av risikoer sees på som ikke tilstrekkelig.

DSB gjennomførte en risikoanalyse av et scenario med et cyberangrep mot norsk ekom-infrastruktur spesifikt transportnettet (Direktoratet for Samfunnssikkerhet- og Beredskap, 2014, s.188). Det må nevnes at et mobilnettverk er en del av ekomsektoren, men som avhenger av transportnettet, men synes å kunne passe her. Det interessante er hvordan det dette scenarioet kartlegges til å ikke ha noe særlig høy sannsynlighet, men derimot et av de scenarioene totalt sett som har høyest konsekvenser for kostnader ved nedetid eller bortfall. For hvordan sårbarheten i ekom-nettet hadde betydningen for påvirkningen av andre kritiske samfunnsfunksjoner og identifiserte at fem samfunnsfunksjoner som ble påvirket i stor grad, og som videre fører til alvorlige følgerhendelser for befolkningen (Direktoratet for Samfunnssikkerhet- og Beredskap, 2014, s.7). På bakgrunn av dette ligger det mye kunnskap rundt beregning av risikoer. Det viser også hvordan forståelse og håndtering av risiko, uavhengig av sannsynligheten av at den inntreffer eller mangel kunnskap om teknologien, så er konsekvensene så store og dermed uakseptabel at, i tilfelle av 5G-nettet, så gjøres tiltak.

Selv med usikkerhetselementet rundt verifiseringen av elektronisk utstyr til 5G-nettet, synes likevel å gi norske myndigheter kunnskap rundt en betydelig risiko i 5G-nettverkt. Med Lysnes kunnskap om rundt elektronisk utstyr og digital infrastruktur, har man likevel kommet til en kunnskap i form av en usikkerhet, på bakgrunn av blant annet kompleksitet i utstyret og verdikjeder, som gjør at alt utstyr uavhengig leverandør ikke lar seg sjekke. Så selv om det er stor usikkerhet ved det elektroniske utstyret, så hindrer ikke dette norske myndigheter å håndtere dette. Denne usikkerheten men innsikten i rundt verifisering av elektroniske utstyr, kombineres med hvordan norske myndigheter har kunnskap om de potensielle ødeleggende effektene og konsekvensene ved at 5G-nettet tas ned, og hvordan det er denne sårbarheten, lengden på nedetiden, norske myndigheter ønsker å håndtere. Likevel beregner norske myndigheter at en sannsynlighet dette nettopp skjer, er veldig lav.

Selv om det utrykkes som å være alvorlige og uakseptabel risiko ved nedetid i 5G-nettet, foreslås det risikotiltak som er mer risikoreduserende og sprer risikoer ved å vedta sikkerhetskravet om 50 prosent for leverandører fra land Norge ikke har et sikkerhetspolitisk samarbeid med (Huawei). Norske myndigheter har kalkulert seg til at, slik som vist tidligere i analysen, at risikoen om 50 prosent er akseptabelt i den forstand at dersom 50 prosent av 5G-nettet tas ned, truer ikke dette nasjonal sikkerhet. På bakgrunn av dette, synes det ikke som norske myndigheters risikoforståelse av 5G førte til en føre-var-logikk, selv om usikkerhetselementet og mangel på full kunnskap gir en gjenklang om uberegnelige risikoer som synes å være en likhet mellom Beck og Foucault.

For selv om Aradau og Van-Münster (2007) argumenterer for en føre-var-logikk som effekt av håndtering av risiko, argumenterer Corry (2012, s. 248) til at en denne logikken er bare et av flere effekter (og derfor virkemidler) av en risikologikk. Astrup poengterte flere ganger offentlig hvordan det er opp til mobiloperatørene å gjøre sine valg, og i tillegg etter å ha blitt konfrontert med Lysnes utsagn om kinesernes tekniske muligheter til å skru av sykehusene vår og mobilnettene våre, sier han: *«Og dette er jo grunnen til at vi har en dialog med mobilselskapene, NETTOPP om hvordan vi skal utforme sikkerhetskravene på en slik måte at vi kan sikre oss best mulig»* (nrk.no, 2019e). Dette synliggjøres hvordan norske myndigheter fra og med høsten 2018 gikk inn i dialog med et ønske om å utforme sikkerhetskrav for risiko- og sårbarhetsredusering for det kommende 5G-nettverket. Dette kan vise den politiske

effekten ved en risikologikk, ved at håndteringen av sikkerhetsutfordringen ved utrullingen av 5G-nettet innebærer et mer langsiktig styringsperspektiv, enn av å være akutt.

Digitaliseringsministeren legger vekt på å håndtere sikkerhetsfordringen gjennom styringsverktøy som risiko- og sårbarhetstiltak for å håndtere situasjonen, da å forby eller nekte noen aktør ikke hindrer en hendelse å skje i 5G-nettverket: *«Vi må også redusere sårbarhetene i nettene våre over tid. Og det betyr at vi kan ikke gjøre oss av én enkelt leverandør litt uavhengig av hvilken leverandør det måtte være. La oss si at selskapene, de tre mobilselskapene ble enige om at … alle velger Ericsson. Ericsson har en feil som ingen visste om, som gjør at man kan komme inn bakveien eller på en annen måte, så bryter hele nettet vårt sammen. Så, det å redusere sårbarhet og risiko er også en viktig del av hensynene som jeg må ta når vi skal utforme kravene for utrullingen av 5G»,* sier Astrup (nrk.no, 2019d).

Astrups uttalelse og departementets dialog med private aktører, det mer spesielle ved cybersikkerheten. For spesielt i kritisk digital infrastruktur som telekommunikasjon og mobilnettverk er det private selskap som er eiere og dermed ansvarlig for sikkerheten. Men siden denne infrastrukturen i større og økende grad viser seg å få betydning for både samfunnssikkerhet og nasjonal sikkerhet, består cybersikkerheten knyttet til denne typen infrastruktur et komplekst samarbeid mellom offentlig og privat og der privat sektor er aktivt involvert når det gjelder utformingen av sikkerhetstiltak og opprettholdelse av cybersikkerheten (Friis og Reichborn-Kjennerud, 2016: 39). «*Det er jo på en måte vårt minimums krav, vårt krav til sikkerhet, og så vil selskapene selv gjøre de endelige beslutningene om valg av leverandør. Det ønsker ikke vi å blande oss inn i*» (informant 6).

Det Friis og Reichborn-Kjennerud (2016) legger vekt på er hvordan på hvordan tiltak innenfor cybersikkerhet innebærer derfor ofte «myke tiltak» som øke bevisstheten, informasjonsdeling, beste-praksiser på tvers av aktører for å håndtere utfordringer som følger kompleksiteten av aktører og leverandørkjeden som følger med produsering av 5G-nettverket: *«Og da må man heller jobbe sammen på standarder, beste-praksiser, jobbe sammen med konkurrentene våre som vi gjør, delta i alle mulige standardiserings organisasjoner for å heve sikkerhetsnivået globalt og ikke bare peke på at om vi bare plukker ut Huawei så vil alt bare bli mye tryggere og sikrere, det har jeg ingen tro på»,* sier Orderløkken (youtube.com, 2019).

Orderløkkens forståelse av løsningen sikkerhetsutfordringen er peker mer på langsiktige tiltak og investeringer som disse «myke tiltakene» som tiltak for å redusere risiko og sårbarheter. I tillegg hvordan Huawei og Orderløkken legger vekt på etablering av test-sentere slik at kjøpere kan verifisere det elektroniske utstyret, peker mot en slik «myk-tiltak-tankegang». Slike typer risiko- og sårbarhetsreduserende tiltak er forsøk på å transparens og åpenhet enn hemmelighold Corry (2012, s.248). For når Lysne argumenterer med under NUPI-debatten hvor enkelt og reelt det teknisk er for en leverandør å både lekke informasjon og slå utstyret av, sier Huaweis daværende sikkerhetssjef Orderløkken*: «Jeg sier at hundre prosent sikkerhet er ikke mulig. Du må gjøre mange tiltak for å heve sikkerheten … år etter år egentlig, så det der … mange måter å minimere risikoen på, og det er de måtene man må ta tak i»* (youtube.com, 2019). Orderløkken synes å også erkjenne argumentet til Lysne, om den manglende evne i å undersøke fullt ut elektronisk utstyr som foreligger hos alle leverandører, men legger heller til grunn at større transparens gjennom test-senter og de andre myke tiltakene er passende tiltak.

4.2.1 Oppsummering av andre analysedel

Gjennom det teoretiske rammeverket riskification, viser det hvordan 5G-debatten retter oppmerksomheten i større grad innover mot teknologi og egne system. Ikke bare at det er et fokus på og rom for det tekniske, men at dette perspektivet fokuserer på teknologiens materialitet i større grad er aktivt del av diskursen som føres om 5G. Her sees sikkerhetsutfordringen mot 5G-nettverket at det eksisterer en komplekset i form av sårbarheter i både programvare og hardvare uavhengig av leverandørens opprinnelsesland, og som ikke lar seg undersøke fullt ut. I tillegg legges det vekt på hvordan dette igjen påvirkes av en ytterligere kompleksitet ved at det er mange aktører som inngår produsering av programvare og hardvare og å finne ut av hvor disse produseres. I tillegg så utrykkes det hvordan mange av de elektroniske deler hos alle potensielle 5G-leverandører allerede produseres i et land Norge ikke har et sikkerhetspolitisk samarbeid med. Fellesnevneren er uansett hvordan sikkerhetsforståelsen er retten mot bakenforliggende forhold som legger til rette for at en fremtidig uønsket cyber hendelse mot 5G-nettet er mulig.

Fremtredende aktørene 5G-debatten, Olav Lysne og Tore Orderløkken (daværende sikkerhetssjef i Huawei) synes begge å være enige at hundre prosent sikkerhet ikke er mulig, i

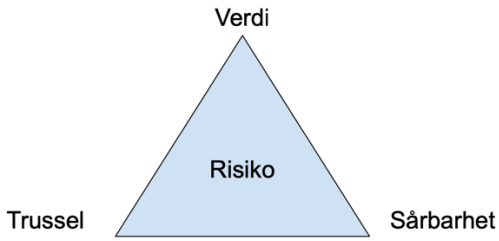
form av å undersøke fullt ut. Derimot mener Lysne at man må ha drive kjøp av 5G-teknologi basert på blind tillit. Han legger heller vekt på redusering av sårbarheter gjennom resiliens og da leverandørdiversitet (styrking av resiliens hos referanseobjektet). Så den dagen det skjer noe, så må vi kunne skru av den delen og være sikker på at Norge har et mobilnettverk som fortsetter å fungere. Orderløkken søker også redusering av sårbarheter, men oppfatter at risikoen kan minimere mest mulig gjennom myke tiltak som test-sentere, vise transparens, beste praksis, drive awareness, og på den måten bygge tillit.

Risikoforståelsen i 5G-debatten viser også hvordan dette fører til et mer langsiktig perspektiv enn at det preges av å være akutt ved at det er et behov å forby selskapet Huawei. Det synes at sikkerheten i 5G-nettet bør og kan håndteres av norske myndigheter gjennom innføring styrking av referanseobjektet dersom det skulle bli en leverandør Norge ikke har et sikkerhetspolitisk samarbeid. Dermed innebærende enn med føre-var-logikk som er mer langsiktig. Derimot, på bakgrunn av det ikke gjøres tilsvarende tiltak for de andre leverandørene (som ble valgt) synes det ikke at nedetid er noe som vil true nasjonal sikkerhet da dette sikkerhetspolitiske samarbeide skal gjøre gjenopprettingstiden raskere og dermed akseptabel.

5.0 Diskusjon: Cyber-sikkerhetisering og cyber-risiko?

Men det er ikke nødvendigvis slik at det er én sikkerhetslogikk eller rasjonale som til enhver tid gjør seg gjeldende når det er snakk om sikkerhetsutfordringer. Det var heller ikke målet med forskningsspørsmålet, da den er ute etter å undersøke en forståelse. Med hvordan moderne samfunn i økende grad står ovenfor sikkerhetsutfordringer som i større grad består av en mer diffuse av karakter, men også i større og økende grad strekker seg transnasjonalt. Riskification er ikke bare med på å undersøke sentrale norske aktørers forståelse av hva som oppfattes som fremtidige sikkerhetsutfordringer knyttet til 5G-nettet og de tiltakene som gjøres for å håndtere dette, men er også med på å synliggjøre en eventuell sikkerhetisering eller tendenser til dette. For i følge Friis og Reichborn-Kjennerud (2016, s.41), vil en analyse av en empirisk case mest sannsynlig kunne finne riskification ved noen tidspunkt, og ved andre tidspunkt kan det å gi et inntrykk av en form for sikkerhetisering. Og i tillegg har en inkludering av disse to teoretiske perspektivene muliggjort en analyse av en sikkerhetsutforing befinner seg i en grense mellom risiko og trussel, som muligens ikke utrykkes som eksistensiell men likevel snakkes om å være alvorlig.

