Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: MSAMAS Master i samfunnssikkerhet	Vår.....semesteret, 20.19.. Åpen / ~~Konfidensiell~~
Forfatter: Karin Sørvik Pedersen Mina Ottestad Gaupseth	..... (signatur forfatter)
Fagansvarlig: Geir Sverre Braut Veileder(e): Geir Sverre Braut	
Tittel på masteroppgaven: Digital sikkerhetskultur i Norge - en studie av dokumenter utgitt av nasjonale aktører. Engelsk tittel: Digital security culture in Norway - a study of documents published by national actors.	
Studiepoeng: 30 stp	
Emneord: Digital sikkerhetskultur, sikkerhetskultur, kultur, digitalisering, informasjonssikkerhet, norske aktører, begrepsbruk, maktforhold, diskurs, samfunnsikkerhet, sikkerhetsarbeid, digital sikkerhet.	Sidetall: ..89.. + vedlegg/annet: ..107.. Stavanger, ..16.05.2019.. dato/år

Forside for masteroppgave
Det teknisk-naturvitenskapelige fakultet

Forord

Etter to år på Universitetet i Stavanger er vi endelig ferdig med en mastergrad i samfunnssikkerhet. Denne studien utgjør mastergradens hovedoppgave og markerer avslutningen på vår grad. I forbindelse med arbeidet med oppgaven har vi flere som vi ønsker å takke.

Først og fremst ønsker vi å rette en stor takk til vår veileder, Geir Sverre Braut. Takk, Geir Sverre - du har vært av stor betydning for oppgaven vår. Vi setter stor pris på at din tilgjengelighet og oppfølging. Dine innspill og støttende ord underveis i prosessen har ikke bare resultert i en flott oppgave, men også et stort læringsutbytte. Videre setter vi stor pris på at du gjennom hele semesteret beholdt troen på både oss og oppgaven vår.

Vi ønsker videre å rette en stor takk til våre veiledere i KPMG, Tor Indstøy og Christopher Berglind. Vi setter stor pris på at dere har tatt dere tid til å bistå oss i arbeidet med oppgaven. Deres innspill, engasjement og oppløftende ord har vært avgjørende for oppgavens prosess og resultat. Tusen takk.

Vi er selv veldig fornøyde med hva vi har fått til, men skal ikke legge skjul på at det har vært en utfordrende prosess. De siste ukene har vært preget av lange dager på biblioteket som har gått på bekostning av både venner og familie. Avslutningsvis ønsker vi derfor å takke våre venner og familie for deres tålmodighet og oppmuntrende ord. Dere har absolutt vært avgjørende for vårt arbeid med oppgaven - tusen takk.

Karin Sørvik Pedersen & Mina Ottestad Gaupseth
Stavanger, 16. mai 2019.

Sammendrag

Denne oppgaven omhandler forståelse av sikkerhetskultur i en digital kontekst. Hensikten er å studere hvordan aktørers forståelse av sikkerhetskultur legger føringer for arbeidet med det som ofte omtales som digital sikkerhetskultur. Aktørene i oppgaven utgjør et utvalg av nasjonale aktører med digitale sikkerhetsinteresser. Sikkerhetskultur er ikke et nytt begrep, men viser seg imidlertid å være av en karakter som gjør begrepet vanskelig å definere. Ser en på begrepet i en digital kontekst kompliseres bildet ytterligere.

Studien er en kvalitativ dokumentanalyse. Det empiriske grunnlaget er basert på et utvalg av offentlig tilgjengelige dokumenter utgitt av nasjonale aktører med interesser av betydning for digital sikkerhet. Oppgavens teorigrunnlag spenner fra teorier om sikkerhetsarbeid, kultur, organisasjons- og sikkerhetskultur, til normale ulykker, maktforhold og sosialkonstruktivisme. Sammen med oppgavens funn, utgjør teoriene et grunnlag for å besvare oppgavens problemstilling: "Hvordan legger forståelsen av sikkerhetskultur i dokumenter utgitt av nasjonale aktører med digitale sikkerhetsinteresser føringer for arbeidet med sikkerhetskultur i en digital kontekst?".

Funnene i oppgaven synliggjør en varierende bruk og en sprikende forståelse av sikkerhetskultur i en digital kontekst. Dette resulterer i ulike tilnærminger til arbeidet med sikkerhetskultur. Tross den sprikende forståelsen av begrepet viser funn at aktørene besitter en felles forståelse av viktigheten. Det kan hevdes at den sprikende forståelsen vil kunne gå på bekostning av det aktørene faktisk enes om.

Studiens konklusjon er at den sprikende forståelsen svekker den potensielle verdien aktørers intensjonelle handlinger vil ha for arbeidet med sikkerhetskultur i en digital kontekst. Den sprikende forståelsen av sikkerhetskultur medfører at sentrale aktører for arbeidet med digital sikkerhet i Norge er preget av ulike tilnærminger. Aktørenes posisjon og inkonsistente forståelse vil resultere i føringer som vil kunne svekke respektives oppfordringer og tiltak for arbeidet. Med andre ord vil ikke-intensjonelle handlinger som oppstår som følge av en inkonsistent forståelse gå på bekostning av aktørenes faktiske intensjoner.

Forkortelser

Difi – Direktoratet for forvaltning og ikt

EU – Europeiske Union

EØS – Det europeiske økonomiske samarbeidsområde

GDPR – General Data Protection Regulation (Personvernfordningen)

IKT – Informasjons- og kommunikasjonsteknologi

JD – Justis- og beredskapsdepartementet

KIT(S) – Konfidensialitet, integritet og autoritet (sporbarhet)

MTO – Menneske, teknologi og organisasjon

NorSIS – Norsk senter for informasjonssikring

NOU – Norges offentlige utredninger

NSM – Norges Sikkerhetsmyndighet

NSR – Næringslivets Sikkerhetsråd

Ptil – Petroleumstilsynet

Innholdsfortegnelse

1 Innledning

I vår verden, som i stadig økende grad digitaliseres, fremmedgjøres vi for vesentlige aspekt av betydning for sikkerhet (Justis- og beredskapsdepartementet, 2016). Forutsetningene for å forstå dagens sårbarhetsbilde er derfor ikke av samme karakter som tidligere. Trusler og risikoer vi står overfor i dag er langt mer dynamiske enn de utfordringene vi tidligere har stått overfor. Sikkerhetsutfordringer er ikke lenger nødvendigvis avgrenset til tid og sted. Det som tidligere utgjorde en trussel på jobb kan i like stor grad utgjøre en trussel i hjemmet.

Som Meld. St. 38 (JD, 2016) formidler, var sikkerhet lettere å vurdere da det som skulle sikres var noe fysisk, håndfast og stabilt. Sikkerhetsutfordringer i dagens samfunn er ikke i nærheten av like begripelige, og digitale angrep vil nødvendigvis ikke være synlig for de som rammes (s. 26). Imidlertid, som Meld. St. 10 påpeker, er ikke digitalisering et valg, men en forutsetning for et moderne samfunn (Justis- og beredskapsdepartementet, 2016, s. 59). Medfølgende sikkerhetsutfordringer kan derfor ikke ignoreres, og må heller aksepteres. Digitaliseringen er utenfor utenfor vår kontroll, som setter begrensninger for sikkerheten. Ifølge Aven, Boyesen, Njå, Olsen, & Sandve (2004, s. 32) kan sikkerhet styres mot virksomhetens definerte mål gjennom risiko- og sårbarhetsanalyser, ledelse og styring, planlegging, opplæring, informasjon, teknisk design og sikkerhetskultur. I henhold til oppgavens teorigrunnlag, kan den menneskelige faktor betraktes som det svakeste leddet i arbeidet med sikkerhet. Med utgangspunkt ovennevnte elementer, og samfunnets digitalisering, tar vi i denne oppgaven utgangspunkt i sikkerhetskultur i en digital kontekst. Oppgaven dreier seg imidlertid ikke om sikkerhetskultur i seg selv, men om hvordan sikkerhetskultur forstås. Om sikkerhetskultur skriver James Reason (1997) følgende:

> Few phrases occur more frequently in discussions about hazardous technologies than safety culture. Few things are so sought after and yet so little understood.
>
> (s. 191)

Som sitatet synliggjør utgjorde sikkerhetskultur et sentralt begrep innen teknologi allerede i 1997. Reasons uttalelse om at begrepet var lite forstått kan ses i lys av uttalelser av Finn-Erik Vinje (i NOU 2006:6, 2006) og Jacob Kringen (2009). Kringen (2009) omtaler hyperonym som et lingvistisk begrep for et overordnet konsept som dekker en rekke fenomener, som igjen klassifiseres av en rekke underbegreper (s. 22). Ifølge Vinje og Kringen er sikkerhet og kultur begrep som kan forstås som hyperonymer (Kringen, 2009; NOU 2006:6, 2006). Sikkerhetskultur kan dermed forstås som et begrep sammensatt av to ord som i utgangspunktet dekker flere fenomener. Det er med andre ord ikke rent unaturlig at begrepet sikkerhetskultur kan være vanskelig å forstå. Det er verdt å påpeke at Reasons uttalelse stammer fra 1997 og at forståelsen av begrepet vil være av en annen karakter i dag. Oppgaven tar imidlertid for seg begrepet i en relativt ny kontekst som bærer preg av stadige endringer. Det er derfor aktuelt å reise problematikken selv 20 år etter.

Tema i oppgaven er forståelse av digital sikkerhetskultur i Norge. Oppgaven tar utgangspunkt i en dokumentanalyse som baseres på dokumenter utgitt av nasjonale aktører med interesser relatert til digital sikkerhet. Studiens formål er å avdekke hvilke føringer respektives forståelse av sikkerhetskultur legger for arbeidet med sikkerhetskultur i en digital kontekst.

1.1 Valg og begrunnelse for oppgavens tema

Vår begrunnelse for valg av tema i oppgaven kan forstås som todelt. Vi ønsket i første omgang å basere studien på et tema som både var verdifullt for oss på et personlig plan, men også av betydning for forskning og arbeidet med sikkerhet i Norge. Sikkerhet i digital kontekst er noe vi begge interesserer oss stort for, men som vi har savnet i mastergraden studieprogram. Vårt valg av tema for oppgaven har derfor vært et åpenbart og klart valg siden starten. I forkant av arbeidet med masteroppgaven utformet vi en skisse som i hovedsak fokuserte på sikkerhetskultur i en digital kontekst. Vi ble imidlertid på et tidlig tidspunkt i arbeidet med oppgaven oppmerksomme på en problematikk knyttet til begrepsbruk. Oppgaven, som i henhold til masterskissen skulle omhandle sikkerhetskultur og digitalisering av små og mellomstore virksomheter, ble derfor i stedet en oppgave om betydningen av forståelse av sikkerhetskultur. Vår nysgjerrighet tok overhånd og valget av tema falt

på problematikken som ble presentert innledningsvis: forståelse av digital sikkerhetskultur.

1.2 Problemstilling og forskningsspørsmål

Oppgavens problemstilling er utviklet og konstruert på bakgrunn av oppgavens temavalg. I arbeidet med å formulere en problemstilling var det ønskelig å inkludere elementer som legger føringer for å betrakte norsk sikkerhetstenkning knyttet til digital sikkerhet. Sentrale begreper i oppgaven er sammensatte og flerdimensjonale, som innebærer at de tatt ut av kontekst kan fremstå upresise. Problemstillingen er derfor formulert med et formål om å unngå bruk av tvetydige begreper. Resultatet er en visuelt sett mer omfattende problemstilling, men som i praksis er mer konkretisert og som dermed får et mer innsnevret omfang. Oppgavens problemstilling lyder som følger:

Hvordan legger forståelsen av sikkerhetskultur i dokumenter utgitt av nasjonale aktører med digitale sikkerhetsinteresser føringer for arbeidet med sikkerhetskultur i en digital kontekst?

Med sikte på å besvare oppgavens problemstilling reises følgende forskningsspørsmål:

1. *Hvordan formidles og anvendes sikkerhetskultur i offentlig tilgjengelige dokumenter av betydning for digital sikkerhet?*

2. *Hvordan påvirker dokumenter utgitt av nasjonale aktører arbeidet med sikkerhetskultur i en digital kontekst?*

1.3 Oppgavens avgrensninger

Oppgavens tema er av en karakter som resulterer i en naturlig innsnevring av oppgaven. Videre er oppgavens problemstilling og forskningsspørsmål utviklet med hensikt om å avgrense oppgaven ytterligere. Som oppgavens tittel formidler, er studien om digital sikkerhetskultur i Norge. Med utgangspunkt i en avgrensning til Norge er litteratur og datamateriale avgrenset deretter. Videre er studien utelukkende basert på dokumenter som er tilgjengelig for offentligheten. Funnene som knyttes

direkte til aktørenes forståelse er i hovedsak basert på respektives foreliggende tekster. Det er imidlertid verdt å påpeke at empirisk data ikke utelukkende baseres på aktørenes selvskrevne tekster. For å belyse problemstillingen har det vært nødvendig å også inkludere dokumenter som gjør det mulig å kartlegge et helhetlig bilde av området som studeres.

Aktørene i oppgaven er avgrenset til institusjoner og organisasjoner som har publisert dokumenter som er anses å være av relevans for oppgavens problemstilling. Videre er utvelgelse av foreliggende tekster avgrenset til tekst publisert i perioden 2015-2019. Studien er utelukkende basert på en studie av dokumenter og sier derfor ikke noe om hvordan aktørenes forståelse er av betydning for arbeidet med sikkerhetskultur i praksis.

1.4 Begrepsavklaring

Bransjenorm eller atferdsnorm er et regelsett for en spesifikk bransje, med sikte på å gi konkrete regler og retningslinjer for hvordan virksomhetene skal innrette seg for å etterleve kravene i personvernsforordningen. Det er frivillig å utarbeide og tilslutte seg en slik norm, men det er ønskelig at de fleste virksomheter gjør det (Datatilsynet, u.å.). En atferdsnorm er utviklet av bransjen selv, men er godkjent av Datatilsynet og/eller Personvernrådet/EU-kommisjonen dersom normen gjelder behandlingsaktiviteter i flere medlemsland.

Definisjonsmakt er betydningen at noe eller noen har makt til å skape definisjoner: makt til å få gjennomslag for sin versjon av virkeligheten. Se kapittel 3.6.

Foreliggende tekst er data som er etablert uavhengig av forskerens medvirkning (Thagaard, 2018, s. 53).

Hyperonym er et lingvistisk begrep for et overordnet konsept som dekker en rekke fenomener**,** som igjen klassifiseres av en rekke underbegreper (Kringen, 2009, s. 22).

Nasjonale aktører forstås her som en person, gruppe eller institusjon som spiller en aktiv rolle, ofte på et bestemt område (Persvold, 2019) med nasjonal dekning.

Norges offentlige utredninger (NOU) er en serie av statlige rapporter med formål om å presentere og drøfte kunnskapsgrunnlag, mulige handlingsvalg eller strategier for utvikling, samt iverksetting av tiltak for løsninger av samfunnsmessige problemer. Ofte utgjør utredningene første trinn i en lengre beslutningsprosess rettet mot et spesifikt område (Hansen, 2018).

Norm er på mange måter knyttet til verdier, og defineres av Braut (2000), som forestillinger og følelser om hva som er rett og hva som er galt, altså om ulike handlinger som egnede virkemiddel på veien mot verdiene. Verdier er noe en ønsker å oppnå, der normer er handlingsreglene som leder mot verdiene (Braut, 2000).

Verdier kan defineres som forestillinger og følelser om hva som er godt og hva som er vondt, det som er verdt å gjøre til mål for livet (Braut, 2000).

Safety brukes for å beskrive sikkerhet mot uønskede hendelser som resultat av tilfeldigheter (NOU 2006:6, s. 38).

Samfunnssikkerhet er samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger (Meld. St. 10 (2016-2017), s. 9).

Security brukes for å beskrive sikkerhet mot uønskede hendelser som resultat av overlegg (NOU 2006:6, s. 38).

Sårbarheter forstås som betingelsene for at driftsforstyrrelser med negative konsekvenser eller alvorlige hendelser kan skje. Teknologier som er sårbare, og der problemer kan gi katastrofale konsekvenser, kaller vi høyrisikoteknologier (Engen et al. 2016, 139).

Stortingsmelding/Meld. St. benyttes når regjeringen vil presentere saker for Storting uten forslag til vedtak. Meldingene og behandling danner ofte grunnlaget for en senere proposisjon (Stortinget, 2018).

1.5 Oppgavens disposisjon

I oppgavens kapittel 1, Innledning, presenteres studiens tema og problemstilling. Videre begrunnes og beskrives sentrale forhold av betydning for oppgavens innhold og omfang. I påfølgende kapittel, Systembeskrivelse, beskrives det som kan forstås som oppgavens bakteppe. Videre i kapittel 3, Teori, presenteres oppgavens teorigrunnlag. I kapittel 4, Metode, presenteres oppgavens dokumentanalyse og sentrale forhold knyttet til forskningsprosessen. I kapittel 5, Resultat, presenteres oppgavens empiri. I kapittel 6, Diskusjon, drøftes oppgavens empiriske funn i lys av oppgavens teorigrunnlag. I påfølgende kapittel, Konklusjon, besvares oppgavens forskningsspørsmål og problemstilling. Avslutningsvis, i kapittel 8 og 9, følger oppgavens litteraturliste og vedlegg.

2 Systembeskrivelse

Som presentert i oppgavens innledning dreier studien seg om et begrep med et utgangspunkt som resulterer i utfordringer knyttet til forståelse. Samtidig befinner vi oss i et svært digitalisert samfunn, og i en kontekst som for bare tiår tilbake ikke en gang eksisterte. Digitaliseringen av samfunnet er preget av høy utviklingshastighet. Videre opplever vi informasjonsstrømmen på området som kontinuerlig og omfattende. Sikkerhetsutfordringene endres fortløpende, og situasjon og forhold kan være av en annen karakter allerede i morgen. For vår oppgave, med et tema tilknyttet forhold som er i stadig endring, blir systembeskrivelsen særlig viktig. Den stadig økende digitaliseringen som adresseres innledningsvis i oppgaven resulterer i at nåværende forhold er avgjørende for oppgavens aktualitet. Med utgangspunkt i en digital kontekst kan det tenkes at oppgavens aktualitet og verdi vil kunne svekkes i løpet av relativt kort tid. Aktualiteten av oppgavens overordnede problematikk, knyttet til forståelse av begrep, kan imidlertid forstås som mer statisk og stabil.

2.1 Tilnærming til sikkerhet i oppgaven

Aven (1997) anvender sikkerhetsbegrepet relatert til ”evnen til å unngå skader og tap som følge av uønskede hendelser” (s. 12). Denne forståelsen av begrepet har lenge stått sentralt i olje- og gassvirksomheten, og var særlig utbredt frem til sikkerhetsbegrepet i senere tid i større grad har blitt benyttet i kombinasjon med helse og miljø (helse, miljø og sikkerhet) (Haukelid, 1999, s. 43). Opprinnelsen og bruksområdet av forståelsen Aven (1997) presenterer er preget av en teknisk tilnærming. Ordlyden og innholdet i beskrivelsen av sikkerhet er imidlertid ikke preget av det. Det kan derfor argumenteres for at forståelsen Aven formidler også er anvendbar i vår oppgave, hvor tilnærmingen til sikkerhet er av kulturbasert karakter. Definisjonen vektlegger evne, som i henhold til Språkrådet (u.d.) betyr ”egenskap til å greie noe, kraft, (økonomisk) kapasitet”. Betydningen av ordet ”evne” legger dermed føringer for at definisjonen av sikkerhet kan betraktes i både teknisk og sosial forstand.

I likhet med mange andre fenomener, betraktes sikkerhet ulikt perspektiver i mellom, som naturligvis vil være av betydning for hvordan fenomenet defineres og tolkes. Vår tilnærming til sikkerhet er av naturlige årsaker preget av innholdet i masterprogrammet (se Vedlegg A), som i hovedsak betrakter sikkerhet i et

samfunnsperspektiv. Perspektiver og forståelser som vektlegges i masterprogrammet samsvarer i stor grad med de elementer som fremheves i Stortingsmeldinger knyttet til samfunnssikkerhet. Meld. St. 10 (2016-2017) fremhever kultur, holdninger og ledelses betydning for samfunnssikkerheten i Norge. Dette er elementer som vil være av betydning for hvordan mennesker forholder seg til risiko, og hvor forberedt en er på å håndtere en alvorlig hendelse (JD, 2016, s. 26). Med det til grunn, betraktes sikkerhet i denne oppgaven som et menneskelig og organisatorisk fenomen, og forstås dermed som et sosialt konstruert konsept.

Sikkerhet i virksomheter beskrives gjerne som et ledelsesansvar, men norsk lovverk stiller krav til deltakelse fra både arbeidstaker og arbeidsgiver (Arbeidsmiljøloven, 2005, § 2-3). Nordmenns verdier, holdninger, interesser og motivasjon bidrar dermed til at sikkerhet blir et felles ansvar. Trygstad og Hagen (2007) betrakter norsk ledelsesforankring i lys av kulturelle forklaringer, og hevder at litteratur viser ”stor grad av samsvar mellom samfunnsverdiene og en ledelseskulturen man empirisk finner i norske bedrifter” (s. 35). Grunnleggende elementer i norsk kultur vil spille inn for organisasjonskulturen, og dermed sikkerhetskulturen i norske virksomheter – som igjen vil påvirke sikkerheten. Kontekst har av den grunn en vesentlig betydning i denne studien av sikkerhetskultur.

2.2 Konfidensialitet, integritet og tilgjengelighet

Begrepet informasjonssikkerhet forveksles og brukes gjerne om en annen med begrepene cyber security, IKT-sikkerhet og digital sikkerhet. I dag benyttes informasjonssikkerhetsbegrepet ofte i en kontekst hvor det er gitt at informasjonen som omtales er digital data. Det som i hovedsak skiller informasjonssikkerhet fra cyber security er at førstnevnte utelukkende omhandler informasjon, uavhengig av format. Cyber security derimot, er ikke avgrenset til informasjon, men til sårbarheter relatert til IKT (NorSIS, 2016, s. 24) Det digitale aspektet av informasjonssikkerhet inngår dermed i Cyber Security, men utgjør bare en andel av begrepets totale betydning (von Solms & van Niekerk, 2013).

Informasjonssikkerhet, er ifølge Direktoratet for forvaltning og ikt (Difi) (u.å), å sikre behandlingen av informasjon med hensyn til konfidensialitet, integritet og tilgjengelighet (KIT). I praksis vil det si å sikre at informasjon ikke blir kjent for

uvedkommende, sikre at den ikke blir endret utilsiktet eller av uvedkommende, og at informasjonen er tilgjengelig ved behov. Begrepene KIT står derfor sentralt i definisjonen av informasjonssikkerhet. KIT anses som sikkerhetsmål som skal bidra til å sikre informasjon i alle former, og dermed også de systemer som informasjonen lagres eller behandles i.

NOU 2015:13 (2015) presenterer tre andre begreper tilknyttet til informasjonssikkerhet: autentisitet, ikke-fornektning, og sporbarhet. Autentisitet er tett knyttet til integritet, men hvor autentisitet handler om å sikre opphavet til informasjonen (NOU, 2015:13, 2015, s. 35). Ikke-fornekting, også knyttet til integritet, handler om at en digital handling ikke skal kunne benektes i etterkant. Sporbarhet omhandler muligheten til å finne ut hva som har skjedd i etterkant, eksempelvis hvem som har håndtert informasjonen og hvor den har blitt kommunisert (NOU, 2015:13, s. 35). Dette er imidlertid KIT som utgjør begrepene som i hovedsak forbindes med informasjonssikkerhet.

2.3 Sikkerhet i Norge

Arbeid med digital sikkerhet i Norge

Ansvaret for sikkerhet blir, ifølge Engen O. A., Kruke, Lindøe, Olsen, Olsen, & Pettersen (2016), beskrevet av norske myndigheter som et ansvar til den som eier eller er operatør av systemet. Det er også en samfunnsoppgave som ivaretas gjennom lover, direktiver, nasjonal forvaltning og regulering (Engen et al., 2016, s. 140). Hvordan den norske statsforvaltning forholder seg til arbeidet med sikkerhet kan forstås som rammer for arbeidet med sikkerhet i Norge, og dermed oppgavens kontekst. Med det til grunn, kan særlig NOU 2015:13 *Digital sårbarhet – sikkert samfunn* (2015) og NOU 2018:14 (2018) *IKT-sikkerhet i alle ledd* være verdt å vise til. Videre formidler Stortingsmeldingene, Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn – samfunnssikkerhet* og Meld. St. 38 (2016-2017) *IKT-sikkerhet - et felles ansvar* sentrale forhold som kan bidra til å beskrive konteksten oppgaven befinner seg i. Ovennevnte stortingsmeldinger og NOUer synliggjør at arbeidet med digital sikkerhet i Norge blir prioritert av politiske organer, og oppfordrer samtidig andre aktører til å gjøre det samme.

I NOU 2018:14 presenteres statens målsettinger for IKT-sikkerheten (2018, s. 25). NOUen trekker frem at myndighetene har en hovedprioritet om å tilrettelegge for at både offentlige og private virksomheter skal ta i bruk nye digitale løsninger. Det påpekes videre at en forutsetning for en vellykket digitalisering er at det skjer innenfor rammer hvor IKT-sikkerheten ivaretas (2018:14, s. 25). Områder som trekkes frem som av særlig betydning for nasjonal IKT-sikkerhet er: forebyggende IKT-sikkerhet, avdekke og håndtere digitale angrep, IKT-sikkerhetskompetanse og kritisk infrastruktur (NOU 2018:14, s. 25).

Vektlegging av kompetanse er en gjenganger i overnevnte dokumenter. Kompetanse inkluderes i flere definisjoner av sikkerhetskultur (Aven et al., 2004; Koch & Richter, 2004; NSM, 2014) og kan forstås som en viktig faktor i arbeidet med sikkerhetskultur. Kompetanse vil videre være en forutsetning for hvordan en forstår begrepet sikkerhetskultur. I Meld. St. 38 (JD, 2016) fremkommer blant annet følgende:

> Regjeringen vil legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse gjennom en nasjonal kompetansestrategi for IKT-sikkerhet. IKT-sikkerhet gjelder alle. Ved at de unge tidlig lærer trygg bruk og forstår nødvendigheten av IKT-sikkerhet, legges grunnlaget for at oppvoksende generasjoner har med seg IKT-sikkerhetskompetanse inn i det videre utdanningsløpet og arbeidslivet.
>
> (s. 12).

Videre formidler Meld. St. 10 (JD, 2016) at regjeringen vil "legge til rette for en langsiktig oppbygging av IKT-sikkerhetskompetanse, gjennom å utarbeide en nasjonal kompetansestrategi for IKT- sikkerhet. Tiltaket innebærer også bevisstgjøringsaktiviteter rettet mot befolkningen og virksomheter." (s. 10).

Oppdaterte regulatoriske rammer

Endringer i utforming av norsk statsforvaltning synliggjør ikke bare endringene digitaliseringen krever, men også at statsforvaltningen tar digitaliseringen på alvor. Eksempelvis skal det etableres et nytt direktorat (Digitaliseringsdirektoratet), hvor Difi og Altinn skal inngå. Direktoratet skal være i drift fra 1. januar 2020 og vil ha vil

ha staten, kommunene, næringsdrivende og frivillig sektor som sine målgrupper (Kommunal- og moderniseringsdepartementet, Finansdepartementet, 2019).

Endringene og faktumet at Norge tar digitalisering på alvor gjenspeiles også i utviklingen av det norske lovverket. Den nye sikkerhetsloven, som trådte i kraft 1. januar 2019, resulterer i endrede regulatoriske krav for IKT-sikkerheten i Norge. Loven skal forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Den nye loven stiller tydeligere krav til informasjonssystemer, infrastruktur og objekter av sentral betydning for nasjonal sikkerhet enn den tidligere utgaven av loven. Loven er gjeldende for virksomheter innenfor de aller fleste samfunnssektorene (Forsvarsdepartementet, 2018). Ifølge NSM (u.å) legger sikkerhetsloven større vekt på hva virksomhetene skal oppnå, og ikke lenger like stor grad hvordan de oppnår målene. Videre vil virksomhetene, ifølge NSM (u.å), også ha ansvar for å gjennomføre regelmessige vurderinger av risiko og iverksette forebyggende sikkerhetstiltak for å oppnå forsvarlig sikkerhet.

Med utgangspunkt i GDPR (General Data Protection Regulation), som erstatter EUs personverndirektiv fra 1995, fremmet regjeringen i 2018 en proposisjon om ny personopplysningslov (JD, 2018). Regjeringens forslag resulterte i en ny personopplysningslov som trådte i kraft 20. juli 2018. Ifølge JD (2018) var gjennomføringen av forordningen et prioritert arbeid for regjeringen. Forordningen har resultert i endringer og nye regler for bedrifter og organisasjoner. Den gjelder for alle aktører, både private og offentlige, som behandler, lagrer og bearbeider digital informasjon (JD, 2018).

Det oppdaterte personvernregelverket medførte en endring i omfang og betydning for personvernombudet. Blant annet stilles det tydeligere krav til personvernombudets kvalifikasjoner, uavhengighet og rammebetingelser. Det er etter innføringen obligatorisk for de fleste statlige og kommunale virksomheter, samt en rekke private organisasjoner og virksomheter, å oppnevne et personvernombud (Datatilsynet, 2018, s. 56). Tall fra Datatilsynet (2018, s. 56) viser en økning av personvernombud fra 755 i 2017 til 1484 i 2018, og dermed også en reell endring på sikkerhetsområdet.

Beskrivelse av nåværende status, i form av fokusområder og endringer i forbindelse med digital sikkerhet, synliggjør oppgavens kontekst. Aktørene som utgjør utgangspunktet for oppgavens empiriske data, og respektives beskrivelser av seg selv, kan sammen med kontekst forstås som oppgavens bakteppe.

2.4 Sentrale aktører i oppgaven

I dette kapittelet presenteres aktørene som har utgitt dokumentene som studeres i oppgaven. Beskrivelsene av aktørene som presenteres er i hovedsak hentet fra respektives hjemmesider.

Regjeringen

Regjering er navnet på Norges utøvende organ. Regjeringen er ledet av Statsministeren, og er videre sammensatt av statsråder/ministere som har hver sine arbeidsområder. Regjeringen har ansvar for å iverksette de beslutningene Stortinget beslutter. Videre kommer regjering forslag til lover og statsbudsjettet til Stortinget (Stortinget, 2019).

Stortinget

Stortinget er Norges folkevalgte forsamling, og omtales gjerne som en nasjonalforsamling. Stortinget består av 169 stortingsrepresentanter fra alle 19 fylker. Stortinget vedtar alle lover og statsbudsjettet i Norge. Stortinget har også som oppgave å kontrollere regjeringen (Stortinget, 2018).

Justis- og beredskapsdepartementet (JD)

Justis- og beredskapsdepartementet (JD) er ansvarlig for rettsvesenet, kriminalomsorgen, politi- og påtalemyndigheten, redningstjenesten, samfunnssikkerhet, utlendingsmyndigheter og polarområdene (Regjeringen, u.d.).

