Ingrid Skjørland

og

Renate Thoreid

Hvordan evner sentrale aktører å samhandle ved IKT- hendelser?

Masteroppgave 2018

Masteroppgave i Risikostyring og sikkerhetsledelse
ved Universitetet i Stavanger

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Vårsemester 2018

FORFATTER:

Renate Thoreid og Ingrid Skjørland

VEILEDER:

Lillian Katarina Stene

TITTEL PÅ MASTEROPPGAVE:

Hvordan evner sentrale aktører å samhandle ved IKT-hendelser?

EMNEORD/STIKKORD:

Samvirkeprinsippet, beredskap, kriser og krisehåndtering, øvelser, informasjon og kommunikasjonsteknologi, IKT

SIDETALL: 76 (94 totalt)

STAVANGER/OSLO 17.10.2018

Forord

Renate Thoreid og Ingrid Skjørland er forfattere av denne masteroppgaven som representerer slutten på vårt masterstudium i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Formålet med masteroppgaven har vært å se nærmere på det sist innførte prinsippet av de fire prinsippene for samfunnssikkerhet og beredskap, *samvirkeprinsippet*. De øvrige prinsippene er ansvar, - likhet- og nærhetsprinsippet.

Tema vi har valgt for masteroppgaven er ikke tilfeldig. Renate Thoreid har lang erfaring fra informasjonssikkerhet og beredskap og jobber til daglig som Business Security Manager i Telenor. Ingrid Skjørland har jobbet i Justis- og beredskapsdepartementet (JD) i 11 år. Hovedansvarsområder er politiberedskap og sentral krisehåndtering.

Vi har gjennom dette studiet og arbeidet med masteroppgaven fått et godt og bredt grunnlag og økt kunnskap om samfunnssikkerhet, risiko, og sårbarhet. Det har vært krevende, lærerikt og givende å skrive denne masteroppgaven, og det er flere personer vi ønsker å takke for hjelp og god veiledning gjennom tiden det har tatt å skrive denne oppgaven.

En stor takk går til vår veileder på UIS, Lillian K. Stene for tilbakemeldinger og nyttige innspill gjennom arbeidet med masteroppgaven. Vi vil også takke DSB og NSM for å ha stilt ressurser til rådighet. Til slutt ønsker vi å takke hverandre for et godt samarbeid gjennom hele studieperioden og utarbeidelsen av masteroppgaven.

Oslo 17. oktober 2018

Renate Thoreid og Ingrid Skjørland

Sammendrag

Bakgrunn for denne oppgaven er at samvirkeprinsippet ble innført som et nytt bærende element i det nasjonale samfunnssikkerhets- og beredskapsarbeidet blant annet på bakgrunn av erfaringene etter angrepene 22. juli. Samvirkeprinsippet stiller *«krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeid med forebygging, beredskap og krisehåndtering»*. Innføring av samvirkeprinsippet medfører ingen endring i de tre øvrige prinsippene; ansvar, likhet og nærhet (Meld. St. 29 (2011-2012)).

Den teknologiske utviklingen gjennom de siste tiårene har bidratt til gjennomgripende samfunnsmessige endringer i form av et sterkt digitalisert samfunn som i all hovedsak har effektivisert hverdagen for de fleste av oss. Digitaliseringen innebærer en økt risiko ved at sentrale samfunnsfunksjoner har blitt langt mer sårbare, blant annet i form av lange og uoversiktlige verdikjeder, som gjerne spenner over mange sektorer og flere land (*Digital sårbarhet- sikkert samfunn* NOU 2015: 13). Flere og mer komplekse systemer er bærere av funksjoner og tjenester (verdier) vi er avhengige av i samfunnet. En stor andel uønskede hendelser som rammer IKT-systemer er utilsiktede, men tilsiktede hendelser er et økende problem (Meld. St. 10 (2016-2017)). Det gjennomføres stadig flere angrep, det avdekkes flere raffinerte angrepsmetoder og aktørene som står bak synes mer og mer ressurssterke.

Det er ikke mulig å eliminere denne risikoen – angrep vil inntreffe og enkelte av disse vil være vellykkede sett fra angriperens side. En velfungerende koordinert innsats for å fange opp indikasjoner på angrep, minimere skade, redusere konsekvenser, gjenopprette sikker drift, samt etterforske IKT-sikkerhetshendelser, vil være viktig fremover på alle nivåer i samfunnet for å redusere risiko. Slik motstandskraft mot alvorlige IKT-sikkerhetshendelser etableres gjennom effektiv ressursbruk i et samspill mellom virksomhetene, sektorene og det nasjonale sektorovergripende nivået.

Håndtering av hendelser og kriser krever at involverte aktører samhandler så vel horisontalt som vertikalt med andre relevante aktører for å oppnå et best mulig resultat.
Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM) er to sentrale aktører innen samfunnssikkerhetsarbeidet. Innenfor samfunnsoppdraget til både DSB og NSM skal de begge ha oversikt over risiko og sårbarheter innenfor sine

ansvarsområder, og de skal være pådrivere i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser. Øvelser er ett av flere virkemidler regjeringen benytter for å bedre relevante aktørers evne til å håndtere en hendelse den dagen den oppstår (Instruks for departementenes arbeid med samfunnssikkerhet, Justis- og beredskapsdepartementet 1. september 2017). Evaluering av terrorhendelsene 22. juli avdekket at sentrale aktører med ansvar for kritiske samfunnsfunksjoner hadde utfordringer med koordinering og samhandling.

Formålet med denne oppgaven er å undersøke hvordan aktørene DSB og NSM tolker og etterlever samvirkeprinsippet, herunder hvordan det fungerte mellom aktørene under planleggingen av Øvelse IKT16.
Vi ønsker med denne oppgaven å besvare følgende problemstilling:

> *Hvordan etterlever aktørene Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?*

Vi utarbeidet i tillegg tre forskningsspørsmål for svare ut problemstillingen.

1. Hva legger DSB og NSM i begrepet samvirkeprinsippet?
2. Hvordan organiseres beredskapsplanlegging internt og eksternt i DSB og NSM?
3. Hvilke faktorer hemmer samhandling mellom DSB og NSM?

Forskningsspørsmålene hadde som mål både å få en klarhet i hvilke overordnede dokumenter og planer som er førende og legger premisser for hva som legges i prinsippet samvirkeprinsippet, og hvordan DSB og NSM samhandler og organiserer beredskapsarbeidet. Samtidig skulle forskningsspørsmålene kartlegge hvilke forventinger DSB og NSM har til hverandre og hva samhandling innebærer for aktørene.

Som metode for denne oppgaven har vi valgt en kvalitativ tilnærming, og vi har gjennomført intervjuer med representanter fra DSB og NSM. I tillegg har vi analysert relevante dokumenter for å finne ut i hvilken grad DSB og NSM etterlever samvirkeprinsippet. En utfordring vi har hatt gjennom arbeidet med oppgaven har vært at deler av dokumentasjonen er unntatt offentlighet jf. lov om rett til innsyn i dokument i offentleg verksemd (offentleglova).

Resultatet har blitt en oppgave som viser at selv om regjeringen innførte samvirkeprinsippet etter 22. juli, så viser erfaringer fra hendelser og øvelser, for eksempel Øvelse IKT16, at det fortsatt er behov for å styrke samvirket mellom beredskapsaktørene.

Denne oppgaven **konkluderer** med at intensjonen i samvirkeprinsippet mellom DSB og NSM i all hovedsak ble oppfylt under planleggingsfasen av Øvelse IKT16, men at det fortsatt er utfordringer knyttet til læring etter hendelser og øvelser. Både DSB og NSM er ansvarlige for beredskapsordninger og tiltak som skal bidra til å øke samfunnets totale evne til å håndtere IKT-hendelser.

Innholdsfortegnelse

Forkortelser

RSU	Regjeringens sikkerhetsutvalg
JD	Justis- og beredskapsdepartementet
FD	Forsvarsdepartementet
FAD	Fornyings og administrasjonsdepartementet
NSM	Nasjonal sikkerhetsmyndighet
DSB	Direktoratet for samfunnssikkerhet og beredskap
DIFI	Direktoratet for forvalting og ikt
NBS	Nasjonalt beredskapssystem
SBS	Sivilt beredskapssystem
BFF	Beredskapssystem for Forsvaret
NOU	Norsk offentlige utredninger
FCKS	Felles cyberkoordineringssenter
SRM	Sektorvise responsmiljøene
NØEF	Nasjonalt øvelses- og evalueringsforum
EKOM	All form for elektronisk kommunikasjon
IKT	Informasjon og kommunikasjonsteknologi
CERT	Computer Emergency Response Team
VDI	Nasjonalt varslingssystem for digital infrastruktur
DDoS	Distributed denial-of-service

Figurer

1 Innledning

Innledningsvis vil vi forklare bakgrunnen for vår problemstilling. Vi vil deretter si noe om hvilke temaer vi ønsker å belyse. Avslutningsvis vil vi si noe om hvilke avgrensinger vi har valgt, og hvordan vi har bygd opp oppgaven.

Den senere tids samfunnsutvikling, blant annet den teknologiske utviklingen, har bidratt til gjennomgripende samfunnsmessige endringer. Utviklingen har i tillegg ført til større sårbarheter, blant annet i form av lange og uoversiktlige verdikjeder, som gjerne spenner bredt over mange sektorer og flere land. En effekt av den digitale utviklingen er en kraftig endring i samfunnets risiko- og sårbarhetsbilde. Samfunnssikkerhet dreier seg både om proaktivt sikkerhetsarbeid for å hindre utvikling av kriser, samt om akutt håndtering av de krisesituasjoner vi ikke kan forebygge. Samfunnssikkerhet handler imidlertid også om læring etter kriser slik at vi står sterkere neste gang en eventuell krise skulle ramme oss, (Kruke 2012). En konkret definisjon av begrepet samfunnssikkerhet kom i St. meld. nr. 17 (2001-2002) Samfunnssikkerhet *«Veien til et mindre sårbart samfunn»*. I stortingsmeldingen ble samfunnssikkerhet definert som:

«Den evne samfunnet som sådan har til å opprettholde viktige samfunnsfunksjoner og ivareta borgernes liv, helse og grunnleggende behov under ulike former for påkjenninger».

Justis- og beredskapsdepartementet (JD) opprettet *Utvalget om digitale sårbarheter* ved kgl. res. 20. juni 2014. Utvalget leverte sin utredning i november 2015, (NOU 2015: 13) også omtalt som Lysneutvalgets rapport. Utvalget kom med en rekke anbefalinger for å minske den digitale sårbarheten. Av anbefalingene fremkommer blant annet at det er behov for å styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet, samt å etablere et helhetligrammverk for digital hendelseshåndtering.

En stor andel uønskede hendelser som rammer IKT-systemer er utilsiktede, men tilsiktede hendelser er et økende problem (Meld. St. 10 (2016-2017)). Det fremkommer videre av Lysneutvalgets rapport at for å minske de digitale sårbarheter kreves det samarbeid og samvirke mellom myndigheter, virksomheter og etater som har et selvstendig ansvar i arbeidet med forebygging, beredskap og krisehåndtering. Samvirkeprinsippet ble innført i Meld. St.

29 (2011-2012), og stiller «krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeid med forebygging, beredskap og krisehåndtering». Innføringen av samvirkeprinsippet medfører ingen endring i de tre øvrige prinsippene; ansvar, likhet og nærhet (NOU 2012: 14).

Samvirkeprinsippet er sentralt for utvikling og styrket beredskap i samfunnet, og er et sentralt tema i denne oppgaven. I Perspektiver på samfunnssikkerhet (Engen et. al. 2016) påpekes det at en virksomhets beredskapsplan tydelig skal presisere ansvarsforholdet for både offentlige og private aktører. Dette gjelder også for de frivillige aktører. Videre fremkommer det at en beredskapsplan må være fullt kompatibel med planer i andre relevante organisasjoner på samme nivå, og organisasjoner lavere og høyere i responshierarkiet. Det medfører behov for både vertikal og horisontal koordinering samt for koordinering på tvers av organisasjonsgrensene. I veileder utgitt av DSB, om *Departementenes systematiske samfunnssikkerhets- og beredskaps arbeid* (DSB 2015) fremkommer tilsvarende krav for departementene, herunder at planverket skal reflektere prinsippet om samvirke. Videre poengteres det at alle aktører har et selvstendig ansvar for å sikre et optimalt samvirke og samarbeid med andre relevante aktører, slik at best mulig utnyttelse av ressurser kan sikres på tvers av sektorer og ansvarsnivåer. Allerede i 1994 i kgl. res *Om Justisdepartementet samordningsfunksjon på beredskapssektoren* (kgl. res. 16.9.94), fikk Justisdepartementet et sektorovergripende ansvar innenfor det sivile beredskapsområdet, og departementet ble blant annet gitt et koordineringsansvar for den sivile beredskapssektoren. I kgl. res. 10. mars 2017 nr. 312 fikk Justis- og beredskapsdepartementet en generell samordningsrolle på samfunnssikkerhetsområdet. DSB understøtter departementet i samordningsrollen (Instruks for departementenes arbeid med samfunnssikkerhet 2017). Sentralt i denne oppgaven er empiri der våre funn kan være med å belyse og nyansere temaer knyttet til samvirke og samvirkeprinsippet.

1.1 Bakgrunn

De overordnede målene for samfunnssikkerhetsarbeidet er beskrevet i Meld. St. 10 (2016–17). Det er et mål for regjeringens arbeid med samfunnssikkerheten at befolkningen skal oppleve stor grad av trygghet gjennom:

- *Effektivt å forebygge og om mulig forhindre uønskede hendelser som kan true liv, helse, viktige verdier og myndighetsfunksjoner og andre kritiske samfunnsfunksjoner.*
- *Sikre en effektiv beredskap og operativ evne og kapasitet til å håndtere alvorlig kriminalitet, kriser og ulykker.*
- *Sikre god evne til raskt å gjenopprette samfunnskritiske funksjoner dersom uønskede hendelser ikke har latt seg forebygge.*
- *Sikre en god læring på grunnlag av inntrufne hendelser og øvelser.*

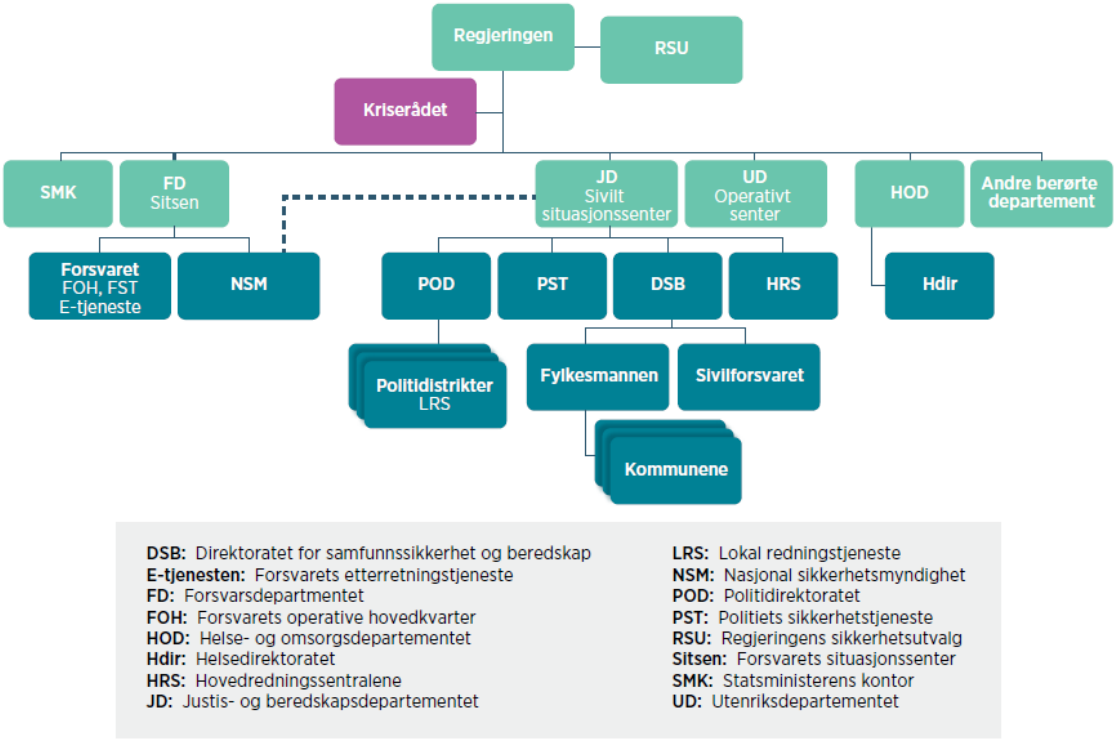
Utgangspunktet er at det enkelte departement har ansvar for samfunnssikkerhet og beredskap innenfor egen sektor. Justis- og beredskapsdepartementet har i tillegg til sitt sektoransvar en samordningsrolle for å sikre et helhetlig og koordinert arbeid med samfunnssikkerhet og beredskap på tvers av sektor. Arbeidet med samfunnssikkerhet og beredskap skal være: *«Målrettet, systematisk og sporbart og være integrert i departementets planverk, styringssystemer og i styringsdialogen med underliggende virksomheter»* (kgl. res. 15.06.12 – Instruks for departementenes med samfunnssikkerhet og beredskap. Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering). Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge gjennomført av DSB i 2016 omfatter spørsmål om befolkningens risikopersepsjon og inntrykk av beredskap i Norge. Undersøkelsen viser det er en relativt bred enighet i befolkningen om påstanden: *Norge er et trygt land å bo i*. En andel på 29 % oppgir at de alt i alt har et godt eller svært godt inntrykk av beredskapen mot større hendelser i Norge, mens en andel på 22 % oppgir at de alt i alt har et svært dårlig eller dårlig inntrykk av beredskapen mot større hendelser i Norge. En andel på 51 % av befolkningen oppgir at de er helt enig i denne påstanden at 35 % av befolkningen er mest bekymret for de kommende fem år er, terrorangrep på norsk jord og 30 % er bekymret eller svært bekymret for cyberangrep på styringssystemer. 69 % av befolkningen er minst bekymret for forsyningskrise (mangel på forsyning av mat, drivstoff eller lignende) og 66 % er ikke bekymret for krigshandlinger på norsk jord. Hendelsene innbyggerne tror at ansvarlige myndigheter vil håndtere best er naturhendelser som fjellskred (58 %), orkan (49 %) og flom (60 %) samt større transportulykker (53 %). Undersøkelsen konkluderer altså med at det kun er terrorangrep befolkningen er mer bekymret for enn cyberangrep på sentrale styringssystemer (Befolkningsundersøkelse om risikopersepsjon og beredskap i Norge, DSB 2016).

Allerede i 2000 slo Sårbarhetsutvalgets utredning fast at IKT-systemene har blitt en av samfunnets bærebjelker, og at samfunnet er blitt mer sårbart for svikt i disse systemene (NOU 2000: 24 Et sårbart samfunn). Lysneutvalget ble satt ned av regjeringen i 2014 for å kartlegge samfunnets digitale sårbarhet. Innenfor utvalgets mandat lå det å foreslå konkrete tiltak for å styrke beredskapen og å redusere den digitale sårbarheten. I den endelige rapporten som ble utgitt i november 2015 fastslo utvalget at Norge er blant verdens mest digitaliserte land, og at Internett og IKT-systemer er blitt stadig mer integrert i alle deler av samfunnet, herunder i kritiske samfunnsfunksjoner (NOU 2015: 13 Digital sårbarhet-sikkert samfunn). IKT-sikkerhet er en integrert del av arbeidet med samfunnssikkerhet og beredskap. IKT-sikkerhet omfatter både tekniske og administrative sikringstiltak, og innebærer beskyttelse av både IKT-systemer og informasjonen i disse iht. integritet, konfidensialitet og tilgjengelighet. IKT-sikkerhet handler derfor om beskyttelse av «alt» som er sårbart fordi det er koblet til, eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. Begrepet IKT-sikkerhet brukes i mange sammenhenger synonymt med begrepet cybersikkerhet. Vi vil i denne oppgaven benytte begrepet IKT-sikkerhet.

For departementene vil føringer som gis av JD, NSM og Direktoratet for forvaltning og IKT (DIFI) være et viktig grunnlag for dette arbeidet. Det samme vil retningslinjer gitt i Nasjonal strategi for informasjonssikkerhet (2012) og Handlingsplan – Nasjonal strategi for informasjonssikkerhet (2017). Informasjonssikkerhet defineres her som hvordan informasjonen beskyttes mot uønsket innsyn (konfidensialitet), at informasjonen er tilgjengelig når det er ønskelig (tilgjengelighet), og at informasjonen er beskyttet mot endring/manipulering (integritet). Hovedformål med å utgi en Nasjonal strategi for informasjonssikkerhet (2012) er å angi hvilken retning og hvilke prioriteringer som skal ligge til grunn for myndighetenes informasjonssikkerhetsarbeid de nærmeste årene. Strategien omtaler strategiske prioriteringer, og for hver prioritering er det angitt en målbeskrivelse for satsingen, statusbeskrivelse og utvalgte områder som skal vektlegges framover. Eksempler på utvalgte områder er å ivareta informasjonssikkerheten på en mer helhetlig og systematisk måte, styrke IKT-infrastruktur, sørge for felles tilnærming til informasjonssikkerhet i statsforvaltningen, sikre samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-hendelser og sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet. Strategien har også som hovedmål å kontinuerlig bidra til innsats for bevisstgjøring og høy

kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet.

Den nasjonale strategien er utarbeidet av Fornyings- administrasjons- og kirkedepartementet (FAD), Forsvarsdepartementet, JD og Samferdselsdepartementet. Oppfølgingen av strategien skal dessuten bidra til at beslutningstakere i offentlig og privat sektor spesielt, og befolkningen generelt, skal få økt bevissthet om hvilke sikkerhetsutfordringer vi står overfor. Det er Kommunal og moderniseringsdepartementets (KMD) ansvar å sørge for at statsforvaltningen har en felles tilnærming til arbeidet med informasjonssikkerhet. Med bakgrunn i dette har KMD utarbeidet en egen Handlingsplan – Nasjonal strategi for informasjonssikkerhet (2017). Roller og ansvar innenfor IKT-sikkerhetsområdet reguleres av en rekke lover og forskrifter. Det fremkommer av disse at Justis- og beredskapsdepartementet er gitt et samordningsansvar for IKT-sikkerhet i sivil sektor, både innenfor og utenfor sikkerhetsloven (kgl. res. 1.9.2017). Departementet har i tillegg ansvar for IKT-sikkerhet som faller inn under sikkerhetsloven i sivil sektor, og et generelt samordningsansvar for samfunnets sivile sikkerhet. Berørte fagdepartementer, myndigheter og næringslivet skal involveres i dette arbeidet.



TABELL 1. Organiseringen av sentral krisehåndtering ved sivile nasjonale kriser (iht. Meld. St. 21 (2012–2013) Terrorberedskap).

[13] Meld. St. 29 (2011–2012) Samfunnssikkerhet.

Figur 1: Organisering av sentral krisehåndtering ved sivile nasjonale kriser (Meld. St. 21 (2012-2013) Terrorberedskap).

Samfunnssikkerhetsarbeidet i Norge er organisert etter fire helt sentrale prinsipper. Dette er ansvar-, likhets-, nærhets - og samvirkeprinsippet (Meld. St. 29 (2011–2012) Samfunnssikkerhet).

«En gjennomgående erfaring etter 22. juli 2011 er at alle aktørene må samvirke for å sikre at innsatsen håndteres best mulig. Innføringen av samvirkeprinsippet som et bærende element i den nasjonale samfunnssikkerhets- og beredskapsarbeidet, gjøres blant annet på bakgrunn av erfaringene etter angrepene 22. juli (Meld. St. 29 (2011-2012) s.12). Samvirkeprinsippet stiller «krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre best mulig samvirke med relevante aktører og virksomheter i arbeid med forebygging, beredskap og krisehåndtering». Innføring av samvirkeprinsippet medfører ingen endring i de tre øvrige

*prinsippene; ansvar, nærhet og likhet» (*NOU 2012: 14). Prinsippet innebærer i praksis at alle organisasjoner skal ha et bevisst forhold til gjensidige avhengigheter, og hvilke andre organisasjoner det kan være aktuelt å samhandle med (Meld. St. 29 (2011-2012)).

I Samfunnssikkerhetsinstruksen (kgl. res. 1.9.2017- Instruks for departementenes arbeid med samfunnssikkerhet Justis- og beredskapsdepartementet) gis det ytterligere føringer for hvordan prinsippet skal forstås:

«*Samvirkeprinsippet betyr å utvikle gode former for samarbeid med de aktører det er nødvendig å samarbeide med, avklare og ta hensyn til avhengigheter, og se ressursene som helhet. Felles beredskapsforberedelser i form av planer, trening, øvelser, evaluering og læring står sentralt. Alle aktører har et selvstendig ansvar for å sikre et optimalt samvirke, koordinering og samarbeid med relevante aktører».*

Godt samvirke forutsetter altså forståelse, tillit og kjennskap til hverandres ressurser, kompetanse, organisering og kultur, og en vilje til å stille ressurser til disposisjon. Godt samvirke oppnås der partene møtes med en åpen holdning til andres perspektiv og kompetanse, og der oppmerksomheten er rettet mot at oppgaven totalt sett blir løst på best mulig måte. Beredskap betyr grovt sett å være beredt, altså å være forberedt på å håndtere krisesituasjoner.

*"Successful strategic crisis management is the result of 80 % generic planning, 15 % improvisation, and 5 % luck" (*Weisæth, L., et. al: 2002).

Weiseth argumenterer altså for at god planlegging er hovedfaktoren til vellykket krisehåndtering, resten beror på evnen til improvisasjon underveis og en dose flaks. I kapitel 3.2 kommer vi tilbake til beredskap og beredskapsplanlegging, hvor vi omtaler det nasjonale beredskapsplanverket og underliggende planverk. Formålet med denne oppgaven er å se nærmere på hvordan DSB og NSM etterlever samvirkeprinsippet. For å få svar på dette har vi blant annet studert planleggingsfasen av tidenes største Informasjons- og kommunikasjonsteknologi (IKT) øvelse i Norge, Øvelse IKT16. Årsaken til at vi har valgt disse aktørene er fordi DSB var ansvarlig for å gjennomføre øvelsen, og NSM hadde en sentral rolle inn i planleggingsarbeidet i kraft av sitt ansvar og fagmiljø for blant annet

informasjonssikkerhet. Nærmere omtale av aktørene er beskrevet i kapittel 2. Kontekst og kapittel. 2.1 Introduksjon til aktørene. Scenarioet i Øvelse IKT16 inneholdt omfattende IKT-angrep som lammet flere sektorer og forvaltningsområder, og så på hvordan samvirkeprinsippet ble utøvet under planleggingen av øvelsen mellom deltakere i øvelsen. Oversikt over deltakere i øvelsen er som vist i figur 2.

1.2 Problemstilling og forskningsspørsmål

Problemstillingen kunne vært knyttet opp til hvilken som helst sektor og forvaltningsområde, men vi har valgt å avgrense oppgaven til å se på samvirkeprinsippet og hvordan henholdsvis DSB og NSM etterlever dette.

Tittelen på denne oppgaven lyder som følger: Hvordan evner sentrale aktører å samhandle ved IKT-hendelser? Med bakgrunn i dette, har vi formulert følgende problemstilling for denne oppgaven:

> *Hvordan etterlever aktørene Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?*

Ut i fra denne har vi formulert tre forskningsspørsmål:

1. Hva legger DSB og NSM i begrepet samvirkeprinsippet?
2. Hvordan organiseres beredskapsplanlegging internt og eksternt i DSB og NSM?
3. Hvilke faktorer hemmer samhandling mellom DSB og NSM?

