Universitetet i Stavanger

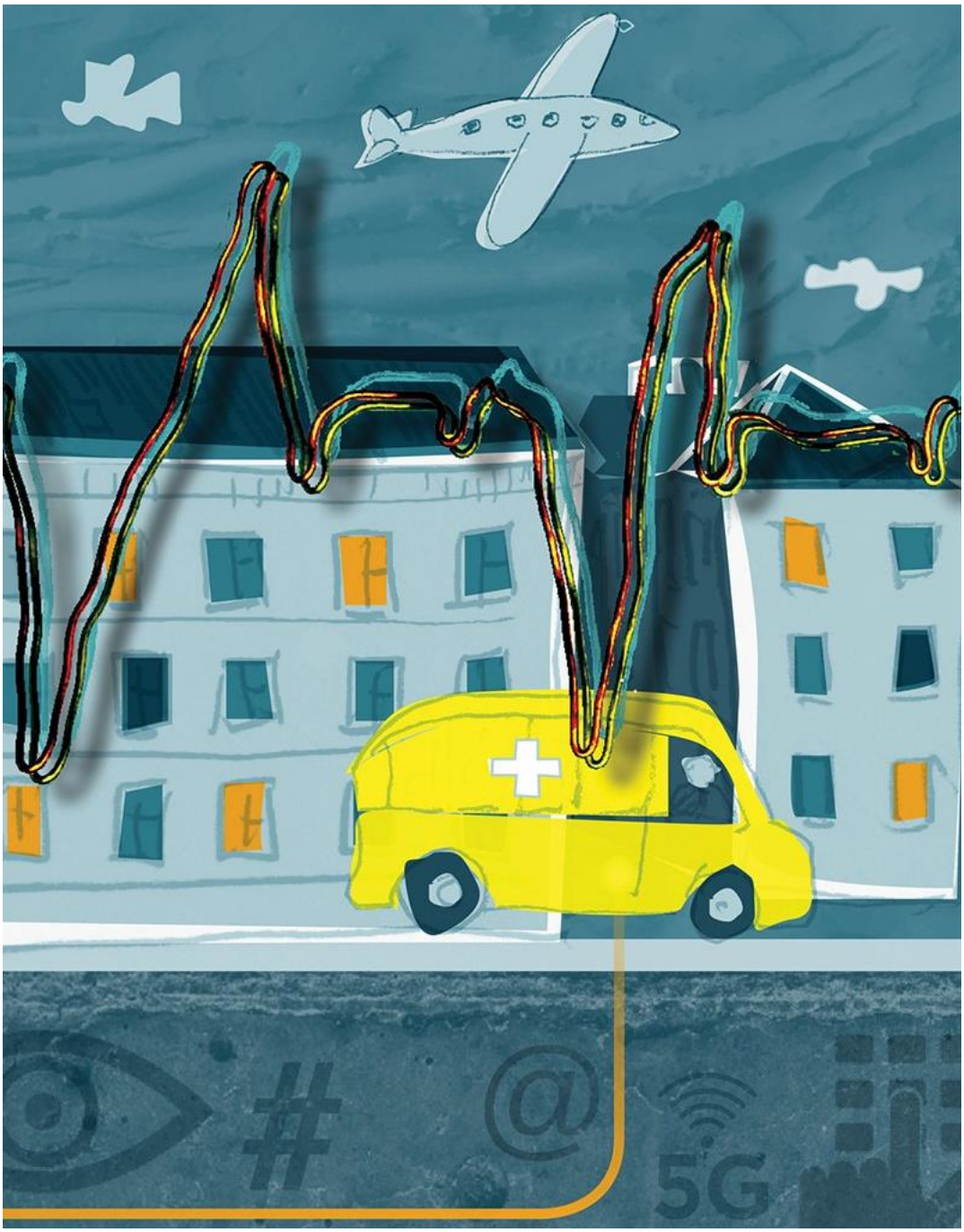
DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram: Master i samfunnssikkerhet	**Vårsemesteret 2021** Åpen
Forfattere Jo Lindberg Augestad og Nora Sande	Jo Augestad / Nora Sande
Fagansvarlig: Eivind Lars Rake **Veileder:** Eivind Lars Rake	
Tittel på masteroppgaven: «*Protect your system, Amigo*» - En studie om norske kommuners beredskapsarbeid med digital risiko **English title:** «*Protect your system, Amigo*» - A study of Norwegian municipalities' preparedness work regarding digital risk	
Emneord: Beredskap, beredskapsplanlegging, beredskapsetablering, beredskapsanalyse, sikkerhetskultur, risiko, risikopersepsjon, ROS, risikoanalyse, risikobilde, kommuner, kommunal beredskapsplikt, kommunalt beredskapsarbeid, digital risiko, digitalisering, digital sikkerhet, sårbarhet	**Sidetall: 94** **+ vedlegg/annet: 119** Stavanger, 14. juni 2021

«*Protect your system, Amigo*»

En studie om norske kommuners beredskapsarbeid med digital risiko



Illustrasjon hentet fra Kommunal- og moderniseringsdepartementet (2021, s. 148).

Masteroppgave i Samfunnssikkerhet

Universitetet i Stavanger

Vår 2021

Innholdsfortegnelse

Sammendrag

Til tross for at arbeidet med digital sikkerhet startet tidlig i Norge, er det tydelig at digitaliseringen har skapt både endringer og utfordringer i offentlige institusjoners risikobilde. Dette gjelder også lokalforvaltningen, der mange tjenester og systemer som brukes daglig har blitt digitalisert. Dette stiller nye krav til kommunene. Utgangspunktet for studien var en hypotese om at kommuner er sterke på mange beredskapsområder, men at den digitale risikoen stiller nye krav til både ROS-analyser og beredskapsarbeid. Prosjektets problemstilling var derfor «Hvordan integreres digital risiko og digitale uønskede hendelser i det kommunale beredskapsarbeidet?».

For å besvare problemstillingen, har vi sett nærmere på fire forskningsspørsmål. I det første undersøkte vi hvordan kommunene selv oppfatter eget beredskapsarbeid, sett i lys av det lovpålagte og styrende rammeverket. I det andre undersøkte vi hvordan digital risiko inngår i den kommunale arbeidsprosessen for utvikling av beredskap. I det tredje beskrev vi hvordan digital risiko og digitale uønskede hendelser blir omtalt og beskrevet i beredskapsplanen. I det fjerde diskuterte vi de mest sentrale utfordringene knyttet til å integrere digital risiko i beredskapsarbeidet. Hovedfunnene i studien viser følgende:

- Det er utfordrende å følge det lovpålagte og styrende rammeverket for kommunalt beredskapsarbeid. Mangel på tid, kompetanse og ressurser er gjennomgående utfordringer.
- Samvirkeprinsippet bør i større grad integreres i kommunenes beredskapsorganisering, for å styrke samarbeidet mellom IT- og beredskapsmiljøet.
- Kommuner bruker tilsynelatende fire virkemidler for å håndtere digital risiko.
    - Digital risiko overlates ofte til de med mest kompetanse, ofte IT-avdelingen.
    - Bruk av interkommunale IT-selskaper eller private tjenestetilbydere er utbredt.
    - Digital risiko avdekkes og bearbeides gjerne reaktivt etter hendelser inntreffer.
    - Enkelte kommuner integrerer digital risiko i ROS-analyser, men det er varierende hvor ofte dette leder til etablering av beredskap.

Oppsummert sett integreres digital risiko i det kommunale beredskapsarbeidet *i liten grad.* Det virker som at digital risiko i beredskapssammenheng er utfordrende, men også viktig og aktuelt. Dataangrepet på Østre Toten i januar 2021 har bidratt til å sette tematikken på dagsorden i kommunene.

Forord

Ved innlevering av denne masteroppgaven markeres også slutten på to x fem år som student. Først Oslo og Kristiansand, og deretter Stavanger. Det har vært et pågående kjør av skole, jobb og dårlig samvittighet - men også nye vennskap, opplevelser og mestringsfølelse. Det er sånn sett knyttet en stor grad av ambivalens til denne innleveringen.

Vi ser grunn til å takke et spesielt knippe mennesker, som har hjulpet oss med å komme gjennom både oppgaven, og studietiden generelt.

Først rettes en takk til familiene våre. Til våre mødre, Heidi og Katrine, for at dere forstått hva livet som masterstudent innebærer. Til våre fedre, Trygve og Rune, for at dere alltid har hjulpet til med de utfordringene hverdagen byr på. Og til hver av våre brødre, Oscar og Eirik, for at dere alltid har vært der som livets venn, og største inspirasjonskilde til å yte ekstra. En stor takk rettes også til samboerne våre, Albulena og Martin, for å ha stått støtt i et antall (påtvungne) diskusjoner om hvordan vi har kunnet gjøre oppgaven bedre. Dere må alle vite at jobben dere har gjort som motivatorer, humørspredere og korrekturlesere har vært uvurderlig.

En særskilt takk rettes mot de 16 informantene som bidro til datainnsamlingen. Vi håper funnene i oppgaven er lønn verdt for tiden dere tok dere til å dele erfaringene deres med oss. Deretter vil vi takke hverandre; for et samarbeid gjennom masterstudiet som, objektivt sett, ikke kunne funket bedre. Selv om vi har befunnet oss på hver vår kant av landet denne våren, har samarbeidet og vennskapet vært bunnsolid. Avslutningsvis vil vi takke veilederen vår, Eivind Rake, for all tid og energi du har brukt på oss gjennom halvåret. Hjelpen din har vært enestående, og vi er evig takknemlige for å ha fått mulighet til å lære av deg.

Vi håper oppgaven vår kan være en liten påminnelse, for både oss selv og andre, om at man aldri vil bli ferdig utlært i det man holder på med. Det er i hvert fall noe vi tar med oss videre.

Stavanger, UiS, og studietiden generelt – takk for denne gang! Nå styres skuta inn mot Oslo, der en ny arbeidshverdag innen cybersikkerhet venter på oss begge.

Jo og Nora,

Stavanger, 10. juni 2021.

Liste over forkortelser

ALARP	As low as reasonably practicable
CEO-fraud	Direktørsvindel
CIM	Digitalt verktøy for beredskap og krisehåndtering
DDoS	Distributed denial of service
Digdir	Digitaliseringsdirektoratet
DSB	Direktoratet for samfunnssikkerhet og beredskap
FHI	Folkehelseinstituttet
IT	Informasjonsteknologi
IKS	Interkommunalt selskap
IKT	Informasjons- og kommunikasjonsteknologi
Kommune–CSIRT	Kommune-cyber security incident response team
KS	Kommunesektorens organisasjon
NGI	Norges geotekniske institutt
NorSIS	Norsk senter for informasjonssikring
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet
PST	Politiets sikkerhetstjeneste
ROS-analyse	Risiko- og sårbarhetsanalyse
SSB	Statistisk sentralbyrå

Liste over tabeller

Liste over figurer

1.0 Innledning

«Do remember: 'Cybersecurity is much more than an IT topic'.»
- Stéphane Nappo (2019)

De siste tiårene har nærmest alle norske kommuner tatt i bruk digitale systemer, for å oppnå fordeler som effektivisering og oversikt over store mengder data. Dette har medført store utfordringer knyttet til et helt nytt spekter av risikomomenter som kan ramme kommunene. Arbeidet med å løse disse utfordringene knyttet til den *digitale risikoen* har gått parallelt med inkorporeringen av de digitale systemene. Det synes dermed å ha foregått et digitaliseringskappløp, der målet er todelt; å ta i bruk det siste og beste av digitale verktøy på alle driftsområder i virksomheten, og samtidig sørge for at disse fungerer på en så sikker, trygg og forsvarlig måte som mulig.

Natt til lørdag 9. januar 2021 ble Østre Toten kommune utsatt for en *digital uønsket hendelse*, i form av et omfattende løsepengevirusangrep. Dataangrepet krypterte all digital informasjon i kommunen, og lammet alt fra låsesystemer og oppvarming, til brannalarmer og systemer for innkreving av eiendomsskatt. Hendelsen skjedde som følge av at noen hadde klart å ta seg inn bak brannmurene, slettet alle sikkerhetskopier og kryptert all data. Meldingen kommunens ansatte fikk opp på dataskjermene, var *"Protect your system, Amigo"* (Helgestad, 2021, 5:50). Hendelser tilsvarende den de opplevde i Østre Toten viser hvor avhengige vi har blitt av digitale verktøy, men også hvor sektorovergripende digitale hendelser kan være. Denne typen sammensatt risiko, bestående av både digitale og ikke-digitale komponenter, er noe som i større grad må integreres i beredskapsarbeidet til kommunene.

Isolert sett er digitale uønskede hendelser ofte mindre synlige og håndfaste enn de tradisjonelle, fysiske uønskede hendelsene, som flom, brann og personskade. Likevel kan det oppstå fysiske ettervirkninger som en konsekvens av en digital hendelse, og motsatt. En av hendelsene som utmerker seg i forbindelse med dette, var da en pasient ved et sykehus i Tyskland døde som følge av at de digitale systemene var nede (Hagen, 2020). Tilsvarende kan et lynnedslag kutte telefonlinjer og tilgangen til Internett, og påvirke samfunnets varslingssystemer. Digitale uønskede hendelser kan med andre ord ikke lenger sees isolert, eller kun håndteres i en IT-avdeling. De må sees i sammenheng med alle de andre risikoene som undersøkes. Da er det essensielt at rammeverkene, verktøyene, metodene og prinsippene som brukes for å etablere beredskapen innbefatter all type risiko; både digital og fysisk.

Justis- og beredskapsdepartementet stilte følgende spørsmål på Direktoratet for samfunnssikkerhet og beredskaps (DSB) webinar, Digital Sikkerhet 2020: *«Er det noen forskjell på håndteringen av digitale hendelser versus andre typer kriser?»*. I prinsippet ikke, ifølge Justis- og beredskapsdepartementet (Aker, 2020, 14:45). For å lykkes på disse områdene forutsetter det gode beredskapsplaner som er basert på grundige risiko- og sårbarhetsanalyser. Dekker de klassiske risiko- og sårbarhetsanalysene (ROS-analyse) som gjennomføres i kommuner, den reelle risikoen som foreligger i den digitale sfæren av virksomheten? Eller er fokuset fortsatt rettet mot de mer velkjente og fysiske risikoene som brann, flom og jordskred?

Denne studien tar sikte på å utforske hvordan kommuner evner å inkludere digital risiko i det eksisterende beredskapsarbeidet. Risikobildet betegnes ofte som dynamisk og raskt endrende - noe digitaliseringen bidrar til (Nasjonal Sikkerhetsmyndighet [NSM], 2020). Det stilles både forventninger og krav til håndtering av risikobildet, der noen av disse er formulert i både lover og forskrifter. Et helhetlig arbeid med risiko krever imidlertid mer enn som så. Det krever interesse, oppmerksomhet, kompetanse og vilje. Er det tilstrekkelig fokus på dette i norsk kommunal sektor?

1.1 Problemstilling og forskningsspørsmål

Beredskap og digital sikkerhet blir ofte behandlet som to separate fagdisipliner. Med formål om å kunne se disse to i sammenheng, er studiens problemstilling følgende:

> ***Hvordan integreres digital risiko og digitale uønskede hendelser i det kommunale beredskapsarbeidet?***

Med *integreres* menes hvordan den kommunale beredskapen håndterer, og tar hensyn til, risikoen for at det oppstår en hendelse i et digitalt system som får konsekvenser for digitale og/eller fysiske verdier. Denne risikoen vil videre refereres til som *digital risiko*, mens en slik uønsket hendelse vil refereres til som *digital uønsket hendelse*.

Problemstillingen vil besvares ved hjelp av fire forskningsspørsmål, som skal veilede arbeidet med teori, datainnsamling, analyse og diskusjon. De fire forskningsspørsmålene dekker sentrale momenter som må utredes og drøftes, før problemstillingen kan besvares i sin helhet. I det første spørsmålet vil vi forsøke å sammenligne hvordan kommunene oppfatter eget beredskapsarbeid, sett i sammenheng med det lovpålagte og styrende rammeverket for kommunalt beredskapsarbeid, som vi vil gå gjennom i kapittel 3. Spørsmålet er følgende:

1. *Hvordan oppfatter kommunene sitt beredskapsarbeid i forhold til det lovpålagte og styrende rammeverket?*

Deretter vil vi se nærmere på hvordan den digitale risikoen blir tatt hensyn til i den metodikken kommunene bruker for å etablere beredskapen. Følgende forskningsspørsmål vil besvares:

2. *Hvordan inngår digital risiko i den kommunale arbeidsprosessen for utvikling av beredskap?*

Etter å ha sett på hvordan kommunene gjør det, vil vi diskutere hvordan digitale uønskede hendelser og digital risiko kan uttrykkes og beskrives. Spørsmålet besvares med utgangspunkt i informantenes oppfatning av hvordan det gjøres i dag. Spørsmålet lyder:

3. *Hvordan beskrives digitale uønskede hendelser i beredskapsplanverket?*

Som en oppsummering av de tre foregående spørsmålene, vil vi sammenfatte de utfordringene vi har sett som mest fremtredende. Svarene her vil kunne hjelpe med å se veien videre for å utvikle det kommunale beredskapsarbeidet til å passe inn i den digitale tidsalderen. Formuleringen av det fjerde forskningsspørsmålet er dermed som følger:

4. *Hvilke utfordringer opplever kommunene i beredskapsarbeidet for å håndtere digitale uønskede hendelser?*

1.2 Avgrensning

For å tydeliggjøre prosjektets formål er det nødvendig å avgrense temaet.

I prosjektet forholder vi oss til begrepet digital sikkerhet, ikke informasjonssikkerhet. Grunnen til dette er fordi digital sikkerhet knytter seg opp mot mange systemer, både digitale og ikke-digitale, som må inkluderes i sikkerhetsarbeidet. Vi kommer nærmere inn på definisjonene av, og herunder skillet mellom, informasjonssikkerhet og digital sikkerhet i kapittel 2.2.2.

Vi skiller heller ikke mellom tilsiktede og utilsiktede hendelser. Dette fordi vi er av den oppfatning at konsekvensene er viktigere enn årsakene når det kommer til å vurdere alvorligheten av en risikokilde.

Gjennom prosjektet har vi ikke intervjuet fylkeskommunene som kommunene i utvalget vårt hører til. Vi har heller ikke snakket med faginstanser som DSB, NSM, Digitaliseringsdirektoratet (Digdir) eller lignende, for å få deres mening om hvordan

kommunalt beredskapsarbeid har klart å henge med i digitaliseringen. Prosjektet avgrenses også til å ikke sammenligne funn fra våre kommuner med kommuner i andre land enn Norge. Disse beslutningene ble tatt av hensyn til prosjektets omfang.

Avslutningsvis avgrenses prosjektet til ikke å se på store internasjonale IKT-selskaper, og hva slags rolle de spiller i kommunal digital sikkerhet, hva gjelder definisjonsmakt og påvirkning. Dette kunne vært relevant, da enkelte aktører leverer IKT-tjenester til mange kommuner. Hvis dette hadde blitt inkludert kunne vi undersøkt hva slags risiko som følger inkorporeringen av enkelte digitale systemer. Dette er imidlertid valgt bort på grunn av prosjektets omfang.

1.3 Faglig relevans

Det nasjonale samfunnssikkerhetsprinsippet *nærhet* tufter på en idé om at virksomheten som står en risiko nærmest, har mest kompetanse om omgivelsene rundt, og dermed best forutsetning for å håndtere den. Ettersom kommuner står overfor ulike risikobilder, som vi vil se nærmere eksempler på i kapittel 2.1.1 Kommune-Norge, er det mest effektivt og hensiktsmessig at beredskapsarbeidet er tilpasset disse lokale omstendighetene. Dette prinsippet gir kommunene en avgjørende rolle i norsk samfunnssikkerhet. Et prosjekt som ser nærmere på kommuners beredskapsarbeid kan derfor argumenteres for å ha sterk faglig relevans til en masterstudie innenfor samfunnssikkerhet.

Med et moderne industrielt samfunn følger et komplekst og dynamisk risikobilde. Virksomheter er blant annet kritisk avhengig av strøm og nettilgang, og dermed også samarbeid på tvers av fagområder, for å klare å opprettholde de tjenestene de har ansvar for. Digital saksbehandling i kommunen er et eksempel på dette: uten strøm- eller nettilgang vil de ha store problemer med å få tilgang til sine systemer og arkiver. Uten tilstrekkelig samarbeid med leverandøren av IKT-løsningen virksomheten benytter seg av, vil de sannsynligvis få store problemer med å løse hendelser. For å imøtekomme dette risikobildet, er det viktig å etablere beredskap for digitale uønskede hendelser. Vi antar at kommuner har omfattende kunnskap og erfaringer med beredskapsarbeid og risikostyring fordi dette er lovpålagt i krav og forskrifter, og fordi de har arbeidet med dette lenge. Utgangspunktet for studien er at digitaliseringen fører til noen utfordringer knyttet til beredskapsarbeid og risikostyring (Justis- og beredskapsdepartementet, 2021). Vi mener derfor at en studie av hvordan digital risiko blir tatt hensyn til i praksis er av stor faglig relevans for samfunnssikkerhetsfeltet.