Finansdepartementet (FD)

Finansdepartementet (FD) er ansvarlig for å planlegge og iverksette den økonomiske politikken, budsjettpolitikken, skatte- og avgiftspolitikken, finansiell stabilitet og forvaltning av Statens pensjonsfond (Regjeringen, u.d.). Departementet er ansvarlig for blant annet utarbeiding av nasjonalbudsjettet og forberedelse av statsbudsjettet (Berg L., Finansdepartementet, 2015).

Direktoratet for e-helse (e-helse)

Direktoratet for e-helse er et fag- og myndighetsorgan underlagt Helse- og omsorgsdepartementet, etablert 1. januar 2016 på bakgrunn av behovet for sterkere nasjonal styring og bedre organisering av IKT-feltet (Direktoratet for e-helse, u.å).

I forbindelse med presentasjonen av e-helse trekkes Normen frem. Normen er et organisatorisk knutepunkt med sekretariat under e-Helse (Bjerkan, 2018). Normen betegnes også som en atferdsnorm innen helse- og omsorgssektoren, og er utarbeidet og forvaltet av organisasjoner og virksomheter i sektoren. Normen stiller seg uavhengig andre lovgivninger og krav til informasjonssikkerhet og personvern i sektoren (Direktoratet for e-helse, 2018, s. 9).

Direktoratet for forvaltning og ikt (Difi)

Direktoratet for forvaltning og ikt har ansvar for å følge opp forskrift om universell utforming av ikt-løsninger, knyttet til likestillings- og diskrimineringsloven (Direktoratet for forvaltning og ikt, u.d.).

Datatilsynet

Datatilsynet er et uavhengig forvaltningsorgan underordnet Kongen og Kommunal og moderniseringsdepartementet (KMD), men også ombud. Tilsynet har som oppgave å føre kontroll med at personvernregelverket etterleves og medvirke til at enkeltpersoner ikke krenkes gjennom bruk av opplysninger som kan knyttes til dem (Datatilsynet, u.d.).

Nasjonal sikkerhetsmyndighet (NSM)

Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjon og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. (NSM, 2014). En grov inndeling av NSMs fagområder er IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet (NSM, 2014). NSM fører også tilsyn med over 50 bedrifter i året. Hovedmålet med tilsyn, beskrives av NSM, som å avdekke behov for forbedring av virksomhetenes forebyggende sikkerhetstjeneste og vurdere den enkeltes virksomhets sikkerhetstilstand (2014).

Norsk senter for informasjonssikring (NorSIS)

NorSIS inngår i regjeringens helhetlige satsing på informasjonssikkerhet i Norge. NorSIS skal opptre som en informasjonssikkerhetsinstans og samarbeide med virksomheter for gjennomføring av informasjonssikkerhetstiltak. NorSIS' målgruppe er norske virksomheter, både i offentlig og privat sektor (NorSIS, u.d.). NorSIS skal videre bidra til at informasjonssikkerhet blir en naturlig del av målgruppens hverdag. Dette skal gjøres gjennom å bevisstgjøre om trusler og sårbarheter, opplyse om konkrete tiltak gjennom nyheter, råd og veiledninger, samt påvirke til gode holdninger innen informasjonssikkerhet (NorSIS, u.d.).

Næringslivets Sikkerhetsråd (NSR)

Næringslivets sikkerhetsråd er en medlemsorganisasjon som har som formål om å forebygge kriminalitet mot næringslivet. Arbeidet gjøres gjennom formaliserte og aktive nettverk bestående av offentlige sikkerhetsmyndigheter og medlemmer fra næringslivet. Videre foregår arbeidet i form av rådgivning, kurs og seminarer. NSR gir råd og oppdatert informasjon til virksomheter om sikkerhetstiltak knyttet til blant annet datakriminalitet og informasjonspionasje (NSR, u.d.).

3 Teori

Dette kapittelet presenterer oppgavens teorigrunnlag. Innledningsvis presenteres teorier om sikkerhetsarbeid og organisatoriske ulykker. For en redegjørelse av de begreper oppgaven tar for seg, gis det videre en presentasjon av kultur, sikkerhetskultur og organisasjonskultur. Videre presenteres ulike maktforhold, i samfunnet og i tekst, og Foucaults teorier om diskurs og sosialkonstruktivisme, som gir et innblikk i hvordan tekster og aktører påvirker forståelsen, og kan legger føringer for arbeidet med sikkerhetskultur. Samlet sett danner teorikapittelet et grunnlag for å analysere og diskutere oppgavens datagrunnlag.

3.1 Arbeid med sikkerhet

I løpet av de siste tiår har fokusområder i sikkerhetsarbeidet skiftet karakter en rekke ganger. Fokuset flyttet seg først fra tekniske løsninger over til menneskelige feilhandlinger, men vektlegger nå i større grad sikkerhet gjennom systemtiltak rettet mot organisasjon og ledelse (Aven et al., 2004, s. 27). Ifølge Aven et al. (2004), omtaler Hale, Baram og Hovden (1998) tre epoker innen styring av sikkerhet. I den tredje epoken, som vi befinner oss i nå, fokuseres det på organisasjon og sikkerhetsledelse. Særlig vektlegges relasjoner og samspillet mellom ulike faktorer i organisasjon eller samfunn. Arbeid med sikkerhet kan forstås som styring av sikkerhet. Ifølge Aven et al. (2004, s. 32) kan sikkerhet styres mot virksomhetens definerte mål gjennom risiko- og sårbarhetsanalyser, ledelse og styring, planlegging, opplæring, informasjon, sikkerhetskultur og teknisk design. Videre skriver Aven et al. (2004) at styring dreier seg om:

> (...) både om å fastsette mål, utforme tiltak eller virkemidler og å "overvåke" den praktiske gjennomføringen. Styring, både på samfunns- og organisasjonsnivå, kan være vanskelig av mange grunner, ikke minst fordi aktørene - individer og grupper - som skal iverksette tiltak, ikke alltid følger de planer og prosedyrer som er fastlagt.
>
> (s. 36)

Som sitatet formidler er styring avhengig av relasjoner innad i en organisasjon, i form av relasjoner mellom ansatte og ledelse, men også på tvers av ulike avdelinger. Aven et al. (s. 36) påpeker at styring videre dreier seg om hvordan ulike aktører tolker informasjon, og hvilke verdier og normer som råder i organisasjonen. Med andre ord

vektlegges særlig samspillet mellom menneske og organisasjon i arbeid med sikkerhet.

Jan-Pierre Bento (Bento, 2001, s. 3) hevder at alle kompliserte hendelser er relatert til samspillet mellom menneske, teknologi og organisasjoner (MTO). Ifølge Bento er 70-80% av alle rapporterte hendelser innen luftfart i Sverige relatert til MTO (s. 3). Det er ikke teknologien som representerer den største sikkerhetsmessige utfordringen, men mennesket rundt den (Sjølstad, Høie, & Daler, 2010, s. 37). I lys av et spørsmål knyttet til hvorfor organisasjon og mennesker i sosiotekniske systemer ikke presterer bedre, belyser Bento (2001) flere faktorer som bidrar til problemer knyttet til MTO:

- Det tas ikke hensyn til mennesket når nye teknologier introduseres
- Det tas ikke hensyn til menneskets begrensninger ved drift, vedlikehold og utprøving av tekniske systemer
- Kunnskaper om atferd blir ikke brukt i praktiske, tekniske sammenhenger.
- Det er ikke i tilstrekkelig grad vektlagt analyse av menneskelig atferd i problemanalysen
- Det er mangelfull kompetanse om de faktorer som bidrar til feilhandling
- Oppgaveanalyse blir ikke gjennomført ved utvikling av arbeidsoppgaver, opplæring og instrukser
- Det er en tendens til å skylde på, eller henvise til, tekniske årsaker
- Prosessen/systemet er i kontinuerlig drift

(s. 4)

Som nevnt overfor og som utdraget synliggjør, vil menneskelige faktorer være avgjørende, men ikke utelukkende en årsak til at hendelser oppstår. Hendelser vil omtrent alltid oppstå som følge av en kombinasjon av flere grunnleggende årsaker (Bento, 2001, s. 7).

3.2 Normale ulykker

I NSMs rapport *Risiko 2017* (NSM, 2017, s. 24) beskrives et nytt og endret sårbarhetsbilde. I henhold til NSM kan digitalisering i samfunnet medføre at kritiske samfunnsfunksjoner og systemer blir mer sårbare. Digitaliseringen øker kompleksiteten som følge av blant annet lange verdikjeder bestående av en rekke ulike aktører. De lange verdikjedene resulterer i utfordringer knyttet til virksomheters oversikt over egne sårbarheter. Sikkerhetshendelser ett sted kan gi uventede feil og

konsekvenser et annet sted i verdikjeden. Det er derfor utfordrende å ha kontroll over eget sårbarhetsbilde, da virksomheter vil kunne arve sårbarheter fra andre ledd i kjeden. Vi opplever at NSMs beskrivelser av samfunnets sårbarhetsbildet samsvarer med sentrale trekk i Charles Perrows (1999) teori om Normal Accidents. Tross det faktum at Perrow ikke tar den digitale konteksten i betraktning er hans teori fortsatt relevant i dag.

I Normal Accidents Theory, eller teori normale ulykker, ser Perrow på strukturer i teknologiske systemer (Engen et al., 2016, 143). Perrow forklarer feil og suksess som en funksjon av hvordan systemene er oppbygd (s. 143). Videre vektlegger Perrow systemers strukturelle egenskaper og samfunnsaktørene som er ansvarlig for systemenes eksistens i sin teori. Perrow presenterer de strukturelle karakteristikkene ved å klassifisere systemenes dimensjoner fra lineær til kompleks, og hvordan de er knyttet sammen, fra løst til tett koblede systemer (Engen et al., 2016, s. 144). De systemer som er tett koblede og komplekse har noen særegne strukturelle trekk som gjør ulykker normale (Engen et al., 2016, s. 145). Komplekse systemer har med andre ord, ifølge Perrow, en unaturlig nærhet mellom deler og enheter i et system som kan skape uforutsette interaksjoner. Dahlberg (2004) skriver følgende om normale ulykker:

> I menneskesprog betyder det, at små og tilsyneladende uskyldige fejl i systermerne kan resultere i katastrofer, fordi systemets dele interagerer på kryds og tværs af de funktionsakser, designerne har indbygget.
>
> (s. 17)

Avhengigheter i tett koblede systemer medfører at buffere, redundans og erstatninger må bli designet inn i systemet på forhånd. Det er dog ikke mulig å eliminere risikoen for feil eller ulykker ved å innføre sikkerhetssystemer og rutiner, fordi normalfeilene nødvendigvis er innebygget i systemet (Dahlberg, 2004, s. 17). I Perrows analyser av de høyteknologiske systemer, konkluderer han med at noen teknologier (som atomkraftverk) må avvikles. Perrow begrunner konklusjonen med at det i høyteknologiske systemer vil oppstå ulykker uansett hvor mye ressurser en bruker på sikkerhet. Disse ulykkene omtales derfor som normale ulykker.

I sitt etterord i boken *Normal accidents* (1999, s. 380) kommenterer Perrow Diane Vaughns analyse av Challanger-ulykken. Ifølge Kringen (2009, s. 52) mente Vaughn at de underliggende faktorene som bidro til ulykken var forårsaket av sosiale og kognitive prosesser knyttet til "normalisering" av avvik. Ifølge Perrow (1999, s. 379) oppstod Challenger-ulykken som følge av at organisasjonen tillot at produksjonspress gikk på bekostning av sikkerhet (Perrow, 1999, s. 379). Perrow stiller seg derfor kritisk til Vaughns analyse, og mener at den ikke tar hensyn til eksterne faktorer, som politiske beslutningsprosesser og økonomisk makt: "We miss a great deal when we substitute culture for power." (Perrow, 1999, s. 380).

3.3 Kultur

Det er en økende interesse for sammenhengen mellom kultur, sårbarhet og sikkerhet i organisasjoner. 22. juli-kommisjonens rapport, blir av Engen et al. fremhevet som av betydning for tilknytningen kultur og organisasjon har fått til samfunnssikkerhet (2016, s. 156). I henhold til Engen et al. (2016, s. 157) konkluderte kommisjonen med at grunnleggende holdninger og kultur hos ledere i norsk forvaltning var en sentral faktor i forklaringen av hva som gikk galt den 22. juli 2011. Ifølge Engen et al. (2016, s. 157) fremhever teorien *Man made disasters* av Barry A. Turners hvordan delte antakelser og normer styrer den kollektive oppmerksomheten og atferd knyttet til risiko og sikkerhet i organisasjoner. Videre skriver Engen et al. (2016, s. 157) at kultur, ifølge Turner og Pidgeon, kan forme en blindhet for visse farer og trusler. Dette kan medføre at ulykker inkuberer og til slutt resulterer i en katastrofe.

Før vi ser nærmere på kultur-begrepet i kombinasjon med sikkerhet er det formålstjenlig å ta en nærmere titt på kultur-begrepet isolert sett. Kulturbegrepet, brukt til å beskrive sentrale trekk ved et samfunn kan defineres på flere måter. Per Morten Schiefloe (1999) ser på ulike definisjoner av kultur i en samfunnskontekst, og skriver følgende: "Sammenfattet kan vi forstå kan vi forstå kultur i denne betydningen som *akkumulert erfaring og etablering av verdier utbredt og akseptert i samfunnet og som overføres mellom generasjoner.*" (1999, s. 2). Schiefloe (2011, s. 198) deler kultur inn i tre hovedgrupper av fundamenter: 1) språk, 2) kunnskap, tro og verdier, og 3) normer og sanksjoner. Kultur kan forstås som et system på flere nivåer, som betyr at kulturer eksisterer i deler av samfunn, eksempelvis i en organisasjon

(Schiefloe, 2011). Uavhengig av strukturelt nivå, legger Schein (i Schiefloe, 2011) følgende mening i ordet kultur:

> Et mønster av grunnleggende antakelser - skapt, oppdaget eller utviklet av en gruppe etter hvert som den lærer å mestre sine problemer med ekstern tilpasning og intern integrasjon - som har fungert tilstrekkelig bra til at det blir betraktet som sant og til at det læres bort til nye medlemmer som den rette måten å oppfatte, tenke og føle på i forhold til disse problemene.
>
> (s. 7)

Som sitatet poengterer overføres kulturen gjennom sosialisering og opplæring til nye medlemmer. Det vil kreve kunnskap og etterlevelse av kulturen for å bli akseptert som et fullverdig og integrert medlem (Schiefloe, 2011, s. 198). Selv om kultur ofte, ifølge Schiefloe (1999, s. 6), knyttes til samfunnsnivå, er det også mulig å tilnærme seg kultur fra et individuelt ståsted. Dette begrunnes med at kultur er noe mennesker tilegner seg gjennom læring og er en sentral del i den sosiale arven som mennesker i et samfunn har til felles. Mennesker er bærere, brukere og formidlere av kultur (Schiefloe, 1999, s. 6).

Videre er, ifølge Schiefloe (1999, ss. 23-24), alle kulturer er materielt forankret, da kultur er noe som eksisterer innenfor rammer av menneskeskapte og naturgitte omgivelser. Kulturer er i den forstand bærere av teknologi, i form av redskaper og kunnskap som anvendes i produksjon av tjenester og varer. Utrykket kulturelt etterslep dreier seg om en tilstand hvor den materielle utviklingshastigheten er større enn den forståelsesmessige og institusjonelle utviklingen. Ifølge Schiefloe (1999, s. 24) kan manglende samsvar mellom materiell og intellektuell utvikling gi opphav til sosiale problemer og konflikt.

3.4 Sikkerhetskultur

Som sitatet om sikkerhetskultur av Reason (1999) presentert innledningsvis viser til, er sikkerhetskultur et mye omdiskutert begrep. Aven et al. (2004) henviser til en definisjon av sikkerhetskultur gitt av The Health and Safety Commission i England:

> Sikkerhetskulturen i en organisasjon er produktet av individets og gruppens verdier og holdninger, av kompetanse og atferdsmønstre som viser forpliktelse og dyktighet i forhold

til organisasjonens helse- og sikkerhetsprogrammer. Organisasjoner som har en positiv sikkerhetskultur er kjennetegnet ved en kommunikasjon bygget på gjensidig tillit, felles oppfatning om betydning av sikkerhet, og med tiltro til at organisasjonens sikkerhetsmål fungerer effektivt.

(s. 34)

Som sitatet formidler betraktes sikkerhetskultur gjerne på et virksomhetsnivå. Med utgangspunkt i sitatet hevder Aven et al. (2004) videre at : "Sikkerhetskulturen handler om den kollektive forståelse av *hva* som som er farlig og *hvordan* en bidrar til å reduseres farene." (s. 34). Også Koch og Richter (2004) hevder at sikkerhetskultur sees på som et aspekt av den organisatoriske kulturen:

We define safety culture as the shared and learned meanings, experiences and interpretations of work and safety—expressed partially symbolically—which guide peoples' actions towards risks, accidents and prevention. Safety culture is shaped by people in the structures and social relations within and outside the organization.

(s. 705)

I en virksomhet omtales sikkerhetskultur ofte som viktig for å forstå hvilke særtrekk som kan bidra til større eller mindre fokus på sikkerhet (Aven et al., 2004, s. 33). Sikkerhetskultur i en virksomhet vil blant annet være avgjørende for hvordan sikkerhetstiltak betraktes med tanke på økonomi og tidsmessige hensyn. Et eksempel er hvorvidt en organisasjon velger snarveier og lettvinte løsninger på bekostning av sikkerhetsmål (Aven et al., 2016, s. 34).

James Reason (1997) presenterer begrepet "impossible accidents". Westrum (i Reason, 1997, s. 38) argumenterer for at virksomheter som bedriver potensielt farlige aktiviteter må ha en forestilling om hva som kan gå galt dersom de skal forhindre at ulykker oppstår. I forkant av en ulykke vil det omtrent alltid forekomme faresignaler, men for å identifisere disse kreves en forestilling om den potensielle ulykken (Reason, 1997, s. 39). Det er imidlertid umulig å forutse alt fremtiden bringer, og en kan umulig besitte en forestilling om enhver mulig ulykke.

3.5 Organisasjonskultur

Som det fremkommer overfor, blir sikkerhetskultur gjerne i beskrevet i lys av organisasjoner og organisasjonskultur. Astrid og Geir Kaufmann (2009, s. 266) presenterer følgende som en populær forståelse av organisasjonskultur: "måten vi gjør tingene på her hos oss". Videre hevder de at sosiologiske definisjoner vektlegger virkelighetsoppfatningene, verdiene og normene som binder en gruppe sammen (s. 266). Hovedfunksjonene til en organisasjonskultur er, ifølge Kaufmann og Kaufmann (2009), å skape identitet, stabilitet, mening og forplikte. Organisasjonskulturen kan øke medarbeidernes identitetsfølelse, forpliktende engasjement overfor målene og hvor kulturen klargjør, skaper mening og stabilitet (s. 269). Edgar H. Schein (1987) hevder at:

> (…) faguttrykket kultur bør reserveres for grunnleggende antakelser og oppfatninger som deles av alle medlemmene i en organisasjon, som opererer ubevisst og som på en grunnleggende og "tatt-for-gitt" måte definerer organisasjons syn på seg selv og sine omgivelser.
>
> (s. 5)

Kaufmann og Kaufmann (2009) tar for seg hvordan en organisasjonskultur oppstår og utvikles. Utvikling av organisasjonskultur er knyttet til forholdet mellom lederen, ytre miljø og medarbeiderne. For det første kan grobunnen for en kultur være preget av at grunnleggerne eller lederne hatt dynamiske personligheter med sterke verdier og klare visjoner. Det andre som trekkes frem at kultur synes å delvis kunne oppstå gjennom den felles erfaringen og forståelsen som en oppnår gjennom regelmessig samvær på jobben. Henning Bang (1987) oppsummerer definisjoner av organisasjonskultur fra ulike perspektiv i en definisjon:

> Organisasjonskultur er de sett av felles delte normer, verdier og virkelighetsoppfatninger som utvikler seg i en organisasjon når medlemmene samhandler med hverandre og omgivelsene.
>
> (s. 24)

I en organisasjon vil det imidlertid være flere kulturer som råder. Ifølge Kaufmann og Kaufmann (2009, s. 268) vil det innad i en organisasjonskultur eksistere mindre kulturer, som kalles subkulturer. Kaufmann og Kaufmann vektlegger at endring i organisasjoners kultur kan være en lang og krevende prosess, da verdier, normer og organisasjonskultur (s. 273). Videre hevder Kaufmann og Kaufmann at det ifølge Yukl (2006) og Robbins (2003) først og fremst skjer kulturendringer dersom organisasjoner konfronteres med en overlevelseskrise (s. 273). Dette kan ses i lys av hva Guldenmund (2007, s. 726) formidler, nemlig at organisasjoner ikke ses på som et lukket system. Årsaken er at lokale forhold ikke utelukkende bestemmer kulturen i organisasjonen:

> Actually, when a company has not experienced any serious problems during its existence there probably will not be a typical culture (Schein, 1992); its culture will be determined largely by external (national, regional) conditions and the (educational, social-economic, religious) background of its workforce (Guldenmund et al., 2006).
>
> (Guldenmund, 2007, s. 726)

3.6 Michel Foucault og sosialkonstruktivisme

I henhold til sosialkonstruktivisme blir menneskers virkelighetsforståelse formet og kontinuerlig utviklet av situasjoner, opplevelser, historie og kontekst (Engen et al., 2016, s. 98). Det vil si at virkelighetsoppfatning er et sosial konstruert fenomen, og som dermed innebærer at virkeligheten ikke eksisterer som en objektiv størrelse. Virkeligheten blir i et sosialkonstruktivistisk perspektiv skapt gjennom sosiale interaksjoner.

Et sannhetsregime innebærer, ifølge Engen et al. (2016), at det eksisterer visse oppfatninger og praksiser angående hva som oppfattes som riktige og legitime handlinger, og derfor også hva som er galt og illegitime handlinger. Ifølge Michel Foucault (i Engen et al., 2016, s. 106) produseres sannheten gjennom ekspertsystemene som inngår i den statlige administrasjonen, der retningslinjer og anbefalinger for hvordan befolkningen bør oppføre seg i ulike situasjoner blir produsert. Nevnte prosesser bidrar til å skape oppfatninger om hva som er norm for "god" atferd og eventuelt hva som ikke er (Engen et al., 2016, s. 106).

I forord og etterord i Michel Foucaults bok, *Seksualitetens historie 1* (Foucault, 1999, s. 181), kommenterer Espen Schaanning at Foucaults strategi i vitenskapelige undersøkelser var å relativisere (i Foucault, 1999, s. 181). Dette innebærer at Foucault satt tidligere tankesett opp mot tankesett i daværende tid. Fortidens mennesker hadde et annet tankesystem, og slik kan det tolkes at tankesystemene vil utvikle og endre seg også i fremtiden (Foucault, 1999, s. 181). Ifølge Schaaning, mener Foucault at de ulike vitenskapsgrenenes utvikling og historie skyldes en økning i fornuft, men snarere en gradvis fjerning av fordommer og overtro til fordel for sannheten (i Foucault, 1999, s. 181).

I henhold til Østbye, Helland, Knapskog, Larsen, & Moe (2013, s. 95) viser Foucault i sin bok, *Galskapens historie i klinikkens tidsalder,* til hvordan diskursene om sinnssykdom var betinget av datidens kunnskap og sosiale maktstrukturer. Foucault studerte hvordan daværende diskurs begrenset hva som kunne sies om og gjøres med mentalt syke, og samtidig legitimere maktutøvelse av ulike slag (s. 95). Studiene gir nåtidens mennesker forutsetninger til å bli oppmerksomme på at fortidens mennesker var rasjonelle og fornuftige på sitt vis, gitt sin tid (Schaanning i Foucault, 1999, s. 181). Ifølge Østbye et al. (2013, s. 95) gir Foucaults studier gir et innblikk i hvordan sosiale mekanismer, som kunnskap og makt, regulerer i gitt historisk kontekst hva som kan sies og tenkes om et bestemt fenomen.

3.7 Makt og maktforhold

Det norske samfunnet kan betegnes som et pluralistisk politisk system. Et pluralistisk system innebærer en maktfordeling mellom lovgivende, utøvende og dømmende makt. Det inkluderer også en maktdeling mellom ulike politiske partier. I tillegg må det foreligge en spredning av makt mellom ulike maktgrupper, både i offentlige og private grupper. Ole T. Berg trekker frem private virksomheter og interesseorganisasjoner som eksempler (2018a). Berg kommenterer følgende om maktforhold i pluralistiske systemer:

> De fleste vestlige land preges likevel fortsatt av at makt stanser makt. Delvis uavhengig av forfatningsmessige regler er det vokst frem komplekse politiske systemer preget av en vanskelig beskrivbar fordeling av makt mellom en lang rekke organer.
>
> (2018a)

Organene Berg viser til gjelder nasjonalforsamling og regjering, forvaltningsetater, partier, interesseorganisasjoner, store virksomheter, adhoc-bevegelser og massemedier (2018b). Makt er av Max Weber definert som: ”power is the probability that one actor within a social relationship will be in a position to carry out his own will despite resistance, regardless of the basis on which this probability rests.” (i Berge, Meyer, & Trippestad (red.), 2003, s. 25). Aktøren Weber omtaler trenger dog ikke vær en identifiserbar person. En aktør kan være en institusjon, organisasjon, et politisk parti, kirke eller bank (Berge et al., 2003, s. 25). Johannes Brinkmann betrakter maktforhold og definisjoner. Om maktdefinisjoner skriver Johannes Brinkmann (1991) følgende:

> Makt settes iblant lik all slags påvirkning, inklusive respektert kompetanse og medbestemmelse gjennom ”påpekning av beste løsning”. Da blir maktbegrepet alt for vidt, og fjerner seg også vel langt fra dagligtalen. En bør i definisjon helst ta hensyn til store forskjeller i maktmidler eller sanksjoner. Makt kan i noen tilfeller bygge på ”hardere” maktmidler som tvang og vold, og i andre tilfeller på mykere midler som autoritet og innflytelse.
>
> (s. 68)

Autoritet og innflytelse, som Brinkmann (1991) presenterer som mykere maktmidler, kan sees i sammenheng med definisjonsmakt. I henhold til Nasjonal digital læringsarena (2018) betyr definisjonsmakt ”(...) å ha makt til å påvirke hvordan folk oppfatter et fenomener, og hvilke meninger de utvikler.” Tore Slaatta (1999) omtaler definisjonsmakt som makt til å innvirke på hvem som får tilgang til det offentlige ordskiftet, og makt til å omforme ”subjektive” problemer til ”objektive” (Slaatta, 1999). Aktører i besittelse av definisjonsmakt kan dermed influere for hva, hvordan og hvorfor som er viktig i den samfunnsmessige konteksten en befinner seg i, her sikkerhetskultur i en digital kontekst i Norge.

3.8 Makt i tekst

Maktforhold eksisterer også i form av tekst. I *Maktens tekster* (Berge et al., 2003, ss. 200-218) gis det ved eksempler fra vitenskapelige tekster et svar på hvordan en tekst får institusjonell makt (s. 20). Meyer påpeker at samfunnsvitenskapelige tekster kan

ha stor makt, og hevder videre at utvelgelsen av eksempler ikke er tilfeldig. Tankekategorier og fakta i samfunnsvitenskapelige tekster er premissleverandører for offentlige beslutningsprosesser, og at vi alle berøres av deres makt (s. 20). Videre understreker Meyer at makten som omtales ikke er av personlig karakter, men at men av forhold knyttet til forfatterens rolle som forsker og samfunnsborger (s. 20).

Amund Børdahl (i Berge et al., 2003, s. 45) beskriver makten som spredt, i og av prosa, men også omvendt: at prosaens spredning er tilknyttet maktforhold. Ifølge Børdahl skal sistnevnte forstås på to måter. For det første bidrar maktinstitusjoner til å spre bestemte tekster i samfunnet, eksempelvis gjennom skoleverket og rettsvesenet. For det andre er enhver prosatekst i seg selv en spredning i form av språk, og hvordan språk spres gjennom en tekst vil blant annet gi uttrykk for makt (s. 45).

Kjell Lars Berge (Berge et al., 2003 s. 25) hevder at all maktutøvelse ikke utelukkende lar seg forstå som av bevisst hensikt: ”Maktutøvelsen forutsetter også en gjensidig intensjonelle rettethet. Handlingen som utøves overfor en eller annen, av en eller annen, må – bevisst eller ubevisst – forstås som noenlunde likt av begge parter.” (s. 25). Maktutøvelse krever derfor at visse forhåndsbestemte gjensidighetsnormer er etablert, forstått og overholdt. I tillegg krever maktutøvelsen at makthandlingen utøves på en måte som begge parter kjenner igjen (s. 25). Oppgaven til en tekst dekker nettopp dette: ”Den skal ha noen egenskaper som gjør det mulig å skjønne hva slags handling som faktisk skal utføres, og hva den innebærer for aktøren som skal handle, og for aktørene det blir handlet i forhold til.” (s. 25).

Kjell Lars Berge (2003, ss. 30-31) deler studien av forholdet mellom makt og tekst i tre ulike dimensjoner: teksten som 1) unik handling, 2) forekomst av en tekstnorm, og 3) representasjon av en viss ideologisk posisjon eller diskurs. Førstnevnte dreier seg om at enhver tekst besitter en egenverdi, og kan konstituere et eget meningsunivers hvor forholdet mellom tekstskaper og tekstmottaker er gitt mening i selve teksten. Uavhengig av tekstskaperens status og institusjonelle posisjon kan dermed teksten ha eller skaffe seg makt, som følge av at leseren utelukkende lar seg overtale av teksten innhold og formidling (ss. 30-31). Dimensjon nummer to tar for seg at tekst, uavhengig av innhold, har eller skaffer seg makt på bakgrunn av hvor den stammer fra. Et relevant eksempel for oppgaven er retningsgivende tekster, som eksempelvis

lover og forordninger fra statsmakten (s. 31). Den tredje dimensjonen tar utgangspunkt i at tekst kan ha eller skaffe makt ved å gjenta, bekrefte, forsterke og/eller kvalifisere ”en *viss ideologisk posisjon* som vi må forstå teksten ut fra dersom vi skal forstå den på en relevant måte, det vil si som den teksten den er ment til å være i en særskilt kontekst.” (ss. 31-32). Dimensjonen kan knyttes til sentrale forhold i nåværende sikkerhetsepoke, hvor fokus i større grad rettes mot organisasjon og sikkerhetsledelse. Tekster som representerer denne ideologien kan dermed, i henhold til dimensjonen, ha eller skaffe makt.

4 Metode

Dette kapittelet tar sikte på å gi en grundig presentasjon av metodikken som ligger til grunn for oppgaven. Innledningsvis presenteres kvalitativ metode og oppgavens metode, dokumentanalyse. I kapittel 4.2, Dokumentanalyse, gis en gjennomgang av teorier og tilnærminger som utgjør sentrale forhold i vår tilnærming til og gjennomføring av oppgavens dokumentanalysen. Før selve gjennomføringen presenteres i kapittel 4.4, tar kapittelet for seg utgangspunktet for og utvikling av studiens forskningsspørsmål. Videre presenteres empirisk datagrunnlag og kvalitetsvurderinger av oppgaven. Avslutningsvis gis en oppsummering av tre forstudier som ble gjennomført i forkant av arbeidet med selve masteroppgaven, og som har vært av bestemmende for oppgavens utvikling.