Det gjennomføres årlig en nasjonal tverrsektoriell øvelse med overordnet mål å øve samhandling på tvers av sektorer. I 2016 ble det øvet IKT-baserte hendelser, og øvelsen ble omtalt som Øvelse IKT16. For å besvare problemstillingen har vi gjennomført undersøkelser knyttet til planlegging og dels til gjennomføring av øvelsen. Vi har intervjuet relevante personer i de to virksomhetene og vi har gjennomført dokumentstudier.

1.3 Avgrensninger av oppgaven

Vi har valgt en avgrenset tilnærming der vi har hatt til hensikt å finne ut hvordan de to virksomhetene DSB og NSM tolker og etterlever samvirkeprinsippet. Mange deltagere fra offentlige og private virksomheter og fra ulike sektorer og forvaltningsområder var involvert i Øvelse IKT16, oversikten vises i figur 2, Deltakere i Øvelse IKT16. Vi har valgt å se på aktørene DSB og NSM fordi planleggingen av øvelsen skulle ledes av DSB i tett samarbeid med blant annet NSM, som også var sentral i utforming av scenario og ønskede øvningsmål.

Evalueringsrapporten etter Øvelse IKT16 er unntatt offentlighet. Ved begjæring om innsyn i rapporten ble vi innvilget delvis innsyn og har fått tilgang til kapittelet om *Myndighetenes opprettholdelse av tillit og troverdighet*, herunder informasjonshåndtering under gjennomføring øvelsen. I og med at evalueringsrapporten er unntatt offentlighet har vi primært konsentrert oss om å se på planleggingsfasen av Øvelse IKT16, der det var mulig for oss å få tilgang til informasjon. Planleggingsfasen var en omfattende prosess som gikk over ett år, og som DSB var hovedansvarlig for å gjennomføre. NSM ble også gitt en meget sentral rolle i planleggingsfasen ved at de mottok eget oppdragsbrev fra JD om å utvikle et rammeverk for digital hendelseshåndtering (Brev 5.4.2016 fra JD til NSM). Oppdraget var resultatet av en direkte anbefaling fra Lysneutvalget (NOU 2015: 13). Rammeverket for digital hendelseshåndtering er nærmere beskrevet i kapitel 5, Empiri.

DSB er en gitt oppgave med å understøtte JDs tilsynsrolle med departementene (kgl. res. 15.6.2012). Nærmere studier av hvordan DSB fyller denne rollen ville formentlig kunne ha gitt oss ytterligere informasjon om hvordan DSB tolker og etterlever samvirkeprinsippet. Av hensyn til omfanget av oppgaven har vi valgt ikke å gå nærmere inn på DSBs rolle som tilsynsetat på vegne av JD.

1.4 Oppbygning av oppgaven

Oppgaven er bygget opp av 7 hovedkapitler med underkapitler, i tillegg kommer referanser og vedlegg.

I kapitelene 1 og 2 presenteres innledningen som gir en beskrivelse av bakgrunnen for oppgaven. Videre introduseres valget av problemstilling, forskningsspørsmålene og avgrensning av oppgaven. Oversikt over aktørene i oppgaven og relevante lover og forskrifter inngår også i disse kapitlene.

Kapittel 3 omhandler det teoretiske rammeverket som anvendes for å belyse problemstillingen. Teorien bygger på relevante teorier om kriser, beredskap og beredskapsplanlegging, krisehåndtering og om samvirkebegrepene.

Kapitelet 4 tar for seg valg av metode og gjennomføringen av undersøkelsen. Metodekapittelet avsluttes med kritiske betraktninger knyttet til valg av metode og gjennomføringen av oppgaven.

I kapittel 5 presenteres empirien som viser en oversikt over de sentrale funnene fra dokumentstudier, forskningsspørsmålene og intervjuene.

Kapittel 6 tar for seg diskusjon som kobler sammen det teoretiske rammeverket med empirien, for å belyse og drøfte problemstillingen og forskningsspørsmålene.

I kapittel 7 presenteres konklusjoner i forbindelse med oppgavens problemstilling og tanker rundt videre forskning.

I kapittel 8 dokumenteres kildehenvisninger og referanser, samt relevante vedlegg til oppgaven.

2 Kontekst

2.1 Introduksjon av aktørene i oppgaven

Direktoratet for Samfunnssikkerhet og beredskap, (DSB) er underlagt Justis- og beredskaps departement (JD), og har en viktig rolle i å understøtte departementets ansvar for å samordne det nasjonale samfunnssikkerhets- og beredskapsarbeidet. DSB skal ha oversikt over risiko og sårbarheter i samfunnet, skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og skal sørge for god beredskap og effektiv ulykkes- og krisehåndtering. I tillegg er DSB fagmyndighet innen krisekommunikasjon. DSB utgir årlige scenarioanalyser. Analysene omhandler risiko knyttet til katastrofale hendelser som kan ramme det norske samfunnet og som samfunnet bør være forberedt på å møte. DSB skal i samarbeid med JD utarbeide ny veileder til departementenes samfunnssikkerhetsarbeid og iverksette tiltak for å gjøre veilederens innhold kjent (Tildelingsbrev fra Justis- og beredskapsdepartementet 2018).

Sentralt for denne oppgaven er DSBs oppdrag om å understøtte JDs koordineringsrolle innenfor det nasjonale samfunnssikkerhets- og beredskapsarbeid. (Instruks for Direktoratet for samfunnssikkerhet og beredskap 2005), og å understøtte JDs samordningsrolle på samfunns-sikkerhetsområdet (Samfunnssikkerhetsinstruksen 2017).

Direktoratets koordinering skal legge grunnlaget for et godt og helhetlig forebyggende arbeid og gode beredskapsforberedelser innenfor offentlig forvaltning og samfunnskritisk virksomhet. Koordineringsrollen ivaretas gjennom dialog og avklaringer med berørte parter,

hvor det tas utgangspunkt ansvaret øvrige departementer og sektorer har. DSB skal blant annet ha oversikt over sårbarhets- og beredskapsutviklingen i samfunnet og ta initiativ for å forebygge hendelser med sikte på å hindre tap av liv, helse, miljø, viktige samfunnsfunksjoner og store materielle verdier. Videre skal DSB bistå JD og øvrige departementer ved koordinering av håndtering av større kriser og katastrofer i fredstid på sivil side, herunder sikkerhetspolitiske kriser og i krig. Virksomheten skal også initiere, planlegge og gjennomføre nasjonale beredskapsøvelser på sivil side i tråd med fastsatte øvelsesplaner, og bistå departementene og deres sektorer med øvelses- og kompetansetiltak.

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. NSM er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. NSM er administrativt underlagt Forsvarsdepartementet, og rapporterer med faglig ansvarslinje til Justis- og beredskapsdepartementet for oppgaveløsning i sivil sektor og til Forsvarsdepartementet for militær sektor. NSM innhenter og vurderer informasjon av betydning for gjennomføring av forebyggende sikkerhetstjeneste. På bakgrunn av dette utarbeider NSM hvert år en rapport om et helhetlig IKT-risikobilde og sikkerhetstilstanden.

NSMs rapport, Risiko 2018 er én av fire trussel- og risikovurderinger som utgis årlig. De øvrige tre utgis av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og DSB. I rapporten, Risiko 2018 (NSM, 2018 s. 8) vurderer NSM risikoen for at samfunnet skal rammes av spionasje, sabotasje, terror og andre alvorlige handlinger. Følgende fremgår av rapporten:

«*Norge står overfor økende risiko for å bli rammet av sikkerhetstruende hendelser. Dette skyldes vedvarende, nye og et raskt økende antall sårbarheter, særlig innenfor det digitale domenet. Samtidig ser NSM en negativ utvikling i trusselbildet. Dette kan medføre at samfunnskonsekvensene av hendelser som skyldes ondsinnede handlinger øker*».

NSM er også utøvende organ i forhold til andre land og internasjonale organisasjoner. NSM skal innhente og vurdere informasjon av betydning for gjennomføringen av forebyggende sikkerhetstjeneste, samt søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester når dette tjener norske interesser. NSM skal videre føre

tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av sikkerhetsloven overholdes, og eventuelt gi pålegg om forbedringer, bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste. NSM skal drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur og et nasjonalt varslingssystem for digital infrastruktur og gi informasjon, råd og veiledning til virksomheter.

2.2 Lover og forskrifter

Lover og forskrifter gir viktige rammebetingelser for arbeidet med samfunnssikkerhet og beredskap. I dette avsnittet omtales de mest relevante lover, forskrifter og instrukser knyttet til samfunnssikkerhet og beredskap som er styrende for DSB og NSM.

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven)

LOV-1998-03-20-10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). **§ 1. Formål:**

a. *Loven har som formål å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser,*
b. *ivareta den enkeltes rettssikkerhet, og*
c. *trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste*

NSMs samfunnsoppdrag fremkommer av loven, herunder at NSM skal koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden. Videre skal NSM bidra til at sikkerhetstiltak utvikles, og at de skal iverksette forskning og utvikling på områder av betydning for forebyggende sikkerhetstjeneste.

Forskrift om informasjonssikkerhet

FOR-2001-07-01-744: Forskrift om informasjonssikkerhet. **§ 1-1. Formål og virkemåte:**

Forskriften har samme formål og virkeområde som sikkerhetsloven. Forskriften gjelder også for informasjon sikkerhetsgradert i samsvar med NATOs bestemmelser.

Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)

FOR-2017-09-01-1349: Instruks for departementenes arbeid med samfunnssikkerhet

Formålet: Denne instruksen presiser kravene til departementenes arbeid med samfunnssikkerhet. Formålet er å styrke samfunnets evne til å forebygge kriser og til å håndtere alvorlige hendelser gjennom et helhetlig og koordinert arbeid med samfunnssikkerhet.

Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller

FOR-2005-06-24-688: Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller. **1. Formålet med instruksen:**

Formålet med instruksen er å gi nærmere retningslinjer for hvordan Direktoratet for samfunnssikkerhet og beredskap (DSB) i praksis skal utøve sin koordinerende rolle i forhold til arbeid med samfunnssikkerhet og beredskap på sivil side, i forhold til aktiviteter, objekter og virksomhet med potensial for store ulykker, og i forhold til virksomheter som omfattes av storulykkeforskriften.

2.3 Øvelse IKT16

Fakta om øvelsen:
Justis- og beredskapsdepartementet vurderte i samråd med Forsvarsdepartementet og Samferdselsdepartementet at det var behov for gjennomføring av en tverrsektoriell nasjonal IKT-øvelse og besluttet å gjennomføre Øvelse IKT16. DSB fikk i oppdrag av Justis- og beredskapsdepartementet å være ansvarlig for planlegging, gjennomføring og evaluering av øvelsen (Brev 10.11.2015 fra JD til DSB). Arbeidet ble utført i tett samarbeid med NSM, Nasjonal kommunikasjonsmyndighet (Nkom), Forsvaret, politiet, PST og Difi. Øvelse IKT16 ble gjennomført 29. og 30. november 2016. Scenariet for øvelsen var et omfattende IKT-angrep som lammet flere sektorer og forvaltningsområder, og tok utgangspunkt i åpne trussel- og risikovurderinger fra NSM, PST og E-tjenesten (Regjeringen.no).

Formålet med øvelsen var å sette Norge bedre i stand til å håndtere et større IKT-angrep som rammer på tvers av sektorer. *Øvelsen skal ha fokus på konkret håndtering av et IKT-angrep, og i mindre grad håndtering av konsekvenser som følge av angrepet. Øvelsen skal inkludere relevante respons- og fagmiljøer, og skal inkludere sektorvise responsmiljøer slik at den nasjonale strukturen for IKT-hendelser blir testet. Samhandling, ansvars- og rolleavklaring mellom sektorer, fagmiljøer og forvaltningsnivåer skal stå sentralt* (Brev 10.11.2015 fra JD til DSB).

Øvelsen samlet deltagere fra over 50 offentlige og private virksomheter og de sektorvise responsmiljøer innen IKT.

Figur 2: Deltakere i Øvelse IKT16 (Øvingsdirektiv for Øvelse IKT16)

I forbindelse med Øvelse IKT16 ble det utgitt pressemelding på regjeringen.no der justis- og beredskapsminister Anders Anundsen uttalte:

- Tidenes største IKT-øvelse i Norge ble gjennomført 29. og 30. november 2016. Scenarioet for Øvelse IKT16 inneholdt omfattende IKT-angrep som lammet flere sektorer og forvaltningsområder.

– Vi øver for å bli bedre i stand til å håndtere et større IKT-angrep som rammer på tvers av sektorer. Da får vi testet hvordan vi varsler, samarbeider og rapporterer mellom sektorer og nivåer. Målet er at relevante myndigheter og responsmiljøer skal kunne varsle og håndtere et alvorlig IKT-angrep på en god måte, sier Anundsen videre. IKT-sikkerhet er et viktig satsingsområde for regjeringen. IKT-sikkerhetsarbeidet må sees i et helhetlig perspektiv, på tvers av sektorene, og i sammenheng med det øvrige arbeidet for samfunnssikkerhet. Øvelser er et viktig verktøy for å avdekke svakheter og forbedringspunkter, og derigjennom styrke evnen til håndtering av omfattende IKT-angrep.

– Norge er et av de mest digitaliserte landene i verden. Men den raske digitaliseringen har medført endringer i vårt risikobilde siden utviklingen også har ført med seg nye sårbarheter. Mange kritiske samfunnsfunksjoner er avhengig av digitale løsninger, og store IKT-angrep kan få omfattende konsekvenser dersom de ikke håndteres riktig og godt, sier justis- og beredskapsminister Anundsen (regjeringen.no).

3 Teori

I dette kapittelet vil vi ta for oss relevant teori som danner grunnlaget for å drøfte problemstillingen og forskningsspørsmålene. Det teoretiske grunnlaget som er valgt er knyttet opp til sentrale begreper i denne oppgaven, kriser, beredskap og beredskapsplanlegging, øvelser, krisehåndtering, herunder definisjoner av beredskapsprinsippene og særskilt samvirkeprinsippet. Valg av teori er gjort på bakgrunn av oppgavens problemstilling, herunder forskningsspørsmålene.

3.1 Kriser

3.1.1 Definisjon på kriser

Ordet krise, kommer fra det greske ordet *krisis* og betyr avgjørende vending, plutselig forandring, skjebnesvanger endring. Ordet har lenge vært i brukt i det norske språket i ulike sammenhenger (Cullberg 1994). Det finnes mange slags kriser og nesten like mange definisjoner på hva en krise er:

«En alvorlig trussel mot strukturer, verdier og normer i et sosialt system som under tidspress og usikkerhet gjør det nødvendig å foreta kritiske beslutninger» (Rosenthal, Charles, 't Hart 1989:10).

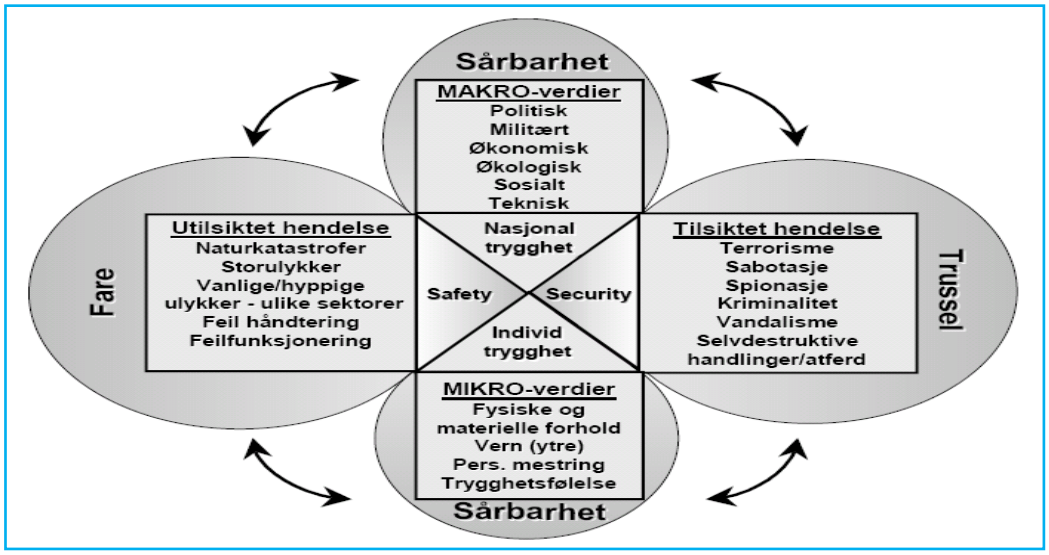
22. juli-kommisjonen viser i sin rapport til professor Arjen Boins definisjon av en krise. I følge Boin *utgjør krisen en alvorlig trussel mot grunnleggende samfunnsstrukturer – eller mot sentrale verdier knyttet til sikkerhet, velferd, liv og helse – som krever en rask reaksjon under stor grad av usikkerhet* (NOU 2012: 14 s. 209).

DSB opererer med et utvidet krisebegrep som sier at en virksomhet er i krise når det oppstår en situasjon som truer eller kan true virksomhetens kjernevirksomhet og/eller troverdighet. NOU 2000: 24 – *Et sårbart samfunn, 2.3.3; DSB (2001), Informasjonsberedskap og strategisk krisekommunikasjon, s. 8.).*

Vi ser at alle definisjonene peker på en uønsket hendelse, og at hendelsen vil svekke eller ramme en organisasjon, viktige samfunnsverdier, et sosialt system eller et samfunn. Rosenthal et. al. (1989, i Engen, Kruke, Lindøe, Olsen, Olsen og Pettersen 2016) peker dessuten på behovet for å fatte kritiske beslutninger under tidspress. Definisjonene til både Rosenthal et. al. (1989, s. 10) og Boin (gjengitt i NOU 2012: 14 s. 209) synes å være sentrale for IKT-hendelser som vi ser nærmere på i denne oppgaven. Som tidligere nevnt har den digitale utviklingen ført til større sårbarheter, gjerne i form av lange og uoversiktlige verdikjeder, som spenner bredt over mange sektorer og land (NOU 2015: 13). Så vel ikke tilsiktede, som tilsiktede hendelser vil derav kunne ramme grunnleggende infrastruktur og viktige samfunnsverdier horisontalt og vertikalt, både nasjonalt og internasjonalt, og det vil være behov for å fatte beslutninger. Beslutningene vil gjerne måtte tas under tidspress og med mangelfullt beslutningsgrunnlag i den hensikt å gjenopprette situasjonen. Kriser er uforutsigbare i sin natur, og de krever at beslutninger tas raskt uten at man nødvendigvis forutser følgene de vil få. Det er likevel mulig å planlegge for at kriser kan oppstå, og ha et system for å håndtere disse. Dette vil vi komme nærmere tilbake til i kapittel 3.2 Beredskap og beredskapsplanlegging.

3.1.2 Ulike kriser

Det finnes ulike typer kriser. Kriser som oppstår plutselig og på kort varsel, og kriser som er av mer langvarig karakter. Eksempler på ulike kriser er naturkatastrofer, samfunnsskapte kriser, sammenbrudd i teknologiske systemer, opprør eller sosiale konflikter, terrorangrep, sult og epidemier og komplekse humanitære kriser. Figur 3 nedenfor illustrerer omfang og mangfold av kriser og sårbarhet for samfunnet og individet generelt. Den presenteres som en oversikt over kompleksiteten som dreier seg om forhold knyttet til sårbarheter i ulike samfunnsfunksjoner, utilsiktede hendelser og overlagte ondsinnede handlinger som kan ha stor betydning for samfunnssikkerhet. Den vertikale aksen beskriver sårbarhet i alt fra nasjonale institusjoner til faktorer som påvirker trygghet for enkeltmennesker (Kruke, Olsen, og Hovden 2005).



Figur 3: Sikkerhetens omfang og mangfold (Kruke, Olsen, og Hovden 2005).

Teknologiske kriser eller feil i teknologiske systemer, kan ramme befolkningen og lokalsamfunnet på ulike måter. Med teknologi forstår vi materielle objekter, teknikker og kunnskap som gir oss mennesker mulighet til å endre og kontrollere den materielle verden. I følge Engen (Engen et. al. 2016) er teknologi derfor både konkret og abstrakt.

Engen legger videre vekt på at teknologi og samfunn er sammenvevd ved blant annet at svikt eller forstyrrelser i et teknologisk system, som for eksempel elektrisitetsforsyningen, raskt blir kritisk for mange mennesker (Engen et. al. 2016). Dette skaper systemiske risikoer i samfunnet. Bortfall av kritisk infrastruktur som datatrafikk eller transport kan få store konsekvenser, og liv og helse kan stå på spill. Videre fremgår det av (Engen et. al. 2016) at Norge har opplevd samfunnskritiske kriser i form av både strøm og mobilbrudd av kortere varighet de siste årene og at digitalisering har medført at feil i programvare et sted kan få konsekvenser for hele nettet til mobiloperatørene. Hendelsen i Telenors mobilnett i juni 2011 som rammet samfunnskritisk infrastrukturer er et eksempel på samfunnskritiske kriser som omtales av (Engen et. al. 2016).

Engen et. al. (2016) omtaler kritisk infrastruktur som teknologiske systemer som leverer løsninger og tjenester av stor betydning for samfunnet. Videre fremkommer det at teknologi er materielle objekter, teknikker og kunnskap som gir menneskene muligheter til å endre og kontrollere den materielle verden og er både konkret og abstrakt.

3.1.3 Gundels krisematrise

Stephan Gundel klassifiserer kriser i fire kategorier (Gundel, 2005). Han begrunner behovet for klassifisering med at første steg i å kontrollere krisen er å gi den navn og senere analysere den. Vet vi hvilken type krise det dreier seg om, kan vi ta frem «verktøykassen» som passer typen krise vi står overfor, og dermed dra nyttig erfaring fra tidligere kriser.

"Dealing with crises means dealing with nightmares and nightmares become less of a threat if someone turns on the light" (Gundel 2005:106).

Gundel sin modell beskriver en klassifisering av kriser basert på deres forutsigbarhet og mulighet for påvirkning. Modellen illustrerer i hvilken grad kriser kan forutsees (predictability) og i hvor stor grad ansvarlige myndigheter kan påvirke krisen (influence), før eller under krisen. Gundel trekker fram at det er mulig å identifisere fire karakteristiske krisetyper, som vist i figur 4; konvensjonelle, uventede, upåvirkelige og fundamentale kriser.

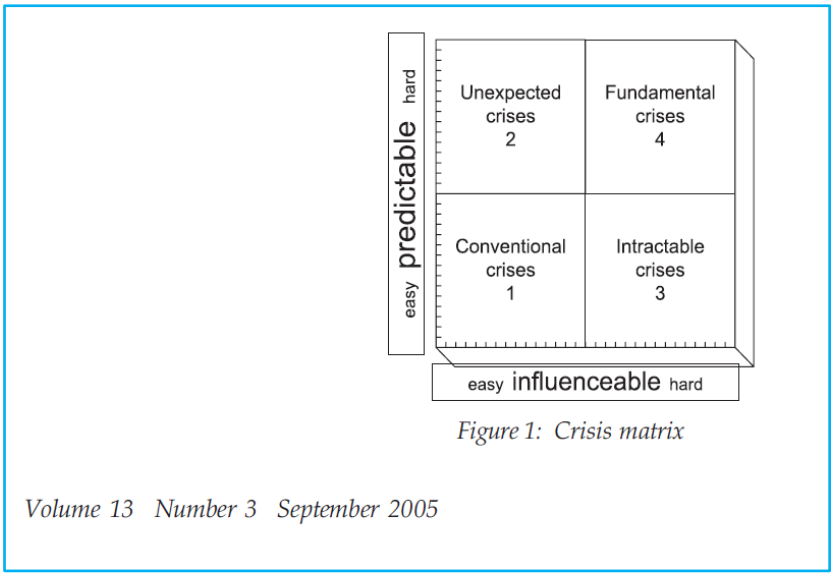


Figure 1: Crisis matrix

Volume 13 Number 3 September 2005

Figur 4: Krisematrise: Forutsigbarhet og mulighet for påvirkning (Gundel 2005:112).

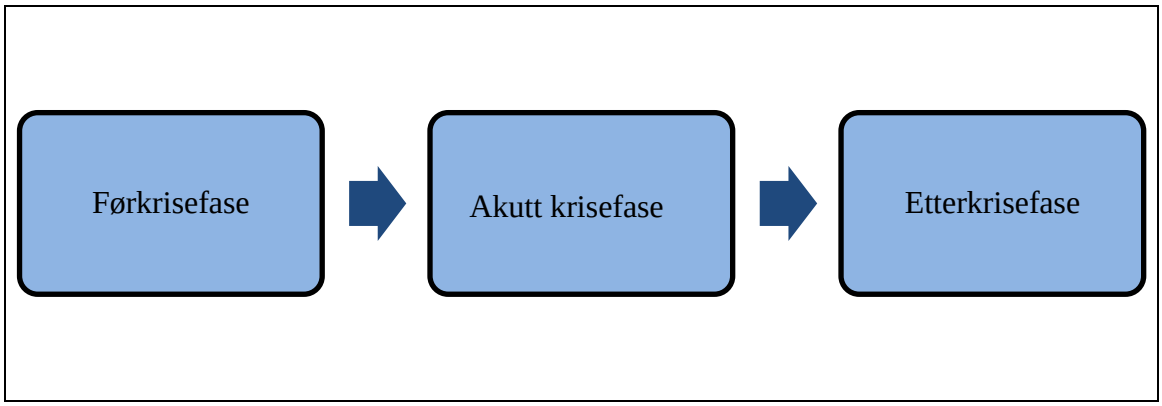
En konvensjonell krise (1) kjennetegnes ved opplevelsen av at man har tid til rådighet og at krisen er kontrollerbar som følge av tidligere erfaringer. Uventede kriser (2) er ofte preget av mangel på kontroll og tidligere erfaringer, samt uklare årsak og virkningsforhold.

En upåvirkelig krise (3) er ofte preget av vanskelige forhold og i liten grad av påvirkningskraft under og etter krisen. Denne typen kriser kalles også for politiske kriser, ettersom de ofte leder til konflikter og debatt omkring etablerte institusjoner og definisjonskamper mellom aktører. Det er ofte uenighet om hvordan krisen oppstod, hvordan den bør defineres og håndteres.

Den mest komplekse typen av kriser ansees å være en fundamental krise. Den kjennetegnes av uventede og uoversiktlige hendelser som er vanskelige å håndtere og kartlegge. Gundel poengterer at krisens utviklingshastighet vil påvirke i hvor stor grad de ansvarlige myndigheter opplever at de kan påvirke og kontrollere krisen. Bear et. al. (2005) og Garreau (2005) (gjengitt i Boin, 2009), omtaler også utfordringer knyttet til innføring av teknologi, blant annet til at teknologiutviklingen akselererer i et forbløffende tempo, hvilket skaper revolusjonerende muligheter, men at dette også innebærer utfordringer som det er vanskelig å se for seg.