Som nevnt forsøker studien å sette søkelyset på to fagfelt som ofte behandles individuelt. Det er ingen tvil om at det kreves spesialiserte fagmiljøer innenfor både samfunnssikkerhet og digital sikkerhet, men dette kan ikke utelukke den gjensidige avhengigheten mellom de to fagfeltene. Studien forsøker derfor å ha en helhetlig og tverrfaglig tilnærming til samfunnssikkerhet og digital sikkerhet, for å belyse mulighetene som kan følge av dette.

1.4 Tidligere forskning

I prosjektet er det gjennomført omfattende litteratursøk, der vi ikke har lyktes med å finne tidligere forskning som sier noe om hvordan kommuner integrerer digital risiko i beredskapsarbeidet. Dette kompliseres ytterligere av at litteratur om digital risiko raskt blir utdatert. For å få nok oppdatert stoff om temaene, har vi inkludert bidrag fra både forskningsinstitutt og offentlige rapporter og undersøkelser. Her er det samlet inn artikler om henholdsvis digital sikkerhet, og kommunal beredskap. Dette er gjort for å gi mer innsikt i hva som tidligere har blitt sagt om de to områdene, til tross for at de ikke er sett under ett. Det blir dermed vår oppgave å veve de to fagområdene sammen i dette forskningsprosjektet.

I rapporten *Analyser av krisescenarioer* beskriver DSB (2019) risikoområdet "digitale angrep". Her legges det vekt på at digitale verdikjeder er komplekse og uoversiktlige. I tillegg påpekes det at flyktigheten i det digitale markedet er høy, noe som forklares med at leverandører byttes ut, selskaper kjøpes opp, ny teknologi oppstår og gammel byttes raskt ut (DSB, 2019). Dette skaper ytterligere kompleksitet i risikobildet. Videre analyserer DSB to krisescenarioer, som tar for seg digitale angrep mot henholdsvis finansiell infrastruktur og ekom-infrastruktur (red.anm. elektronisk kommunikasjon). Sistnevnte analyse trekker frem konsekvenser for kommunens kommunikasjonsevne. DSB gjennomførte en lignende analyse i 2014, og påpekte da at krisekommunikasjonsverktøyet CIM, avløp-, renovasjon- og vannforsyningen, primærhelsetjenesten, og koordinering mellom nødetater kunne settes ut av spill. Derfor understrekte DSB blant annet at virksomheter *må* stille spørsmål ved egen beredskap, og hvorvidt den er god nok til å håndtere en digital hendelse (DSB, 2014a).

Norge har flere nasjonale strategier for hvordan man skal håndtere digitaliseringen, som også blir relevant å se på i denne sammenheng. *Nasjonal strategi for digital sikkerhet* sier hvordan blant annet kommuner skal imøtekomme utfordringer som følger av den raske digitale

utviklingen. Ett av fem hovedfokusområder i den nyeste versjonen er økt samarbeid (Departementene, 2019a). En annen strategi som ble ferdigstilt parallelt med denne, er *Nasjonal strategi for digital sikkerhetskompetanse*. Denne sier blant annet at virksomheter har et *betydelig* forbedringsbehov, og at:

> «Norske toppledere synes det er krevende å overvåke risikolandskapet. Undersøkelsen viser kompetanseutfordringer, spesielt når det kommer til kombinasjonen mellom teknologiinnsikt, erfaring fra ledelse og risikohåndtering.» (Departementene, 2019b).

I forbindelse med å undersøke beredskapsarbeidet for digital risiko, er dette svært interessant.

På oppdrag fra Kommunesektorens Organisasjon (KS) ga SINTEF og NTNU i 2016 ut forskningsrapporten *Kommunal beredskapsplikt – gir nye krav en bedre beredskapsevne?*. Her ble kommuners evne til å forstå og oppfylle krav og forventninger fra sivilbeskyttelsesloven og forskrift om kommunal beredskapsplikt kartlagt. Selv om ikke rapporten eksplisitt nevner noe om kommunenes evne til å inkludere digital risiko i beredskapsarbeidet, er det likevel flere funn som er interessante å se på. Blant annet finner forfatterne at beredskapsarbeidet i små (<20 000 innbyggere) og mellomstore (20 000-50 000 innbyggere) kommuner dels er personavhengig, ettersom det ofte er driftet på initiativ fra "ildsjeler" i kommunen som påtar seg mer ansvar enn som egentlig kan forventes. Denne personavhengigheten gjør kontinuiteten i beredskapsarbeidet sårbar. Rapporten ser også behovet for flere tiltak for å styrke kommunenes evne til å oppfylle den kommunale beredskapsplikten. Blant annet pekes det på behov for tydeligere kommunikasjon rundt hva som forventes av kommunene, mer (eller omprioritering av) ressurser for å styrke beredskapsarbeidet, kompetanseheving og mer samarbeid, samt flere lokale øvelser som utfordrer samvirket i kommunen. Hovedfunnet i rapporten er at kommunenes evne og forvaltningsmessige handlingsrom bør styrkes for å kunne ivareta eget ansvar for beredskapsarbeidet (SINTEF, 2016).

Avslutningsvis kan Anne Marit Staurheims masteroppgave fra Universitetet i Stavanger nevnes. Staurheim så blant annet på hvor god beredskap tre fylkeskommuner har for å håndtere en uønsket hendelse som går utover IT-sikkerheten (Staurheim, 2013). Funnene tilsa at gjennomføringen av ROS-analysene i stor grad virket tilfeldig og lite systematisert når det kom til digital risiko. Utvalget til prosjektet, som bestod av rådmenn, IT-sjefer og IT-medarbeidere, virket også svært usikre rundt oppbyggingen og innholdet av beredskapsplanen på IKT. Det var heller ingen av fylkeskommunene som arrangerte IKT-relaterte øvelser regelmessig. Selv

om oppgaven er fra 2013, og dermed antakeligvis er nokså utdatert i lys av den digitale utviklingen, er funnene interessante i en nyere studie om et lignende tema.

1.5 Oppgavens struktur

Oppgaven er delt inn i åtte kapitler. I det første kapittelet har prosjektet og dets faglige relevans blitt presentert.

I kapittel to gjennomgås konteksten for oppgaven, herunder kommuner og deres ansvar og oppgaver, og den digitale tidsalderen. I kapittel tre går vi gjennom det lovpålagte rammeverket for beredskapsarbeidet i kommuner. Her ser vi på sivilbeskyttelsesloven, forskrift om kommunal beredskapsplikt, relevante veiledere, samt samfunnssikkerhetsprinsippene.

Kapittel fire presenterer oppgavens teoretiske forankring. Hovedfokuset her er risikoforståelse og -analyse, beredskapsetablering, kriterier for "god" beredskap og organisasjonskultur. I sistnevnte står sikkerhetskultur og risikopersepsjon sentralt.

I kapittel fem redegjøres det for de metodiske valgene som er gjort underveis i studien. Her drøftes også studiens kvalitet i lys av validitet, reliabilitet og etterprøvbarhet.

I kapittel seks analyseres datamaterialet fra 16 intervju og ti tilsynsrapporter. I kapittel syv følger en diskusjon av oppgavens forskningsspørsmål, der de empiriske funnene ses i sammenheng med teorien.

I kapittel åtte avrundes oppgaven ved å oppsummere hovedfunnene, for deretter å presentere problemstillingens konklusjon. Oppgaven avsluttes med våre anbefalinger til kommunene, samt våre forslag til videre forskning.

2.0 Kontekst

Formålet med dette kapittelet er å gi en innføring i konteksten rundt kommuners beredskapsarbeid. Vi vil først presentere fakta om kommuner, herunder forskjeller i kommune-Norge, kommuners forvaltningsoppgaver og beredskapsarbeid. Deretter vil vi redegjøre for hva vi mener med digitalisering og digital sikkerhet. Avslutningsvis vil vi liste opp et utvalg av relevante aktører i forbindelse med kommuners arbeid med digital sikkerhet.

2.1 Kommuner

Med formål om å utdype arbeidsområdene til kommunene, belyser statsviteren Dag Ingvar Jacobsen fire perspektiver på norske kommuner. De fire beskriver kommunen som et territorium, en tjenesteyter, en del av nasjonalstaten og en politisk arena og administrativ ledelse (Jacobsen, 2009). Alle disse områdene er med på å illustrere kommunens rolle og posisjon. Kommunene har mange rammebetingelser som settes av de statlige myndighetene, men grunntanken bak å ha et politisk styrt forvaltningsorgan på lokalt nivå kan sies å være at offentlige tilbud og tjenester skal tilpasses og prioriteres etter lokale forhold og behov. Dette kan sees i sammenheng med nærhetsprinsippet, som vi går nærmere inn på i kapittel 3.4. Organiseringen med kommuner kan med andre ord forstås som en desentralisering av beslutningsmyndighet og makt.

Kommuneloven legger de nødvendige rammene for kommunenes selvstyre (Kommuneloven, 2018, § 1). Det er spesielt to momenter i denne loven som kan øke forståelsen av kommunens autonomi og rolle i den nasjonale forvaltningen. For det første fastslår loven det kommunale selvstyret, og understreker at en kommune er et eget rettssubjekt, og at begrensninger i det kommunale selvstyret må gjøres i lov eller forskrift. For det andre gir loven noen prinsipper for nasjonale myndigheters forhold til det kommunale selvstyret. I dette ligger at det kommunale selvstyret ikke skal begrenses mer enn det som er nødvendig for å nå nasjonale mål. I tillegg påpekes det at offentlige oppgaver bør tillegges det forvaltningsorganet som er nærmest innbyggerne (Kommuneloven, 2018, § 2-2).

2.1.1 Kommune-Norge

Per 1. januar 2020 bestod Norge av 356 kommuner (Kartverket, 2021). I et land som Norge, som strekker seg omtrent 180 mil fra sør til nord, har 2 500 mil kystlinje, utallige bukter, fjorder, fjell og daler, og en befolkning på om lag fem millioner, er det store variasjoner mellom

kommunene (Jacobsen 2009, s. 21). De varierer i både innbyggertall og geografi, areal og befolkningstetthet, men også i næringsvirksomhet og produksjon. Alle disse forholdene påvirker kultur, normer, verdier og økonomi, og gjør det således utfordrende å sammenligne kommunene. Forholdene gir kommunene ulike forutsetninger for å "lykkes". Dette gjør at forklaringen på hvorfor noe er på en konkret måte i én kommune, sannsynligvis vil ha en helt annen forklaring i en annen.

Variasjonene mellom kommunene er særs relevant sett i sammenheng med beredskapsarbeid. Ettersom kommuner er preget av ulikt antall innbyggere, ulik geografi, ulik industri og ulikt klima får de følgelig svært forskjellige risikobilder. Dette medfører også at kommuner har ulike tilnærminger til risikohåndtering og beredskapsarbeid. Eksempelvis er det nærliggende å anta at Stavanger, som er en oljekommune langs kysten, tilnærmer seg beredskap på en helt annen måte enn Åmot kommune, som er en innlandskommune med mye militær aktivitet.

2.1.2 Kommunens oppgaver

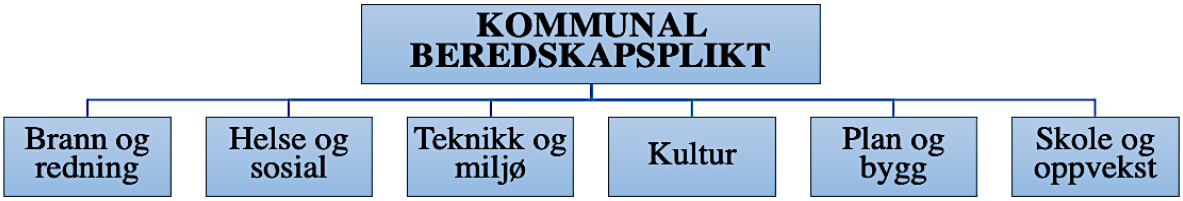
Kommunen er en del av det tredelte forvaltningshierarkiet med staten som øverste ledd, fylkeskommunen som mellomledd, og kommunen som nederste ledd. Som innbyggernes nærmeste forvaltningsorgan er kommunen lovpålagt å ivareta flere viktige arbeidsoppgaver og ansvarsområder. Disse oppgavene kan deles i tre:

- Tjenesteytende funksjoner (eks. utdannelse, helse, oppvekst, tekniske tjenester).
- Forvaltningsoppgaver (eks. behandling av byggesaker, sosialstøtte, bevillinger).
- Samfunnsutvikling (eks. næringsutvikling, byplanlegging og -utvikling).

(Christensen, Egeberg, Lægreid og Aars 2014, s. 145). I tillegg står kommuner fritt til å påta seg frivillige oppgaver og ansvarsområder. Med denne bredden av oppgaver er de lokale folkevalgte politikerne sterkt presset når det kommer til å prioritere oppgaver og ta hensyn til innbyggernes behov. En av oppgavene som *må* prioriteres, er det kommunale beredskapsarbeidet.

2.1.3 Kommunalt beredskapsarbeid

Kommunenes plikt til å ta hensyn til sikkerhetsmessige utfordringer i lokalsamfunnet, kalles for den kommunale beredskapsplikten (DSB, 2014b). Modellen under viser hvordan denne plikten skal dekke alle områdene i kommunen.



Figur 2.1: Kommunal beredskapsplikt. (Tilpasset etter modell i Veileder til helhetlig ROS-analyse i kommunen (DSB, 2014b, s. 14)

Kommunens beredskapsarbeid reguleres gjennom forskrift om kommunal beredskapsplikt. Kvalitetskravene til disse lovpålagte arbeidsoppgavene er hovedsakelig gitt i rettslige standarder, noe som bidrar til at dette arbeidet gjennomføres med ulik kvalitet og omfang. Forskriften gir føringer for hva ROS-analysene skal innebære, hvor ofte de skal gjennomføres, samt krav til hvordan oppdatering og revisjon, samarbeid mellom kommuner, øvelser, opplæring og dokumentasjon skal gjennomføres (Forskrift om kommunal beredskapsplikt, 2011). Forskriften vil bli gjennomgått, paragraf for paragraf, i kapittel 3.2 Forskrift om kommunal beredskapsplikt.

DSBs Kommuneundersøkelser gir de mest oppdaterte statusrapportene for hvordan det står til med sikkerhet- og beredskapsarbeidet i norske kommuner. Tallene fra 2021 reflekterer kommunenes beredskapsarbeid i 2020. Det største forbedringspotensialet ligger i å ha oppdaterte analyser og planverk. Blant annet sier 97 % at de har en overordnet beredskapsplan, men kun 53 % reviderte den i 2020. 97 % sier de har gjennomført helhetlige ROS-analyser, der 70 % har gjennomført det de siste fire årene. 84 % hadde gjennomført øvelser i egen beredskapsorganisasjon de siste to årene (DSB, 2021). Disse tallene belyser hvor aktivt kommuner jobber med beredskapsplanverket. Kvaliteten på arbeidet kan sies å variere litt. 47 % av kommunene oppfyller minimumskravene til beredskapsplanen, og 66 % oppfyller minimumskravene til ROS-analysen. Disse kravene kommer vi nærmere inn på i kapittel 3.0 Lovpålagt og styrende rammeverk. Det må imidlertid påpekes at tallene i undersøkelsen sannsynligvis er påvirket av covid-19-pandemien.

2.2 Den digitale tidsalderen

I dette delkapittelet vil vi redegjøre for metodikk, begreper og utfordringer knyttet til digital sikkerhet, for å bygge en forståelse av hvordan digital risiko både kan sammenstilles og differensieres fra andre typer risikoer.

Den digitale utviklingen har skjedd svært raskt, og har vært stadig mer utbredt de siste ti årene. I Norge har denne utviklingen vært enda mer omfattende enn i mange andre land, noe som har resultert i at Norge, sammen med Sverige, er verdens mest digitaliserte land (NOU, 2018:14). I tillegg til dette, har også Norge vært et foregangsland når det kommer til sikkerhetsarbeid på området. I 2003 ble Norge et av de første landene i verden til å lansere en nasjonal strategi for digital sikkerhet (Departementene, 2019a). Likevel påvirker digitaliseringen fortsatt risikobildet i stor grad. Etterretningstjenesten og Nasjonal Sikkerhetsmyndighet trekker frem digitale ondsinnede operasjoner for å være en betydelig risiko for offentlige virksomheter (Etterretningstjenesten, 2021; NSM, 2021). Tilsvarende trekker Norsk senter for informasjonssikring (NorSIS) og Kommune-CSIRT frem digitale trusler som en stor risiko for norske kommuner (NorSIS, 2021; Kommune-CSIRT, 2021). Det kan likevel være utfordrende å forstå hva slags hendelser, og følgelig hva slags konsekvenser, digital risiko kan innebære.

Den digitale sfæren er ikke uløselig separert fra fysiske systemer, og derfor er det viktig med en forståelse av hvordan digital sikkerhet står i sammenheng med øvrig sikkerhetsarbeid. En av grunnene til at digitale systemer ikke kan separeres fra fysiske systemer handler om det finnes mange gråsoner, der fysiske og digitale komponenter utgjør ett og samme system. Nødnett, som får radiotilgang via signaler som går mellom fysiske radioterminaler og basestasjoner, er et eksempel på dette. Uten det digitale oppsettet vil ikke basestasjonene ha noen funksjon, og uten basestasjonene vil ikke Nødnett fungere. Her er altså systemet avhengig av både digitale og fysiske komponenter. Et annet eksempel er moderne og teknologiske brannvarslingsanlegg. Teknologien i et slikt anlegg kan innebære seriekobling, meldingsvarsling til beboere, varsling til brannvesen, styring av dører og fjernstyring av vifter. I tillegg vil dette anlegget bestå av mer mekaniske komponenter som sprinkelanlegg, vifter, branndører og lignende. Det er ett og samme system, der svikt i enten de digitale eller mekaniske komponentene påvirker systemet som helhet. Det er dermed utfordrende å tegne et skille mellom digital og fysisk risiko når hele systemet skal risikovurderes. Denne tankegangen kan trekkes til større systemer, og illustrerer viktigheten av en helhetlig og samlet tilnærming til risiko og beredskap. Et svært aktuelt eksempel er dataangrepet på Colonial Pipeline, 6. mai i år. Selskapet leverer nesten halvparten av drivstoffet til USAs østkyst. Som direkte følge av dataangrepet ble oljeledningen satt ut av drift, som medførte at over halvparten av bensinstasjonene i Atlanta og North-Carolina var tomme for drivstoff. Selskapet endte opp med å betale 40 millioner kroner i løsepenger (Thommesen, 2021).

2.2.1 Digitalisering og digitale systemer

Det kreves en avgrensning for å kunne definere et digitalt system, særlig om målet er å få oversikt over egne digitale systemer. For å kunne kartlegge risikoer og sårbarheter i eget system er det kritisk å forstå hvor systemet "starter" og "stopper". Denne avgrensingen kompliseres ytterligere når systemet er koblet opp mot Internett. Bergsjø mfl. gir en generell definisjon av informasjonssystemer, som også brukes synonymt med digitale systemer: *«et informasjonssystem defineres som maskinvare, programvare og tilknyttede tjenester»* (Bergsjø mfl., 2020, s. 19).

Vi forstår digitalisering som en prosess der noe, eller noen, i større eller mindre grad tar i bruk, og blir mer avhengig av, informasjons- og kommunikasjonsteknologi (IKT). Mange prosesser som før var basert på arbeidskraft og papirarbeid har i dag blitt delvis eller helt flyttet over til digitale plattformer. I de fleste tilfeller har ikke arbeidskraften blitt digital, men heller verktøyene som en arbeidstaker bruker til å utføre arbeidsoppgaver. Et eksempel på dette er saksbehandlere som tidligere drev med papirarbeid, men nå jobber via datamaskiner.

Ofte er et av hovedformålene med digitalisering å gjøre livet vårt enklere. Digitalisering skal gjerne effektivisere, automatisere og forenkle oppgaver som tidligere har vært ressurs- og tidkrevende. Denne prosessen krever imidlertid store mengder data om nærmest alt vi gjør, som må måles og registreres. Denne dataen legger følgelig til rette for å analysere og tilpasse teknologien til våre behov og bruksområder. I denne prosessen ligger det mange sårbarheter, særlig relatert til at dataen kan misbrukes og anvendes til helt andre formål enn det som var tiltenkt (Bergsjø mfl., 2020). Et tenkt eksempel kan være om en ondsinnet aktør får tilgang til store mengder helseopplysninger om en stor folkegruppe. Denne informasjonen kan selges videre til farmasøytiske selskaper, som da får inngående informasjon om behovet for deres medisiner. Dette kan legge grunnlaget for utpressing ved å true med å redusere tilbudet, eller å øke prisene.