Analysen her synes å synliggjøre hvordan debatten har et fokus på Huawei og Kina og som aktører, og der Kina utrykkes som en trussel, mye knyttet til Kinas sikkerhetslov og norske sikkerhetstjenesters men der det også er et sårbarhetsfokus knyttet til Norges digitale avhengighet og som et av de mest digitaliserte landene i verden og kompleksiteten ved teknologien og verdikjedene som gjør oss ikke i stand til å sjekke for alle mulige sårbarheter. Caset synes å synliggjøre nettopp hvordan det ikke er en sikkerhetsforståelse som preger diskusjonen rundt 5G-utrullingen men hvordan disse kan ha en relasjon til hverandre. Avdelingsdirektøren for en mobiloperatør sa dette knyttet til identifisering og beregning av risiko: *«Men det er ikke noe matematisk øvelse akkurat den sannsynlighetsbiten, det er en kompetanseøvelse altså du må ha god kunnskap egen virksomhet sine sårbarheter og du må ha god kunnskap om trussel aktører og hvilke metoder de bruke og hvordan de opererer»* (informant 5).



Figur 2: Risikotrekant (NSM, 2015:10)

Denne risikotrekanten synes å vise hvordan trussel er deltakende når det gjelder estimering av risiko, men hvordan et fokus på sårbarhet er noe som reduserer risikoen (sannsynligheten for at uønsket hendelse skal skje): *«Risikotrekanten til NSM består av verdi, trussel og sårbarhet. Verdien den kan du gjøre lite med. Trusselen, den kan også gjøre lite med, den er jo der. Det eneste du kan skru på av disse her, det er sårbarhet. Sårbarhet kan du redusere ved å ha diversitet, mer robusthet, spre ting, flere leverandører og så videre. Da kan du redusere risiko-arealet. Og det er den vi kan påvirke»* (informant 4). Derimot viser det at selv om det til stede trussel aktører, så er det sårbarhetene man kan gjøre noe med. Dette synes å være fremtredende ved 5G-debatten, der den ikke preges av den eksistensielle trusselen eller hyper-sikkerhetiseringen men der det er et større fokus på referanseobjektets sårbarhet knyttet til 5G-utrullingen og hvor sårbare vi er og har blitt , noe som er fremtredende innenfor riskification (Corry, 2012, s.247). Det er derfor det snakkes og vektlegges på å håndtere 5G-

utrullingen ved styrking av resiliens hos referanseobjektet (dersom mobiloperatørene skulle velge leverandør fra land som Norge ikke har et sikkerhetspolitisk samarbeid med).

Analysen av 5G-debatten viser spesielt med hvordan en kombinasjon av perspektivet om riskification sammen med Hansen og Nissenbaums (2009) 'teknifisering' har synliggjort mer bredden i aktører som deltar i forming av 5G-debatten og cybersikkerheten rundt. I tillegg er det med på å gi en dypere forståelse av dagens elektronikk og teknologiens mulighetsrom når det kommer til 5G-teknologi som en sannsynliggjører for cyberangrep. For på den måten så synliggjøres hvordan 5G-debatten har en viss likhet mellom cyber-sikkerhetiseringsteorien og risikologikken. Hvordan 5G-debatten preges av å være en teknisk diskurs. Ved å benytte cyber-sikkerhetiseringsteorien har det belyst hvordan diskursen kan synes være preget av en simultan sikkerhetisering og teknifisering, og man med dette fungere på en måte som også kan hindre en sak fra å bli politisert, spesielt når det gjelder mangel på politisk debatt blant politiske folkevalgte, men muligens også ikke blir sikkerhetisert (Hansen og Nissenbaum, 2009:1168). Ved at aktører henviser til det teknologiske faktum at elektroniske utstyr ikke lar seg test uavhengig for utstyret kommer fra, ligger det en usikker der uansett og som må håndteres. For det er med diskursen sin parallelle (og simultane) sikkerhetisering og teknifisering, der gjennom den rasjonelle og tekniske i diskursen at sikkerhetisering gjemmer sine politiske røtter. For eksempel hvordan noen av uttalelsene kan depolitisere saken, ved at konstrueringen av trussel og fiende heller er koblet opp mot en «objektiv» og «nøytral» teknologi (Hansen og Nissenbaum, 2009, s.1168).

Dette tydeliggjøres den tydelige rollen til teknologen Olav Lysne i 5G-debatten, som ytterliggere forsterkes gjennom sin posisjon gjennom det offentlige utvalgsarbeidet om digital sikkerhet i Norge. Han er uten tvil den personen totalt sett uavhengig av sosial posisjon, autoritet og faglige bakgrunn som blir hyppigest intervjuet av norske media og samtidig henvist til av informantene under intervjuene. Han utrykker offentlig hvilke tiltak som burde implementeres, men det gjøres mer koblet ifra på en mer nøytral og objektiv måte ved å ikke knytte sin forståelse av sikkerhetsproblemet opp mot Huawei og Kina, men legger vekt på hvordan dette er et sikkerhetsproblem globalt uavhengig av hvem som er leverandør for 5G-nettet i Norge. Derimot utrykker ikke dette krever en teknisk løsning ovenfor noen annen type løsning, selv om hans forslag og råd peker på en teknologisk løsning ved kontrollert heterogenitet eller diversitet, gjennom at dersom Norge finner ut at det er noen man ikke

kunne stole på så kan man skru av disse delene og fortsatt ha et mobilnettverk som fungerer (Lysne, 2018).

Videre kan det diskuteres hva det innebærer at sikkerhetsforståelsen i 5G-debatten ikke synes å vise hverken en tydelig sikkerhetisering eller cyber-sikkerhetisering, men mer en teknisk diskurs der både teknologisk eksperter og teknologien selv hadde hovedrollen, mens aktører i politiske posisjoner var heller sjelden vare når det kom til 5G-utrullingen i Norge. For det er interessant hvor lite offentlig tilstedeværelse det er har vært når det gjelder involvering og uttalelser fra politiske aktører, og politisk debatt knyttet til 5G-utrulling og leverandørvalget i Norge. Det har også vært vanskelig å få politiske aktører til å stille til intervju. Ved ett tilfelle var svaret på forespørsel om intervju, at informanten ikke kunne noe om dette. Det kan også spekuleres om at siden dette er en sak som i hovedsak omhandlet Kina som Norge har hatt en utfordrende relasjon til tidligere og derfor ikke ønsker å ytre seg eller at det generelt er konsensus knyttet til den saken. Informant med bakgrunn innenfor forskning på sikkerhet og forsvars svarer på dette ved å si: *«Det blir å spekulere, men jeg vil anta det. Og det at det er teknisk vanskelig og krevede og sånt. Men det er ingen partier i Stortinget som er sånn veldig heia Kina lissom. Og noen er mer kritiske enn andre selvfølgelig og noen er mer for fri handel enn andre»* (informant 2).

For noe som skiller cyber-sikkerhetiseringen fra risikologikken, er hvordan risikologikken ikke bare inkluderer det tekniske aspektet men også inkluderer det substansielle ved tekniske. Nettopp at her spiller det teknologiske som det materielle en mer aktiv rolle, og fokuset og forståelsen av sikkerhetsproblemet er vendt mot bakenforliggende faktorer som sårbarheter i egne system og teknologi. Og tar mer utgangspunktet i de digitale systemet i seg selv, og ikke bare teknologiens rolle i form av teknologiske ekspertenes rolle og deres evne til å fremstille 5G-utrullingen som noe som avhenger av teknisk ekspertise og avgjørelse (Friis og Reichborn-Kjennerud, 2016, s.37). For caset om 5G-debatten synliggjører i forlengelse av dette et viktig diskusjonstema når det digitale og teknologiske møter politikk og sikkerhetspolitikk. Når det tekniske møter den folkevalgte. For det første med teknologiske eksperten Lysne sin sentrale rolle i den offentlige debatten, hyppig sitert og intervjuet person, men også arbeidet og ledet utvalgsarbeid om nasjonal digital sikkerhet og har vært rådgiver til regjeringen knyttet leverandørvalget.

Videre, hva kan 5G-debatten fortelle oss utover selve uttalelsene i datamaterialet for analysen. I følge Buzan, de Wilde og Wæver (1998, s.29) bør ikke sikkerhetisering sees på som et ideal, men at målet må være at alle saker befinner seg innenfor en slik politisering. For et vellykket tilfelle av sikkerhetisering, innebærer det at presentering av eksistensielle trusler legitimerer for å bryte vanlige politiske spilleregler og prosesser som nettopp er fundamentet i et demokrati. Målet må vell sies at alle saker som omhandler Norge som nasjon, samfunn og sin befolkning bør behandles innenfor disse spillerreglene. At sakene sak fremstår åpen, har valgmuligheter og er til gjenstand for offentlig debatt. At det er noe som det enes rundt om, og derfor innebærer prinsippet om ansvar og under demokratisk politisk kontroll.

For analysen synes å synliggjøre et større nasjonalt offentlig ansvar i 5G-debatten enn tidligere ved 4G-utrullingen. For det første gjennom hvordan saken behandles innenfor ordinær normal politisk prosedyrer. For når stortingspolitikere ønsker svar og tiltak fra justisminister Wara, responderes dette av digitaliseringsministeren Astrup, og er i henhold til styringsprinsippene innenfor norsk digital sikkerhet og derfor vanlig prosedyre. Prinsipper bygger på ansvarsprinsippet, likhetsprinsippet og samvirkeprinsippet. Ansvarsprinsippet innebærer at departementet som til daglig har et ansvarsområde, for eksempel ekomsektoren i Norge, har også ansvaret for dette i nødvendige sikkerhets- og beredskapsforberedelser og er utøvende organ ved kriser og katastrofer (NOU:13, 2015, s. 61).

På denne måten kan man muligens se en slags «return of the state» slik Deibert og Rohozinski (2010: 30) finner i sin analyse, selv om det i dette tilfelle er et beskjedent tilfelle av statlig involvering, men da muligens en betydningsfull en når det gjelder insentiv for hvilke 5G-leverandør operatørene valgte. For det er ingen tydelig «return of the state» i en tradisjonell måte, men en «heteropolaritet» innebærende flere aktører inkluderende offentlige myndigheter, selskaper men også private globale aktører som leverer og drifter komponenter som inngår infrastrukturen og derfor utgår statlig kontroll (Deibert og Rohozinski, 2010, s.16).

For dette med ansvar innenfor cybersikkerhet krevende, noe analysen av 5G-debatten viser. Med private selskap som eiere av den digitale infrastrukturen, er det disse som har ansvaret for sikkerheten for i sine nett og informasjonen som er der. Det er disse som derfor har ansvar for valg av leverandør. Men man ser i saker der infrastruktur, objekter og informasjon som får en verdi og en betydning for nasjonal sikkerhet, kan norske myndigheter gjøre vedtak å legge

dette under norsk sikkerhetslov noe som ble gjort for ekomsektoren og 5G (Kommunal- og moderniseringsdepartementet, 2019 og 2020). På denne måten kan man si at norske myndigheter i større grad enn tidligere går inn og tar ansvar for norske mobilnettverk enn tidligere, ser dette som en strategisk verdi og viktigere enn noen gang for både norske befolkning, samfunn og nasjon. Men samtidig så synliggjører den offentlige debatten hvordan det er mobiloperatørene som skal gjøre sine valg av leverandør for 5G, noe som ofte blir presisert av Astrup i media, men også av avdelingsdirektøren i departementet: *«Det er vårt minimumskrav, vårt krav til sikkerhet, og så vil selskapene gjøre de endelige beslutningene om valg av leverandør. Det ønsker ikke vi å blande oss inn i»* (informant 6). Dette offentlig-private samarbeidet synliggjøres også med hvordan dette sikkerhetskravet ble utformet i samarbeid og dialog med mobiloperatørene. I tillegg var dette sikkerhetskravet hemmelig for offentligheten inntil valget om leverandør ble gjort.