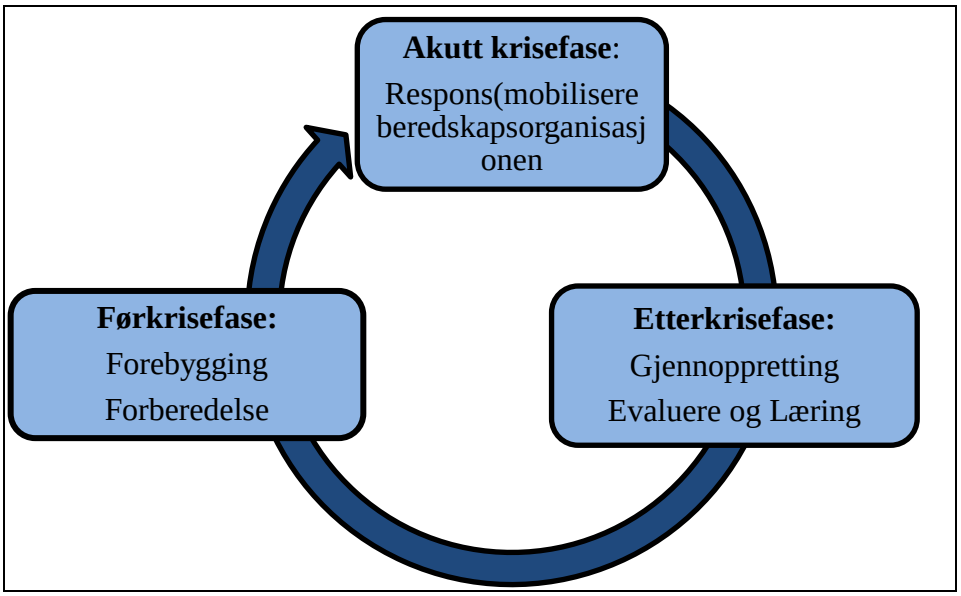
3.1.4 Krisefaser

Engen et. al. (2016) presenterer krisefaser som en lineær og sirkulære prosess. Figur 5 viser krise som en lineær prosess, der krise blir delt inn i tre fundamentale faser, førkrisefase, akutt krisefase og etterkrisefase. Den lineære faseinndelingen peker på at en krise har en klart definert start og slutt. For å få en helhetlig tilnærming til samfunnssikkerhet og beredskap må akutt-fasen sees i sammenheng med førkrigfasen, ved å identifisere trusler og vurdere risikoer. En krise er en dynamisk hendelse som bør betraktes som en prosess som starter lenge før den akutte situasjonen inntreffer, og som kan vare lengre enn slutten på den akutte krisefasen.



Figur 5: Krisefaser som en lineær prosess basert på Engen et. al. (2016).

En annen måte å presentere krisefasene på er som en sirkulær prosess som vist i figur 6. Essensen i den sirkulære prosessen er at en vil alltid komme tilbake til en førkrisefase etter en krise. Det vil ikke si at en kommer tilbake til den samme førkrisefasen, slik tilstanden var når krisen for første gang ble skapt. Derimot er tanken ved den sirkulære prosessen at læring skal ha skjedd. Hensikten er å ta med seg erfaring fra førkrisefasen, akutt krisefasen og etterkrisefasen, i forhold til beredskap og krisehåndtering, inn i den nye førkrisefasen. Det vil forhåpentligvis føre til at samfunnet er mer motstandsdyktig mot neste krise som kommer (Engen et. al. 2016). En konsekvens av å erkjenne at vi er i en førkrisefase i forhold til neste krise, kan være at en er mer varsom for de svake signalene som viser at en akutt krise er på vei.



Figur 6: Krisefaser som en sirkulær prosess basert på Engen et. al. (2016).

De ulike krisefasene inngår som en del av en kontinuerlig prosess av beredskapsarbeidet. Førkrisefasen er rettet mot forståelse og erkjennelse av krisen og i denne fasen inngår risiko og beredskapsanalyse, beredskapsplan, etablere beredskapsstrukturer og ressurser. I akuttfasen inngår respons og mobilisering av beredskap og i etterkrisefasen inngår normalisering, gjenoppretting, evaluering og læring.

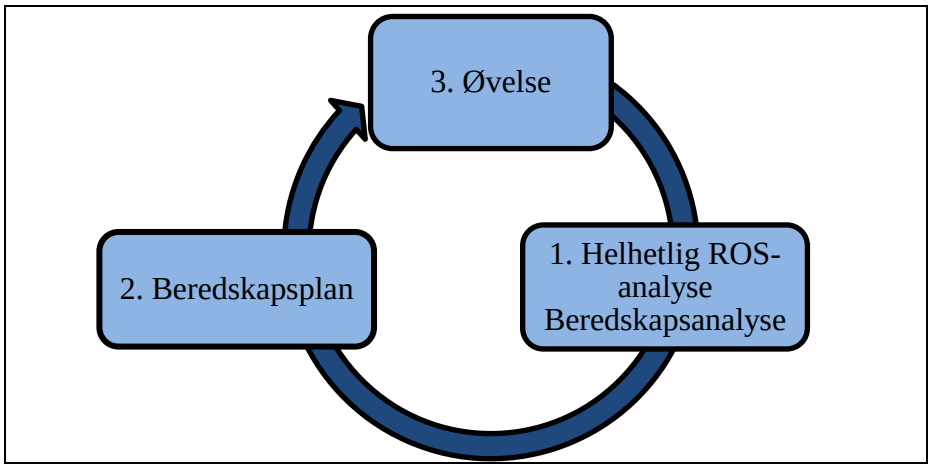
I dette studiet vil det være naturlig å fokusere på fasen som handler om forebygging, forberedelser og planlegging, altså førkrisefasen. Dette fordi studiet vil undersøke planleggingsfasen av Øvelse IKT16. Med utgangspunkt i dette må vi se på et utvidet krisebegrep. Det utvidede krisebegrepet ser den akutte fasen i sammenheng med både

førkrisefasen og etterkrisefasen i forrige krise, noe som må til for at vi skal få en helhetlig tilnærming til samfunnssikkerhets- og beredskapsarbeidet. Kvaliteten på krisehåndteringen i den akutte fasen vil være helt avhengig av hva som er gjort av forebygging og forberedelser i førkrisefasen. Sentralt i forberedelsene for krisehåndtering står beredskap og beredskapsarbeid (Engen et. alt. 2016).

3.2 Beredskap og beredskapsplanlegging

Engen et. al. (2016, s. 280) beskriver at beredskap grovt sett «betyr å være forberedt», det vil si å være forberedt på å kunne håndtere en situasjon. Beredskap er på mange måter å forberede seg på å håndtere en ekstraordinær situasjon, og kan defineres som «*tiltak for å forebygge, begrense eller håndtere ekstraordinære hendelser*». Engen et. al. (2016) viser her til NOU (2000: 24), og påpeker i det videre at formålet med beredskap er å forutse mulige trusler og utfordringer slik at de kan håndteres på en effektiv måte, for så å etablere ressurser og utstyr for å håndtere disse. Engen et. al. (2016) viser til at god beredskap bygger på flere aktiviteter og presenterer disse over fire faser:

- Det må innledningsvis gjennomføres analyser av risiko for å etablere en oversikt over aktuelle trusler eller farer, trusler eller farer som historisk har påvirket samfunnet, samt fremtidens nye potensielle trusler, vi viser her til (Perry og Lindell 2003).
- For det andre vil en beredskapsanalyse både gi rammene for hendelser det skal etableres beredskap for, samt dimensjonering av beredskapen for disse hendelsene.
- For det tredje vil en beredskapsplan dokumentere den beredskapen som etableres (organisering, utstyr, ressurser) på bakgrunn av analysene.
- For det fjerde vil relevant trening og øving, samt mobilisering i krisesituasjoner, gi grunnlag for evaluering av beredskapen som er etablert. Modellen under viser denne sammenhengen.



Figur 7: Sammenheng mellom ROS, beredskapsplan og øvelser basert på Engen et. al. (2016).

Det fremkommer videre av Engen et. al. (2016) at en beredskapsplan skal sikre samvirke og tydelig presisere ansvarsforholdet for alle involverte aktører. Det gjelder spesielt for offentlige og private aktører, men også for frivillige aktører. En viktig suksessfaktor i håndteringen av større kriser er effektiviteten i samarbeidet mellom ulike responsaktører. Kompleksiteten i samfunnet øker, noe som medfører at kriser og katastrofer involverer stadig flere aktører. Samvirkeprinsippet har derfor kommet inne som et sentralt prinsipp i samfunnssikkerhets- og beredskapsarbeidet. Engen et. al. (2016) viser til at samvirkeprinsippet er omtalt i St. meld nr. 29 (2011-2012). Organisasjonene må kjenne til hverandres mandater, strukturer, kapasiteter og begrensinger, samt mekanismer for koordinering for best mulig å benytte de ofte begrensede ressursene som er tilgjengelige. I henhold til Perry og Lindell (2003 s. 338) er beredskapsforberedelser et svar samfunnet har på trusler fra omgivelsene. De definerer beredskap som:

«The readiness of a political jurisdiction to react constructively to threats from the environment in a way that minimizes the negative consequences of impact for the health and safety of individuals and the integrity and functioning of physical structures and systems».

Det er flere forfattere som tilbyr retningslinjer eller kriterier for beredskapsplanlegging, blant annet Perry og Lindell (2003) og Quarantelli (1998). I Guidelines for the Emergency Planning Process (Perry og Lindell, 2003:226) fremgår det at siden terrorangrepene 11. september 2001, har regjeringer over hele verden investert betydelige ressurser i å utarbeide berskapsplaner om terrorisme. Spesielt i USA har den føderale regjeringen opprettet nye lokale sikkerhetsorganisasjoner og oppfordret statlige og lokale myndigheter til å utarbeide

lokale planer. Den store vektleggingen av skriftlige planer har en tendens til å trekke oppmerksomheten bort fra planleggingsprosessen og det opprinnelige målet om å oppnå samfunnsberedskap. Beredskap er dynamisk og betinget av pågående prosesser. En skriftlig beredskapsplan er en viktig del av, men ikke en tilstrekkelig betingelse for, fellesskapets beredskap. Beredskap er en tilstand. En skriftlig beredskapsplan garanterer ikke beredskap. Å kunne utvikle et godt beredskapsplanverk avhenger også av de menneskene som står bak planverket og deres kompetanse (Perry og Lindell 2003). I retningslinjene gjennomgås konseptene for samfunnsberedskap og beredskapsplanlegging, og deres forhold til trening, øvelser og skriftlig plan. Det er særlig de 10 retningslinjer med vekt på den kontinuerlige planleggingsprosessen som reflekterer hvor det kan oppnås en hensiktsmessig og praktisk krisehåndtering. Retningslinjene baserer seg på beredskapslitteratur for natur- og teknologiske katastrofer, og kan benyttes til enhver miljømessig trussel. I det følgende omtales 4 av de 10 retningslinjene som vi anser som mest relevant for vår problemstilling (Perry og Lindell 2003):

- *Beredskap bør være basert på nøyaktig kunnskap om trusselen og om sannsynlig menneskelig respons.* Riktig kunnskap om trusselen kommer fra trusselvurderinger og sårbarhetsanalyser som kartlegger hvilke trusler virksomheten står ovenfor og sannsynligheten for at den inntreffer. Retningslinjen er en påminnelse om å finne den mest tilgjengelige kunnskapen, vel viten om at det beste ikke nødvendigvis er det optimale.

- *Beredskapsplanlegging bør fokusere på tverrfaglig koordinering.* Den fjerde retningslinjen omhandler at krisehåndtering i stor grad handler om oppnåelsen av tverrfaglig koordinering og samhandling mellom gruppene som skal håndtere krisen.

- *Beredskap bør inkludere opplæring av sentrale ressurser*. Planleggingsprosesser har mange målgrupper, blant annet fordi mange forskjellige personer, roller og organisasjoner er inkludert beredskapsplanene og involvert i øvelser.

- *Effektiv planlegging bør sørge for å teste foreslåtte responsoperasjoner.* Øvelser av beredskapsplaner bidrar til kommunikasjon med alle aktørene i planverket kommer i kontakt med hverandre. Øvelser bidrar også til økt kunnskap og omfattende prøving av beredskapsplaner, personell, prosedyrer, muligheter, utstyr og materiell.

Quarantelli (1998) presenterer også generelle prinsipper eller retningslinjer for god beredskapsplanlegging. Han påpeker at kvaliteten på beredskapsplanleggingen avhenger av i hvilken grad planleggingen faktisk møter disse prinsippene. Han mener med andre ord at det er mulig å si noe om kvaliteten på en beredskapsplanlegging før beredskapen testes i en øvelse eller i en virkelig hendelse.

Begrepet helhetlig beredskap har vært brukt i lengre tid og det har vært et overordnet mål å systematisere fragmentert beredskaps- og samfunnssikkerhetsarbeid. Denne tankegangen om system og helhet er tatt videre. Basert på sentrale statlige føringer, og som viktige bidrag til å forebygge uønskede hendelser, bygge robuste samfunn og være bedre forberedt på å håndtere eventuelle kriser, er det sentralt i arbeidet med beredskapsarbeid at det gjennomføres risiko- og sårbarhetsanalyser og internkontroll som et styringsprinsipp (Aven et. al. 2004). Dette kan også sees på som en del av systemtenkningen i beredskapsarbeidet. Helhetlig beredskap skal etableres som begrep for å samle og integrere de forskjellige tiltak innen beredskapsarbeidet. Systemtenkningen skal være grunnlaget for å ivareta samfunnssikkerhet i arealplanleggingen.

En viktig suksessfaktor i håndteringen av større kriser er effektiviteten i samarbeidet mellom ulike responsaktører. Organisasjoner må kjenne hverandres mandater, strukturer, kapasiteter og begrensinger samt mekaniser for koordinering, for på best mulig måte å kunne utnytte de ofte begrensede ressursene. Bred kunnskap om de forskjellige organisasjonene og hvordan de er avhengig av hverandre må komme ut av beredskapsprosessen, og det vises til øvelser som et virkemiddel for å sette et kritisk søkelys på beredskapsplanverket, prosedyrer, nivået på ansatte, fasiliteter, utstyr og ressurser (Engen et. al. 2016). Øvelser omtales i det videre i kapittel 3.3.

Kultur

Engen et. al. (2016) diskuterer betydningen av kultur som faktor for sikkerheten i organisasjoner, og om kultur er noe man *har* eller om det er noe som *er*, og viser til at organisasjonskultur i forvaltningen ble trukket frem som en av forklaringene på den dårlige håndteringen av terrorangrepene 22. juli 2011. Etter Tsjernobylkatastrofen har det vært gjort mange forsøk på å definere og operasjonalisere begrepet sikkerhetskultur, og det har vært gjennomført empiriske undersøkelser uten at forskere og sikkerhetseksperter har blitt enige om kulturens betydning for sikkerheten. Flere organisasjonsteoretikere, blant annet Turner og Pidgeon (1997) mener at kultur omhandler et til tider komplekst system av symboler og

meninger, bestående av myter, ritualer og andre verdimessige uttrykk som gjennomsyrer sikkerheten i en organisasjon. I følge Engen et. al. (2016) er omtalen av 22. juli-kommisjonens behandling av forvaltningskulturen i stor grad beskrevet som noe som *er*, og at man må anerkjenne betydningen av kultur knyttet til det ikke å se farer og problemer, også blant ledere. I følge Turner og Pidgeon (1997) uttrykker kulturer systemer av meninger, der en bestemt gruppe forstår verden rundt seg.

3.3 Øvelser

Øvelser inngår som en sentral del av beredskapsprosessen og er viktig for å kunne teste ut beredskapen hos ulike organisasjoner og robusthet i infrastruktur og institusjonell praksis. Det er naturlig å tenke at øvelser har effekt på hvordan vi håndterer uønskede hendelser. Øvelser kan sees på som en del av en sammenhengende prosess, bestående av planlegging, trening øving og oppdatering av planverk og beredskapsressurser og strukturer (Engen et. al. 2016). Øvelser og trening gir rom for både innspill til de grunnleggende analysene og til eventuelle behov for justeringer av beredskapsplaner. I veileder fra 2015 skriver DSB at øvelser er et viktig virkemiddel for å trene krisehåndtering og teste planverket. Øvelser skal videre gjøre aktørene bedre rustet til å ivareta sine oppgaver i håndteringen av uønskede hendelser eller kriser. Gjennom øvelser får deltakerne viktig lærdom om sine beredskapsplaner og organisasjon og forbedringspunkter (Departementenes systematiske samfunnssikkerhets og beredskapsarbeid, DSB 2015).

Forskrift om kommunal beredskapsplikt § 7. *Øvelser og opplæring* omhandler hvilke krav kommunene må ivareta når det gjelder gjennomføring av øvelser. Kommunen er pliktet til å gjennomføre øvelser annen hvert år der scenarioene for øvelsene bør hentes fra kommunens helhetlige risiko- og sårbarhetsanalyse (Engen et. al. 2016). Det vises videre til at det er tre forskjellige typer øvelser; *tabletopøvelser*, *funksjonelle øvelser* og *fullskalaøvelser*. Øvelsene varierer i omfang, målsetning, metodikk, grad av realisme og involvering av aktører. Tabletopøvelser er en forenklet form for øvelse, og har lav kompleksitet og bærer preg av rask organisering. Slike øvelser innebærer at deltakerne diskuterer seg frem til handlingsvalg med utgangspunkt i oppgaver som tar for seg ulike scenarioer. Funksjonelle øvelser krever flere ressurser, både i form av planlegging og gjennomføring, men legger til rette for å teste deler av beredskapsplanen. En funksjonell øvelse har mer realisme enn rundbordøvelser, men har likevel begrensninger i samvirke med andre aktører. Den siste øvelsesformen er fullskalaøvelser, som beskrives som den mest omfattende og krevende av de tre.

Fullskalaøvelser tar utgangspunkt i realistiske scenarioer, og preges av høyt stress og tidspress. Øvelsene er svært ressurskrevende, både i planlegging, gjennomføring og etterarbeid av øvelsen. I fullskalaøvelser involveres hele beredskapsorganisasjonen, og formålet med øvelsen er å se hvordan organisasjonen fungerer i en helhet og i samvirke med andre aktører (Engen et. al. 2016). Tidligere gjennomførte øvelser slik som Cyberangrep i Ukraina, Telenors Cyberdawn 2013, Nasjonal cyberøvelse for ekom og IKT16 kan ansees som fullskalaøvelser. Her øver aktørene blant annet på samvirke seg imellom, hvor de også må forholde seg til andre aktører og virksomheter. Dette kan eksempelvis være virksomheter som er inkludert i felles infrastruktur og inngår i scenariet for øvelsene. Det er ofte involvering av mange ulike aktører i øvelsene. Aktørene vil som oftest ha en rolle dersom en gitt hendelse inntreffer. Dette kan være ansatte, avdelinger, organisasjoner.. Engen peker på at for å få tilfredsstillende utbytte av øvelser bør en rekke aktører involveres (Engen et. al 2016). Øvelse IKT16 er et eksempel på en slik øvelse hvor relevante og sektorvis responsmiljøer er inkludert slik at den nasjonale strukturen for IKT-hendelser skal kunne testes. Samhandling, ansvar- og rolleavklaring mellom sektorer, fagmiljøer og forvaltningsnivåer er sentralt i fullskalaøvelser. Oversikten over aktørene i Øvelse IKT16 er gjengitt i figur 2.) Engen viser til at en øvelse må være så realistisk og nær opp til en virkelig hendelse som mulig for at organisasjonen skal få tilstrekkelig læring av øvelsene (Engen et. al. (2016). Dette vil fremme muligheten for læring hos aktørene.

3.4 Krisehåndtering

Krisehåndtering må sees i forbindelse til kriser, beredskap og beredskapsplanlegging beskrevet i kapitlene 3.1 og 3.2. Målet med beredskapsarbeid er å forberede oss på å håndtere kriser som kan oppstå. Engen har beskrevet fasene i en krisehåndtering og vi har valgt denne modellen fordi vi mener at disse modellene gir de grundigste beskrivelsene av krisehåndteringen (Engen et. al. 2016). Som beskrevet i kapittel 3.1.4 har Engen delt beredskapsarbeidet i relasjon til kriser inn i 3 faser:

1. *Førkrisfase:* Denne fasen preges av å forberede samfunnet til å kunne håndtere en ventet eller uventet krise. Her vil risikoanalyse, beredskapsanalyse, beredskapsplan og etablering av beredskapsstrukturer og ressurser være sentrale temaer.

2. *Akutt krisefase:* Denne fasen preges av at en uønsket hendelse har inntruffet og utløst en krisesituasjon. Sentrale temaer her er alarmering, utrykning og den første akutte innsatsen på ulykkesstedet.
3. *Etterkrisefase:* Der krisen normaliseres og evalueres og man tar lærdom av de virkelige hendelsene som finner sted eller som man trener og øver på. Kruke, Olsen et. al. (2016) ser på fasene som en sirkulær prosess og ikke som en lineær prosess.

Gundel (2005) har utviklet modeller for å kunne forstå og beskrive kriser, jf. Gundels krisematrise for å karakterisere krisetypologi, fig.4. Kruke og Olsen (2012) påpeker at det å forstå og beskrive kriser er vesentlig for å være i stand til å lede krisehåndteringen og i denne konteksten selve endringsprosessen. Hvordan man ser på den aktuelle situasjonen og videre hvordan man velger å kategorisere den, er avgjørende for beslutningstaking og for hvordan beslutningene følges opp i praksis.

3.4.1 Krisekommunikasjon

Engen et. al (2016) påpeker at kommunikasjon mellom ulike responsaktører er avgjørende for nødvendig informasjonsutveksling og koordinering, og videre at samvirkeprinsippet hviler på en forutsetning om at de involverte aktørene klarer å kommunisere med hverandre. Engen et.al. (2016) viser til Timothy Coombs et. al. (2010), en anerkjent forsker på krisekommunikasjon som beskriver krisekommunikasjon som en prosess bestående av kunnskapsforvaltning og styring av respons eller reaksjon. Det genereres kunnskap i kriser, og denne kunnskapen må kommuniseres til dem som trenger den, og det må etterfølge en nødvendig respons på kunnskapen som gjør at konsekvensene av krisen, skadeomfanget, reduseres mest mulig (ibid).

Det fremkommer videre av Engen et. al. (2016) at kunnskapsgenerering betyr å få tak i informasjon om hva som skjer i en krisesituasjon og om få situasjonsforståelse. Engen (2016) vises her til Endsley (1988) og Weick m.fl. (1999). Den genererte kunnskapen kommuniseres så til relevante aktører som analyserer kunnskapen og danner seg et mer overordnet bilde på hva som skjer. Denne kunnskapsforvaltningen danner så grunnlaget for en respons som er tilpasset den situasjonsforståelsen som kommer ut av kunnskapsforvaltningen. Krisekommunikasjon kan sees på som en fortløpende prosess mellom ulike aktører i en krise, med det formål å få mottakere til å ta hensyn til informasjonen i sin respons på krisen. Engen et. al. (2016) definerer derfor krisekommunikasjon som kommunikasjon med det formål å få

aktører til å tilpasse sin adferd til den informasjonen som kommuniseres i en krise. Dette mener vi er svært relevant teori opp mot hovedtemaet i vår oppgave. Et omfattende ikt-angrep vil kunne sette kritisk infrastruktur ut av funksjon og ramme sentrale samfunnsfunksjoner, som blant annet strømforsyning og banktjenester. I en slik situasjon vil det være avgjørende at myndighetene er i stand til å kommunisere til befolkningen på en måte som gjør at befolkningen responderer på den måten som myndighetene ønsker i den gitte situasjonen. Engen et. al. (2016) diskuterer videre spørsmålet om tillit i krisekommunikasjonen, og det trekkes fram aspekter som kredibiliteten eller troverdigheten til informanten og gyldigheten til informasjonen. Det er derfor viktig at krisehåndteringen og krisekommunikasjonen er fundamentert på et gyldig informasjonsgrunnlag.

3.5 Samvirke

3.5.1 Sam-begrepene

Samvirke kan defineres som «*å arbeide sammen for et bestemt mål eller formål*» (Kristiansen et. al. 2017 s. 16 og 26), og videre som «*en prosess hvor beredskapsaktører i fellesskap løser felles problemer»*. Kristiansen et. al. (2017, s. 11) viser til at begrepet samvirke er beslektet med begrepene samhandling og samarbeid. Begrepet samvirke benyttes når ulike hierarkier og organisatoriske enheter jobber opp mot hverandre i en krisesituasjon, mens samhandling og samarbeid brukes i forbindelse med hva som skjer i et team og internt i et hierarki (ibid).

I mangel på en etablert definisjon i Norge støtter Holtan et. al. (2015) seg til en svensk definisjon av samvirke:

*"Den interaksjon som skjer mellom to eller flere aktører i den hensikt å samordne sine virksomheter og at samordning av virksomheter innebærer at disse koordineres for å oppnå felles mål. "[...] Samvirke er den metode som velges når de aktørene hvis virksomhet som skal samordnes med er selvstendige i forhold til hverandre og ingen part har beslutningsrett overfor hverandre» (*Wahlberg mfl., 2003 gjengitt i Holtan mfl., 2015:12).

Engen et. al. (2016, s 283 og 289) viser til den definisjonen av samvirkeprinsippet som er omtalt i St. meld nr. 29 (2011-2012): *"Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering"*.

Samvirkeprinsippet kan dermed forstås som en interaksjon mellom aktører som i utgangspunktet ikke er avhengige av hverandre, men som i fellesskap og over tid arbeider mot felles overordnede mål. Samhandling og samarbeid kan sees på som arbeidsformer som benyttes internt i organisasjoner og i arbeidsgrupper og team.

For denne oppgaven vil det være relevant å benytte definisjonen av samvirkeprinsippet som Engen et. al. (2016) viser til, med henvisning til St. meld nr. 29 (2011-2012).

4 Metode

Formålet med dette kapittelet er å presentere metoden som vi har brukt underveis i denne oppgaven, våre refleksjoner over valg av metode, datainnsamling og hvilke vurderinger vi har foretatt med hensyn til validitet (gyldighet) og reliabilitet (pålitelighet). Vi vil også gjennomgå hvilke utfordringer oppgaven har gitt i forhold til valg av metode, gjennomføring av intervjuer, svare ut forskningsspørsmålene og utforming av oppgaven.

4.1 Kort om metode

" Før jeg ved, hva jeg skal undersøge, kan jeg ikke vide, hvordan jeg skal gjøre det." Dette sitatet av den danske samfunnsforskeren Jette Fog (1979) gir på en enkel og grei måte uttrykk for metodeforståelse. Sitatet markerer klart at man står ovenfor et valg av metoder, og at man har flere likestilte metodiske tilnærmingsmåter innenfor samfunnsvitenskapene. Disse går gjerne under navnene kvalitative og kvantitative metoder. Jacobsen (2005) legger til at metode er et hjelpemiddel for å gi en beskrivelse av virkeligheten, og sier at hensikten med en empirisk undersøkelse er å framskaffe kunnskap. Metode et hjelpemiddel i vår oppgave og de har både sterke og svake sider i forhold til gyldighet og pålitelighet. Det viktige er at vi velger den metoden som er best egnet ut fra den problemstillingen vi arbeider med (Jacobsen 2005). Robert Yin omtaler en temastudie som en empirisk undersøkelse av et samtidig fenomen i dets virkelige livs rammer (Yin 2012). Det betyr at resultatene ikke kan generaliseres, men formålet er å komme frem til mer kunnskap og bedre problemstillinger. Yin sier videre at en temastudie er å foretrekke når slike samtidige fenomener og hendelser analyseres i tilfeller hvor forskeren ikke har noen direkte kontroll med analyseenheten. Vår mulighet til å påvirke svarene i undersøkelsen er et slikt samtidig fenomen uten mulighet til manipulering.

Det er ikke noe absolutt skille mellom kvalitative og kvantitative metoder. Grovt og enkelt kan man si at den grunnleggende forskjellen kommer til uttrykk i det at en innenfor

kvantitativ metode omformer data til tall og mengdestørrelser. Ut fra det gjennomfører man så statistiske analyser. Innenfor kvalitative metoder er det forskerens forståelse eller tolkning av informasjoner som står sentralt, for eksempel tolkning av meningsrammer, motiver, sosiale prosesser eller sammenhenger. Alt dette har den fellesnevneren at det ikke kan, eller bør tallfestes. Kvalitative undersøkelser er preget av fleksibilitet og kvantitative undersøkelsen av strukturering. Dette kommer klart til uttrykk dersom man sammenligner en intervjuguide fra en kvalitativ intervjuundersøkelse med et spørreskjema fra en kvantitativ spørreundersøkelse. Kvantitative tilnærminger har sin styrke i å forklare fenomen og gjennom statistiske teknikker kan man også gjøre generaliseringer. Siktemålet med kvalitative undersøkelser er i større grad å skape økt forståelse for de problemene man arbeider med.