4.1 Kvalitativ metode

Oppgaven er et studie av dokumenter og vil derfor typisk omtales som en dokumentanalyse. Vår forskningsmetode er basert på en kvalitativ tilnærming. Tove Thagaard trekker frem søken etter forståelse av sosiale fenomener som en typisk karakteristikk for kvalitativ forskning (Thagaard, 2018, s. 11). Repstad (2007, i Thagaard, 2018, s. 11) hevder at ordet kvalitativ viser til kvaliteter, som vi si egenskaper eller karakterer ved fenomener. I vårt studie er derfor en metode av kvalitativ art et naturlig og hensiktsmessig valg.

Ifølge Thagaard (2018, s. 11) er kvalitative metoder et felt i utvikling, som påvirkes og gjenspeiles av endringene i samfunnet. Samfunnet er i økende grad preget av en visuell kultur, som har resultert i nye forskningsmetoder (s. 12). Et fellestrekk for metoder av kvalitativ karakter at analysene er forbeholdt data i form av tekst (s. 13). Kvalitative metoder egner seg godt i studier av tema hvor det eksisterer lite forskning, og som derfor krever åpenhet og fleksibilitet (s. 12). Thagaard påpeker at kvalitative metoder er særlig egnet for studier av kulturelle fenomen. Sikkerhetskultur i seg selv, er ikke et nytt fenomen, men konteksten sikkerhetskulturen studeres i er absolutt av nyere karakter. Ifølge Silverman (2014, i Thagaard, 2018, s. 12) legger en kvalitativ tilnærming føringer for at en kan studere fenomen som ville vært vanskelig å få tilgang til ved bruk av andre metoder. I henhold inndelingen av kvalitative metoder, kan oppgavens metode betraktes som en analyse av forliggende tekster og visuelle

uttrykksformer. Foreliggende tekster representerer i denne oppgaven offentlig tilgjengelige dokumenter utgitt av et utvalg norske aktører.

Oppgavens forskningsdesign er i stor grad fleksibelt, som ifølge Thagaard er et kjennetegn for kvalitative studier (s. 16). Marshall og Rossman (2016, s. 100 i Thagaard, 2018, s. 50) vektlegger betydningen av å innarbeide fleksibilitet ved utforming av forskningsdesign. I praksis innebærer dette å ivareta muligheten for at fremgangsmåten kan justeres underveis i forskningsprosessen. Fleksibiliteten åpner for at en kan endre strategien for utviklingen av oppgavens datagrunnlag basert på hvor godt den planlagte strategien fungerer (s. 50). Hovedpoenget er at funn kan åpne for muligheter for å gjøre nye funn. Ved et fleksibelt design til grunn åpner en for at en kan inkludere element som ikke var inkludert i studiens opprinnelige strategi. Ifølge Thagaard (2018, s. 50) gir et fleksibelt, problemorientert forskningsdesign dermed mulighet for en spesielt grundig belysning av problemstillingen.

4.2 Oppgavens dokumentanalyse

Ifølge Thagaard kan en dokumentanalyse betraktes som et feltarbeid på internett eller i et bibliotek (s. 119), hvor dokumenter vil ha en rolle tilsvarende et objekt har i et intervju eller en observasjon. En dokumentanalyse er som ordlyden formidler i hovedsak en analyse av dokumenter. Dokumenter kan imidlertid være så mangt, som resulterer i at det innenfor metoden vil være store variasjoner i analysene. Studiens forskningsdesign blir derfor avgjørende for den metodiske utførelsen.

Thagaard viser til flere eksempler på dokumentanalyser. Eksempelvis, vil en i dokumentanalyse av kilder om saksforhold analysere med hensyn til kildekritiske vurderinger. I et studie av faglitteratur knyttet til et bestemt tema derimot, vil en derimot ta utgangspunkt i sentrale publikasjoner for å deretter oppsøke kildene som refereres til (s. 21). Sigmund Grønmo (2004, s. 142) på sin side, presenterer en form for dokumentanalyse som han omtaler som kvalitativ innholdsanalyse. Ifølge Grønmo vil en kvalitativ innebære en systematisering av utvalgte element med formål om å belyse studiens problemstilling (s. 142). Dette innebærer også eksempelvis bilder, som er et av flere forhold som skiller en kvalitativ innholdsanalysen fra vår dokumentanalyse. Med andre ord er tilnærmingene til metoden av ulikt omfang og karakter. Før selve utførelsen av metoden presenteres, vil påfølgende derfor

presentere tilnærminger og teoretiske retninger som har inspirert og farget vår utførelse av oppgavens dokumentanalyse. Utførelse og mer spesifikke konkrete forhold vil presenteres og beskrives nærmere i kapittel 4.4. Se kapittel 4.5 for empirisk datagrunnlag.

4.2.1 Fremdrift inspirert av grounded theory

Enkelte trekk ved oppgavens dokumentanalyse er i tråd med grounded theory, utviklet av Barney Glaser og Anselm Strauss (Hartman, 2001, s. 28). Grounded theory er en omfattende prosess med formål om å genere ny teori ved bruk av konkrete kriterier og fremgangsmåter. Glaser (i Hartman, 2001, s. 30) forklarer at en grounded theory forskningsprosess skal innledes med færrest mulig forutsatte meninger. I forskning med utgangspunkt i grounded theory vil allerede eksisterende teorier derfor unnvikes. I praksis vil det si at en starter med ”blanke ark” (Hartman, 2001) som innebærer at studien ikke tar utgangspunkt i en problemstilling som vil være styrende forskningen.

Til forskjell fra grounded theory tar ikke vår studie utgangspunkt i fullstendig blanke ark. I oppgaven unnvikes heller ikke allerede eksisterende teorier, men i likhet med grounded theory har ikke problemstillingen vært styrende for arbeidet. Med utgangspunkt i skissen vi utviklet i forkant av studien hadde vi en idé om hvor vi ville. Vi var imidlertid hele tiden åpne nye element og innfallsvinkler. Dette innebar at vi i studiens innledende fase ikke hadde en klar tanke om hvordan studiens metodiske forløp ville utarte seg. I likhet med grounded theory har derfor selve utviklingen av datagrunnlaget vært avgjørende for oppgavens retning. Kathy Charmaz (2006) omtaler grounded theory som:

> Used well, grounded theory quickens the speed of gaining clear focus on what is happening in your data without sacrificing the detail of enacted scens. Like a camera with many lenses, first you view a broad sweep of the landscape. Subsequently, you change your lens several times to bring scenses closer and closer into view.
>
> (s. 14)

Charmaz sin beskrivelse av hvordan grounded theory fungerer er i stor grad overførbar til denne oppgavens dokumentanalyse. Prosessen Charmaz beskriver ved hjelp av kamera og linser, innebærer i praksis at funn åpner for nye funn, men at det

krever tilpasning av verktøy. Datainnsamling og analyse kan dermed betraktes som gjensidig avhengige og vil foregå parallelt. I tråd med sitatet overfor, startet oppgavens dokumentanalyse som et søk i et større landskap, men som etter hvert fikk en naturlig innsnevring som følge av funn gjort underveis i søket. Funn gjort i den tidlige fasen av prosjektet, la føringer for videre søk og analyser. Vi kan på vår side visuelt beskrive oppgavens dokumentanalysens en strøm av data gjennom en stor trakt. I starten av trakten er åpningen vid og stor, men jo nærmere utløpet en kommer, jo mer innsnevret blir åpningen.

4.2.2 Egenskaper som typisk inngår i en diskursanalyse

Typiske formål for kvalitative analyser er å oppnå en helhetlig forståelse av spesifikke forhold, eller å utvikle teorier og hypoteser om bestemte samfunnsmessige sammenhenger (Grønmo, 2004, s. 265). Sistnevnte er formål samsvarer i stor grad med formålet i vår oppgave. Formålet om utvikling av teorier og hypoteser kan imidlertid forstås som samsvarende med formålet i grounded theory.

Grønmo trekker frem diskursanalyse som en fremgangsmåte i analyser hvor formålet er en helhetlig forståelse (s. 282). Diskursanalyser er i likhet med dokumentanalyser en kvalitativ metode hvor en studerer data relatert til menneskelige uttrykksformer. I motsetning til en dokumentanalyse, er en diskursanalyse imidlertid i større grad basert på verbale uttrykksformer (Thagaard, 2018, s. 117-120). Vår oppgave er utelukkende en dokumentanalyse, men er i stor grad preget av forhold om står sentralt i en diskursanalyse. Spesielt av betydningen for selve analyseringen av data er det relevant å vise til egenskaper ved en diskursanalyse. Ifølge Grønmo vil kvalitativ innholdsanalyse av tekster være en viktig fremgangsmåte i forbindelse med en diskursanalyse (s. 142). Med andre ord vil en dokumentanalyse utgjøre et sentralt element i en gjennomføring av en diskursanalyse, så fremt det omhandler tekst. Med det til grunn er det ikke rent unaturlig at forholdet tilsynelatende bærer preg av en viss gjensidighet.

Gjennom systematiske og inngående studier av innhold i en bestemt tekst tar diskursanalyse, ifølge Grønmo, sikte på å avdekke hvordan teksten som helhet er strukturert av større tankemønstre (s. 42). Grønmo gir flere eksempler som en kan få innsikt i, men av betydning for vår oppgave står verdier og holdninger særlig sentralt

(s. 142). Det er verdt å understreke at Grønmo tar utgangspunkt i en bestemt form for dokumentanalyse, som derfor avviker noe fra vår. Som Thagaard (2018, s. 120) påpeker får en i studier av samtaler i et diskursanalytisk perspektiv innsikt i hvordan personer forstår sin virkelighet gjennom måten de ordlegger seg på. Det er verdt å legge til at en i hovedsak skiller mellom to tilnærminger til diskursanalyser: lingvistiske analyser og analyser i samfunnsvitenskapelig forstand (Østbye, Helland, Knapskog, Larsen, & Moe, 2013, s. 93). I førstnevnte utgjør selve teksten det sentrale forskningsobjektet, mens i en samfunnsvitenskapelig analyse, i tråd med vår metode, rettes fokus mot samfunnsmessige kontekster og maktspørsmål. I vår oppgave er det med andre ord ikke selve teksten som analyseres. De to tilnærmingene har imidlertid en felles interesse for forholdet mellom språk og samfunn, og språk, som er styrende for oppfatning av den sosiale virkeligheten (Østbye et al., 2013, ss. 93-94).

Diskursanalyser tar utgangspunkt i at virkeligheten kommuniseres gjennom språk, hvor virkeligheten kan forstås gjennom anvendte begrep og tenkemåter (Østbye et al., 2013, s. 94). Østbye et al. (2013, s. 94) påpeker videre at språk, gjennom begrep, språklige ferdigheter og mentale modeller, er betinget av den sosiale konteksten det omgis i. Videre benyttes diskursanalyser for å etablere helhetsforståelse av både meningsytringer og kommunikasjonsprosesser (Grønmo, s. 282). Begrep, tenkemåter og helhetsforståelse av meningsytringer kan forstås som særlig sentralt i vår analyse. Språklige ferdigheter, mentale modeller og kommunikasjonsprosesser er derimot ikke like aktuelt. Det er med andre ord forhold som både samsvarer og avviker, men poenget er at noen sentrale egenskaper er å kjenne igjen i vårt studie.

4.2.3 Farget av forstående studier som hermeneutikk

Hermeneutikk og fenomenologi er hovedtilnærminger i det som omtales som forstående eller fortolkende studier (Grønmo, 2004, s. 391). Hensikten med forstående studier er å utvikle en mer helhetlig forståelse av forhold som gjør det mulig å belyse hvilken mening og betydning som knyttes til handlinger og hendelser i samfunnet (s. 391). Ifølge Grønmo skiller hermeneutikk seg fra fenomenologi da førstnevnte i større grad vektlegger helhetlig forståelse. Fenomenologi legger på sin side hovedvekt i meningsfortolkning. Grønmo påpeker imidlertid at skillet mellom de to tilnærmingene ikke er særlig skarpt og at samtlige forstående studier inkluderer begge element (s. 392). Det er imidlertid en helhetlig forståelse som er av størst

betydning i vår metodiske fremgangsmåte. Med det til grunn ser vi derfor litt nærmere på en hermeneutisk tilnærming.

Ifølge Thagaard vektlegger en hermeneutisk tilnærming at det ikke finnes en faktisk sannhet og at tolkning av fenomener vil være avhengig av flere nivå (Thagaard, s. 37). Den sosiale konteksten som Østbye et al. (2013) påpeker, samsvarer med et sentralt utgangspunkt i hermeneutikken. Ifølge Thagaard (2018, s. 37) er prinsippet om at mening utelukkende kan forstås i lys av den sammenheng det vi studerer befinner seg i grunnleggende i hermeneutisk forskningslogikk (s. 37). En helhetlig forståelse, som adresseres både innledningsvis her og i lys av diskursanalyse er derfor svært sentral. Forhold som studeres i vårt studie, utgjør en del av noe større hele og må derfor ses i lys av det.

Fra et samfunnsvitenskapelig ståsted, tilsvarende vårt, kan et hermeneutisk perspektiv knyttes til det å ”lese” kultur som tekst (Thagaard, 2018, s. 37). Formålet er ifølge Thagaard å oppnå en gyldig forståelse av meningen i teksten. Vår tilnærming til dokumentanalyse kan dog ikke forstås som å ”lese” kultur som tekst. I oppgaven studerer vi ikke kultur, men heller forhold som synliggjør hvordan begrep knyttet til kultur kommuniseres.

Ifølge Hans Gadamer (1997, i Bukve, 2016, s. 68) er menneske i kontinuerlig dialog med omverdenen for å forstå og tolke den. Gadamer ser derfor menneske som aktivt meningsskapende. Ricæur (i Bukve, 2016, s. 69) er hermeneutikk primært en metode for teksttolkning, og i tråd med hans syn, er råstoffet for moderne hermeneutisk analyse ofte oppfattet som en tekst (Bukve, 2016, s. 69). Tekster kan være verbale ytringer fra en eller flere personer, men kan også være beskrivelser av handlinger, fenomen eller sammenhenger.

Uten å gå i detalj, skilles den hermeneutiske logikken mellom tre måter å tolke tekst (Bukve, 2016, ss. 70-71). Felles for tolkningene er vekslingen mellom tolkning av enkeltelement i analysen og omvurdering av den forståelsesrammen eller sammenhengen som elementet inngår i. Prinsippet er at hver ytring eller hvert enkelt tekstelement blir tolket som en del av en helhet. I forskningsprosessen veksler en mellom å konstruere en helhetlig forståelse som samsvarer med det enkeltelementet

som en tolker, og finne ut om nye enkeltelementer kan tolkes ut fra den kontekstforståelse en har (Bukve, 2016, s. 71). Bukve beskriver prosessen ved en hjelp av en puslebrikke:

> (…) på den eine sida held opp ein puslespelbit og prøver å tenke seg kva bilde som vil komme til synes når heile puslespelet er lagt, eller at ein sit med eit nesten ferdig puslespel og blir i tvil om den siste biten som ein har plukka opp eigenleg høyrer til i dette spelet.
>
> (Bukve, 2016, ss. 71-72)

Som følge av oppgavens teorigrunnlag om kultur og sosialkonstruktivisme, samt maktforhold i og av tekst, ser vi i likhet med Gedamer på mennesket som aktivt meningsskapende. De gjennomgåtte dokumenter forstås som uttrykk for hvordan mennesker fortolker og forholder seg til verden, og summen av all dokument-produksjon og samhandling kan sies å være med på å produsere *sannheten* om fenomener. Hvert enkelt dokument ble tolket som en del av en større enhet, og ble analysert i henhold til dets kontekst og vårt teorigrunnlag. Dette henger også tett sammen med sosialkonstruktivisme og inspirasjonen vi har trukket fra grounded theory og diskursanalyse. Siktemålet var å skape en helhetlig forståelse om hvordan tekstproduksjon om fenomenet sikkerhetskultur i en digital kontekst bidrar til arbeidet med nevnte fenomen, og mulig hvordan tekster kan representere underliggende kulturelt betingede holdninger og verdier.

4.2.4 Grunnlag for fortolkning i dokumentanalysen

Det kan, ifølge litteraturviteren Atle Kittang, skilles mellom tre hovedmåter å tolke eller lese tekster på. Disse tre hovedmåtene er: sympatisk, objektiverende og symptomal lesemåte (Østbye et al., 2013, s. 76). Kort oppsummert handler sympatisk lesemåte om å søke etter opphavsforfatterens intensjoner, og her fremheves forfatteren som sentral for å forstå tekstens mening. Objektiverende lesemåten fokuserer på å tolke teksten isolert fra opphavsforfatteren og sosial kontekst (Østbye et al., 2013, s. 76). Den symptomale lesemåten ser på sin side på teksten som et manifest utrykk for underliggende eller skjulte betydninger, og tilnærmingen fokuserer på at tekster er formidlere av betydninger som er av opphavsforfatteren produsert ubevisst (Østbye et al., 2013, s. 76). Denne oppgaven kan sies å ha en

fortolkningsmåte basert på ovennevnte symptomal lesemåte, og det blir derfor gitt en en grundigere innføring i hva dette gjelder og hvilken relevans det har for oppgaven.

Den symptomale tilnærmingen om at tekster er formidlere av betydninger som er ubevisste for forfatteren, kan ha flere forklaringsfaktorer. Normer og forestillinger i den aktuelle settingen, gruppen eller tiden kan være så dominerende eller selvsagte at de fortoner seg som naturlige og allmenngyldige (Østbye et al., 2013, s. 76). Tekstene kan også inneha latente sosiale motsetninger eller konflikter (Østbye et al., 2013, s. 76). Målet med en symptomal lesemåte kan være å rette lys mot disse motsetningene, avdekke de og diskutere deres samfunnsmessige grunnlag. Teksten som analyseres kan være et utgangspunkt for å se på skjulte betydninger eller meningsbærere som ikke umiddelbart er tilgjengelig for leseren (Østbye et al., 2013, s 76).

I denne forbindelse, der oppgaven analyserer en rekke dokumenter, er det med hensikt å forstå tekstens samfunnsmessige kontekst. Det er den sammenhengene tekstene inngår i som er av relevans. Det teoretiske grunnlaget legger også føringer på fortolkningsmåten. Spesielt Foucaults posisjon og perspektiver på hvordan diskurs påvirker utviklingen av samfunn kan trekkes mot en symptomal lesemåte. I henhold til Foucault produseres ”sannheten” gjennom diskurser, strategier, praksis og institusjoner. Det er derfor hensiktsmessig å se på tekster som meningsbærende og en representasjon av hvordan verden blir forstått. Teorigrunnlaget presenterer også at diskurser, holdninger og normer være så dominerende at de fremstår som allmenngyldige og naturlige. Tekster kan derfor sees på å være et symptom på underliggende holdninger og kultur i sin samfunnsmessige kontekst. Tekstene blir fortolket i lys av teorigrunnlaget, og dette gir grunnlag til å være på utkikk etter underliggende kulturelt betingede meninger som ikke tydelig presenteres i teksten.

4.3 Utvikling av oppgavens forskningsspørsmål

I den innledende fasen av arbeidet med masteroppgaven utviklet vi en skisse for oppgaven. Grovt skissert vektla skissen informasjonssikkerhet og sikkerhetskultur i små og mellomstore virksomheter. I henhold til skissen skulle vi skrive en masteroppgaven som tok sikte på å utvikle et verktøy i digitaliseringsprosesser. Skissen resulterte i tre mindre studier, knyttet til informasjonssikkerhet og sikkerhetskultur, som gis en kort oppsummering av i kapittel 4.7. Arbeidet vi la ned i

det som vi omtaler som oppgavens forstudier, la imidlertid føringer for at masteroppgaven tok en annen vending en først tiltenkt. Parallelt med utførelsen av forstudiene holdt vi en løpende dialog med vår samarbeidspartner, KPMG. Funnene i forstudien og dialog med KPMG synliggjorde konturer av det som kan betraktes som en form for umodenhet i norsk sikkerhetstenkning relatert til informasjonssikkerhet. Sammen la funn og møtevirksomhet føringer for at problemstillingen og forskningsspørsmålene i oppgaven skulle kobles til norsk sikkerhetstenking med hensyn til informasjonssikkerhet. I påfølgende tre punkter presenteres områder som vi på bakgrunn av overnevnte forhold anså som aktuelle å se nærmere på:

1. *Begrepsavklaringer.* Definisjoner og språkbruk i offentlige tilgjengelige dokumenter, som utredninger, lovverk og rapporter – bidrar de til gode retningslinjer eller forvirring?

2. *Rollefordeling- og ansvar.* Hvem som har ansvaret for sikkerhet og gjennomføring av tiltak på tvers av organisasjoner og sektorer fremstår som uoversiktlig. Hvordan offentlige utredninger og Stortingsmeldinger presenterer ansvarsroller, samt inndelingen av tilsynsmyndighet, vil ha en innvirkning på informasjonssikkerhet. Rollefordeling innad i virksomheter er også av betydning, og hva virksomheter og organisasjoner må forholde seg til.

3. *Forståelse, kompetanse, tillit og kultur på sikkerhetstenkning med hensyn til informasjonssikkerhet.* Forståelse av informasjonssikkerhet og informasjonssystemer vil ha en innvirkning på arbeidet med sikkerhet. Manglende kunnskap, opplæring, kompetanse og forståelse av hendelsesforløp er sentrale komponenter. Digitaliseringstakt og tillit vil også inngå innunder denne bolken.

Som det fremkommer i kapittel 2, Systembeskrivelse, er oppgavens tema preget av forhold i stadig endring, og som involverer en rekke ulike aktører på tvers av ulike fagfelt. Områdene som trekkes frem er derfor av et omfang som i sin helhet ikke vil kunne adresseres i én masteroppgave. I tråd med oppgavens opprinnelige skisse, var det imidlertid ønskelig å beholde sikkerhetskultur som tema i oppgaven. Videre har et formål og en sterk prioritet i forskningsprosessen vært at studien får betydning for

mer enn vår egen avslutning på mastergraden. Sikkerhetsteori, våre ønsker og målsetninger har vært bestemmende for oppgavens innhold og karakter. Forskningsprosessen ledet oss dermed til spørsmål knyttet til hvordan sikkerhetskultur kommuniseres, og hvordan det virker inn på arbeidet med sikkerhetskultur i en digital kontekst. Forskningsspørsmålene presenteres innledningsvis i oppgaven, men gjentas her for ryddighetens skyld:

1. *Hvordan formidles og anvendes sikkerhetskultur i offentlig tilgjengelige dokumenter av betydning for digital sikkerhet?*

2. *Hvordan påvirker dokumenter utgitt av nasjonale aktører arbeidet med sikkerhetskultur i en digital kontekst?*

Forskningsspørsmålene ble i hovedsak utviklet med formål om å avdekke elementer som faller innenfor de første to områdene som presenteres. Funnene i studien har imidlertid i stor grad også berørt det tredje området, som understreker kompleksiteten i feltet vi befinner oss i. Det har imidlertid vært nødvendig å gjøre noe avgrensninger, men som beskrives nærmere i oppgavens innledning i kapittel 1.3.

4.4 Gjennomføring av metode

Innsamling av data er innarbeidet i beskrivelser av både kvalitative og kvantitative metoder og refererer til data som benyttes i forskningsprosessen (Thagaard, 2018, s. 28). Thagaard (2018) utfordrer begrepet *innsamling av data* og forholder seg heller til begrepet *utvikling av data* i forbindelse med kvalitativ forskning. Thagaard argumenterer med at tolkning av tekster og visuelle uttrykksformer vil prege datagrunnlaget en besitter. Forskerens forståelse av virkeligheten en studerer vil virke inn på datagrunnlaget, og dermed kan *utvikling av data* betraktes som et mer korrekt begrep (s. 28).

I tråd med beskrivelser av vår fremgangsmåte som fremkommer i kapittel 4.4, var oppstarten preget et vidt og åpent søk. Oppgavens tema om forståelse av sikkerhetskultur i digital konktest, utgjorde midlertid en naturlig innramming. Den trykkende informasjonsstrømmen på området la videre føringer for å utelukkende utvikle empirisk data basert på nyere kilder. Overnevnte forhold og sentrale begreper i

problemstilling og forskningsspørsmål utgjorde i hovedsak søkekriteriene som lå til grunn for oppgavens utvelgelse av dokumenter. Sentrale stikkord i søk er: sikkerhetskultur, digital sikkerhet, informasjonssikkerhet, sikkerhetsbevissthet, digital sikkerhetskultur, digital kompetanse og sikkerhet i Norge.

Søket kan betegnes som en strategisk utvelgelse, basert på systematiske vurderinger av hvilke enheter som ut fra teoretiske og analytiske formål er mest relevante og mest interessante (Grønmo, 2004, s. 102). Strategiske vurderinger underveis i studien kan lede til revurderinger av hvilke enheter som skal inkluderes i utvalget, noe som forutsetter en fleksibel utvelging av enheter (Grønmo, 2004, s. 103).

Av praktiske og ressursmessige årsaker har en strategisk utvelgelse av dokumenter vært en naturlig utvalgsform. Med en kompleksiteten knyttet til oppgavens tema, som følge av utviklingstakt og aktørnettverk, har det vært en prioritet og inkludere for mange dokumenter. Som Grønmo (2004, s. 105) skriver:

> Jo flere enheter som inngår i studien, desto mindre informasjon om hver enhet er det mulig å håndtere. Jo mer informasjon som samles inn om hver enhet, desto færre enheter er det mulig å ta med.
>
> (s. 105).

Dette synliggjør hvorfor og hvordan gjennomføringen har vært preget aktiviteter med vekslende fokus og parallelle løp. Det var i oppstartsfasen av studien ingen forhåndsbestemmelser angående datamaterialet med tanke på antall enheter og omfang. Utviklingen av data har dermed seg selv vært bestemmende oppgavens innhold. Videre har møtevirksomhet med veiledere i KPMG og andre representanter for sentrale aktører i sikkerhets-Norge spilt en betydningsfull rolle for utvelgelsen.

Av hensyn til kildekritiske vurderinger har vi forholdt oss til en fremgangsmåte presentert av Thagaard (2018, s. 119). Fremgangsmåten er presentert i lys av analyser av dokumenter som kilde om saksforhold, men er bygget opp av element av stor relevans for vår oppgave. I første omgang en vurdering av enhetens relevans for oppgavens problemstilling. Videre foretok vi en vurdering av enheten eller dokumentets potensiale med tanke på utbytte i form av hvilken informasjon vi kunne

hente ut. Vurderinger av datamaterialets autentisert og troverdighet har ikke vært av særlig omfattende karakter. Empirisk datagrunnlag er utelukkende basert på dokumenter av tilgjengelighet for det offentlige utarbeidet av norsk aktører og institusjoner med sikkerhetsinteresser på et nasjonalt nivå. Det har dermed ikke vært særlig grad til å tvile på verken troverdighet eller formål. Spørsmål relatert til hvorvidt materiale er ekte har derfor heller ikke vært av betydning. Kildekritiske vurderinger knyttet til oppgaven i sin helhet adresseres i kapittel 4.6 Oppgavens kvalitetsvurderinger.

Analyseringen av innholdet har som nevnt foregått parallelt med utviklingen av data. Som presisert i kapittel 4.2 Oppgavens dokumentanalyse, har vi i analysen studert hvordan språk, definisjoner og tekster kan legge føringer for arbeid med sikkerhet. I henhold til oppgavens teorigrunnlag kan overnevnte forhold være bestemmende for risikoforståelse og virkelighetsoppfatning. Fokus har dermed vært rettet mot aktørers makt, i form av definisjonsmakt, men også i form av makt i respektives tekster. I likhet med utgangspunktet for diskursanalyser har det derfor vært ønskelig å studere hva og hvilke som oppfatninger som kommuniseres i oppgavens datagrunnlag. Vi understreker at metoden utelukkende er en dokumentanalyse, men at særlig analysering av innholdet i dokumentene er i tråd med sentrale trekk i en diskursanalyse.

4.5 Empirisk datagrunnlag

I dette kapittelet presenteres dokumenter som utgjør grunnlaget for oppgavens empiri. Dokumentene vil sammen med andre kilder i oppgaven presenteres i sin helhet i oppgavens litteraturliste i kapittel 8.

4.5.1 Norges offentlige utredninger

- *NOU 2015:13 Digital sårbarhet – sikkert samfunn*
- *NOU 2018:14 IKT-sikkerhet i alle ledd*

4.5.2 Stortingsmeldinger

- Meld. St. 10 (2016-2017) *Risiko i et trygt samfunn. Samfunnssikkerhet* (JD, 2016)
- Meld. St. 38 (2016-2017) *IKT-sikkerhet. Et felles ansvar* (JD, 2016)

4.5.3 Rapporter

- *Trusler og trender 2016-17* (NorSIS, 2016)
- *Trusler og trender 2017-18* (NorSIS, 2017)
- *Trusler og trender 2018-19* (NorSIS, 2018)
- *The Norwegian Cyber Security Culture* (Malmedal & Røislien, 2016)
- *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017)
- *Nasjonal strategi for digital sikkerhet* (Departementene, 2019)
- *Nordmenn og digital sikkerhetskultur 2017* (NorSIS, 2017)
- *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018)
- *Informasjonssikkerhetskultur.* Oppsummerende rapport fra sikkerhetstoppmøtet 20.04.2016. (NorSIS, 2016)
- *Risiko 2016* (NSM, 2016)
- *Risiko 2017* (NSM, 2017)
- *Risiko 2018* (NSM, 2018)
- *Risiko 2019* (NSM, 2019)
- *Helhetlig IKT-risikobilde 2015* (NSM, 2015)
- *Helhetlig IKT-risikobilde 2016* (NSM, 2016)
- *Helhetlig IKT-risikobilde 2017* (NSM, 2017)
- *Et sikkert digitalt Norge - IKT-risikobilde 2018* (NSM, 2018)
- *Statsbudsjettet* (Finansdepartementet, 2018)
- *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen 5.3)* (Normen, 2018)
- *Årsrapport for 2018* (Datatilsynet, 2018)
- *Mørketallsundersøkelsen 2016* (NSR, 2016)
- *Mørketallsundersøkelsen 2018* (NSR, 2018)
- *ForBedring - kartlegging av sikkerhetskultur i spesialhelsetjenesten* (Nasjonalt pasientsikkerhetprogram, 2017)
- *The ISACA/CMMI Institute Cybersecurity Culture Report* (ISACA & CMMI, 2018)

4.5.4 Nyhets- og leserinnlegg

I tilfeller hvor nyhetsartikler eller leserinnlegg er aktuelt blir dette påpekt i teksten. Denne typen dokument anses som relevant da de kan gi indikasjoner på hvordan næringslivet forholder seg til sikkerhetskultur. Hvordan arbeidet med sikkerhetskultur

presenteres og diskuteres kan belyse ulike forståelser av sikkerhetskultur. Videre kan denne typen dokumenter aktualisere tema ved å gi eksempler aktuelle utfordringer.