Risikolitteraturen går inn på hvordan risikostyring og styringsverktøy for å redusere risiko har endret seg gjennom historien og i fremveksten av neo-liberalisme (Aradau og Van-Münster, 2007, s.100). Gjennom et skifte til neo-liberalisme, har dette også ført til et skifte fra kollektiv offentlig ansvar og sosial solidaritet, og mot privat og individuelt ansvar for sin egen sikkerhet. For med den norske privatiseringen av blant annet Telenor (er fortsatt del-eier), fører til en forskyving av makt, kontroll og ansvar for drift og sikkerhet. Men det er tydelig at med 5G, involveres offentlige myndigheter i drifte og sikkerheten i norske telekom-selskap i større grad enn ved for eksempel 4G-utrullingen. *«Så jeg tror det var med 4G, så gikk det litt ... så var det telekom-selskapene som satte og gjorde de vurderingene, det var ikke så mange som stilte spørsmål i andre miljø. Sånn typisk at man kunne stilt krav»* (informant 6). Men det har vært en offentlig evaluering gjennom spørsmål fra Kontroll- og konstitusjonskomiteen på Stortinget rundt offentlige myndigheters ansvar for 4G. Daværende justisminister Grete Faremo skrev: «*I 2010 vurderte NSM hvorvidt sikkerhetsloven og lov om elektronisk kommunikasjon hadde mekanismer for å redusere risiko som beskrevet. Det ble innhentet vurderinger også fra Post- og teletilsynet (nå Nkom) i denne prosessen. NSMs daværende konklusjon var at det forelå en risiko, men at ingen av regelverkene var anvendelige*». Videre sa hun at dette skulle sees nærmere ved utarbeiding av den nye sikkerhetsloven (tek.no, 2018).

Analysen av 5G-nettet synliggjører denne balansegangen og kompleksiteten av ansvar mellom offentlig og privat når det kommer til ansvar for den digitale sikkerheten i det

fremtidige mobilnettet i Norge. Norske myndigheter i større grad ønsker å være mer involvert i utforming av sikkerheten i det fremtidige mobilnettverket i Norge, men samtidig ikke ønsker å involvere seg og ønsker at mobiloperatørene tar selvstendige valg. På denne måten at de kom med et minimumskrav fra offentlig side, noe de ikke har gjort eller hadde mulighet til tidligere. For i den nye sikkerhetsloven fra 2019, er det ny bestemmelse som gir offentlige myndigheter styringsverktøy, og som gir norske myndigheter mulighet til å hindre eller sette vilkår ved selskapers kjøp av skjermverdig infrastruktur som innebærer en ikke ubetydelig risiko. Denne benyttet de seg av ved valget av 5G-leverandør, med vilkår om et sikkerhetskrav 50 prosent på basestasjoner til 5G fra leverandører Norge ikke har et sikkerhetspolitisk samarbeid med (Kommunal- og Moderniseringsdepartementet, 2020).

Dette kan gi en indikasjon på hvordan risikoforståelsen i 5G-debatten kan peke mot en governmentality-tilnærmingen. Hvordan 'dispositif' fungere både som et metodologisk og epistemologisk verktøy for alle de ulike måtene aktørene forsøker å identifisere, beregne og håndtere risikoer knyttet til valg av 5G-leverandør (Aradau og Van-Münster, 2007, s. 97). Spesielt med hvordan den nye sikkerhetsloven fra 2019 gjør det mulig for norske myndigheter å stoppe eller sette krav ved enkeltinnkjøp av kritisk infrastruktur. På denne måten synes norske myndigheter å ha kunnet utnyttet lovverket som styringsverktøy for å gjøre risiko- og sårbarhetsreduserende i det fremtidige 5G-nettet: sende varsel til mobiloperatørene om å gjøre risikoreduserende tiltak, legge ekom-sektoren og deretter 5G-nettet under norsk sikkerhetslov og deretter følge opp med sikkerhetskravet på 50 prosent.

Hva med cyber-resiliens?

Analysen identifiserte gjennom rammeverket om riskification, en sikkerhetsforståelse i 5G-debatten som var preget av et fokus om å håndtere sikkerhetsutfordringen gjennom styring og styrke resiliens hos selve referanseobjektet 5G-nettverket gjennom å legge opp til leverandør-diversitet mot leverandører som kommer fra land Norge ikke har et sikkerhetspolitisk samarbeid med. Dette synes å bringe nysgjerrigheten mot hva et resiliensperspektivet kan kunne komme å bidra med i forklaring av norske sikkerhetsforståelse i 5G-debatten. Konseptet om 'resiliens' innenfor sikkerhet har blitt brukt som et økende perspektiv og operasjonell strategi på innenfor nasjonal sikkerhet og risiko- og krisehåndtering i lys av terrorhendelser i mer moderne tid (Cooper & Walker, 2011: 152). Resiliens har blitt mer fremtredende ved at det ble en økende bekymring rundt nasjonal sikkerhet og kritiske

infrastruktur samtidig med en periode med privatisering av tidligere offentlig infrastruktur- og tjenester (Cooper & Walker, 2011, s.153). Prinsippet om resiliens legger vekt på at trusler mot kritiske infrastrukturer som nettopp ikke kan hindres fullt ut, men legger vekt på enten evnen til å motstå, overleve eller komme tilbake fra en hendelse.

Det er flere grunner til at resiliensperspektivet foreslås som et mulig teoretisk rammeverk som burde undersøkes knytte til 5G-debatten ved en senere anledning:

For det første, så hvordan sikkerhetskravet om til norske myndigheter
50 prosent leverandørdiversitet, vitner om slik risikification synliggjorde i analyse, at cyber hendelser mot 5G-nettet ikke kan hindres fullt ut. Avdelingsdirektøren sa i intervju på spørsmål om hvorfor det ble stilt et sikkerhetskrav på 50 prosent: *«Det handler om rest-risikoen. Og opp mot at det scenariet kunne bli så alvorlig at det tar lang tid å gjenopprette en sårbarhet hvis man skulle står ovenfor et villet angrep, som da kommer innenfra, man kan ikke utelukke det .... det kan man egentlig ikke utelukke fra noen, det kan skje»* (informant 6). En katastrofal hendelse blir i følge resilienslogikken sett på som å skje på bakgrunn av at det er en systematisk begrenset mulighet for offentlig styring og statlig planlegging, og strategien erstatter her kortsiktig hjelpearbeid og respons med et mål om å permanent tilpasning i og gjennom kriser (Cooper & Walker, 2011, s.154). Her legger da avdelingsdirektøren til grunn usikkerheten i elektronisk utstyr og vår evne til å ikke kunne teste og verifisere all elektronikk til 5G-nettet.

For det andre, på spørsmål om hvorfor det ikke ble satt krav om at all 5G-utstyr skulle komme fra land Norge har et sikkerhetspolitisk samarbeid med, sier avdelingsdirektøren: *«Det handler om innovasjon, investeringsvilje. Altså dette er markedslederen Huawei, kommer ikke fra et land Norge har sikkerhetsavtale med men samtidig har vært veldig viktig for den globale innovasjonen som skjer i mobilsammenheng. Så et forbud syns vi ikke ville være nødvendig for det første»* (informant 6). For resiliens som et sikkerhetskonsept har i stor grad basert seg på Foucaults konsept om governmentality, der resiliens som sikkerhetskonsept blir analysert som et styringsverktøy og logikk innenfor et neo-liberale styringsregime som favoriserer marketslogikken. Lysne anbefalte i sitt arbeid og offentlig i media om full leverandør-diversitet, mens norske myndigheter knyttet dette til bare til land Norge ikke har et sikkerhetspolitisk samarbeid med og beregnet en risiko opp til 50 prosent som akseptabelt. På bakgrunn av dette hadde det vært interessant og studert videre mulige politiske implikasjoner

ved praksisen i cybersikkerhet i en tid der det er en tilsynelatende verdiøkning knyttet til å hvordan digital infrastruktur i økende grad oppfattes på en viktigere verdi som skal sikres, men samtidig ønsker en global åpen økonomi og teknologisk økosystem.

For det tredje, når det gjelder å ha et fokus på katastrofale hendelser, innebærer resilienslogikken en kompleks tidsdimensjon med både fortid, fremtid og nåtid som spiller inn og sammen i de tiltak og handlinger som gjøres for sikkerheten sin skyld. Nettopp hvordan man samtidig forsøker å håndtere og komme over hendelser som har skjedd og har materialisert seg, men også hvordan overleve fremtidige ødeleggende hendelser og farer basert på lærdom fra håndtering av hendelser i fortiden. Det er derfor resiliens, til forskjell fra risiko, ikke bare innebærer tiltak redusere sannsynlighet for fremtidige hendelser, men også beredskap og takle hendelsene når det inntreffer (Dunn Cavelty, Kaufmann og Søby Kristensen, 2015, s.7).

Knyttet til 5G-debatten, kunne dette aspektet ved resilienslogikken kastet lys om hvordan sikkerhetsforståelsen kunne ha vært preget av andre tidligere cyberangrep eller hendelser og /eller hvordan 4G-utrullingen ikke var en del av politisk håndtering den gang. Ved hvordan debatten viser at det ønskes en viss diversitet i form alternativer eller sikkerhetskravet om 50 prosent. Dette viser hvordan resilienslogikken kan innebære et nåtidselement ved at et cyberangrep alltid er en vedvarende risiko og dermed må det legges opp til diversitet som kan ta over når det skjer. I tillegg kan fremtidselementet komme til syne med hvordan norske myndigheters sikkerhetsforståelse er preget av et fremtidsperspektiv når det gjelder å ta høyde for ulike scenarioer som fred, krise og krig. I tillegg hvordan man har på bakgrunn av lærdom på bakgrunn av den teknologiske utvikling, økte digitale avhengighet og verdier sammen med at Huawei sto for 90 prosent av mobilnettverket, fikk norske myndigheter til å tenke at dette ikke var godt nok i fremtidsperspektiv (informant 6). For dette er store teknologiske investeringer som blir etablert og er det over et godt stykke tid.

6.0 Konklusjon

Sikkerhetsforståelsen sett i lys av teorien om cyber-sikkerhetisering så viser analysen hvordan i 5G-debatten i stor grad snakkes om hvordan aktøren Kina er en trussel mot Norge og 5G-nettverket, hovedsakelig bakgrunn den påståtte relasjonen mellom kinesiske myndigheter og Huawei. I tillegg påvirkes dette av at Kina er Huaweis opprinnelsesland, og at derfor at hele selskapet globalt er underlagt den relative nye sikkerhetsloven som krever at alle innbyggere og selskap samarbeider med etterretningsvirksomhet om det etterspør. Offentlig så utrykkes dette som å ha sammenheng med de norske sikkerhetstjenestenes identifisering av Kina som en av de største trusselaktørene i det digitale rom. Det blir heller ikke snakket om en eksistensiell trussel i tråd med den opprinnelig sikkerhetiseringsteorien, at hverken 5G-utbyggingen og Huawei snakkes om at trusselen er eksistensiell, såpass akutt, krever den absolutte prioritet og derfor må stoppes gjennom nødtiltak utenfor det vanlig politiske prosessen (Buzan, de Wilde og Wæver, 1998). De potensielle sikkerhetiserende aktørene som norske myndigheter og sikkerhetstjenestene som er deltakende i debatten her artikulerer seg på en sånn måte i 5G-debatten at saken er såpass akutt og truende mot Norge og derfor legge opp til at ekstraordinære tiltak bør implementeres. Selv om debatten ikke avslører at det har vært en sikkerhetiserende aktør i tråd med hvordan hverken Hansen og Nissenbaum (2009) eller Buazan et al. (1998) legger til grunn, synliggjøres analysen en tendens til PST som en sikkerhetiserende aktør, når det gjelder aktørens rolle innflytelse og legitimeringen rundt bekymringen av Huawei.

Utover dette synes ikke analysen å kunne avdekke en sikkerhetsforståelse i 5G-debatten som peker mot en hyper-sikkerhetisering med multi-dimensjonale cyber hendelser med påfølgende følgerhendelser i 5G-nettverket i tråd med Hansen og Nissenbaum (2009). Eneste er kronikken til oberstløytnant Hågen Karlsen fra Forsvaret, der bekymringen om 5G-nettet og Huaweis rolle artikuleres gjennom både hyper-sikkerhetisering, hverdagslige sikkerhetspraksiser og teknifisering. Derimot synes det ikke at dette kan legges noe stor vekt i form av en prosess av cyber-sikkerhetisering, da den ikke henvises til av mange andre eller fører til noe utvikling videre i 5G-debatten. Likevel synes teksten å gi et eksempel på det spesielle innenfor cyber-sikkerheten, med hvordan trusselen blir artikulerte gjennom de tre modusene, en dynamikk som er spesielt for cybersikkerheten. Ikke bare det, hvordan det i tillegg gjøres koblingen mellom individuelle og kollektive referanseobjekt gjennom hvordan det digitale domenet operer og konsekvensene ved at 5G-nettverket påvirkes eller tas ned.