4.2 Valg av metode

4.2.1 Kvalitativ metode

Metoden for datainnsamling i vår oppgave var blant annet en kvalitativ undersøkelsesmetode med intervju. Som tidligere nevnt gir kvantitative spørsmål gode svar i den betydningen at de egner seg for sammenligning. På den annen side ville vi kunne miste verdifulle tolkninger som ikke kommer frem i ja/nei svar, men som vi ville kunne fått i åpne spørsmål. Ved å benytte kvalitativ metode kommer man ofte tett på menneskene man skal intervjue og de kvalitative spørsmålene gir rom for at informantene kan svare utfyllende og gi" gode" svar på hvorfor de svarte som de gjorde. Jacobsen (2005) hevder at ved å benytte kvalitativ metode kan man ikke intervjue mange personer. En øvrig ramme på 20 er ofte mer enn nok. Det finnes ikke bare ett, men flere ulike kriterier for utvelgelse av informanter, som for eksempel tilfeldig utvalg, bredde og variasjon. På bakgrunn av vår problemstilling var det naturlig å svare på denne ved å benytte intervjuer som datainnsamlingsmetode. Kriteriene for utvelgelse av informantene er basert på en målrettet utvalgsmetode ved at vi har valgt ut informanter med mye kunnskap som vi mener kan gi oss mye god og interessant informasjon (Jacobsen 2005). I vårt arbeid med gjennomføring av intervjuene og for å få svar på forskningsspørsmålene, ble vi henvist av både DSB og NSM til gjennomgang av offentlige dokumenter, slik som NOU 'er, veiledninger, høringssvar med flere. Unntaket fra dette var at vi fikk tilgang til DSBs krisehåndteringsplan fra november 2017. Krisehåndteringsplanen beskriver systemer og rutiner for respons til uønskede hendelser uavhengig av årsak til hendelsen og hvor den finner sted. I tillegg har vi benyttet Øvelse IKT16 for å belyse samhandling mellom ulike aktører, øvelsen er nærmere omtalt i kapittel 2.3 Øvelse IKT16.

4.2.2 Hvem vi har intervjuet og hvorfor

En utvalgsprosess kan sies å gå gjennom et sett definerte faser og steg. Det første steget i enhver utvalgsundersøkelse, er å få en mest mulig fullstendig oversikt over alle de vi ønsker å undersøke. For å besvare oppgavens problemstilling ble det viktig å finne antallet enheter og de rette informantene (Jacobsen 2005). Regjeringen fremhever i Meld. St. 10 (2016-2017) «*Risiko i et trygt samfunn*», at funn etter reelle hendelser og øvelser skal følges opp gjennom en ledelsesforankret tiltaksplan. Vi hadde derfor som utgangspunkt at vi ønsket å snakke med informantene som representerte ledelsesnivået i NSM og DSB. Med lederforankring som utgangspunkt tok vi innledningsvis telefonisk kontakt med avdelingsledere som den ene av forfatterne hadde kjennskap til gjennom Justis -og beredskapsdepartementet. Vi søkte i den innledende fasen av utvelgelsesprosessen å få kartlagt hvordan samvirkeprinsippet fungerte under planleggingen av Øvelse IKT16, og vi ble henvist til navngitte personer på saksbehandlernivå som hadde jobbet aktivt med forberedelsene til øvelsen gjennom et helt år. Vi fikk totalt oppgitt navnet på seks personer. En av disse viste seg å ha permisjon, og ble derfor ikke fulgt opp. Ved telefonisk henvendelse til de øvrige fem personene fikk vi positiv respons på vår forespørsel om de ønsket å bidra til undersøkelsen. Den ene av de fem responderte ikke på vår neste henvendelse og ble ikke ytterlige fulgt opp. Vi intervjuet derav i alt fire informanter, to fra hver virksomhet. Utvalget av informantene kunne i stor grad hjelpe oss med å belyse den delen av problemstillingen som er knyttet til Øvelse IKT16. De hadde alle hatt roller i planleggingsarbeidet gjennom et helt år, og var godt kjent med de prosessene som var gjennomført. Videre fikk vi nyttige innspill til sentrale dokumenter som kunne bidra til å svare ut forskningsspørsmålene.

4.2.3 Gjennomføring av intervjuene

Etter en innledende telefonsamtale med informantene utformet vi et følgebrev hvor vi forklarte formålet med masteroppgaven, og hvor vi ba om den enkeltes samtykke til å bli intervjuet. Vi utarbeidet videre en intervjuguide basert på de spørsmålene vi ønsket svar på. Slik fikk vi ivaretatt nødvendig informasjon til og samtykke fra informantene. I den ene virksomheten ble det stilt som premiss at spørsmålene ble godkjent på ledernivå før selve intervjuet fant sted og dette ble fulgt opp. Intervjuene foregikk med personlig oppmøte på den ene informantens arbeidsplass, et ved oppmøte på den ene forfatterens arbeidsplass, og de to siste intervjuene ble av praktiske hensyn foretatt over telefon. Intervjuene varte mellom 30 og 90 minutter. Det ble ikke benyttet opptak under gjennomføringen av intervjuene. Umiddelbart

etter intervjuene ble notatgrunnlaget renskrevet og sendt til informantene på epost for gjennomgang slik at feil og mangler kunne korrigeres. I den ene virksomheten ble også svarene lederforankret ved at grunnlaget ble oversendt informantenes nærmeste leder. Grunnlaget stod urørt etter lederforankring. Funn fra intervjuene er sammenfattet og ligger til grunn for den senere analysen og drøftingen i denne oppgaven.

4.2.4 Dokumentanalyse

Dokumentanalyse er en forskningstradisjon innenfor kvalitativ metode. Ordet dokument refererer til alle skriftlige kilder som er relevante for forskerens analyse, som brev eller offentlige dokumenter. Hensikten med dokumentanalysen er å få et helhetlig bilde av ulike typer bakgrunnsdokumenter (Jacobsen 2005). Gjennom dokumentanalyse får man oversikt over ulike opplysninger hvor man selv nødvendigvis ikke har tilgang til alle kildene. Ved bruk av dokumentanalyse må kildene som analyseres vurderes etter den konteksten de settes i. I oppgaven har vi analysert relevante dokumenter for å finne ut i hvilken grad de sentrale aktørene DSB og NSM etterlever samvirkeprinsippet. Som empirisk materiale har vi tatt utgangspunkt i rapporten fra 22. juli-kommisjonen (NOU 2012: 14), andre relevante NOUer og relevante stortingsmeldinger. Vi har videre benyttet offentlige dokumenter fra Øvelse IKT16 og utført litteratursøk for å få mer informasjon om øvelsen. I tillegg har vi gjennomgått offentlige tilgjengelige dokumenter produsert av både DSB og NSM som understøtter hvordan de to etatene etterlever samvirkeprinsippet. Vi har også fått delvis innsyn i dokumenter som er unntatt offentlighet. Et eksempel er DSBs kriseplan.

Den samlede litteraturen anser vi som tilstrekkelig grunnlag til å finne svar på problemstillingen og forskningsspørsmålene. Aktuelle offentlige dokumenter, som for eksempel NOU `er, stortingsmeldinger, høringssvar og veiledere, er i hovedsak funnet på hjemmesidene til regjeringen, DSB og NSM. I tillegg er det foretatt litteratursøk etter hva det har vært behov for å finne mer informasjon om, som for eksempel statistisk materiale.

4.3 Relabilitet og validitet

Forskning tilsier at det er viktig å vurdere om de data man samler inn og bruker er av tilstrekkelig kvalitet til at man kan bruke dem til å trekke konklusjoner. De to vanligste måtene å måle datakvalitet på, er å sjekke reliabilitet og validitet. Validitet kan forklares som

gyldighet, og reliabilitet kan forklares som pålitelighet, det vi ønsker er resultater som er riktige og som vi kan stole på (Jacobsen 2005).

4.3.1 Reliabilitet (pålitelighet)

Vi har gjennom valg av metode forsøkt å fremstille hvordan vi har gått frem for å begrunne våre valg med tanke på å sørge for å ivareta påliteligheten i dataene vi har samlet inn. For å styrke påliteligheten i oppgaven, har vi gitt detaljerte beskrivelser av teori og metodevalg og begrunnet disse. Vi har videre beskrevet konteksten for datainnsamlingen og hvordan intervjuene ble utført. I kapittel 5.2, der resultatene av intervjuene blir presentert, har vi gjengitt sitater fra kildematerialet. Informantenes uttalelser blir igjen tolket og drøftet i kapittel 6. Dette gjør analyseprosessen tydelig for de som skal lese oppgaven og er i tillegg med på å sikre oppgavens pålitelighet. I drøftingsdelen sørger vi for reflektert diskusjon og drøfting. En svakhet ved oppgaven er at NSM og delvis DSB kun uttalte seg generelt med hensyn til forskningsspørsmålene. De henviste oss som tidligere informert til offentlige dokumenter som svar på spørsmålene. Dette var noe vi ikke på forhånd var forberedt på og dette kan svekke pålitelighet av funnene som har kommet fram i denne oppgaven.

4.3.2 Validitet (gyldighet)

Validitet er knyttet til tolkning av data og handler om gyldigheten av de tolkninger forskeren kommer frem til. Begrepet validitet kan understrekes ved å stille spørsmål om de tolkninger vi kommer frem til er gyldige i forhold til den problemstillingen vi har formulert. Forskeren styrker validiteten ved å gå kritisk gjennom analyseprosessen (Yin 2012). For å ivareta validitet i masteroppgaven har vi stilt kritiske spørsmål til våre vurderinger av datamaterialet. Å vurdere validitet handler også om det finnes annen forskning som kan bekrefte funnene i oppgaven. I denne oppgaven har vi valgt å styrke validiteten ved å referere til relevant teori og empiri som er fremskaffet på en så god måte som overhode mulig for å få kunnskap om vår problemstilling. I tillegg har vi fått nyttig og kritisk veiledning gjennom hele prosessen. Validitet kan deles inn i intern og ekstern validitet.

Intern validitet

Intern validitet handler om gyldigheten i dataene og informasjonen som er samlet inn. Før en kan trekke konklusjoner ut fra dataene må de være testet på en aller annen måte for videre å bli kvalitetssikret (Jacobsen 2005). Intern gyldighet går på om resultatene oppfattes som riktige, hvorvidt forskningen har dekning i dataene for de konklusjonene som trekkes. Testen

av gyldighet kan skje gjennom å vise funn og resultater til de menneskene som har gitt informasjonen, eller gjennom å kritisk gjennomgå resultatene (ibid). Får å oppnå best mulig intern gyldighet ønsket vi at informantene selv skulle gjennomgå og kontrollere informasjonen som ble nedskrevetetter intervjuet. Da vil informantene ha mulighet til å gi en indikasjon på om de kjenner seg igjen i oppsummeringen som ble presentert. Dette kalles informantvalidering, og måten vi valgte å gjennomføre dette på var å oppsummere i slutten av hvert intervju hva vi hadde oppfattet gjennom intervjuet. Da fikk informantene mulighet til å bekrefte eller rette på vår oppfatning av informasjonen som hadde blitt gitt i intervjuet. I tillegg til informantvalidering gikk vi selv gjennom intervjuene og resultatene, for å sikre en så god intern gyldighet som mulig.

Ekstern validitet

Ekstern validitet handler om hvorvidt funnene man gjør kan generaliseres, i tillegg sier ekstern validitet også noe om overførbarhet. Jacobsen (2005) understreker at kvalitative metoder sjeldent har til hensikt å generalisere de utvalgte enhetene som studeres til en større gruppe enheter (populasjonen). Det å slå fast omfanget eller hyppigheten av et fenomen er også i liten grad formålet til kvalitative metoder. Dette studiet har ikke hatt som mål å være generaliserende, likevel kan vi trekke flere sammenligninger og se flere tendenser, som kan si noe om forholdene utover de virksomhetene vi har valgt. Samstemmighet og likheter på flere områder har gjort det mulig å danne seg et bilde av samvirke i de virksomhetene vi har valgt ut. Disse likhetene og sammenhengene kan tyde på at funnene har relevans, utover de virksomhetene vi har studert. For å styrke den eksterne gyldigheten ytterligere kunne flere informanter fra DSB og NSM blitt intervjuet. Ved å inkludere flere informanter ville dette kunne bidratt til tydeligere å se mønstre og likhetstrekk, samt å styrke eller svekke de ulike funnene.

Etiske refleksjoner

Grunnleggende prinsipper for forholdet mellom informant og forsker bygger på informert samtykke, krav om privatliv og korrekt gjengivelse av datagrunnlaget som blir samlet inn (Jakobsen 2005). Dette har vi forsøkt ivaretatt ved at informantene fikk informasjon i eget følgebrev om formålet med oppgaven. I følgebrevet opplyste vi om at alle informantene og svarene ville bli anonymisert. Vi informerte samtidig om at vi har taushetsplikt. En oppsummering etter intervjuene ble oversendt informantene for gjennomgang, og i tillegg fikk de

informasjon om hvordan vi skulle benytte datamaterialet samt at notater fra intervjuene ville bli makulert. For å ivareta konfidensialitet har vi valgt å ikke gjengi hvilke avdelinger informantene organisatorisk tilhører. Vi mener at vi på denne måten har ivaretatt åpenhet og konfidensialitet til informantene og deres besvarelse (Jacobsen 2005).

Den ene av oppgaveskriverens stilling har medført refleksjoner rundt det faktum at dette studiet er gjennomført mot underliggende etater og hvilke utfordringer det eventuelt kunne medføre. Det er ikke direkte styringslinje mellom avdelingen oppgaveskriveren jobber i og de underliggende etatene. Likevel møtes oppgaveskriveren og enkelte av informantene på noen arenaer, og da gjerne i en kontekst hvor oppgaveskriverens rolle har vært av overordnet karakter. Det ble reflektert noe rundt denne problemstilling og hvilke konsekvenser dette kunne få for informantenes svar, som for eksempel å sette egen virksomhet i dårlig lys. Det er knyttet noe usikkerhet til om den ene oppgaveskriverens stilling *faktisk* bidro til en slik påvirkning. Relativt likelydende tilbakemeldinger fra informantene kan tolkes i en slik retning, men dette blir kun en tolkning fra vår side. For det andre var det behov for å tenke gjennom om oppgaveskriverens kunnskap om fagområdet i dette studiet ville bidra til noe forutinntatthet fra vår side. Samvirkeprinsippet er ikke knyttet til en virksomhet eller en sektor, den bakenforliggende forventingen gjelder alle aktører som har en rolle innen samfunnssikkerhetsarbeidet. Likevel tilflyter det informasjon via kommunikasjonskanaler i arbeidslivet til begge oppgaveskriverne som på et mer overordnet nivå sier noe om hvordan samvirkeprinsippet etterleves. Nå er det slik at forsking i sin natur neppe kan være helt objektiv, dette gjelder også for oss, og etter vår vurdering er det både fordeler og ulemper knyttet til å ha kunnskap om feltet det forskes på. En relativ god forståelse for historikk og problemstillinger kan være en fordel, men her må man være oppmerksom på at førkunnskap kan resultere i at vi som oppgaveskrivere kan fatte feilslutninger. Vi hører det informantene sier uten egentlig å lytte tilstrekkelig til det som faktisk blir sagt. Slike feilslutninger kan forekomme når man selv har innsikt i en problemstilling som blir undersøkt (Olsvik 2013).

5 Empiri

Dette kapittelet omhandler resultater fra datainnsamlingen, innhentet fra dokumentstudier og intervjuene. Denne informasjonen vil sammenholdes med teoribidragene i den kommende

drøftingen. Målet er å belyse utvalgt empiri som gjør det mulig å besvare problemstillingen og forskningsspørsmålene. Følgende dokumenter vil bli presentert i dette kapittel:

- Rapport fra 22. juli kommisjonen
- Lysneutvalgets rapport
- Rammeverk for digital hendelseshåndtering
- IKT trusselbildet
- Mørketallsundersøkelsen 2016
- Evalueringsrapport Øvelse IKT16

5.1 Dokumentstudier

5.1.1 Rapport fra 22. juli-kommisjonen

Rapporten fra 22. juli-kommisjonen (NOU 2012: 14) beskriver en grundig og nøktern, men svært detaljert gjennomgang av terrorangrepene som skjedde mot regjeringskvartalet og mot AUF-leiren på Utøya. Kommisjonens gjennomgang peker på en rekke kritikkverdige forhold og fundamentale utfordringer både i det forebyggende arbeidet fra myndighetenes side og i forbindelse med håndteringen av hendelsene. Utfordringene er særskilt knyttet til risikoforståelse og sikkerhetskultur i flere av etatene som er ansvarlige for samfunnssikkerhet og beredskap i Norge. Blant annet fremheves behovet for å forstå og forbedre kommunikasjon, samhandling og informasjonsflyt mellom ulike offentlige og private aktører som er involvert i arbeidet med samfunnssikkerhet. I tillegg stiller kommisjonen spørsmål ved gjennomføringsevnen til offentlige myndigheter og etater, det vil si evnen til å bruke resultater fra risikovurderinger til å iverksette risikoreduserende tiltak. Den peker videre på betydelige behov for endringer og går langt i å begrunne årsakene til at myndighetene sviktet i å ivareta sikkerhet og beredskapsoppgaver på tvers av sektorer, som blant annet mangel på samhandling. I følge kommisjonen var noe av årsaken at det manglet erkjennelse av hvilke farer samfunnet står ovenfor, en manglende evne til å koordinere og samhandle på tvers av etater og sektorer og til å gjennomføre planer og vedtak, samt dårlig lederskap og kommunikasjon. Kommisjonen konkluderer med at svikten i stor grad handlet om kultur, holdning og ledelse og at lederskap må begynne på toppen (NOU 2012:14 s. 16).

Videre kommer kommisjonen med 31 anbefalinger, der kommisjonens viktigste anbefaling er at «*ledere på alle nivå i forvaltningen systematisk arbeider med å styrke sine egne og organisasjonenes grunnleggende holdninger og kultur knyttet til risikoerkjennelse,*

gjennomføringsevne, samhandling, IKT-utnyttelse, og resultatorientert lederskap» (NOU, 2012: 14 s. 458).

Stortingsmeldingen om samfunnssikkerhet levert våren 2012 (Meld. St. 29 (2011-2012)), tar til orde for at et *samvirkeprinsipp* legges til de etablerte prinsipper om ansvar, likhet og nærhet, og dette er etter kommisjonens oppfatning et godt initiativ (NOU 2012: 14 s. 454). De øvrige prinsippene er ytterligere omtalt noe senere i dette avsnittet.

22. juli kommisjonens granskning etter terroraksjonen har medført at forventningene til beredskap har økt, noe som også er beskrevet i utredningen om ny sikkerhetslov (Samhandling for sikkerhet NOU 2016: 19, s.18). Den nye sikkerhetsloven legger betydelig vekt på samvirke mellom ulike aktører og samarbeid på tvers av sektorer og nivå. «*Nasjonen Norge er ikke sterkere enn det svakeste ledd, og reell samhandling for sikkerhet er den viktigste forutsetningen for å lykkes i å forbedre Norges sikkerhet – skritt for skritt*».

Det fremkommer videre av rapporten at DSB i 2010 gjennomførte et kritisk tilsyn med FADs arbeid med samfunnssikkerhet og beredskap. Her framkom det at FAD burde styrke krisehåndteringsevnen slik at den samsvarte med det risiko- og sårbarhetsbildet som ble lagt til grunn for departementets sikkerhetsarbeid knyttet til regjeringskvartalets bygninger. Dette ble også påpekt ved tilsyn i 2007. Som et viktig virkemiddel ble det pekt på gjennomføring av øvelser og evaluering av øvelser. Kommisjonens hovedanbefaling var: «*Ledere på alle nivåer av forvaltningen systematisk arbeider med å styrke sine egne og organisasjonens grunnleggende holdninger og kultur knyttet til risikoerkjennelse, gjennomføringsevne, samhandling, IKT utnyttelse og resultatorientert lederskap»* (NOU 2012: 14 s. 458).

Har samfunnssikkerheten blitt bedre etter 22. juli 2011? I Sintef sin populærvitenskapelige rapport fra forskningsprosjektet *The next disaster (NEXUS*), fremkommer det at risikoerkjennelsen i samfunnet generelt og blant aktører som arbeider med samfunnssikkerhet og beredskap, har økt. Terrorangrepene 22. juli 2011 ser ut til å ha hatt en lignende effekt på samfunnssikkerhets- og beredskapsområdet som Alexander Kielland-ulykken hadde på HMS-arbeidet i norsk petroleumsvirksomhet (Rapport fra NTNU: 2017).
Dette i form av en økt bevissthet om at hendelser med lav sannsynlighet og store konsekvenser må komme på dagsorden og bli prioritert. Det øves mer, og scenarioene er mer krevende enn tidligere – ikke bare i form av større og flere hendelser, men også gjennom

involvering av flere aktører og økt fokus på samvirke. En omfattende rekke med tiltak er iverksatt i justissektoren. De aller fleste av disse er imidlertid av strukturell art, mens 22. juli kommisjonens hovedkonklusjon i stor grad pekte på kulturelle utfordringer. I tiden etter 22. juli 2011 ble mye ressurser brukt på samfunnssikkerhet på relativt kort tid. Disse ressursene har imidlertid blitt skjevt fordelt mellom de ulike forvaltningsnivåene. Det kommunale og regionale nivået har ikke blitt styrket i samme grad som departements- og direktoratsnivået. Dette til tross for at forventningene til kommunenes arbeid med samfunnssikkerhet er økende, blant annet gjennom forskrift om kommunal beredskap. Rapporten finner få tegn til at samordningsproblemet er løst. Et nytt samvirkeprinsipp er innført, men vi kan ikke se at dette i seg selv er tilstrekkelig til at ressursene skal finne hverandre (Rapport fra NTNU: 2017).

Prinsipper for samfunnssikkerhet

Det norske samfunnssikkerhets- og beredskapsarbeidet bygget frem til 2012 på tre hovedprinsipper når det gjelder forebygging og håndtering. Det er bred enighet om prinsippene, og de står sterkt i det norske sikkerhets- og beredskapsfeltet. De ble innført i St.meld.nr. 24 (1992-1993), og har blitt bekreftet i flere senere stortingsmeldinger. Prinsippene har vist seg hensiktsmessige, men kommuniserer imidlertid i for liten grad nødvendigheten av godt samvirke mellom de ulike ansvarlige aktørene og behovet for å se samfunnets totale ressurser i sammenheng (Meld. St. 29 (2011-2012)). Som tidligere omtalt ble derfor samvirkeprinsippet innført på nasjonalt nivå i 2012. Innføringen av samvirkeprinsippet innebærer ikke noen endring i de grunnleggende ansvarsforholdene Meld. St. 29 (2011-2012)). I det videre omtales de fire prinsippene nærmere.

Ansvarsprinsippet betyr at den myndighet, virksomhet eller etat, som til daglig har ansvaret for et område, også har ansvaret for nødvendige beredskapsforberedelser og for den utøvende tjeneste ved kriser og katastrofer.

Likhetsprinsippet betyr at den organisasjon man opererer med under kriser skal være mest mulig lik den organisasjon man har til daglig.

Nærhetsprinsippet innebærer at kriser organisatorisk skal håndteres på et lavest mulig nivå. Den som har størst nærhet til krisen, vil vanligvis være den som har best forutsetninger for å forstå situasjonen og dermed er best egnet til å håndtere den.

Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.

Samvirkeprinsippet ble nærmere omtalt i kapittel 3.5 Samvirke.

5.1.2 Lysneutvalgets rapport

Sommeren 2014 nedsatte regjeringen et utvalgt for å kartlegge samfunnets digitale sårbarheter, Lysneutvalget. Utvalget skulle foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Bakgrunnen for arbeidet var at IKT har skapt store endringer i samfunnet de siste tiårene. Gevinstene har vært betydelige for innbyggere, næringsliv og samfunnet som helhet. Beskyttelse av det åpne og frie internett er avgjørende for verdiskapning og vekst. Avhengigheten av IKT i samfunnet, næringslivet og privat sammenheng er stor og økende. IKT utgjør nå grunnmuren for all samhandling på tvers av sektorer. Denne utviklingen har gjort IKT til en strategisk sikkerhetsutfordring. Infrastrukturen som ligger til grunn for at tjenestene fungerer, har blitt kritisk for at samfunnet skal fungere normalt. Den raske utviklingen av IKT-teknologi fører til rask endring og fornyelse av eksisterende digitale løsninger. Ved både tilsiktede (kriminalitet, terror, spionasje) og ikke-tilsiktede hendelser (ulykker, naturhendelser) er det behov for å beskytte informasjonen og sørge for at våre nettverk og systemer er sikre og stabile til enhver tid. Utvalget leverte sin rapport i november 2015, og det fremkommer der flere forslag til tiltak for å styrke beredskapen og redusere digitale sårbarheter i samfunnet (NOU 2015: 13 Digital sårbarhet - sikkert samfunn). Utvalgets hovedanbefalinger tas videre inn i St. meld 10 (2016-2017) Risiko i et trygt samfunn, og av hovedanbefalingene fremkommer blant annet å styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet, herunder å etablere et helhetlig rammeverk for digital hendelseshåndtering.

Justis- og beredskapsdepartementet la i 2017 frem en egen stortingsmelding om oppfølgingen av Lysneutvalgets anbefalinger (Meld. St. 10 (2016-2017)). Det fremkommer av stortingsmeldingen at Justis- og beredskapsdepartementet har et samordningsansvar for det forebyggende IKT-sikkerhetsarbeidet i sivil sektor.

Rammeverk for digital hendelseshåndtering

Anbefalingen fra Lysneutvalget ble fulgt opp ved at NSM ble gitt i oppdrag å utarbeide et rammeverk for digital hendelseshåndtering i den hensikt å avklare og tydeliggjøre innsatsen

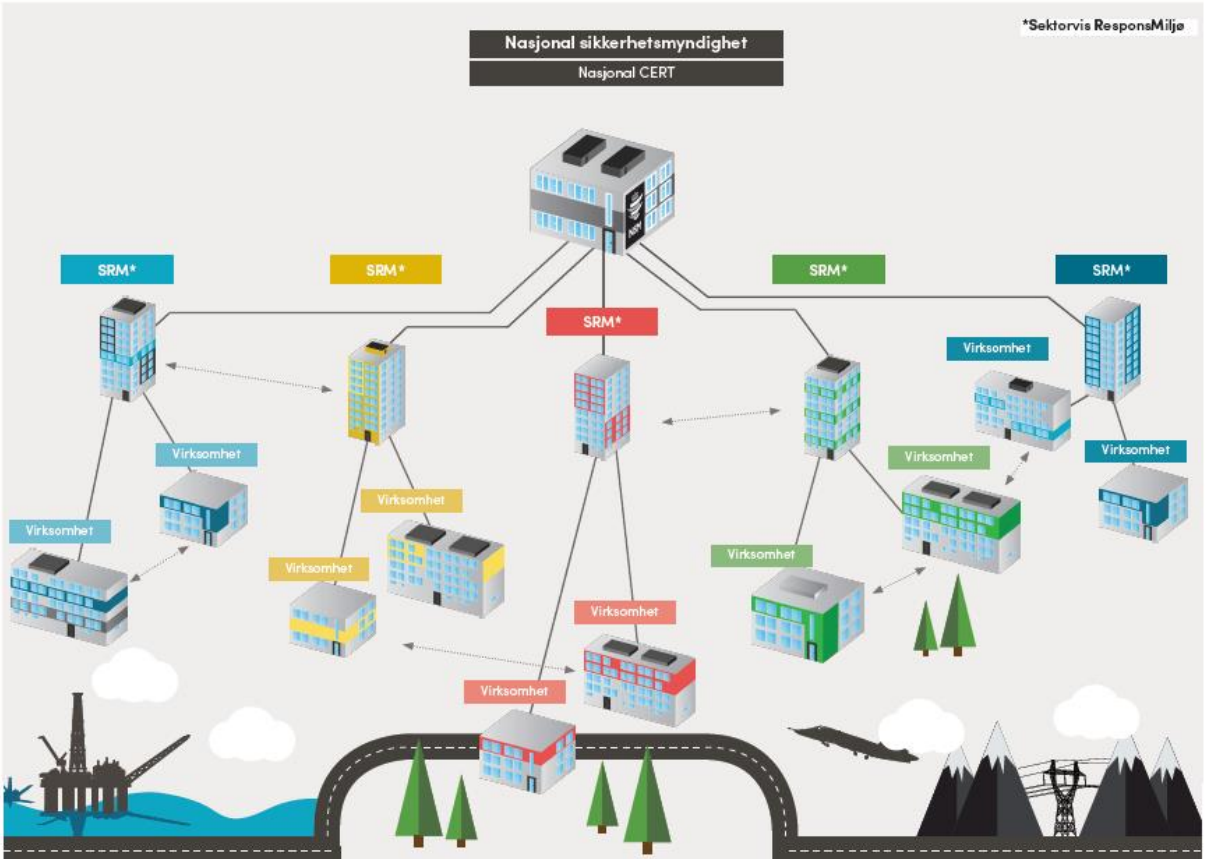
mellom relevante aktører innen hendelseshåndtering og straffeforfølgning. I desember 2017 ble rammeverk for håndtering av IKT-hendelser fastsatt av Justis- og beredskapsdepartementet i samråd med Forsvarsdepartementet. Det nye rammeverket erstatter modell for håndtering av IKT-hendelser, og er en systematisk tilnærming som inkluderer alt fra virksomheter til de sektorvise responsmiljøene (SRM) til Norwegian Computer Emergency Response Team, NorCERT og departementene.