4.6 Oppgavens kvalitetsvurderinger

Vurderinger av foreliggende teksters kvalitet er en vesentlig faktor i studien. I dette kapittelet presenteres utfordringer og sentrale forhold knyttet kildekritiske vurderinger.

4.6.1 Reliabilitet og validitet

Reliabilitet kan knyttes til spørsmålet om hvorvidt kritiske vurderinger av prosjektet viser at forskningen er utført på en måte som er pålitelighet og tillitsvekkende. Vurdering av reliabilitet fremheves av Marshall & Rossman (i Thagaard, 2018, s. 187), sammen med troverdighet, som kriterium for at forskning skal kunne betraktes som utført på en slik måte. Thagaard (s. 119) trekker frem at kilder må vurderes i henhold til konteksten de er skapt i.

Betydningen av reliabilitet i et kvalitativt studie er av en annen karakter enn i et kvantitativt studie. I kvantitive studier skal det tilrettelegges for at prosjektet skal kunne reproduseres og gi de samme resultatene (repliserbarhet) (Thagaard, 2018, s. 187). I nyere forskning, hvor interaksjonistiske og konstruktivistiske perspektiver er mer dominerende enn tidligere, er ikke repliserbarhet betraktet som et kriterium i syn på kvalitative metoder (Thagaard, 2018, s. 187). I praksis vil det ofte heller ikke være mulig å gjennomføre gjentatte innsamlinger av data om de samme fenomenene. Blant annet kan skyldes dette at samfunnsmessige fenomener er i stadig endring, som er aktuelt for vårt studie. Videre kan undersøkelsesopplegget kan være for komplekst eller for fleksibelt til at datainnsamlingen kan gjentas på nøyaktig samme måte (Grønmo, 2004, s. 240). Gitt oppgavens kontekst, kan oppgaven dermed beskrive som lite repliserbar. Fenomener som diskuteres i denne oppgaven er gitt en kontekst i stadig endring. Den konteksten en beskriver i dag, kan være av en helt annen karakter i morgen.

Studiens forskningsdesign bærer er preget av at aktiviteter i fremgangsmåten foregår parallelt. I løpet av prosessen med utvikling av data har vi gjennom møtevirksomhet mottatt innspill og forslag til dokumenter som kunne være av relevans.

Fremgangsmåten i oppgaven kan dermed ikke beskrives som en systematisk prosess som var planlagt i forkant av utføringen av dokumentanalysen.

Som følge av overnevnte forhold har en omfattende metodisk presentasjon vært prioritert. Det gis derfor en omfattende beskrivelse av hva hvilke teorier og tilnærminger som ligger til grunn for gjennomføringen av oppgavens dokumentanalyse. Aktivitetene som inngår er videre beskrevet slik at leseren kan få en forståelse for hvordan prosessen i studien. Metodekapittelets omfattende omfang gjenspeiler vårt ønske om transparens og troverdighet. Ifølge Thagaard (2018, s. 188) kan også reliabiliteten styrkes ved at det er flere forskere involvert i forskningsprosjektet, enten i form av samarbeid eller at andre blir bedt om å gjøre en kritisk evaluering av arbeidet. Denne oppgaven er et resultat av et samarbeid mellom to studenter, under veiledning av andre. Videre er alle inkluderte dokumenter og tekstbidrag oppgitt med referanser for å bidra til økt reliabilitet.

Validitet kan forstås som datamaterialets gyldighet overfor problemstilling og forskningsspørsmål som skal belyses. Validiteten er høy dersom undersøkelsesopplegget og datainnsamlingen resulterer i data som er relevant for problemstillingen (Grønmo, 2004, s. 241). Validiteten er dermed et uttrykk for hvor godt datamaterialet svarer til forskerens intensjoner. Validiteten er lav dersom undersøkelsesopplegget er lite treffende for problemstillingen. Validitet er først og fremst relatert til utvelgingen av enheter og informasjonstyper (Grønmo, 2004, s. 242).

Vi omtaler gjerne oppgavens empirigrunnlag som foreliggende tekster. Studier av foreliggende tekster skiller seg fra andre typer studier, da tekstene ikke er utviklet med formål om å bli analysert. Faktumet at studien baseres på foreliggende tekster kan dermed anses som en styrke med tanke på både validitet og reliabilitet. Faktumet at vi selv ikke har utarbeidet teksten sløyfer et ledd i prosessen for utvikling av data. Vår kompetanse og forståelse vil naturligvis påvirke prosessen, men da ikke før vi selv leser og analyserer tekstene. De foreliggende tekstene formidler aktørers meninger og holdninger til bestemte fenomen, uten påvirkning fra oss som forskere. Det er verdt å påpeke at vi kan oppfatte de foreliggende tekstene som noe som avviker fra opphavsforfatterens intensjon. Det er videre verdt å trekke frem at vi i noen

tilfeller har inkludert data som ikke direkte bører sikkerhetskultur og digital informasjonssikkerhet. Dette er gjort med hensikt om å gi en innsikt i hvordan konsepter og begreper benyttes, nevnes og undersøkes forskjellig.

4.6.2 Styrker og svakheter

Vi er klar over at vår kontekstuelle forståelse og kildekritiske vurderinger er av betydning for studiens resultater. Oppgavens forskningsdesign legger til rette for at kan reaktivitet unngås. Kildene blir ikke påvirket under selve utviklingen da tekstene ikke endres som følge av analysen. Et problem kan imidlertid være at forskerens perspektiv kan påvirke utvelgelsen av tekster og påfølgende tolkning (Grønmo, 2004, s. 180). Et snevert perspektiv kan bidra til at utvalget av tekster blir skjevt, og at tolkningen blir ensidig. Tekster som kunne vært eller kan bidratt til at problemstillingen belyses kan overses fordi innholdet ikke passer inn i forskerens perspektiv (Grønmo, 2004, s. 180). Tolkningsmuligheter som er viktige eller interessante, blir mulig ikke oppdaget eller drøftet som følge av at det ikke samsvarer med forskerens perspektiv.

En annen utfordring under utvikling av data kan være at forskerens kildekritiske forståelse er for begrenset, og som kan være av betydning for tolkningen (Grønmo, 2004, ss. 180-181). Slike problemer kan forebygges ved at ulike tekster vurderes i forhold til hverandre, og ved at tekstene vurderes i lys av andre kilder og foreliggende kunnskap. Tolkning av tekstene kan videre bli påvirket av forskerens kontekstuelle forståelse. Innholdet kan bli feilaktig tolket, fordi det ikke er vurdert tilstrekkelig hvem teksten er representativ for eller hvilken betydning teksten har (Grønmo, 2004, s. 181).

Hermetikken vektlegger særlig forskerens rolle. Sosiale og kulturelle erfaringer blir tatt med inn i enhver analyse, noe som kalles fordommer eller forforståelse i hermeneutikken. Analytiker eller forsker kan ikke fristilles fullstendig fra disse. I denne oppgaven er det heller ikke ønskelig å fristille seg helt fra forforståelse, da vår faglige bakgrunn og oppfatninger har vært førende for forskningsprosessen. Ifølge Østbye et al. (2013, s. 66) er det også i dette møtet mellom forforståelse og tekster fortolkningen foregår.

Hermeneutisk selvrefleksjon omhandler forskerens refleksjon over seg selv og sine fordommer i analysen. Denne prosessen, i en hermeneutisk tradisjon, blir beskrevet som et arbeid som skal kunne gi økt selvinnsikt. I hermeneutikken handler det om at tekstanalysen skal gi ny kunnskap om teksten, men også økt kunnskap om seg selv (Østbye et al., 2013, s. 67). Det handler også om å plassere forskeren eller analytikeren i en større sammenheng, sosialt, kulturelt og historisk (Østbye et al., 2013, s. 67). Selvrefleksjon som sådan, med sikte om økt personlig innsikt, er mulig ikke av størst relevans for denne oppgaven. Det trekkes imidlertid inspirasjon fra hermeneutiske selvrefleksjonen for å reflektere rundt noen av antagelsene og forutsetningene som ligger til grunn.

Med ovennevnte utfordringer til grunn, er det verdt å påpeke at vårt perspektiv og vår fagbakgrunn har influert teorigrunnlaget og problemstillingen. Utdanning og perspektiv på sikkerhet og annet teorigrunnlag vil også farge vårt syn på utvelgelsen av tekster og tolkningen av disse. I lys av oppgavens teori om sosialkonstruktivisme, vil også hvordan vi oppfatter verden være konstruert av våre erfaringer, oppfatninger, interaksjoner og samhandling. Eksempelvis vil vår forståelse av verden i stor grad være basert og influert av de aktører og institusjoner som nettopp denne oppgaven tar for seg. Formidlede tekster oppfattes dermed av oss som autentiske, og det som presenteres av disse aktøren oppfattes i stor grad som ”sant”. Dette kan nærmest forstås som en målefeil i metoden. Utvalget kan derfor være begrenset som følge av vår oppfattelse av hvem som er legitime maktutøver. Tekstene formidler imidlertid likevel aktørenes forståelse av sikkerhetskultur, uavhengig vår oppfatning av aktørene og institusjoner.

I lys av grounded theory, diskursanalyse og hermeneutisk forskningslogikk, har vi forsøkt å vurdere tekstene mot hverandre, mot foreliggende kunnskap om temaet, og i lys av sin kontekst. Lokale forhold er bestemmende bestemmende for kultur, organisasjonskultur og sikkerhetskultur. Det er av den grunn vært hensiktsmessig å benytte seg av kilder som beskriver forholdene i Norge, med norske opphavsforfattere. Videre har en fremgangsmåte preget av parallelle aktiviteter resultert i at utvelgelsen i mindre grad har vært styrt av egne antakelser. Videre gir, ifølge Thagaard (2018, s. 11), analyser av visuelle og digitale uttrykksformer oss en forståelse av karakteristiske trekk for vår kultur, som i seg selv berører oppgavens

tema og problemstilling. Et valg av en dokumentanalyse som metode anses derfor som hensiktsmessig for å besvare problemstillingen.

Tross en avgrenset problemstilling, er konteksten preget omfattende informasjonsstrøm og dokumentproduksjon som krever forhåndsbestemte avgrensninger av datagrunnlag. Vi har med det til grunn forholdt oss til dokumenter utgitt i perioden 2015-2019. Dette begrenser naturligvis oppgaven, men har vært nødvendig med hensyn til oppgaven tidsramme. Faktumet at vi utelukkende har basert studien på offentlig tilgjengelige dokumenter har imidlertid gjort det mulig å komme tidlig i gang med dokumentanalysen. Det store antallet dokumenter gjør det imidlertid ikke mulig å gå gjennom samtlige dokumenter i sin helhet. Det kan være en svakhet, men dersom vi har lykkes i å fange opp det som er relevant for vår problemstilling er det heller en styrke at vi inkludert et så stort antall. Det er imidlertid ingen garanti for at vi har fanget opp alt som vil ha en potensiell betydning for oppgavens problemstilling. Utvelgelsen av dokumenter kan forstås som noe ensidig, men som følge av oppgavens problemstilling har dette vært nødvendig.

Vi er videre oppmerksomme på vår bruk av sekundærkilder i oppgaven. Oppgavens rammer, som innebærer norske forhold, har lagt føringer for å oppsøke litteratur deretter. I de tilfeller hvor det har vært mulig og hensiktsmessig å oppsøke primærkilder har vi gjort dette. Ved innhenting av litteratur av betydning for oppgavens metode har vi bevisst valgt å forholde oss til norske forfattere. I metodisk sammenheng fant vi det lite hensiktsmessig å oppsøke primærkilden, og som dermed resulterer i bruk av sekundærkilder. I forbindelse med metode, og i andre tilfeller hvor sekundærkilder benyttes, har kildenes kontekst vært avgjørende. Konteksten er dermed gitt av (vår) primærkilde, og utsnittet må sees i lys av denne konteksten.

4.6.3 Etiske vurderinger

Forskning er av stor betydning, både for enkeltmennesker, for samfunnet og global utvikling. Forskning er også en betydelig maktfaktor på alle disse nivåene. Av begge grunner er det vesentlig at forskning foregår på måter som er etisk forsvarlige (De nasjonale forskningsetiske komiteene, 2009). De nasjonale forskningsetiske

komiteene (2016) lister opp fire prinsipper som gjelder for all forskning: respekt, gode konsekvenser, rettferdighet og integritet.

Thagaard (2018, s. 20) skriver at all vitenskapelig forskning krever at forskere forholder seg til etiske prinsipper, både internt i forskningsmiljøer og i relasjon til andre. Hun trekker spesielt frem redelighet og nøyaktighet i hvordan forskningsresultatene blir presentert, og hvordan andres arbeid kilderefereres. Et grunnleggende prinsipp er å unngå plagiat, noe som anses som uakseptabelt og et alvorlig brudd på etiske standarder (Thagaard, 2018, ss. 20-21). I denne oppgaven har det vært særlig relevant med god henvisningsskikk og å skille mellom vårt arbeid og arbeidet til andre. Dette vises blant annet i kapittel 5, Resultat, der datagrunnlaget blir presentert for hvert enkelt kapittel. Også kapittel 4.5, Empirisk datagrunnlag, ble utformet med sikte på å tydelig vise hvor datamaterialet ble hentet fra. Alle referanser som er brukt i oppgaven er referert i sin helhet i kapittel 8.

Da det ikke benyttes intervju eller andre metoder som er av betydning for personopplysninger vil ikke hensynet til konfidensialitet (av personopplysninger) være av særlig betydning. Når det er sagt, har vi vært i mange samtaler med dyktige personer som velvillig har gitt oss innblikk i temaet. Vi har valgt å ikke navngi spesifikke personer eller organisasjoner, til tross for at disse personene har gitt oss nyttig informasjon i form av forslag til data. Unntaket er våre veiledere i KPMG.

I den grad rapporter og dokumenter kritiseres, er det viktig å poengtere at kritikken ikke er rettet mot enkeltpersoner. Kritikken tar utgangspunkt i det som presenteres i rapportene, uavhengig tekstforfatter. Dette blir gjort med hensikt om å belyse de forskjeller og inkonsekvente benyttelsene av begreper og tilhørende beskrivelser. Informasjonen som presenteres i oppgaven er funnet i offentlig tilgjengelig dokumenter, og kan ikke beskrives som verken sensitiv eller konfidensiell informasjon. Det har derfor ikke vært aktuelt å søke om særlige tillatelser. Ved å søke etter offentlig tilgjengelig informasjon, har det heller vært aktuelt med kildekritiske vurderinger og god henvisningsskikk.

4.7 Oppsummering av forstudier

Som referert til tidligere, utførte vi i en tidlig fase av arbeidet med masteroppgaven tre mindre studier knyttet til oppgavens tema. Studiene betraktes og beskrives som forstudier i masteroppgaven. I dette kapittelet presenteres forstudiene og funn som har vært styrende for utviklingen av studiens problemstilling og forskningsspørsmål. Ytterligere informasjon og data knyttet til studiene er vedlagt i Vedlegg B, C og D.

4.7.1 Studie av begrepet informasjonssikkerhet

I et møte med våre veiledere i KPMG ble vi opplyst om at respektive i liten grad vektlegger KIT i sitt arbeid. Fokus på KIT er ikke like vektlagt som tidligere, og det blir i større grad fokusert på andre aspekt. Deres ståsted og holdning til sikkerhetsmålene som inngår i den tradisjonelle definisjonen av informasjonssikkerhet skapte grobunn for å se nærmere på verdien av å forholde seg til KIT.

Når og hvordan definisjonen av informasjonssikkerhet og konseptet KIT oppstod er uklart, men tolkningen har blitt adresseres i rapporter og artikler publisert flere tiår tilbake. Poenget er å understreke det faktum at definisjonen av begrepet nærmest har stått uendret over en tidsperiode preget av et digitalt skifte. Utfordringene relatert til sikring av informasjon er definitivt av en annen karakter i dag enn for bare tiår tilbake. Det kan dermed stilles spørsmål til hvorvidt det er hensiktsmessig å forholde seg til KIT med tanke på de digitale utfordringene virksomheter står overfor i dag. Vi gjennomgikk *Defining Information Security*, av Bjørn Lundgren og Niklas Möller (2017), som i sin publikasjon studerer den tradisjonelle forståelsen av informasjonssikkerhet, herunder begrepene KIT. De argumenterer for at definisjonen er for vid, men samtidig for smal, til å korrekt adressere problematikken informasjonssikkerhet- og systemer står ovenfor i dag.

Lundgren og Möller (2017) definerer KIT som ”insecure states as secure and secure states as insecure” (Lundgren & Möller, 2017, s. 4), som de da hevder bidrar til at definisjonen blir både for vid og smal. I enkelte standarder, lovverk, veiledere vektlegges ytterligere egenskaper som sporbarhet, ikke-fornekting og autentisitet lagt til (Lundgren & Möller, 2017, s. 4). Fra forfatternes perspektiv er imidlertid en

inkludering av ovennevnte egenskaper ikke tilstrekkelig, da heller ikke de kan bidra til å fange opp samtlige informasjonssikkerhetutfordringer.

Lundgren og Möllers (2017, s. 21) foreslår å se bort fra KIT og ikke lenger vektlegge sikkerhetsmålene i definisjon av informasjonssikkerhet. De foreslår en alternativ definisjon av informasjonssikkerhet som tar utgangspunkt i at sikkerhet er en relativt størrelse. Ifølge forfatterne vil forståelse og oppfatning av sikkerhet være relativ til interessentens tolkning. Motsetningen vil dermed være at informasjonssikkerhet- og systemer er sikre uavhengig interessent (Lundgren & Möller, 2017). Forfatterne betrakter en dimensjon av informasjonssikkerhet som ikke fremkommer i den tradisjonelle definisjonen av informasjonssikkerhet. I henhold til den tradisjonelle forståelsen, er informasjon sikre uavhengig av interessent, så lenge sikkerhetsmålene KIT oppnås.

4.7.2 Studie av KIT i informasjonssikkerhetshendelser

Basert på funnene i den første studien ønsket vi å vurdere om det er mulig å skille sikkerhetshendelser fra hverandre med hensyn til de ulike sikkerhetsmålene KIT. PwC leverte i 2017 en rapport til Helse Sør-Øst RHF, ”*Rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastuktur (iMod)*”. Ifølge rapportens sammendrag gjorde PwC i perioden 4. mai 2017 – 21. juni 2017 undersøkelser knyttet til påstander om at sensitive personopplysninger, har vært tilgjengelige for en ekstern leverandør (PwC, 2017, s. 3). Hovedfunnene i rapporten viser at 36 brukere tilknyttet en avtale mellom ESN (Enterprise Services Norge AS) og HSØ har fått utvidede administratorrettigheter som innebærer muligheter for tilgang til helseopplysninger (PwC, 2017, s. 3). Informasjonssikkerheten ble kompromittert, som kan per definisjon betraktes som sikkerhetsbrudd på målene konfidensialitet, integritet og tilgjengelighet.

I studien ble et utsnitt av sikkerhetshendelsene, presentert i PwCs rapport kapittel 1-6, gjennomgått og analysert i henhold til sikkerhetsmålene KIT. Det ble gjort i lys av paradigmet som presenteres i *NOU 2013:15 Digital sårbarhet – sikkert samfunn.* Utsnittet av sikkerhetshendelsene og respektives markering av plassering i henhold til sikkerhetsmålene blir presentert i sin helhet i Vedlegg A. Det påpekes at utsnittet av

sikkerhetshendelser ikke er strategisk utvalgt, men gjennomgått etter deres presenterte rekkefølge.

4.7.3 Studie av sikkerhetskultur i tilsynsrapporter

Med masterskissens utgangspunkt til grunn, hvor sikkerhetskultur i virksomheter var i fokus, har vi studert utbredelse og bruk av sikkerhetskultur-begrepet i tilsynsrapporter. I utgangspunktet søkte vi etter rapporter som vurderer sikkerhetskultur i hendelser relatert til utfordringer knyttet til informasjonssikkerhet. Det var imidlertid få dokument hvor både informasjonssikkerhet og sikkerhetskultur representerte sentrale stikkord.

I søket etter tilsynsrapporter fant vi to dokumenter som betrakter sikkerhetskultur som begge tilhører olje- og gassnæringen. I Rammeforskriften, som gjelder for petroleumsvirksomheter og enkelte landanlegg, blir det stilt krav til det som omtales som helse-, miljø- og sikkerhetskultur. I henhold til Rammeforskriften (2010, § 15) skal en god HMS-kultur omfatte alle faser og aktivitetsområder som fremmes gjennom kontinuerlig arbeid for å redusere risiko og forbedre HMS.

I ”Rapport etter tilsyn med Total sin planlegging og gjennomføring av bore- og brønnoperasjoner på Martin Linge” og ” Rapport etter granskning av hendelse 18.12.2010 på Njord A hvor slip joint falt ned på boredekk” identifiseres brudd som berører denne forskriften. I førstnevnte ble det identifisert forbedringspunkter knyttet til blant annet sikkerhetskultur, erfaringsoverføring og synlig ledelse. I sistnevnte rapport beskrives sikkerhetskulturen på Njord A som mangelfull. Det begrunnes med at brudd på flere sikkerhetskrav demonstrerer at sikkerhetskulturen om bord på Njord A var dårlig (Petroleumstilsynet, 2010, ss. 30-31).

4.7.4 Resultater fra forstudiene

Resultatene fra forstudiene viser til at spesielt begrepsbruken innenfor digital sikkerhet fremstår som problematisk for et systematisk og helhetlig sikkerhetsarbeid med informasjonssikkerhet i Norge. Forstudiene *Begrepet informasjonssikkerhet* og *KIT i informasjonssikkerhetshendelse* tar for seg denne problematikken. Studiene skaper et fundament for videre undersøkelser av begrepsbruk, språk og definisjoner i veiledere, strategier, offentlige dokumenter og lignende. Vår tredje forstudie *Sikkerhetskultur i tilsynsrapporter*, viser at det er få dokumenter hvor både

informasjonssikkerhet og sikkerhetskultur representerer sentrale stikkord. En naturlig årsak kan være at det i fåtallet forskriftene i det norske lovverket stilles krav til sikkerhetskultur.

5 Resultat

Nåværende sikkerhetsepoke oppfattes av Hale og Hovden (i Kringen 2009, s. 45) som et delvis resultat av modning innen sikkerhetsfeltet. Med en vektlegging av organisatoriske og kulturelle faktorer er det ikke unaturlig at begrepet sikkerhetskultur er en gjenganger i offentlige tilgjengelige dokumenter. Flesteparten av dokumentene som analyseres i studien fremhever viktigheten av sikkerhetskultur, og trekker frem sikkerhetskultur som et område med forbedringspotensial. Som det fremkommer i oppgaven er Norge et av verdens mest digitaliserte land, og digital informasjonssikkerhet med tilhørende kultur kan sies å være på dagsordenen. Gjennomgåtte dokumentene viser imidlertid i liten grad til klare og entydige definisjoner. Hvordan begrepet kommuniseres spriker stort. Digitaliseringstakten foregår så hurtig at det ikke er urimelig å se for seg at det eksisterer et kulturelt etterslep, hvor den forståelsesmessige utviklingen angående digital sikkerhet ikke er like utviklet som de informasjonssystemer og digital infrastruktur mennesker omgis av.

Det kreves ikke et omfattende nettsøk for å finne noe som kan tolkes i tråd med antakelsen om at det eksisterer et kulturelt etterslep knyttet til digitalisering. Oppgaven kan forankres i hendelser som beskrives og vurderes i rapporter utviklet av ulike aktører, men også hendelser som presenteres i det offentlige nyhetsbildet. Nyhetsbildet i Norge preges til tider av digitale hendelser og utfordringer virksomheter, organisasjoner og forvaltning står overfor i dagens samfunn. I påfølgende avsnitt presenteres tre saker kjent fra nyhetsbildet i løpet av de tre første månedene i 2019.

Bergen kommune ble pålagt et gebyr på 1,6 millioner av Datatilsynet i etterkant av at en barneskoleelev fikk tilgang til filer med passord og brukernavn til flere tusen elever og lærere i Bergensskolen (Johansen, 2019). Gebyret Bergen kommune ble pålagt er det første etter innføringen av den nye personvernforordningen (Johansen, 2019). Tidlig i februar 2019 ble det også kjent at Visma var utsatt for et omfattende hacking-angrep i løpet av høsten 2018 (Eriksen, Hagen, & Walnum, 2019). Det er antatt at kinesisk etterretning stod bak angrepet og at motivet skal ha vært å stjele forretningshemmeligheter fra Vismas kunder. Videre ble Hydro ble i mars 2019 utsatt

for et omfattende angrep. Dataangrepet omfattet et løsepengevirus og et angrep mot Hydros bruker- og påloggingssystemer. Datasystemet til Hydro ble stengt ned og det ble krevd løsepenger for å "låse opp" dataene konfiskert av hackerne (Brekke, Hirsti, Lied, Ravndal, & Svaar, 2019). Disse tre hendelsene viser at det til tross for utvikling i norsk sikkerhetstenkingen oppstår en rekke sikkerhetsbrudd. I påfølgende kapitler presenteres funnene fra oppgavens dokumentanalyse.

5.1 Ingen unison forståelse

I NorSIS-rapporten *Trusler og trender 2018-19* (NorSIS, 2018) gir et søk på "sikkerhetskultur" flere treff. Under overskriften "Hva er sikkerhetskultur?" står følgende:

> Digital sikkerhetskultur handler om å beskytte digitale verdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Den kan derfor forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til alt som er digitalt. Digital sikkerhetskultur er derfor et sett med handlingsmønstre, og et sett med idéer, holdninger og kunnskaper. I en organisasjon kan digital sikkerhetskultur enten være slik ledelsen ønsker at den skal være, eller ikke slik de ønsker at den skal være. I det siste tilfellet vil sikkerhetskulturen kjennetegnes av lav kunnskap og forståelse for digitale verktøy, uvilje til å bruke disse og manglende tillit til digitale tjenester og teknologi.
>
> (NorSIS, 2018, s. 9)

Overskriften tilsier at en skal få en beskrivelse av sikkerhetskultur, men innholdet under dreier seg utelukkende om det som omtales som digital sikkerhetskultur. NorSIS viser ikke til en tydelig avklart definisjon av sikkerhetskultur, men gir heller det som kan betraktes som en beskrivelse av konseptet, men da i lys av det digitale aspektet. I *Trusler og trender 2017-18* (NorSIS, 2017) betraktes ikke sikkerhetskultur, verken alene eller i kombinasjon med andre ord. Ordet anvendes, med unntak av en gang, utelukkende i forbindelse med henvisninger til andre arbeid.

I rapportene *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018), *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017) og *Ungdom og digital informasjonssikkerhetskultu*r (Malmedal & Røislien, 2017) publisert av NorSIS identifiseres "sikkerhetskultur" en rekke ganger. Ordet fremkommer imidlertid, ikke overraskende, i de fleste tilfeller kombinasjon med "digital" (som digital

sikkerhetskultur), i tråd med rapportenes titler, eller som ”informasjonssikkerhets-kultur”. Ingen av rapportene definerer sikkerhetskultur-begrepet i alene. I NorSIS' hovedrapport, *The Norwegian Cyber Security Culture* (Malmedal & Røislien, 2016) finnes heller ikke en klar definisjon av sikkerhetskultur. NorSIS oversetter selv rapportens tittel til ”Den norske informasjonssikkerhetskulturen”, og det tas derfor utgangspunkt i at security culture kan forstås som sikkerhetskultur. Det er imidlertid en forskjell mellom safety og security, men det norske begrepet ”sikkerhet” omfavner begge begrep (Vinje, i NOU 2006:6, 2006, s. 38). Som i de andre rapportene av NorSIS fremkommer ”sikkerhetskultur”. Det er imidlertid i kombinasjon med et annet ord, som i dette tilfellet er cyber (cyber security culture). Samtlige rapporter beskriver dog ved flere tilfeller hvordan de forstår digital sikkerhetskultur og/eller informasjonssikkerhetskultur:

> Det finnes flere definisjoner på informasjonssikkerhetskultur, og selv om det ikke ser ut til å være én definisjon som fagfolk ser ut til å enes om, så omfatter de fleste definisjonene noen nøkkelområder: Det handler om å beskytte informasjonsverdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Informasjonssikkerhetskultur kan derfor forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til informasjonsverdier. Informasjons- sikkerhetskultur er derfor et sett med handlingsmønstre, og et sett med idéer og holdninger
>
> (Malmedal & Røislien, 2017, s. 35)

Forholdsvis like utgaver av dette sitatet fremkommer i alle rapporter. Også i *The Norwegian Cyber Security* (Malmedal & Røislien, 2016, s. 28) fremkommer tilsvarende innhold, men da på engelsk. I *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018) er imidlertid ”informasjonssikkerhetskultur”-begrepet skiftet ut med ”digital sikkerhetskultur”, men beskrivelsen er som nevnt tilsynelatende lik. Videre fremkommer også følgende beskrivelse av digital sikkerhetskultur:

> Digital sikkerhetskultur er samfunnets felles verdier, holdninger, normer, kunnskaper og handlinger om det å kunne ta del i et digitalisert samfunn på en trygg måte. Den digitale sikkerhetskulturen skal gjøre både den enkelte, og samfunnet i sin helhet, mer mindre sårbare mot digitale trusler
>
> (Malmedal & Røislien, 2018, s. 7)

Også i *Mørketallsundersøkelsen 2018* (NSR, 2018) nevnes sikkerhetskultur i kombinasjon med ”digital”. Digital sikkerhetskultur anvendes blant annet i et forebyggende tiltak som skal bidra til redusert sårbarhet og reduserte konsekvenser: ”Kartlegg virksomhetens digitale sikkerhetskultur for å avdekke om det er behov for å igangsette tiltak.” (s. 56). Begrepet blir imidlertid ikke nærmere beskrevet. I *Mørketallsundersøkelsen 2016* (NSR, 2016) anvendes ikke sikkerhetskultur-begrepet i det hele tatt. Heller ikke i *Risiko 2016* (NSM, 2016) nevnes sikkerhetskultur. I NSMs rapport *Risiko 2017* (NSM, 2017) derimot, gis følgende definisjon: “Sikkerhetskultur er summen av de ansattes kunnskap, motivasjon, holdninger og atferd.” (s. 37). I rapporten *Risiko 2018* (NSM, 2018) omtales sikkerhetskultur slik:

> I tillegg til å integrere sikkerhetsstyring i virksomheten, bør det legges til rette for god sikkerhetskultur i virksomheten. Beslutninger om sikringstiltak er ikke bare avhengig av sikkerhets- og risikoforståelse, men vil også påvirkes av den rådende sikkerhetskultur. Sikkerhetskultur preger også hvordan virksomhetens innførte sikringstiltak etterleves av virksomhetens medarbeidere
>
> (NSM, 2018, s. 20)

Det gis med andre ord ingen beskrivelse eller definisjon av sikkerhetskulturbegrepet. Begrepet blir heller ikke verken definert eller beskrevet i noen av NSMs rapporter om IKT-risikobilde utgitt i perioden 2015 til 2018. Begrepet fremkommer imidlertid i *Helhetlig IKT-risikobilde 2017* (NSM, 2017, ss. 44-47) og i *Helhetlig IKT-risikobilde 2015* (NSM, 2015, s. 57), men kun i forbindelse med blant annet beskrivelser av viktigheten av god sikkerhetskultur.