I debatten så artikuleres de aktuelle referanseobjektene til å være både individuelle referanseobjekt som «du» som norske individer og brukere av mobilnettverket. Som kollektive referanseobjekt legges det vekt på norsk suverenitet gjennom at det snakkes om 5G-utbyggingen vil utfordre «nasjonal råderett» og «nasjonal kontroll» over kritisk infrastruktur. På denne måten så dras nasjonal sikkerhet inn i 5G-debatten. Men det snakkes også «samfunnet», «norske økonomien» som kollektive referanseobjekt, noe som

Det som 5G-debatten gir et eksempel på, og som er eget med cybersikkerheten, er hvordan cybersikkerheten nettopp kobler sammen individuelle og kollektive referanseobjekt gjennom hvordan en cyber hendelses multi-dimensjonale effekter kan påvirke på tvers av individ, samfunnet og Norge som stat. Det sentrale innenfor cybersikkerheten er nettopp denne dynamikken og måten referanseobjekt som «nettverket» her sett på som 5G-nettet, «individet» er knyttet til nasjonal- og statssikkerhet (Hansen og Nissenbaum, 2009, s.1171). Men det må poengteres at ingen aktuelle sikkerhetiseringsaktører i 5G-debatten gjør en slik kobling i sine uttalelser. Derimot viser analysen gjennom cyber-sikkerhetiseringsteoriens 'teknifisering', dynamikken mellom sikkerhet og det tekniske som spesielt innenfor cybersikkerheten, og hvordan eksperter i økende grad blir deltakende og definerende «sikkerhetiseringsaktører» i en sak knyttet til cybersikkerhet i det kommende 5G-nettet. Dette synliggjøres gjennom Olav Lysnes tydelige tilstedeværelse i debatten gjennom hvordan han henvises til i nyhetsmedia og er et hyppig intervjuobjekt, men i tillegg henvises til av samtlige informanter til oppgaven. Ikke minst at han står bak offentlige utredninger knyttet til digital sikkerhet og vært rådgiver til norske myndigheter knyttet til denne saken (youtube.com, 2019).

Riskification viser derfor hvordan forståelsen av sikkerhetsutfordringen med 5G-utrullingen ikke har vært preget av å være så akutt med en tilstedeværelse av en eksistensiell trussel og derfor behov for ekstraordinære tiltak behandling av saken utenfor vanlig behandlingsprosess. Spesielt hvordan dette perspektivet får fram hvordan sikkerhetsforståelse i 5G-debatten i stor grad preges av et fokus på sikkerhetsutfordringer i bakenforliggende faktorer bak et cyberangrep. At det er disse faktorene som gjør et cyberangrep mulig. Spesifikt hvordan aktører i debatten legger vekt på sikkerhetsutfordringen i 5G-nettet knyttet til kompleksiteten i form av sårbarheten i elektronisk utstyr (hardvare og programvare), som gjør at dette ikke kan sjekkes fullt ut. Dette kombineres med fokuset på Norges avhengighet til det digitale og

mobilnettverket. Videre følger utfordringen med digitale avhengigheter mellom aktører i levering av 5G-nettverket (verdikjeder), og kompleksitet knyttet til alle deltakende aktører på et globalt nivå som inngår i denne verdikjeden. På bakgrunn av dette synes riskification å ha fått fram en dypere og inngående forståelse for menneskers begrensede mulighet for full kunnskap om teknologiens muligheter i form av intenderte og uintenderte sårbarheter i 5G-utstyret.

Interessant er det hvordan riskification viser en sikkerhetsforståelse hos norske myndigheter der det ikke ønskes å hindre Huawei fra å levere 5G-utstyr, med hensynet til å raskere komme tilbake etter eventuelt bortfall eller cyberangrep gjennom et sikkerhetspolitisk samarbeid synes å være viktigst. På bakgrunn av sårbarheter i *alt* elektronisk utstyr synes det gjøres risiko- og sårbarhetstiltak er forbeholdt leverandører Norge ikke har et sikkerhetspolitisk samarbeid med (sikkerhetskravet om 50 prosent). Videre hvordan det hovedsakelig er viktig for norske myndigheter å balansere mellom investering og global handel og økonomi med sikkerhetshensyn. Det er interessant å se en så offentlig debatt knyttet til en global diskusjon rundt 5G-utrullingen og der politiske delen gjennom tilstedeværelse av politiske aktører har vært så og si ikke tilstedeværende. Med en debatt preget av riskification gjennom en teknisk diskurs, men samtidig hvordan dette tekniske får sin viktighet og alvor knyttet til de risikoreduserende tiltak som ble gjort.

7.0 Kritikk og refleksjoner

Det teoretiske rammeverkets tilnærming og prinsipper, har klart implikasjoner for de muligheter og avgrensinger for hva som har kunnet analyseres her, men som må reflekteres rundt og evalueres. Videre viktigheten av å stille seg kritisk til disse, samt hva andre mulige teoretiske tilnærminger som kunne gjort seg relevant her, drøftes her. I forlengelse av denne kritikken vil det legges fram forslag til videre forskning basert på funnene i analysen her og de potensielle teoretiske rammeverkene.

7.1 Konstruktivistisk tilnærming til forskningsspørsmålet

Både risikoteorien og sikkerhetiseringsteorien baseres på samme konstruktivistiske epistemologiske tilnærmingen på 'sikkerhet' som innebærende et sett diskursive regler (talehandling), og legger ikke vekt på institusjoner og materielle objekters føringer for

sikkerhet (Corry, 2012, s.237). Den post-strukturalistiske diskursive ontologi innebærer en forståelse av språk som grunnlaget og bakgrunnen for hva som blir til. Den politiske diskursen avhenger av bestemte konstruksjoner av problematiseringer og subjektivitet, men at disse også i utgangspunktet blir konstruert gjennom diskursen (Hansen, 2006, s.17). At det er bare gjennom språket at objekter, stater, levende organismer og materielle strukturer får mening og blir utstyrt med en bestemt mening, og at det ikke er noen objektivt utover språklig representasjon (Hansen, 2006:18). Formålet med analysen her er å stille analysere, identifisere og debattere tilstedeværelse av sikkerhetslogikker og ikke en epistemologisk analyse der jeg stiller spørsmål ved om det er nettopp talehandlinger eller praktiserende institusjoner som utgjør den passende vitenskapelige studie av sikkerhet og spesifikk sikkerhetsforståelsen i 5G-nettet (Corry, 2012, s. 239). For med sikkerhetiseringsteorien som hovedsakelig befinner seg innenfor en lingvistisk og sosialkonstruktivistisk tilnærming til sikkerhet og som en mer intersubjektivistisk praksis, har i større grad ignorert rollen til 'ting' i artikulering sikkerhet eller usikkerhet (Aradau, 2010, s.493).

For Aradau (2010, s.492) argumenterer for å se ikke bare se kritisk infrastruktur om en kompleks sammensetning av sosiale praksiser, men hvordan dette springer ut fra hvordan materialiteten muliggjører og avgrenser hva som kan bli sagt og gjort i arbeidet med å sikre 5G-nettet. For 5G-nettverkt er som nevnt en infrastruktur bestående av både hardware og software som bestanddeler for at nettverket kan fungere. Analysen av 5G-debatten, gjennom riskification, synliggjører den sentrale rollen elektroniske utstyret i seg selv når sikkerheten skal utformes og 5G-leverandør skal velges. Analysen sammen med intervjuene avslører hvordan mobilnettverket i seg selv som et objekt og med sin 'løk-struktur' eller arkitektur som tar høyde for «robusthet» og «diversitet», og som videre legger føringer for sikkerhetsforståelsen i 5G-debatten i form av hvilke sikkerhetstiltak som er mulige eller passende. Det er for eksempel innenfor cyber-resiliens en teknisk dimensjon med hvordan nettverket sammensetning og struktur av objekter og tjenester (ledninger, kabler, servere og programvare) som muliggjøre ulike ruter og alternativ, og dermed er prinsipper teknisk redundans med å skape resiliens i 5G-nettverket (Kaufmann, 2013, s. 276). I intervju har informantene utrykt hvordan store deler av sikkerheten av et mobilnettverk allerede bygges opp i standarden og som utvikles internasjonalt, og der handlingsrommet man har nasjonalt er å legge flere sikkerhetsløsninger oppå dette igjen i form av redundans, diversitet og alternativ (informant 4 og informant 5).

Aktør-nettverksteori (heretter ANT) vektlegger også materielle objekters agent-rolle når det gjelder forming av oppfattelse av trussel og deretter legger føringer for de politiske handlinger og løsninger ved uønskede hendelser i cyberdomenet. Tilnærmingen kritiserer den konstruktivistiske tilnærmingen på cyber, ved at hendelser som har effekt for den cybersikkerheten som føres, heller oppstår gjennom materialistiske objekter i den tekniske-sfæren, og at det er dette som ligger til grunnlag for politisk handling. Derfor er det heller et behov for å studere disse hendelsene og hvordan disse opererer, før hendelsene videre blir tolket av politikere, og at derfor spiller diskurs en mindre del i analysen (Balzaq og Dunn Cavelty, 2016, s.180). Derimot var formålet med forskningsspørsmålet å analysere sikkerhetsforståelsen og ikke hvordan sikkerhetiseringen får fram materialiseringen av kritisk digital infrastruktur. Det legges ikke til grunn her at mobilnettverket som kritisk infrastruktur og som et objekt ikke spiller en rolle, men gjennom cyber-sikkerhetiseringens teknifisering og risikologikken fokus på bakenforliggende faktorer identifiserer teknologiens materielle rolle, men hvordan dette fanges opp i uttalelser og talehandlinger i 5G-debatten.

7.2 Kritikk av metodetilnærming

Buzan, de Wilde og Wæver (1998) legger opp til at sikkerhetiseringslogikken studeres direkte gjennom diskursen og ikke gjennom indikatorer, og tillegg baseres teorien opprinnelig på talehandling med det at det er uttalelsen selv som er handlingen. Ved å si ordene, så gjør man noe. Det interessant er ikke om det refereres til noe mer objektivt sant (Buzan, de Wilde og Wæver, 1998, s. 26). At det som skiller seg ut med sikkerhetiseringen er den spesifikke retoriske strukturen som inkluderer at saken handler om overlevelse og handling gis prioritet. Det handler ikke om å konstruere noe som en objektiv trussel og sannhet, om en *faktisk* trussel som er til fare for noen objekter og derfor må beskyttes, men det er heller prosessen med konstrueringen av en delt forståelse av hva som det kollektivt blir sett på og respondert på som en trussel. Ved å inkludere intervju som datamaterialet, kan dette være med på å sette meg i bedre stand til å analysere en eventuell tilstedeværelse av en slik kollektiv og intersubjektiv sikkerhetsforståelse i 5G-debatten.

For en sikkerhetisering er intersubjektiv og sosialt konstruert (Buzan, de Wilde og Wæver, 1998, s. 31). På denne måten kan intervju sette meg i en bedre i stand til å analysere denne dynamikken og konstruksjonen mer inngående og styrke meg i den tolkning av uttalelser som

gjøres i 5G-debatten. Det er derfor ikke bare det at intervju inkluderes, men i tillegg til at informantene er aktører som allerede på en eller annen måte er tilstede i den offentlige debatten fra før av. Sikkerhetiseringen legger allerede vekt på aktørenes kulturelle kapital og sosiale posisjon for å kunne utøve talehandling. Informantene i intervjuene er nettopp i denne sosiale posisjonen, har en kulturell kapital og har derfor en viss autoritet når det gjelder 5G-debatten. Dette er snakk om informanter som tettes på den sikkerheten som føres i 5G-mobilnettverket og ekomsektoren i Norge. Det er snakk om informanter som er avdelingsdirektører i mobilselskap og leverandørselskap som er eiere av mobilnettverket i Norge og leverer teknologi til mobilnettverket. Det er snakk om avdelingsdirektør i departementet som har det offentlige ansvaret for sikkerheten i ekomsektoren og har i tillegg behandlet saken.

Men at å triangulere med intervjudata kan derfor kan styrke tolkningsgrunnlaget mitt. For samtidig sier Buzan, de Wilde og Wæver (1998) at en talehandling ikke defineres gjennom å uttale ordet «sikkerhet», men at det tolkes her som at denne talehandlingen innebærer en større sammensetning av delt kollektiv konstruering av en eksistensiell trussel som innebærer et behov for raske nødtiltak og at dette aksepteres av store deler av det relevante publikumet i den aktuelle saken. For sikkerhet er en mer generell form som har en distinkt mening, men som varierer i form. Sikkerhet i følge Buzan, de Wilde og Wæver (1998: 27) betyr overlevelse i møte med eksistensielle trusler, men hva som sees på som å være en eksistensiell trussel er ikke den samme på tvers av sektorer. Dette er nettopp på bakgrunn av den intersubjektive og sosiale konstruering av trussel, som nevnt ovenfor. På bakgrunn av dette, argumenteres det at en inkludering og triangulering av intervju kan bidra til å analysere denne konstrueringen av trussel og variasjoner på tvers av sektorer som er deltakende i 5G-debatten. Jeg var heller varsom i analyseprosessen, å se under hvilke omstendigheter og sosiale betingelser en sikkerhetiseringslogikk kunne gi indikasjoner av en sikkerhetisering i 5G-debatten, og at dette må dokumenteres i resultatet i oppgaven.