Det framgår av rammeverket at det i Norge er en økende erkjennelse av at vi som et sterkt digitalisert og åpent demokratisk samfunn lever med risiko for at det kan inntreffe alvorlige IKT-sikkerhetshendelser. Risikoen knytter seg særlig til tre forhold:

1. Flere og mer komplekse systemer er bærere av funksjoner og tjenester (verdier) vi er avhengige av i samfunnet
2. Vi opplever stadig flere angrep, stadig mer raffinerte angrepsmetoder og stadig mer ressurssterke aktører
3. Det er en sterkere avhengighet mellom virksomheter som understøtter kritisk infrastruktur og kritiske samfunnsfunksjoner, og lengre og mer uoversiktlige verdikjeder

Det er ikke mulig å eliminere risikoen for at angrep vil inntreffe, og enkelte av disse vil være vellykkede sett fra angriperens side. En velfungerende koordinert innsats for å fange opp indikasjoner på angrep, minimere skade, redusere konsekvenser, gjenopprette sikker drift samt etterforske IKT-sikkerhetshendelser, vil være viktig fremover på alle nivåer i samfunnet for å redusere risikoen. Slik motstandskraft mot alvorlige IKT-sikkerhetshendelser etableres gjennom effektiv ressursbruk i et samspill mellom virksomhetene, sektorene og det nasjonale sektorovergripende nivået. Det er prinsippene *ansvar, likhet, nærhet, og samvirke*, som skal være styrende for hendelseshåndtering, også for IKT-hendelser. Den største forskjellen mellom en ordinær hendelse og en IKT-hendelse er at håndteringen i tillegg baseres på at det finnes sektorvise responsmiljøer. Disse er gitt en nøkkelrolle i å sikre at alle relevante aktører mottar informasjon til rett tid, slik at virksomhetene i sektoren kan iverksette nødvendige tiltak. SRM skal koordinere i egen sektor og være knutepunkt for informasjon og informasjonsflyt med fagdepartement og NSM, både til og fra sektoren (Rammeverk for digital hendelseshåndtering 2017). Figur 8 nedenfor er hentet fra «*Rammeverk for håndtering*

av IKT-hendelser 2017» og viser en oversikt over kommunikasjonen mellom NSM, RSM og virksomheter i og mellom sektorene:



Figur 8: Kommunikasjon mellom NSM, SRM og virksomheter i og mellom sektorer.

Rammeverket for digital hendelseshåndtering gjelder hele krisespekteret, fra fred, via sikkerhetspolitiske kriser, til krig. For de øvre deler av konfliktspennet sees rammeverket i sammenheng med Nasjonalt beredskapssystem (NBS). Rammeverket beskriver koordinering opp til ansvarlig departement, herunder det overordnede ansvaret og departementets rolle. Rollen til regjeringen, Kriserådet eller Regjeringens sikkerhetsutvalg (RSU) blir derimot ikke beskrevet i rammeverket. IKT-hendelser, som i rammeverket omtales som cyberhendelser, blir i rammeverket definert som tilsiktede handlinger i det digitale rom. Frem til det er avklart om en hendelse er tilsiktet, eller ikke, skal den håndteres som en tilsiktet handling.

Hensikten med rammeverket er å gi en samlet tilnærming til hendelseshåndtering for at virksomheter effektivt kan delta i en koordinert respons på IKT-angrep. Rammeverket forsøker å avklare og tydeliggjøre innsatsen mellom relevante virksomheter innen digital hendelseshåndtering for på den måten å sette Norge i bedre stand til å håndtere cyberangrep

som rammer i og på tvers av sektorer. Rammeverket er på denne måten et verktøy for å styrke den nasjonale evnen til å håndtere IKT-angrep.

Rammeverket er dynamisk og skal revideres ved behov, noe NSM er ansvarlig for å utføre. Dette skal eksempelvis gjøres ved endringer i nasjonale krav eller etter erfaringer fra øvelser og reelle IKT-angrep.

5.1.3 IKT trusselbildet

I NSMs årlige rapport om *Helhetlig IKT- risikobilde 2017* som har til hensikt å øke bevisstheten om IKT-sikkerhet, fremkommer det at Norske virksomheter står overfor en rekke trusler som kan medføre økonomiske tap, at informasjon kommer på avveie eller tjenester blir utilgjengelige, og i verste fall føre til alvorlige konsekvenser for liv og helse. Tilfeldige, uønskede hendelser har også betydning for risikobildet. Nasjonal kommunikasjonsmyndighet (Nkom) viser til at Norge i 2016 hadde tre tilfeller av ekstremvær som forårsaket skader på infrastruktur som ga utfall av kraft og elektronisk kommunikasjon (ekom). Uønskede hendelser kan også oppstå som følge av menneskelige feil, uten at det ligger ondsinnede intensjoner bak. Eksemplene på feilkonfigurering av IKT-utstyr, uforvarende aktivering av skadevare og andre handlinger som i god tro forårsaker uønskede hendelser, er mange.

I rapporten fremkommer det videre at NSM ser vedvarende trender fra foregående år, og enkelte nye, viktige utviklingstrekk. De erfarer et jevnt trykk av målrettede digitale spionasjeoperasjoner fra statlige aktører mot norske offentlige og private virksomheter. Spionasje mot høyteknologi, forsvarsinteresser, virksomheter knyttet til kritisk infrastruktur så vel som ettverksoperasjoner mot politiske, økonomiske og militære mål, vedvarer også i 2017. I tillegg til nettverksoperasjoner mot primærmål, registrerer de i økende grad målrettede operasjoner mot underleverandører og kontraktører. Dette er virksomheter som gjerne har svakere sikkerhetsmekanismer og derfor utnyttes bevisst som en inngang for å nå det egentlige målet. I 2017 er det registrert operasjoner som har til hensikt å få tilgang til IT-tjenesteleverandørers kunder og deres data. NSM har de siste årene også sett at trusselaktører kompromitterer tilfeldige systemer for å utnytte disse videre i nettverksoperasjoner mot andre mål. Dette betyr at god grunnsikring av nettverk og servere er viktig, selv om man ikke anser egen virksomhet å være et attraktivt mål i seg selv.

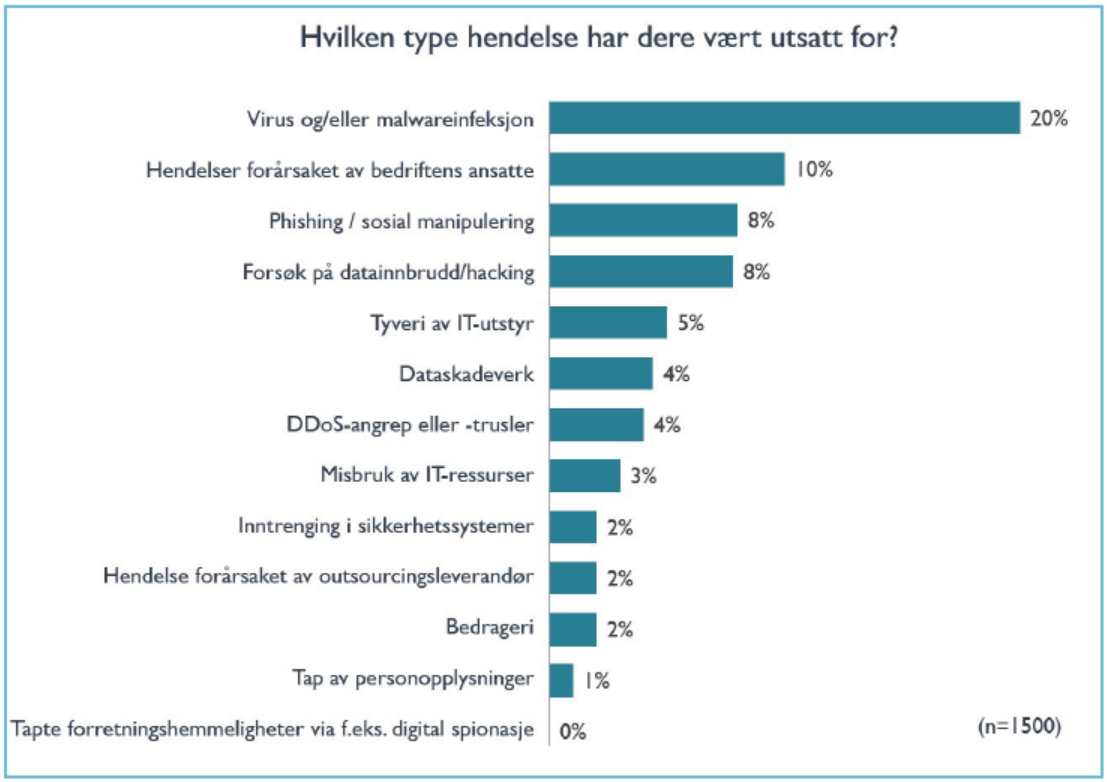
NSM NorCERT er den operative delen av NSM. De er Norges nasjonale CERT og cybersenter. NSM NorCERT håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur

og informasjon, og er den viktigste arenaen for IKT-samarbeid og et nasjonalt samlingspunkt. De er en koordinerende enhet for IKT-sikkerhetshendelser, dedikert til cybersikkerhet og hendelseshåndtering. NSM erfarer fortsatt at digitale angrep så godt som alltid innledes med bruk av ulike varianter av skadevare distribuert via e-post, og at denne typen angrep fremstår med økende grad av profesjonalitet (NSM risikorapport 2017).

Helse Sør–Øst er t Et eksempel på en uønsket hendelse og at trussel aktøren er en avansert og profesjonell aktør er Helse Sør-Øst saken og datainnbruddet via sykehuspartner HF i januar 2018. Det fremgår av internettsiden til Helse Sør-Øst og NSM at hendelsen er håndtert i henhold til etablerte beredskapsrutiner, i samarbeid med HelseCERT (Norsk Helsenett SF) og NorCERT og partene i felles cyberkoordineringssenter (FCKS), NSM, Etterretningstjenesten, PST og Kripos. Det har vært gjennomført en rekke tiltak for å fjerne trusselen, og ytterligere tiltak vil gjennomføres i tiden fremover (www.helse-sorost.no).

Mørketallsundersøkelsen 2016

Mørketallsundersøkelsen 2016 er den tiende undersøkelsen som foretas av Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget. Undersøkelsen er enestående i Norge og er et viktig bidrag til å kartlegge omfanget av datakriminalitet og IT-sikkerhetshendelser, samt bevissthet omkring informasjonssikring og omfanget av sikringstiltak i norske virksomheter. Alle svar er anonymisert slik at verken respondenter eller deres virksomheter har mulighet til å bli identifisert. Mørketallsundersøkelsen utarbeides annet hvert år og undersøkelse bygger videre på Mørketallsundersøkelsen fra 2014. Utdrag av hovedfunnene i Mørketallsundersøkelsen 2016 viser at over en fjerdedel av norske virksomheter, 412 av 1500 – 27 %, har opplevd uønskede sikkerhetshendelser det siste året. Virksomhetene forteller at dette fører til produktivitetstap i 4 av 10 tilfeller (i form av tapte arbeidstimer), men kun 2 av 10 oppgir at de har hatt kostnader som følge av slike hendelser. Dette viser at virksomhetene mangler oversikt over hva sikkerhetshendelsene koster dem, eller undervurderer disse kostnadene. Kun 9 prosent av virksomhetene som utsettes for angrep tar saken videre til politiet. Det tilsier at det skjuler seg betydelige mørketall, og for de kriminelle nettverk er denne typen angrep mot norske virksomheter i praksis straffrie.



Figur 9: En oversikt over hvilke type sikkerhetshendelser virksomhetene ble rammet av i 2016. Mørketallundersøkelsen (NSR 2016).

Undersøkelsen viser at norske virksomheter fortsatt lider økonomiske tap fra sikkerhetshendelser som kunne vært unngått ved hjelp av grunnleggende tiltak. NSM viser til fire anbefalte tiltak mot dataangrep som kan stoppe en stor del av angrepene mindre virksomheter utsettes for dersom de implementeres: *1. Oppgrader program- og maskinvare, 2. Vær rask med å installere sikkerhetsoppdateringer, 3. Ikke tildel sluttbrukere administratorrettigheter og 4. Blokker kjøring av ikke-autoriserte programmer*. Mørketallsundersøkelsen 2018 ble publisert få uker før denne oppgaven ble ferdig og viser blant annet at virksomhetene har liten oversikt over kostnadene knyttet til sikkerhetshendelser, kostnader som er estimert til et titalls milliarder kroner årlig. Virus- og malwareinfeksjon er den sikkerhetshendelsen som rammer flest. 21 prosent av virksomhetene oppgir å ha blitt utsatt for dette i løpet av 2017. Sammenlignet med Mørketallsundersøkelsen 2016, er det en klar økning i antall virksomheter som utsettes for phishing (digital snoking), forsøk på hacking og faktisk hacking, distributed denial-of-service, DDoS angrep eller trusler om det, og bedrageri.

5.1.4 Evalueringsrapport Øvelse IKT16

Som tidligere nevnt er det utarbeidet en evalueringsrapport etter Øvelse IKT16 som er unntatt offentlighet jf. offentleglova. Evalueringsgruppen som gjennomførte arbeidet ble tverrfaglig satt sammen for å sikre en så helhetlig tilnærming som mulig til evalueringsarbeidet. Arbeidet ble ledet av DSB. Evalueringsgruppen hadde deltakere fra NSM, NKOM, politiet, Forsvaret, Norges vassdrags- og energidirektorat, Helsedirektoratet og FinansCERT.

Vi har fått innsyn i den delen av evalueringsrapporten som omhandler myndighetens kommunikasjonshåndtering til publikum. Rapporten henviser til stortingsmelding 10, (Meld. St. 10 (2016-2017, s. 58)) hvor det er beskrevet at krisekommunikasjon skal være en integrert del av alle øvelser på alle nivå i forvaltningen. Det understrekes at «Øvelser er avgjørende for å bli god på krisekommunikasjon». Det var ikke alle virksomhetene som valgte å øve krisekommunikasjon under øvelsen. Dette utfordret planleggingen og gjennomføringen av mediespillet. Spesielt var det utfordrende for de myndigheter som øvet krisekommunikasjon at de ikke kunne samvirke med de myndigheter de ville ha samhandlet med i en reell situasjon. Flere øvende virksomheter har gitt tilbakemelding på at det ikke kom godt nok frem i planleggingen at mediespillet skulle ha så stor rolle i øvelsen, og hadde derfor ikke forberedt seg på dette.

Det fremkommer videre av evalueringsrapporten at de statelige virksomhetene informerte om på hvilken måte egen sektor var rammet av angrepet og om, men i mindre grad, hvordan sektoren jobbet med å få publikumstjenestene til å fungere. Dette bidro til at informasjon fra myndighetene fremsto som for dårlig koordinert, som fragmentert og mindre samordnet enn hva som kan forventes og som bør bestrebes. Mange virksomheter henviste befolkningen til Kriseinfo.no, et nettsted som administreres av DSB. Kriseinfo.no publiserer lenker til allerede publiserte pressemeldinger fra myndighetene slik at all relevant informasjon samles på et sted. Formålet er å gjøre det enklere for befolkningen å finne relevant informasjon (https://www.dsb.no/). Av evalueringen fremkom at informasjonen som ble lagt ut på Kriseinfo.no var mindre relevant, og at informasjonen som ble lagt ut der i liten grad bidro til å danne et samlet bilde av situasjonen.

Det fremkommer videre av evalueringsrapporten at tilbakemeldingene fra de øvende virksomhetene peker på at myndighetene under øvelsen ikke i tilstrekkelig grad ivaretok befolkningens behov for relevant og brukerorientert informasjon om hvilken situasjon Norge

sto i og hvilke konsekvenser IKT-angrepene fikk for befolkningen og tjenester de er avhengige av. Det var også mangel på informasjon om hvordan befolkningen skulle forholde seg til situasjonen, eller betryggelse om at hendelsen ble forsvarlig håndtert. Dette understreker også betydningen av å øve krisekommunikasjon, og å sette av tilstrekkelige ressurser til det. Avslutningsvis i kapitelet om myndighetenes håndtering av krisekommunikasjon mot befolkningen, oppsummeres det med at ved ekstraordinære hendelser og kriser vil befolkningens informasjonsbehov være nærmest utømmelig. Dersom myndighetene bruker for lang tid på å gå ut med et budskap, kan både ekte og falske nyheter ha satt sitt preg på situasjonen (Evalueringsrapport Øvelse IKT16 2017).

5.2 Kvalitativ intervjuanalyse

5.2.1 Funn fra intervjuene med DSB og NSM

I dette kapittelet vil funn fra intervjuene med informantene fra DSB og NSM bli presentert. Vi har valgt å omtale virksomhetene og funnene fra informantene samlet, fordi disse i all hovedsak var samsvarende. I det videre presenterer vi funnene på spørsmålene som ble stilt om planverk, deretter funn om samvirke og samhandling under selve planleggingsfasen. Under intervjuene ble vi gjort oppmerksomme på at deler av virksomhetenes planverk er gradert etter sikkerhetsloven eller unntatt offentlighet jf. offentleglova og at vi derfor ikke fikk utfyllende svar på noen av spørsmålene vi stilte.

Planverk

På spørsmål om DSB og NSM er omtalt i den andre virksomhetens planverk, svarte informantene noe forskjellig. Alle kunne likevel bekrefte at den andre virksomheten på en eller annen måte var omtalt i eget planverk. Informantene fra begge virksomhetene gav informasjon om at de var omtalt i vaktinstrukser og på varslingslister. En av informantene fra DSB opplyste videre at:

«NSM er omtalt i planverket ved at virksomheten står omtalt på DSBs varslingslister ved hendelses- krisehåndtering. De står også på distribusjonslister for deling av relevant informasjon, også utenom håndteringsfaser».

Samvirke og samhandling

I oppdragsbrev fra JD til DSB 10. november 2015, fremkommer det at DSB skal lede planleggingen og at den skal utføres i tett samarbeid med andre sentrale aktører som NSM, Nkom, Forsvaret, Difi, mfl. Allerede her ser vi at JD har vektlagt samvirkeprinsippet i sitt

oppdrag til DSB, og DSB er ansvarliggjort i forhold til å involvere relevante aktører. Vår oppgave ble i det videre å finne ut om DSB tok dette ansvaret, og hvordan og hvor omfattende dette i praksis ble gjennomført, og da særskilt i forhold til NSM.

På spørsmål om på hvilket tidspunkt ble virksomhetene involvert i hverandres planleggingsarbeid? «*Informantene fra DSB kunne opplyste at NSM ganske raskt ble identifisert til å være en av de viktigste aktørene inn i øvelsesplanleggingen basert på at NSM er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet*».

Informantene hadde en enstemmig oppfatning av at DSB hadde tatt et tidlig initiativ overfor NSM, men også overfor de øvrige navngitte aktørene til et første felles informasjons- og planleggingsmøte. Som nevnt i kapittel 2.3 *Øvelse IKT16*, samlet øvelsen deltagere fra 50 offentlige og private virksomheter og de sektorvise responsmiljøer innen IKT. Figur 2 side 14 viser en oversikt over deltakere i Øvelse IKT16 (Øvingsdirektiv for Øvelse IKT16).

Foruten de som var nevnt i oppdragsbrevet fra JD, hvordan ble de øvrige kartlagt og involvert? I følge flere av informantene ble dette temaet diskutert på de innledende møtene mellom DSB, NSM og de øvrige etatene som tidlig var identifisert som deltagere. En av informantene opplevde at både DSB og NSM hadde et bevisst forhold til at begge etatene hadde et særskilt ansvar for å involvere andre aktuelle aktører. En annen av informantene sier at det var stor bevissthet fra spesielt NSM sin side om å involvere de sektorvise responsmiljøene innen IKT. Dette ble fulgt opp fra DSB ved at de i løpet av planleggingsfasen, som varte i ett år fra de mottok oppdragsbrevet datert 10.11.15 og til øvelsen ble gjennomført i november 2016, gjennomførte tre større planleggingskonferanser. I tillegg ble det gjennomført to dreiebok-konferanser hvor dreieboken for Øvelse IKT16 ble utviklet.

Informantene fra både DSB og NSM opplyser at foruten de formaliserte skrivebords-konferansene og dreiebok møtene hvor alle aktørene var til stede, var det god og tilstrekkelig bilateral kontakt mellom de to virksomhetene gjennom hele planleggingsperioden. Dette kunne være i form av møter, telefonsamtaler eller epost utveksling. Flere av informantene fortalte at de opplevde at det var god bevissthet rundt, og gjensidig respekt for hverandres faglige kompetanse.

På overordnet nivå kan det på bakgrunn av disse funnene anslåes at DSB fulgte opp samvirkeprinsippet overfor NSM med det ansvaret de hadde som hovedansvarlige for øvelsesplanleggingen. NSM på sin side responderte med å stille sin fagkompetanse til rådighet.

Under planlegging av øvelsen ble verktøyet Project Place, en variant av SharePoint, benyttet som kommunikasjonsplattform. På spørsmål om bruken av verktøyet understøttet samvirkeprinsippet mellom DSB og NSM svarte en av informantene:

«Gitt den gode bilaterale kontakten DSB og NSM hadde gjennom hele planleggingsperioden var bruken av SharePoint kun et supplement med tanke på samvirkeprinsippet mellom de to virksomhetene».

På spørsmål om DSB og NSM samarbeidet om dokumentproduksjon bekreftet alle informantene at dette ble gjort. NSM hadde i tillegg et oppdrag om å utarbeide et rammeverk med beskrivelse av roller og ansvar i forbindelse med IKT-hendelser, jf. anbefaling i Lysneutvalgets rapport.

Under intervjuene fremkom det at det var noe forskjellig kultur virksomhetene imellom på hvordan gradert informasjon skulle håndteres med hensyn til "need to know/nice to know prinsippet". En av informantene opplyste at det hadde vært noe diskusjon og refleksjon rundt dette uten at det skapte nevneverdige problemer.

Avslutningsvis ble alle informantene uavhengig av intervjuguiden spurt om de mente at samvirkeprinsippet mellom DSB og NSM ble etterlevd etter intensjonen. Samtlige av informantene svarte at de mente at intensjonen med samvirkeprinsippet ble oppfylt og etterlevd under planleggingsfasen.

5.3 Forskningsspørsmål

I denne delen av oppgaven vil vi presentere empiri som er knyttet til de tre forskningsspørsmålene. Med unntak av den informasjonen vi fikk i forbindelse med intervjuene, ble vi av både DSB og NSM henvist til offentlige dokumenter for å få ytterlige informasjon for å svare ut forskningsspørsmålene. Vi ble henvist til stortingsmeldinger og veiledere utgitt av de to etatene, og til høringsuttalelser- og svar som de har avgitt. I tillegg

fikk vi tilsendt informasjon i form av et møtereferat fra DSB om evaluering av samvirkekonferansekonseptet og vi ble på anmodning innvilget delvis innsyn i deres interne krisehåndteringsplan.

5.3.1 Hva legger DSB og NSM i begrepet samvirkeprinsippet?

DSB viser til egen veileder utgitt i 2015 om Departementenes systematiske samfunnssikkerhets og beredskapsarbeid for deres forståelse av samvirkeprinsippet. Her fremkommer det at departementenes planverk, herunder rutiner og prosedyrer, skal reflektere prinsippet om samvirke. Dette innebærer at det i planverket skal fremkomme hva departementet har gjort for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. Videre fremkommer det at det vil kunne oppstå kriser som den enkelte virksomhet eller departement ikke vil kunne håndtere alene, der ulike samfunnsområder og interesser må ses i sammenheng. Alle aktører har et selvstendig ansvar for å sikre et optimalt samvirke og samarbeid med andre relevante aktører, slik at best mulig utnyttelse av ressurser kan sikres på tvers av sektorer og ansvarsnivåer (DSB; veileder 2015). DSB viser også til omtalen av begrepet samvirkeprinsippet i samfunnssikkerhetsmeldingen "Risiko i et trygt samfunn" (Meld St. 10 (2016-2017)), og at de legger beskrivelsen der til grunn for sin forståelse av samvirkeprinsippet. Av veilederen fremkommer også at helhetlig arbeid med samfunnssikkerhet og beredskap er et begrep som samler og integrerer de forskjellige faglige tiltak innen beredskapsarbeidet. Det er viktig at prosessene omkring beredskapsplanleggingen utgjør en samordnet helhet og ikke fremstår som et knippe ukoordinerte tiltak. Beredskapsarbeidet må derfor settes i system og kvalitetssikres» (DSB; veileder 2015).

Av relevans for forskningsspørsmålet har vi mottatt referat fra DSB om evaluering av forumet Samvirkekonferansekonseptet, opprettet i 2015 (Referat av 4.12.2017). DSB viser til forumet som et tiltak for å operasjonalisere samvirkeprinsippet. Bakgrunnen for etableringen av forumet var behovet for informasjonsdeling i hektiske faser i håndteringen av hendelser. Konferansene, som gjennomføres på VTC (videokonferanse), har vært mest benyttet under ekstremvær, men også ved terrorhendelser i utland, og i opptakten til høytidsdagene i mai måned, med forhøyet terrortrussel. De mest involverte aktørene deltar, avhengig av hendelsen. Etter evalueringen av konseptet i 2017 ble det konkludert med at deltakerne i all hovedsak hadde gode erfaringer med å delta. Det fremkom videre at flere mente at konferansene samlet sett a et bedre grunnlag for egen krisehåndtering, også sett i lys av at de gjennom forumet får

kunnskap om andres arbeid, ansvarsområder og oppgaver (DSB; referat av 4.12.2017). DSB viser også til deres ansvar for rapportering på samordningskanal som et verktøy for å sikre samvirke, og den tilsvarende rollen de har for Fylkesmennene gjennom Fylkesberedskapsråd.