I *Normen 5.3* nevnes “sikkerhetskultur” ved én anledning. I forordet av dokumentet fremkommer følgende: “Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur og ha gode tiltak for å sikre at dette fungerer og samtidig håndtere og lære av tilfeller der den ikke fungerer (Normen, 2018, s. 4). Det gis ikke en utfyllende definisjon eller videre forklaring av verken begrep eller konsept. Heller ikke *Årsrapport for 2018* (Datatilsynet, 2018) forklarer sikkerhetskulturbegrepet. Det fremkommer imidlertid i rapporten at “Innholdet i begrepene “digitale ferdigheter og digital dømmekraft” må defineres nærmere” (s. 51). Ettersom dette sier noe om holdninger, verdier og atferd kan dette tolkes som i

tråd med inngående elementer i sikkerhetskultur. I *Risiko- og sårbarhetsanalyse (ROS),* en rapport om Finanssektorens bruk av informasjons- og kommunikasjonsteknologi (IKT) (Finanstilsynet, 2018), beskrives heller ikke sikkerhetskultur. Dog fremkommer følgende setning: ”Foretakenes sikkerhetsrammeverk, opplæring av ansatte, sikkerhetskrav i avtaler med leverandørene og organisering av sikkerhetsområdet danner grunnlaget for en god sikkerhetskultur i arbeidet med å forebygge arbeidet med å forebygge digitale angrep.” (2018, s. 64).

Meld. St. 10 (2016-2017) betrakter ikke sikkerhetskultur alene, men formidler følgende: “Våre verdier, holdninger, meninger, kunnskaper og holdninger til sikkerheten i det digitale rom kan oppsummeres i begrepet IKT-sikkerhetskultur” (JD, 2016). Begrepet stortingsmeldingen benytter er ulikt begrepene de fleste andre rapporter forholder seg til. ”Sikkerhetskultur” nevnes to ganger i *Meld. St. 38 (2016-2017)* (JD, 2016), men blir ikke betraktet nærmere. *Nasjonal strategi for digital sikkerhet* (Departementene, 2019) presenterer heller ikke en definisjon av begrepet, men anvender begrepet i et delmål, “Befolkningen har en god digital dømmekraft og god sikkerhetskultur” (Departementene, 2019), tilhørende det overordnede målet: ”Norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har en bedre evne til egenbeskyttelse mot uønskede digitale hendelser.” (s. 13). Heller ikke NOU 2015:13, NOU 2014:12 og NOU 2018:14 definerer sikkerhetskultur-begrepet. Begrepet nevnes i noen tilfeller, men betraktes ikke nærmere. Det er heller ikke gjort funn av ”sikkerhetskultur” i *Statsbudsjettet 2019* (Finansdepartementet, 2018).

Datagrunnlag:
The Norwegian Cyber Security Culture (Malmedal & Røislien, 2016), *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017), *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017)*, Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018)*, Trusler og trender 2018-19* (NorSIS, 2018)*, Trusler og trender 2017-18* (NorSIS, 2017)*, Mørketallsundersøkelsen 2018* (NSR, 2018)*, Mørketallsundersøkelsen 2016* (NSR, 2016)*, Risiko 2016* (NSM, 2016)*, Risiko 2017* (NSM, 2017), *Risiko 2018* (NSM, 2018)*, Helhetlig IKT-risikobilde 2017* (NSM, 2017)*, Helhetlig IKT-risikobilde 2015* (NSM, 2015)*, Normen 5.3* (Normen, 2018)*, Årsrapport for 2018* (Datatilsynet, 2018), *Risiko- og sårbarhetsanalyse (ROS)*

(Finanstilsynet, 2018), *Nasjonal strategi for digital sikkerhet* (Departementene, 2019), *NOU 2015:13 Digital sårbarhet – sikkert samfunn* (NOU 2015:13, 2015), *NOU 2018:14 IKT- sikkerhet i alle ledd* (NOU 2018:14, 2018),, *Meld. St. 38 IKT-sikkerhet - Et felles ansvar* (JD, 2016), *Meld. St. 10 2016-2017 Risiko i et trygt samfunn. Samfunnssikkerhet* (JD, 2016)

5.2 Vaklende begrepsbruk

NorSIS utga i 2016 den omfattende rapporten *The Norwegian Cyber Security Culture* (Malmedal & Røislien, 2016). Da det som anses som hovedrapporten ble publisert, omtalte NorSIS selv, rapporten som en ”rapport om den norske informasjonssikkerhetskulturen” (NorSIS, 2016). I *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017, s. 13) formidles tilsvarende budskap: ”Rapporten beskriver informasjonssikkerhetskulturen for nasjonen som helhet, men det er åpenbart at ulike grupper i samfunnet har ulike utfordringer og muligheter.”. I *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017, s. 7) omtales også hovedrapporten som et studie av informasjonssikkerhetskultur. I *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018) derimot, blir hovedrapporten omtalt som en rapport om digital sikkerhetskultur: ”I vår hovedrapport fra 2016 utviklet NorSIS et konsept for å beskrive digital sikkerhetskultur og en metode for å kartlegge den.” (Malmedal & Røislien, 2018, s. 8). Rapporten beskrives med andre ord ikke lenger som en rapport for om informasjonssikkerhetskultur, men i stedet en rapport om digital sikkerhetskultur. I *Ungdom og digital sikkerhetskultur*, som ble ugitt året etter hovedrapporten, fremkommer følgende:

> Vi gjorde funn i vår studie fra 2016 som antydet at alder er en signifikant faktor for store deler av det vi beskriver som informasjonssikkerhetskultur. Merk at vi behandler begrepene informasjonssikkerhetskultur og digital sikkerhetskultur som synonymer i denne studien.
>
> (Malmedal & Røislien, 2017, s. 9)

Selv om rapportens tittel omfatter digital sikkerhetskultur, anvender forfatterne i hovedsak begrepet informasjonssikkerhetskultur. I teksten identifiseres ”informasjonssikkerhetskultur” nærmere 50 ganger, mens antall ganger ”digital sikkerhetskultur” identifiseres kan telles på hånd. Som det fremkommer i forrige sitat,

blir det dog påpekt at begrepene behandles som synonymer. Det samme påpekes i *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017), men heller ikke her benyttes ”digital sikkerhetskultur” i utpregende grad. I *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018), som i motsetning til de to andre, beskriver hovedrapporten som et studie av digital sikkerhetskultur (og ikke informasjons-sikkerhetskultur), foreligger også en tilsvarende merknad: ”I denne rapporten brukes informasjonssikkerhetskultur og digital sikkerhetskultur som synonymer. ” (s. 8). I sistnevnte rapport, fremkommer imidlertid ”informasjonssikkerhetskultur” én gang i løpet av hele rapporten. Den ene gangen ordet forekom, var i setningen sitert overfor, som formidler budskapet om behandling som synonymer. Med andre ord benyttes ikke informasjonssikkerhetskultur-begrepet i det hele tatt, og ”digital sikkerhetskultur” har tilsynelatende tatt fullstendig over.

2017, året hvor NorSIS publiserte *Ungdom og sikkerhetskultur* (Malmedal & Røislien, 2017) og *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017), kan nærmest betraktes som et vendepunkt for respektives begrepsbruk. I utgangspunktet er ”Informasjonssikkerhetskultur” er et fremtredende begrep i begge rapportene. Ordet fremkommer ofte, og spørreskjema som ligger til grunn for undersøkelsene, fremstiller studiene som undersøkelser av informasjonssikkerhetskultur (s. 38). I tredje kapittel i *Nordmenn og digital sikkerhetskultur,* Den Norske digitale sikkerhetskulturen (s. 13), gis en beskrivelse av digital sikkerhetskultur. ”Digital sikkerhetskultur” fremkommer dog ikke en eneste gang i teksten, og beskrivelsene gis baseres utelukkende på ”informasjonssikkerhetskultur”. Tilsvarende tendenser er å se i *Ungdom og digital sikkerhetskultur.* Begge rapportene forholder seg i hovedsak til ”informasjonssikkerhetskultur”, men bare frem til et visst punkt. I rapportenes hovedkonklusjon tar ”digital sikkerhetskultur” tilsynelatende over for informasjonssikkerhets-begrepet: ”Denne studien viser at det er tildels store forskjeller mellom kjønnene når det gjelder digital sikkerhetskultur, men den gir ikke svar på hvorfor det er slik.” (Malmedal & Røislien, 2017, s. 96). Informasjonssikkerhetskultur-begrepet fremkommer verken i konklusjon eller i rapportens anbefaling for videre arbeid. Den samme utviklingen observeres i *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017), som også utelukkende anvender ”digital sikkerhetskultur” i rapportens konkusjon. I siste del av rapportene har NorSIS tilsynelatende fullt og helt forlatt informasjonssikkerhetskultur til fordel

for digital sikkerhetskultur. Dette er en oppsiktsvekkende diskré utfasing av et begrep som har stått svært sentralt i store deler av NorSIS sitt arbeid. Det kan stilles spørsmål til hvordan og hvorfor en så stor endring i begrepsbruk har gått forbi i stillhet.

Datagrunnlag:
The Norwegian Cyber Security Culture (Malmedal & Røislien, 2016), *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017), *Nordmenn og digital sikkerhetskultur* (NorSIS, 2017)*, Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018)

5.3 Et begrep som omfatter mye

Informasjonssikkerhetskultur har som påvist stått sentralt i NorSIS' arbeid. De presenterer hvordan de forstår begrepet, men viser ikke til en tydelig avklart definisjon av begrepet. Gjør en et enkelt søk på definisjon av informasjonssikkerhetskultur i Google, er funnene få. I en oppsummerende rapport fra sikkerhetstoppmøtet i 2016, *Informasjonssikkerhetskultur* (NorSIS, 2016) påstås følgende: "Informasjonssikkerhetskultur omtales gjerne som summen av våre verdier, meninger, holdninger, interesser, kunnskap og handlinger." (s. 5). Dette er ikke en definering av begrepet, men heller en forsiktig uttalelse som kan forstås som et forsøk på å beskrive fenomenet. Det er imidlertid noe som likevel ikke stemmer her. Det vises til summen av en rekke elementer, men med hensyn til hva? Tilføyer en elementer fra definisjonen av informasjonssikkerhet, kan påstanden potensielt sett gi mer mening, men den utgjør fortsatt ingen tydelig definisjon.

"Digital sikkerhetskultur" som NorSIS benytter i sine siste rapporter, blir definert i *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018) som "samfunnets felles verdier, holdninger, normer, kunnskaper og handlinger om det å kunne ta del i et digitalisert samfunn på en trygg måte." (s. 7). Begrepet digital sikkerhetskultur, slik NorSIS definerer det, kan dermed forstås som dekkende for samtlige digitale trusler og sårbarheter. Kombinasjonen av ordene "digital" og "sikkerhetskultur" formidler med andre ord et budskap som tilsier at begrepet omfatter alt som foregår digitalt. Definisjonen adresserer dermed ikke avgrensningen til informasjon, slik informasjonssikkerhetskultur gjør. Elementer i det ene ordet inngår ikke i det andre, og det kan dermed argumenteres for at en "synonymisering"

av begrepene ikke kan rettferdiggjøres. Informasjonssikkerhetskultur-begrepet på sin side, mangler et element som sørger for at begrepet forsås som informasjonssikkerhet i digital kontekst. Som nevnt presenterer imidlertid Meld. St. 10 (2016-2017) (JD, 2016) en annen variant, IKT-sikkerhetskultur. Begrepet benyttes dog som et oppsummerende ord knyttet til elementer av betydning for sikkerheten i det digitale rom. Det resulterer med andre ord i at sikkerheten som betraktes omfavner sikkerhet utover sikkerhet av digital informasjon. Elementene som i Meld. St. 10 betraktes som av betydning, samsvarer imidlertid med de elementer som andre aktører forstår som inngående i sikkerhetskultur i en digital informasjonssikkerhetskontekst.

Ingen av ordene klarer dermed å korrekt adressere konseptet en forsøker å sette ord på. Det er åpenbare utfordringer knyttet til begrepsavklaring og terminologi. Et korrekt beskrivende begrep i en kontekst hvor en helt konkret ser på kultur for hvordan en forholder se til digital informasjon eksisterer ikke.

Datagrunnlag:
Informasjonssikkerhetskultur (NorSIS, 2016)*, Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018), *Meld. St. 10 Risiko i et trygt samfunn - Samfunnssikkerhet* (JD, 2016).

5.4 Uflaks og tilfeldigheter oppgis som årsak til sikkerhetsbrudd

NSRs to siste utgaver av Mørketallsundersøkelsen (NSR, 2016, s. 3) er basert på en ny innsamlingsmetode, som gjør at de ikke er sammenlignbare med tidligere undersøkelser. Det er imidlertid tall fra de to siste rapportene som synliggjør en trend verdt å belyse (NSR, 2016). I *Mørketallsundersøkelsen 2016* (NSR, 2016) oppga 412 av 1500 virksomheter at de har opplevd uønskede sikkerhetshendelser. Den verste hendelsen, som de 412 virksomhetene var utsatt for, ble av 74% av respondentene betraktet som inntruffet som følge av uflaks eller en tilfeldighet. 55% anser også menneskelig feil som en medvirkende faktor (s. 16). I siste utgave av undersøkelsen, *Mørketallsundersøkelsen 2018* (NSR, 2018), ble 572 respondenter som i løpet av 2017 hadde vært utsatt for sikkerhetsbrudd, stilt et tilsvarende spørsmål: ”Var noen av følgende faktorer årsak til at sikkerhetsbrudd oppsto?”. På spørsmålet svarte 67% av respondentene at uflaks eller tilfeldigheter var årsaken. På det samme spørsmålet svarer 55% av respondentene ”ja” til at menneskelig feil var en faktor.

I undersøkelsen fra 2016 (NSR, 2016) hevdes det at tallene tyder på at virksomhetene i liten grad oppfatter angrepene som spesifikt rettet mot dem. Det kan for så vidt være tilfellet, men er samtidig bare én av mange mulige måter å tolke tallene på. Respondentene har kun mulighet til å besvare spørsmålene med ja, nei og kanskje, som dermed ikke legger særlige føringer for tolkning av bakenforliggende årsak. Hvorvidt et sikkerhetsbrudd betraktes som tilfeldigheter eller uflaks vil være preget av forståelse, både av tilfeldigheter og uflaks som ord, og for sikkerhetsstyring. Like mye som slutningen i rapporten, kan faktumet at respondentene betrakter hendelsene som uflaks skyldes ansvarsfraskrivelse, manglende forståelse eller rett og slett dårlig ordvalg.

Datagrunnlag:
Mørketallsundersøkelsen 2016 (NSR, 2016)*, Mørketallsundersøkelsen 2018* (NSR, 2018)

5.5 Ukorrekt fremstilling av forskning

Med en tilsynelatende svak begrepsavklaring og definisjon vil misforståelse av konseptet nærmest kunne betraktes som en naturlig konsekvens. Det finnes flere dokumenter hvor sikkerhetskultur betraktes som noe som må skapes, og anses dermed som noe som enten eksisterer eller ikke. I et innlegg publisert av Glasspaper (2018), med tittelen *Hva skal til for å skape en sikkerhetskultur?*, presenteres resultater fra en undersøkelse rundt cyber-sikkerhet. Ifølge Glasspaper sier rapporten at kun 34% av respondentene er bevisste på hvilken rolle de har i å skape en sikkerhetskultur i deres organisasjon (Glasspaper, 2018). Tittelen, og dette utsagnet formidler et budskap som tilsier at sikkerhetskultur enten eksisterer eller ikke eksiterer. I rapporten forfatteren viser til, The ISACA/CMMI Institute Cybersecurity Culture Report (2018), fremkommer følgende: ”34 percent believe that their workforce clearly understands their role in achieving the organizations desired cyber security culture” (ISACA & CMMI, 2018).

Videre i innlegget av Glasspaper blir det hevdet at 42% av respondentene i undersøkelsen oppgir at de ikke har etablert en plan for å skape en sikkerhetskultur (Glasspaper, 2018). I undersøkelsens rapport fremkommer følgende: “In

organizations that have yet to establish an effective cyberculture, 58 percent cite a corresponding lack of a clear management plan (…).” (ISACA & CMMI, 2018, s. 4). Prosentandelene tyder på at dette utdraget er utgangspunktet for påstanden i innlegget av Glasspaper. Glasspaper utelukker imidlertid moment av vesentlig betydning for fremstillingen av innholdet i undersøkelsen.

Innlegget av Glasspaper gir dermed en feilaktig fremstilling av innholdet i undersøkelsen, som forårsaker at en stiller seg kritisk til den opprinnelige rapporten. Glasspapers ukorrekte fremstilling av sikkerhetskultur som konsept, får det til å se ut som ISACA og CMMIs arbeid baseres på en feilaktig forståelse av sikkerhetskultur som konsept, som egentlig ikke er tilfellet.

Datagrunnlag:
Hva skal til for å skape en sikkerhetskultur? (Glasspaper, 2018), *ISACA/CMMI Institute Cybersecurity Culture Report* (ISACA & CMMI, 2018).

5.6 Uenighet om måling av informasjonssikkerhetskultur

Informasjonssikkerhetskultur var ifølge NorSIS et ”velkjent” begrep da de startet kartleggingen av norsk informasjonssikkerhetskultur. Likevel erfarte de at det eksisterte lite litteratur om hva konseptet faktisk er. Erfaringene resulterte i at NorSIS (2016) i samarbeid med eksperter innen informasjonssikkerhet og innen kultur-vitenskap utarbeidet en grundig beskrivelse av det teoretiske grunnlaget for informasjonssikkerhetskultur. NorSIS (Malmedal & Røislien, 2017) hevder at konseptet først og fremst ble utviklet og brukt av virksomheter og personer innen fagområdet, og utpeker det som en årsak til at informasjonssikkerhetskultur i samfunnet er utfordrende å måle (ss. 15-16).

Digital sikkerhetskultur ble ifølge *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018) utelukkende betraktet som en inngående del av organisasjonskultur, og dermed kun av betydning for virksomheter (s. 13). Denne tilnærmingen har resultert i at digital sikkerhetskultur har blitt betraktet som et verktøy for effektivitet og etterlevelse av krav (s. 13). Videre i rapporten blir det påpekt at studier av digital sikkerhetskultur fokuserer atferdsdimensjonen. Det trekkes frem at studier typisk dreier seg om hvorvidt person vil klikke på en ”phishing-lenke”

(s. 13), som da utelukkende baseres på atferd. Resultater fra slike studier vil i hovedsak si noe om hva som allerede gjøres, og dermed lite om hva som vil skje i fremtiden (s.14). NorSIS hevder dog at det er en generell oppfatning om at digital sikkerhetskultur også omhandler verdier og holdninger, i tillegg til atferd (s. 13). Det kan dermed være interessant å stille spørsmål til hvorfor noen likevel forholder seg til, men også aksepterer denne tilnærmingen.

NorSIS betrakter følgende åtte kjerneelement som beskrivende for informasjonssikkerhetskultur: felleskap, styring og kontroll, tillit, risikooppfattelse, optimisme for teknologi og digitalisering, kompetanse, interesse og atferdsmønstre (Malmedal & Røislien, 2016, s. 30). Disse komponentene er derfor avgjørende for NorSIS' kartlegging og undersøkelse av informasjonssikkerhetskultur. NorSIS' hovedrapport, *The Norwegian Cyber Security Report* (Malmedal & Røislien, 2016) baseres på en deskriptiv tilnærming. En slik tilnærming tar utgangspunkt i alle sikkerhetskulturer er ulike, og dermed ikke kvantitativt sammenlignbare. NorSIS omtaler på sine hjemmesider rapporten, *The Security Culture Report* (CLTRe, 2017), som er basert på en motstridene tilnærming. I CLTRes rapport måles sikkerhetskultur i ulike bransjer, som blir sammenlignet ved hjelp av indexer (NorSIS, 2017). I en intervallskala presenteres indexene kategorisert etter bransje – jo høyere index, jo bedre sikkerhetskultur. I en slik normativ tilnærming, foreligger det der dermed en antagelse om at noen kulturer faktisk er bedre enn andre. NorSIS har midlertid påpekt at det ikke er noe i veien for at noen av kjerneelementene i informasjonssikkerhetskultur betraktes som normative fenomener, som eksempelvis atferd (NorSIS, 2017).

I en presentasjon av Håkon Styri (2017) på vegner av Difi betegnes sikkerhetskultur som et godt eksempel på å beskrive informasjonen en ønsker å bruke til styring og som beslutningsgrunnlag. Videre gis eksempler knyttet til utfordringen med å beskrive hvilke attributter som skal måles. Styri (2017) gir følgende forslag til indikatorer som kan brukes i en enkel analyse: forståelse for informasjonssikkerhet, regeletterlevelse, tillit og medvirkning. I likhet med NorSIS vektlegges med andre ord andre forhold enn atferd. Videre kan disse elementene å kjenne igjen dimensjonene som CLTRe (2017) betrakter som inngående i sin kartlegging av sikkerhetskultur: holdninger, oppførsel, bevissthet, kommunikasjon, etterlevelse, normer og ansvar.

Rapporten fra CLTRe blir dermed også et eksempel på et studie som ser elementer utover atferd, som NorSIS hevder de fleste studier fokuserer på.

ForBedring, en kartleggingsundersøkelse av sikkerhetskultur i spesialisthelsetjenesten, har som formål om å forbedre arbeidsmiljø og pasientsikkerhetskultur (Nasjonalt pasientsikkerhetprogram, 2017). Undersøkelsen kartlegger pasientsikkerhetskultur og arbeidsmiljø i den formelle organisasjonen ved følgende tema: engasjement, teamarbeidsklima, sikkerhetsklima, arbeidsforhold, konflikter, opplevd ledelsesatferd, fysisk miljø og oppfølging (Nasjonalt pasientsikkerhetprogram, 2017, s. 8). Denne undersøkelsen er dog ikke relatert til informasjonssikkerhet, men er inkludert som et bidrag til å si noe om hvordan sikkerhetskultur måles. Temaene som legges til grunn får også denne kartleggingen til å fremstå som en undersøkelse hvor elementer utover atferd-dimensjonen tas i betraktning. Ser en nærmere på påstandene som legges til grunn i vurderingen, ser en at det ikke nødvendigvis er tilfellet. Vurderingen av eksempelvis sikkerhetsklima er sterkt farget av atferdsbaserte påstander:

- Jeg melder fra om avvik og hendelser som kan føre til skade eller feil
- Det er trygt å si i fra om kritikkverdige forhold her
- Vi diskuterer åpent de feil og hendelser som oppstår for å lære av dem
- Mine kolleger oppmuntrer meg til å si fra om jeg er bekymret for sikkerheten
- Her blir medisinske feil (behandlingsrelaterte forhold som gir/kunne gitt negativt utfall for pasient) håndtert riktig
- Jeg ville føle meg trygg hvis jeg var pasient her

(Nasjonalt pasientsikkerhetprogram, 2017, s. 27).

I et innlegg på NSMs hjemmesider, med tittelen *Kan vi måle sikkerhetskultur?*, står følgende:

> Vi kan måle kunnskapsnivå hos de ansatte og anta at atferden står i forhold til det målte kunnskapsnivå. Men å kunne si noe om sikkerhetskultur ved bare å måle om et større antall av de ansatte svarte ”riktig” på en spørreundersøkelse er å lure seg selv.
>
> (NSM, 2014)

Videre trekkes det frem at det er mulig å skape et bilde av sikkerhetsatferden i en organisasjon ved å måle enkeltaktiviteter. Tiltak som trekkes frem er å holde oversikt med rapporterte sikkerhetsbrudd og sikkerhetstruende hendelser, holde oversikt over nettverksaktivitet i virksomheten og holde oversikt med dataangrep eller virusinfeksjoner (NSM, 2014). Avslutningsvis formidler NSM at virksomheter også tester sikkerhetsatferd ved å utsette ansatte for hendelser som involverer sosial manipulering, men som medføre etiske og moralske utfordringer. Det som egentlig adresseres i innlegget er hvordan en kan måle atferd, som de selv beskriver som ikke tilstrekkelig for å måle sikkerhetskultur. Spørsmålet som reises i tittelen, om sikkerhetskultur kan måles, får med andre ord lite oppmerksomhet. Det er tydelig at dette er et spørsmål med et svar som er vanskelig å sette ord på.

Datagrunnlag:
The Norwegian Cyber Security Culture (Malmedal & Røislien, 2016), *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018)*, Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017)*,The Secuirty Culture Report 2017* (CLTRe, 2017), *Kan vi måle sikkerhetskultur?* (NSM, 2014)*, Måling av informasjonssikkerhet* (Styri, 2017)*, ForBedring – kartlegging av sikkerhetskultur i spesialisthelsetjenesten* (Nasjonalt pasientsikkerhetprogram, 2017).

5.7 Forskjeller på samfunn- og organisasjonsnivå

I rapporten *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017) poengteres den terminologiske utfordringen knyttet til informasjonssikkerhetskultur-begrepet. Videre vektlegges problematikken knyttet til hvilket nivå begrepet skal anvendes på, og om begrepet kan betraktes som gyldig på ulike nivåer i samfunnet (s. 17). Som kjent hevder NorSIS at informasjonssikkerhetskultur-begrepet er utviklet av virksomheter med god kjennskap til informasjonssikkerhet, men videre hevdes følgende:

> Selv om konseptet er utviklet i bedrifter, har vi også ”nasjonale” informasjonssikkerhetskulturer. Imidlertid blir ikke disse uttrykt og diskutert på samme vis. For eksempel; Bedrifter, virksomheter og organisasjoner har en tydelig definert hensikt, mens vi sjelden snakker om ”hensikten” til en nasjon

(Malmedal & Røislien, 2017, s. 17)

I rapporten reises dermed et spørsmål til hvorvidt det vil være mulig å utvikle en forståelse av begrepet som sørger for en felles generell forståelse som er anvendbar både på nasjonalt og bedriftsnivå. Videre anerkjennes faktumet at entydig forståelse av begrepets innhold ikke eksisterer. Det formidles dog at begrepet ofte beskrives som "noe som har med atferd å gjøre" (s. 17). I både *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017) og *Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018) fremkommer beskrivelser av både kultur, sikkerhetskultur og informasjonssikkerhetskultur som er forholdsvis like. Det trekkes blant annet frem at kulturelle verdier og normer læres tidlig i livet, gjennom formell utveksling som skole og fritidsaktiviteter, og gjennom sosial interaksjon med venner og familie. Med det poengterer forfatterne at nasjonale kulturene er dypt forankret i oss. Videre skriver forfatterne at nasjonale kulturer består av sub-kulturer hvor eksempelvis alder, kjønn og interesser er avgjørende faktorer, og at digital sikkerhet og informasjonssikkerhetskultur er slike subkulturer (Malmedal & Røislien, Ungdom og digital sikkerhetskultur, 2017, s. 35).

Sett i et virksomhetsperspektiv, er informasjonssikkerhetskultur ifølge *Ungdom og digital sikkerhetskultur* (Malmedal & Røislien, 2017) vanligvis knyttet til sikkerhetsatferden til ansatte. Måling av informasjonssikkerhetskultur er dermed et viktig verktøy for virksomheter, som lenge har vært klar over at intern kultur er av betydning for resultatene (s. 17). Angående informasjonssikkerhet og dens innvirkning for digital sikkerhet, er modenheten i organisasjoner imidlertid lav. Informasjonssikkerhetskultur blir av mange ansett som normative atferdsmønstre som kan endres og forbedres for å oppnå bedre resultater i en organisasjon (s. 17). Denne betraktningen kan forståelig nok ikke overføres til forståelsen av sikkerhetskultur i en nasjon. Som rapporten trekker frem, har en nasjon sjeldent en hensikt, slik en virksomhet normalt sett har. Utfordringen NorSIS vektlegger i sine rapporter er dermed svært relevant for arbeidet med forbedring av informasjonssikkerhetskultur.

Datagrunnlag:
Ungdom og digital sikkerhetskultur (Malmedal & Røislien, 2017)*, Nordmenn og digital sikkerhetskultur 2018* (Malmedal & Røislien, 2018)

5.8 Ansvaret for digital sikkerhet skyves over på virksomheter

Den fjerde utgaven av *Nasjonal strategi for digital sikkerhet* (Departementene, 2019) vektlegger at en i fellesskap må utvikle tiltak som kan styrke den digitale sikkerhet i samfunnet. Under kapittel 3.1, Forebyggende digital sikkerhet, er følgende presentert som det overordnede målet: ”Norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.” (s. 13). Videre beskrives digital sikkerhet som et virksomhetsansvar, men myndighetene skal ifølge strategien tilrettelegge for at virksomheter skal kunne beskytte seg selv mot uønskede digitale hendelser. Ett av de åtte delmålene som knyttes til det overordnede målet er: “Befolkningen har en god digital dømmekraft og god sikkerhetskultur” (Departementene, 2019, s. 13). Et av tipsene som presenteres, og som kan forstås som et tiltak tilkoblet delmålet er:

> Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur
>
> (Departementene, 2019, s. 14)

Tiltaket er imidlertid vinklet mot virksomheter, og ikke befolkningen, som er objektet i delmålet presentert like overfor. Dessuten blir det ikke spesifisert hva som menes med sikkerhetskultur, som i seg selv medfører utfordringer med tanke på kartlegging og forbedring en sikkerhetskultur. Det kan argumenteres for at dette dokumentet ikke er stedet for en nærmere utgreiing, men det er heller ikke identifisert noe annet sted, verken i form av regulatoriske krav eller retningslinjer. Heller ikke sikkerhetsloven (Sikkerhetsloven, 2018) som trådte i kraft 1. januar 2019 nevner sikkerhetskultur, til tross for kapitler om både generelle krav til forebyggende sikkerhetsarbeid (§§ 4-1 - 4-5) og informasjonssikkerhet (§§ 5-1 - 5-6).

I lovverket er sikkerhetskultur-begrepet kun identifisert i Rammeforskriften (2010, § 11), men utelukkende i sammenheng med helse og miljø (helse-, miljø, og sikkerhetskultur). Difi har imidlertid utarbeidet *Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet* (Difi, 2015). Tredje utgave av veilederen formidler hvordan en kan bygge opp et helhetlig opplæringsprogram, og gir råd til hvordan en kan utvikle sikkerhetskulturen (s.1).

Heller ikke i personopplysningsloven (Personopplysningsloven, 2018) fremkommer sikkerhetskulturbegrepet, men det henvises imidlertid til ”atferdsnormer”. Ifølge Datatilsynet er en atferdsnorm ”et regelsett for en spesifikk bransje, og skal gi konkrete regler og retningslinjer for hvordan virksomhetene skal innrette seg for å etterleve kravene i personvernforordningen” (Datatilsynet, u.å.). I avsnitt 5, i artikkel 40 Atferdsnormer i personopplysningsloven stilles det krav til at skal medlemsstatene, tilsynsmyndighetene, Personvernrådet og Kommisjonen oppmuntre til at det utarbeides atferdsnormer (Personopplysningsloven, 2018). Det stilles dog ingen krav til virksomheter om å faktisk utarbeide et slikt regelsett. Normen 5.3 (Normen, 2018) er et eksempel på en atferdsnorm for helsesektoren. Normen 5.3 vil i praksis gjelde de fleste virksomheter innenfor helse- og omsorgssektoren, og er kanskje det tydeligste eksempelet på en atferdsnorm i Norge. Ifølge Normens strategi vites det imidlertid lite om etterlevelse av Normen 5.3, og gjeldende versjon er ikke godkjent av Datatilsynet (Normen, 2019).