2.2.2 Digital sikkerhetsforståelse

Når digital sikkerhet skal defineres er det nødvendig å avklare hva som skal sikres. Et nødvendig skille må derfor gjøres mellom hvorvidt det er systemet i seg selv, eller innholdet i systemet (informasjonen), som skal sikres. I den forstand kan vi trekke et skille mellom *digital sikkerhet* og *informasjonssikkerhet.* Selv om vi forholder oss til IKT-systemer og

informasjonssystemer som synonymer, er ikke digital sikkerhet og informasjonssikkerhet det samme.

Både Departementene (2019a, s. 6) og Meld. St. nr. 5 (2020-2021) definerer digital sikkerhet som «*(...) beskyttelse av 'alt' som er sårbart fordi det er koblet til, eller på annen måte avhengig av, informasjons- og kommunikasjonsteknologi*». Begrepet brukes her synonymt med IKT-sikkerhet og cybersikkerhet. Bergsjø mfl. (2020) bruker også begrepet datasikkerhet om det samme fenomenet. Hva gjelder begrepene IT (informasjonsteknologi) og IKT, er IKT en utvidelse av begrepet IT. I dagligtalen brukes disse begrepene gjerne om hverandre, men vi forholder oss til IT som en fagdisiplin, mens IKT forstås i henhold til definisjonen av informasjonssystemer i kapittel 2.1.1. Eksempelvis jobbet IT-informantene i utvalget med IKT.

Ifølge Digdir handler informasjonssikkerhet om å sikre behandlingen av informasjonen som inngår i visse tjenester (Digdir, u.å.). Et eksempel kan være informasjonen en barnehage har om barna som går der, eller sykdomshistorien en fastlege har om en pasient. Informasjonssikkerhet har derfor tre sikkerhetsmål: konfidensialitet, integritet og tilgjengelighet. Dette betyr at informasjonen ikke skal bli kjent for uvedkommende, at informasjonen ikke står i fare for å bli endret utilsiktet, og at informasjonen er tilgjengelig ved behov. Informasjonssikkerhet og digital sikkerhet er følgelig til dels gjensidig avhengig, da digital sikkerhet bidrar til informasjonssikkerhet (Bergsjø mfl., 2020, s. 18).

2.3 Aktører innen digital sikkerhet i kommunen

En rekke aktører er involvert i det kommunale sikkerhetsarbeidet. Denne delen vil gjøre rede for noen av de aktørene som samarbeider med, eller gir støtte til, kommunene hva gjelder digital sikkerhet, beredskap og hendelses-/krisehåndtering.

Kommunesektorens Organisasjon (KS) er kommunesektorens interesseorganisasjon, og er med på å organisere arbeidet som gjøres i kommunene. Da Østre Toten kommune ble utsatt for løsepengevirusangrepet tidligere i år, sendte KS ut et brev til alle landets kommuner med en rekke råd og anbefalinger for hvordan håndtere trusler i det digitale rom (KS, 2021). KS har også et eget rådgivende organ innen digitalisering og smart bruk av teknologi, kalt KommIT (KS, 2020).

Nasjonal Sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikring, og det nasjonale fagmiljøet for IKT-sikkerhet. NSM spiller en viktig rolle i håndteringen av digitale hendelser i kommunen, da NSM er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser (NSM, u.å.).

Datatilsynet er både tilsyn og ombud. De skal føre kontroll med at personvernregelverket etterleves, og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av personopplysninger som kan knyttes til dem. I tillegg til å gi bøter for brudd på personvernregelverket, tilbyr de rådgivning og kompetansebygging (Datatilsynet, u.å.).

Kommune – CSIRT ble opprettet i januar 2020, og har som formål å støtte kommuner og fylkeskommuner med relevant informasjon om trusler, hendelser og sårbarheter i det digitale rommet. I tillegg skal kommune-CSIRT være et nasjonalt ressurssenter for praktisk rådgivning og støtte ved cyberhendelser og andre digitale utfordringer i kommunene. Kommune-CSIRT er et interkommunalt selskap (IKS) (Kommune-CSIRT, u.å.).

Direktoratet for samfunnssikkerhet og beredskap (DSB) har ansvar for nasjonal, regional og lokal sikkerhet og beredskap. Andre ansvarsområder er industri- og næringslivssikkerhet og kritisk kommunikasjonsinfrastruktur for nød- og beredskapsaktører. De tilbyr også operativ støtte under kriser innenfor samordning, forsterkning og faglig rådgivning (DSB, u.å.). I tillegg publiserer de en rekke veiledere og rapporter knyttet til blant annet beredskapsarbeid, ROS-analyser og gjennomføring av trening og øvelser. Eksempelvis kan kommuner benytte seg av *Veileder for Helhetlig ROS-analyse* i det kommunale beredskapsarbeidet.

Digitaliseringsdirektoratet (Digdir) skal være regjeringens fremste verktøy for en raskere og mer samordnet digitalisering av samfunnet. Digdir jobber blant annet med forebyggende informasjonssikkerhet i offentlig sektor, å utvikle digitale tjenester for innbyggere, kommuner og næringsliv, samt tilsyn for universell utforming av IKT (Digitaliseringsdirektoratet, u.å.).

3.0 Lovpålagt og styrende rammeverk

For å forstå rammeverket for det kommunale beredskapsarbeidet, har vi valgt å presentere relevante lover, forskrifter og styrende prinsipper i et eget kapittel. Kapittelet er også ment å gi en forståelse for hvorfor digital risiko bør sees i sammenheng med det overordnede beredskapsarbeidet i kommunen. Hensikten er ikke å presentere en uttømmende liste over alle bestemmelsene som påvirker arbeidet, da det potensielt ville tatt fokuset bort fra hensikten her; nemlig å få kjennskap til de overordnede kravene. Derfor legges hovedfokuset på sivilbeskyttelsesloven (2010) og forskrift om kommunal beredskap (2011), i tillegg til ulike veiledere og de fire nasjonale samfunnssikkerhetsprinsippene. Som vi kommer nærmere inn på tar ikke disse ressursene for seg digital risiko, med unntak av Veileder til helhetlig ROS. Digital risiko nevnes for øvrig også i samfunnssikkerhetsinstruksen (2017). Denne instruksen omtales riktignok ikke her, ettersom den er rettet mot departementenes arbeid.

3.1 Sivilbeskyttelsesloven

I §§ 14 og 15 i sivilbeskyttelsesloven kommer det frem hvilke oppgaver som følger av den kommunale beredskapsplikten. Sivilbeskyttelsesloven § 14 første ledd sier at:

> "Kommune(r) plikter å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen. Resultatet av dette arbeidet skal vurderes og sammenstilles i en helhetlig risiko- og sårbarhetsanalyse."

Det andre og tredje leddet i paragrafen sier at ROS-analysen skal legges til grunn for kommunens sikkerhet- og beredskapsarbeid. Analysen skal oppdateres i takt med endringer av kommunedelplaner eller endringer i risiko- og sårbarhetsbildet (minimum hvert fjerde år).

I sivilbeskyttelsesloven § 15 sies det videre at det med utgangspunkt i den gjennomførte ROS-analysen skal utarbeides en beredskapsplan. Denne planen skal inneholde en oversikt over forberedte tiltak kommunen har for å håndtere uønskede hendelser. Minimumskravet til innholdet i beredskapsplanen er en plan for kriseledelse, varslingslister, ressursoversikt, evakueringsplan og en plan for å gi informasjon til befolkningen og media. Paragrafen understreker også at planen skal være oppdatert, og at den skal revideres minst én gang årlig. Kommunen må også sørge for at det øves på planen jevnlig.

I § 29 sies det at det skal gjennomføres tilsyn med kommunenes oppfyllelse av §§ 14 og 15.

3.2 Forskrift om kommunal beredskapsplikt

Forskrift om kommunal beredskapsplikt (2011) har hjemmel i sivilbeskyttelsesloven, og utdyper den kommunale beredskapsplikten. Ifølge dens § 1 har forskriften blant annet som formål at «*kommunene skal jobbe systematisk og helhetlig med samfunnssikkerhetsarbeidet på tvers av sektorer i kommunen, med sikte på å redusere risiko for tap av liv eller skade på helse, miljø og materielle verdier*». Forskriftens § 2 stiller krav til å gjennomføre helhetlige ROS-analyser, med følgende minimumskrav til hva de skal omfatte:

a) Eksisterende og fremtidige risiko- og sårbarhetsfaktorer i kommunen.
b) Risiko og sårbarhet utenfor kommunens geografiske område som kan ha betydning for kommunen.
c) Hvordan ulike risiko- og sårbarhetsfaktorer kan påvirke hverandre.
d) Særlige utfordringer knyttet til kritiske samfunnsfunksjoner og tap av kritisk infrastruktur.
e) Kommunens evne til å opprettholde sin virksomhet når den utsettes for en uønsket hendelse, og evnen til å gjenoppta sin virksomhet etter at hendelsen har inntruffet.
f) Behov for befolkningsvarsling og evakuering.

(Forskrift for kommunal beredskap, 2011, § 2). Disse punktene blir avgjørende for det videre arbeidet med beredskapsplanen.

Videre i forskriften stilles det minimumskrav til beredskapsplanens innhold, oppfordring til å etablere hensiktsmessige samarbeid på tvers av kommunene, og krav om at beredskapsplanen skal være oppdatert. I minste fall skal planen revideres én gang årlig, men også i takt med revisjon av andre kommunedelplaner. Forskriften stiller også krav til at planen skal øves på annethvert år. Disse øvelsene bør evalueres for å kartlegge kommunens forbedringspotensial, og eventuelle behov for endringer. § 7 andre ledd sier også at «*kommunen skal ha et system for opplæring som sikrer at alle som er tiltenkt en rolle i kommunens krisehåndtering har tilstrekkelige kvalifikasjoner*». Av § 9 fremkommer det at kommunen skal kunne dokumentere skriftlig at forskriften er oppfylt. I § 10 henvises det til at det er Statsforvalteren som skal føre tilsyn og kontrollere om kommunene opptrer etter forskriften.

3.3 Relevante veiledere

Det finnes også en rekke veiledere som kommunene kan bruke som hjelpemiddel for å utarbeide beredskapsplanen. Veiledere er ikke juridisk bindende, da de heller er ment som en utdypning eller forklaring av en lov eller forskrift. Slike dokumenterer orienterer om departementets politikk og praksis, og er ment for et publikum med variert kompetanse om beredskap. Noen av de mest relevante veilederne for kommuners beredskapsplanlegging er

veileder til helhetlig ROS (DSB, 2014b), veileder til forskrift om kommunal beredskapsplikt (DSB, 2018), veileder til samfunnssikkerhet i kommunens arealplanlegging (DSB, 2017) og veiledning for Statsforvalterens tilsyn med kommunal beredskapsplikt (DSB, 2015).

Som nevnt innledningsvis er det kun Veileder til helhetlig ROS som nevner digitale hendelser - og da først i vedlegg nummer fem. Av 77 eksempler på uønskede hendelser som er opplistet her, er kun tre av dem digitale. Disse er *cyberangrep* og *hacking* i kategorien *"*digitale rom*"* og *langvarig utfall av telekom og IKT* i kategorien "annet" (DSB, 2014b).

3.4 Samfunnssikkerhetsprinsippene

I tillegg til lovene og forskriftene, står fire prinsipper sentralt i samfunnssikkerhet- og beredskapsarbeidet i Norge. Disse har stor innflytelse på alle beslutninger som tas, og kan beskrives som bærebjelken i den offentlige beredskapen. De fire er ansvar-, likhet-, nærhet- og samvirkeprinsippet, og er hjemlet i samfunnssikkerhetsinstruksen (2017). I det følgende vil de gjennomgås med utgangspunkt i kommunal praksis.

Likhetsprinsippet handler om at organiseringen av kommunen skal være mest mulig lik under uønskede hendelser, som under normale omstendigheter. Ansvarsprinsippet handler om at de som har ansvar for et område i en normalsituasjon, også skal ha ansvar for det samme området under en uønsket hendelse. Både likhet- og ansvarsprinsippet kan for eksempel sees i sammenheng med at det er ordføreren som vil fortsette å ha det overordnede ansvaret i en kriseledelse, under en oppstått hendelse. Nærhetsprinsippet sier at beslutningsmyndigheten skal ligge nærmest stedet hendelsen utfolder seg, for å forsøke å sikre mest mulig hurtig og effektiv respons. Dette har vi sett eksempler på i forbindelse med covid-19-pandemien, der det har vært kommuneoverlegen som har hatt ansvar for å vurdere tiltak i kommunen (Folkehelseinstituttet [FHI], 2020). Ansvar-, likhet- og nærhetsprinsippet ble introdusert i St. meld. nr. 17 (2001-2002) *Samfunnssikkerhet. Veien til et mindre sårbart samfunn* (Justis- og politidepartementet, 2002). Samvirkeprinsippet ble først presentert ti år senere, etter 22. juli 2011 (Justis- og politidepartementet, 2012). Dette prinsippet stiller krav til at aktører har et selvstendig ansvar for å sikre samarbeid med andre relevante aktører i arbeidet med beredskap og krisehåndtering.

Sammen skal disse fire prinsippene fremme blant annet oversikt, kunnskap, samarbeid og gjennomføringskraft i både det proaktive og det reaktive beredskapsarbeidet.

4.0 TEORI

De teoretiske bidragene er ment til å legge grunnlaget for analysen av hvordan digital risiko og beredskap kan forstås i sammenheng. Innledningsvis vil vi redegjøre for risiko, sårbarhet og usikkerhet. Som en forlengelse av dette vil vi belyse hvordan digital risiko kan operasjonaliseres som konsept, samt viktige momenter i risikokartlegging og -analyse. Del to av teorikapittelet tar for seg beredskapsetablering og resiliens, samt en beskrivelse av hva "god" beredskap innebærer. Del tre er mer orientert mot organisasjonskultur, der vi ser nærmere på risikopersepsjon, sikkerhetskultur og organisasjonsmodellen til Jacobsen og Thorsvik (2013).

4.1 Risiko

For å forstå hvordan kommunene velger ut hendelser de etablerer beredskapen for, er det nødvendig å se nærmere på risiko og risikoanalyser. Arbeid med risikoanalyser og -kartlegging beror på hvilken forståelse man har av risiko og sårbarhet, samt hvordan man håndterer usikkerhet. Dette ligger til grunn for alt beredskapsarbeid, og er derfor det vi ser på først.

4.1.1 Risiko, sårbarhet og usikkerhet

Det foreligger ingen entydig forståelse av risikobegrepet. Ifølge Aven, Renn og Rosa (2011) brukes risiko både som en forventet kvantitativ verdi, en sannsynlighetsdistribusjon, en usikkerhet eller en hendelse. I tidligere arbeid har Aven og Renn (2010, s. 8) beskrevet risiko som "*usikkerheten og alvorligheten av hendelser og konsekvenser av en aktivitet, med hensyn til noe mennesker verdsetter*". Med en slik definisjon får risikokonseptet flere egenskaper: den fokuserer på usikkerhet og alvorlighet fremfor sannsynlighet, og hvordan resultatet påvirker berørte interessenter. Risiko kan også forstås som et konsept for å analysere usikre konsekvenser av fremtidig utvikling og endring i samfunnet (Renn, 2008). Med denne forklaringen handler risiko i stor grad om å se inn i fremtiden, noe som både i teorien og i praksis er umulig. I den forstand skal arbeidet med risiko legge til rette for å gi den mest kvalifiserte og sannsynlige beskrivelsen av fremtidige utfall, slik at en kan tilpasse sikkerhetsarbeidet deretter. En mer praktisk definisjon av risiko gis i DSBs forslag til ny brann- og redningsvesenforskrift (DSB, 2020, § 2): "*Hvor sannsynlig det er at uønskede hendelser kan komme til å inntreffe, konsekvensene av disse og usikkerheten knyttet til disse vurderingene*". Denne definisjonen legger mer vekt på sannsynligheten for at hendelser inntreffer, i tillegg til usikkerheten knyttet til disse vurderingene. Det tas imidlertid ikke hensyn til verdier.

Risikobegrepet har altså flere egenskaper. For å fremheve disse egenskapene kan vi samle de viktigste momentene fra de tre ovennevnte definisjonene. Det er av vår forståelse at risiko er et konsept for å analysere hvor sannsynlig det er at uønskede hendelser vil inntreffe, konsekvensene av disse, og usikkerheten knyttet til disse vurderingene, med utgangspunkt i det mennesker verdsetter. Det er denne forståelsen av risiko som danner grunnlaget for oppgaven. I kapittel 4.3.1 går vi inn på risikopersepsjon, for å belyse hvordan risiko vurderes ulikt fra person til person.

Sårbarhet er nært tilknyttet risiko. I dette prosjektet er sårbarhet et viktig konsept, blant annet fordi mye av det kommunale beredskapsarbeidet forutsetter, og tufter på, gode risiko- og sårbarhetsanalyser. DSB har utviklet flere veiledere for ROS-analyser, der de i veilederen fra 2014 gjengir definisjonen fra NOU-en *Et sårbart samfunn* (2000:24): «*Sårbarhet er et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet*». Det motsatte av sårbarhet kan sies å være robusthet (Njå, Sommer, Rake og Braut, 2020, s. 52), som kan defineres som «*et systems evne til å stå imot og opprettholde sine funksjoner under ulike former for ytre påkjenninger*» (Aven, Boyesen, Njå, Olsen og Sandve, 2004, s. 124). Robusthet er også en del av begrepet resiliens, som vi kommer nærmere inn på som et mål med beredskapsarbeidet, i kapittel 4.2.

Usikkerhet er også en vesentlig størrelse i risikobegrepet (Njå mfl., 2020), og derfor også i beredskapssammenheng. Når risiko skal vurderes, er det overordnede målet å si noe om hvilke farer som foreligger i fremtiden. Ettersom fremtiden er umulig å forutse, er det viktig for analysens validitet og videre arbeid, å legge ved usikkerheten rundt kalkuleringene. Usikkerhet handler om tvil, og brukes eksempelvis som et mål på tilliten vi har til resultatene i ROS-analysen (se kapittel 4.1.3). Lipshitz & Strauss (1997) beskriver spesielt tre grunner til usikkerhet. Disse er usikkerhet som følger av mangel på informasjon, mangel på forståelse, og konflikter mellom ulike alternativer. Mangel på informasjon handler eksempelvis om tilfeller der sannsynligheten og konsekvensene til en hendelse er ukjent, fordi det er mangel på data. Mangel på forståelse handler ikke nødvendigvis om mangel på informasjon, men utfordringer knyttet til tolkning av data og motstridende informasjon. Konflikter mellom ulike alternativer handler om å ha tilstrekkelig med forståelse og kunnskap om et fenomen, men at alternativene rangeres likt. Et eksempel på sistnevnte kan være utfordringene med å bestemme hvilke grupper som skal vaksineres først mot covid-19, til tross for mye informasjon og forståelse.

Dette fordi det er usikkerhet rundt hva som gir best effekt. Hvis det er mye usikkerhet knyttet til hvor alvorlig en hendelse kan bli, bør man dimensjonere for konsekvenser som kan bli *enda mer* alvorlig enn det vurderingene tilsier.

4.1.2 Hvordan operasjonalisere risiko?

Aven, Røed og Wiencke (2017) foreslår tre overordnede risikokategorier som gjerne brukes i virksomheter. Disse tre kategoriene kan gi en tydeligere forståelse av risiko, og gjøre risiko til et mer anvendelig begrep i beredskapsarbeidet. Den første kategorien er *strategisk risiko* som viser til risiko der konsekvensene for virksomheten er knyttet til dens langsiktige strategier og planer. Den andre kategorien er *finansiell risiko* som viser til risiko der konsekvensene for virksomheten er knyttet til dens økonomiske situasjon. Den tredje kategorien er *operasjonell risiko* som viser til at konsekvensene for virksomheten er knyttet til forhold som påvirker den normale driftsituasjonen (Aven mfl., 2017).

Disse tre kategoriene er ikke et alternativ til de ulike forståelsene av risiko, men heller et supplement. Det vil si at disse tre kategoriene kan undersøkes ved hjelp av både statistiske og empiriske data, samt mer subjektive og kvalitative vurderinger. Hva som er mest fordelaktig vil variere ut fra blant annet mengden tilgjengelig informasjon, fagområde og kontekst. Vi antar at operasjonell risiko går best overens med digital risiko, fordi uregelmessigheter i de digitale systemene ofte kan føre til avvik fra normal driftssituasjon.