NSM legger til grunn Instruks for departementenes arbeid med samfunnssikkerhet (2017) for sin forståelse av samvirkeprinsippet. Formålet med instruksen er å presisere kravene til departementenes arbeid med samfunnssikkerhet for å styrke samfunnets evne til å forebygge kriser og til å håndtere alvorlige hendelser gjennom et helhetlig og koordinert arbeid med samfunnssikkerhet. Det fremgår av instruksen at arbeidet med samfunnssikkerhet skal være basert på et system for risikostyring, preget av sammenheng og kontinuitet. Systemet omfatter prosessen fra å formulere mål for og definere ansvarsområdene innenfor samfunnssikkerhetsarbeidet, til å identifisere farer, analysere risiko, vurdere om risikonivået er forsvarlig eller ikke og iverksettelse av eventuelle risikoreduserende tiltak. Kravene i instruksen følger trinnene i en slik risikostyringsprosess. På bakgrunn av risikoanalysen og en vurdering av tiltak, skal departementene vurdere, beslutte og gjennomføre tiltak slik at sårbarheter og svakheter blir redusert innenfor hele ansvarsområdet. Dette for å oppnå størst mulig robusthet innen samfunnskritiske funksjoner, og slik at organisasjon og ledelse i departementet og underliggende etater og virksomheter er forberedt på og kan håndtere ulike typer kriser. Alle departementer har et selvstendig ansvar for å ta den nødvendige kontakt med andre departementer for å sikre at arbeidet blir godt koordinert i henhold til samvirkeprinsippet. Prinsippet slik det fremkommer av instruksen betyr å utvikle gode former for samarbeid med de aktørene det er nødvendig å samarbeide med, avklare og ta hensyn til avhengigheter, og se ressursene som helhet. Felles beredskapsforberedelser i form av planer, trening, øvelser, evaluering og læring står helt sentralt. Alle aktører har et selvstendig ansvar for å sikre et optimalt samvirke, koordinering og samarbeid med relevante aktører.

5.3.2 Hvordan organiseres beredskapsplanlegging internt og eksternt i DSB og NSM?

Kapitlet omhandler hvilke tiltak DSB og NSM har iverksatt for å sikre bedre samvirke opp mot eksterne aktører før og under kriser. Intern beredskapsplanlegging i NSM har vi liten forutsetning for å gå inn i da vi ikke har fått innsyn i deres interne planverk. Vi har fått delvis innsyn i DSBs interne kriseberedskapsplan og vil omtale funn i den.

JD fikk i medhold av kgl.res 14.3. 2017 fullmakt til å etablere nasjonale krav til IKT-sikkerhet i sivil sektor. Dette innebærer blant annet at JD utformer regjeringens politikk for IKT-

sikkerhetsområdet, herunder etablerer nasjonale krav for både offentlige og private virksomheter. NSM er på nasjonalt nivå ansvarlig for å koordinere håndteringen av alvorlige IKT angrep på samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner og for å organisere og drifte et nasjonalt varslingssystem for digital infrastruktur. For å sikre at alle relevante aktører mottar korrekt varslingsinformasjon og settes i stand til å gjøre nødvendige tiltak, skal sektordepartementene vurdere behov for å etablere sektorvise responsmiljøer (SRM) innen eget ansvarsområde. I 2013 fikk NSM NorCERT tilført en vesentlig styrking som blant annet førte til at de nå har et operasjonssenter som er bemannet 24/7. Samtidig har den enkelte virksomhet et selvstendig ansvar for å etablere og opprettholde tilstrekkelig sikkerhet for egne systemer, herunder å kunne håndtere IKT-hendelser. Det fremkommer av Nasjonal strategi for informasjonssikkerhet (2012) at målsetting er at det skal finnes responsmiljøer i alle samfunnssektorer. Hensikten med etableringen av sektorvise responsmiljøer er å styrke forebyggings- og håndteringssamarbeidet og responsmiljøet skal bistå sin sektor med kompetanse, samt være knutepunkt for informasjon og informasjonsflyt, både til og fra sektorene. NSM NorCERT skal koordinere håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur på nasjonalt nivå, og bidra med beslutningsstøtte til myndighetene. Koordineringen innebærer blant annet å dele relevant og frigitt informasjon med de sektorvise responsmiljøene, politiet, samfunnskritiske virksomheter og andre aktuelle aktører.

NSM har utarbeidet retningslinjer for etablering av sektorvise responsmiljøer som angir krav til et minimumsnivå av kapasitet og kompetanse. Retningslinjene tar utgangspunkt i en nivådeling som innebærer samarbeid mellom et virksomhetsnivå, et sektornivå og et nasjonalt nivå. Innretningen på, og omfanget av, responsmiljøene må vurderes på grunnlag av egne risikovurderinger i den enkelte sektor. Den enkelte virksomhet og sektor må vurdere hvorvidt det er hensiktsmessig å besitte håndteringsevne og kompetanse i eget miljø, om det bør innhentes eksternt fra kommersielle aktører, eller om virksomheten bør gå sammen med etablerte sektormiljøer for å sikre høy kost/nytte-effekt.

Flere sektorvise responsmiljøer er etablert og tre av de som er sentrale for norsk infrastruktur er Tele/Ekom-CERT, FinansCERT og KraftCERT. Nkom er i ferd med å etablere Tele/Ekom-CERT i egen organisasjon, mens FinansCERT og KraftCERT har blitt opprettet som et spleiselag mellom ulike aktører. Andre eksempler er responsmiljøet for forsvarssektoren

(Cyberforsvaret/BKI), helsesektoren (HelseCSIRT), universitets- og høyskolesektoren (UNINETT-CERT) og justissektoren (Justis-CSIRT). Responsmiljøene har et stort potensiale, men trenger tid og ressurser til å videreutvikles. I tillegg til de sektorvise responsmiljøene finnes det virksomheter som har egne sterke responsmiljøer, som f.eks. Telenor.

Rammeverket for håndtering av IKT-hendelser beskriver hvordan samvirket mellom virksomheter, sektorer og nasjonalt nivå skal foregå. For sentral koordinering ved cyberhendelser mellom de nasjonale organene NSM, Etterretningstjenesten, PST og KRIPOS er det etablert et felles cyberkoordineringssenter (FCKS). Hensikten med rammeverk for håndtering av IKT-sikkerhetshendelser er å avklare og tydeliggjøre innsatsen mellom relevante aktører for å sette samfunnet bedre i stand til å håndtere alvorlige IKT-sikkerhetshendelser som rammer på tvers av sektorer. På denne måten skal rammeverket bidra til mer effektiv håndtering av alvorlige IKT-sikkerhetshendelser, fra virksomhetsnivå til politisk nivå, gjennom god utnyttelse av samfunnets samlede ressurser. Det skal videre bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser. Målgruppen for rammeverket er offentlige og private virksomheter som har betydning for kritisk infrastruktur og/eller kritiske samfunnsfunksjoner, sektorvise responsmiljøer, myndigheter som har en rolle knyttet til håndtering av IKT-sikkerhetshendelser og departementene. Rammeverket beskriver en systematisk tilnærming til håndtering av IKT-sikkerhetshendelser på tvers av virksomheter og sektorer for å sikre en effektiv nasjonal sektorovergripende håndteringsevne, hvor det enkelte departements konstitusjonelle ansvar også ivaretas. De etablerte beredskapsprinsippene legges til grunn. Rammeverket kommer ikke i konflikt med tiltak i Nasjonalt beredskapssystem (NBS) som vil kunne bli iverksatt ved store alvorlige hendelser.

I samsvar med Nasjonal strategi for informasjonssikkerhet (2012) og Handlingsplan – Nasjonal strategi for informasjonssikkerhet (2017), legger rammeverk for håndtering av IKT-sikkerhetshendelser til grunn at de sektorvise responsmiljøene (SRM) skal ha en sentral rolle i hendelseshåndteringen. Rammeverket stiller krav til hvilke oppgaver responsmiljøene må ivareta og hvilke egenskaper responsmiljøene må ha. Det legges vekt på at departementene har et overordnet ansvar for organiseringen av sektorvise responsmiljøer slik at disse får den sentrale rollen i nasjonal hendelseshåndtering som rammeverket legger opp til. Rammeverket beskriver også hvilke evner virksomhetene selv forutsettes å ha relatert til håndtering av IKT-

sikkerhetshendelser. Kravene som stilles er i det vesentlige i overensstemmelse med tidligere modell for håndtering av IKT-sikkerhetshendelser fra 2014, men detaljeringsgraden er høyere i rammeverket. I tillegg beskriver rammeverket sentrale aktører og fordeling av ansvar mellom aktører med en rolle i hendelseshåndteringen. NSMs grunnprinsipper for IKT-sikkerhet definerer et sett med prinsipper for hvordan IKT-systemer bør sikres for å beskytte verdier og leveranser. Grunnprinsippene er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet.

DSB gjennomførte i 2015 en omdømmeundersøkelse der resultatene fra undersøkelsen viser at sju av ti har et godt helhetsinntrykk av DSB, og at DSB scorer høyt på faglig kvalitet og dyktige medarbeidere, men undersøkelsen peker også på forbedringsområder for ulike tjenesteområder og virkemidler. DSB scorer for eksempel lavest på innovasjon og intern samhandling, og respondenter fra brann- og redningsvesenet og 110-sentraler er mest kritiske i sine tilbakemeldinger til Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017).

I krisehåndteringsplanen til DSB (2017) fremkommer det innledningsvis at DSB skal ha en beredskap for å kunne håndtere og begrense konsekvensene av uønskede hendelser og kriser. DSB må kunne utføre sine oppgaver relatert til sin samordningsrolle, samt som støtte til Justis- og beredskapsdepartementet og andre departementer i henhold til kgl. res. 24.6.2005. Planen beskriver systemer og rutiner for respons for uønskede hendelser, uavhengig av årsak til hendelsen og hvor den finner sted. Det fremkommer videre at linjeledere har det samme ansvaret, den samme myndigheten og de samme kravene til leveranser som de har i en normalsituasjon. Den beskriver organisasjonens viktigste oppgaver ved kriser som rammer DSB, og DSBs ansvar ved kriser som rammer samfunnet. Det fremkommer videre av planen hvilke funksjoner som er faste kontaktpunkter, hvilke funksjoner som skal varsles, og hvilke teknologiske systemer som skal benyttes ved varsling. Den beskriver også forventninger til fagavdelingene i organisasjon, og hvilke forberedelser de skal gjøre. Som vedlegg til kriseplanen ligger agendaen for de faste møtene som vil bli gjennomført i organisasjonen ved kriser. I tillegg ligger retningslinjer for hvilke eksterne beredskapsaktører DSB skal varsle og rapportere til, på samordningskanal. DSB har ansvar for opprettelse av, drift og administrasjon av beredskapsressurser som de skal forberede for at *andre* skal kunne håndtere konsekvensene av uønskede hendelser. Vedlegg til kriseplanen beskriver disse

beredskapsordningene, som blant annet skogbrannhelikopter, Sivilforsvarsdistriktene og Redningsinnsats til sjøs (Rits).
Av tiltak som er mer eksternt rettet kan nevnes DSBs ansvar for å bemanne og drifte Kriseinfo.no, en nettportal som gir samlet informasjon fra norske myndigheter før, under og etter kriser. På Kriseinfo.no finner en den offisielle informasjonen fra myndighetene samlet på et sted, og portalen skal gi befolkningen det de søker etter i slike situasjoner (DSB.no)
DSB har også ansvaret for at viktige samfunnsfunksjoner har tilgang til et trygt, robust og tidsmessig kommunikasjonssystem for ledelse og samhandling i daglig virke og ved større hendelser. Av tiltak som også er internasjonalt rettet skal DSB fungere som nasjonalt kontaktpunkt for krisehåndteringsmekanismer i NATO, FN og EU (ibid).
Direktoratet eier Nødnett og har ansvar for forvaltning og videreutvikling av det i tråd med brukernes behov. I 2017 ble det norske Nødnett koblet sammen med det svenske nødnettet Rakel i det norsk-svenske prosjektet Grenseoverskridende kommunikasjon.
Sammenkoblingen av de to nødnettene skal gjøre samvirke og kommunikasjon enklere mellom de to landene, samt bidra til effektivisering av områdene langs grensen (https://www.dsb.no/).

5.3.3 Hvilke faktorer hemmer samhandling mellom DSB og NSM?

God samhandling mellom sektormyndigheter og nasjonale myndigheter er essensielt for å oppnå et forsvarlig sikkerhetsnivå. Mange vil huske 22. juli-kommisjonens utsagn om at 22. juli angrepene er historien om ressursene som ikke fant hverandre da det gjaldt som mest. Utvalgets arbeid har avdekket at mangelfull samhandling har vært og er et problem også i forbindelse med anvendelsen av den nåværende sikkerhetsloven. Utvalgets viktigste tilbakemelding til samfunnet er derfor en sterk oppfordring til styrket *samhandling for sikkerhet* (NOU 2016: 19).

I 2015 la Riksrevisjonen fram *Riksrevisjonens undersøkelse av Justis- og beredskapsdepartementets arbeid med samfunnssikkerhet og beredskap*, Dokument 3:7 (2014-2015*)*. Funnene i denne rapporten var så vidt grove at flertallet i kontroll- og konstitusjonskomitéen oppfordret Riksrevisjonen til å gjennomføre en tilsvarende undersøkelse etter to år for å se om iverksatte tiltak etter den første rapporten hadde ført til tilsiktede forbedringer. Anbefalingen ble fulgt, og rapporten om Riksrevisjonenes oppfølgingsundersøkelse av Justis- og beredskapsdepartementet, Dokument 3: 8 (2016-2017)

ble avgitt 2.5.2017 Dokument 3:8 (2016-2017). Funn fra Dokument 3:7 (2014-2015) omtales ikke ytterligere i oppgaven.

I Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017) fremkommer det at erfaringer fra tidligere øvelser viser at informasjonsdeling, ansvar og rolleforståelse har vært en utfordring, blant annet mellom NSM og politiet. Det vises i rapporten til utfordringer fra tidligere hendelser og øvelser, som blant annet cyberangrep i Ukraina i 2014, Telenors Cyberdawn 2013 og Nasjonal cyberøvelse for ekom og kraft 2015. I forberedelsene til Øvelse IKT16 var derfor rolle- og ansvarsavklaringer et sentralt tema.

Umiddelbart etter Øvelse IK16 innhentet DSB, som evalueringsansvarlig for øvelsen, inntrykk og kommentarer fra deltakerne (Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet 2016-2017). Deltakerne pekte på at følgende forhold var utfordrende:

- å etablere en felles situasjonsforståelse
- å sikre god informasjonsflyt mellom responsmiljøer og myndigheter
- å dele og formidle gradert informasjon
- å sikre god kommunikasjon til befolkningen

De største utfordringene knyttet til oppfølging av øvelser og hendelser gjelder tiltak på tvers av sektorer. I dag planlegger, gjennomfører og følger DSB opp sivile tverrsektorielle øvelser på nasjonalt nivå hvor formålet er å forbedre krisehåndteringsevnen nasjonalt og avdekke utfordringer som krever samordning på tvers av sektorer. Det er i tillegg etablert et nasjonalt øvelses- og evalueringsforum (NØEF) som skal bidra til å løfte fram sektorovergripende forbedringspunkter ved evalueringer etter øvelser og hendelser. Riksrevisjonen mener det er positivt at det er etablert en arena hvor aktørene på tvers av sektorer kan bli enige om hvem som er ansvarlige for å rette opp forbedringspunktene. Etter Riksrevisjonens vurdering gjenstår det fortsatt utfordringer med hensyn til oppfølging av øvelser og hendelser på tvers av sektorer, blant annet knyttet til fordeling av oppgaver og ansvar, og konkretisering av læringspunkter (ibid).

I DSBs høringssvar til grunnlaget for ny sikkerhetslov (NOU 2016:19) fremkommer følgende: *«Gråsonene mellom sikkerhetsarbeid etter sikkerhetsloven og øvrig sikkerhets- og*

beredskapsarbeid blir mye større enn i dag. Dette vil medføre uklarhet i rolle- og ansvarsdelingen. Rapporten berører ikke disse problemstillingene. NSM mangler kompetanse på å gjøre vurderinger, føre tilsyn og gi råd om sikkerheten i kritiske samfunnsfunksjoner i tråd med lovforslaget. Dette er oppgaver DSB allerede har i dag. Forslaget vil medføre duplisering av kompetanse og byråkratisering, uten at disse problemstillingene drøftes nærmere. DSB bør ha rollen som Sikkerhetsmyndighet etter loven. Myndighetsutøvelse fra hemmelige tjenester (som NSM) må være langt tydeligere avgrenset enn det forslaget legger opp til. Rapporten inneholder ingen drøfting av kompetansekrav til Sikkerhetsmyndigheten og alternativer til å legge ansvaret til NSM. Et utvidet gradert regime vil hemme samarbeid og kommunikasjon internt i virksomhetene, mellom tilsynsetatene og vis-à-vis lokalsamfunnet. Slike virkninger av lovforslaget er ikke vurdert» (Brev 19.1.2017).

Ny sikkerhetslov har ikke trådt i kraft, og forskriftene til loven er i skrivende stund på alminnelig høring med svarfrist 1.10.2018. I forskriftene er NSM tillagt rollen som Sikkerhetsmyndighet (Regjeringen.no/høringer-forskrifter sikkerhetslov).

I det følgende gjengis de sentrale hovedpunktene i NSMs høringsuttalelse til grunnlaget for ny sikkerhetslov (NOU 2016: 19):

«NSM støtter hovedinnretningen på det lovforslaget som er utarbeidet av Sikkerhetsutvalget. Lovforslaget må imidlertid følges opp med en betydelig satsning på forebyggende sikkerhet i alle ledd. Uten en slik satsning vil kompleksiteten i forslaget kunne medføre en svekket sikkerhet sett opp mot dagens tilstand».

Regjeringen nedsatte IKT-sikkerhetsutvalget i 2017. Oppdraget til utvalget var å se på regelverk og organisering innenfor IKT-sikkerhet, med målsetting om økt IKT-sikkerhet. Som en del av utvalgets arbeidsmetodikk har det blitt sendt ut et spørreskjema til en rekke virksomheter, blant annet til både DSB og NSM. Spørsmål 8 refereres i det følgende: «*Hvordan opplever din virksomhet samarbeid og koordinering innenfor IKT-sikkerhet mellom myndighetsorganer med ansvar for IKT-sikkerhet?»* DSBs svar er ganske omfattende, og inneholder blant annet følgende påstand: «*NSM sitter ikke på oversikten over de mulige konsekvensene av en IKT-sikkerhetshendelse, det er det de enkelte fagmyndigheter og DSB som gjør»*. Spørsmål nr. 13 retter seg mot om den enkelte virksomhet får dekket behovet for

råd og veiledning innenfor IKT-sikkerhet. Til dette svarer DSB at de ikke gjør det i tilstrekkelig grad. «*Både NSM og Nkom synes å ha begrensede ressurser til å bistå med rådgiving» (Svar fra DSB på spørreskjema: Brev 20.2.2018).* NSMs svar på IKT-sikkerhetsutvalget spørreskjema er unntatt offentlighet, og vi er etter begjæring nektet innsyn.

6 Drøfting

I det følgende kapittelet blir utvalgte funn fra dokumentgjennomgang og intervjuer drøftet i lys av oppgavens utvalgte teori som ble presentert i kapittel 3. Formålet med drøftingen er å forsøke å besvare oppgavens forskningsspørsmål for så å nærme seg svaret på problemstillingen:

«*Hvordan etterlever Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?*»

Med utgangspunkt i intervjuene med DSB og NSM i planleggingsfasen av Øvelse IKT16 og oppgavens forskningsspørsmål er kapitelet delt inn i tre delkapitler. Første delkapittel fokuserer på forståelsen av samvirkeprinsippet hos aktørene, andre delkapittel på beredskapsplanlegging i DSB og NSM og det tredje delkapittelet fokuser på hva samvirke mellom DSB og NSM innebærer, og drøfting av eventuelt hemmende faktorer for et godt samvirke. Ved gjennomgang av funnene i dette studiet erfarte vi at tiltak som naturlig faller inn som beredskapsplanleggingstiltak også bidrar til et godt samvirke. Innholdet i drøftingen følger derfor ikke kategorisk strukturen i oppgaven.

6.1 Hva legger DSB og NSM i begrepet samvirkeprinsippet?

Flere sentrale punkter i rapporten fra 22. juli-kommisjonen er særskilt knyttet til at det er et behov for å forstå og forbedre kommunikasjon, samhandling og informasjonsflyt mellom ulike offentlige og private aktører som er involvert i arbeidet med samfunnssikkerhet og beredskap. Rapporten peker på at ledere på alle nivå i forvaltningen systematisk må arbeide med å styrke sine egne og organisasjonenes grunnleggende holdninger, kultur og ledelse og at lederskap må begynne på toppen (NOU 2012: 14).

I empirikapittelet omtales myndighetenes innføring av samvirkeprinsippet i 2012 (Meld. St. 29 (2011-2012)). Her stilles det krav til at virksomheter og etater som DSB og NSM, har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i

arbeidet med forebygging, beredskap og krisehåndtering. Dette er i samsvar med teori om viktigheten av at beredskapsplaner skal sikre samvirke og tydelig presisere ansvarsforholdet for alle involverte aktører (Engen et. al. 2016). I følge Engen et. al. (2016) gjelder dette spesielt for offentlige og private aktører, men også for frivillige aktører. En viktig suksessfaktor i håndteringen av større kriser er effektiviteten i samarbeidet mellom ulike responsaktører. Kompleksiteten i samfunnet øker, noe som medfører at kriser og katastrofer involverer stadig flere aktører. Organisasjonene må kjenne til hverandres mandater, strukturer, kapasiteter og begrensinger, samt mekanismer for koordinering for best mulig å benytte de ofte begrensede ressurser som er tilgjengelige (Engen et. al. 2016).

Ett av virkemidlene DSB har benyttet for å operasjonalisere samvirkeprinsippet, er ved å opprette et samvirkekonferansekonsept. Ved behov tar DSB initiativ til samvirkekonferanser for aktører på etatsnivå som er involvert i krisehåndtering. Det fremkommer i referat fra DSB om evaluering av Forumet Samvirkekonferansekonseptet, at deltakerne i all hovedsak har gode erfaringer med å delta i forumet:

«Bakgrunnen for at vi etablerte samvirkekonferansen var behovet for informasjonsdeling i hektiske faser i håndtering av hendelser. I situasjoner med liten tid til å respondere er det av stor betydning å få en felles tilnærming, så langt som mulig oppnå et felles situasjonsbilde av hva vi står overfor, hvordan er lignende situasjoner håndtert tid ligere og hvordan kan vi best løse hver våre oppgaver i situasjonen vi står i. Hva trenger vi? Og hva kan vi bistå hverandre med?»

Flere av deltakeren mente at konferansene samlet sett gir bedre grunnlag for egen krisehåndtering, også sett i lys av at de gjennom samvirkeforumet får kunnskap om andres arbeid, ansvarsområder og oppgaver. Videre ble det pekt på at samvirkekonferansene bidro til å løfte blikket og sørget for at alle kunne få den samme informasjonen. Dersom mulig er det ønskelig at DSB har et større ansvar for å sy sammen et felles situasjonsbilde i forkant av konferansen, slik at dette kan presenteres ved oppstart slik at møtet kan bli mer effektivt (DSB, referat 4.12.2017).

Intervjuene med DSB og NSM bekrefter at intensjonen med samvirkeprinsippet ble etterlevet under planleggingsfasen av Øvelse IKT16. På spørsmål om DSB og NSM er omtalt i den andre virksomhetens beredskapsplanverk svarte begge virksomhetene at de var omtalt i vaktinstrukser og på varslingslister. En av informantene fra DSB opplyste at:

«NSM er omtalt i planverket ved at virksomheten står omtalt på DSBs varslingslister ved hendelses- krisehåndtering. De står også på distribusjonslister for deling av relevant informasjon, også utenom håndteringsfaser».

Det fremkommer av intervjuene fra informantene i DSB at:

«Selv om det ikke hadde ligget føringer i oppdragsbrevet fra JD om å involvere andre aktører, så mener jeg at DSB ville ha lagt opp til et nært samarbeid spesielt med NSM, fordi de er «eiere» av faget som skulle øves».

Dette viser at DSB har god kunnskap om NSM sitt mandat og fagområde som Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet, og at de på den bakgrunn anså NSM som en svært relevant aktør å samhandle med. Engen et.al. (2016) vektlegger nettopp kunnskap om hverandres mandater, strukturer, kapasiteter og begrensinger samt mekanismer for koordinering. Dette begrunnes både med muligheten for å kunne utnytte ofte begrensede ressurser på en best mulig måte, men også viktigheten av å ha kunnskap om gjensidige avhengigheter.

Informantene fra både DSB og NSM opplyste at det på et tidlig tidspunkt ble diskutert hvilke andre etater det var viktig å få med som deltagere under planlegging av øvelsen. Dette ble gjort på de innledende møtene der DSB, NSM og de øvrige deltagerne som er oppgitt i oppdragsbrevet fra JD, var til stede. Som det fremkommer under empirikapittelet, opplyste en av informantene at han opplevde at både DSB og NSM hadde et bevisst forhold til at begge etatene hadde et særskilt ansvar for å involvere andre aktuelle aktører. En annen av informantene sier at det var stor bevissthet fra spesielt NSM sin side på å involvere de sektorvise responsmiljøene innen IKT. Funnene fra intervjuene avdekker i liten grad at det var utfordringer knyttet til samvirkeprinsippet mellom DSB og NSM under planleggingsfasen av Øvelse IKT16.

Oppsummering

På virksomhetsnivå viser de to aktørene i all hovedsak til offentlige dokumenter når det gjelder de to etatenes forståelse av samvirkeprinsippet, som for eksempel stortingsmeldinger og instrukser, der myndighetenes forventinger til hvordan samvirkeprinsippet skal forstås og etterleves er beskrevet. De viser videre til egne høringsuttalelser til pågående lovarbeid og til det offentlig oppnevnte IKT-sikkerhetsutvalget. Høringsuttalelsene, særskilt de utgitt av DSB, avdekker at det synes å være en holdning til NSM kompetanse og kapasiteter som kan synes

noe bekymringsfull med tanke på kultur og holdninger for å sikre et godt samvirke. På saksbehandlernivå, under et gitt oppdrag som Øvelse IKT16, bekrefter vår funn at DSB og NSM har en forståelse av samvirkeprinsippet som samsvarer med teori om godt samvirke basert på Engen et. al. (2016). Funn gjort i forbindelse med intervjuene bekrefter også at samvirkeprinsippet fungerte godt under den et år lange planleggingsprosessen til Øvelse IKT16.

6.2 Hvordan organiseres beredskapsplanlegging internt og eksternt i DSB og NSM

I dette delkapitlet gjennomføres drøftingen ved å dele kapitlet inn i tre hoveddeler. Den første delen fokuserer på beredskapsplanlegging eksternt i DSB og NSM. Den andre delen fokuserer på beredskapsplanlegging internt i DSB og NSM og den tredje delen fokuserer på krisekommunikasjon under Øvelse IKT16.