Når det gjelder beslutningen med å ikke benytte diskursanalyse i tråd med Hansen (2006), var dette på grunnlag av hvordan sikkerhetiseringsteorien har sitt eget analytiske rammeverk for analysering av sikkerhetisering (Buzan, de Wilde og Wæver, 1998, s.25). I tillegg så var ikke formålet forskningsspørsmålet å analysere en sikkerhetsforståelse i form av en kollektiv virkelighetsforståelse men heller identifisering av disse teoretiske perspektivene mer direkte ut av tekstmaterialet.

7.4 Annen kritikk og begrensinger ved studien

Hovedutfordringen med analysen synes å være kombinasjon av bruk av flere teoretiske perspektiv sammen med metodetriangulering, noe som har vært utfordrende. Det er utfordrende å behandle et så stort datamateriale (intervju og dokument), få oversikt og strukturere det men også å transkribere alt. Det er i alle fall tidkrevende for alle som skulle vurdere noe lignende. På en annen side, synes jeg å ikke kunne være foruten intervjumaterialet. Det har gitt en helt ny innsikt knyttet til kvalitativ forskning, og hvordan dette har gitt meg en annen kunnskap men også inngående dybdekunnskap i sammenhenger knyttet til faktiske empiriske prosesser og hendelser.

Det har vært krevende å forstå lesingen av sikkerhetiseringsteorien når det gjelder hvordan det empiriske materialet skal leses og kodes. For samtidig som den synes å ha et handlingsrom, stiller den samtidig visse krav og betingelser. Med hvordan den legger opp til visse at det er visse sikkerhetiseringsaktører som er privilegerte og kan uttale seg om sikkerhet og sikkerhetisere, synes denne analysen å vise hvordan mindre synlige aktører deltar i debatten. Ikke bare det men på bakgrunn av intervju med informantene samt forsøkene med å få intervjue politikere viser hvordan det ikke ønskes å snakke for mye om saken på bakgrunn av det inngår en del av nasjonal sikkerhet og kritisk infrastruktur. Hvordan kan da et teoretisk rammeverk som baserer seg på talehandling da fange opp hvordan saker blir en del av norsk sikkerhet, når den synes å omfatte deler av nasjonal sikkerhet allerede men den følger ikke denne prosedyren om talehandling.

7.5 Forslag til videre forskning

På bakgrunn av diskusjonen om muligheten for at et resiliensperspektiv på dette case kunne bidra med å forklare visse sider ved sikkerhetsforståelsen i 5G-debatten knyttet til sikkerhetshåndtering- og forståelse følger neo-liberalisme og kapitalisme knyttet til et ønske om å gjøre sikkerhetsvurderinger opp mot et ønske om mest mulig frihandel og åpen og global økonomi. Det hadde vært interessant å gå nærmere inn på dette, og studere og reflektere rundt eventuelle implikasjoner det har for sikkerheten og hvordan disse to hensynene skal eller bør møtes. Hvilke implikasjoner har det ved en eventuell sånn sikkerhetspraksis- og forståelse?

Ikke bare det, men på bakgrunn av et mulig resiliensperspektiv det hadde også vært interessant og tatt utgangspunkt i teoretiske rammeverkene til enten Balzacq og Cavelty (2016) eller Aradau (2010) og studert mer inngående rollen til det materielle, selve 5G-infrastrukturen og mobil infrastrukturen, knyttet til 5G-utrullingen. Hvordan denne infrastrukturen i seg selv har en teknisk dimensjon, et teknisk sikkerhetsnivå gjennom sin arkitektur og inneholdende tekniske prosedyrer for å skape resiliens. Det å videre forstå hvordan dette spiller inn på menneskers problematiseringer og forståelser av fremtidige farer, uønsket hendelser, trusler og risikoer (Kaufmann, 2013, s.276). Dette kombinert med hvordan globale verdikjeder synes å ha fått en endret persepsjon når det gjelder bekymring rundt Huawei som en mulig trussel og risiko, og hvordan private selskap synes å få en geopolitisk verdi (Lysne, Elmokashfi, Schia, Gjesvik og Friis, 2019s. 15).

I forlengelse av på bakgrunn av hvordan 5G-debatten i stor grad omhandlet og gikk inn hvordan man ikke kan teste elektronisk utstyr og samt kompleksiteten til dagens elektroniske utstyr, hadde det vært interessant og tatt utgangspunktet Aradau (2014, s.76) analyse av hvordan og på hvilken måte denne kunnskap legger til grunn for visse problematiseringer om fremtidige usikre hendelser, og som resilienslogikken kan gi en løsning på og eventuelt kontrollere. Umiddelbart synes 5G-debatten å kunne omhandle i mellom to epistemiske regimer: risk/uncertainty og surprise/novelty. For hvordan 5G-nettet som mobilnettverk med sin kompleksitet i form av nettverksstruktur og verdikjeder kan innebære en usikkerhet der fremtidige hendelser alltid mulig og fremvoksende og der det ukjent ikke kan gjøres kjent gjennom risikostyring (Aradau, 2014, s.77).

Ikke minst, hadde det på bakgrunn av en inngående analyse av bare Norge som case, hadde det vært interessant og gjort komparativt case for å analysere en videre variasjon når det gjelder sikkerherhetsforståelse i 5G-debatten som har vært så fremtredende over hele verden og som har ført til at EU har gjort en helhetlig risikovurdering av cybersikkerheten i 5G-nettverket, men også pålagt sine medlemsland å gjøre enkeltstående risikoanalyser (EU, 2019). Dette kan gi en mulighet til å analysere en større variasjon når det gjelder tilstedeværelse av en cyber-sikkerhetisering/sikkerhetisering og/eller riskification, noe som gir større innsikt og implikasjonene eller effektene ved en slik forståelse eller tilstedeværelse av sikkerhetslogikk(er).

Det hadde på bakgrunn av denne analysen vært interessant og gjort en normativ analyse knyttet til hvordan og på hvilken måte det digitale påvirker norsk sikkerhetspolitikk men også relasjonen mennesker, det digitale og norsk sikkerhetspolitikk. For analysen kan viser hvordan digitale enheter, infrastruktur og informasjonen som er innenfor der i økende grad sees på som ha en strategisk verdi når man ser hvordan 5G-nettverket underlegges norsk sikkerhetslov. På bakgrunn av dette kan man kanskje spekulere i betydningen av at stadig flere digitale enheter, infrastruktur og tjenester rundt betraktes som kritisk infrastruktur.

Basert på norske myndigheters vektlegging av et sikkerhetspolitisk samarbeid innenfor cybersikkerheten når det gjelder evne til å komme tilbake fra bortfall eller cyberangrep, hadde det vært interessant og undersøkt temaet om internasjonalt cybersikkerhetssamarbeid, hvordan dette gjøres og hvilke utfordringer som er med ulike staters sikkerhetspolitiske interesser kombinert med en cyberspace som kjenner ingen territorielle grenser, politiske skillelinjer eller ideologi.

Litteratur

Aradau, Claudia & Rens Van Munster. (2007). *Governing Terrorism Through Risk: Taking Precautions, (un)Knowing the Futur*e. European Journal of International Relation. Sage Publications and ECPR European Consortium for Political Research Vol. 13(1): s. 89-115.

Aradau, Claudia, Luis Lobo-Guerrero & Rens Van Munster (2008). *Security, Technologies of Risk, and the Political: Guest Editors' Introduction'*. Security Dialogue – Special Issue on Security, Technologies of Risk, And the Political, 39 (2-3): s. 147-154

Aradau, Claudia (2010). *Security That Matters – Critical Infrastructure and Objects of Protection*. Sage Publications i Security Dialogue Vol. 41(5): 491-514,

Aradau, Claudia (2014). *The promise of security: resilience, surprise and epistemic politics*. Resilience, 2:2, s. 73-87, DOI: 10.1080/21693293.2014.914765

Balzacq, T., Cavelty, D. M. (2016). *A theory of a actor-network for cyber-security*. European Journal of International Security, Vol. 1, part 2, s. 176-198. British International Studies Association.

Beckmann, N. M., Hall, L. R. (2013). *Elite Interviewing In Washington, DC*. Kapittel 10 i Mosley, Layna (2013, ed.): Interview Research in Political Science. Pp. 196-208. Ithaca, N.Y.: Cornell University Press.

Betz, D. J., Stevens, T. (2013). *Analogical reasoning and cyber security*. Security Dialogue 22(2), s. 147-164.

Beyers, J., Braun, C., Marshall, D. & de Bruycker, I. (2014). *Let's Talk! On the practice and method of interviewing policy experts*. Interest Groups & Advocacy, vol 3, no. 2, s. 174-187

Bleich, E., Pekkanen, R. (2013). *How to Report Interview Data*. Kapittel 4 i Mosley, Layna (2013, ed.): Interview Research in Political Science. Pp. 84-108. Ithaca, N.Y.: Cornell University Press.

Bratberg, Ø. (2007). *Tekstanalyse for samfunnsvitere*. 2.utgave. Cappelen Damm Akademisk. Oslo, Norge.

Bryman, A. (2016). *Social Research Methods*. Fifth Edition. Oxford University Press.

Buzan, B., de Wilde, J., Wæver, O. (1998). *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Center for a New American Security (2020). *Sharper The 5G – Analysis from CNAS experts on the most critical challanges in U.S. foreign policy*. Hentet fra: https://www.cnas.org/publications/commentary/sharper-5g-future 28.04.20

Cooper, M., Walker, J. (2011). *Genealogies of resilience: From systems ecology to the political economy of crisis adaption*. Special Issue on The Global Governance of Security and Finance. Security Dialogue 42(2): s. 143-160.

Corry, O. (2012). *Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change*. Millenium: Journal of International Studies, 40 (2): s. 235-258.

Corry, O. (2014). *From Defense to Resilience – Environmental Security beyond Neo-liberalism*. International Political Sociology 8: s. 256-274.

Dagbladet.no (2019). *Huawei-bråket: Krever Huawei-svar, men Wara vil ikke ta spørsmålet*. Hentet fra: https://www.dagbladet.no/nyheter/krever-huawei-svar-men-wara-vil-ikke-ta-sporsmalet/70742781
Publisert 08.02.19. Hentet 03.01.20

Dagens Næringsliv (2019). *Anbefaler flere leverandører for å hindre spionasje*. Hentet fra: https://www.dn.no/telekom/mobilnett/spionasje/huawei/anbefaler-flere-leverandorer-for-a-hindre-spionasje/2-1-546244. Publisert: 20.02.19. Hentet: 02.04.20.

Deibert, J. R., Rohozinski, R. (2010). *Risking Security: Policies and Paradoxes of Cyberspace Security*. International Political Sociology 4, s. 15-32. International Studies Association.

Direktoratet for samfunnssikkerhet og beredskap (2020). *Risikostyring i digitale verdikjeder*. Tilgjengelig fra: https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf Hentet: 02.03.20

Direktoratet for samfunnssikkerhet og beredskap. (2016) *Samfunnets kritiske funksjoner*. Tilgjengelig fra: https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf Hentet: 02.03.20

Direktoratet for samfunnssikkerhet og beredskap (2014). *Nasjonalt risikobilde 2014*. Tilgjengelig fra: https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014.pdf Hentet: 02.03.20

Dunn Cavelty, Myriam. (2007a). *Cyber-Terror – Looming threat of Phantoom Menance? The Framing of the US Cyber-Threat Debate*. Journal of information technology & politics, Vol. 4 (1), s. 19-36.

Dunn Cavelty, Myriam (2007b). *Securing the digital age*. i *International Relations and Security in the Digital Age,* red. Eriksson, J. Og Giacomello, G, pp. 87-105. Routledge, USA.

Dunn Cavelty, Myriam. (2008a). *Cyber-Security and Threat Politics: Us Efforts to Secure the Information Age*. London: Routledge.

Dunn Cavelty, Myriam (2008b). *Like a pheonix from the ashes: The reinvention of critical infrastructure protection as distributed security*. kapittel 3 i boka: «Securing 'the Homeland': Critical infrastructure, risk and (in)security», s. 40-62. London: Routledge

Dunn Cavelty, Myriam. (2013). *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in Cyber-Security Discourse*. International Studies Review 12 (1): s. 105-22.

Dunn Cavelty, Myriam. (2018). «Cybersecurity Research Meets Science and Technology Studies». Politics and Governance, Volume 6, Issue 2, pp. 22-30. Lisboa: Cogitatio.