Vi har ikke identifisert en eksplisitt forklaring av hva som menes i *Nasjonal strategi for digital sikkerhet* (Departementene, 2019)*,* med at myndighetene skal legge til rette for at virksomheter skal kunne beskytte seg selv mot uønskede digitale hendelser. Tilsyn kan dog forstås som et av bidragene. I Meld. St. 38 beskrives tilsyn som et virkemiddel for myndigheter for å etterse at virksomhetene etterlever regler og krav (JD, 2016, s. 36; PwC, 2017). Det er dog ikke avdekket tilsynsrapporter knyttet til digital sikkerhet hvor sikkerhetskultur blir betraktet. Det fremkommer av Datatilsynets, *Årsrapport fra 2018* (Datatilsynet, 2018), at fysisk tilsyn har blitt nedprioritert som følge av at ressurser har blitt prioritert til nytt regelverk og tilpassing til dette. Datatilsynet argumenterer for at dette har vært en riktig prioritering, med tanke på både viktighet, og et faktum at virksomhetene har bedre tid til å tilpasse seg det nye regelverket før de blir kontrollert (Datatilsynet, 2018, ss. 25-26).

Datagrunnlag:
Nasjonal strategi for digital sikkerhet (Departementene, 2019), *Rammeforskriften § 11* (2010)*, Atferdsnormer* (Datatilsynet, u.å.)*, Personopplysningsloven* (2018)*, Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet* (Difi, 2015)*,*

Årsrapport for 2018 (Datatilsynet, 2018)*, Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten. Versjon 5.3* (Normen, 2018)*, Strategi for Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (2019-2021)* (Normen, 2019)

6 Diskusjon

I dette kapittelet diskuteres empirisk data i lys av oppgavens teorigrunnlag. Innledningsvis adresseres i hovedsak funn som typisk berører forskningsspørsmål 1. Videre i kapittelet løftes momenter som i større grad er treffende for begge forskningsspørsmålene. Avslutningsvis knyttes de diskuterte forhold opp mot oppgavens problemstilling.

6.1 Lik forståelse av sikkerhetskultur forutsetter mer en kontekst

Som presentert i kapittel 5.1, indikerer funn i oppgaven at det ikke eksisterer en unison forståelse av sikkerhetskultur i digital kontekst aktørene imellom. I henhold til oppgavens teorigrunnlag kan måten aktørene formidler og anvender sikkerhetskultur på anses som representativ for respektives forståelse av sikkerhetskultur. I lys av oppgavens innledning og teorigrunnlag vil vi belyse flere forhold som kan forstås som av betydning for aktørenes forståelse. Som adressert i oppgavens innledning, er både sikkerhet og kultur ord som kan forstås som begrep som dekker en rekke fenomener. Kontekst kan dermed tenkes å være av spesiell betydning. Videre blir forutsetningene for en lik forståelse tvilsomt bedre når ordene settes sammen som sikkerhetskultur.

I kapittel 3.4, Sikkerhetskultur, synliggjøres det som kan forstås som en sentral utfordring knyttet til forståelse av sikkerhetskultur i en digital kontekst. Beskrivelsene og definisjonene av sikkerhetskultur i teorigrunnlaget er utelukkende basert på eller presentert i lys av organisatoriske forhold og nivå. Det er tilsynelatende ingen anerkjent og utbredt definisjon som lykkes i å adressere konseptets innhold uavhengig av strukturelt nivå. Med utgangspunkt i virksomhetsnivå omhandler sikkerhetskultur ifølge Aven et al. (2004, s. 34) den kollektive forståelse av *hva* som er farlig og *hvordan* en bidrar til å redusere disse farene.

Definisjonen av Aven et al. (2004, s. 34) kan alene synliggjøre hvorfor ulike aktører vil besitte ulike oppfatninger av hva sikkerhetskultur. Hva som legges i *hva*, og hva som avgjør hva som legges i *hvordan* vil være sterkt betinget av kultur. I en digital kontekst vil det naturligvis eksistere noen grunnleggende forhold som vil være av betydning for de aller fleste. Eksempelvis vil overordnede, klart etablerte verdier som sikkerhetsmålene i informasjonssikkerhet: konfidensialitet, integritet og

tilgjengelighet stå sentralt. Imidlertid vil *hva*, og hvilke verdier som ligger til grunn i de ulike sikkerhetsmålene kunne variere stort. Som det fremkommer i oppgavens forstudie hevder Lundgren og Möller (2017, s. 4) at informasjonssikkerhet er interesserelativt. Kulturrelaterte betingelser som kunnskap, tro, verdier og normer (Schiefloe, 2011, s. 198) vil derfor være avgjørende for *hva* som betraktes som farlig. Kultur kan dermed forstås som som bestemmende for hvordan en forstår sikkerhetskultur.

En kollektiv forståelse av *hva* som er farlig vil i et avgrenset område som en virksomhet vil være relativt oppnåelig sammenlignet med en enighet i et nasjonalt perspektiv. I utgangspunktet kan en gitt kontekst som det digitale aspektet forstås som en bedring av forutsetningene for at de ulike aktørene skal besitte en lik forståelse av sikkerhetskultur. Tatt forrige avsnitt i betraktning, kan det tenkes at konteksten må være avgrenset til et strukturelt nivå for at en gitt kontekst skal bidra til å bedre forutsetningene. For sikkerhetskultur i en overordnet digital kontekst er ikke denne avgrensningen reell. Sikkerhetsarbeid i Norge er et felles ansvar, som per definisjon innebærer at arbeidet også med sikkerhetskultur vil foregå på alle nivå. I lys av teorigrunnlaget og arbeidet med sikkerhetsarbeid i Norge er det dermed ikke rimelig å forvente en unison forståelse. Dessuten er konteksten er preget av et dynamisk omfang og uklare rammer, som i seg selv svekker forutsetningene for en unison forståelse av sikkerhetskultur i en digital kontekst.

6.2 Sikkerhetskultur i digital kontekst

Konteksten innebærer at de ulike aktørene, til tross for en tilsynelatende felles interesse for digital sikkerhet, vil være preget av respektives posisjon og plassering i samfunnets. Aktørens rolle og plassering, og dermed interesse, gjenspeiler hvordan respektive forholder seg til begrepet sikkerhetskultur. Under tittelen "Hva er sikkerhetskultur?", skriver NorSIS (2018, s. 9) blant annet følgende : "Digital sikkerhetskultur handler om å beskytte digitale verdier fra ulike former for trusler som rettes mot innebygde sårbarheter. Den kan derfor forstås som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til alt som er digitalt.". Det kan se ut til at NorSIS tar konteksten for gitt, da de selv utelukkende opererer i en digital kontekst.

I det vi vil beskrive som NSMs forsøk på å definere sikkerhetskultur i *Risiko 2017* (NSM, 2017) er elementene som fremkommer forholdsvis like de som fremkommer i NorSIS sin beskrivelse. Ifølge NSM er sikkerhetskultur "(...) summen av de ansattes kunnskap, motivasjon, holdninger og atferd" (s. 37). Vi omtaler sitatet som et forsøk da definisjonen kan se ut til å mangle et vesentlig aspekt. Definisjonen innlemmer ikke elementenes relasjon til sikkerhet, og samsvarer derfor i større grad med en definisjon av kultur. Sitatene synliggjør imidlertid at det eksisterer en relativ klar enighet om hva som ligger i kulturdelen av begrepet. Det kan med andre ord se ut til at det er kultur i kombinasjon med sikkerhet i en digital kontekst som utfordrer den felles forståelsen.

Sammenligner en teoretikeres definisjoner av sikkerhetskultur, eksempelvis definisjonene til og Koch og Richter (2004, s. 705) og The Health and Safety Commission i Aven et al. (2004, s. 34), kan en se at elementene som vektlegges forholdsvis like. Videre er begge definisjonene datert 2004, som synliggjør at det allerede da eksisterte en noenlunde enighet om sikkerhetskultur. Tross det, henviser ingen av aktørene innlemmet i oppgaven til sikkerhetsteori i forbindelse med beskrivelser av begrepet. I dokumentene hvor sikkerhetskultur anvendes, gir flertallet av aktørene forholdsvis vage og forsiktige beskrivelser av hva de legger i begrepet sikkerhetskultur. En gjenganger er beskrivelser som formidler hvordan begrepet *kan* forstås. Hvorfor verken overnevnte sitat eller andre, er tilknyttet en teoretisk forankret definisjon er vanskelig å si. Uten å spekulere for mye, kan det tenkes å ha en sammenheng med problematikken knyttet til at det i teorien ikke fremkommer en definisjon som gjelder uavhengig av strukturelt nivå. Funnene viser imidlertid at beskrivelsene innlemmer elementer som i stor grad samsvarer med innholdet i teoretiske definisjoner. Det er derfor, til tross for manglende kildehenvisning, ikke helt utenkelig at det aktører formidler er basert på teoretisk forankrede definisjoner.

Manglende kildehenvisninger i dokumentene kan beskrives som en gjennomgående trend. I dokumentene blir det ved flere tilfeller hevdet og påstått ulike forhold som ville vært interessant å se nærmere på, men som ikke lar seg gjøre da kildehenvisninger uteblir. Manglende henvisninger i foreliggende tekster svekker ikke bare oppgavens empiriske datagrunnlag, men også våre forutsetninger som forskere. Digital sikkerhet er preget av forhold som tidligere ikke engang eksisterte, og som et

resultat blir tradisjonell sikkerhetsteori utfordret. I lys oppgavens teorigrunnlag, om sosialkonstruktivisme og diskurs, og videre makten sentrale aktører besitter, kan det aktørene formidles oppfattes som *sannheten*. Vårt utgangspunkt som forskere kan dermed forstås som påvirket av omstendighetene vi studerer. Dette diskuteres imidlertid nærmere i kapittel 4.6, Oppgavens kvalitet.

Funnet som fremstilles i kapittel 5.5, Ukorrekt fremstilling av forskning, er et glimrende eksempel på hvorfor kildehenvisninger er viktig. Funnet synliggjør ikke bare viktigheten av kildehenvisninger i denne studien, men alltid. I et innlegg skrevet av Glasspaper (2018), med tittelen "Hva skal til for å skape en sikkerhetskultur?", er det flere forhold som skurrer. Tittelen i seg selv strider mot grunnleggende forutsetninger for kultur, og dermed også sikkerhetskultur. Forfatteren av innlegget fremstiller sikkerhetskultur som noe som enten eksisterer eller ikke, som med utgangspunkt i kulturteori kan forstås som ukorrekt. Teksten resulterte at vi ble kritiske til den opprinnelige rapporten som innlegget henviser til. Det viste seg imidlertid at det ikke var primærkilden som baserte seg på en feilaktig forståelse av sikkerhetskultur. Glasspapers ukorrekte fremstilling kan sies å være uheldig av flere årsaker. I første omgang vil det kunne svekke troverdigheten til rapporten og dens forfattere uten grunn. Videre vil det kunne bidra til misforståelser og skape usikkerhet for lesere som allerede besitter en viss kompetanse. Hvorvidt denne feilaktige fremstillingen skyldes lite gjennomtenkt språkbruk, dårlig oversettelse eller rett og slett en gal forståelse av kultur kan vi bare spekulere i. Dette er videre ikke bare et eksempel på hvorfor det er viktig at forfatter oppgir kilder, men også at det er viktig å være kritisk til kildene en bruker.

6.3 Sikkerhetskultur i en digital kontekst anses som viktig

Tross resultater som indikerer at det foreligger ulike forståelser av hva sikkerhetskultur i en digital kontekst er, viser studien en forholdsvis lik forståelse av viktigheten av sikkerhetskultur og arbeidet med det. Faktumet at aktørene innlemmer forholdsvis like elementer i sine beskrivelser kan tolkes som at det foreligger en viss felles og forholdsvis lik idé om hva sikkerhetskultur omfatter.

Ifølge NorSIS var det de omtaler som informasjonssikkerhetskultur et "velkjent" begrep da de startet en kartlegging av norsk informasjonssikkerhetskultur. Som de

selv har poengtert, eksisterte det imidlertid lite litteratur om hva konseptet faktisk innebar. Hvorvidt begrepet informasjonssikkerhetskultur var et velkjent begrep kan dog diskuteres. I lys av foregående diskusjon om konteksten NorSIS opererer i, kan det tenkes at de ikke skiller mellom sikkerhetskultur og sikkerhetskultur i digital forstand. Hvorfor NorSIS omtaler begrepet som velkjent er usikkert, da de verken forklarer eller viser til andre kilder. Det kan imidlertid tenkes at det er en påstand som løftes på bakgrunn av NorSIS sine egne undersøkelser.

NorSIS hevder videre at en generell oppfatning av digital sikkerhetskultur er at konseptet omhandler verdier, holdninger og atferd (Malmedal og Røislien, 2017, s. 13). Hvorvidt NorSIS' påstand er tilfelle kan vi ikke bekrefte. Det er imidlertid avdekket flere forhold som styrker påstanden. Oppfatningen NorSIS beskriver inkluderer de samme elementene som typisk tilhører kultur, som ifølge våre funn synes å være en tilsynelatende enighet om. En forholdsvis lik idè om hva sikkerhetskultur omfatter, er til tross for ulik forståelse av hva det er, ikke være rent unaturlig. Som diskutert, vil kultur være bestemmende for sikkerhetskultur. I henhold til oppgavens teori om arbeid med sikkerhet, er epoken vi befinner oss i nå preget av fokus på organisasjon og sikkerhetsledelse (Aven et al., 2004, s. 27). Dette innebærer at relasjoner og samspillet mellom ulike faktorer i organisasjoner og samfunn vektlegges.

Videre er det som Sjølstad, Høie og Daler (2010, s. 37) formidler, menneskene rundt teknologien som utgjør den største sikkerhetsmessige utfordringen. I lys av oppgavens systembeskrivelse og teori, fremstår sikkerhetskultur som et sentralt begrep i arbeidet med sikkerhet i Norge. Som adressert tidligere vil aktørene være i besittelse av ulike verdier, men gitt en norsk kontekst kan det tenkes at de overordnede verdiene vil bære preg av noen grunnleggende likheter. Det er dermed ikke uten grunn at sikkerhetskultur settes på agendaen av aktørene. Antall dokumenter synliggjør i seg selv at sikkerhetskultur er særlig fremtredende i sikkerhetsarbeidet, og dermed implisitt også for arbeidet med sikkerhetskultur.

6.4 Ulike forståelser forårsaker ulike tilnærminger

Norge utgjør et av verdens mest digitaliserte land, som krever et kontinuerlig arbeid og tilpasning av landets sikkerhet. Foreliggende tekster synliggjør at arbeidet

innebærer at sikkerhetskultur settes på dagsordenen og blir prioritert. Som Aven et al. (2004, s. 32) formidler kan sikkerhetskultur bidra til å å styre virksomheter mot definerte mål. I lys av det og studiens funn kan måling av sikkerhetskultur beskrives som et hett tema.

Funnene knyttet til måling synliggjør at det aktørene imellom foreligger uenigheter knyttet til hvordan sikkerhetskultur kan, bør og/eller skal måles. I lys av den sprikende forståelsen av sikkerhetskultur kan uenigheten anses som åpenbar. I et arbeid mot et definert mål, vil forståelsen av målet være bestemmende for veien dit. Er forståelsen ulik vil også veien dit bære preg av tilsvarende variasjoner. For eksempel vil en vellykket bygningsprosess være avhengig av en forestilling om hva et hus er. Hvorvidt en idé er tilstrekkelig avhenger av målsetningen, men skal en bygge et solid og robust hus forutsetter det en avklaring med tanke på materialer og fremgangsmåter. Eksempelet er overførbart til til arbeidet med sikkerhetskultur, da tilnærmingen til måling vil være bestemmende for måleresultatet. Med andre ord vil resultatet være sterkt avhengig av hva en måler, og hvordan en måler det vil være bestemmende for resultatet. En manglende unison forståelse kan dermed beskrives som uheldig med tanke på det potensielle utbytte av arbeidet som legges ned i måling av sikkerhetskultur.

Som det fremkommer i kapittel 5.6 påstår NorSIS at studier av digital sikkerhetskultur i stor grad fokuserer på atferdsdimensjonen (Malmedal og Røislien, 2018, s. 13). Knyttet til denne påstanden savnet vi kildehenvisninger, da vi ikke besitter en tilsvarende oppfatning. Hvorvidt dette er tilfelle er ikke noe denne studien verken kan bekrefte eller avkrefte. Det kan dog tenkes at det kan være tilfelle, da måling av atferd for virksomheter uansett vil gi et bidrag i positiv forstand. I lys av både oppgavens teori og empirisk data er det imidlertid klart at målinger utelukkende basert på atferd ikke vil kartlegge underliggende faktorer og den faktiske sikkerhetskulturen.

Som det videre fremkommer i resultatene blir det også av NSM påpekt at måling av sikkerhetskultur ikke utelukkende kan baseres på atferd. Tross det, skriver de i et innlegg som tilsynelatende skal svare på hvorvidt en kan måle sikkerhetskultur, utelukkende om hvordan en kan måle atferd. De adresserer i liten grad spørsmålet de selv stiller seg i innleggets overskrift: “Kan vi måle sikkerhetskultur?”. Hvorvidt dette

skyldes et lite gjennomtenkt valg av overskrift eller noe annet, er vanskelig å bedømme, men kan uansett anses som uheldig. NSM er tilsynelatende enig med NorSIS om at måling av atferd er ikke er tilstrekkelig, men evner ikke å formidle en annen måte å utføre målinger på. NSMs innlegg og Styris presentasjon svekker kan imidlertid forstås som svekkende for NorSIS sin uttalelse om at studier i stor grad fokuserer på atferd.

Et mål på atferd er imidlertid et mål på noe, som i bunn og grunn kan utgjøre den faktiske årsaken til at atferdsdimensjonen i flere tilfeller er det eneste som vektlegges. For det første er atferd langt enklere å måle enn de andre dimensjonene som eksempelvis NorSIS legger til grunn for måling av sikkerhetskultur. For det andre foreligger det ingen regulatoriske krav som legger føringer for at virksomheter skal gjennomføre målinger. Det vil videre være naivt å tro at alminnelige virksomheter vil prioritere ressurser på noe som per definisjon ikke er pålagt. Fåtallet av virksomheter har sikkerhet som kjernevirksomhet, og drift vil dermed være preget av en målsetting tilknyttet økonomi. Måling kan dog, til tross for at lovverket ikke eksplisitt krever det, forstås som en naturlig del av sikkerhetsbevisstheten som vektlegges i lover og forskrifter. Hvorvidt virksomheter iverksetter tiltak for kartlegging kan forstås som avhengig av kulturen organisasjonen besitter.

Diskusjonen om måling av atferd kan knyttes til tilnærmingene som legges til grunn ved måling av sikkerhetskultur. En normativ tilnærming, som legger føringer for å betrakte sikkerhetskulturer som gode og dårlige, åpner særlig for at atferd utgjør en sentral parameter. Ifølge NorSIS, som legger til grunn at sikkerhetskulturer er ulike, er denne tilnærmingen upassende. NorSIS betrakter heller sikkerhetskulturer som unike og dermed ikke sammenlignbare. Med det til grunn forholder NorSIS seg til en deskriptiv tilnærming. Dette er ikke nærmere studert i oppgaven, men no vi likevel trekker frem da det belyser uenighetene om grunnleggende element som er sentrale for arbeid med sikkerhetskultur i form av måling.

Den sprikende forståelsen kan forårsake følger av betydning for verdien av det aktørene har til felles, nemlig viktigheten av sikkerhetskultur. Som diskutert er imidlertid aktørene i besittelse av en forholdsvis lik idé om hva begrepet omfatter, men eksempelvis vil hvordan de ulike elementene vektlegges kunne variere stort.

Hvordan aktørene forholder seg til måling av sikkerhetskultur synliggjør denne problematikken. Veien til målet er dermed ulik.

6.5 Fra informasjonssikkerhetskultur til digital sikkerhetskultur

I aktørenes tekster fremkommer sikkerhetskultur ofte i kombinasjon med ord som knytter begrepet til konteksten vi befinner oss i. Studiens resultater synliggjør en problematikk knyttet til språkbruk og begrep på flere måter. I lys av funnene i kapittel 5.4 kan det hevdes at ingen av begrepene aktørene benytter fanger opp dimensjonene som er i omløp i konteksten. Hva vi betrakter som dimensjoner i omløp er de elementene som respektive innlemmer i sine beskrivelser.

I første omgang er det verdt å trekke frem et ord som er særlig mye brukt: informasjonssikkerhetskultur. Begrepet har vært fremtredende i rapporter av NorSIS. I sine rapporter har NorSIS ved flere anledninger beskrevet hva begrepet dreier seg om og hvordan det kan forstås. Det er imidlertid ikke avdekket en tydelig, avklart definisjon, verken av NorSIS eller av andre. Det vi først bet oss merke i da vi ble introdusert for begrepet informasjonssikkerhetskultur, var at den digitale dimensjonen ikke fremkommer i selve ordet. Begrepet adresserer konseptets tilknytning til behandling og lagring av informasjon, men ikke avgrensningen til den digitale dimensjonen. Som tidligere påpekt, operer NorSIS i en kontekst hvor det er gitt at en forholder seg til det digitale, men begrepet kan til tross for det kritiseres for å være for lite presist.

Det kan imidlertid se ut til at NorSIS selv oppdaget at informasjonssikkerhetskultur ikke var det mest treffende begrepet, og at det fantes andre ord som i større grad adresserer det de omtalte som informasjonssikkerhetskultur. I sine rapporter gjennom de siste årene har NorSIS, som påvist i oppgavens resultat, gradvis forlatt informasjonssikkerhet-begrepet til fordel for *digital sikkerhetskultur*. I flere av deres rapporter blir det påpekt at begrepene blir behandlet som synonymer. Slik vi forstår merknaden vil det i praksis si at begrepene innebærer det samme. Ser en på hvordan begrepene behandles i *Ungdom og digital sikkerhetskultur* (2017), *Nordmenn og digital sikkerhetskultur* (2017) og *Nordmenn og digital sikkerhetskultur 2018* (2018), kan en forstå hvorfor NorSIS hevder at de behandler ordene som synonymer. I rapportene fra 2017 forstås informasjonssikkerhetskultur i relasjon til

informasjonsverdier. Det samme gjelder for rapporten utgitt året etter, men til forskjell fra de andre rapportene anvender NorSIS informasjonssikkerhetskultur istedenfor digital sikkerhetskultur. Med forholdsvis like beskrivelser til grunn kan det dermed fremstå som korrekt å hevde at ordene behandles som synonymer.

Ser en nærmere på begrepene, med tanke på kombinasjon av ord, kan det dog argumenteres for at en behandling som synonymer ikke kan rettferdiggjøres. Det at informasjonssikkerhetskultur forstås som relatert til informasjonsverdier er forholdsvis opplagt, men det er ingenting i begrepet digital sikkerhetskultur som indikerer en tilknytning til informasjon. Det kan på den ene siden dermed argumenteres for at relasjonen mellom sikkerhetskultur og informasjonsverdier resulterer i at informasjonssikkerhetskultur vil være mer presist begrep enn digital sikkerhetskultur. På den andre siden, dekker digital sikkerhetskultur den digitale dimensjonen som informasjonssikkerhetskultur-begrepet ikke fanger opp. *Digital*, slik vi forstår det, legger imidlertid føringer for at begrepet forstås som dekkende for alt som foregår digitalt. Digital sikkerhetskultur innlemmer dermed ikke avgrensningen til informasjon, slik som informasjonssikkerhetskultur. Det er dermed en vesentlig forskjell i hva begrepenes sammensetning av ord formidler. Hvorvidt det ene begrepet er mer korrekt eller presist enn det andre kan i seg selv utgjøre en omfattende diskusjon.

Poenget er at ingen av ordene innlemmer elementer som sørger for at begrepet alene formidler innholdet som gis i beskrivelsen NorSIS legger til grunn. Dersom formålet faktisk har vært å sette ord på sikkerhetskultur knyttet til behandling av digital informasjon, kan det tenkes at et ord som faktisk adresserer konseptet vil være en kombinasjon av ordene NorSIS forholder seg til. I henhold til NorSIS beskrivelser av begrepet, kan *digital informasjonssikkerhetskultur* forstås som mer treffende. Kombinasjonen resulterer i et noe mer omfattende ord, men som i det minste dekker alle elementene som er relevante for konseptet i gitt kontekst. Det kan dog se ut til NorSIS sitt formål ved endringen ikke nødvendigvis var å innlemme alle elementene.

I likhet med *Nordmenn og digital sikkerhetskultur 2018* (2018) gis det også i *Trender og trusler 2018-2019* (2018) en beskrivelse av digital sikkerhetskultur. Med første øyekast ser beskrivelsen i stor grad ut til å korrelere med hva som formidles i de andre

rapportene, men det er én vesentlig forskjell. Ifølge rapporten kan digital sikkerhetskultur forstås " (...) som de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til alt som er digitalt." (2019, s. 9). Digital sikkerhetskultur, som tidligere ble relatert til informasjonsverdier, betraktes nå i relasjon til *alt som er digitalt*. Denne beskrivelsen samsvarer i det minste med hvordan vi forstår *digital*, men er imidlertid ulik NorSIS sine andre beskrivelser av digital sikkerhetskultur.

I lys av ovennevnte forhold kan det dermed forstås som ukorrekt av NorSIS å hevde at ordene behandles som synonymer. Det skal nevnes at det i *Trusler og trender 2018-2019* (2019) ikke blir påpekt at informasjonssikkerhetskultur og digital sikkerhetskultur behandles som synonymer. Hvorvidt dette skyldes at informasjonssikkerhetskultur ikke fremkommer i rapporten i det hele tatt, eller om NorSIS ikke lenger betrakter de som synonymer er ikke klart. Det som i motsetning er klart, er at NorSIS, gjennom gradvise og tilsynelatende lite synlige endringer, ikke bare har endret begrep, men også beskrivelsen av det mest sentrale begrepet i sitt arbeid.

6.6 Utvikling i begrepsbruk

Endringen i begrepsbruken som adresseres i forrige kapittel kan i utgangspunktet anses som en positiv utvikling i arbeidet med sikkerhetskultur. Beskrivelsen som innlemmer "alt som foregår digitalt" medfører imidlertid per definisjon en utvidelse av NorSIS sitt arbeidsområde. Det kan dog argumenteres for at det ikke utgjør særlig forskjell, da verdier i det som foregår digitalt i hovedsak kan forstås som relatert til informasjon.

Det vi ikke betrakter som positivt, og som vi henger oss mer opp i, er hvordan endringen har utspilt seg. Da endringen i begrepsbruk først ble identifisert, oppstod spørsmål knyttet til hvorfor NorSIS i det hele tatt skulle forlate informasjonssikkerhetskultur til fordel for digital sikkerhetskultur. I praksis utgjorde endringen tilsynelatende ingen forskjell, da begrepene uansett ble behandlet som synonymer. Hvorfor NorSIS valgte å forholde seg til ordene som synonymer til tross for at en enkelt kan argumentere for at de ikke er det, kan trolig forstås som et resultat av at NorSIS sin hovedundersøkelse er basert på informasjonssikkerhetskultur.

NorSIS har dog aldri påstått at begrepene *er* synonymer. Det skal imidlertid sies at ved å bruke data fra undersøkelser basert på informasjonssikkerhetskultur som datagrunnlag for studier om digital sikkerhetskultur er det i praksis det de gjør.

Videre forstås ikke digital sikkerhetskultur som noe særlig mer treffende enn informasjonssikkerhetskultur med tanke på konsept og kontekst. Ser en på det totale bildet, hvor både begrep og beskrivelse av begrepet er endret, kan det dog tenkes at NorSIS faktisk ikke var interessert i å innlemme informasjon-dimensjonen i det "nye" begrepet. Utviklingen som er avdekket i rapportene, kan nærmest tolkes som en kamuflert begrepsendring. Det er ikke gitt, men uansett intensjon, kan det stilles spørsmål til hvorfor NorSIS ikke gjorde et nummer ut av endringen. Det er ikke utenkelig at NorSIS selv anser endringen som en korrigering, og som dermed ubetydelig for andre enn dem selv. Det kan stilles spørsmål til hvilke signaler inkonsekvente beskrivelser og endringen totalt sett utgjør.

Det kan tenkes at utfasingen av begrepet informasjonssikkerhetskultur til fordel for digital sikkerhetskultur er et resultat av utvikling av NorSIS' forståelse. Selve endringen kan sees i lys av teori av Foucault om at tankesystemer og oppfatninger endrer seg over tid (Foucault, 1999, s. 181). Videre er diskurser omkring bestemte fenomener, ifølge Foucault, betinget av kunnskap og sosiale maktstrukturer (Østbye et al, 2013, s. 95). Ifølge Foucault skyldes ikke utviklingen nødvendigvis økning i fornuft, men snarere en fjerning av overtro og fordommer. Dette er nok litt fjernt fra NorSIS' utfasing av begrepet, da endring i begrepsbruk tvilsomt fjerning av overtro eller fordommer. Økt innsikt og kunnskap om tema og fenomen kan dog være en bidragsfaktor til endring også i begrepsbruk. I henhold til ulike teorier knyttet til makt vil NorSIS kunne påvirke andre aktører i Norge gjennom sine rapporter. Som følge av NorSIS' posisjon i samfunnet kan måten de anvender og forstår begrepet også legge føringer for hvordan andre aktører forholder seg til begrepet, og kan derfor også bidra til at diskursen omkring begrepet endrer seg over tid. Dette er imidlertid ikke utelukkende gjeldende for NorSIS, men for samtlige aktører.

6.7 Makt i diskursen

Resultater som særlig knyttes til forskningsspørsmål 1 kan trekkes frem i flere av diskusjonsmoment som i større grad er relatert til forskningsspørsmål 2, om hvordan

aktørers dokumenter påvirker arbeidet med sikkerhetskultur. Hvorfor og hvordan aktørenes formidling og anvendelse av begrepet har innvirkning på arbeidet med sikkerhetskultur, kan på bakgrunn av oppgavens teorigrunnlag, forklares av flere faktorer. I teorien presenteres definisjonsmakt, som utgjør en sentral rolle for aktørenes påvirkning på arbeidet med sikkerhetskultur. Samtlige aktører i oppgaven besitter posisjoner og roller i samfunnet som forstås som i besittelse av en form for definisjonsmakt. Med til grunn kan det hevdes at aktører vil kunne påvirke arbeidet med sikkerhetskultur i form av både det som kan betraktes som intensjonelle handlinger, men også som følge av faktorer som virker inn uavhengig av hensikt. Intensjonelle handlinger kan forstås som konkrete forhold som eksempelvis strategier, oppfordringer, tiltak, krav og andre bestemmelser. Også påstander og generelle uttalelser kan forstås som handling basert på en hensikt om å formidle et visst budskap.