4.1.3 Risikoanalyser og kartlegging av risiko

Etter et større fokus på risikostyring i petroleumsindustrien på 90-tallet, begynte dette fokuset etter hvert å smitte over til andre sektorer - deriblant til kommunen (Njå mfl., 2020, s. 23). Risikobasert styring er styring som bygger på kunnskap om risiko. Denne kunnskapen blir ofte veid opp mot andre forhold for å ta beslutninger, deriblant økonomi, beskyttelse av verdier, effektive løsninger, og lignende. I praksis er det ikke alltid sånn at beslutningen lander på alternativet med lavest risiko, til tross for at risikoen er tatt med i betraktningen. Et eksempel her kan være å digitalisere arkivene innenfor offentlig forvaltning: mens digitaliseringen vil medføre effektivitet, vil sårbarheten kunne sies å øke. Njå mfl. (2020, s. 22) mener derfor at det er riktigere å snakke om risiko*informert*, fremfor risikobasert, styring.

Dagens risikosamfunn er kjennetegnet av avansert teknologi, komplekse organisasjoner og individuelle handlinger, i omgivelser som stadig endrer seg (Njå mfl., 2020, s. 20). Ettersom

risiko er et flersidig og dynamisk fenomen, utelukkes muligheten for en standardisert evaluering og håndtering. Vi er avhengig av å analysere det kontinuerlig, etter hvert som risikobildet forandrer seg. Dette er viktig for å sørge for sikkerheten i samfunnet, og verne om verdier som blant annet liv, helse og økonomi.

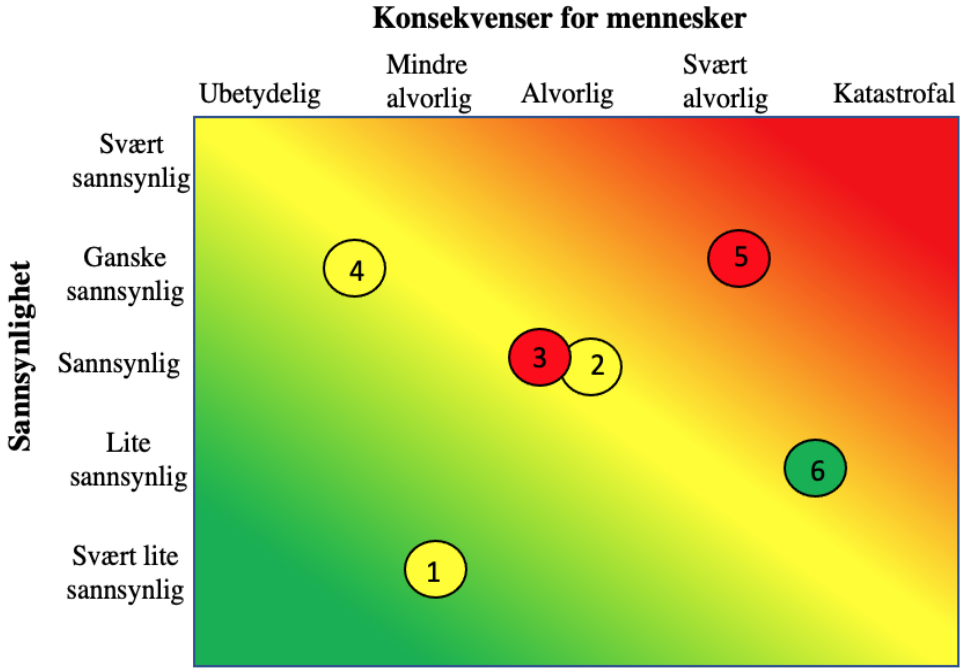
Hensikten med å gjennomføre ROS-analyser er altså å kartlegge fremtidige trusler, samt systemets evne til å håndtere dem. Ifølge Njå mfl. inneholder en "komplett" ROS-analyse:

1. Analyser av årsaker til hendelser, sannsynligheter og frekvenser av disse.
2. Analyser av konsekvenser, og tap som følge av disse hendelsene. Dette kan uttrykkes ved for eksempel tap av liv, skade på mennesker, informasjon, miljø, og økonomi.

(Njå mfl., 2020, s. 284). Som nevnt tidligere er det viktig å inkludere usikkerhet i begge punktene, samt hvilke forutsetninger man har for å gjennomføre analysene. Dette styrker analysens validitet og pålitelighet, slik at beslutningene blir bedre og mer effektive.

En ROS-analyse vil avdekke mange risikomomenter med ulik alvorlighetsgrad. En enkel og oversiktlig måte å fremstille disse risikomomentene på er gjennom trafikklysmodellen. Her kan vi kategorisere fargene på følgende måte:

- Ikke-tolerabel risiko (rød).
- Tolerabel risiko (gul).
- Akseptabel risiko (grønn).



Figur 4.1: Trafikklysmodellen (Etter inspirasjon fra Njå mfl. 2020, s. 348).

Akseptabel risiko innebærer en aktivitet eller hendelse der risikoen er så lav at risikoreduserende tiltak ikke anses som nødvendig. Det er heller de to andre vi vil gjøre noe med. *Tolerabel* risiko betyr at aktiviteten eller hendelsen innebærer en risiko som vi kan tolerere på nåværende tidspunkt, men at risikoreduserende tiltak er nødvendig. Den gule sonen kalles også for ALARP-området, som står for "as low as reasonably practicable". Målet er å få risikomomentene som ligger i den gule sonen over i den grønne. Risikomomentene som ligger i den røde sonen representerer *ikke-tolerabel* risiko, og er aktiviteter eller hendelser som krever omfattende risikoreduserende tiltak. Om dette ikke lar seg gjøre bør man vurdere å avslutte aktiviteten, eller redusere sannsynligheten for at hendelsen kan inntreffe. I denne modellen representerer også fargen på risikomomentene (1-6), usikkerheten. Den røde fargen betyr høy grad av usikkerhet, den gule symboliserer moderat grad, mens den grønne tilsier liten grad av usikkerhet. Dette betyr at selv om blant annet 2 og 3 er på linje med hverandre, vil 3 potensielt være mye farligere enn 2, ettersom det er høy grad av usikkerhet rundt denne. Her bør man reflektere rundt hva som er årsaken til usikkerheten, som vi beskrev i kapittel 4.1.1. Dette vil kunne bidra til at ROS-analysen i større grad reflekterer det reelle risikobildet. Hovedpoenget med tabellen er at hendelser som skårer høyt på sannsynlig, konsekvens og/eller usikkerhet bør inngå som dimensjonerende faktorer i beredskapsplanverket. Trafikklysmodellen kan i denne sammenhengen fungere som et nyttig og pedagogisk verktøy.

4.2 Beredskap

Beredskap handler om å være forberedt på å håndtere en situasjon. Beredskap kan finnes i tre former: som en prosess, et produkt og en tilstand. Beredskap som *prosess* viser til at blant annet regelmessige risikoanalyser, etablering, trening og øving samt evaluering skal legge til rette for håndtering av identifiserte uønskede hendelser. Denne prosessen skal lede frem til *produktet* beredskapsplan, som bør forstås som et levende dokument som endres i takt med et skiftende risikobilde. Til slutt skal både beredskapsprosessen og -produktet lede frem til en *tilstand* av "å være beredt". Beredskap og krisehåndtering er to forskjellige aktiviteter, men må likevel forstås som to gjensidig avhengige aktiviteter.

Begrepet beredskap har forandret seg mye med årene. NOU 2000:24 definerte det som «*tiltak for å forebygge, begrense eller håndtere kriser og andre uønskede hendelser*» (NOU 2000:24, s. 20). Dette er samme definisjon som Lunde (2019) bruker. En slik definisjon er enkel, men sier ingenting om hva slags tiltak og konsekvenser det er snakk om. Meld. St. 10 (2016-2017)

Risiko i et trygt samfunn - Samfunnssikkerhet beskriver beredskap som «*planlagte og forberedte tiltak som gjør oss i stand til å håndtere uønskede hendelser slik at konsekvensen blir minst mulig*» (Justis- og beredskapsdepartementet, 2017, s. 22). Denne utdyper mer om tiltak og konsekvenser, men sier heller ikke noe om hva slags type tiltak. Ulike tiltak beskrives derimot av Njå mfl. (2020, s. 266) som tekniske, operasjonelle og organisatoriske.

På bakgrunn av dette forstår vi beredskap som en kombinasjon av disse definisjonene, der beredskap innbefatter alle planlagte og forberedte tiltak, både tekniske, operasjonelle og organisatoriske, som skal gjøre oss i stand til å forebygge, begrense og håndtere uønskede hendelser, og redusere konsekvensene av det inntrufne. En slik definisjon sier både noe om tiltak og konsekvenser, i tillegg til å fokusere på muligheten for å begrense og redusere hendelsene. Dette er viktige momenter å ha med i forståelsen av hvordan kommuner integrerer digital risiko i beredskapsarbeidet.

Mens beredskap handler om å være beredt for det som *kan* skje, handler resiliens om å klare seg bra til tross for opplevelser med stor risiko. Resiliens kan forstås som et sikkerhetsmål, eller en tilstand man ønsker å oppnå (Pidgeon & O'Leary, 2000). Et eksempel på resiliens vil være dersom hjemmetjenesten i en kommune opplever å miste tilgang til de digitale systemene der dagsplanen og adressene til brukerne ligger, men likevel klarer å opprettholde den daglige driften. Det handler med andre ord om å opprettholde funksjonene og egenskapene under utfordrende forhold, slik at organisasjonen kommer styrket ut av det (Sutcliffe & Vogus, 2007). Slike utfordrende forhold kan være alt fra små feil og forstyrrelser, til større kriser. For å oppnå dette må man være forberedt på alt som kan skje. David Woods (2006) argumenterte for at resiliente organisasjoner må ha en oppdatert forståelse av risiko, og tilpasse seg deretter. Dette poenget står muligens enda sterkere i dagens situasjon, i forbindelse med den teknologiske utviklingen.

I dette prosjektet har det vist seg lite hensiktsmessig å skille mellom beredskap og digital beredskap. For det første har vi ikke lyktes i å finne teoretiske bidrag på digital beredskap, som snakker om annet enn passordbeskyttelse og systemsikring. For det andre er det rent prinsipielt det samme. NOU-en *Digital Sårbarhet - Sikkert Samfunn* (2015:13) henviser til daværende instruks for departementenes arbeid med samfunnssikkerhet (2012) når de lister kravene som stilles til det forebyggende beredskapsarbeidet. I NOU-en utdypes det at kravene omfatter "*alle typer forebygging, beredskap og krisehåndtering, inkludert IKT-hendelser"* (NOU, 2015:13, s.

62). Dette ble videreført i samfunnssikkerhetsinstruksen (2017), som erstattet instruksen fra 2012. I lys av at IKT-sikkerhet skal være en integrert del av samfunnssikkerhetsarbeidet (Samfunnssikkerhetsinstruksen, 2017), forholder vi oss til at beredskapsarbeidet omfatter både fysiske og digitale hendelser.

4.2.1 Etablering av beredskap

Det finnes flere modeller og tilnærminger til hvordan beredskap etableres. Selv om det er enkelte variasjoner mellom disse teoriene, kan det argumenteres for at hovedessensen er det samme. I det følgende vil vi se nærmere på Ivar Lundes (2019) modell av beredskapsprosesssen, for å forklare hva det å etablere beredskap konkret innebærer. Deretter vil vi beskrive Rake og Sommers (2018) beredskapshjul, som er en steg-for-steg-metode for beredskapsetablering.

4.2.1.1 Beredskapsprosessen

Lunde argumenterer for at man bør etablere beredskap ved å følge en tredelt prosess, bestående av identifisering, etablering og evaluering. En slik fremgangsmåte sikrer en systematisk og kontinuerlig tilnærming til beredskapsarbeidet. Utgangspunktet for denne prosessen er hentet fra petroleumsregelverket, men flere virksomheter er underlagt rammeverk tilsvarende dette (Lunde, 2019, s. 60). Dette gjelder for eksempel rammeverket for kommunal beredskapsplikt, som vi har snakket om tidligere.

Identifisering

Som en del av identifiseringsprosessen tar man med seg tidligere erfaringer og gjennomførte analyser inn i beredskapsarbeidet. Først gjøres en beredskapsanalyse, på bakgrunn av ROS-analysene. En beredskapsanalyse defineres som «*en analyse som omfatter etablering av definerte fare- og ulykkessituasjoner, herunder dimensjonerende ulykkessituasjoner, etablering av funksjonskrav til beredskap og identifikasjon av tiltak for å dimensjonere beredskapen*» (Lunde, 2019, s. 62). Virksomhetens ambisjoner for beredskapen fastsettes altså her, gjennom ytelsesrammer, ytelseskrav og nødvendige ressurser. Ytelsesrammene brukes for å beskrive hendelsene beredskapen etableres for å håndtere. Disse hendelsene er basert på det som har fremkommet av risikoanalysen, og er plukket ut på bakgrunn av at de har høyest risiko. Disse hendelsene har mange navn. Noen kaller dem for eksempel definerte fare- og ulykkeshendelser, mens andre kaller dem dimensjonerende hendelser. Sammen vil de utvalgte hendelsene utgjøre det som kalles *beredskapsområdet* (Lunde, 2019).

Ytelseskravene er de kravene man har til responsen og håndteringen av disse hendelsene. Disse kravene kan komme av virksomhetens interne krav, pålagte krav fra myndighetene, eller offentlighetens krav og forventning til håndteringen. Slike krav kan enten være kvalitative eller kvantitative. Et kvantitativt krav er at responstiden til Politiet skal være på plass innen ti minutter eller kortere på minimum halvparten av hasteoppdragene i tettsteder med mellom 2 000 til 19 000 mennesker (Politiet, 2020). Et mindre målbart, kvalitativt krav, vil kunne være at Politiet skal være på hendelsesstedet "snarest mulig" etter at operasjonssentralen er varslet.

Det må også identifiseres både eksterne og interne ressurser for å sikre en tilfredsstillende beredskap. De ressursene man eventuelt måtte mangle, vil fremkomme av en såkalt GAP-analyse. Der sammenlignes det man har fra før, med det man trenger for å håndtere de dimensjonerende hendelsene.

Etablering

Når rammer, krav og ressurser er identifisert i beredskapsanalysen, er neste steg å etablere beredskapen. Her skal strategien dokumenteres i den faktiske beredskapsplanen, altså det dokumentet som aktivt benyttes i en beredskapssituasjon. Beredskapsetablering har to hovedformål. Det første er å dokumentere hvilke beredskapsressurser som skal benyttes, hvordan disse er organisert, og hvordan de skal respondere og agere i en beredskapssituasjon. Det andre er at beredskapsressursene må læres, trenes og øves slik at de er kvalifisert nok til å gjøre de oppgavene de er tillagt i dokumentasjonen. Sistnevnte er også en del av kompetansehevingen i modellen.

Evaluering

Den siste delen av beredskapsprosessen handler om evaluering. Hovedformålet er å kontrollere at beredskapen er tilfredsstillende; at den fungerer i praksis, er effektiv, oppfyller krav, og har en akseptabel kostnad. Dersom planen *ikke* er det, går modellen over i en ny runde med å fastsette nye rammer, ressurser og krav. Evalueringsfasen kommer gjerne etter øvelser, eller etter håndteringen av en uønsket hendelse. Denne delen av beredskapsprosessen må foregå kontinuerlig, for å sikre at beredskapsplanen alltid er oppdatert. Dersom dette ikke gjennomføres, vil beredskapsplanen stå i fare for å bli et "fantasidokument" (Clarke og Perrow, 1996). Et fantasidokument vil for eksempel komme av at praktiske erfaringer ignoreres, eller at planen bygger på ressurser som ikke finnes. Et slikt dokument vil ikke noen være tjent med.

4.2.1.2 Beredskapshjulet: seks trinn

Rake og Sommer (2018) bruker en litt mer punktvis og konkret modell for å forklare hvordan man etablerer og vedlikeholder beredskap for en virksomhet. Denne modellen kalles beredskapshjulet, og er bygd opp av seks ulike trinn:

Trinn 1: Først fastsettes mål, rammer og forankring for beredskapen. Dette kommer gjerne av krav og forventninger fra både øvrige myndigheter og innbyggerne i kommunen.

Trinn 2: Ved hjelp av en ROS-analyse kartlegges det hvilke uønskede hendelser som kan inntreffe. Tidligere erfaringer, både egne og andres, bør vektlegges her. Etter januar 2021 bør for eksempel de enkelte kommunene vurdere egen evne til å håndtere spredning av det muterte covid-19-viruset (etter hendelsen i Nordre Follo kommune), et lengre strømbrudd over flere dager (etter strømbrudd som følge av ekstremværet i Sirdal kommune), eller internasjonalt dataangrep mot kommunen (etter dataangrepet mot Østre Toten kommune).

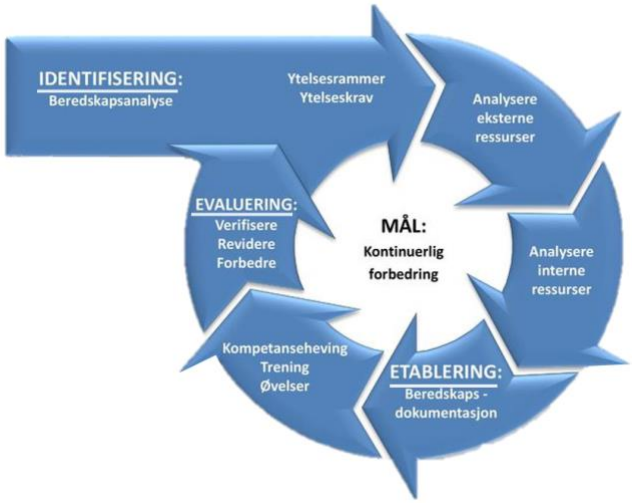
Trinn 3: Gjennomføre beredskapsanalyse for å avgjøre hvilke dimensjonerende hendelser som bør inkluderes i beredskapsplanen. Her er målet å fastsette behov, tiltak og krav for beredskapen. Ytelsesrammene, ytelseskravene og ressursene fastslås blant annet her.

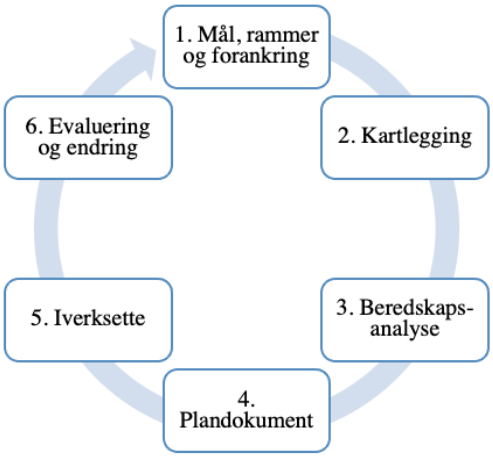
Trinn 4: Utarbeidelse av plandokumenter, herunder beredskapsplanen, beskrivelse av beredskapsorganisasjonen, opplæringsplaner, planer for trening og øvelser, plan for investering, og lignende.

Trinn 5: Her skal planene iverksettes. Dette innebærer å gjennomføre de nødvendige opplæringene og øvelsene, gjøre relevante aktører oppmerksomme på den nye planen, og skaffe nødvendige ressurser som ikke kommunen har fra før av (etter en GAP-analyse).

Trinn 6: Etter hvert som virksomheten får erfaringer fra øvelser og faktiske hendelser, bør planen evalueres. Da kan man se, og eventuelt utføre nødvendige endringer som trengs for å forbedre den. Av hjulets fasong fremstilles beredskapsarbeidet her som en evigvarende prosess, der «evaluering og endring» går over i en ny runde med «mål, rammer og forandring». Dette understreker det kontinuerlige og systematiske arbeidet med beredskapen, der en plan aldri vil kunne spikres som et fullstendig ferdigstilt dokument.

Trinn 1-3 i beredskapshjulet tilsvarer i stor grad det Lunde beskriver som identifiseringsfasen i den tredelte beredskapsprosessen. Det viktigste som skiller de to modellene er at Lundes variant ikke har mål, rammer og forankring som utgangspunkt for prosessgjennomføringen. Her er Rake og Sommer derimot tydelige på at dette er første steg av beredskapsarbeidet. Arbeidet som gjøres her legger selve fundamentet for de videre trinnene. Beredskapshjulets trinn 4 og 5 beskriver videre prosessen som Lunde omtaler som etableringsfasen. Evalueringsfasen kommer deretter i beredskapshjulets trinn 6.





Til venstre, figur 4.2: Lundes beredskapsprosess (inspirert av Lunde, 2019). Til høyre, figur 4.3: Rake og Sommers beredskapshjul (2018).

Som sagt innledningsvis i dette delkapittelet, er det mye av det samme som går igjen i modellene. Dette reflekterer at beredskapsprosessen er et godt utarbeidet fagfelt, med bred enighet om hvordan prosessen med å etablere beredskap bør gjennomføres. Likevel mener vi at Lunde får frem de store forskjellene mellom identifisering-, etablering- og evalueringsfasen, mens Rake og Sommer tydeliggjør viktigheten av beredskapsarbeidets mål og rammer som grunnlag for selve utformingen. Derfor mener vi begge modellene fortjener en plass her.