Etterretningstjenesten (2020). *Fokus 2020*. Tilgjengelig fra: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/Fokus%202020.pdf/_/attachment/inline/639faaf2-7009-4056-9e0d-6dc5a6c5519b:1b228e374a207c8f79b1d8a166d902d7c0edd5e1/Fokus%202020.pdf Hentet: 04.10.20

Europeiske Union (2019). *EU coordinated risk assessment of the cybersecurity of the 5G network*. Report from NIS Cooperation Group. Tilgjengelig fra: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security Publisert 09.10.19. Hentet 11.10.19.

E24.no, (2018). *Regjeringen vurderer tiltak som kan ramme Huawei*. Hentet fra: https://e24.no/boers-og-finans/i/oRozGV/regjeringen-vurderer-tiltak-som-kan-ramme-huawei. Publisert 16.12.18

E24.no, (2019a). *Handelskrig og sikkerhetspolitikk påvirket Telias 5G-valg: - Men vi kunne valgt Huawei*. Hentet fra: https://e24.no/teknologi/i/g7KLj9/handelskrig-og-sikkerhetspolitikk-paavirket-telias-5g-valg-men-vi-kunne-valgt-huawei Publisert 08.10.19. Hentet: 28.04.20.

E24.no, (2019b). *Mistilliten mot Huawei – Regjerings ukjente krav rammet Huawei*. Hentet fra: https://e24.no/teknologi/i/GG2l44/regjeringens-ukjente-krav-rammet-huawei Publisert 13.12.19. Hentet: 28.04.20

E24.no, (2019c). *Teleselskapene visste om regjeringens «Kina-krav»: Telenor vil bruke Huawei-utstyr likevel*. Hentet fra: https://e24.no/teknologi/i/RR2bv8/teleselskapene-visste-om-regjeringens-kina-krav-telenor-vil-bruke-huawei-utstyr-likevel. Publisert: 13.12.19. Hentet: 05.04.20

Friis, K., Reichborn-Kjennerud, E. (2016a). *From cyber threats to cyber risks*. I Friis, K., Ringsmose, H. (eds.), Conflict in Cyberspace. Abingdom: Routledge, pp. 27-44.

Gerring, J. (2004). *What Is a Case Study and What Is It Good For?*. American Political Science Review, Vol. 98, No. 2.

Gerring, J. (2017). *Qualitative Methods*. The Annual Review of Political Science, 20:s. 15-36.

Greenwald, G. (2014). *Overvåket: Edward Snowden, NSA og overvåkningsstaten*. Cappelen Damm. Oslo

Hansen, L. & Nissenbaum, H. (2009). *Digital Disaster, Cyber Security, and the Copenhagen School*. International Studies Quarterley, Vol. 53, s. 1155-1175.

Hansen, L. (2006). *Security as Practice: Discourse analysis and the Bosnian war*. Routledge

Hellevik, O. (2011). *Forskningsmetode i sosiologi og statsvitenskap*. Universitetsforlaget AS. Oslo.

Kaufmann, M. (2013). *Cyber-resiliens i EU*. Internasjonal Politikk, Årgang 71, Nr. 2, s. 274-283. Norsk Utenrikspolitisk Institutt. Universitetsforlaget. Oslo.

Kommunal- og Moderniseringsdepartementet (2020). *Sikkerhetsloven – krav om «forsvarlig sikkerhet» for neste generasjons mobilnett, 5G*. Internt dokument datert til 14.01.20.

Kommunal- og Moderniseringsdepartementet (2019). *Sikkerhetsloven – vedtak om at virksomhet underlegges loven*. Datert til 05.09.19.

Leech, L. Beth, Baumgartner, R. Frank, Berry, M. Jeffrey, Hojnacki, Marie, Kimball, C. David (2013). *Lessons From The «Lobbying And Policy Change» Project*. Kapittel 11 i Mosley, Layna (2013, ed.). *Interview Research in Political Science*. s. 196-208. Ithaca, N.Y.: Cornell University Press.

Levy, S. J. (2008). *Case Studies: Types, Designs, and Logics og Inference*. Conflict Management and Peace Science. Sage Publications

Libicki, C. M. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation. ProQuest Ebook Central.

Lynch, J. (2013). *Aligning Sampling Strategies With Analytical Goals*. Kapittel 1 i Mosley, Layna (2013, ed.): Interview Research in Political Science. Pp. 31- 44. Ithaca, N.Y.: Cornell University Press.

Lysne, O., Elmokashfi, A., Schia, N. N., Gjesvik, L., Friis, K. (2019). «Critical Communication Infrastructure and Huawei». Tilgjengelig gjennom: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3426222

Lysne, O. (2018). *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?*. Simula SpringerBriefs on Computing Volume 4.

Norsk Kommunikasjonsmyndighet (2020). «EkomROS 2020: Den digitale grunnmuren». Tilgjengelig fra: https://www.nkom.no/aktuelt/nkoms-risikovurdering-av-ekomsektoren-for-2020 Hentet: 20.10.2020

Norsk Kommunikasjonsmyndighet (2019). *EkomROS 2019: Den digitale grunnmuren*. Tilgjengelig fra: https://www.nkom.no/rapporter-og-dokumenter/ekomros-2019 Hentet: 03.03.20

Norsk Sikkerhetsmyndighet (2020). *Risiko 2020*. Tilgjengelig fra: https://nsm.no/getfile.php/131421-1587034764/Hermans%20undermappe%20med%20bilder/NSM_Risiko_2020_web_0104.pdf Hentet: 03.03.20

Norsk Sikkerhetsmyndighet (2015). *NSM Sikkerhetsfaglig råd*. Tilgjengelig fra: https://www.regjeringen.no/globalassets/departementene/fd/dokumenter/rapporter-og-regelverk/nsm-sikkerhetsfaglig_raad_2015_web.pdf Hentet: 04.10.20

NOU 2015: 13. (2015). *Digital sårbarhet – Sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Tilgjengelig gjennom: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf 02.03.20

NOU 2000:24. (2000). *Et sårbartsamfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet*. Hentet fra: https://www.regjeringen.no/contentassets/1c557161b3884335b4f9b89bbd32b27e/no/pdfa/nou200020000024000dddpdfa.pdf 02.03.20 .

Nrk.no (2019a). *Dagsrevyen – Huawei er bekymret over justisministerens uttalelser*. Hentet fra: https://tv.nrk.no/serie/dagsrevyen/201901/NNFA19011019/avspiller. Publisert 10.01.19. Hentet: 18.05.20.

Nrk.no (2019b). *Urix 30.jan.2019 – Huawei og samfunnssikkerhet*. Hentet fra: https://tv.nrk.no/serie/urix/201901/NNFA53013019/avspiller. Lastet ned: 11.05.20

Nrk.no (2019c). *PST advarer: - Vær oppmerksom på Huawei*. Hentet fra: https://www.nrk.no/norge/pst-advarer_-_-vaer-oppmerksom-pa-huawei-1.14414252 Publisert 04.02.19. Lastet ned: 30.03.20

Nrk.no (2019d). *Dagsrevyen*. Hentet fra: https://tv.nrk.no/serie/dagsrevyen/201902/NNFA19020419/avspiller. Publisert: 04.02.19. Hentet: 15.05.20

Nrk.no (2019e). *Debatten: I lomma på Kina*. Hentet fra: https://tv.nrk.no/serie/debatten/201902/NNFA51021219/avspiller. Publisert: 12.02.19. Hentet: 15.05.20.

Nrk.no (2019f). *Dagsrevyen: 11. Telia vraker Huawei*. Hentet fra: https://tv.nrk.no/serie/dagsrevyen/201910/NNFA19100819/avspiller. Publisert: 08.10.19. Hentet: 15.05.20.

Nrk.no (2019g). *Søndagsrevyen: Huawei ute av 5g-nettet*. Hentet fra: https://tv.nrk.no/serie/dagsrevyen/201912/NNFA03121519/avspiller. Publisert: 15.12.19. Hentet: 15.05.20.

Nrk.no (2019h). *Huawei tilbyr Norge en «No-spy-agreement»*. Hentet fra: https://www.nrk.no/norge/huawei-tilbyr-norge-en-_no-spy-agreement_-1.14553738 Publisert 16.05.19. Hentet fra: 25.10.20

Nrk.no (2019i). *Dagsrevyen: Telenor – 5G*. Hentet fra: https://tv.nrk.no/serie/dagsrevyen/201912/NNFA19121319/avspiller Publisert 13.12.19. Hentet: 18.05.20.

Petersen, L. K. (2011). *Risk analysis – A field within security studies?*. European Journal of International Relations, 18(4) s. 693-717.

Politiets Sikkerhetstjeneste (2019). *Trusselvurdering 2019*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2019/. Lastet ned: 30.03.20

Politiets Sikkerhetstjeneste (2020). *Trusselvurdering 2020*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/ Lastet ned: 30.03.20

Regjeringen (2019). *5G*. 26.04.2019. Hentet fra: https://www.regjeringen.no/no/tema/transport-og-kommunikasjon/elektronisk-kommunikasjon/ekomartikler_2019/5g/id2642585/ 28.04.20

Repstad, P. (1993). *Mellom nærhet og distanse. Kvalitative metoder i samfunnsfag*. 2. utgave. Oslo: Universitetsforlaget.

Repstad, P. (2007). *Mellom nærhet og distanse. Kvalitative metoder i samfunnsfag*. 4. utgave. Oslo: Universitetsforlaget.

Samferdselsdepartementet (2018a). *Sikkerhet i ekomnettet*. Internt dokument datert 09.11.18. Oslo

Samferdselsdepartementet (2018b). *Varsel om tydeliggjøring av sikkerhetskrav til utstyrsleverandører i norske ekomnett*. Internt dokument datert 05.12.18. Oslo

Regjeringen.no (2014). *Regjeringen nedsetter digitalt sårbarhetsutvalg*. Hentet fra: https://www.regjeringen.no/no/aktuelt/Regjeringen-nedsetter-digitalt-sarbarhetsutvalg/id764159/ Publisert 20.06.14. Besøkt: 13.10.20

Schwartz-Shea, Peregine og Dvorva Yanow (2012). *Interpretive research design: Concepts and methods*. 1. utgave. New York: Routledge.

Tek.no (2018). *Huawei stenges ute i flere land – i Norge får det store kontrakter*. https://www.tek.no/nyheter/nyhet/i/BRm5QE/huawei-stenges-ute-i-flere-land-i-norge-far-de-store-kontrakter . Publisert 27.08.19. Hentet: 30.03.20

Tek.no (2019). *Sikkerhetsekspert om Huawei-situasjonen: - Dette er et problem fra helvete*. Hentet fra: https://www.tek.no/nyheter/nyhet/i/kJe47B/sikkerhetsekspert-om-huawei-situasjonen-dette-er-et-problem-fra-hel Publisert 19.06.19. Hentet: 30.03.30

The White House (2019). *Executive Order on Securing the Information and Communications Technology and Services Supply Chain*. Hentet fra: https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/ 27.04.20.

Tv2.no (2019a). *Hva er det egentlig med Kina og Huawei?*. Hentet fra: https://www.tv2.no/nyheter/10397549/. Publisert 06.02.19. Hentet: 30.03.20

Tv2.no (2019b). *Dette skrekk-scenariet bekymrer ekspertene*. Hentet fra: https://www.tv2.no/a/10397350/ . Publisert 08.09.19. Hentet: 30.03.20

Tv2.no (2014). *PST frykter kinesisk 4G-spionasje*. Hentet fra:https://www.tv2.no/2014/02/09/nyheter/innenriks/spionasje/huawei/5279820 Publisert: 14.09.19. Hentet: 30.03.20

Youtube.com (2019). *Huawei: En risiko eller ikke?* Hentet fra: https://www.youtube.com/watch?v=IgXq_aCi9GA Publisert: 06.03.19. Hentet: 11.05.20

Vedlegg

Vedlegg 1: Oversikt over informanter til intervju

Navn	Stilling	Organisasjon
Informant 1	Professor i informasjonssikkerhet	Universitet
Informant 2	Seniorforsker	Forskningsinstitutt
Informant 3	Avdelingssjef	Mobilleverandør
Informant 4	Seniorrådgiver i ICT	Norsk Sikkerhetsmyndighet
Informant 5	Avdelingssjef	Mobiloperatør
Informant 6	Avdelingsdirektør	Departement
Informant 7	Avdelingsdirektør	Mobiloperatør

Vedlegg 2: Informanter som ble forsøkt kontaktet men som ikke førte fram.