I lys av hva Foucault formidler, vil diskurser, strategier, praksis og institusjoner legge føringer for hvordan verden forstås. Gjennom utallige prosesser knyttet til disse forholdene blir *sannheten* til. De sosiale mekanismene som kunnskap og makt, som i denne sammenheng fremkommer i tekster, kan i henhold til Foucault forstås som bestemmende for hva som blir sagt, tenkt og gjort. Slik kan det sies at aktørene også påvirker arbeidet implisitt kun ved at de ytrer og publiserer meninger om sikkerhetskultur. Videre kan, som Berg (2018) skriver, " (...) makt stanse makt", som i praksis vil kunne bety at aktørene vil kunne svekke hverandres ord.

I lys av teorigrunnlaget om diskurs og maktforhold, kan det være fruktbart å reflektere over vårt eget bidrag. Oppgavens hensikt er å gi et bidrag til sikkerhetsarbeidet i Norge. Ved å påpeke sprikende forståelse av sikkerhetskultur, kritisere ordlyd og presentasjon av begreper, tar vi en rolle der vi sier at noe er rett og noe er galt. Vi kan som sådan tenkes at også vi bidrar til diskursen omkring sikkerhetskultur.

6.8 Makt i tekster

I lys av besittelse av makt uavhengig av intensjon, kan uenigheten om måling av sikkerhetskultur mellom NorSIS og CLTRe trekkes frem. NorSIS utgjør en ledende aktør i sikkerhetsarbeidet i Norge og vil ifølge teori om definisjonsmakt. I utgangspunktet vil NorSIS besitte en tilsynelatende større makt enn et konsulentfirma

som CLTRe. Dette må imidlertid ikke være tilfelle. I henhold til oppgavens teorigrunnlag vil flere forhold knyttet til tekster virke inn på aktører og teksters maktforhold. Vi referer til Berge (Berge et al., 2013) som deler inn forholdet mellom makt og tekst i tre dimensjoner.

Ifølge Berges beskrivelser av den første dimensjonen, *tekster som unik handling*, kan tekster ha eller skaffe makt som unik og individuell handling både avhengig og uavhengig av skaperens status og institusjonelle posisjon (s. 30). Avhengigheten Berge legger til grunn, samsvarer med hvordan vi betrakter definisjonsmaktens innvirkning. Poenget er imidlertid at tekst kan ha eller skaffe makt uten at skaperen i utgangspunktet besitter betydelig makt. Med det til grunn kan en tekst av CLTRe derfor ha en betydelig makt, som potensielt sett kan overgå definisjonsmakten som styrker tekster av NorSIS. Det er dog lite realistisk at et relativt ukjent konsulentfirma gjennom en tekst vil overskride makten NorSIS' besitter som følge av sin posisjon. Uavhengig av tekstens maktstyrke, vil det i realiteten trolig være NorSIS og deres publikasjoner som innehar mest makt. Faktumet at NorSIS kritiserer CLTRes arbeid vil ha innvirkning for hvordan CLTRes publikasjoner oppfattes. Denne studien er imidlertid ikke en lingvistisk tekstanalyse**,** og vi har heller ikke forutsetninger for å betrakte det faktiske maktforholdet.

Også i tekstmaktdimensjon 2, t*ekster som forekomst av en tekstnorm*, kan definisjonsmakt anses som inngående. *Nasjonal strategi for digital sikkerhe*t (Departementene, 2019) kan trekkes frem som et eksempel på en tekst i overensstemmelse med Berges andre tekstdimensjon. Strategien er utgitt av sentrale departement i Norge og kan betraktes som en retningsgivende tekst, som i henhold til teorigrunnlaget medfører at teksten i seg selv har makt (s. 31). En tekst i tråd med tekstdimensjon 2 vil derfor ha en naturlig stor gjennomslagskraft. Videre kan *Nasjonal strategi for digital sikkerhe*t (Departementene, 2019 også ses som inngående i tekstdimensjon 3, *tekst som representasjon av en viss ideologisk posisjon eller diskurs*. I det gjeldende sikkerhetsparadigmet er det uten tvil en oppfatning om at sikkerhetskultur er viktig, uavhengig av hvordan aktører formidler det. Ved at strategien presenterer og repeterer sikkerhetskultur knyttet til både delmål og tiltak, kan det sies at den bekrefter og forsterker en allerede ideologisk posisjon - sikkerhetsparadigmet og *sannheten* om at sikkerhetskultur er viktig og riktig å

fokusere på. I oppgavens empirigrunnlag er det ikke én aktør som påstår at sikkerhetskultur *ikke* er viktig.

6.9 Manglende forutsetninger til å forstå digitale sikkerhetsbrudd

Utdanning og kompetanse vil bidra til bedre forståelse for digital sikkerhet og dermed også forutsetningene for å unngå sikkerhetsbrudd. Et fullstendig fravær av sikkerhetsbrudd vil imidlertid i henhold til teorien om normale ulykker være nærmest umulig. Ifølge Perrow vil det i noen teknologiske systemer forekomme ulykker, uavhengig av hvor mye ressurser en bruker på sikkerhet. Ifølge hans teori har tett koblede og komplekse systemer særegne og strukturelle trekk som gjør ulykker "normale". Digitale systemer kan forstås som system av typen Perrow omtaler. Selv med et høyt kompetanse- og kunnskapsnivå vil det dermed være vanskelig å oppnå en tilstrekkelig forståelse for systemene og dermed opphav til sikkerhetsbrudd.

Ifølge Westrum (i Reason, 1997, s. 38) vil det i forkant av en ulykke forekomme faresignaler, men som ikke vil fanges opp med mindre en besitter en forestilling av ulykken som vil oppstå. Reason omtaler dette som "impossible accidents", da mennesker aldri vil være kapable til å forutse fremtiden. Det er ikke en gang et faktum som avhenger av kunnskap, men den faktiske virkeligheten. Med teori om normal ulykker til grunn, vil dermed ulykker forekomme selv med uendelige ressurser. Perrows teori om normale ulykker kan anses som noe fatalistisk, da hendelsene ikke anses som mulige å avverge med menneskelig inngripen. Skal en kunne fullt og helt forhindre sikkerhetsbrudd må systemene avvikles.

I dagens digitaliserte samfunn er vi avhengige av komplekse systemer. En fullstendig avvikling av disse systemene vil være urealistisk. Samfunnet og dets driv fremover er og vil være avhengig av teknologi og komplekse systemer. Ifølge Bento (2001) er to av årsakene til at MTO-problemer fortsatt eksisterer: 1) "det tas ikke hensyn til mennesket når nye teknologier introduseres", og 2) "det tas ikke hensyn til menneskets begrensninger ved drift, vedlikehold og utprøving av tekniske systemer" (s. 4). Logikken som ligger til grunn er at systemer er kompliserte og tar ikke hensyn til menneskers begrensninger og forståelsesrammer. Bentos (2001) forståelse av MTO-problemer kan knyttes til det Schiefloe (1999, s. 23) omtaler som et kulturelt etterslep. Mennesker, eller institusjoners utvikling, har ikke de nødvendige

forståelsesmessige rammene for å håndtere den materielle utviklingen. I henhold til Foucault og hans perspektiv på utvikling av kunnskap vil det imidlertid være fullt mulig å endre forståelsesmessige rammer. Kompetansehevende tiltak, bevisstgjøring og klargjøring av konsepter, samt begrep, bidra til å endre de forståelsesmessige rammene som medfører begrensninger i forståelsen av hendelsesforløp. Dersom den forståelsesmessige rammen endres, kan det tenkes at det i større grad vil være mulig å forhindre uønskede hendelser i digitale systemer.

Perrows teori tar utgangspunkt i atomkraftverk og andre teknologiske systemer som kan føre til fysiske hendelser, og gjerne med fare for tap av liv. Med andre ord var Perrows teori om normale ulykker utviklet lenge før digitaliseringen virkelig gjorde sitt inntog. Uønskede hendelser i en digital kontekst er av en annen karakter, som frem til nå i hovedsak har vært forbeholdt konsekvenser i form av tap i økonomi og omdømme. Samfunnets stadig økende avhengighet til kritisk infrastruktur i form av digitale løsninger øker samtidig sårbarheten. Hendelser, som eksempelvis nedetid, i digitale verdikjeder som påvirker infrastruktur kan helt klart resultere i konsekvenser som berører mennesker i fysisk forstand.

I NSRs undersøkelser fra 2016 og 2018 oppgis uflaks og tilfeldigheter som årsak til informasjonssikkerhetsbrudd. På spørsmålet "var noen av følgende faktorer årsak til at sikkerhetsbrudd oppsto?" oppga 67 % av respondentene uflaks eller tilfeldigheter som årsak. Resultatet fra undersøkelsen er i seg selv oppsiktsvekkende, men det er flere forhold som er verdt å kommentere. Bruk av ordet flaks kan være en indikator på at respondentene mangler forståelse for hvordan et sikkerhetsbrudd utvikler seg.

Undersøkelsen er imidlertid utformet av NSR med forhåndsdefinerte svaralternativ, som etter etter vår tolkning vil kunne svekke resultatet knyttet til spørsmålet som stilles. Av flere grunner kan det anses å være uheldig at *uflaks og tilfeldigheter* legges frem som en mulig årsak. For det første vil en fremleggelse av uflaks som et alternativ legge til rette for at respondenten kan fraskrive seg ansvaret for at bruddet oppstod. Det kan være et bevisst valg, men også som følge av manglende forståelse for utviklingen av sikkerhetsbruddet. For det andre vil hva NSRs forståelse av uflaks ikke nødvendigvis samsvare med respondentenes forståelse av begrepet. Eksempelvis hevder NSR at resultatene er et tegn på at virksomheter i liten grad oppfatter angrep

som spesifikt rettet mot dem. Dette er kun en av mange mulige forhold å knytte opp uflaksen til. Eksempelvis det være tilfelle at respondenten betraktet uflaks som i betydning av hvorvidt *de* ikke klarte å forhindre hendelsen. Det kan derfor argumenteres for at NSR er i overkant påståelige i sin betraktning.

6.10 Arbeid med sikkerhetskultur via virksomheter

Som diskutert synliggjør studien at sikkerhetskultur i praksis vil forstås og dermed tilsynelatende påvirke ulikt avhengig av nivå i samfunnet. Eksempelvis gjenspeiler de ulike tilnærmingene til måling dette. NorSIS undersøker sikkerhetskultur både i virksomheter og nasjonalt, mens CLTRe utelukkende undersøker på organisasjonsnivå. Forskjellene kan belyse utfordringene knyttet til faktumet at sentrale aktører legger mye av ansvaret for arbeidet med sikkerhetskultur over på virksomheter. *Nasjonal strategi for digital sikkerhet* (2019) vektlegger at fellesskapet må utvikle tiltak som kan styrke den digitale sikkerheten i Norge. Strategiens målgruppe er imidlertid myndigheter og virksomheter, og med det til grunn er tiltakene som presenteres i hovedsak rettet mot overnevnte. Det i seg selv er ikke problematisk, tvert imot er det heller positivt at det finnes en strategi med konkrete mål og tiltak for arbeid sikkerhetskultur.

Strategien kan i lys av maktforholdet diskutert tidligere betraktes som sterkt normgivende og førende for arbeidet. Som påpekt tidligere vil virksomheter naturligvis ha andre intensjoner enn en aktør med sikkerhetsinteresser for nasjonen Norge. Fåtallet av norske virksomheter har sikkerhet som kjernevirksomhet, og vil dermed være drevet av økonomisk gevinst. Hva nasjonale sikkerhetsaktører legger i begrepet sikkerhetskultur vil med det til grunn ikke nødvendigvis samsvare med hvordan en alminnelig virksomhet oppfatter det. Det er imidlertid klart at arbeidet med sikkerhetskultur ikke utelukkende foregår i virksomheter. Basert på gjennomgåtte dokumenter er det imidlertid mye som ser ut til å foregå på organisasjonsnivå. Som også diskutert tidligere relateres sikkerhetskultur ofte til organisasjoner, i både sikkerhetsteori og organisasjonsteori. Det er derfor ikke rent unaturlig at virksomheter blir tildelt ansvar.

I henhold til Avsnitt 5, Artikkel 40 i personvernopplysningsloven stilles det krav til at medlemsstatene, tilsynsmyndigheter, Personvernrådet og Kommisjonen skal

oppmuntre til at det utarbeides atferdsnormer i virksomheter. Det er imidlertid ingen krav til at virksomheter skal utarbeide og implementere en atferdsnorm. Det kan derfor tenkes at de som faktisk ville hatt størst utbytte av en atferdsnorm er de som ikke prioriterer det. Videre vil de virksomheter som faktisk velger å utvikle en atferdsnorm besitte stor handlingsfrihet med tanke på innhold. Normen 5.3 er et eksempel på en atferdsnorm. Normen gir konkrete regler og retningslinjer for hvordan virksomheter skal innrette seg for å etterleve krav. Den fokuserer imidlertid lite eksplisitt på sikkerhetskultur, men faktumet at atferdsnormen faktisk eksisterer kan si mye om sikkerhetskulturen i helsesektoren.

Ifølge NorSIS' rapport, *Trusler og Trender 2018-2019* (2018), kan digital sikkerhetskultur forstås som "(...) de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til alt som er digitalt" (s. 9). Sitatet er hentet fra et avsnitt som videre betrakter digital sikkerhetskultur i en organisasjon, men som sitatet viser er ikke sikkerhetskultur forbeholdt organisasjoner. Dette er ingen nyhet, men dog verdt å understreke for den videre diskusjonen av sikkerhetskultur i organisasjoner.

Kultur i en organisasjon vil ifølge Guldenmund (2007, s. 726) være "determined largely by external (national, regional) conditions and the (educational, social-economic, religious) background of its workforce". Med andre ord vil de overnevnte elementene som ligger til grunn for enkeltindivider være noe en tar med seg som ansatt i en organisasjon. Som også Schiefloe (1999, s.6) skriver er mennesker bærere, brukere og formidlere av kultur. Hvilke mennesker som inngår i en organisasjon vil dermed være bestemmende for organisasjonskultur og dermed også sikkerhetskulturen. Mennesker som utgjør ansatte i en organisasjon er formet forkant av ansettelsesforholdet og vil derfor prege kulturen i organisasjonen. I henhold til teori av Schiefloe og Guldenmund er det ikke urimelig å anta at eksisterende holdninger, erfaringer og verdier blir integrert i organisasjonskulturen. Med dette til grunn kan det derfor argumenteres for at det er behov for fokus på sikkerhetskultur før et ansettelsesforhold. Som Guldenmund (2007, s. 726) uttrykker, er ikke organisasjoner lukkede systemer, og kulturen vil være preget av eksterne faktorer og bakgrunnen til arbeidsstyrken. NorSIS' forståelse av digital sikkerhetskultur vil inkludere mennesker på individnivå, så vel som på organisasjonsnivå.

Grunnskoleutdanning og andre kompetansehevende tiltak kan dermed utgjøre et viktig moment. Vi påstår ikke at utdanning og kompetanse ikke er i fokus, men forsøker heller å understreke at det er flere forhold som bekrefter viktigheten av fokus på kompetanseheving også før et ansettelsesforhold.

Sikkerhetsteoretiske definisjoner er i stor grad hentet fra teoretikere som tar for seg sikkerhet i et organisatorisk perspektiv. Det er derfor ikke uten grunn de ikke fokuserer på individnivå, da det er et er organisatoriske ulykker og systemer som utgjør fokuset. Det som imidlertid er nytt i dagens samfunn, og som disse teoriene kanskje ikke fanger opp, er at sikkerhetsutfordringer knyttet til informasjonssikkerhet kan møte mennesker i alle aspekt av livet - ikke bare i organisasjoner eller i drift av systemer. De dynamiske sikkerhetsutfordringene digitaliseringen medfører er i liten grad adressert i sikkerhetsteoriene, da det er ikke lenger et like klart skille mellom arbeidsliv og privatliv. Det kan derfor hevdes at det er et økende behov for sikkerhetskultur på individnivå, da mennesker forholder seg til digitale systemer også i den private sfæren. Aktørene som utgjør empirigrunnlaget har ulike samfunnsoppdrag og fokusområder. De er like fullt aktører med sikkerhetsinteresser med hensikt om å bidra til økt sikkerhet i nasjonen Norge. For dette formålet, kan det være hensiktsmessig med en definisjon som treffer uavhengig strukturelt nivå.

6.11 Forståelsens betydning for arbeidet med sikkerhetskultur

Hver enkelt aktørs forståelse, uavhengig av overensstemmelse med sikkerhetsteori, har i seg selv innvirkning for arbeidet med sikkerhetskultur. Samtlige aktører forstås som i besittelse av definisjonsmakt, og i henhold til Berg (2018a) vil makt kunne stanse makt. Aktørenes forståelse kan dermed forstås å virke mot hverandre. Sprikende forståelse av sikkerhetskultur vil som diskutert dermed virke inn på arbeidet med sikkerhetskultur. Som tidligere adressert vil ulike forståelser forårsake virkninger som preger arbeidet som aktørene intensjonelt legger ned. I et allerede komplekst bilde bidrar med andre ord ulike forståelser til å komplisere bildet ytterligere.

Som diskutert er det en felles enighet om viktigheten av sikkerhetskultur, men som kan forstås å miste sin verdi som følge av den sprikende forståelsen aktørene imellom. Ikke bare svekker det arbeidet med sikkerhetskultur i form av konkrete handlinger,

men også i form av andre forhold. En sprikende forståelse i arbeidet med sikkerhetskultur kan som diskutert forårsake en tilsvarende arbeidsprosess. Det er videre verdt å påpeke faktumet at sentrale aktører er uenige kan tenkes å sende ut negative signaler i samfunnet. Når de som kan forstås som ledende aktører enes om målet, er det utfordrende for andre å forholde seg til hva som formidles.

Denne studien synliggjør hvordan arbeidet med sikkerhetskultur vil påvirke av aktørers forståelse av sikkerhetskultur. Som diskutert vil forståelsen være av betydning for hvordan en arbeider med sikkerhetskultur i form av hva som gjøres, hvordan, og hvem som pålegges ansvar. Studien er imidlertid av en vitenskapsteoretisk karakter, og resultatene må tolkes deretter. Det kan dog tenkes at studien vil kunne å ha en viss forvaltningsmessig verdi. Faktumet at det ikke eksisterer en unison forståelse av begrepet sikkerhetskultur resulterer i det som vi anser som skjeve forutsetninger for arbeidet med sikkerhet i et helhetlig perspektiv.

Teoretisk sett, basert på våre funn, vil grunnleggende forhold som begrepsbruk og språk være av vesentlig betydning for forståelse, og dermed videre for arbeidet med sikkerhetskultur. I lys av studiens resultater kan det hevdes at forutsetningene for at aktørene skal oppnå en felles forståelse er manglende. Hvorvidt det er hensiktsmessig å strebe etter en såkalt unison teoretisk forståelse vil dermed være avhengig av hvilke følger forståelsen gir i praksis**.** Som en forlengelse av studien kunne en studie av hvordan den sprikende forståelsen gjenspeiles i aktørenes praktiske arbeid vært interessant. Tatt forutsetningene i betraktning er det ikke utenkelig at nåværende forståelse er av en karakter som må anses som tilstrekkelig tilfredsstillende. Dersom nåværende forståelse resulterer i en praksis som kan betraktes som tilfredsstillende, vil det være lite hensiktsmessig å etterstrebe en fullstendig unison forståelse. Dersom praksis imidlertid viser seg å være av en karakter som kan regnes som utilstrekkelig, kan fokus på å oppnå en felles forståelse av sikkerhetskultur være av vesentlig betydning for arbeidet med sikkerhetskultur.

7 Konklusjon

Med utgangspunkt i studiens funn og diskusjon tas det i dette kapittelet sikte på å besvare oppgavens problemstilling. Innledningsvis i kapittel 7.1 presenteres sentrale funn knyttet til oppgavens forskningsspørsmål som vil være av vesentlig betydning for å kunne gi et svar på problemstillingen. I lys av forholdene forskningsspørsmålene belyser trekkes en konklusjon som gir et svar på oppgavens problemstilling. Avslutningsvis, i kapittel 7.2 Veien videre, presenteres forslag og tanker knyttet til en mulig forlengelse av studien.

7.1 Forståelse av sikkerhetskultur i en digital kontekst

Oppgavens empiriske data baseres hovedsakelig på dokumenter av nasjonale aktører med digitale sikkerhetsinteresser. Funnene i foreliggende tekster synliggjør at aktørene besitter en felles forståelse av viktigheten av sikkerhetskultur. Hvordan de ulike aktørene formidler og anvender begrepet sikkerhetskultur i lys av digitale forhold er imidlertid ikke i overensstemmelse. I lys av empiriske data kan vi hevde at det ikke eksisterer en unison forståelse av hva begrepet omfatter. Det foreligger med andre ord ikke en definisjon som kan forstås som ledende eller overordnet i arbeidet med digital sikkerhet i Norge. Aktørenes formidling og anvendelse av sikkerhetskultur er dermed sprikende.

Studien viser videre at forståelsen aktørene besitter vil kunne påvirke arbeidet med sikkerhetskultur. Foreliggende tekster vil påvirke arbeidet med sikkerhetskultur som følge av 1) aktørenes posisjon, og dermed besittelse av definisjonsmakt og, 2) aktørenes teksters makt. En sprikende forståelse av sikkerhetskultur aktører i mellom er dermed uheldig. Aktørenes formidling, anvendelse og påvirkningskraft er av betydning for oppgavens problemstilling:

Hvordan legger forståelsen av sikkerhetskultur i dokumenter utgitt av nasjonale aktører med digitale sikkerhetsinteresser føringer for arbeidet med sikkerhetskultur knyttet til digital informasjon?

Studien viser at aktørers forståelse legger føringer for arbeidet. Aktørenes felles oppfatning om viktigheten av sikkerhetskultur legger føringer som kan klassifiseres

som intensjonelle, i form av oppfordringer, foreslåtte tiltak, strategier og lignende. Aktørenes sprikende forståelse av sikkerhetskultur kan imidlertid forårsake virkninger som kan forstås som ikke-intensjonelle føringer. Inkonsekvent begrepsbruk og forståelse av hva begrepet omfatter kan anses å begrense de ulike aktørenes påvirkningskraft. Studien viser dermed at forståelsen av sikkerhetskultur ikke bare vil kunne legge føringer, men også forårsake føringer i form av utilsiktede virkninger.

Med det til grunn, konkluderer vi med at aktørenes sprikende forståelse legger og forårsaker føringer som går på bekostning av det aktørene faktisk enes om. De ikke-intensjonelle handlingene kan derfor forstås som svekkende for det arbeidet som intensjonelt legges ned. Dette resulterer i at utbyttet av en oppfordret handling vil miste sin potensielle verdi for arbeidet med sikkerhetskultur.

7.2 Veien videre

Teoretisk sett er betydningen av den sprikende forståelsen av vesentlig betydning for arbeidet med sikkerhetskultur. Det er imidlertid ikke gitt at teorien gjenspeiler praksis. I en videre studie ville det derfor vært hensiktsmessig å overføre problemstillingen til en studie med metoder som gjør det mulig å studere arbeidet med sikkerhetskultur i praksis.

Dersom en videre studie med metoder som sørger for en mer praktisk tilnærming til en tilsvarende problemstilling viser tilsvarende tendenser, vil denne studien være av potensielt stor betydning for arbeidet med sikkerhetskultur i Norge. Dersom nåværende forståelse og begrepsbruk resulterer i en lite tilfredsstillende praksis, kan det argumenteres for at fokus på et forståelse være verdifullt. I lys av funnene i denne studien vil et felles begrepsapparat bidra til en mer helhetlig tilnærming til sikkerhetskultur i en digital kontekst.

Det kunne videre vært nyttig å studere hvorvidt det er hensiktsmessig å skille mellom sikkerhetskultur og digital sikkerhetskultur. Digitaliseringen vil, om ikke allerede nå, omfatte alle aspekt av livet. Av betydning for arbeid med sikkerhet kan det derfor tenkes at det på sikt ikke vil være hensiktsmessig å forholde seg til to forskjellige begrep.

8 Litteraturliste

Aven, T. (1997). *Pålitelighets- og risikoanalyse* (3. utg.). Oslo: Universitetforlaget.

Aven, T., Boyesen, M., Njå, O., Olsen, K. H., & Sandve, K. (2004). *Samfunnssikkerhet.* Oslo: Oslo Universitetsforlag.

Bang, H. (1987). *Organisasjonskultur.* TANO A.S.

Bento, J.-P. (2001). *Menneske - teknologi - organisasjon. Veiledning for gjennomføring av MTO-analyser.* Petroliumstilsynet.

Berg, L. P. (2015, 14. april). *Finansdepartementet*. Hentet 4. april, 2019 fra Store norske leksikon: https://snl.no/Finansdepartementet

Berg, O. (2018a, 23. desember). *Maktfordelingsprinsippet*. Hentet 30. april, 2019 fra Store norske leksikon: https://snl.no/maktfordelingsprinsippet

Berg, O. T. (2018b, 29. juni). *Pluralisme - politikk*. Hentet 30. april, 2019 fra Store norske leksikon: https://snl.no/pluralisme_-_politikk

Berge, L. K., Meyer, S., & Trippestad (red.), T. A. (2003). *Maktens tekster* (1.utg.). (T. A. Trippestad, Red.) Oslo: Gyldendal Norsk Forlag.

Bjerkan, J. (2018, 6. juli). *Normen*. Hentet 4. april., 2019 fra Norsk sykepleierforbund: https://www.nsf.no/vis-artikkel/3954001/663309/Normen

Braut, G. S. (2000, 10. desember). Verdigrunnlaget for medisinen i komande tider. *Tidsskrift for den norske legeforening*.

Brekke, A., Hirsti, K., Lied, H., Ravndal, D., & Svaar, P. (2019). *Skreddersydd dobbeltangrep mot Hydro*. Hentet 20. mars, 2019 fra NRK: https://www.nrk.no/norge/skreddersydd-dobbeltangrep-mot-hydro-1.14480202

Brinkmann, J. (1991). *Sosiologiske grunnbegreper.* Oslo: Ad Notam.

Bukve, O. (2016). *Forstå, forklare, forandre: om design av samfunnsvitskaplege forskingsprosjekt.* Oslo: Universitetsforlaget.

Charmaz, K. (2006). *Constructing grounded theory.* London: Sage.

CLTRe. (2017). *The Security Culture Report 2017.* Hentet fra: https://get.clt.re/security-culture-report-2017/.

Dahlberg, R. (2004). *Den menneskelige faktor, historiens svageste ledd.* Aschehoug.

Datatilsynet. (u.d.). *Atferdsnormer*. Hentet april 2018, 2019 fra Datatilsynet: https://www.datatilsynet.no/regelverk-og-verktoy/atferdsnorm/

Datatilsynet. (2018). *ÅRSRAPPORT FOR 2018. Tall og tendenser fra Datatilsynets virksomhet.* u.s.: Hentet fra: https://www.datatilsynet.no/globalassets/global/om-oss/aarsmelding/arsmeldingen2018.pdf.

Datatilsynet. (u.å.). *Datatilsynet*. Hentet 4. april 2019 fra Datatilsynets oppgaver: https://www.datatilsynet.no/om-datatilsynet/oppgaver/

De nasjonale forskningsetiske komiteene. (2009, 23. april). *Forskningsetikk*. Hentet 2. april, 2019 fra De nasjonale forskningsetiske komiteene: https://www.etikkom.no/forskningsetiske-retningslinjer/naturvitenskap-og-teknologi/Forskningsetikk/

De nasjonale forskningsetiske komiteene. (2016, 31. mai). Generelle forskningsetiske retningslinjer. Hentet fra: https://www.etikkom.no/forskningsetiske-retningslinjer/Generelle-forskningsetiske-retningslinjer/.

Departementene. (2019). *Nasjonal strategi for digital sikkerhet*. Hentet fra: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf.

Direktoratet for forvaltning og ikt. (2015). *Veileder i kompetanse- og kulturutvikling innen informasjonssikkerhet.* Hentet fra: https://www.difi.no/sites/difino/files/veileder_kompetanse_og_kulturutvikling_informasjonssikkerhet_v3.pdf.

Direktoratet for e-helse. (2018). *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.* Hentet 25. februar, 2019 fra https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf

Direktoratet for e-helse. (u.å). *Om Direktoratet for E-helse.* Hentet 17. februar, 2019 fra Direktoratet for E-helse: https://ehelse.no/om-oss/om-direktoratet-for-e-helse

Direktoratet for forvaltning og ikt. *Begrepsliste: Informasjonssikkerhet*. Hentet februar 8, 2019 fra Direktoratet for forvaltning og ikt: https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet

Direktoratet for forvaltning og ikt. (u.d.). *Difi*. Hentet 5. april, 2019 fra Om oss: https://uu.difi.no/om-oss

Engen, O. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., & Pettersen, K. A. (2016). *Perspektiver på samfunnsikkerhet.* Oslo, Norge: Cappelen Damm Akademisk.

Eriksen, N., Hagen, A., & Walnum, N. A. (2019). *Norske Visma har blitt hacket*. Hentet 20. mars, 2019 fra Dagbladet.no: https://www.dagbladet.no/nyheter/norske-visma-har-blitt-hacket/70738785

Finansdepartementet. (2018). *Proposisjon til Stortinget (Prop. 1 S 2018-2019).*: Hentet fra:https://www.statsbudsjettet.no/upload/Statsbudsjett_2019/dokumenter/pdf/gulbok.pdf.

Finanstilsynet. (2018). *Risiko- og sårbarhetsanalyse (ROS) 2017.*: Hentet fra: https://www.finanstilsynet.no/contentassets/b9cb0cab82304c4498a1562a002bafce/risiko--og-sarbarhetsanalyse-2017.pdf.

Forsvarsdepartementet. (2018, desember 20). *Ny sikkerhetslov skal gjøre Norge tryggere*. Hentet 06.04, 2019 fra Regjeringen: https://www.regjeringen.no/no/aktuelt/ny-sikkerhetslov/id2623522/

Foucault, M. (1999). *Seksualitetens historie 1.* Norge: Pax Forlag.

Glasspaper. (u.å.). *Hva skal til for å skape en sikkerhetskultur?* Hentet 5. april 2019 fra Glasspaper: https://www.glasspaper.no/nyheter/2018/oktober/sikkerhetskultur-i-virksomheter/

Grønmo, S. (2004). *Samfunnsvitenskapelige metoder* (2. utg.) Bergen: Fagbokforlaget.

Guldenmund, F. W. (2007, juli). *The use of questionnaires in safety culture research - an evaluation.* Vol. 45, No. 6 (ss. 723-743). Hentet fra: https://www.sciencedirect.com/science/article/pii/S0925753507000239?via%3Dihub

Hansen, T. (2018, 26. september). *Norges offentlige utredninger*. Hentet 2. mai 2019 fra Store norske leksikon: https://snl.no/Norges_offentlige_utredninger_(NOU)

Hartman, J. (2001). *Grundad teori. Teorigenerering på empirisk grund.* Lund, Sverige: Studentlitteratur.