Beredskapsplanlegging eksternt i DSB og NSM

Engen et. al. (2016) skriver at beredskap grovt sett «betyr å være forberedt», det vil si å være forberedt på å kunne håndtere en situasjon. I følge Aven et. al. (2004) kan all planlegging spores tilbake til en grunnleggende tro på at forberedelser har en positiv innvirkning på resultatene. I teorikapittelet ble målet med beredskapsarbeid introdusert som det å forberede seg på å håndtere kriser som kan oppstå. Engen et. al. (2016) har videre beskrevet tre faser i en krisehåndtering hvor de ulike krisefasene inngår som en del av en kontinuerlig prosess av beredskapsarbeidet. De ulike krisefasene og deres nærmere beskrivelse omtalt i kapitel 3 ovenfor, og handler om forståelse og erkjennelse av krisen, respons og mobilisering av beredskap, normalisering og gjenoppretting, evaluering og ikke minst læring av øvelser. DSB har gjennom flere år hatt som del av sitt samfunnsoppdrag å planlegge, gjennomføre og evaluere sivile tverrsektorielle øvelser på nasjonalt nivå. Øvelse IKT16 var den sivile tverrsektorielle øvelsen for 2016. Øvingsmålet for Øvelse IKT16 var særskilt rettet mot samhandling og koordinering mellom deltakere i øvelsen. Øvelsen kan relateres til de forskjellige krisefasene ved at erfaringer og læring forhåpentligvis vil føre til at samfunnet er mer motstandsdyktig mot neste krise som kommer (Engen et. al. 2016). I teorikapittelet illustrerer figur 3, side 17, omfanget og mangfoldet av ulike typer kriser og sårbarheter for samfunnet og individet generelt. Den presenteres som en oversikt over kompleksiteten som dreier seg om forhold knyttet til sårbarheter i ulike samfunnsfunksjoner, utilsiktede hendelser og overlagte ondsinnede handlinger som kan ha stor betydning for samfunnssikkerhet (Kruke,

Olsen, og Hovden 2005). Hensikten med Øvelse IKT16 var å forberede samfunnet på å kunne håndtere en ventet eller uventet IKT krise. Scenariet for øvelsen var et omfattende IKT-angrep som kan defineres som en teknologisk krise, der feil i teknologiske systemer kan ramme befolkningen og lokalsamfunnet på ulike måter (Engen et. al. 2016), og tok utgangspunkt i åpne trussel- og risikovurderinger fra NSM, PST og E-tjenesten. Riktig kunnskap om trusselen kommer fra trusselvurderinger og sårbarhetsanalyser (Perry og Lindell 2003).

I teorikapittelet omtaler vi klassifisering av kriser i fire kategorier, henholdsvis konvensjonelle og uventede kriser, upåvirkelige og fundamentale kriser (Gundel 2005). Gundel (2005) begrunner behovet for klassifisering med at første steg i å kontrollere krisen er å gi den navn og senere analysere den. Vet vi hvilken type krise det dreier seg om, kan vi ta frem «verktøykassen» som passer krisetypen vi står overfor, og dermed dra nyttig erfaring fra tidligere kriser. Scenarioet i Øvelse IKT16 kan sies å være en uventet krise som omtalt i Gundel (2005) hvor utvalgte myndigheter og responsmiljøer skulle håndtere et alvorlig IKT angrep i henhold til Rammeverk for digital hendelseshåndtering. Utarbeidelsen av rammeverket er en direkte oppfølging av Lysneutvalgets rapport (NOU 2015: 13). Rammeverket er utarbeidet under ledelse av NSM og skal avklare og tydeliggjøre innsatsen mellom relevante aktører innen hendelseshåndtering og straffeforfølgning, altså en rolle- og ansvarsavklaring. Dette skal igjen bidra til en mer effektiv håndtering av alvorlige IKT-sikkerhetshendelser, fra virksomhetsnivå til politisk nivå, gjennom god utnyttelse av samfunnets samlede ressurser. Det skal videre bidra til å skape god situasjonsoversikt gjennom aggregering og koordinering av informasjon om alle relevante IKT-sikkerhetshendelser. Utarbeidelse av rammeverket er i tråd med NSM sitt samfunnsoppdrag som Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet. Et utkast til rammeverket ble etter oppdrag fra JD (Oppdragsbrev 5.4.2016) benyttet under gjennomføringen av Øvelse IKT16 for å bidra til at de øvende skulle kunne øve roller og ansvar, avklare grensesnitt og forbedringsområder. Vi vil hevde at dette er i samsvar med Aven et. al. (2004) sin påstand om at all planlegging kan spores tilbake til en grunnleggende tro på at forberedelser har en positiv innvirkning på resultatene.

Engen et. al. (2016) viser til at førkrisefasen er rettet mot forståelse og erkjennelse av krisen og i denne fasen inngår risiko og beredskapsanalyse, beredskapsplaner, etablere beredskapsstrukturer og ressurser. Utarbeidelse av Rammeverket for digital

hendelseshåndtering som et forberedende tiltak i førkrisefasen for håndtering av neste IKT-hendelse må sies å være helt i tråd med intensjonen i Engen et. al. (2016) om forberedelser i førkrisefasen. Tiltaket som forberedelse for vellykket krisehåndtering støttes også av utsagnet:

*"Successful strategic crisis management is the result of 80 % generic planning, 15 % improvisation, and 5 % luck" (*Weisæth. et. al. 2002).

Engen et. al. (2016) omtaler flere typer øvelser og hva som kjennetegner disse i form av kompleksitet og organisering. Han nevner blant annet fullskalaøvelser hvor utgangspunktet for en slik øvelse er realistiske scenarioer, som er ressurskrevende både i planlegging, gjennomføring og etterarbeid. I fullskalaøvelser involveres hele beredskapsorganisasjonen, og formålet med øvelsen er å se hvordan organisasjonen fungerer i en helhet og i samvirke med andre aktører (Engen et. al. 2016). Øvelse IKT16 kan sies å være et eksempel på en fullskalaøvelse hvor relevante og sektorvise responsmiljøer var inkludert slik at den nasjonale strukturen for IKT-hendelser kunne testes. Samhandling, rolle- og ansvars avklaring mellom sektorer, fagmiljøer og forvaltningsnivåer stod sentralt i øvelsen. Vi har tidligere i oppgaven omtalt hvilke aktørene som var involvert i Øvelse IKT16, disse er gjengitt i figur 2 side 14.

Engen et. al. (2016), viser til at en øvelse må være så realistisk og nær opp til en virkelig hendelse som mulig for at organisasjonen skal få tilstrekkelig læring av øvelsene. Dette vil fremme muligheten for læring hos aktørene. Vår vurdering er at Øvelse IKT16 var en realistisk øvelse ved at scenariet var et omfattende IKT-angrep som hadde som mål å lamme flere sektorer og forvaltningsområder. Øvelsen tok utgangspunkt i åpne trussel- og risikovurderinger fra NSM, PST og E-tjenesten. Dette grunnlaget understøtter at formålet med øvelsen var å forberede aktuelle aktører på å håndtere en hendelse man antar kan inntreffe, i dette tilfellet et større IKT angrep, og altså i tråd med teori om behovet for å øve realistisk.

Kruke, Olsen et. al. (2016) peker på beredskapsplanlegging som en lineær prosess der krisen normaliseres og evalueres, og det tas lærdom av de virkelige hendelsene som finner sted eller som man øver og trener på den såkalte etterkrisefasen. Når det gjelder tilstrekkelig læring av øvelsene viser et sentralt funn i Riksrevisjonens undersøkelse av Justis- og beredskapsdepartementets arbeid med samfunnssikkerhet og beredskap, at det ikke gjennomføres systematisk evaluering og oppfølging etter øvelser og hendelser (Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017). Undersøkelsen viste videre at læringspotensialet etter hendelser ikke ble unyttet godt

nok. Riksrevisjonens anbefaling var at læringspotensialet etter hendelser og øvelser kartlegges, utnyttes og formidles på en mer systematisk måte. DSB har arbeidet med å systematisere erfaringer fra øvelser og hendelser, men den hevder at det fortsatt gjenstår utfordringer med hensyn til oppfølging av øvelser og hendelser på tvers av sektorer, blant annet knyttet til fordeling av oppgaver og ansvar, og konkretisering av læringspunkter (ibid). Det kan på bakgrunn av disse funnene i denne oppgavens empiri synes å være et gap mellom forventinger til etterkrisefasen (Kruke, Olsen et. al. 2016) og de konklusjoner som fremkommer i Riksrevisjonen oppfølgingsundersøkelse av Justis- og beredskapsdepartementet.

Som nevnt i kapittel 5, ble NSM NorCERT oppgradert til et døgnbemannet senter i 2013. Senterets oppgave er å koordinere håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur på nasjonalt nivå og informere og gir bistand til håndtering av IKT-hendelser. Koordineringen innebærer blant annet å dele relevant og frigitt informasjon med de sektorvise responsmiljøene, politiet, samfunnskritiske virksomheter og andre aktuelle aktører. I NSMs høringssvar til grunnlaget for ny sikkerhetslov, støtter NSM departementets forslag om å lovfeste nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur (NorCERT) og nasjonalt varslingssystem for digital infrastruktur (VDI) (Oppdragsbrev 17.1.2017). Funksjonene VDI og NorCERT har allerede i mange år vært en omfattende del av NSM oppgaver, og er en viktig brikke i leveranser fra NSM. Oppgavene i den forbindelse har nær sammenheng med mange av de øvrige oppgaver som er tillagt den sektorovergripende NSM-funksjonen, som blant annet å gi råd og veiledning til andre virksomheter

Med bakgrunn i disse forholdene vil vi hevde at NSM sin rolle som pådriver for etablering av sektorvise responsmiljøer er tiltak som er gjennomført for å styrke samfunnets samlede evne til å motstå IKT-angrep, og de er i tråd med de føringer NSM er gitt i samfunnsoppdraget.

DSBs samfunnsoppdrag er av en noe annen karakter enn NMS sitt i den forstand at de har et ansvar for å opprette, drifte og administrere beredskapsressurser for at *andre* skal kunne håndtere konsekvensene av *alle* typer uønskede hendelser, ikke bare IKT-hendelser. Drift av skogbrannhelikopter, Sivilforsvarsdistriktene og Redningsinnsats til sjøs (Rits) er eksempler på tiltak på denne type ressurser (DSB kriseplan 2017). DSB har en viktig rolle i å understøtte departementets ansvar for å samordne det nasjonale samfunnssikkerhets- og beredskapsarbeidet. Etaten skal ha oversikt over risiko og sårbarhet i samfunnet, skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og skal

sørge for god beredskap og effektiv ulykkes- og krisehåndtering. De har også ansvar for tiltak som er internasjonalt rettet ved at DSB skal fungere som nasjonalt kontaktpunkt for krisehåndteringsmekanismer i NATO, FN og EU (ibid).

DSBs ansvar og utvikling for Nødnettet må sies å være et tiltak helt i tråd med teorien til Engen et.al. (2016) om at kommunikasjon mellom ulike responsaktører er avgjørende for nødvendig informasjonsutveksling og koordinering, og videre, - at samvirkeprinsippet hviler på en forutsetning om at de involverte aktørene klarer å kommunisere med hverandre. Sammenkoblingen av det norske Nødnettet og det svenske nødnettet Rakel i 2017, er et eksempel på et tiltak som bidrar til samvirke og kommunikasjon over landegrensene og er helt i tråd med forståelsen til Engen et. al. (2016:283) *(...) «ved at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering».*

Læring etter øvelser

Engen et. al. (2016), viser til at en øvelse må være så realistisk og nær opp til en virkelig hendelse som mulig for at organisasjonen skal få tilstrekkelig læring av øvelsene. Måloppnåelsen etter Øvelse IKT16 er oppsummert i Tverrsektoriell evaluering av Øvelse IKT16 (DSB: 2017). Rapporten er unntatt offentlighet jf. offentleglova, og vi har kun fått innsyn i den delen av evalueringsrapporten som omhandler myndighetens kommunikasjonshåndtering til publikum. Drøftingen av dette temaet fremkommer under Krisekommunikasjon under Øvelse IKT16 senere i dette kapitlet. Med bakgrunn i at evalueringsrapporten er unntatt offentlighet er vi ikke kjent med de endelige funn etter evalueringen, og om målet med øvelsen ble oppnådd. Funn i Riksrevisjonens oppfølgingsrapport av Justis- og beredskapsdepartementet (2016-2017) konkluderer imidlertid med at i forbindelse med den umiddelbare gjennomgangen etter Øvelse IKT16, gav deltagerne tilbakemeldinger som gir oss et bilde på måloppnåelsen. Der fremkommer det blant annet at det var utfordringer knyttet til å etablere en felles situasjonsforståelse og å sikre god informasjonsflyt mellom responsmiljøer og myndigheter. Det var krevende å dele og formidle gradert informasjon og sist, men ikke minst, at det var utfordringer knyttet til å sikre god kommunikasjon til befolkningen (Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet 2016–2017). Dette gir oss et inntrykk av måloppnåelsen under

Øvelse IKT16, men ikke god nok innsikt i om kravene i Meld. St. 10 (2016-2017) er fulgt opp.

Perry og Lindell (2003) viser i en av sine retningslinjer for gode planleggingsprosesser at effektiv planlegging bør sørge for å teste foreslåtte responsoperasjoner. Øvelser av beredskapsplaner bidrar til at kommunikasjon med alle aktørene i planverket kommer i kontakt med hverandre. Øvelser bidrar også til økt kunnskap og omfattende prøving av beredskapsplaner, personell, prosedyrer, muligheter, utstyr og materiell. Funn i studiet av planleggingsfasen av Øvelse IKT16 samsvarer med deler av denne teorien, med gjennomføring av samvirkekonferanser med alle de involverte aktørene og jevnlige møter og kontakt på bilateralt nivå mellom DSB og NSM som sentrale elementer gjennom prosessen.

Beredskapsplanlegging internt i DSB og NSM

Under teorikapittelet og omtalen av samvirkeprinsippet fremgår det at myndigheter, virksomheter og etater har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering. I Engen et. al. (2016) fremgår det at beredskapsplaner skal tydeliggjøre ansvarsforholdet for alle involverte aktører. Dette gjelder spesielt offentlige og private aktører, men også frivillige aktører. Kompleksiteten i samfunnet øker, noe som medfører at kriser og katastrofer involverer stadig flere aktører. Videre påpekes det at en viktig suksessfaktor i håndteringen av større kriser er effektiviteten i samarbeidet mellom ulike responsaktører.

Som nevnt under forskningsspørsmål i kapittel 5.3.2 foran, har vi ikke fått innsyn i NSM sin interne kriseplan, men vi har fått delvis innsyn i DSBs interne kriseplan. Av DSBs kriseplan fremkommer det innledningsvis at DSB skal være i stand til å håndtere og begrense konsekvensene av uønskede hendelser. God beskrivelse av systemer og rutiner er fremtredende. Det legges også vekt på klare ansvarsforhold og hvem som er kontaktpunkter, forventinger til fagavdelingene, hvem som skal varsles og hvilke teknologiske systemer som skal benyttes. Dette funnet må sies å være i tråd med Engens et. al. (2016) teori om at ansvarsforhold skal være tydelige og klargjorte for alle involverte aktører. DSBs kriseplan omfatter også beskrivelse av de beredskapsordninger DSB er ansvarlige for, og om deres rolle og ansvar. Funnet sier ikke noe om effektiviteten til disse aktørene under en krise, men det er grunn til å hevde at intensjonen må antas å være i tråd med Engens et.al. (2016) teori om at kriser og katastrofer involverer stadig flere aktører, og at en viktig suksessfaktor i større kriser

er effektiviteten i samarbeidet mellom de ulike responsaktører. Funnet er i tråd med Perry og Lindells (2003) retningslinje om at krisehåndtering i stor grad handler om oppnåelse av tverrfaglig koordinering og samhandling mellom grupper som skal håndtere krisen.

Mangel på tilstrekkelig informasjon om planverket, spesielt hos NSM, svekker i noen grad vår evne til å drøfte denne delen av problemstillingen på en kritisk måte. I forbindelse med prosessen rundt intervjuene fremkom det at flere av informantene måtte forankre deltagelse hos sin ledelse. De samme informantene måtte også få leders godkjenning til å svare på spørsmålene som fremkom i intervjuguiden, og besvarelsen måtte lederforankres. Vi fikk forståelsen av at denne lederforankringen i all hovedsak ble gjennomført for å sikre at gradert informasjon ikke ble omtalt, og at det ikke har påvirket informantenes subjektive svar på spørsmålene.

Funnene i intervjuene viser likevel at både DSB og NSM i sitt planverk hadde hensyntatt den andre virksomheten som en aktuell aktør å samhandle med under kriser. Dette fremkom blant annet på varslingslister og i vaktinstrukser. Ut fra den informasjonen vi har fått tilgang til er det som tidligere nevnt noe krevende å drøfte om det foreliggende planverket hos de to virksomhetene svarer ut kravene til planverk på en god måte. Det har likevel ikke fremkommet noe i intervjuene som tyder på at vektleggingen av skriftlige planer har vært så omfattende at det har trukket oppmerksomheten bort fra planleggingsprosessen og det opprinnelige målet om å oppnå samfunnsberedskap (Perry & Lindell 2003).

Vi fikk ikke innsyn i NSMs interne krisehåndteringsplan. Vi må derfor støtte oss på den informasjonen som kom fram under intervjuene.

Krisekommunikasjon under øvelsen IKT16

Engen et. al. (2016) påpeker at kommunikasjon mellom ulike responsaktører er avgjørende for nødvendig informasjonsutveksling og koordinering, og videre, - at samvirkeprinsippet hviler på en forutsetning om at involverte aktører klarer å kommunisere med hverandre. Det fremkommer videre av Engen et. al (2016) at kunnskapsgenerering betyr å få tak i informasjon om hva som skjer i en krisesituasjon - om å danne en situasjonsforståelse. Coombs beskriver krisekommunikasjon som en prosess bestående av kunnskapsforvaltning og styring av respons (Coombs 2010). Kunnskapen som genereres i kriser må kommuniseres til de som trenger den, og det må etterfølge en nødvendig respons på kunnskapen som gjør at konsekvensen av krisen, skadeomfanget, reduseres mest mulig. Dette står i kontrast til

funnene i evalueringsrapporten som avdekket svikt i krisekommunikasjonen opp mot publikum.

Et sentralt funn i evalueringsrapporten er at myndighetene ikke i tilstrekkelig grad ivaretok befolkningens behov for relevant og brukerorientert informasjon om hvilken situasjon Norge stod i, og hvilke konsekvenser IKT-angrepene fikk for befolkningen og tjenester de er avhengige av. En konsekvens av dette var at befolkningen ikke visste hvordan de skulle forholde seg til den situasjonen de var i, og heller ikke om hendelsen ble forsvarlig håndtert. Det fremkommer også at en del av den informasjonen som ble lagt ut var mindre relevant, den dannet ikke et samlet bilde over situasjonen. Sentrale elementer i en god krisekommunikasjonsprosess mot publikum synes altså å mangle under Øvelse IKT16. Myndighetene evnet ikke å styre en prosess som gav tilstrekkelig kunnskap til befolkningen om hva som skjedde, hvilke konsekvenser hendelsene fikk og de oppnådde da ikke den ønskede respons ute i samfunnet (Coombs 2010). Mangel på koordinering på myndighetsnivå er også et sentralt funn som svekket krisekommunikasjonen mot befolkningen. Nå kan det muligens hevdes at dette kun var en øvelse, og at det i en reell situasjon ville ha fungert bedre. På den annen side ble det brukt et helt år på å forberede denne øvelsen, og det ble planlagt med et omfattende mediespill for å øve krisekommunikasjon og mediehåndtering. Med dette som bakteppe må det være grunnlag for å si at Engen et. al. (2016) og Coombs (2010) forventninger til kommunikasjon mellom ulike sentrale aktører har et forbedringspotensial når det gjaldt krisekommunikasjonen under Øvelse IKT16.

Oppsummering

Vi har fått lite informasjon om hvordan NSM organiserer sitt interne beredskapsplanverk da informasjonen er unntatt offentlighet. Eksternt er NSM ansvarlig for tiltak og beredskapsordninger som bidrar til å bedre samfunnets beredskap og krisehåndtering ved blant annet IKT hendelser. En del av disse tiltakene er relativt nyetablerte slik at effekten av tiltakene ikke er materialisert, men det er all mulig grunn til å tro at de vil bedre samfunnets evne til god krisehåndtering. Den delen av DSBs interne beredskapsplan som vi har fått innsyn i, ivaretar de krav til beredskapsplanverk som teorien beskriver. Eksternt har DSB ansvaret for en rekke beredskapsordninger som skal bidra til at andre beredskapsaktører skal kunne håndtere konsekvensene av alle typer uønskede hendelser, ikke bare IKT-hendelser.

6.3 Hvilke faktorer hemmer samhandling mellom DSB og NSM

Kapitlet tar utgangspunkt i Engens et.al. (2016) teori om betydningen av at organisasjoner må kjenne hverandres mandater, strukturer, kapasiteter og begrensinger, samt mekanismer for koordinering for best mulig å benytte de ofte begrensede ressurser som er tilgjengelig. Engen et. al. (2016) diskuterer også kultur som en faktor som kan påvirke organisatorisk sikkerhet, og vi ser på forskningsspørsmålet opp mot disse teoriene. Engens et. al. (2016) teorier om krisehåndtering og krav til beredskapsplaner for å sikre samvirke og tydelig presisere ansvarsforholdet for alle involverte aktører, er også aktuelle.

Innledningsvis i oppgaven er samfunnssikkerhet og beredskap og utfordringer knyttet til etatene som er ansvarlig for samfunnssikkerhet og beredskap omtalt. I følge 22. juli kommisjonens rapport er utfordringene særskilt knyttet til risikoforståelse og sikkerhetskultur, mangel på samhandling, mangel på evne til å utnytte potensialet i informasjons- og kommunikasjonsteknologi, dårlig informasjonsflyt og sist, men ikke minst: kultur, holdning og ledelse (NOU 2012: 14).

I arbeidet med denne oppgaven har vi avdekket forhold som kan tolkes som noe manglende tillitt mellom DSB og NSM. Spesielt DSBs høringssvar til grunnlaget til ny sikkerhetslov der det blant annet fremkommer at «*NSM mangler kompetanse på å gjøre vurderinger, føre tilsyn og gi råd om sikkerheten i kritiske samfunnsfunksjoner i tråd med lovforslaget*» (Brev 19.1.2017). Vi tar ikke stilling til om påstanden er riktig, men utsagnet må kunne sies å bære preg av en noe svekket tillit til NSMs kompetanse, selv om vi riktignok kan hevde at DSB med dette viser til at de mener å ha god oversikt over NSMs kapasiteter og begrensinger. Dette er i tråd med Engen et. al. (2016) sin teori om at organisasjoner må ha kunnskap om hverandres strukturer, kapasiteter og begrensinger for å få utnyttet de ressurser som er tilgjengelige. Det fremkommer videre av DSBs høringssvar til ny sikkerhetslov at DSB mener at de allerede har de ovenfor nevnte oppgaver: *«Forslaget vil medføre duplisering av kompetanse og byråkratisering, uten at disse problemstillingene drøftes nærmere»* (Brev 19.1.2017).

Videre mener DSB at de bør ha rollen som Sikkerhetsmyndighet, sitat fra høringssvaret: *«DSB bør ha rollen som Sikkerhetsmyndighet etter loven»*. Det faktum at rollen som Sikkerhetsmyndighet er tillagt NSM i forskriftene til ny sikkerhetslov, som under arbeidet med dette studiet er på alminnelig høring, er helt i strid med DSBs oppfatning av hvem som

bør ha rollen som sikkerhetsmyndighet (regjeringen.no.). Et så vidt sprikende syn på hvilken av de to etatene som skal ha en så viktig rolle, må antas å være en faktor som *kan* hemme den fremtidige samhandlingen mellom de to etatene. Vår forståelse av dette er at det kan være en kulturell holdning hos DSB som er i tråd med påstanden om at kulturer uttrykker systemer av mening, der en bestemt gruppe forstår verden rundt seg, (Turner og Pidgeon 1997). Kultur og grunnleggende holdninger var sentrale faktorer for hva som gikk galt 22. juli 2011 (NOU 2012:14). Den nye sikkerhetsloven er imidlertid ikke trådt i kraft enda og virkningene av den er ikke materialisert. Uenighet på synet om hvem som bør ha rollen som sikkerhetsmyndighet, og eventuelle konsekvenser av dette som en hemmende faktor, må derfor enn så lenge sees på som en hypotese fra oss som ansvarlige for denne masteroppgaven.

Videre er dette sitatet hentet fra høringssvaret «*Myndighetsutøvelse fra hemmelige tjenester må være langt tydeligere avgrenset enn det forslaget legger opp til. Rapporten inneholder ingen drøfting av kompetansekrav til Sikkerhetsmyndigheten og alternativer til å legge ansvaret til NSM. Et utvidet gradert regime vil hemme samarbeid og kommunikasjon internt i virksomhetene, mellom tilsynsetatene og vis-à-vis lokalsamfunnet. Slike virkninger av lovforslaget er ikke vurdert». (*Brev 19.1.2017 s. 1).

Foruten at svaret forsterker oppfatningen av DSBs noe manglende tillit til NSM, avdekker funnet at også denne delen av lovforslaget etter DSBs oppfatning vil hemme samarbeidet og kommunikasjon mellom tilsynsetatene, en rolle både DSB og NSM har i dag. Gode mekanismer for koordinering fremheves som en viktig faktor for godt samvirke av Engen. et.al. (2016). Den uttalte bekymringen må etter vårt syn kunne tolkes å stå noe i motstrid til denne teorien.

Regjeringen nedsatte IKT-sikkerhetsutvalget i 2017. Oppdraget til utvalget var å se på regelverk og organisering innenfor IKT-sikkerhet, med målsetting om økt IKT-sikkerhet. Som en del av utvalgets arbeidsmetodikk har det blitt sendt ut et spørreskjema til en rekke virksomheter, blant annet til både DSB og NSM. Spørsmål 8 refereres i det følgende: *Hvordan opplever din virksomhet samarbeid og koordinering innenfor IKT-sikkerhet mellom myndighetsorganer med ansvar for IKT-sikkerhet?* DSBs svar er ganske omfattende, og inneholder blant annet følgende påstand: *NSM sitter ikke på oversikten over de mulige*

konsekvensene av en IKT-sikkerhetshendelse, det er det de enkelte fagmyndigheter og DSB som gjør.

Spørsmål nr. 13 retter seg mot om den enkelte virksomhet får dekket behovet for råd og veiledning innenfor IKT-sikkerhet. Til dette svarer DSB at de ikke gjør det i tilstrekkelig grad. *Både NSM og Nkom synes å ha begrensede ressurser til å bistå med rådgiving* (Svar fra DSB på spørreskjema: Brev 20.2.2018 s. 3). NSMs svar på IKT-sikkerhetsutvalget spørreskjema er unntatt offentlighet, og vi har ikke fått innsyn i dette. DSBs svar understøtter etter vår vurdering DSBs syn på NSMs manglende kompetanse og ressurser slik det framkom i DSBs høringssvar til grunnlag for ny sikkerhetslov (Brev 19.1.2017). Svaret uttrykker en bekymring knyttet til 22. juli kommisjonens rapport der de ble konkludert med at kultur og grunnleggende holdninger var sentrale faktorer for hva som gikk galt 22. juli 2011 (NOU 2012: 14).

Av Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016–2017) fremkommer det at erfaringer fra tidligere øvelser viser at informasjonsdeling, ansvar og rolleforståelse har vært en utfordring, og at det er behov for å styrke samvirket mellom aktørene. Dette var derfor et tema i forberedelsene til Øvelse IKT16.

Det fremkommer videre av Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017) at DSB innhentet inntrykk og kommentarer fra deltakerne umiddelbart etter Øvelse IKT16. Følgende forhold ble påpekt som utfordrende:

- *å etablere en felles situasjonsforståelse*
- *å sikre god informasjonsflyt mellom responsmiljøer og myndigheter*
- *å dele og formidle gradert informasjon*
- *å sikre god kommunikasjon til befolkningen*

De uttalte utfordringene med å etablere et felles situasjonsbilde, å sikre god informasjonsflyt mellom responsmiljøer og myndigheter, å dele og formidle gradert informasjon samt å sikre god kommunikasjon til befolkningen, henger etter vårt syn nøye sammen. For at de rette tiltakene skal kunne iverksettes er det avgjørende med rettidig informasjon om hva som faktisk skjer. Informasjonen må derav kunne videreformidles til de som har behov for den, og ved større IKT-hendelser vil dette normalt være myndighetene. Myndighetene må, basert på

den informasjonen de får, etablere et situasjonsbilde. På bakgrunn av et rettidig situasjonsbilde vil det iverksettes nødvendige tiltak for å minimere skadene og gjenopprette normaltilstanden. Myndighetene må også kunne kommunisere til befolkningen om hva som skjer, og hvilken respons de ønsker fra befolkningen (Coombs 2010). Basert på disse funnene er det vår vurdering at det fortsatt er mange forbedringspunkter som må gjennomføres før krisehåndteringen er i tråd med Engens et. al. (2016) teori om god krisehåndtering.