Politiets Sikkerhetstjeneste (PST)	Sikkerhetsmyndighet
Etterretningstjenesten (E-tjenesten)	Sikkerhetsmyndighet
Norsk Kommunikasjonsmyndighet (Nkom)	Fagmyndighet og regulator av ekom under KMD
Telia	Mobiloperatør
Olav Lysne	Professor i digital infrastruktur- og sikkerhet
Lene Vågslid	Stortingsrepresentant (Arbeiderpartiet)
Sigbjørn Gjelsvik	Stortingsrepresentant (Senterpartiet)
Anders Werp	Tidligere statssekretær i Samferdselsdepartementet (Høyre)
Trine Schei Grande	Stortingerepresentant (Venstre)

Vedlegg 3: Det utfylte analyseskjemaet over sikkerhetslogikkene

Begrep	Beskrivelse	Analytiske spørsmål	Empiri

<u>Cyber-sikkerhetisering</u>			
Sikkerhetiseringsaktør	Sikkerhetiserende aktører som gjennom talehandling talesetter en eksistensiell trussel mot et referanseobjekt og krever ekstraordinære løsninger og tiltak.	Hvem snakker om en eksistensiell trussel i 5G-debatten?	PST Etterretningstjenesten Tor Mikkel Wara Hågen Karlsen (Oberstløytnant) (Amerikanske Myndigheter)
Referanseobjekt: a)Individuelt	Objekter som snakkes å være eksistensielt truende og som har et kollektivt, legitimt krav for å overleve.	Hvem og hva er det i det norske samfunn som skal skjermes og bør beskyttes?	a)Norske individ som digitale brukere, mobilnettverket
b)Kollektiv			b)Nasjonal råderett, nasjonal kontroll, norsk suverenitet, Norge, norsk kritisk infrastruktur/kritisk

			samfunnsfunksjoner, viktige samfunnsfunksjoner, norske samfunn, norske økonomi
Eksistensiell trussel	Et emne som snakkes om å være en eksistensiell trussel mot et referanseobjekt.	Hva eller hvem snakkes det om å være trusselen?	Kina Cyberangrep fra Kina: spionasje, informasjonsinnhenting, tyveri. Kinas «Silkeveien»: Strategiske globale oppkjøp og investering Tilknytning mellom selskapet Huawei og kinesiske myndigheter. Kinesiske sikkerhetsloven Leverandør av kritisk infrastruktur fra land Norge ikke har sikkerhetspolitisk samarbeid med
Ekstraordinære tiltak	En løsning eller tiltak mot den eksistensielle trussel som overskrider normale politiske prosedyrer og normer.	Hvilke tiltak ble satt i verk i prosessen mot valg av leverandør? Var det unntatt den normale politiske	XXXXXXXXXXXX

Aksept (relevant publikum)	Det relevante publikum som talehandlingen vender seg til, aksepterer bruken av ekstraordinært tiltak og dermed avgjør om	demokratiske prosessen? Hvordan var responsen til myndighetenes tiltak blant politiske folkevalgte og eksperter (og media?)	Stortingspolitikere og media deler PSTs bekymring knyttet il Huawei og Kina som trussel aktør i deg digitale domenet. Ingen uttrykt motsettelse til tiltaket gjort fra departementet. Opposisjonspolitiker ønsker et nordisk industrisamarbeid om telekom. Opposisjonspolitikere (Sp og AP) deler bekymring til PST og er ute etter tiltak fra justisminister. Men hvilke tiltak utrykkes ikke.

Begrep	Beskrivelse	Analytiske spørsmål	Empiri

<u>Cyber-risiko</u> Bakenforliggende forhold for sannsynligheten for angrep	Bakgrunnsfaktorer for muliggjøring av handling: Avhengighet av og mellom digitale system og teknologi, sårbarhet, motstandsdyktighet. Kompleksitet, Sannsynlighetskalkulering.	Snakkes det om det materielle? 5G-teknologien? Snakkes det om det mobile nettverket? Avhengig av 5G-nettet? Hvor viktig blir 5G?	Elektronisk utstyr lar seg ikke verifiseres fullt ut. Hardware og Software i 5G. Tredjepartsrisiko: leverandørkjede Digital avhengighet skaper og øker sårbarheter Ingen sikkerhetspolitisk samarbeid = ingen full tillit
Styring	Styre og ikke forhindre skade. Styring rettet innover mot sårbarheter. Øke resiliens hos referanseobjektet som tiltak.	Vektlegges cybersikkerheten i saken på risikoreduserende tiltak? På hvilken måte? Utrykkes det tiltak eller behov om diversitet,	Lysne: Kontrollert heterogenitet/ leverandørdiversitet Ekom-sektoren legges under norsk sikkerhetslov.

		redundans i 5G-nettverket?	5G-legges under norsk sikkerhetslov av KMD. Sikkerhetstiltak fra KMD: 50% fra land Norge ikke har sikkerhetspolitisk samarbeid med (diversitet) 50%-diversitet som et forebyggende tiltak og sikkerhetsmargin: kun 50% som kan gå ned og dermed ikke true nasjonal sikkerhet. Orderløkken: testsentere for testing av teknologi, awareness, standarder, beste-praksis. Informant 3: testsenter, sikkerhetsmekanisme og prosedyrer
Føre-var-prinsipp (Corry:2012)	Forebyggende tiltak som sikkerhetsmargin		
Langsiktighet (Friis og Reichborn-Kjennerud:2006)	Myke tiltak: beste praksis, standarder, holdningsbygging.		

Vedlegg 4: Eksempelet på koding av datamaterialet ble gjennomført her.

(Data fra egen empiri (intervju) ble også kodet inn i det samme skjemaet, men vises ikke på grunn av anonymiseringen.

Cyber-Sikkerhetisering

1A Sikk. Aktør	1Ba Ref.Objekt: Ind	1Bb Ref.Objekt Koll.	1C Eksi. Trussel	1D Ekstr.Tiltak	1E Aksept
2018 PST v/Martin Bernsen september 2018: «Telenettet er samfunnskritisk infrastrultur. Det kan være problematisk å benytte produkter og tjenester fra land som	2019 Tv2-kronikk: nordmenn som digitale brukere (vipps er nede og har ingen	2018 Mobilnettene bærer stadig større **samfunnsverdier**. De mest kritiske funksjonene er underlagt sikkerhetsloven. Ketil Solvik-Olsen (tek.no, 2018august)	Retriever 2018 Anti-sikk: – Telenor Norge bruker basestasjoner fra Huawei. Vi bruker også et policy control og rating-system fra Huawei, men kjernenettets funksjon er ikke avhengig av	Retriever 2018 Anti-sikk: – Den nye sikkerhetsloven inneholder bestemmelser som gir myndighetene mulighet til å stoppe enkeltinnkjøp til kritisk infrastruktur.	Mikkel Wara deler andre lands bekymringer Lene Vågslid og Sigbjørn Gjelsvik deler PSTs

Cyber-risiko

2A Bakenforligg. Faktor (sårb/tek)	2B Styring	2C Langsiktig
Retriever-dokument 2018 Samferdselsdep. Nov2018: Minner operatørene om at det skal gjøres risiko- og sårbarhetsvurdering (ROS) av anskaffelser av skjermverdig infrastruktur i tråd med sikklov: §29a (2017) og §9-4(2019). Samferdselsdep. Des2018: «Digitaliseringen gir oss store muligheter, men medfører også nye	Retriever-dokument 2018 På spørsmål om hvordan Samferdselsdepartementet stiller seg til bruk av Huawei eller kinesisk teknologi i viktige deler av norsk mobilnett: «Vi stiller krav i ekomloven om at mobilnettene skal ha «forsvarlig sikkerhet». Begrepet forsvarlig sikkerhet er en rettslig standard som utvikles over tid. Det er mobiltilbyderne, altså Telenor, Telia og Ice som har plikt til å vurdere om	Retriver-dokument 2018 Det er mobiltilbyderne, altså Telenor, Telia og Ice som har plikt til å vurdere om egne nett til enhver tid oppfyller kravet om forsvarlig sikkerhet. Nkom fører tilsyn med tilbyderne, forklarer samferdselsminister Ketil Solvik-Olsen. (Tek.no) Vi følger tett med på utviklingen og trusselsituasjonen i Norge. Vi er opptatt av at tilbyderne

Vedlegg 5: Intervjuguider

Intervjuguide for informant 1 og 2

1. Vil gjerne starte veldig generelt. Kan du fortelle meg kort din rolle/arbeid?
- Når det gjelder aktører involvert i Huawei-saken/5G-utbygging: Hva var og er din rolle innenfor denne saken?

Ønsker først å snakke generelt om 5G-nettverket og hva det innebærer og betyr.

2. Hvilken betydning har/får 5G for det norske samfunnet?
- Hvor viktig blir 5G for det norske samfunn? Hvilken deler av samfunnet blir dette ekstra viktig for?
- Spiller 5G en viktig rolle som et ledd eller som en del av et større nettverk eller verdikjede i det norske samfunnet? Om ja, på hvilken måte?

3. Opplever du at det er en større debatt rundt 5G i forhold hvem som er leverandør for av tidligere generasjons mobile nettverk?

4. Etter din mening, *hva* er det som gjør at det er en større debatt rundt 5G enn tidligere?

5. Hvorfor ble 5G-utrullingen et spørsmål om sikkerhet?

6. Hva er det med Huawei som gjør seg til en egnet eller uegnet leverandør av 5G-teknologi?
7. På hvilken måte vil du si at Huawei utgjør en trussel mot 5G-nettverket?
8. Hadde trusselen eller trusselnivået endret seg dersom Huawei ikke var kinesisk? Om ja, på hvilken måte?
9. Dersom ja på spørsmål: hva er det som gjør at man diskuterer og evaluere hvilken aktør/leverandør og tilhørende land som utviklinger, bygger og leverer 5G-teknologi?
10. Er kinesiske leverandører en sikkerhetstrussel mot 5G-nettverk? Er de en trussel mot nasjonal sikkerhet?

11. Er den norske trusselvurderingen av 5G-nettverket tidsmessig dominert av Norges relasjon til Kina og landets relasjon til Huawei?

12. Er det den nåværende sikkerhets- og geopolitiske situasjonen som preger og legger føringer for den norske sikkerheten av 5G-teknologi?

13. Hvem vil du si er truet og må beskyttes i Huawei-saken og i 5G-sikkerheten? Og hvorfor disse?

14. På hvilken måte er de virkemidlene, regelverk og tiltakene som gjøres mot 5G-sikkerheten gode nok? Hvilke tiltak syns du hadde vært passende og burde implementeres?

15. På hvilken måte vil du si at det hastet å komme med tiltak i denne saken i respons til at en avgjørelse om leverandør skulle gjøres?

I den offentlige debatten har det vært diskutert mulighetene for påvirkning av nettverket gjennom både hardvare og programvare:

16. På *hvilken måte* kan man vite mulighetene for dette? Lar det seg vite?

17. Er det muligheter for å undersøke og verifisere all teknologi for sårbarheter og feil?

18. Oppdages det også videre ukjente sårbarheter gjennom bruk av teknologi som man ellers ikke hadde hatt mulighet til å avdekke?

19. Vil du si at det er mindre risiko for cyberangrep nå når det ble valgt en annen leverandør enn Huawei?

Telia har valgt Ericsson som eneste leverandør, mens Telenor enda skal fortsette med noe leveranse fra Huawei:

20. Er det noen i disse som senker cybertrusselen mer en den andre? Ved ja: hvorfor?

21. På hvilken måte kan man best redusere sannsynligheten for cyberangrep mot 5G-nettverk i Norge?

22. På hvilken måte er dette tiltak som gjøres spesifikk mot 5G-teknologi og denne saken, eller generelt for norsk sikkerhet og all infrastruktur?

23. Vil du si at trusselen mot 5G-nettverket ved vedvarende uavhengig av tid?

24. På hvilken måte er trusselen mot 5G-nettverked vedvarende uavhengig av og type leverandør?

25. Er det noe med 5G-teknologien i seg selv som gjør at det er trussel mot 5G-sikkerheten?

26. Ved 5G-sikkerhet, hvilket hensyn ser du som viktigst: identifisere fiendtlige aktører eller fokusere på sårbarheter i eget system? Kan du utype hvorfor?

27. Hvordan vil du beskrive kapasiteten til 5G, når det gjelder å håndtere, overleve og komme tilbake fra et cyberangrep? Fra for eksempel Kina aller kinesiske støttespillere? Er det forskjell fra 4G?

28. Hva vil du si man har lært om sårbarheter og kapasiteten til 4G-netterket? Og eventuelt på hvilken måte mener du at det har lagt føringer for valg av leverandør?

29. På hvilken måte har kunnskap og lærdom fra 4G-nettverket lagt føringer for sikkerheten rundt 5G-nettverket og i valg av leverandør?

30. Hvilket tidsperspektiv bruker man når man organiserer og planlegger videre utrullinger av neste generasjons nettverk (og også videre etter 5G)?