4.2.2 "God" beredskap

Til tross for at studien ikke tar sikte på å måle hvor "god" beredskapen til kommunene er, kan det likevel være greit å ha kjennskap til kvalitetsstempelet "god" i beredskapssammenheng. Dette er fordi det kan si noe om hvor langt kommuner og andre virksomheter bør strekke seg i beredskapsarbeidet. I det følgende delkapittelet ser vi derfor på hva som kan beskrives som "god" beredskap, og hvordan dette eventuelt kan måles. Vi har ikke lyktes med å finne kriterier for god digital beredskap. Punktene under vil imidlertid etter all sannsynlighet gjøre beredskapen mer robust for digitale uønskede hendelser også.

Perry og Lindell (2003) lister opp ti kriterier for god beredskap. I forbindelse med beredskap for digitale hendelser anser vi disse fire for å være mest kritiske å reflektere rundt:

- Beredskapen bør baseres på presis kunnskap om trusselen.
- Kunnskapen og planlegging bør oppmuntre ledelsen til å iverksette nødvendige tiltak.
- Det bør vektlegges interorganisatorisk koordinering, med samarbeid og felles øvelser.
- Det bør sørges for at beredskapen har en opplæringsdel.

Punkt én kan tolkes slik at analysen og planverket bør bero på så mye kunnskap som mulig. Som redegjort for i kapittel 4.1.3 kan risikoanalyser og refleksjoner rundt usikkerhet bidra til viktig kunnskap om uønskede hendelser. Punkt to belyser at det ikke kun kan være beredskapsavdelingen i kommunen som jobber med beredskapsarbeidet, og at dette er en innsats som må nedlegges både oppover og nedover i organisasjonen. At punkt tre vektlegger interorganisatorisk koordinering og samarbeid belyser viktigheten av at IT- og beredskapsansvarlig i kommunen samarbeider for å imøtekomme nye digitale trusler. Punkt fire er avgjørende for de andre tre punktene, i tillegg til at det innebærer kompetanseheving.

Engen mfl. (2016) er innom mye av det samme som Perry og Lindell. Ifølge dem vil en god beredskapsplan kjennetegnes av at den er kortfattet og forståelig, enkel å bruke, og håndterer en dynamisk utvikling. I tillegg inneholder denne lista to unike punkter; nemlig at beredskapsplanen bør evalueres og oppdateres *fortløpende*, og skape bevissthet om den enkeltes rolle og ansvarsområde. Lunde (2019) sier også at beredskap må ha en akseptabel kostnad. Når virksomheter er underlagt et gitt budsjett, som kommuner, står ofte beredskapsarbeidet i fare for å bli nedprioritert av hensyn til andre poster som kan fremstå som mer kritiske. Dermed er det viktig at prislappen på beredskapen er akseptabel, slik at det ikke blir en innsats som kun legges ned én gang, fordi kostnaden var for høy.

Det er ulike måter å måle godheten av beredskapen på, alle med sine metodiske styrker og svakheter. Relatert til identifiseringsdelen i Lundes beredskapsprosess, kan kvaliteten på beredskapen måles ved å sette de eksisterende beredskapsressursene opp mot de lovpålagte og interne ytelseskravene (Lunde, 2019). Denne testen kan gjøres ved for eksempel å avholde en fullskalaøvelse med en av de dimensjonerende hendelsene som scenario. Når øvelsen evalueres kan det vurderes hvorvidt den dimensjonerende hendelsen ble håndtert i henhold til de ytelseskravene som var satt. Hvis kravene ble tilfredsstilt, kan det argumenteres for at virksomheten besitter god beredskap. Dette avhenger naturligvis av hvorvidt ytelseskravene var strenge nok, eller "gode" nok. Kvantitative ytelseskrav er enklere å måle i ettertid, der et

eksempel kan være å måle om hvorvidt Datatilsynet ble varslet innen ti minutter etter hendelsen ble oppdaget. Kvalitative ytelseskrav er mer utfordrende. Her vil det ofte være noe usikkerhet rundt hvorvidt beredskapen faktisk oppfyller kravene, fordi kravene er formulert som rettslige standarder, og ikke representerer et absolutt minimum. La oss si at kravet var «*et omfattende hackerangrep skal varsles til relevante myndigheter innen rimelig tid*». I ettertid må det da vurderes hvorvidt angrepet var omfattende, hvem som var de relevante myndighetene, og hva som hadde vært rimelig tid. Konklusjonen kan bli svært subjektiv, avhengig av hvilke forventninger man har til egen beredskapsorganisasjon.

En mer uformell måte å måle godheten av beredskapen på, er å sammenligne egen beredskap opp mot andre kommuner og virksomheter. De man sammenligner med bør fortrinnsvis være av tilsvarende størrelse, med et lignende risikobilde og tilnærmet like kapasiteter og ressurser. Dette for å gjøre sammenligningen mer realistisk og forholdsmessig. Slike sammenligninger vil bidra til kunnskapsdeling på tvers av organisasjonene, og vil også kunne åpne opp for beredskapssamarbeid og -nettverk. Dette er for eksempel gunstig for kommuner som har mangel på nødvendig kompetanse, eller har en liten beredskapsorganisasjon.

4.3 Påvirkende faktorer i organisasjoners sikkerhetsarbeid

I kontekstkapittelet ble det kort gjort rede for kommuner som en organisasjon. Det er riktignok flere faktorer som kan påvirke arbeidet som gjøres innad i organisasjonen, og som er relevante å se på i forbindelse med sikkerhetsarbeidet i kommunen. I dette delkapittelet vil det redegjøres for risikopersepsjon, sikkerhetskultur og organisasjonsstruktur. Dette er også faktorer som i stor grad påvirker hverandre. For eksempel er de ansattes risikopersepsjon med på å forme sikkerhetstenkingen og -kulturen i organisasjonen, samtidig som sikkerhetskulturen påvirker de ansattes oppfatning av risiko. Tilsvarende vil organisasjonsstrukturen ha mye å si for kulturen blant de ansatte, samtidig som kulturen kan påvirke organisasjonsstrukturen.

4.3.1 Risikopersepsjon

Risikopersepsjon, eller risikooppfattelse, brukes om hvordan individer og interessegrupper har formet sin egen forståelse og oppfatning av risiko. I studier av dette begrepet sees det bort fra ekspertenes matematiske og statistiske risikovurderinger, for heller å fokusere på de subjektive forholdene som ligger til grunn for hvordan enkelte oppfatter og vurderer risiko (Boyesen, 2003). Ifølge Renn (2008, s. 93) formes dette av blant annet forventninger, håp, frykt og følelser

rundt aktiviteter med en viss usikkerhet. Disse kan igjen være knyttet til blant annet kunnskapsnivå, vitenskapelige risikovurderinger eller personlighetsfaktorer.

Wibecke Brun (1997) skiller mellom ulike dimensjoner som påvirker folks risikopersepsjon, hvorpå vi vil trekke frem styrke-, eksponering- og nyhetsdimensjonen. *Styrkedimensjonen* går ut på at jo mer alvorlig og urovekkende de potensielle konsekvensene av en risikokilde er, jo større oppleves risikoen. Hvis man for eksempel er klar over hvor sektorovergripende nedetid i det kommunale nettverket kan være, vil risikoen for at dette kan skje oppleves som mye større. Et mer klassisk eksempel på dette, er hvordan noen opplever risikoen for å fly som stor, ettersom konsekvensene av en flystyrt potensielt kan være katastrofale. På samme måte som at konsekvensene i noen tilfeller gis for stor oppmerksomhet, kan det i andre tilfeller gis *for lite*. *Eksponeringsdimensjonen* handler om hvordan man vurderer sannsynligheter opp mot den relative risikoen for enkeltmennesket. Brun (1997) påpeker her at folk har en tendens til å tenke at uønskede hendelser er mindre sannsynlig å ramme en selv, fremfor andre, ettersom man ikke anser seg selv i samme risikogruppe. Det er for eksempel ikke utenkelig at enkelte kommuner ikke tror at digitale uønskede hendelser vil ramme en selv, slik som det kan ramme andre, fordi en ikke anser seg selv som like sårbar. *Nyhetsdimensjonen* ser på hvorvidt risikoen oppleves som ny og ukjent. Dersom den er ukjent, kan dette gjøre at risikoen føles større – uavhengig av sannsynligheten for at det kan inntreffe. Et eksempel på dette er hvor uoversiktlig og skummel covid-19-situasjonen var i begynnelsen av 2020, grunnet mangel på kunnskap og erfaring. Etter hvert som vi har fått mer kunnskap om viruset, er det grunn til å tro at folks risikopersepsjon har blitt mer rasjonalisert.

Selv om studier av risikopersepsjon ser mer på de subjektive holdningene, argumenterer Renn (2008) for at risiko og risikopersepsjon *ikke* kan sees som to uavhengige områder. Beslutningstaking som angår risikovurderinger bør ta hensyn til oppfatningene folk har av den aktuelle risikoen, for å respondere til usikkerheten som følger med risiko som konsept. Å unnlate å gjøre dette kan føre til kritikk, og i verste fall tap av tillit til beslutningsmyndighetene. Etter kvikkleireskredet i Gjerdrum i desember 2020 har det for eksempel kommet flere reaksjoner på hvorfor Norges Geotekniske Institutt (NGI) ikke hørte på advarslene som kom inn i forbindelse med utbyggingen på området (Tomter mfl., 2020).

4.3.2 Sikkerhetskultur

Sikkerhetskultur er sterkt relatert til organisasjonskultur, som kan defineres som "*delte verdier, tro og holdninger som sammen med organisasjonsstrukturen og kontrollsystemene produserer normer for oppførsel*" (Reason, 1997, s. 192). Ifølge Reason (1997) er en god sikkerhetskultur kjennetegnet ved å være rettferdig og fleksibel, samt oppmuntre de ansatte til å rapportere inn feil, og lære av det.

I forbindelse med dette prosjektets formål, er det hensiktsmessig å se nærmere på *digital* sikkerhetskultur. Dette kan defineres som «*de verdier, holdninger, antakelser, normer og kunnskaper som mennesker bruker når de forholder seg til digitale verdier*» (Bergsjø mfl., 2020, s. 36). I rapporten *Nordmenn og digital sikkerhetskultur 2019* peker NorSIS på åtte kjerneområder som kan beskrive digital sikkerhetskultur på en helhetlig og relevant måte (NorSIS, 2019). Risikopersepsjon, som vi har vært inne på tidligere, er en av disse. I tillegg er det fire andre dimensjoner som er særlige relevante for studiens problemstilling; optimisme for digitalisering, kompetanse, interesse for IKT, og atferdsmønstre.

Fokuset på *optimisme for digitalisering* er i praksis et fokus på holdninger. Personlige holdninger til digitalisering påvirker måten man forholder seg til teknologi på (Bergsjø mfl., 2020, s. 40). Mistillit til digitale tjenester, frykt for datakriminalitet og holdninger til egen datasikkerhet er blant noen elementer som påvirker evnen til å digitalisere på en trygg og effektiv måte. Holdningene til hver enkelt bruker av teknologien vil dermed inngå som et sentralt aspekt i den overordnede digitaliseringsprosessen.

Relatert til digital sikkerhet har *kompetanse* to hovedaspekter. Det første handler om at kunnskap og kompetanse om digitale verktøy og systemer har blitt en slags forutsetning for å delta i det moderne samfunnet (Bergsjø mfl., 2020, s. 40). Dette er et slags paradoks, der man på den ene siden må ha digital kompetanse for å være en aktiv og deltakende borger, samtidig som det i liten grad inngår i skolens læreplaner. Dette medfører at man i stor grad står ansvarlig for å lære dette selv. Dette tar oss videre til neste aspekt, nemlig hvor man henter kunnskapen fra. Innen alle fagfelt og alle kulturer blir noen mer lyttet til enn andre. Disse personene får i større grad mulighet til å definere hva som er riktig og gal kunnskap om digitalisering. Dette krever refleksjon i form av at vi må være kritiske til hvem som har denne myndigheten (Bergsjø mfl., 2020). Relatert til kommunene vil det være forskjell på kunnskapen man henter fra nøytrale myndigheter som NSM, Datatilsynet og NorSIS, sammenlignet med tjenestetilbydere

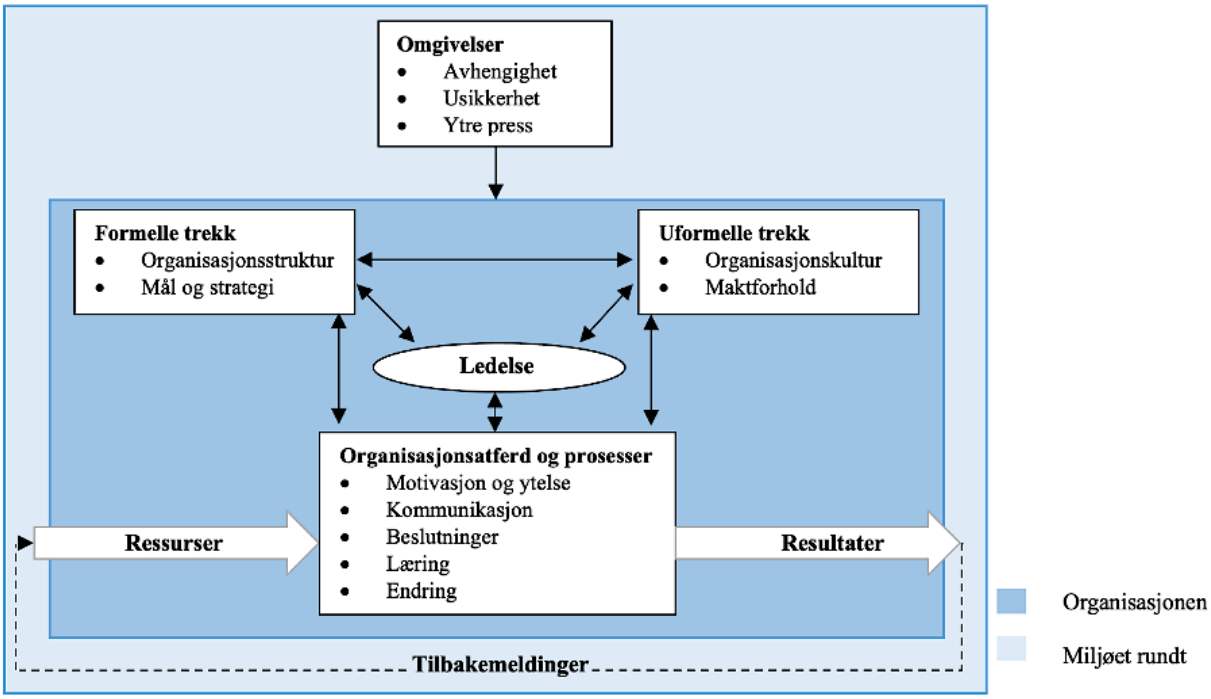
som Apple og Microsoft. Her kan det være hensiktsmessig å reflektere rundt de anbefalinger og råd man får, da selgere av digitale systemer og tjenester ofte vil ha andre intensjoner og en annen agenda enn myndighetene.

Interesse er også en nøkkelfaktor innen digital sikkerhetskultur. Ifølge NorSIS (2019) er interesse med på å utforme holdninger, ferdigheter og kunnskaper. Interesse har også en påvirkning på hvem vi ønsker å assosieres med, hvem vi lytter til og hvem vi ønsker å lære fra (Bergsjø mfl., 2020, s. 42). Det kan dermed antas at uten interesse for IKT og teknologi vil man stille svakere enn andre som har interesse, og dermed også kunnskap, læring og bevissthet.

Atferdsmønstre er også relevant i denne sammenhengen. Noen former for atferd bidrar til digital sikkerhet, mens andre former ikke gjør det. Et konkret eksempel kan være det å dele passord med andre, versus det å ikke gjøre det. En normativ standard for hva som er å anse som "god" digital atferd kan gis av myndighetene, ledende selskaper og eksperter. En utfordring med disse rådene er at de fort blir utdatert, grunnet den raske teknologiske utviklingen. Kunnskap om nettvett som gjaldt for ti år siden er ikke nødvendigvis tilstrekkelig i dag. Et eksempel er at anbefalinger om type passord har endret seg. Før var det vanlig å anbefale kompliserte passord (for eksempel C%s-$€kk), mens det i dag er bred enighet om at det er lengden på passordet som er avgjørende (for eksempel jeglikerålesekrimbøker) (Bergsjø mfl., 2020, s. 42-43).

4.3.3 Jacobsen og Thorsviks organisasjonsmodell

Modellen til Jacobsen og Thorsvik illustrerer den systematiske tankegangen som brukes innen organisasjonsteori. I tillegg viser den tydelig hvordan A i en organisasjon kan påvirke B. Derfor vil vi bruke modellen til å se hvordan ulike faktorer påvirker kommunens beredskapsarbeid.



Figur 4.4: Organisasjonsmodellen (Etter modell av Jacobsen og Thorsvik, 2013).

I det mørkeblå feltet i modellen finner vi kommunen som organisasjon. Alle momenter innenfor dette området påvirkes av hverandre. Ledelsen er med på å påvirke både formelle trekk, som organisasjonsstrukturen og kommunens mål og strategi, og uformelle trekk, som organisasjonskulturen og maktforhold innad. De formelle og uformelle trekkene er igjen med på å påvirke hverandre, i tillegg til ledelsen. Alle er også med på å forme organisasjonsatferden og arbeidet som gjennomføres i kommunen. Sistnevnte påvirkes også av kommunens ressurser; eksempelvis økonomi, arbeidskraft, råvarer, og samarbeid med andre virksomheter eller kommuner. Dette gjelder også beredskapsarbeidet, og således beredskapsplanen, som kommer ut som resultat.

I det lyseblå feltet finner vi miljøet rundt, altså samfunnet. Her får kommunene tilbakemeldinger på det de produserer og iverksetter, som for eksempel sikkerhetstiltakene som innføres etter anmodning fra beredskapsplanen. Disse tilbakemeldingene påvirker ressursene kommunen bruker på å evaluere og revidere planen. Det er også gjennom samfunnet og omgivelsene at kommunen blir presset til å yte, gjennom for eksempel avhengigheten til statlige myndigheter og påfølgende press og forventninger fra media og kommunens innbyggere.

Modellen kan eksemplifiseres. Dersom beredskapsavdelingen i kommunen får tildelt færre økonomiske ressurser fra ett år til det neste, kan dette føre til lavere motivasjon og ytelsesnivå hos de ansatte. Denne atferden kan påvirke den interne kulturen, deriblant sikkerhetskulturen, som kan få ansatte til å ta dårlige sikkerhetsmessige valg. Dårlige beslutninger kan gå utover den nye beredskapsplanen, og således føre til kritiske tilbakemeldinger fra samfunnet. Dersom ledelsen får en ny forståelse for egen sårbarhet, og ser et behov for å iverksette nye sikkerhetstiltak, vil dette endre en del av organisasjonens mål og strategi. Slik vil ledelsens nye risikopersepsjon forplante seg til organisasjonsstrukturen, organisasjonslæringen, og arbeidsprosessen, som igjen vil påvirke de ansattes atferd og kulturen innad i organisasjonen. Slik kan altså endringer i den ene delen av organisasjonen forplante seg videre.

5.0 Forskningsmetode

I et forskningsprosjekt er det essensielt å finne en metodisk strategi som passer det spesifikke prosjektet. Dette vil hjelpe forskerne med både å samle inn dataen, analysere dataen, og finne mening når dataen skal tolkes. Slik frembringer forskningen gyldig og troverdig kunnskap om virkeligheten. I dette kapittelet vil vi redegjøre og argumentere for de metodiske valgene som vi har gjort underveis i prosjektet. Avslutningsvis vil vi drøfte styrker og svakheter knyttet til den valgte metodikken, ved å se nærmere på vanlige kvalitetskriterier i kvalitativ forskning; validitet, reliabilitet og overførbarhet.

5.1 Valg av undersøkelsesopplegg

Oppgavens undersøkelsesopplegg har en abduktiv tilnærming. Abduksjon er en metode som befinner seg i skjæringspunktet mellom induksjon og deduksjon. En induktiv tilnærming går fra empiri til teori, mens en deduktiv tilnærming går fra teori til empiri. Med en abduktiv tilnærming vil man stå overfor en kontinuerlig problemløsende prosess som veksler mellom teori og empiri, der ingen av de to vil ha en overveiende fordel (Jacobsen, 2015). Mens teorien bidrar til å belyse beredskapsrammeverket, forsøker empirien å kartlegge de sosiale aktørenes opplevelse av hvordan dette fungerer i praksis i forbindelse med digital risiko.