I DSBs høringssvar (Brev 19.1.2017) til grunnlaget for ny sikkerhetslov (NOU 2016: 19) hevder DSB at et utvidet gradert regime vil hemme samarbeid og kommunikasjon internt i virksomhetene, mellom tilsynsetatene og vis-à-vis lokalsamfunnet. Slike virkninger av lovforslaget er imidlertid ikke vurdert og loven har heller ikke trådt i kraft per i dag. Vi har derfor ingen kunnskap om enkelte av forslagene i ny sikkerhetslov faktisk vil hemme samarbeidet mellom tilsynsetatene, herunder DSB og NSM. Likevel er det verdt å merke seg at DSB allerede før loven trer i kraft er bekymret for at et utvidet gradert regime vil kunne hemme fremtidig samarbeid.

Funn fra intervjuene med DSB og NSM belyser at det hersker forskjellige kulturer mellom virksomhetene om hvordan gradert informasjon skal håndteres med hensyn til "need to know/nice to know" prinsippet. En av informantene opplyste at det hadde vært noe diskusjon og refleksjon rundt dette uten at det kunne sies å ha skapt nevneverdige problemer.

En mulig feilkilde i dette studiet er at vi ikke har lykkes med å få særlig innsyn i NSM sin noe lukkede verden. Ut over den noe begrensede informasjonen vi fikk i forbindelse med intervjuprosessen har vi blitt henvist til offentlige dokumenter. Noen av disse gir oss oversikt over hva NSM har iverksatt av tiltak for å operasjonalisere samvirkeprinsippet, men vi vet lite om kultur og holdninger hos NSM.

Avslutningsvis i dette kapitlet vil vi understreke at det de siste årene er blitt gjennomført en rekke tiltak for å styrke samhandlingen mellom relevante aktører både generelt, men også særskilt for IKT-hendelser. Tiltakene som er gjennomført er basert på evalueringer etter reelle hendelser og øvelser. Målsetting med tiltakene er å styrke det tverrsektorielle samarbeidet. Det er for eksempel etablert en rekke sektorvise responsmiljøer (CERTer), Rammeverk for håndtering av IKT-hendelser er utarbeidet og det er etablert et felles Cyberkoordineringssenter (FCKS). Senteret har som mål å koordinere de hemmelige tjenestenes innsats på cyberområdet der formålet er å tilrettelegge for kommunikasjon mellom

de forskjellige virksomheter og etater i større grad enn tidligere. Det må nevnes at både rammeverket og FCKS er relativt nyetablerte, effekten av disse kan derfor ikke sies å være materialisert. På den andre siden viser et sentralt funn i Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017) at tross en del innførte tiltak er det fortsatt utfordringer knyttet til arbeidet med samfunnssikkerhet og beredskap, blant annet på samvirkeområdet mellom helt sentrale aktører som DSB og NSM. Undersøkelsen dokumenterer også at det ikke gjennomføres systematisk evaluering og oppfølging etter øvelser og hendelse. Undersøkelsen viser videre at læringspotensialet etter hendelser ikke blir unyttet godt nok, og at læringen ikke er systematisert. Riksrevisjonens anbefaling er at læringspotensialet etter hendelser og øvelser kartlegges, utnyttes og formidles på en mer systematisk måte.

Oppsummering

Det er fortsatt utfordringer knyttet til sentrale faktorer for god krisehåndtering som å etablere en felles situasjonsforståelse, sikre god informasjonsflyt mellom responsmiljøer, dele og formidle gradert informasjon og å sikre god kommunikasjon til befolkningen. Funnene er hentet fra evalueringer etter øvelser og hendelser, og gjelder foruten DSB og NSM også andre beredskapsaktører. Det er fortsatt et behov for å utnytte læringspotensialet bedre etter øvelser og hendelser. Regelverk kan være en hemmende faktor for godt samvirke i den grad det bidrar til å knytte usikkerhet til rolle- og ansvarsavklaringer. Våre funn avdekker at kultur og holdninger mellom DSB og NSM kan være en hemmende faktor mellom de to aktørene på virksomhetsnivå. Funnene viser imidlertid at det er gode samarbeidsforhold på lavere nivå i de to virksomhetene.

7 Konklusjon

Formålet med dette studiet har vært å besvare følgende problemstilling:

Hvordan etterlever aktørene Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?

For å svare på problemstillingen ble det utformet tre forskningsspørsmål – hvordan DSB og NSM forstår samvirkeprinsippet, hvordan beredskapsplanleggingen organiseres hos de to aktørene, og hvilke faktorer som hemmer samhandling mellom DSB og NSM.

Et sentralt funn i studiet er at det er gjennomført en rekke tiltak for å bedre beredskapen og krisehåndteringsevnen i samfunnet etter 22. juli, herunder evnen til samvirke mellom sentrale beredskapsaktører. Tiltakene er i all hovedsak initiert på myndighetsnivå, det vil si fra regjeringen eller fra enkelte departementer. Oppdraget med å følge opp tiltakene er gitt underliggende etater, blant annet DSB og NSM. Effekten av flere av tiltakene som er av relevans for vårt studie, som for eksempel Rammeverk for digital hendelseshåndtering og opprettelse av flere sektorvise responsmiljøer, har et stort potensiale, men trenger tid og ressurser til å videreutvikles. Gjennomføring av sektorovergripende øvelser, krav til evalueringer og krav til systematisk oppfølging av læringspunkter, er pågående prosesser hvor det fortsatt er store forbedringspotensialer. (Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet 2016-2017). Etableringen av Samvirkekonferansekonseptet er en operasjonalisering av samvirkeprinsippet fra DSB sin side og etableringen av Nasjonalt øvelses- og evalueringsforum under ledelse av DSB er positivt og skal bidra til at det skal bli enklere å bli enige om hvem som er ansvarlig for å rette opp forbedringspunktene.

Både DSB og NSM henviste oss til konkrete offentlige dokumenter med henblikk på hva de på virksomhetsnivå legger i samvirkeprinsippet. Gjennomgang av aktuelle dokumenter viser funn som kan synes at det er noe motstrid i oppfatningen av hvem som bør ha ansvaret for hvilke oppgaver på enkelte områder, og at DSB har noe manglende tillit til NSMs kompetanse og ressurser. Funnene er basert på DSBs høringssvar på grunnlaget for ny sikkerhetslov (NOU 2016: 19) Samhandling for sikkerhet og på svar på spørreskjema fra IKT-sikkerhetsutvalget. Et lovverk må klargjøre roller og ansvarsforhold og ikke bidra til uklarheter som vanskeliggjør samarbeidsforholdene. Funnene uttrykker også en holdning til NSM fra DSB sin side som kan være noe foruroligende med tanke 22. juli kommisjonens rapport om at kultur og holdninger ble trukket frem som en årsak til at mye gikk galt den 22. juli (NOU 2012: 14). Det er imidlertid viktig å understreke at ny sikkerhetslov ikke har trådt i kraft, og at IKT-sikkerhetsutvalgets arbeid ikke er avsluttet, og at det derfor er for tidlig å konkludere med at dette vil bli et problem. Vi har gjennom dette studiet ikke fått klarlagt om NSM har andre oppfatninger av samvirkeprinsippet enn de føringer som er gitt fra myndighetsnivå, som definisjoner i stortingsmeldinger og instrukser utgitt av JD, da deres

høringssvar på både grunnlaget til ny sikkerhetslov og svar til IKT-sikkerhetsutvalget er unntatt offentlighet.

Funnene fra arbeidet med dette studiet understøtter imidlertid at det praktiske samvirket mellom de to etatene under planlegging av Øvelse IKT16 synes å være i tråd med de forventninger som stilles til samvirkeprinsippet hos Engen et. al. (2016) og de definisjoner som er gitt fra myndighetsnivå i Meld. St. 29 (2011-2012). Svarene fra informantene fra DSB og NSM er så vidt samsvarende at det er vanskelig å konkludere annerledes. Det er riktignok noe usikkerhet knyttet til hvor detaljert virksomhetens planverk beskriver samhandling med den andre etaten da vi ikke har fått innsyn i dette. DSB og NSM var velvillig innstilt i forhold til hverandre, var klar over hverandres faglige styrker og at de var gjensidig avhengige av hverandre for å lykkes best mulig med å planlegge øvelsen. De var også opptatt av hvilke andre virksomheter og fagmiljøer som måtte involveres for å få et best mulig resultat av Øvelse IKT 16.

Tanken om at beredskapsplanverk er en vesentlig del av det forebyggende arbeidet med samfunnssikkerhet og beredskap, gjenspeiles særskilt i DSBs interne planverk. Interne og eksterne samvirkeaktører, herunder også NSM, omfattes av planverket, varslings- og møterutiner er beskrevet. DSB har også opprettet flere arenaer i den hensikt å inkludere sentrale aktører for bedre samvirke, og har gitt ut en rekke veiledere som blant annet skal være et verktøy for en helhetlig, systematisk og strukturert tilnærming til arbeidet med samfunnssikkerhet og beredskap. NSMs interne beredskapsplanverk har vi ikke fått innsyn i, men funn i intervjuene bekrefter at DSB er en av aktørene som er omtalt i planverket.

Funnene i dette studiet viser at det er gjort mye bra arbeid de siste årene for å bedre samvirket mellom sentrale aktører, men at det fortsatt er utfordringer knyttet til samvirket generelt og også mellom de to aktørene DSB og NSM. Vi mener at samvirke krever samhandling. God samhandling krever tillitt og kjennskap til hverandre. Samhandlingsdeltakerne er fortrinnsvis ute etter en gevinst ved samhandlingen. Gevinsten er å kunne løse sitt oppdrag best mulig. Denne masteroppgaven har vist at en erkjennelse av profesjonsavhengigheter på tvers av virksomheter er viktig for å oppnå ønsket gevinst. Kunnskap om hverandre er helt avgjørende for å kunne oppnå en avhengighetserkjennelse. For å sikre slik kunnskap hos alle aktører må derfor slike avhengighetsforhold nedfelles i internt planverk. I tillegg viser oppgaven at tillitt mellom aktørene er viktig for å oppnå godt samvirke. En arbeidskultur som bygger på tillit er derfor også avgjørende i tillegg til et godt planverk. Resultatet har blitt en oppgave som viser

at selv om regjeringen innførte samvirkeprinsippet etter 22. juli, så viser funnene at det fortsatt er behov for å styrke samvirket mellom beredskapsaktørene. Vi vil derfor avslutte med å slå fast at faktorene avhengighetserkjennelse, kunnskap om den andres ansvarsområder, tillittskultur og godt planverk, er avgjørende faktorer for å ivareta samvirkeprinsippet.

7.1 Svar på problemstilling

Hvordan etterlever aktørene Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?

Både DSB og NSM synes å ha et bevisst og avklart forhold til hvilke forventninger samvirkeprinsippet legger på de som nasjonale beredskapsaktører, og det er igangsatt mange tiltak for å operasjonalisere samvirkeprinsippet. I konkrete oppdrag, som å forberede Øvelse IKT16, fungerte samvirkeprinsippet godt mellom de to aktørene. I lys av Engens et. al. (2016) vurderinger om god beredskap og effektiv krisehåndtering, er det likevel fortsatt en del utfordringer. Dette skyldes at effekten av flere av de iverksatte tiltakene enda ikke er materialisert, mangel på oppfølging av funn etter hendelser og øvelser og sist men ikke minst, ledelse, kultur og holdninger.

7.2 Forslag til videre forskning

Denne oppgaven har vært avgrenset til å se på hvordan de to aktørene DSB og NSM etterlever samvirkeprinsippet. Det kan i framtiden være av interesse å undersøke om samvirke mellom andre aktører samsvarer med funnene fra denne oppgaven. I videre forskning vil det være interessant å se på «kjernen» av utfordringene om og hvordan samvirkeprinsippet i det videre blir etterlevet mellom andre sentrale aktører i krisehåndtering. Det kan bidra til å belyse hensikten med samvirkeprinsippet. Vi er kjent med at det er gjennomført flere forskingsprosjekter på dette temaet, og det vil være av interesse å se nærmere på noen av prosjektene, for å få et overordnet bilde på utviklingen. NEXUS er et eksempel på et prosjekt som har studert endringer og læringsprosesser som har funnet sted i etterkant av terrorhandlingene i Oslo og på Utøya 22. juli 2011. Oppsummeringen av hovedfunnene i forskningsprosjektet viser at risikoerkjennelsen i samfunnet generelt, og blant aktører som arbeider med samfunnssikkerhet og beredskap, har økt. Oppfølgingen av terrorangrepene 22. juli 2011 ser ut til å ha hatt en effekt på samfunnssikkerhets- og beredskapsområdet i form av en økt bevissthet om at hendelser med lav sannsynlighet og store konsekvenser må komme på dagsorden og bli prioritert. Vi er i det videre spente på å se hvilken retning utviklingen i norsk

samfunnssikkerhet og beredskap tar, med tanke på Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementet (2016-2017) og implementering av ny sikkerhetslov som trer i kraft i januar 2019.

8 Referanser

Albrechtsen, Eirik; Almklov, Petter Grytten; Antonsen, Stian; Nyheim, Ole Magnus; Nilsen, Marie; Bye, Rolf Johan; Johnsen, Stig Ole; Wasilkiewicz, Kinga; Aalberg, Asbjørn. (2017). *Har samfunnssikkerheten blitt bedre etter 22. juli 2011? Populærvitenskapelig rapport fra forskningsprosjektet The next disaster (NEXUS).* 2017. Hentet fra https://www.sintef.no/globalassets/sintef-teknologi-og-samfunn/rapporter-sintef-ts/nexus-sluttrapport.pdf

Aven, Terje, Marit Boyesen, Ove Njå, Kjell H. Olsen og Kjell Sandve (2004). *Samfunnssikkerhet.* Universitetsforlaget, Oslo.

Befolkningsundersøkelsen om risikopersepsjon og beredskap i Norge og grafisk rapport. Hentet fra https://www.dsb.no/globalassets/dokumenter/nyheter/rapport_bu_2016.pdf

Boin, A., Hart, P., Stern, E. & Sundelius, B. (2005). *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge, Cambridge.

Coombs, W.T. & Holladay, S.J. (2010). *The Handbook of Crises Communication.* Malden, Mass: Blackwell Publishing Ltd.

Cullberg, J. (1994). *Mennesker i krise og utvikling: en psykodynamisk og sosialpsykiatrisk studie*. [Oslo]: Aschehoug.

DSB (2015). *Departementenes systematiske samfunnssikkerhets- og beredskaps arbeid*. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

DSB (2017). *Høringsuttalelse til NOU 2016:19. Samhandling for sikkerhet.* Brev 19.1.2017. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap. Hentet fra https://www.dsb.no/globalassets/dokumenter/nyheter/traavik-uttalelse_dsb.pdf

DSB (2018). *IKT-sikkerhetsutvalget spørreskjema med svar fra DSB*: Brev 20.2.2018. Direktoratet for samfunnssikkerhet og beredskap.

DSB (2017). *Tverrsektoriell evaluering av øvelse IKT 16* – Unntatt offentlighet. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Direktoratet for samfunnssikkerhet og beredskap, DSB internettside. Hentet fra https://www.dsb.no/

DSB (2017). *DSBs krisehåndteringsplan.* Unntatt offentlighet. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

DSB (2017). *Referat fra evaluering av samvirkekonferansekonseptet.* Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Justis- og beredskapsdepartementet (2018). *Tildelingsbrev til Direktoratet for samfunnssikkerhet og beredskap fra Justis- og beredskapsdepartementet.* Hentet fra https://www.dsb.no/globalassets/om-dsb/tildelingsbrev-2018.pdf

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

Fornyings-, administrasjons- og kirkedepartementet (2012). *Nasjonal strategi for informasjonssikkerhet*. Oslo: Fornyings-, administrasjonens og kirkedepartementet.

Forsvarsdepartementet (2018). *Høringsnotat forslag til forskrift til ny Sikkerhetslov 2. juli*. Hentet fra https://www.regjeringen.no/contentassets/61541372f9f74ed1982b0a4338d791f2/horingsnotat---forskrifter-til-sikkerhetsloven.pdf

Forskrift om informasjonssikkerhet (2001). (FOR-2001-07-01-744).

Holme, Idar Magne og Solvang, Bernt Krohn (1998). *Metodevalg og metodebruk*. Tano, Oslo.

Holtan, S., Sollid, S.J.M., Fivel, P.M., Knutsen, T.H., Davidsen, J., Bjelland, B., Eidem, S. (2015). *Veien mot bedre samvirke.* Rapport fra ekspertgruppe februar 2015. Rygge beredskapssenter. Hentet fra http://ryggeberedskapssenter.no/wp-content/uploads/2013/06/Rygge-ekspertrapport-2015_FINAL.pdf

IKT-sikkerhetsutvalget. Hentet fra https://www.regjeringen.no/no/dep/jd/org/styre-rad-og-utval/tidsbegrensede-styrer-rad-og-utvalg/IKT-sikkerhetsutvalget/id2570775/

Innbrudd i datasystemene til Sykehuspartner i Helse Sør-Øst. Hentet fra https://www.helse-sorost.no/nyheter/innbrudd-i-datasystemene-til-sykehuspartner-i-helse-sor-ost

Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller (2005). (FOR-2005-06-24-688).

Justis- og beredskapsdepartementet (2017). Kongelig resolusjon av 14.3.2017. *Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet.* Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet. *Oppdragsbrev Øvelse IKT 16 til Direktoratet for samfunnssikkerhet og beredskap* (Brev av 10.11.2015). Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet. *Oppdragsbrev Rammeverk for digital hendelseshåndtering til Nasjonal sikkerhetsmyndighet* (Brev av 5.4.2016). Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet (2017). *Rammeverk for håndtering av IKT-sikkerhetshendelser*. Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet (2017). *Instruks for departementenes arbeid med samfunnssikkerhet (Samfunnssikkerhetsinstruksen).* Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet (2012). Kongelig resolusjon av 15.06-2012 – *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap. Justis- og*

beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering. Oslo: Justis- og beredskapsdepartementet.

Jacobsen, Dag Ingvar (2005). *Hvordan gjennomføre undersøkelser?* Innføring i samfunnsvitenskapelig metode, Høyskoleforlaget, Oslo.

Kristiansen, E., Magnussen, L., I. og Carlström, E. (2017). *Samvirke - en lærebok i beredskap.* Oslo: Universitetsforlaget AS.

Kruke, Bjørn Ivar (2017). *Risiko og sikkerhet i krise- og konflikter, Kriser og krisehåndtering.* Handouts fra forelesning i Risiko og sikkerhet. Stavanger: Universitetet i Stavanger.

Kruke, Olsen og Hovden (2005). *Samfunnssikkerhet forsøk på en begrepsfesting*.

Kruke, Bjørn Ivar. (2012). *Samfunnssikkerhet og krisehåndtering: Relevans for 22. juli 2011*. 22. juli-kommisjonen. Notat 7/12: 22. juli kommisjonen.

Kommunal – og moderniseringsdepartementet (2017). Handlingsplan – *Nasjonal strategi for informasjonssikkerhet.* Oslo: Kommunal – og moderniseringsdepartementet.

Meld. St. 10 (2016-2017). *Risiko i et trygt samfunn.* Oslo: Justis- og beredskapsdepartementet

Meld. St. 21 (2012–2013). *Terrorberedskap – Oppfølging av NOU 2012: 14 Rapport fra 22. juli-kommisjonen.* Oslo: Justis- og beredskapsdepartementet.

Meld. St. 29 (2011-2012). *Justis- og beredskapsdepartementet, Samfunnssikkerhet.* Oslo: Justis- og beredskapsdepartementet.

Mørketallsundersøkelsen (2016). *Informasjonssikkerhet, personvern og datakriminalitet.* Hentet fra http://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf

Mørketallsundersøkelsen (2018). *Informasjonssikkerhet, personvern og datakriminalitet.* Hentet fra https://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketallsunders%C3%B8kelsen%202018%20low.pdf

NRK internettside. Hentet fra https://www.nrk.no/norge/dsb-undersokelse_-nordmenn-frykter-terror-mest-1.13362972

NOU 2000:24 (2004). *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Oslo: Justis og beredskapsdepartementet.

NOU 2015:13 (2015). *Digital sårbarhet- sikkert samfunn- Beskytte enkeltmenneske og samfunn i en digitalisert verden.* Oslo: Justis- og beredskapsdepartementet.

NOU 2012:14 (2012). *Rapport fra 22. juli-kommisjonen.* Oslo: Statsministerens kontor.

NOU 2016:19 (2016). *Samhandling for sikkerhet.* Oslo: Justis- og beredskapsdepartementet.

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

NSM (2018). *Risiko 2018.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

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

NSM (2016). *Ti viktigste tiltak mot dataangrep.* Hentet fra https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf

NSM (2017). *Høringsuttalelse til NOU 2016:19. Samhandling for sikkerhet. (Brev* 17.1.2017) Hentet fra https://www.regjeringen.no/contentassets/b12eac7f085b4e0885b3f60f17435ecc/nasjonal-sikkerhetsmyndighet_med-merknader.pdf?uid=Nasjonal_sikkerhetsmyndighet_(NSM)

NSM Nasjonal sikkerhetsmyndighet, NSM internettside. Hentet fra https://www.nsm.stat.no/

NSM Ni av ti dataangrep kunne blitt unngått hvis fire enkle råd var blitt fulgt. Hentet fra http://www.dagbladet.no/nyheter/nsm---ni-av-ti-dataangrep-kunne-blitt-unngatt-hvis-fire-enkle-rad-var-blitt-fulgt/60414334

NSM (2017). *Rammeverk for håndtering av IKT-sikkerhetshendelser*, versjon pr 7.12.2017. Hentet fra https://nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Offentleglova. (2009). Lov om rett til innsyn i dokument i offentleg verksemd (LOV-2006-05-19-16).

Olsvik, E. H (2013). *Vitenskapsteori for politiet.* Gyldendal, Oslo.

Perry, Ronald W, og Lindell, Michael K. (2003). *Preparedness for Emergency Response*: *Guidelines for the Emergency Planning Process Disasters (s. 336-350).* Oxford, USA: Blackwell Publishing.

Quarantelli, E. L. (1998). *Major Criteria For Judging Disaster Planning And Managing Their Applicability In Developing Countries.* Preliminary paper # 268, Newark, University of Delaware Disaster Research Center.

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* Aldershot, Burlington USA, Singapore, Sydney, Ashgate.

Rosenthal, U., Charles, M.T., og ´t Hart, P. (Eds.) (1989). *Coping with crises: The management of disasters, riots and terrorism.* Springfield, IL, Charles C Thomas.

Riksrevisjonen (2014-2015). *Riksrevisjonens undersøkelse av Justis- og beredskapsdepartementets arbeid med samfunnssikkerhet og beredskap* Dokument 3:7 (2014-2015) Oslo: Riksrevisjonen.

Riksrevisjonen (2016-2017). *Riksrevisjonens oppfølgingsundersøkelse av Justis- og beredskapsdepartementets arbeid med samfunnssikkerhet og beredskap,* Dokument 3:8 (2016–2017). Oslo: Riksrevisjonen.

Samfunnssikkerhetsinstruksen (2017). *Instruks for departementenes arbeid med samfunnssikkerhet* (FOR-2017-09-01-1349).

Sikkerhetsloven (2010). Lov om forebyggende sikkerhetstjeneste (LOV-1998-03-20-10)

St.meld. nr. 17 (2001-2002). *Samfunnssikkerhet. Veien til et mindre sårbart samfunn*. Oslo: Justis- og politidepartementet.

St.meld.nr. 24 (1992-1993). *Det fremtidige sivile beredskap.* Oslo: Justis og politidepartementet.

Turner, B. A., & Pidgeon, N. F. (1997). Man-made disasters (2. edn). Oxford: Butterworth-Heinemann.

Weisæth, L. Knudsen, Ø. Jr. and Tønnessen, A. (2002). *Technological disasters, crisis management, and leadership stress*. Journal of Hazardous Materials 93: 33-4.

Yin, R. K. (2012). *Applications of case study research* (3. utg.). Los Angeles: Sage.

Øvelse IKT16. Hentet fra https://www.regjeringen.no/no/aktuelt/tidenes-storste-ikt-ovelse/id2521945/

Vedlegg

Vedlegg 1: Brev til informantene

Vedlegg 2: Intervjuguide

Vedlegg 1: Brev til informantene

INTERVJUER I FORBINDELSE MED MASTEROPPPGAVE I RISIKO, SIKKERHET OG SÅRBARHET

Vi deltar for tiden på masterstudiet, Risiko, Sikkerhet og Sårbarhet ved Universitetet i Stavanger. Som en del av studiet skal vi, Renate Thoreid fra Telenor og Ingrid Skjørland Justis og beredskapsdepartementet skal skrive en masteroppgave hvor vi ønsker å se nærmere på denne problemstillingen:

1. *Hvordan etterlever aktørene Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet samvirkeprinsippet?*

For å få svar på vår problemstilling og gjennomføre en analyse har vi behov for å intervjue et utvalg av personer som var involvert i planleggingen av Øvelse IKT16.

Håper på din velvilje på vår forespørsel.

Vi gjør oppmerksom på at alle vi skal intervju og svarene vil bli anonymisert. Samtidig har vi taushetsplikt.

På forhånd tusen takk for hjelpen!

Med vennlig hilsen

Renate Thoreid Ingrid Skjørland

Vedlegg 2: Intervjuguide

Spørsmål til intervjukandidater i forbindelse med oppgaveskriving på masterstudiet Risiko, Sikkerhet og Sårbarhet.

- Navn på intervjukandidat:

- Funksjon i det daglige og funksjon under planlegging av øvelsen:

1. Hvilken rolle hadde din virksomhet under planleggingen av øvelsen?

A- Planverk:

1. Er Direktoratet for samfunnssikkerhet (DSB) og Nasjonal sikkerhetsmyndighet (NSM) omtalt i virksomhetens planverk?
2. Hvis ja, på hvilken måte?
3. Dersom du svarte ja på de to første spørsmålene, ble denne delen av planverket benyttet/fulgt under planleggingsfasen?

B- Planleggingsfase Øvelse IKT16:

1. På hvilket tidspunkt ble virksomhetene involvert i hverandres planleggingsarbeid?

2. Hvem tok initiativet, og hvordan ble den andre etaten involvert?

Direktoratet for samfunnssikkerhet og beredskap (DSB) og Nasjonal sikkerhetsmyndighet (NSM) er begge offentlige etater som skal ha oversikt over risiko og sårbarhet i samfunnet. DSB skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og skal sørge for god beredskap ulykkes- og krisehåndtering. NSM er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet.

3. Var de sentralene rollene direktoratene innehar gjenstand for refleksjon/diskusjon og med fokus om felles ansvar ovenfor de øvrige involverte aktørene i øvelsen?
    a. Moa -«samvirket» DSB og NSM om dette?

4. Ble det gjennomført møter bare mellom DSB og NSM?

5. Hvilke andre arenaer ble eventuelt benyttet?

6. *Projekt place ble benyttet som kommunikasjonsplattform under planlegging av øvelsen.*
   Understøttet bruken av verktøyet Project Place samvirkeprinsippet mellom DSB og NSM?
7. Samarbeidet DSB og NSM om dokumentproduksjon?

8. *DSB er underlagt Justis- og beredskapsdepartementet (JD). NSM er administrativt underlagt JD, og faglig underlagt Forsvarsdepartementet(FD).*

   a) Var det behov for avklaringer mot JD som felles ledelse?
   b) Skapte den faglige styringslinjen til FD utfordringer under planleggingen?