Haukelid, K. (1999). *Risiko og sikkerhet. Forståelser og styring.* Oslo: Universitetsforlaget.

ISACA & CMMI. (2018). *The ISACA/CMMI Institute Cybersecurity Culture Report.* Hentet fra: http://www.isaca.org/SiteCollectionDocuments/Cybersecurity-Culture-Report.pdf.

Johansen, E. N. (2019). *NRK.no*. Hentet 20. mars 2019 fra Milliongebyr etter sikkerheitsflause blir ståande – historisk gebyr til Bergen kommune:

https://www.nrk.no/hordaland/datatilsynet-star-fast-pa-milliongebyr-_-historisk-bot-til-bergen-kommune-blir-staande-1.14479734

Justis- og beredskapsdepartementet. (2016). *IKT-sikkerhet - Et felles ansvar.* (Meld. St. 38 2016-2017).: Hentet fra: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf.

Justis- og beredskapsdepartementet. (2016). *Risiko i et trygt samfunn — Samfunnssikkerhet.* (Meld. St. 10 2016–2017). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/.

Justis- og beredskapsdepartementet. (2018, 7. juli). *Ny personopplysningslov og EUs personvernforordning*. Hentet 8. april, 2019 fra Regjeringen: https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/ny-personopplysningslov/id2592984/

Kaufmann, G., & Kaufmann, A. (2009). *Psykologi i organisasjon og ledelse* (4. utg). Bergen: Fagbokforlaget.

Koch, C., & Richter, A. (2004, oktober). Integration, differentiation and ambiguity in safety cultures. *Safety Science, 42* (8), ss. 703-722.

Kommunal- og moderniseringsdepartementet, Finansdepartementet. (2019, 14. mars). *Samler digitaliseringsinnsatsen i ett direktorat*. Hentet 3. mai, 2019 fra Regjeringen: https://www.regjeringen.no/no/aktuelt/samler-digitaliseringsinnsatsen-i-ett-direktorat/id2632365/

Kringen, J. (2009). *Culture and control: regulation of risk in the Norwegian petroleum industry.* Oslo: Centre for Technology, Innovation and Culture, Faculty of Social Sciences, University of Oslo Unipub.

Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven) (LOV-2005-06-17-62), § 2-3 (2005).

Lundgren, B., & Möller, N. (2017, 15. november). *Defining Information Security.* Hentet 20. februar, 2019 fra 10.1007/s11948-017-9992-1

Malmedal, B., & Røislien, H. E. (2018). *Nordmenn og digital sikkerhetskultur 2018.* Hentet fra https://norsis.no/wp-content/uploads/2018/11/Nordmenn-og-digital-sikkerhetskultur-2018-web.pdf.

Malmedal, B., & Røislien, H. E. (2016). *The Norwegian Cyber Security Culture.* Hentet fra https://norsis.no/wp-content/uploads/2016/09/The-Norwegian-Cybersecurity-culture-web.pdf.

Malmedal, B., & Røislien, H. E. (2017). *Ungdom og digital sikkerhetskultur.* Hentet fra https://norsis.no/wp-content/uploads/2017/08/Ungdom_og_digital_sikkerhetskultur_web.pdf.

Nasjonal digital læringsarena. (2018, 17. februar). *Medienes definisjonsmakt*. Hentet 9. mai, 2019 fra NDLA: https://ndla.no/subjects/subject:14/topic:1:79218/resource:1:79124

Nasjonalt pasientsikkerhetprogram. (2017, mars). *ForBedring - kartlegging av sikkerhetskultur i spesialhelsetjenesten*. Hentet 4. april, 2019 fra https://www.pasientsikkerhetsprogrammet.no/aktuelt/nyheter/_attachment/4305?_download=false&_ts=15c1b0e4cce

Normen. (2018). *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten. Versjon 5.3.*: Hentet fra: https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf.

Normen. (2019). *Strategi for Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (2019-2021)*. Hentet fra: https://ehelse.no/Documents/Normen/2%20Normen%20prosessdok/Strategi%20for%20Normen%202019-2021%20v1.0.pdf.

Norsk senter for informasjonssikring. (2016, 27. september). *Den norske informasjonssikkerhetskulturen*. Hentet 10. april, 2019 fra NorSIS: https://norsis.no/den-norske-informasjonssikkerhetskulturen/

Norsk senter for informasjonssikring. (2016, september). *Den norske informasjonssikkerhetskulturen*. Hentet 28. februar, 2019 fra Norsk senter for informasjonssikring: https://norsis.no/den-norske-informasjonssikkerhetskulturen/

Norsk senter for informasjonssikring. (2016). *Informasjonssikkerhetskultur. Oppsummerende rapport fra toppsikkerhetsmøtet 20.04.2016.* Hentet fra: https://norsis.no/wp-content/uploads/2016/11/Sikkerhetstoppmøtet-Rapport-Informasjonssikkerhetskultur.pdf.

Norsk senter for informasjonssikring. (2017). *Nordmenn og digital sikkerhetskultur.* Hentet fra: https://norsis.no/wp-content/uploads/2017/11/Nordmenn-og-digital-sikkerhetskultur-2017.pdf.

Norsk senter for informasjonssikring. (2017, mai 16). *Ny rapport om informasjonssikkerhetskultur*. Hentet 2. februar, 2018 fra Norsk senter for informasjonssikring: https://norsis.no/ny-rapport-om-informajonssikkerhetskultur/

Norsk senter for informasjonssikring. (u.d.). *Om NorSIS*. Hentet 4. april, 2019 fra Norsk senter for informasjonssikring: https://norsis.no/om-norsis/

Norsk senter for informasjonssikring. (2016). *Trusler og trender 2016-17*. u.s.: Hentet fra: https://norsis.no/wp-content/uploads/2016/07/trusler-og-trender-2016_final-c.pdf.

Norsk senter for informasjonssikring. (2017). *Trusler og trender 2017-18*. u.s.: Hentet fra: https://norsis.no/wp-content/uploads/2017/12/tt17-18_web_endelig_v2.pdf.

Norsk senter for informasjonssikring. (2018). *Trusler og trender 2018-19*. u.s.: Hentet fra: http://norsis.no/upload/trusler%20og%20trender%202018-19%20web.pdf.

NOU 2006:6. (2006). *Når sikkerheten er viktigst — Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner* . Justis- og beredskapsdepartemenetet. Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/.

NOU 2012:14. (2012). *Rapport fra 22. juli-kommisjonen.* Hentet fra: https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn.* Hentet fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet.* Hentet fra: https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

Norsk sikkerhetsmyndighet. (2014, 20. april). *Dette gjør NSM*. Hentet 4. april, 2019 fra NSM: https://www.nsm.stat.no/om-nsm/tjenester/

Norsk sikkerhetsmyndighet. (2018). *Et sikkert digitalt Norge - IKT-risikobilde 2018.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm_ikt-risikobilde_2018_web.pdf.

Norsk sikkerhetsmyndighet. (u.å). *Generelt om ny sikkerhetslov*. Hentet 25. april, 2019 fra NSM: https://rise.articulate.com/share/k58m6mGHKjK2Htg5GSk6UJrzgUepxA4C#/lessons/OeC3gyjOFWir8hnHFpCZwoZ1jnIZfhDC

Norsk sikkerhetsmyndighet. (2015). *Helhetlig IKT-risikobilde 2015.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf.

Norsk sikkerhetsmyndighet. (2016). *Helhetlig IKT-risikobilde 2016.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/nsm_helhetlig_ikt_risikobilde_2016_web_enkel.pdf.

Norsk sikkerhetsmyndighet. (2017). *Helhetlig IKT-risikobilde 2017.* Hentet fra: https://www.nsm.stat.no/globalassets/helhetlig_ikt-risikobilde_2017_orig_low.pdf.

Norsk sikkerhetsmyndighet. (2014, 7. juni). *Kan vi måle sikkerhetskultur?*. Hentet april 08, 2019 fra NSM: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/kan-vi-male-sikkerhetskultur/

Norsk sikkerhetsmyndighet. (2014, 21. februar). *Om NSM*. Hentet 4. april, 2019 fra NSM: https://www.nsm.stat.no/om-nsm/).

Norsk sikkerhetsmyndighet. (2016). *Risiko 2016. Kan risiko styres?* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf.

Norsk sikkerhetsmyndighet. (2017). *Risiko 2017. Risiko og sårbarheter i en ny tid.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf.

Norsk sikkerhetsmyndighet. (2018). *Risiko 2018. Verdifulle individer, verdifulle virksomheter, verdifull infrastruktur*. Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf.

Norsk sikkerhetsmyndighet. (2019). *Risiko 2019. Krafttak for et sikrere Norge.* Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf.

Norsk sikkerhetsmyndighet. (2014, 12. mai). *Sikkerhetskultur*. Hentet 25. april, 2019 fra Nasjonal sikkerhetsmyndighet: https://www.nsm.stat.no/om-nsm/tjenester/sikkerhetsstyring/sikkerhetskultur/

Næringslivets Sikkerhetsråd. (2016). *Mørketallsundersøkelsen 2016.* Hentet fra: https://www.nsr-org.no/getfile.php/137423-1474384915/Bilder/Mørketallsundersøkelsen/morketallsundersokelsen_2016.pdf.

Næringslivets Sikkerhetsråd. (2018). *Mørketallsundersøkelsen 2018.* Hentet fra: https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen%202018%20low.pdf.

Næringslivets Sikkerhetsråd. (u.d.). *Næringslivets Sikkerhetsråd*. Hentet 4. april, 2019 fra Næringslivets Sikkerhetsråd: https://www.nsr-org.no/om-nsr/

Perrow, C. (1999). *Normal Accidents: living with high-risk technologies.* Princeton, New Jersey: Princeton University Press.

Personopplysningsloven. (2018). *Lov om behandling av personopplysninger* (LOV-2018-06-15-38). Hentet fra: https://lovdata.no/lov/2018-06-15-38.

Persvold, A. Z. (2019, 30. april). *Aktør*. Hentet 11. mai, 2019 fra Store norske leksikon: https://snl.no/aktør

Petroleumstilsynet. (2010). *Rapport etter gransking av hendelse 18.12.2010 på Njord A hvor slip joint falt ned på boredekk.* Hentet fra: http://www.ptil.no/getfile.php/1314146/Tilsyn%20på%20nettet/Granskinger/2010_1424_Rapport%20Gransking%20Njord%20A%20-%20løftehendelse.pdf.

PwC (2017). *Helse Sør-Øst RHF. Rapport fra ekstern gjennomgang av programmet for modernisering av IKT- infrastruktur (iMod).* Hentet fra: https://www.helse-sorost.no/Documents/Styret/Styremøter/2017/20170628/077-2017%20Vedlegg%201%20-%20HSØ%20FY%202017%20-%20Rapport%20iMod%20v%201.0.pdf.

Rammeforskriften (petroleumsvirksomheten). (2010). *Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg* (FOR-2010-02-12-158). Hentet fra: https://lovdata.no/forskrift/2010-02-12-158.

Reason, J. (1997). *Managing the risks of organizational accidents.* England: Ashgate Publishing Limited.

Regjeringen. (u.d.). *Finansdepartementet*. Hentet 4. april, 2019 fra Regjeringen.no: https://www.regjeringen.no/no/dep/fin/id216/

Regjeringen. (u.d.). *Justis- og beredskapsdepartementet*. Hentet 4. april, 2019 fra Regjeringen.no: https://www.regjeringen.no/no/dep/jd/id463/

Schein, E. H. (1987). *Organisasjonskultur og ledelse. Er kulturendring mulig?* Oslo: Mercuri Media Forlag.

Schiefloe, P. M. (1999). *Kultur.* Trondheim: Allforsk.

Schiefloe, P. M. (2011). *Mennesker og samfunn. Innføring i sosiologisk forståelse* (2. utg.). Bono.

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet.* (LOV-2018-06-01-24). Hentet fra: https://lovdata.no/lov/2018-06-01-24.

Sjølstad, T., Høie, T. A., & Daler, T. (2010). *Håndbok i datasikkerhet: informasjonsteknologi og risikostyring.* Trondheim: Tapir akademisk.

Slaatta, T. (1999). *Medier, makt og demokrati. Makt- og demokratiutredningens rapportserie, ISSN 1501-3065.* UiO: det samfunnsvitenskapelige fakultetet. Oslo: Hentet fra: https://www.sv.uio.no/mutr/publikasjoner/rapporter/rapp1999/rapport6.html#Medier.

Språkrådet. (u.d.). *Bokmålsordboka*. Hentet 4. april, 2019 fra Bokmålsordboka | Nynorskordboka: https://ordbok.uib.no/perl/ordbok.cgi?OPP=EVNe&ant_bokmaal=5&ant_nynorsk=5&begge=+&ordbok=begge

Stortinget. (2019, 23. april). *Hva gjør regjeringen?* Hentet 15. mai, 2019 fra Stortinget: https://www.stortinget.no/no/Stortinget-og-demokratiet/stortinget-undervisning/5.-7.-trinn/hva-gjor-regjeringen/

Stortinget. (2018, 28. juni). *Hva gjør Stortinget?* Hentet 15. mai, 2019 fra Stortinget: https://www.stortinget.no/no/Stortinget-og-demokratiet/stortinget-undervisning/5.-7.-trinn/hva-gjor-stortinget/

Stortinget. (2018, 18. oktober). *Om regjeringens publikasjoner*. Hentet 2. mai, 2019 fra Stortinget: https://www.stortinget.no/no/Stortinget-og-demokratiet/Arbeidet/Om-publikasjonene/Regjeringens-publikasjoner/

Styri, H. (2017, oktober 30). *Måling av informasjonssikkerhet*. Hentet 2. april, 2019 fra Difi: https://www.difi.no/sites/difino/files/maling_-_informasjonssikkerhet_-_hakon.pdf

Thagaard, T. (2018). *Systematikk og innlevelse. En innføring i kvalitative metoder* (5. utg.). Bergen: Fagbokforlaget.

Trygstad, S. C., & Hagen, I. M. (2007). *Ledere i den norske modellen. Fafos Rådsprogram 2006-2008.* Hentet fra: https://www.fafo.no/media/com_netsukii/20024.pdf.

Universitetet i Stavanger. (u.å.). *Master i Samfunnssikkerhet.* Hentet 1. mars, 2019 fra https://www.uis.no/course/?code=MSAMAS_1&parentcat=10161

von Solms, R., & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers and Security*. No. 38 (ss. 97-102).

Østbye, H., Helland, K., Knapskog, K., Larsen, L. O., & Moe, H. (2013). *Metodebok for mediefag* (4. utg.). Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Vedlegg

A Emnebeskrivelse: Masteroppgave i samfunnssikkerhet

Følgende er hentet fra Universitetet i Stavangers hjemmeside (Universitetet i Stavanger, u.å.).

Ved hjelp av teori, forskningsmetode og innsamlede data skal studentene utarbeide en skriftlig masteroppgave innen fagområdet samfunnssikkerhet. Masteroppgavene kan ha svært forskjellig form, noen kan være empiriske, mens andre er rent teoretiske. Hovedmålet med masteroppgaven er at studentene skal gjennomføre et selvstendig forskningsarbeid. Studenten skal vise evne til systematisk tenkning, faglig fordypning og saklig vurdering. I tillegg skal studentene få trening i relevant bruk av kildestoff for å vise hvordan eget arbeid kan plasseres i forhold til eksisterende forskning.

Læringsutbytte

Ved avslutningen av emnet forventes det at studenten

Kunnskaper

- har tilegnet seg så god oversikt over studieprogrammets teoriområder og perspektiver at hun/han kan gjøre et informert valg med tanke på teoriforankring for eget oppgavetema.

Ferdigheter

- er i stand til å formulere en avgrenset problemstilling for egen undersøkelse og sette denne inn i et større perspektiv.
- kan demonstrere innsikt i det valgte teorigrunnlaget, og er i stand til å benytte dette i analyse av den konkrete problemstilling.
- kan skape overblikk og systematisere et empirisk materiale med henblikk på å analysere den valgte problemstilling.

Generell kompetanse

- kan demonstrere bevissthet om sammenhengene mellom problemformulering, teoretiske perspektiv, analyse og konklusjon.

B Forstudie 1 – KIT i informasjonssikkerhetshendelser

PwC leverte rapporten ”Rapport fra ekstern gjennomgang av programmet for modernisering av IKT-infrastuktur (iMod)” i 2017. PwC gjorde perioden 4. mai 2017 – 21. juni 2017 undersøkelser angående påstander om at sensitive personopplysninger hadde vært tilgjengelige for en ekstern leverandør (PwC, 2017, s. 3). Hovedfunnene i rapporten viser at 36 brukere tilknyttet en avtale mellom ESN (Enterprise Services Norge AS) HSØ hadde fått utvidede administratorrettigheter som innebærer muligheter for tilgang til helseopplysninger (PwC, 2017, s. 3). Informasjonssikkerheten hadde blitt kompromittert, og kan betraktes som et brudd på sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet. Utgangspunktet vårt var å se på hvorvidt det er hensiktsmessig å klassifisere sikkerhetsbrudd etter KIT.

Kapittel 1-6 i PwCs rapport ble analysert og vurdert i henhold til sikkerhetsmålene KIT. Kapitlene presenterer totalt 8 påstander og spørsmål om forhold som PwC har undersøkt og vurdert. Vurderingene har i dette studiet blitt kategorisert etter hvorvidt sikkerhetsbrudd kan betraktes som brudd på et eller flere av sikkerhetsmålene KIT. Tabellen nedenfor viser informasjonsutfordringene kategorisert etter sikkerhetsmålene KIT, der “x” indikerer brudd på sikkerhetsmål.

Tabell: Kategorisering av utfordringer der *K* står for konfidensialitet, *I* for integritet, *T* for tilgjengelighet og *S* for sporing.

Informasjonssikkerhetsutfordringer	**K**	**I**	**T**	**S**	**Forslag til alternative kategorier**
1. Sykehuspartner har ikke tilstrekkelig kontroll på tilgangsstyring (PwC, 2017, s. 14)	x	x	x	x	
2. Sykehuspartner har ikke tilstrekkelig sporbarhet på tilganger til helseopplysninger (PwC, 2017, s. 15)	x		x	x	
3.1 Hvilke tilganger er blitt tildelt personell tilknyttet kontrakten? (PwC, 2017, s. 15)	x	x		x	
3.2 Har tilganger blitt misbrukt? (PwC, 2017, s. 16)	x	x	x	x	
3.3 Har personell tilknyttet kontrakten aksessert	x	x	x	x	x

helseopplysninger? (PwC, 2017, s. 17)					
4. HPN/ESN har så langt ikke kunnet dokumentere at det foreligger databehandleravtaler med samtlige underleverandører som oppfyller kravene i avtalen med Sykehuspartner (PwC, 2017, s. 17)	x	x	x		Usikkerhet

Gjennomgangen vår av PwCs rapport er oppsummert i tabellen ovenfor. Det fremkommer av tabellen at det krysses av på de fleste kategorier på overskriftene i rapporten. Tabellen kan dermed gi en indikasjon at det ikke er mulig å skille mellom KITS-begrepene ved sikkerhetsbrudd, og at begrepene har et visst overlapp. Grunnet et utydelig skille mellom KITS og klassifisering av kategoriene kan det argumenters for at det er lite hensiktsmessig å skille mellom målene i relasjon til informasjonssikkerhet. Det reiser derfor spørsmål om det er ønskelig å videreføre KITS inn i en digital tidsalder, hvorvidt det er hensiktsmessig, og hva er da som eventuelt kan definere informasjonssikkerhet

C Forstudie 2 – Begrepet informasjonssikkerhet

På bakgrunn av forstudie 1 reiste spørsmålet seg om hvorvidt defineringen av informasjonssikkerhet var hensiktsmessig i en digital tidsalder. Det ble derfor gjort et søk etter litteratur som tar for seg begrepsbruk knyttet til informasjonssikkerhet. Det viste seg å være vanskelig å finne litteratur som gir alternative forståelser, og det ser ut til at informasjonssikkerhet definert gjennom KIT(S) står sterkt i både akademia og i offentlig tilgjengelige dokumenter. Denne studien tar for seg en artikkel av Bjørn Lundgren og Niklas Møller som gir en alternativ definisjon.

Forfatterne Bjørn Lundgren og Niklas Möller (2017) studerer i sin publikasjon ”Defining Information Security” den tradisjonelle forståelsen av informasjonssikkerhet, herunder begrepene konfidensialitet, integritet og tilgjengelighet (KIT). De argumenterer for at definisjonen er for vid, men samtidig for smal, til å korrekt adressere problematikken informasjonssikkerhet- og systemer står ovenfor.

Med KIT som grunnsteiner i arbeidet med informasjonssikkerhet, kan en ifølge forfatterne ikke på en korrekt måte håndtere “soft issues”. Samtidig feiler den tradisjonelle definisjonen i å anerkjenne den kontekstuelle og normative naturen til sikkerhet (Lundgren & Möller, 2017, s. 1). Ifølge Lundgren og Möller (2017) definerer konfidensialitet, integritet og tilgjengelighet som ”insecure states as secure and secure states as insecure” (Lundgren & Möller, 2017, s. 4), som de da hevder bidrar til at definisjonen blir både for vid og smal. I enkelte standarder, lovverk, veiledere vektlegges ytterligere egenskaper som sporbarhet, ikke-fornekting og autentisitet lagt til (Lundgren & Møller, 2017, s. 4). Fra forfatternes perspektiv er imidlertid inkludering av ovennevnte egenskaper ikke tilstrekkelig, da heller ikke de kan bidra til å fange opp samtlige informasjonssikkerhetutfordringer. Videre påpekes det som lite hensiktsmessig å utelukkende kartlegge hvorvidt det har oppstått et informasjonssikkerhetsbrudd, da det også er viktig å fastslå sannsynlighet for og grad av brudd (Lundgren og Möller, 2017, s. 4).

Lundgren og Möllers (2017, s. 21) foreslår å se bort fra KIT og ikke lenger vektlegge sikkerhetsmålene i definisjon av informasjonssikkerhet. De foreslår en alternativ

definisjon av informasjonssikkerhet som tar utgangspunkt i at sikkerhet er en relativt størrelse:

AA (information): the information I is secure for stakeholder H, if and only if: for every agent A, and every part of P of I, A has just the appropriate access to P, relative to H;

AA (information system); an information system S is secure for stakeholder H if, and only if: For every agent A, and every part P of S, A has just the appropriate access to P relative to H

(2017, s.11).

Ifølge forfatterne vil forståelse og oppfatning av sikkerhet være relativ til interessentens tolkning. Motsetningen vil dermed være at informasjonssikkerhet- og systemer er sikre uavhengig interessent (Lundgren & Möller, 2017). Forfatterne betrakter en dimensjon av informasjonssikkerhet som ikke fremkommer i den tradisjonelle definisjon av informasjonssikkerhet. I henhold til den tradisjonelle forståelsen, er informasjon sikre uavhengig av interessent, så lenge sikkerhetsmålene KIT oppnås.

Følger en Lundgrens og Möllers tankegang, kan det argumenteres for et behov for en redefinering av informasjonssikkerhet for å korrekt adressere den problematikken virksomheter, organisasjoner og statlig forvaltning står overfor i dag.

D Forstudie 3 – Sikkerhetskultur i tilsynsrapporter

Det var ønskelig å se på om det eksisterte tilsynsrapporter som vurderer sikkerhetskultur relatert til informasjonssikkerhetsbrudd. Vi kontaktet Helsetilsynet og Datatilsynet uten resultat. Heller ikke i offentlig tilgjengelig tilsynsrapporter vises det til både informasjonssikkerhet og sikkerhetskultur. Det er med andre ord få tilsynsrapporter hvor både informasjonssikkerhet og sikkerhetskultur representerer sentrale stikkord. En naturlig årsak kan være at det i fåtallet av forskriftene i det norske lovverket stilles krav til sikkerhetskultur.

I del III Oppfølging av Lysneutvalgets anbefalinger i Meld. St.38 (2016-2017) *IKT-sikkerhet i alle ledd* beskrives status på tiltak relatert til problembeskrivelsene Lysneutvalget beskriver i NOU 2015:13 *Digital sårbarhet - sikkert samfunn*. En av problembeskrivelsene dreier seg om at den gode sikkerhetstradisjonen som er opparbeidet i olje- og gassektoren bør videreføres til det digitale området. Ifølge Meld. St. 38 har blant annet Ptil bidratt til overføring HMS-tradisjonene og normer og regelverk har siden 2015 blitt videreutviklet og tilpasset fagområdet. Tilsynsrapporter og granskningsrapporter som inkluderer sikkerhetskultur er i hovedsak forbeholdt olje- og gassnæringen. Regjeringen foreslår imidlertid, i Statsbudsjettet for 2019, å øke bevilgningen til Statens helsetilsyn med 23 millioner kroner relatert til tilsyn med (varselordning og) IKT-løsningene i helse-og omsorgstjenesten (Statsbudsjettet, 2019). Det trenger imidlertid ikke bety flere tilsynsrapporter innen IKT i helsesektoren som vektlegger sikkerhetskultur.

Rammeforskriften § - 15. God helse-, miljø- og sikkerhetskultur

I rammeforskriften, som gjelder for petroleumsvirksomheter og enkelte landanlegg, blir det stilt krav til det som omtales som helse-, miljø- og sikkerhetskultur. Lovverkets inkludering av sikkerhetskultur legger åpenbart føringer for at tilsynsmyndigheter og virksomheter innen petroleum må forholde seg til konseptet. Lovverket formidler imidlertid ikke hvordan virksomheter skal gjennomføre systematiske vurderinger som sikrer samme vurderingsgrunnlag. I henhold til Rammeforskriften § - 15. God helse-, miljø- og sikkerhetskultur skal en god HMS-kultur som omfatter alle faser og aktivitetsområder fremmes gjennom kontinuerlig arbeid for å redusere risiko og forbedre HMS (Rammeforskriften

(petroliumsvirksomheten), 2011). Paragrafen er kortfattet og lite konkret, som resulterer i stort rom for egen tolkning. Det kan stilles spørsmål til hvorvidt det er hensiktsmessig å stille krav til sikkerhetskultur når innholdet i begrepet er såpass vagt. Som kjent betraktes sikkerhetskultur av mange som eksempelvis god eller dårlig - her igjen vil en stå overfor et definisjonsspørsmål. Hva som betraktes som god eller tilfredsstillende sikkerhetskultur vil påvirkes av virksomhetens holdninger, verdier, interesser, som igjen er bestemmende for sikkerhetskultur. Forståelsen av, og tilnærmingen til konseptet er med andre ord avgjørende for hvordan virksomheter forholder seg til sikkerhetskultur.

Tilsyn med Total på Martin Linge

Rapporttittel: Rapport etter tilsyn med Total sin planlegging og gjennomføring av bore- og brønnoperasjoner på Martin Linge.

Ptil gjennomførte i løpet av februar og mars 2017 en tilsynsaktivitet med Total E&P Norge AS (Total). I rapporten ble det identifisert forbedringspunkter knyttet til blant annet sikkerhetskultur, erfaringsoverføring og synlig ledelse. Funnene berører kravene i henhold til Rammeforskriften § 15 – god helse-, miljø,- og sikkerhetskultur og Styringsforskriften § 6 – Styring av helse, miljø og sikkerhet. Ifølgende utdrag, fra rapportens *kapittel 5.2.3 Sikkerhetskultur og synlig ledelse* begrunnes funnene:

> Det ble registrert at brønnservice selskapene ikke deltok i systematisk erfaringsoverføring slik Total og Mærsk gjennomførte for egne ansatte i boremannskapet i forberedende møter på heliporten i forkant av utreise til innretningen.
>
> Det ble uttalt av arbeidstakerne at synlig ledelse i arbeidsområdene var lav. Videre ble det uttalt av ledende personell at det var begrenset tilgjengelig tid til ledelse i uteområdene.
>
> Det ble registrert at arbeidstakerne ble utsatt for støy i uteområdene ved opprensking og avbrenning av hydrokarboner som hadde varighet over flere døgn. Støynivået ble målt til å være i området 114 – 130 decibel ute på dekk.
>
> Det ble uttalt at det var registrert høyere H2S innhold i brønnen enn antatt i planleggingen. Det ble stilt spørsmål ved bestandighet til det valgte kveilerør og motstandsdyktighet i forhold

til H2S spesifikasjon i brønnen. De valgte løsningene var medvirkende til at det inntraff en hendelse med kjemisk nedbrytning av stålmaterialet og påfølgende lekkasjer i kveilerøret

(Ptil, 2017, s. 5),

Granskning av hendelse på Njord A

Rapporttittel: Rapport etter granskning av hendelse 18.12.2010 på Njord A hvor slip joint falt ned på boredekk.

En slip joint på omtrent 23 tonn falt cirka 4 meter ned før den traff en lastebukk, og deretter ned på arbeidsbordet og videre ned på boredekk, før den til slutt traff borebua og stanset. Den utløsende årsaken var feil bruk av elevatoren, men manglende sikkerhetskultur betraktes som en av de bakenforliggende årsakene. I rapportens kapittel 5.1.9 *Dårlig sikkerhetskultur* beskrives sikkerhetskulturen på Njord A som mangelfull. I beskrivelsen av avviket fremkommer følgende:

> Det er demonstrert at mangelfull etterlevelse av krav var gjennomgående fra toppen i linjeledelsen om bord ned til og med utførende ledd. Selskapenes manglende evne til å implementere og sørge for etterlevelse av egne og regelverket sine krav, sammen med de gjennomgående og til dels kollektive brudd på disse kravene demonstrerer at sikkerhetskulturen om bord på Njord A var dårlig
>
> (Ptil, 2010, s. 30-31)

Ifølge denne rapporten betraktes sikkerhetskulturen som dårlig fordi kravene som er satt ikke overholdes.

I henhold til § 6. Styring av helse, miljø og sikkerhet skal den ansvarlige sikre at styringen av HMS omfatter de aktivitetene, ressursene, prosessene og organisasjonen som er nødvendig for å sikre forsvarlig virksomhet og kontinuerlig forbedring, jf. rammeforskriften § 17. Videre formidler paragrafen at ansvar og myndighet skal være entydig definert og samordnet til enhver tid, og at de nødvendige styrende dokumentene skal utarbeides, og de nødvendige rapporteringslinjene etableres (Rammeforskriften (petroleumsvirksomheten), 2011) (Rammeforskriften (petroliumsvirksomheten), 2011).

Eksemplene er tatt med for å vise at det eksisterer tilsynsrapporter som tar for seg sikkerhetskultur. Det er som nevnt innledningsvis i kapittelet ikke avdekket tilsynsrapporter som undersøker både informasjonssikkerhet og sikkerhetskultur. Olje-og gassnæringen kan like fullt tjene som gode eksempler på at det kan føres tilsyn med sikkerhetskultur. Det er imidlertid trolig gjort på bakgrunn av at Rammeforskriften stiller krav til dette. Da det i Meld. St. 38 vises til at sikkerhetstradisjonen i olje- og gassnæringen bør overføres til det digitale, kan det mulig være av nytte å vurdere hvorvidt det skal utformes et lovverk som stiller krav til sikkerhetskultur også i andre virksomheter.