Danermark, Ekström, Jakobsen og Karlsson (2002, s. 80) beskriver abduktive prosjekter som å være i stand til å forstå noe på en ny måte, ved å observere og tolke det i et nytt rammeverk. Blaikie (2010) påpeker også at en abduktiv tilnærming besvarer problemstillinger ved å produsere forståelse fremfor forklaring. Dette poengterer at det ikke nødvendigvis finnes ett svar på problemstillingen, noe som kan gjøre det utfordrende å vurdere gyldigheten til prosjektet. Det er derfor essensielt å påpeke at formålet med prosjektet vårt er å skape større innsikt, og en bredere forståelse av beredskapsrammeverket som fenomen, fremfor å presentere et fasitsvar. Det er på dette punktet Blaikie (2010) og Danermark mfl. (2002) sin forståelse av abduksjon skiller seg noe. Mens teorien er *utgangspunktet* for forskningen for Danermark mfl. (2002), er teorien *sluttproduktet* av forskningen for Blaikie (2010), der forskningen har kommet frem til ny teori og et nytt konseptuelt rammeverk. Dette var ikke formålet med vårt prosjekt. Vi undersøkte det valgte fenomenet gjennom et sett etablerte teorier og rammeverk, for så å forsøke å tilegne oss ny forståelse av dette ved å innhente sosiale aktørers opplevelser og oppfatning av konseptet. Med andre ord var ikke målet å generalisere funnene i form av ny teori, men heller å oppnå en bredere forståelse av beredskap som konsept.

5.1.1 Kvalitativ metode

Det er to hovedmåter å samle inn og analysere data: kvalitativt eller kvantitativt. En kvantitativ metode vil skape forståelse ved bruk av tall for å generere statistikk, og er dermed godt egnet for testende problemstillinger som har til hensikt å finne hyppigheten eller omfanget av et fenomen (Johannesen, Tufte og Christoffersen, 2011). En kvalitativ metode vil skape forståelse gjennom ord, deriblant samtale og tekst (Bryman, 2004). Denne metoden er dermed egnet for eksplorerende problemstillinger, der hensikten er å oppnå nyanser mellom et mindre utvalg.

Ettersom vi var ute etter å få en forståelse av hvordan kommuner jobber med beredskapsplanleggingen, anså vi kvalitativ forskningsmetode som hensiktsmessig. Selv om vi trolig kunne ha oppnådd en god forståelse av beredskapsarbeidet med en kvantitativ metode, tror vi at den kvalitative tillot oss å gå *enda mer* i dybden av hver enkelt kommunes opplevelser og erfaringer. Dermed kunne vi også kartlegge flere nyanseforskjeller.

5.1.2 Ontologi, epistemologi og metodologi

Sovacool, Axsen og Sorrell (2017) mener at gode forskningsprosjekter anerkjenner hvordan ontologi, epistemologi og metodologi påvirker forskningen. I de tilfeller der det sees på hva sosiale aktører mener og fortolker, slik som her, er dette spesielt viktig. Derfor vil vi kort gå gjennom disse begrepene.

Ontologi handler om læren om hva som eksisterer, ergo hvilken virkelighetsoppfatning man har (Jacobsen, 2015, s. 24). Den ontologiske forståelsen vil variere både mellom enkeltmennesker og større grupper, og vil dermed også være forskjellig hos forskere og informanter. På grunn av dette vil det være problematisk å gi en universell forklaring på verden, eller enkeltfenomener.

Epistemologi omhandler læren om å lære, altså hvordan man tilegner seg kunnskap (Johannessen mfl., 2011). Ettersom ulike mennesker har ulike ontologier, er det også uenigheter om hvordan man kan samle kunnskap om verden. Spørsmålet om dette lar seg gjøre, står også sentralt.

Metodologi handler dermed om refleksjoner over hvilke metoder som tas i bruk i empiriske undersøkelser, for å samle inn kunnskap om verden (Johannessen mfl., 2011). Denne metoden

vil dermed være svært påvirket av hvilket syn man har på den virkeligheten man ønsker å innhente kunnskap om.

Grunnen til at disse tre begrepene er relevante i denne sammenheng, er fordi det bidrar til å belyse hvordan samspillet mellom virkelighetsforståelse, kunnskap og metode kan påvirke forskningsfunnene. I vårt tilfelle, der data blant annet ble samlet inn gjennom intervju, påvirket informantenes egen ontologi det som kom frem, mens vår metodologi og epistemologi påvirket hvordan vi tolket det.

5.1.3 Forskningsstrategi

Blaikie (2010) skriver at en forskningsstrategi handler om prosedyrene som foreligger for å besvare problemstilling og forskningsspørsmål. Å fremlegge forskningsstrategien er med på å styrke forskningens transparens og reliabilitet, som vi vil komme tilbake til i kapittel 5.4 Forskningskvalitet: metodiske styrker og svakheter. Med hensikt om å gi en oversiktlig forklaring av prosessen vi gjennomgikk for å ferdigstille prosjektet, presenteres tabellen nedenfor.

Januar	*Hva ble gjort*	Utformet tidlig en plan for semesteret og hadde første møte med veileder. Fant relevant litteratur og begynte å videreutvikle prosjektskissen. Satt sammen et førsteutkast til teorikapittel. Avtalte tidspunkt for intervju med 13 informanter, men hadde også fått en del avslag som følge av covid-19-pandemien.
	Hensikt	Ettersom vi holdt til i ulike byer i Norge, var det viktig å ha en strukturert plan for fremgangen til prosjektet, tidligst mulig. Grunnet covid-19 startet vi planlegging av digital gjennomføring av intervju.
Februar	*Hva ble gjort*	Fikk endelig tilbakemelding fra alle informanter, og avtalte tidspunkt for 16 intervju. Skrev førsteutkast til kontekstkapittel og metodekapittelet. Brukte mye tid på å intervjue, transkribere og kode i Nvivo.
	Hensikt	Viktig å starte tidlig med intervju, for å ha god tid til transkribering og koding. Utkast til kapittel 1 og metodekapittel ble påbegynt for å få lage en enda tydeligere rød tråd for oss selv i oppgaven, før vi gikk i gang med intervju
Mars	*Hva ble gjort*	Justeringer i teorikapittelet, som følge av informasjonen i intervjuene. Pågikk parallelt med analyseringen av dataen fra intervjuene, for å planlegge og utforme empirikapittelet.
	Hensikt	Som forventet medførte intervjuene behov for større endringer i teorikapittelet, for å tilpasse temaene hverandre. Dette ble tatt tak i øyeblikkelig, for å unngå skjevheter i oppgavens sammenheng, som kunne forplantet seg videre i oppgaven, og ødelagt for sluttresultatet.

April	*Hva ble gjort*	Som følge av sykdom med covid-19 ble prosjektet satt på vent de første to ukene i april. Da vi kom i gang igjen gikk vi sammen gjennom kontekst-, lover-, teori og empiri-kapittelet, for å linke de sammen og utforme disposisjon til diskusjonskapittelet. De to siste ukene av april gikk til å utforme diskusjonen.
	Hensikt	Planen var å ha et tilnærmet ferdig utkast av oppgaven innen begynnelsen av mai, slik at de siste ukene kunne brukes til endring, korrektur og forbedring, samt konklusjon.
Mai	*Hva ble gjort*	Flere gjennomlesninger resulterte i større endringer i diskusjonskapittel, samt mindre endringer i teori og kontekst. Mye fokus på sammenheng, korrektur og referansebruk.
	Hensikt	Ferdigstilte dokumentet, for å unngå dårlig tid opp mot leveringsfrist.
Juni	*Hva ble gjort*	Estetiske og pedagogiske endringer i dokumentet. Ferdigstilte dokumentet for innlevering.

Tabell 5.1: Forskningsstrategien

5.2 Datagenerering

I dette delkapittelet vil vi presentere semi-strukturerte intervju og dokumentundersøkelse som kvalitativ metode, for så å redegjøre for hvordan vi gikk frem for å finne informanter til prosjektet. Til slutt gjennomgår vi intervjusituasjonen og utformingen av intervjuguiden.

Det finnes en rekke muligheter for å samle inn kvalitativ data, der det kan skilles mellom primær- og sekundærdata. Primærdata samles inn for første gang, direkte fra mennesker eller grupper. Slik blir datainnsamlingen skreddersydd for den aktuelle problemstillingen. Sekundærdata er, på den andre siden, samlet av en annen forsker, ofte til en annet formål.

5.2.1 Semi-strukturerte intervju

Ettersom vi fant lite forskning som så på det samme som det vi undersøkte, valgte vi å samle inn primærdata gjennom semi-strukturerte intervju. Dette er den mest brukte innsamlingsmetoden innenfor kvalitativ metode, ifølge Alvesson og Deetz (2000), trolig fordi det følger mye positivt med innsamlingsmetoden. Eksempelvis sørget semi-strukturerte intervju for at alle informantene ble spurt om de samme temaene, samtidig som vi kunne gå nærmere inn på de enkelte temaer underveis i intervjuet. Et strukturert intervju ville gjort det vanskelig å gå i dybden av enkelttemaer som dukket opp under intervjuet, og et ustrukturert intervju ville gjort det vanskelig å sikre at alle informantene ble spurt om det samme. Den semi-strukturerte metoden var således mer fleksibel, enkel å gjennomføre, og egnet til å avsløre flere detaljer om den enkelte kommune. I tillegg gjorde den det enklere for informantene å utdype

og tydeliggjøre egne svar. Slik kunne vi også imøtekomme utfordringer, som faren for å tolke informantenes svar feil.

5.2.2 Dokumentundersøkelse

I tillegg til intervjuene, gjorde vi en dokumentundersøkelse av sekundærdata. I disse undersøkelsene tok vi for oss tilsynsrapportene til de ti kommunene i utvalget. Disse rapportene er resultat av tilsynet Statsforvalteren har gjennomført med kommunens beredskapsplikt, og er funnet under "tilsyn" på nettsiden til de ulike statsforvalterne.

Tilsynsrapportene undersøker hvorvidt kommunene oppfyller bestemmelsene i forskrift om kommunal beredskap og sivilbeskyttelsesloven. Rapportene undersøker med andre ord gapet mellom kommunens beredskapsarbeid og det lovpålagte rammeverket. Disse rapportene brukes til å underbygge informantenes påstander om de samme temaene som rapportene tar for seg, og flettes derfor inn i empirikapittelet. Det er kun konklusjonen i de ulike rapportene som inkluderes. Selve innholdet i rapportene drøftes derfor ikke, men ses kun i lys av informantenes beretninger. I rapportene registreres brudd på sivilbeskyttelsesloven §§ 14 og 15 eller forskrift om kommunal beredskapsplikt som "avvik". Områder Statsforvalteren mener kommunen har forbedringspotensial, men som ikke oppfyller definisjonen til avvik, registreres som "merknad".

Bruken av tilsynsrapportene medfører imidlertid noen utfordringer hva gjelder prosjektets etterprøvbarhet. Av hensyn til anonymiseringen av informantene og kommunene kan det ikke refereres til disse rapportene. Dette må betraktes som en metodisk svakhet. Det må også påpekes at tilsyn med kommunal beredskapsplikt kun gjennomføres hvert fjerde år. Dette har medført at flere av rapportene er eldre. Fire er fra 2017, én fra 2018, én fra 2019 og én er fra 2021. Tre er fra så tidlig som 2016 (se tabell 5.4 for en detaljert oversikt). Mye har naturligvis endret seg siden den tid, så innholdet i disse rapportene kan dermed ha begrenset validitet. Likevel anses tilsynsrapportene for å ha forskningsmessig verdi, da de kan underbygge påstandene til informantene i utvalget.

5.2.3 Utvalget

Sammen med veileder planla vi å snakke med ti forskjellige kommuner. Dette var for å få et større nyansebilde, og flere kommunale erfaringer å sammenligne, uten at det ville ta altfor mye tid med hensyn til prosjektets sluttdato.

Da vi skulle velge ut de ti kommunene var det viktig for oss at de i størst mulig grad gjenspeilet hele kommune-Norge. Derfor valgte vi å invitere to kommuner fra alle de fem landsdelene.

Landsdel	Fylker	Antall kommuner	Areal (km^2)	Innbyggertall per 01.01.20 (rundet av til nærmeste 1000)
Vestlandet	Møre og Romsdal, Vestland, Rogaland	92	57 550	1 382 000
Sørlandet	Agder	25	16 434	307 000
Østlandet	Viken, Oslo, Vestfold og Telemark, Innlandet	121	94 585	2 726 000
Midt-Norge	Trøndelag	38	42 202	469 000
Nord-Norge	Nordland, Troms og Finnmark	80	112 985	485 00

Tabell 5.2: Informasjon om Norges landsdeler (Tallene er hentet fra Statistisk Sentralbyrå [SSB] (2020) og SSB (2021)).

Å velge to kommuner fra hver landsdel var et bevisst forsøk på å imøtekomme at landsdelene består av et ulikt antall kommuner, som ikke nødvendigvis samsvarer med arealet eller innbyggertallet. Eksempelvis rommer Østlandet cirka tre ganger så mange kommuner som Midt-Norge, selv om Midt-Norge er halve størrelsen. Tilsvarende bor det fem ganger så mange mennesker på Østlandet som i Nord-Norge, til tross for at Nord-Norge er like stort som Østlandet og Sørlandet til sammen i areal. Sørlandet og Midt-Norge består også bare av ett fylke hver, noe som muligens kan forklares med at disse landsdelene er mindre i størrelse og har færre antall kommuner enn de andre. Hensikten med å velge to fra hver landsdel ville på denne måten ta et visst hensyn til disse ulikhetene i landet, til tross for at det ville medføre skjevheter på enkeltområder som areal, antall fylker og kommuner og innbyggertall.

Basert på SSBs oppdaterte liste over kommuners innbyggertall fra 2021, talte vi oss frem til at medianstørrelsen var 5 196,5 (SSB, 2021). Dermed var det viktig at en stor andel av kommunene ville være under, og rundt, denne størrelsen. Vi bestemte oss for følgende tredelte kategorisering, basert på innbyggertall.

Størrelse på kommune	Befolkningstall
Liten	0 - 4 999
Mellomstor	5 000 – 19 999
Stor	Over 20 000

Tabell 5.3: Størrelseinndeling av kommuner.

Denne kategoriseringen er blant annet brukt av SSB og Digitaliseringsdirektoratet i en rapport om *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner* (Digdir, 2020). Med dette utgangspunktet valgte vi ut kommuner, så tilfeldig det lot seg gjøre med disse

forutsetningene: to fra hver landsdel, med variert befolkningstall. De aktuelle kommunene ble deretter ringt til, for å få tak i kontaktinformasjonen til de personene som hadde det spesifikke ansvarsområdet vi var ute etter. Totalt tok vi kontakt med 15 kommuner, der tre takket nei, og to ikke svarte. De som ikke svarte ble purret på to ganger, uten at det ga noe mer svar. Til slutt stod vi igjen med følgende ti kommuner:

Kommune	Landsdel	Størrelse, basert på befolkningstall	Tilsynsrapport årstall
K1	Sørlandet	Liten	2016
K2	Nord-Norge	Liten	2018
K3	Vestlandet	Liten	2017
K4	Midt-Norge	Liten	2021
K5	Sørlandet	Mellomstor	2016
K6	Østlandet	Mellomstor	2017
K7	Nord-Norge	Stor	2017
K8	Østlandet	Stor	2017
K9	Vestlandet	Stor	2016
K10	Midt-Norge	Stor	2019

Tabell 5.4: Utvalget til prosjektet

Til tross for at pseudonymene K1-K10 kan fremstå som noe uoversiktlig i empirikapittelet, er det et bevisst valg for å tilrettelegge for forskningens etterprøvbarhet. En tommelfingerregel er at K1-K4 er små kommuner, K5 og K6 er mellomstore, og K7-K10 er store. Ved behov for å finne ut av kommunens geografiske plassering eller antall år siden sist tilsyn, anbefales det å bla tilbake til denne tabellen.

Ettersom problemstillingen vår krevde at vi så nærmere på både kommunenes IT- og beredskapsmiljø, ville vi forsøke å snakke med én representant fra hvert av miljøene i kommunene. For enkelthetens skyld velger vi å kalle de to for "IT-informanten" og "beredskapsinformanten", ettersom de ulike informantene hadde ulike stillingstitler. Blant beredskapsinformantene kunne for eksempel noen ha stillingen som beredskapsrådgiver, andre som beredskapskoordinator, mens andre hadde en helt annen stilling, med beredskapsansvaret inkludert i arbeidsoppgavene. Sistnevnte gjaldt mest de små kommunene. Tilsvarende gjaldt IT-miljøet, der noen kunne være IT-sjef, andre var enhetsleder for teknisk enhet, mens en var daglig leder i et interkommunalt selskap som kommunen benyttet seg av for IKT-tjenester. Dette utdypes nærmere i kapittel 6.1 Informantenes stillinger og ansvarsområde.

For å ivareta oppgavens validitet, ved å sørge for at IT- og beredskapsinformanten ikke ville kunne komme til å pynte på sannheten overfor både oss og hverandre dersom de ble intervjuet

sammen, ønsket vi å snakke med én informant av gangen. Resultatet av denne beslutningen ble at vi var nødt til å invitere IT-informanten og beredskapsinformanten hver for seg. Dermed ble tilfellet i fire av de ti kommunene, at den ene takket ja, og den andre takket nei. I alle de fire tilfellene var det IT-informanten som takket nei. Årsakene som ble lagt til grunn var:

> «Denne uken er det vinterferie her, og ellers full kalender så noe utfordrende å få tid på kort varsel.» (K1, IT)
>
> «(...) vi ønsker ikke å delta.» (K2, IT)
>
> «Jeg prøver å prioritere jobben som må gjøres, og får derfor ikke tid til dette også.» (K3, IT)
>
> «(...) melder pass i denne omgangen.» (K8, IT)

Likevel valgte vi å beholde disse kommunene som en del av utvalget vårt, ettersom beredskapsinformanten på dette tidspunktet allerede hadde takket ja til invitasjonen.

5.2.4 Intervjusituasjon og intervjuguide

Ettersom januar og februar var perioder med mye restriksjoner og nedstenging i forbindelse med covid-19-pandemien, planla vi fra start å avholde intervjuene digitalt. Det ble bestemt at kommunikasjonsprogrammet Zoom var en god plattform å møtes på, da det ikke krevde noe abonnement eller brukerkonto for informantene. Dette var gunstig med tanke på at ulike kommuner bruker ulike digitale plattformer og løsninger. På Zoom kunne vi opprette et digitalt "møterom", med et venterom som informantene måtte vente i før vi slapp dem inn i møterommet. Det ble også bestemt at vi skulle ha de samme arbeidsoppgavene ved hvert intervju, i et forsøk på å unngå skjevheter (bias) i datainnsamlingsmetoden, og dermed oppnå et mer pålitelig resultat. Vi bestemte at den ene skulle ha ansvar for å føre samtalen, mens den andre skulle ha ansvar for å notere underveis i intervjuet.

Alle de 16 ulike intervjuene foregikk dermed relativt likt. Etter at informanten hadde blitt sluppet inn i møterommet på Zoom, startet vi samtalen med å fortelle hvordan intervjuet ville foregå. Deretter introduserte vi oss selv kort, for at informanten skulle føle en mer relasjonell tilknytning til oss som forskere. Dette ble gjort på bakgrunn av at intervju er en samtale mellom personer, der det er viktig med gjensidig tillit til andreparten. Etter dette leste vi opp en nedskrevet tekst om prosjektet, slik at vi forsikret oss om at alle informantene satt med det samme faglige utgangspunktet til intervjuet. Teksten som ble lest opp var følgende:

> «Formålet med prosjektet er å undersøke hvordan norsk kommunal sektor tar hensyn til digitale uønskede hendelser og digital risiko i sitt beredskapsarbeid. I den forbindelse undersøker vi hvordan beredskaps- og IT-miljøer arbeider sammen. Utgangspunktet for studien er en hypotese om at kommuner er svært kompetente, og nyter lang og omfattende erfaringer på beredskapsområde knyttet til mer tradisjonelle risikoer, men at digitaliseringen har ført til en endring i risikobilde, og følgelig nye utfordringer for beredskapsarbeidet. Denne studien gjennomføres ved å intervjue et lite utvalg på cirka ti kommuner, og stille spørsmål vedrørende deres beredskapsarbeid.»

Etter opplesningen forsikret vi oss om at informanten tillot oss å ta lydopptak av resten av samtalen. Deretter fikk informanten fortelle litt om seg selv og sitt ansvarsområde, før vi gikk i gang med intervjuguiden, som vi hadde sendt ut en ukes tid i forveien.

Intervjuguiden som hadde blitt sendt ut på forhånd, bestod av seks planlagte og åpne spørsmål, markert med fet skrift i intervjuguiden (se vedlegg 1). Denne hadde blitt utformet med intensjon om å finne ut mest mulig om kommunens beredskapsarbeid for digital risiko, og hva informanten selv mente om dette arbeidet. Fokuset lå på kommunens organisasjonsstruktur, beredskapsplanens funksjonalitet, samarbeidet mellom IT- og beredskapsavdelingen, eventuelle utfordringer med å løse digital risiko, og egenopplevde digitale hendelser. Intervjuguiden var testet av oss en ukes tid i forkant av intervjuet, for å sørge for flyt og sammenheng i spørsmålene, og for å kartlegge hva vi skulle fokusere på.