31. Har det i denne prosessen vært hentet innspill fra andre land?

32. På hvilken måte spilte andre stater og overnasjonale organisasjoners (EU) avgjørelser og standpunkt for Norges valg av leverandør? Har dette vært viktig for Norge? Hvorfor har dette vært viktig/uviktig?

33. Hvordan og på hvilken måte jobber Norge innenfor cybersikkerhet (og herunder 5G) når det gjelder å sikre norske digital infrastruktur?

Intervjuguide for informant 3

Ønsker først å snakke generelt om 5G-nettverket og hva det innebærer og betyr.

34. Hvilken betydning får 5G for det norske samfunnet? Hvor viktig blir det mener du?

35. Hvilke viktige ting endrer seg fra 4G til 5G?

36. Hvordan opplevde du den offentlige debatten knyttet til skepsisen og mistilliten til Huawei for levering av 5G-nettverket?

37. Opplever du at det er en større debatt rundt 5G i forhold hvem som er leverandør for av tidligere generasjons mobile nettverk? *hva* er det som gjør det?

38. hvordan vil du si den norske sikkerhetsforståelsen har vært? (Det med vektlegging på aktør, versus vektlegging av teknologi, sårbarheter).

39. I anbudsrunden med Telenor, hvilke(t) punkt(er) var det som gjorde at dere ikke ble valgt som leverandør?

40. Hadde diskusjonen rundt trusselen endret seg dersom Huawei ikke var kinesisk? Om ja, på hvilken måte?

41. Hva mener du er den største trusselen mot 5G-nettverket?

42. Hvem vil du si 5G-sikkerheten er rettet mot eller er til for? Hvorfor disse?

43. Hvilket tidsperspektiv bruker mobiloperatører (og for så vidt leverandører) i utvikling, utrulling og drift av det mobile nettverket? (Om selskap som Telenor går inn for å bruke samme leverandør lang fram i tid, og bytte av leverandører er ikke økonomisk ønskelig)

44. Har norske myndigheter håndtert denne saken på en god måte syns du? Hvordan burde den har blitt løst? Hvilke tiltak og løsninger syns du hadde vært passende

45. I hvilken grad mener du at tiltakene som er et resultat av andre staters tiltak, uttalelser og avgjørelser?

46. Hvem sitter med kontrollen over det mobile nettverket, leverandør og/eller operatør?

47. I hvilken grad klarer operatører å identifisere og kalkulere risiko og sårbarheter i digitale system som 5G-nettet?

48. Vil du si at det er mindre risiko for cyberangrep nå når det ble valgt Ericsson?

49. På hvilken måte kan man best redusere sannsynligheten for cyberangrep mot 5G-nettverk i Norge?

50. Hvilke konsekvenser har det for sikkerheten og for Norge, for de tiltak og løsninger som ble gjort i denne saken?

51. Selv om det fram til nå ikke har vært offentlige kjente sikkerhetshendelser mot det mobile nettverket, vil det si at det ikke er noe sannsynlighet for uønskete sikkerhetshendelser i fremtiden?

Intervjuguide for informant 4

Ønsker først å snakke generelt om 5G-nettverket og hva det innebærer og betyr.

52. Hvilken betydning får 5G for det norske samfunnet? Hvor viktig blir det mener du?

53. Hvilke viktige ting endrer seg fra 4G til 5G?

54. Hvordan opplevde du den offentlige debatten knyttet til skepsisen og mistilliten til Huawei for levering av 5G-nettverket?

55. Opplever du at det er en større debatt rundt 5G i forhold hvem som er leverandør for av tidligere generasjons mobile nettverk? *hva* er det som gjør det?

56. hvordan vil du si den norske sikkerhetsforståelsen har vært? (Det med vektlegging på aktør, versus vektlegging av teknologi, sårbarheter).

57. Hva har X rolle vært i denne prosessen opp mot valget av leverandør?

58. X har uttrykt at det var en risiko ved 4G-nettet, var det ubetydelig den gang?

59. Hva mener du er den største trusselen mot 5G-nettverket?

60. Hadde diskusjonen rundt trusselen endret seg dersom Huawei ikke var kinesisk? Om ja, på hvilken måte?

61. Hvorfor kan man ikke fortsette med kinesiske leverandører for 5G-nettverket?

62. Til syvende og sist: hvem har ansvaret for sikkerheten rundt 5G-nettverket?

63. Hvem vil du si 5G-sikkerheten er rettet mot eller er til for? Hvorfor disse?

64. Har norske myndigheter håndtert denne saken på en god måte syns du? Hvilke tiltak og løsninger syns du hadde vært passende

65. I hvilken grad mener du at tiltakene som er et resultat av andre staters tiltak, uttalelser og avgjørelser?

66. Hvem sitter med kontrollen over det mobile nettverket, leverandør og/eller operatør?

67. I hvilken grad klarer operatører å identifisere og kalkulere risiko og sårbarheter i digitale system som 5G-nettet?

68. Vil du si at det er mindre risiko for cyberangrep nå når det ble valgt Ericsson?

69. På hvilken måte kan man best redusere sannsynligheten for cyberangrep mot 5G-nettverk i Norge?

70. Hvilke konsekvenser har det for sikkerheten og for Norge, for de tiltak og løsninger som ble gjort i denne saken?

71. Hvilke konsekvenser får det dersom 5G-nettverket forstyrres, påvirkes (inkl. spionasje) eller tas ned?

Intervjuguide for informant 5

Starter litt med generelt om 5G:

1. Hvilken betydning får 5G for Norge? Og hvorfor det?

2. Opplever du at det er en større debatt rundt 5G enn tidligere generasjons mobile nettverk? *Hva* er det som gjør dette?

3. Hvilke sikkerhetsutfordringer fører utrullingen av 5G med seg? (cyber)

4. Hva vil du si er den største trusselen mot det kommende 5G-nettverket?

5. På hvilken måte vil du si at aktøren Huawei utgjorde en trussel mot 5G-nettverket?

6. Hadde trusselen eller trusselnivået endret seg dersom Huawei ikke var kinesisk? Om ja, på hvilken måte?

Hvordan har Huawei klart seg ved levering av 4G-teknologi?

Ville det vært i X interesse å kunne samarbeid videre med Huawei og tillate levering av 5G-utstyring dersom sikkerhetsloven ikke hadde vært vedtatt og implementert?

Hvem sitter med kontrollen av det mobile nettverket? Leverandør eller operatør?

Hva kriterier spilte inn da dere skulle vurdere og velge leverandør?

I hvilken grad la sikkerhetshensyn føringer for valget av leverandør?

Hvilket tidsperspektiv benytter X ved teknologisk utvikling, utrulling av nye generasjoner mobile nettverk og valg av leverandør?

Tenker dere ut ifra et nasjonalt sikkerhetsperspektiv eller forretningsperspektiv?

Hvilket ansvar mener du X har innenfor sikkerheten av 5G-nettverket? Og for hvem ønsker dere å beskytte og hva ønsker dere å beskytte?

Hva tenker du om 50%-kravet fra norske myndigheter?
Hva betyr dette 50%-kravet for dere? Hvilke konsekvenser?

Hvilke tiltak syns du hadde vært passende og burde implementeres? Hvorfor?

Vil du si at det er mindre risiko for cyberangrep nå når det ble valgt en annen leverandør enn Huawei?

På hvilken måte kan man best redusere sannsynligheten for cyberangrep mot 5G-nettverk i Norge?

Hva blir Huawei sin rolle i deres mobile nettverket framover?

Er det vanlig at det velges flere leverandører til deres mobile nettverk?

Hvor stor rolle spilte det for dere andre lands valg av leverandør?

Intervjuguide for informant 6

1. Kan du først si litt kort om din rolle og ansvar og om din faglige bakgrunn?

72. Hvordan opplevde du den offentlige debatten knyttet til skepsisen og mistilliten til Huawei for levering av 5G-nettverket?

73. Hvilken betydning får 5G for det norske samfunnet? Hvor viktig blir det mener du?

74. Opplever du at det er en større debatt rundt 5G i forhold hvem som er leverandør for av tidligere generasjons mobile nettverk? *hva* er det som gjør det?

75. Hvilke viktige ting endrer seg fra 4G til 5G?

76. Hva har KMDs rolle vært i denne prosessen opp mot valget av leverandør?

77. Hvordan har kommunikasjonen mellom departementet og mobiltilbyderne vært?

78. Hva mener du er den største trusselen mot 5G? Mot det mobile nettverket?

79. Til syvende og sist: hvem har ansvaret for sikkerheten rundt 5G-nettverket?

80. Hvorfor kan ikke Norge fortsette med kinesiske leverandører for 5G-nettverket, siden de allerede har levert 2G, 3G og 4G?

81. Hvem vil du si 5G-sikkerheten er rettet mot eller er til for? Hvorfor disse?

82. Hva er det som er viktig at sikres i neste generasjons mobile nettverk ved utrulling av 5G?

83. Vil du si at det er mindre risiko for cyberangrep nå når det ble valgt Ericsson? Er det bedre sikkerhet i det kommende mobile nettverket etter at Ericsson ble valg?

84. På hvilken måte kan man best redusere sannsynligheten for uønsket hendelser mot 5G-nettverk i Norge?

85. Hvorfor er 50%-regelen **bare** knyttet til leverandører Norge ikke har et sikkerhetspolitisk samarbeid med?

86. Hvor viktig er hensynet mellom konkurranse i telekom-bransjen og sikkerhetshensyn? Hensyn mellom økonomi (gunstig/ugunstig med flere leverandører) og sikkerhet?

87. Hvorfor ble det satt 50%?

88. Hvilken dialog har dere med andre departement om dette? Og spesielt knyttet til 50%-kravet?

89. Hvilke konsekvenser får det dersom 5G-nettverket forstyrres, påvirkes (inkl. spionasje) eller tas ned?

90. Hva gjør Norge om det mobile nettverket framover blir tatt ned? Om fiberkabler inn til Norge blir påvirket

91. Hvilken kontakt har dere hatt med andre land angående dette?

92. Hvor viktig har det vært for hva andre land valgte?

Intervjuguide for informant 7

Kan du kort fortelle om din rolle i Telenor og i prosessen mot valg av leverandør? Og litt om din faglige bakgrunn?

Hvor viktig blir 5G for Norge? For hvem?

Hva er det som har endret seg fra 4G til 45G? Hva konkret endrer seg med 5G (teknisk sett. Er snakk om det blir mer master osv)

Mener du det er større debatt rundt 5G enn ved utrullingen av 4G? Hvorfor det?

Hvordan opplevde du debatten rundt Huawei og leverandørvalget i perioden mot valget av leverandør for 5G-utstyr?

Hva er de største truslene mot 5G-nettet syns du?

Hvilke konsekvenser får det dersom 5G-nettet forstyrres, påvirkes (inkl. spionasje) eller tas ned? Hvor kritisk er det?

Hvilke tiltak og løsninger har X dersom 5G skulle falle ut og få nedetid?

Hvordan var dialogen mellom dere og myndigheten i prosessen imot valg av leverandør?

Skal dere skifte ut alt utstyr av Huawei i 5G-nettene?

Hvem er det som ansvaret for sikkerheten rundt det mobile nettverket og 5G-sikkerheten i Norge?

Hvem har kontrollen over det mobile nettverket, leverandør og/eller operatør?

Hvem er det dere har sikkerheten for? Hvem er dere tar hensyn til eller ser for dere når sikkerheten i teknologien settes opp?

Hvorfor kan ikke Norge fortsette med kinesiske leverandører for 5G-nettverket, siden de allerede har levert 2G, 3G og 4G?

Vil du si det er mindre risiko cyberangrep (at 5G-nettverket forstyrres, påvirkes, tyveri) nå når det ble valgt Ericssson?

Hvilke konsekvenser får det at Huawei ikke kan fortsette å levere 5G-utstyr?

På hvilken måte kan man best redusere sannsynligheten for cyberangrep mot 5G-nettverket i Norge?

Har X sammen med norske myndigheter utformet sikkerhetskravene for 5G-nettet? Hvordan og på hvilken måte gjøres dette? Hvem stiller krav til hvem?
Hva syns du om 50%-kravet?

Hvilke konsekvenser har et slik sikkerhetskrav fått for dere? Har det vært ulemper med det?

Hvordan vil du si den norske sikkerhetsforståelsen har vært fra myndighetenes side? (Det med vektlegging på aktør, versus vektlegging av teknologi, sårbarheter).

Hvilke tiltak og løsning syns du hadde vært passende?

Hvilke deler av nettverket leveres skal leveres av 5G-leverandøren?
Hvilke deler av nettverket er 5G?

Vil du si 5G er en grunnleggende nasjonal funksjon eller kritisk infrastruktur? Evt. vil det bli det?

Er det mulighet for at hele det mobile nettverket kan gå ned samtidig, på tvers av operatører? Hvordan skjer isåfall det?