Ved å ha formulert intervjuguiden til å bestå av åpne spørsmål, kunne informantene tolke spørsmålet som de selv ville. I den faktiske intervjusituasjonen fulgte vi opp med oppfølgingsspørsmål som *også* var planlagt på forhånd, men som informanten ikke hadde blitt tilsendt i intervjuguiden (se vedlegg 2). Dette valgte vi å gjøre som et resultat av en intern diskusjon i forkant av intervjuene, om hvorvidt hensikten med intervjuet skulle være skjult eller åpen for informantene. Jacobsen (2015) er blant de i litteraturen som belyser dette spørsmålet. I enkelte tilfeller kan kjennskap til hensikten med forskningen medføre usanne eller upresise opplysninger. Å kun sende ut hovedspørsmålene, som fungerte som hovedtemaene under intervjuet, fungerte som en gylden middelvei. Da kunne informantene føle at de var forberedt på temaene vi ville spørre om, uten nødvendigvis å vite nøyaktig hvilken vinkling vi hadde. De planlagte oppfølgingsspørsmålene sikret også at alle informantene var innom de samme temaene på spørsmålene, som ofte kan være en svakhet i andre semi-strukturerte intervju. I tillegg til de planlagte spørsmålene, ble det også stilt et antall uplanlagte oppfølgingsspørsmål, som en naturlig del av den uformelle samtalen et semi-strukturert intervju kan sies å være. Også

disse spørsmålene var formulert uten direkte føringer, slik at informantene kunne komme med mest mulig informasjon på egenhånd. Dette var for å ivareta oppgavens validitet.

Vi prøvde også etter beste evne å ikke komme med anerkjennende svar mens informanten pratet, som «ja», «okei», og lignende. Dette var for ikke å forstyrre informanten midt i en utdypende refleksjon. Dette var også noe vi forsøkte å unngå ved å holde en kort pause etter at informantene tilsynelatende hadde svart ferdig på et spørsmål, i tilfelle vedkommende ønsket å legge til ekstra informasjon.

Etter å ha stilt alle spørsmålene, oppga vi problemstillingen vår for deretter å spørre om informanten hadde noe mer å tilføye. Dette var også noe som ble bestemt ut fra diskusjonen om hensikten med forskningen skulle være skjult eller ikke. Ved å stille problemstillingen fikk vi til en viss grad forsikret oss om at de viktigste sidene av temaet var dekket gjennom intervjuspørsmålene, uten at kjennskap til problemstillingen la føringer på svarene de oppga ved de andre spørsmålene. Slik ville vi også unngå partiskhet og skjevhet (bias) i den genererte dataen, samtidig som vi forsikret oss om at vi fikk nok informasjon til å svare på problemstillingen til prosjektet.

Alle informantene ble spurt om de ønsket en transkribert versjon av intervjuet. Av alle 16 var det seks som ønsket det. Ingen av disse meldte tilbake om feil eller mangler i ettertid.

5.2.4.1 Lydopptak

Før vi gjennomførte intervjuene, spurte vi alle informantene om muligheten for å ta lydopptak. Dette fikk vi samtykke til av samtlige. For vår del ville opptak gi oss en viss trygghet om at vi fikk med oss alt som ble sagt, i tillegg til at det gjorde det mulig å transkribere intervjuene i ettertid. I tilfelle det skulle skje noe med båndopptakeren eller lydfilen underveis i intervjuet, brukte vi to båndopptakere.

Ettersom intervjuene foregikk digitalt la vi båndopptakerne ved siden av høyttalerne på datamaskinen, slik at informantene ikke så dem. Sett i lys av dette er det rimelig å anta at informantene i liten grad ble påvirket av at det ble tatt opptak av intervjuet. Steinar Kvale (1997) påpeker viktigheten av å være oppmerksom på at lydopptak gir en dekontekstualisert versjon av intervjuet. Dette fordi den ikke inneholder de visuelle aspektene ved situasjonen:

kroppsspråk, ansiktsuttrykk, gestikulering, og lignende. For å imøtekomme dette er det viktig å tenke gjennom transkriberingen som skal gjøres i ettertid.

5.2.4.2 Transkribering

Med flere intervju hver dag i nesten halvannen uke, ville det blitt vanskelig for oss å analysere dataen vi fikk gjennom intervjuene, direkte fra lydopptaket og inn på dataanalyseprogrammet. Derfor valgte vi å transkribere intervjuene først. I de fleste tilfeller ble dette gjort i løpet av den samme dagen som intervjuene ble holdt. I enkelte tilfeller ble de transkribert ferdig dagen etter. Transkriberingsprosessen tok forholdsvis kort tid å gjennomføre, ettersom en av oss hadde notert underveis i intervjuene. På den måten bestod transkriberingen for det meste av å fylle inn utelatte ord og setninger.

Transkribering som prosess kan være problematisk i form av at det ikke finnes en objektiv oversettelse fra muntlig til skriftlig uttrykkelse. For eksempel kan ironi, tenkepauser og lignende, være vanskelig å "oversette" skriftlig. Kvale (1997) anbefaler her å vurdere hvordan transkriberingen skal gjøres ut fra hva som er hensiktsmessig i den konkrete situasjon. I den forbindelse gjorde vi noen valg. For det første valgte vi å normalisere transkripsjonene, det vil si ikke å skrive på informantens dialekt (Tjora, 2021). Dette var for å ivareta informantenes anonymitet, ettersom enkelte dialekter kan være enkle å kjenne igjen skriftlig. For det andre valgte vi å utelate pauser, nøleord og ufullstendige setninger fra transkriberingen. Grunnen til dette var fordi vi kun var ute etter det faglige informantene uttalte seg om. Nøling og ufullstendige setninger var dermed ikke ting vi anså som relevant for å svare på problemstillingen. Denne måten å transkribere på tok også mindre tid. Ifølge Johannesen mfl. (2011, s. 149) regner man “4:1” når det kommer til transkribering: én times intervju tar fire timer å transkribere. Med 16 intervju ville dette tatt nesten to hele arbeidsuker. Med en mindre detaljfokusert transkribering ble denne tiden betraktelig redusert.

5.3 Dataanalyse

Tjora (2021) sier at det er i dataanalysefasen forskerne virkelig må bruke sin intellektuelle kapasitet og kreativitet. Her skal den viktigste dataen som genereres fra intervjuene og tilsynsrapportene sorteres ut. For å hjelpe oss med dette brukte vi dataprogrammet NVivo 12, som er et verktøy Universitetet i Stavanger oppfordrer til å bruke ved kvalitative undersøkelser. Dette er også et program som biblioteket på universitetet arrangerte kurs og opplæring i.

Sannsynligvis finnes det gode alternativer til NVivo 12, men her var muligheten for å få hjelp fra universitetsbiblioteket et overveiende argument for dette valget.

I analysefasen er det enkelt å gå seg vill. Tjora (2021) påpeker at det på dette stadiet er vanlig å ha brukt mye tid på å utvikle intervjuguiden og å gjennomføre datagenereringen. Dette kan skape problemer når det kommer til å skulle finne ut hvor mye data som *faktisk* trengs til prosjektet. Ettersom vi var klar over at vi raskt ville sitte med flere titalls sider med rådata, planla vi hvordan dataen skulle analyseres i forkant av intervjuene. Intervjuguiden ble derfor utformet med utgangspunkt i hva slags informasjon vi trengte for å besvare forskningsspørsmålene. For å kunne presentere et helhetlig resultat fra datainnsamlingen, skulle empirikapittelet struktureres etter intervjuguiden. Videre skulle diskusjonsdelen struktureres etter forskningsspørsmålene. Hensikten med dette var å skape en tydeligere sammenheng mellom empiridelen og svaret på problemstillingen.

Da vi skulle sette i gang med å utforme kodingen startet vi med å kode temaer med utgangspunkt i intervjuguidens hovedspørsmål. Vi var gjennom hele kodeprosessen bevisst på hvordan de kodede temaene ville brukes i besvarelsen av forskningsspørsmålene. Dette fungerte som en forberedelsesprosess til diskusjonsdelen. For eksempel genererte spørsmålet «Beskriv samarbeidet mellom IT- og beredskapsmiljøet.» koder som «Internt samarbeid», «Ansvaret for digitale kriser» og «Utfordringer knyttet til sjargong og faguttrykk». Selv om denne type koding, som Tjora kaller sorteringsbasert koding, kan kritiseres for å bare si noe om temaene det snakkes om, og ikke *hva* som sies, synes vi dette var en nyttig måte å gjøre det på. NVivo-programmet tillot oss å gå inn i hver enkelt av disse kodene, og få en samlet oversikt over hva de ulike kommunene svarte om dette temaet. Med koden «Utfordringer knyttet til sjargong og faguttrykk» kunne vi for eksempel enkelt finne en liste over utsagn fra kommunene knyttet til dette, som for eksempel:

> «Vi prøver jo å unngå det. For det er en dum greie, hvis du må bruke faguttrykk. Det skaper distanse. Det prøver jeg å unngå.»
>
> «Nei, det opplever jeg egentlig ikke. Hvis vi ikke skjønner, så spør vi. Og omvendt.»

Deretter kunne vi printe ut denne oversikten, og markere det vi synes var viktige poeng å få frem i diskusjonen.

5.4 Forskningskvalitet: metodiske styrker og svakheter

Tre kriterier benyttes spesielt for å undersøke forskningskvalitet; validitet, reliabilitet, og overførbarhet (Tjora, 2021). Alle disse tre vil gjennomgås i dette delkapittelet, for å se nærmere på forskningsmetodens styrker og svakheter.

5.4.1 Validitet

Den kvalitative forskningens validitet, eller gyldighet, handler om forholdet mellom forskningen og den virkeligheten som undersøkes. Tjora (2021) forklarer validitet ved hvorvidt de svarene vi finner i forskningen faktisk er svar på de spørsmålene vi stiller. Høy grad av validitet kan blant annet sikres gjennom pålitelig og transparent datainnsamlingsmetode, og åpenhet til tidligere forskning og kunnskap om temaet. Kvale (1997, s. 165) peker på at validering er viktig i alle stadier av forskningen: i tematiseringen, i planleggingen, i intervjuene, i transkriberingen, i analyseringen, i valideringen og i rapporteringen. Med andre ord er dette et tema som kontinuerlig må følges opp og vurderes gjennom prosjektets utforming. Her har problemstillingen fungert som et viktig rammeverktøy for oss, som har kunnet tilspisses underveis i datainnsamlingen, og etter hvert som vi tilegnet oss mer kunnskap. Dette er en fordel som følger av den abduktive tilnærmingen. En utfordring knyttet til prosjektets validitet, var at vi ikke fant så mye tidligere forskning som sa noe om hvordan kommunal beredskapsplanlegging integrerer digital risiko. Dette kan gjøre det vanskelig å si om funnene utover nettopp det vi har sett på. Likevel har vi funnet en del forskning om kommunalt beredskapsarbeid generelt, samt forskning om en økende sårbarhet knyttet til digitalisering. Dette har til en viss grad gitt oss noe å sammenligne med, selv om ingen av dem eksplisitt har sett på det samme som oss.

5.4.2 Reliabilitet

Reliabilitet, eller pålitelighet, i forskning, handler om intern logikk og sammenheng gjennom hele prosessen. Dette innebærer at forskerne er bevisste potensielle feilkilder, som blant annet målefeil eller partiskhet i forskningen. Dette kan vurderes opp mot etterprøvbarhet, der reliabiliteten kan karakteriseres som god dersom noen ville kommet frem til de samme resultatene ved å gjennomføre tilsvarende studier. Et viktig moment hva gjelder reliabilitet i forskning, er at dataen er samlet inn på en relativ lik måte. Dette var et sterkt fokus underveis i datainnsamlingen, og ble tatt hensyn til ved å gjennomføre alle intervjuene likt: digitalt, med de samme spørsmålene, med den samme bakgrunnsinformasjonen, samme intervjuer og med cirka den samme tidsbruken. En utfordring er likevel at vi alle, både forskere og informanter,

har ulike holdninger til ontologi og epistemologi. I praksis betyr dette at vi ikke kan garantere at alle de ulike informantene har tolket spørsmålene likt. Dette må regnes som en svakhet ved metoden. Det er likevel vanskelig å gjøre noe med, annet enn å forsøke å omformulere spørsmålene dersom informanten åpenbart tolket noe annerledes enn vi hadde tiltenkt. På spørsmålet om hvordan kommunen går frem for å endre beredskapen opplevde vi blant annet noen ganger at vi måtte komme med en presisering av hva som lå i ordet beredskap. Ulik begrepsforståelse er et eksempel på forhold som potensielt kan føre til målefeil i forskning.

Som hjelpemidler for å oppnå reliabilitet i forskningen, kan det legges til transparens og refleksivitet i prosessen. Transparens handler om å være åpen om veien mot forskningsfunnene. Det er også nært knyttet til etterprøvbarhet. Å legge intervjuguiden som vedlegg til det ferdige produktet, er et forsøk på å øke prosjektets transparens.

Refleksivitet handler om å reflektere over egen forskning, rett og slett å tolke egen tolkning. Dette var også en grunn til at vi valgte å lese opp den korte introduksjonsteksten om prosjektet vårt til hver informant, før vi gikk i gang med intervjuguiden. På denne måten kunne vi høre om informantene hadde noen bemerkninger til våre hypoteser og tanker rundt temaet, uten at de visste nøyaktig hvilken problemstilling vi så på. Slik fikk vi refleksjoner rundt eget tema fra folk som hadde kompetanse på området. Tilsvarende hjelpsomt har det vært å kunne diskutere ulike fremgangsmåter med veileder. Gjennom diskusjoner rundt metodevalg, teori og analyse, har vi blitt mer bevisste om våre egne posisjoner og fordommer til de ulike kommunenes beredskapsarbeid.

5.4.3 Overførbarhet

Overførbarhet er knyttet til forskningens relevans, utover de enhetene som er undersøkt. I vårt prosjekt kan dette oversettes til hvorvidt forskningen som er gjort om de ti utvalgte kommunene, kan overføres til andre kommuner i Norge. Dette har vi i stor grad prøvd å ta hensyn til. Som nevnt i 5.2.3 har vi forsøkt å invitere kommuner som gjenspeiler kommune-Norge, selv om dette er utfordrende med et så lite utvalg. Kommune-Norge har en bred skala av ulike kommuner når det kommer til innbyggertall, areal, plassering, digital utvikling, økonomi, og lignende. Til tross for at vi har prøvd å variere i både størrelse og innbyggertall, består kommune-Norge av kommuner med flere markante forskjeller. Noe av det lar seg måle, som for eksempel areal og økonomi, mens andre forhold er vanskelig å måle - som for eksempel sikkerhetskultur og grad av digital utvikling. Derfor er det også vanskelig å si noe om dette har

stor påvirkning på funnene. Det er imidlertid lite som tilsier at kommunene i denne studien har et høyere kapasitetsnivå enn gjennomsnittet i Norge. Ingen av kommunene ble valgt på grunnlag av antakelser om høy eller lav beredskapskapasitet. Unntaket er Oslo, som bevisst ble valgt bort fordi kommunen er vanskelig å sammenligne med andre kommuner.

Av de totalt 15 inviterte kommunene, var det som nevnt to kommuner som ikke svarte, og tre som takket nei grunnet covid-19 og en travel hverdag. Disse kommunene kan beskrives slik:

Svar	Landsdel	Størrelse, basert på befolkningstall
Nei	Østlandet	Stor
Nei	Nord-Norge	Stor
Nei	Sørlandet	Liten
Ingen svar	Sørlandet	Stor
Ingen svar	Vestlandet	Liten

Tabell 5.5: Kommunene som takket nei til å delta.

Vi opplevde dermed kommunene som takket ja, nei og ikke svarte, som relativt tilfeldig.

Selv om utvalget vårt kun utgjør 2,8 % av det totale antallet kommuner i Norge, mener vi at det er en viss grad av overførbarhet til andre kommuner i landet. Det må imidlertid understrekes at utvalget etter all sannsynlighet er for lite til at funnene i studien kan generaliseres uten ytterligere undersøkelser.

5.5 Refleksjoner rundt egen studie

Ulike typer hensyn må tas i forbindelse med all forskning, enten det er av pragmatisk eller etisk art. Mange av disse hensynene blir tatt på grunn av begrensede ressurser for metodologisk mangfoldighet. I vårt tilfelle er for eksempel beredskap et stort tema, som medførte at vi måtte ta noen valg i forbindelse med hvilke teoretiske konsepter vi skulle fokusere på å spørre informantene om. I tillegg til slike faglige hensyn, må det også tas valg knyttet til praktiske forhold. Hadde eksempelvis tidsaspektet vært annerledes, hadde vi gjerne intervjuet representanter fra alle kommunene i Norge.

5.5.1 Etiske hensyn

Tjora tar opp noen generelle etiske betraktninger, med den formening om at etikk bør ligge implisitt i all forskning, uavhengig av de formelle kravene som stilles av blant annet NSD (Tjora, 2021). Blant annet kan aspekter som tillit, konfidensialitet, respekt og gjensidighet prege relasjonen mellom informanten og forskerne. Hvordan vi fremstår, oppfører oss, og

svarer til det informantene sier, kan med andre ord ha mye å si for dataen som samles inn. Forskningsetikk i forbindelse med intervju handler først og fremst om at informantene ikke skal komme til skade (Tjora, 2021). I dette prosjekt har vi ikke gjennomført noen eksperimenter som kan påføre informantene fysisk ubehag. Det var riktignok viktig å være klar over vårt etiske ansvar for ikke å presse informanten psykisk, eller bidra til at kommunene tapte ansikt utad. Spesielt sistnevnte har vi forsøkt å ta hensyn til etter beste evne, gjennom blant annet å tilby å ettersende en transkribert versjon av intervjuet, og å anonymisere informantene.

Vi valgte å anonymisere informantene våre av flere grunner. For det første fordi de to forskjellige informantene fra hver kommune kunne ta opp ting som i verste fall kunne være sensitiv informasjon for kommunens ansatte. Eksempelvis kunne IT-informanten ytre seg om et svakt samarbeid med beredskapsinformanten, eller motsatt. For det andre anonymiserte vi fordi informantene tok opp temaer som potensielt kan gjøre kommunen sårbar for ondsinnede aktører. Dersom en kommune for eksempel valgte å være åpen om at de har for lite fokus på digital risiko, ønsket ikke vi å gjøre dem enda mer sårbare ved å gjøre dette kjent for offentligheten. For det tredje ønsket vi å anonymisere kommunene for å få fokuset bort fra kommunen det var snakk om. I vårt prosjekt har vi ikke vært ute etter å ta kommunene på enkeltområder, da vi heller så på eventuelle sårbarheter i det generelle kommunale beredskapsarbeidet. I frykt for at det skulle bli for mye fokus på hvilken kommune det var snakk om, falt valget på å fjerne fokuset fra det helt. Selv om prosjektet hadde vært lettere å etterprøve dersom kommunene stod frem med navn, er vi overbevist om at anonymiseringen har vært til fordel for datainnsamlingen. Ved å informere informantene om at de ble anonymisert, tror vi at de tillot seg å være mer åpne og sårbare om egen sikkerhetsstatus.

I stedet for sitatsjekk valgte vi å sende en transkribert versjon av intervjuet til informantene som ønsket det. «Bruk av lydopptak er regelen, men sitatsjekk brukes sjelden» – det er her forskning skiller seg fra journalistikken, mener Tjora (2021, s. 22). Dette belyser hensikten med å tilby en transkribert versjon, der informantene kan forsikre seg om at vi oppfattet det de sa, korrekt. Dersom informantene *ikke* hadde vært anonymisert, ville vi prioritert sitatsjekker.

5.5.2 Den digitale relasjonen

Som nevnt tidligere gjorde covid-19-pandemien det vanskelig å gjennomføre intervjuene fysisk. Dette gjorde at de mer tradisjonelle problemstillingene som følger av ansikt-til-ansikt-situasjoner ble mindre relevante for vår situasjon. I stedet fulgte andre fordeler og ulemper,

som vil gjennomgås her. Blant fordelene finner vi at intervjuene ikke krevde mye ressurser i form av tid og penger, ettersom det bare var å trykke seg inn på møtelinken og sette av 30-40 minutter per intervju. Det er ikke usannsynlig at dette gjorde terskelen for å delta, litt lavere.

Likevel førte den digitale intervjusituasjonen med seg et par utfordringer. Eksempelvis var det vanskelig å oppnå den stabile, mellommenneskelige kontakten som man ofte opplever ved et fysisk møte. I stedet ble vi tidvis avbrutt av ustabile nettverk, bortfall av lyd og bilde, og andre ting som følger av hjemmekontor-situasjoner. Under enkelte intervju tok dette ganske mye tid å få plass. Dette kan ha medført noe stress for begge parter, ettersom det var avtalt på forhånd at intervjuet skulle ta 30-40 minutter. I verste fall kan dette ha påvirket hvor utfyllende svar informanten kom med, og hvor rask vi gikk over til neste spørsmål. Det er likevel av vår oppfatning at dette ikke påvirket kvaliteten på datainnsamlingen i særlig grad.

Det var også noen mer praktiske utfordringer som fulgte av den digitale intervjusituasjonen. Ett av intervjuene ble gjennomført på kommunikasjonsplattformen Google Meets på grunnlag av problemer med Zoom. Under to av intervjuene gikk vi over til mobilnett på grunn av ustabilt nettverk. Selv om også dette kunne medføre litt stress på oss som intervjuere, er det lite trolig at informasjonen informanten kom med ble påvirket noe særlig av dette. Under et annet intervju var bildet helt borte, slik at det kun var lyd og en svart skjerm. I denne situasjonen var det litt vanskeligere å tolke det informanten sa, og samtidig opprettholde en god dialog. Innledningsvis kan dette ha påvirket samtaleflyten noe, men det tok ikke lang tid før vi hadde vent oss til situasjonen. I to andre intervju var kameravinkelen plassert på siden av informanten, slik at vi hele tiden så informanten i profil. Dette kan også ha vært med på å forstyrre intervjusituasjonen, da det var vanskelig å oppfatte om vedkommende faktisk fulgte med på det som ble sagt eller ei. Under to andre intervju, begge fra samme kommune, var lyden veldig lav. Dette gjorde det svært vanskelig å følge med på det informantene sa underveis i intervjuet. Heldigvis var lyden mye bedre på lydopptaket som ble tatt underveis, slik at ingen informasjon gikk tapt.

Det var også variasjoner angående hvorvidt informanten hadde lest gjennom intervjuguiden og informasjonsskrivet vi hadde sendt ut på forhånd. Det er ikke sikkert at dette hadde noe å gjøre med den digitale gjennomføringen, men det er samtidig logisk å anta at informantene ville stilt mer forberedt dersom intervjuene ble gjennomført ved et fysisk møte. Det var riktignok ingen forutsetning å ha lest skrivet for å forstå spørsmålene i intervjuguiden. Likevel er det naturlig å anta at informantene ville hatt mer forståelse for prosjektets tema, dersom de hadde lest.

6.0 Empiri

I det følgende kapittelet presenteres hovedfunnene fra datainnsamlingen. Kapittelet er delt inn i åtte deler, organisert etter temaene intervjuguiden var strukturert etter. Først presenteres informantenes stillinger og ansvarsområder, og kommunenes beredskapsorganisasjon. I det tredje delkapittelet kommer vi inn på hvordan kommunene gikk frem for å endre og etablere beredskapen, fra henholdsvis IT-informanten og beredskapsinformantens perspektiv, før vi presenterer hvordan de ulike kommunene inkluderte digitale hendelser i planverket. Videre ser vi på hvordan samarbeidet mellom IT- og beredskapsavdelingene var i kommunene, dernest hva informantene selv mente var den beste måten å jobbe med digital risiko på. Vi er også innom hvorvidt kommunene har opplevd noen digitale hendelser selv. Til slutt presenteres informantenes svar på problemstillingen.

6.1 Informantenes stillinger og ansvarsområde

Utvalget til denne studien bestod av 16 informanter fra ti kommuner, derav ti beredskapsinformanter og seks IT-informanter. Som illustrert i tabell 5.4, var det store variasjoner mellom kommunene hva gjelder geografi og innbyggertall. Det var en naturlig sammenheng mellom innbyggertall og størrelsen på kommuneadministrasjon, og det var en påfølgende tydelig sammenheng mellom kommuneadministrasjonens størrelse og beredskapsinformantenes stillingsinstruks. Jo mindre kommuneadministrasjonen var, jo flere oppgaver inngikk i beredskapsinformantenes ansvarsområde.

Alle IT-informantene jobbet utelukkende med IKT, og det var derfor ingen kobling mellom størrelsen på kommunen og IT-informantens stillingsinstruks. Det må for øvrig nevnes at ettersom IT-informanten i de tre små kommune takket nei til å delta, kan det ikke utelukkes at disse hadde ansvarsområder utover IKT.

6.1.1 Beredskapsinformantene

Arbeidsporteføljen til beredskapsinformantene fra de små kommunene varierte mye, men alle hadde til felles at beredskapsarbeid inngikk i deres ansvarsområde. Det var store variasjoner i hvor mye tid de brukte på beredskap, noe som i flere tilfeller ble begrunnet med at andre arbeidsoppgaver ofte gikk på bekostning av beredskapsarbeidet.

Informanten fra K1 var enhetsleder for samfunn og infrastruktur, og hadde ansvar for beredskap. Informanten hadde også med seg en kollega på intervjuet, som var organisasjonssjef med ansvar for informasjonssikkerhet. Informanten fra K2 var enhetsleder for teknisk etat, og beredskapskontakt i kommunen. Arbeidet som beredskapskontakt var ikke en egen stilling, og hadde heller ikke en egen stillingsprosent, men inngikk som et ansvar i det daglige arbeidet. Informanten påpekte at arbeidet med beredskap kommer i tillegg til det øvrige arbeidet, og ble derfor ofte nedprioritert. Informanten fra K3 var kombinert byggesaksbehandler og beredskapskoordinator. Informanten jobbet i avdeling for plan og forvaltning, og påpekte at det brukes for lite tid på beredskap. Informanten fra K4 jobbet med beredskap i brannvesenet i fire kommuner, i tillegg til å være beredskapskoordinator i kommunen som var en del av utvalget (K4). Stillingsprosenten som beredskapskoordinator ble estimert til å være 10%.

Beredskapsinformantene i de to mellomstore kommunene hadde svært varierte arbeidsoppgaver. Informanten i K5 beskrev seg selv som en "potet" i systemet, i likhet med informanten i K4. Vedkommende jobbet i sentraladministrasjonen, med ansvar knyttet til personal, økonomi, regnskap og fellestjenester. Dette var i tillegg til å ha selvstendig fagansvar for beredskapsarbeidet. Beredskapsinformanten fra K6 jobbet også i sentraladministrasjonen, men som etatsjef. Underlagt denne stillingen var økonomi, personal, IKT, arkiv og stab, i tillegg til beredskap. Vedkommende satt også i kommunens kriseledelse.

I de fire store kommunene jobbet informantene med sikkerhet og beredskap på heltid. Beredskapsinformantene fra K7, K8 og K10 jobbet som beredskapskoordinatorer på heltid, og hadde overordnet ansvar for beredskap i kommunen som sitt hovedvirke. Beredskapsinformanten fra K7 jobbet i tillegg med servicetorget. Beredskapsinformanten fra K9 jobbet også med sikkerhet og beredskap på heltid, men hadde stillingstittelen *Informasjonssikkerhetsansvarlig.* Vedkommende jobbet mye med risikovurderinger, men ikke med krisehåndtering. Informanten satt heller ikke i kriseledelsen.

En gjennomgang av beredskapsinformantenes ansvarsområder viser en tydelig sammenheng mellom antall innbyggere, kommuneadministrasjonen størrelse og mengde ressurser satt av til beredskapsarbeid. Det må imidlertid påpekes at K10, som er den største kommunen i utvalget, kun hadde én ansatt som jobbet med beredskap.

6.1.2 IT-informantene

Det var mindre variasjoner i IT-informantenes ansvarsområde. Dette skyldes sannsynligvis at mye av IT-arbeidet som informantene henviste til handlet om daglig drift. Det er verdt å merke seg at det var en sammenheng mellom størrelsen på IT-miljøet og kommuneadministrasjonens størrelse. Dette var riktignok et forventet funn, og syntes ikke å påvirke informantenes ansvarsområde i særlig stor grad.

IT-informantene fra K4, K6, K7 og K10 var alle IT-ledere i deres kommune. Alle hadde i utgangspunktet samme stilling. IT-avdelingen i K10 var vesentlig større enn de andre miljøene. Informanten fra K5 var den eneste av informantene som jobbet eksternt. Vedkommende var daglig leder i et interkommunalt IT-selskap, med fem andre eierkommuner. Det interkommunale selskapet hadde alt av digitalisering, utvikling og drift av kommunenes digitale systemer. Informanten fra K9 var rådgiver på sikkerhetsarkitektur, og hadde spesialisert seg innenfor IKT-sikkerhet

6.2 Kommunenes beredskapsorganisasjon

I en forlengelse av stillingsbeskrivelsene til beredskapsinformantene, ser vi videre på hvordan beredskapsorganisasjonen i kommunene var strukturert. Det fantes mange likhetstrekk mellom kommunenes beredskapsorganisasjon, uavhengig av befolkningsstørrelse eller geografisk lokasjon. Eksempelvis oppga så å si alle kommunene at de opererte ut fra strategisk, operativt og taktisk nivå, uten at dette var noe vi spurte om. Mange dro frem prinsippene om nærhet og likhet til kommuneorganiseringen i fredstid eller normalsituasjon som førende prinsipp for beredskapsorganisasjonens struktur. Hovedregelen for alle kommunene var at kommunedirektøren eller ordføreren var beredskapsansvarlig. Deretter var det beredskapsinformanten som hadde det overordnede ansvaret for å gjennomføre ROS-analyser, sørge for at de hadde en overordnet plan og at det ble gjennomført øvelser. Hos alle kommunene var beredskapsarbeidet underlagt et stabs- eller etatsområde, men det varierte litt mellom hva dette området het. Blant annet var det underlagt stabsområdet miljø, by og stabsutvikling i K9, plan og forvaltning i K3, og sentraladministrasjonen i de to mellomstore kommunene, K5 og K6.

Alle kommunene hadde en overordnet ROS-analyse og beredskapsplan som beredskapsinformanten var ansvarlig for. Deretter var det ledelsen i de underordnede sektorene i kommune som var ansvarlig for å ha en sektorspesifikk plan. Disse planene konsentrerte seg

om de hendelsene som kunne ramme den spesifikke delen av kommunen. Det var riktignok flere av kommunene som slet med gjennomføringen av dette:

> «(...) den er ikke på plass hos alle.» (K2, beredskap)

> «Det er en stor jobb å få folk til å skjønne det her. Å se seg selv i denne røde tråden, og bygge det ned på de ulike nivåene.» (K7, beredskap)

Så å si alle beredskapsinformantene pekte på eget ansvar for å sørge for at det var en rød tråd mellom beredskapsarbeidet på overordnet nivå, og beredskapsarbeidet på sektornivå.

På spørsmålet om strukturen av beredskapsorganisasjonen ble også temaet om kriseledelse tatt opp, som en del av kommunens strategiske nivå. Denne ledelsen var fast etablert hos alle kommunene, med muligheter for å trekke inn enkeltpersoner fra relevante sektorer dersom det oppstod en hendelse som krevde en viss kompetanse. Mange trakk inn eksempler fra koronapandemien her, der kompetanse fra helsesektoren var svært essensielt å få inn i kriseledelsen. I de fleste tilfellene opererte IKT mer på operativt eller taktisk nivå av beredskapsorganisasjonen. Det var likevel gjennomgående hos alle kommunene at IKT ville bli invitert til en eventuell kriseledelse på strategisk nivå dersom det oppstod en større hendelse som krevde IKT-kompetanse. Det var flere av kommunene som nevnte at dette hadde vært en stadig større diskusjon i det siste, og ville fortsette å være det i tiden fremover, etter angrepet i Østre Toten kommune.

6.3 Endring og etablering av beredskap

Spørsmålet om hvordan kommunene gikk frem for å etablere og endre beredskapen ble tolket på litt forskjellige måter av informantene. Grunnet ulik fagkompetanse og ulike fagfelt var det særlige forskjeller mellom beredskapsinformantene og IT-informantene. Dette var riktignok forventet, da vi på forhånd antok at beredskapsinformantene kunne si noe om systematikken og metoden i beredskapsarbeidet, mens IT-informantene kunne si noe om hvordan de var involvert i prosessen.

6.3.1 Beredskapsinformantene

For beredskapsinformantene fremstod spørsmålet som relativt konkret, da ROS-analyser og utarbeidelse av beredskap og beredskapsplanverk inngikk i alle informantenes portefølje. Det bør imidlertid nevnes at det i flere tilfeller var uklart for informantene hvorvidt beredskap henviste til håndtering av en hendelse, eller det forebyggende og forberedende arbeidet. I alle

tilfellene der dette var uklart, forklarte vi at vi siktet til beredskap som et forberedende og forebyggende arbeid, noe alle informantene var kjent med.

Gjennomgående for alle beredskapsinformantene var et fokus på at ROS-analysene lå som grunnlag for endring og etablering av beredskap, i henhold til lovene og forskriftene. Uavhengig av innbyggertall og størrelse på kommuneadministrasjon svarte beredskapsinformantene mer eller mindre det samme hva gjaldt forhold mellom ROS-analyse og beredskapsplanverk.

> «Vi starter jo alltid med å lage en ROS-analyse, og så gir den grunnlag for beredskapsplanene. Så det ene angir det andre.» (K1, beredskap)

> «Vi har jo et lovverk som sier at vi skal regulere hvert fjerde år, er det vel. Vi starter jo all revidering med å ta utgangspunkt i en overordnet ROS-analyse.» (K6, beredskap)

K8 var den eneste kommunen som påpekte at de også tar i bruk andre verktøy, i tillegg til ROS-analyser. Et eksempel var beredskapsanalyser, der identifisering av dimensjonerende hendelser er en sentral del av analysen. Selv om flere av informantene refererte til dimensjonerende hendelser, ble det ikke påpekt at dette var i sammenheng med beredskapsanalyser. Eksempelvis ble dimensjonerende hendelser omtalt slik:

> «Når vi har funnet disse i ROS-analyse, lager vi planer for hva vi skal gjøre for enten å redusere sannsynligheten for at dette inntreffer, eller konsekvensen, i et fireårsperspektetiv. Basert på de 20 hendelsen vi har, lager vi beredskapsplanen. Og da har vi tiltakskort for hver av hendelsene.» (K6, beredskap)

Vi fant store variasjoner i hvorvidt digitale hendelser var en del av de dimensjonerende hendelsene. Beredskapsinformanten fra K6 utdypet at to av disse 20 hendelsene var digitale uønskede hendelser. Beredskapsinformanten fra K4 påpekte at de hadde diskutert en IKT-relatert hendelse, men at den hadde blitt tatt ut da den ikke skåret høyt nok på sannsynlighet, fare og konsekvens. Beredskapsinformanten fra K2 sa at de hadde omtrent åtte dimensjonerende hendelser, men at ingen av de gikk på IKT. Beredskapsinformanten fra K10 belyste utfordringen med å ikke inkludere IKT-relaterte hendelser som dimensjonerende hendelser slik:

> «Vi har i liten grad etablert den kommunale beredskapen for å svare på IKT-utfordringer fordi det eksterne apparatet vårt har håndtert det innenfor et fornuftig tidsvindu, og så har vi vært tilbake der vi skal. Problemet oppstår jo hvis vi blir uten mobilnett i en uke, skjønner du?» (K10, beredskap)

Flere informanter påpekte at det var varierende kvalitet på ROS-analysen, og at koblingen mellom ROS-analyse og beredskapsplanverk i mange tilfeller burde forbedres. Det var særlig to forklaringer på dette; at det var mangelfull kompetanse nedover i avdelingene på risikoanalysearbeid, og at ROS-analysen var utdatert. Alvorligheten av disse utfordringene varierte mellom kommunene, som illustrert under:

> «Vi har jo beredskapsplan som er tuftet på ROS-analyse. Der vi fikk vi litt pepper under siste tilsyn. Den var litt tynn og litt gammel.» (K5, beredskap)

Det mest alvorlige tilfellet som ble avdekket under intervjuene, var i K3. Der var ROS-analysen 10-11 år gammel, som medførte at beredskapsplanen bygde på utdaterte forutsetninger. I tillegg var selve ROS-analysen blitt borte, som resulterte i at det eneste beredskapsinformanten kunne si om ROS-analysen var det som stod i beredskapsplanen. I tilsynsrapporten til K2 fant vi derimot et enda mer kritisk tilfelle enn dette. Her var det ikke gjennomført en ROS-analyse på nærmere 20 år. Dette kom ikke frem under intervjuet.

Da beredskapsinformanten fra K7 snakket om ROS-analyser på avdelingsnivå, ble det påpekt:

> «De har jo gjort det på papiret i alle år, men det har kanskje ikke vært så systematisk. Litt tilfeldig i de ulike avdelingene, hva de har fokus på.» (K7, beredskap)

Det ble videre henvist til at økonomi, kompetanse og ledelse er viktige faktorer for gjennomføring av risikoanalyser, og hvordan de blir fulgt opp. For å løse denne utfordringen ble det forklart at sikkerhetskultur og kontinuerlig arbeid er viktig.

Hva gjelder fokus på IKT i risikoanalyser, var det mange forskjellige svar. I noen tilfeller ble IKT vurdert fordi det var nedfelt i fylkes-ROS, mens i andre tilfeller handlet det om at IT-miljøet hadde spilt inn sine vurderinger. Det var ingen beredskapsinformanter som eksplisitt påpekte at IKT-relaterte hendelser blir inkludert på grunn av sannsynlighet eller konsekvenspotensial. En interessant bemerkning ble gjort av IT-informanten fra K4, som sa følgende:

> «Men én av de tingene jeg la merke til der, egentlig, er jo det at det blir på en måte forutsatt i alt det andre at de digitale systemene skal være oppe å gå i denne ROS-analysen. Det var litt foruroligende, egentlig.» (K4, IT).

6.3.2 IT-informantene

IT-informantenes svar på spørsmål om endring og etablering av beredskap, dreide seg i stor grad om hvordan deres arbeid med risiko stod i forhold til det overordnede kommunale arbeidet. Fire av de seks IT-informantene var tilsynelatende enige i at det var mangler knyttet til deres arbeid inn mot endring og etablering av den overordnet beredskapsplanen.

> «Altså, vi jobber jo med sikkerhet. Vi har jo egentlig prøvd å løfte det litt mer opp på agendaen nå.» (K7, IT)

> «Sånn som jeg ser det har ikke IKT drift vært flinke nok til å koble sine planer mot den overordnede planen. (...) Det har jo på mange måter vært overlatt til IT å ha beredskapsplaner for IT-systemer. Det har i mindre grad vært tenkt på at det må bygges en beredskap for disse tingene ute i organisasjonen når feilen er der.» (K9, IT)

> «Vi jobber mye på systemnivå og løsningsnivå. Områdevis, da, på en måte. I forhold til risikovurderinger og beredskap. Men det er ganske lite koblet inn mot det overordnede, egentlig. (...) Jeg opplever det som to veldig separate prosesser som egentlig lever hvert sitt liv.» (K10, IT)

Informantene la likevel vekt på at det var risikoanalyser som lå til grunn for IKT drifts beredskapsplaner, men at heller ikke dette var godt nok spilt inn til det overordnede planverket.

Det var dermed tydelig at det, fra IT-informantenes ståsted, var noen uklarheter knyttet til hvordan deres sektorspesifikke risikoanalyser og beredskapsplaner skal tas hensyn til av beredskapsansvarlige. I flere tilfeller ble det lagt vekt på at dette var viktig, ettersom IT er en integrert del av alle kommunenes virksomhetsområder. IT-informanten fra K9 foreslo en potensiell løsning på denne utfordringen:

> «Vi trenger tydeligere verdivurderinger i eventuelle hendelser for å avdekke hva som er de viktigste systemene for organisasjonen. Vi kan jo sitte og mene det og prøve å knytte det opp mot vår målsetting som ligger i den overordnede beredskapsplanen, men vi vil gjerne ha beredskapssjefene med på banen slik at de kan lage en prioriteringsliste og få det forankret helt på toppen. Og så blir jo dette input i våre lokale beredskapsplaner og ha fokus på det viktigste først.» (K9, IT)

I motsetning til de andre IT-informantene, påpekte informanten i K6 at IT-miljøet der i større grad var involvert i utarbeidelsen av det overordnede beredskapsplanverket.

> «De analysene vi gjør blir en del av den totale beredskapsplanen i kommunen. Der det er innenfor vårt fagområde, så er det det [interne analyser] vi leverer til den helhetlige ROS-analysen for all beredskap i kommunen. Der er det en egen beredskapsplan som blir utformet.» (K6, IT)

De utfordringene som flere av informantene påpekte i forbindelse med ROS-analysene, kan underbygges av Statsforvalterens tilsynsrapporter. En gjennomgang av tilsynsrapportene viste at fem av ti fikk avvik på gjennomføringen og kvaliteten av ROS-analysen. Disse fem var K2, K3, K5, K6 og K9. I disse kommunene var altså ikke kravene i forskrift om kommunal beredskapsplikt eller sivilbeskyttelsesloven oppfylt. I tillegg fikk ytterligere to kommuner merknad (K7 og K10). Mer konkret gikk avvikene og merknadene på at ROS-analysen ikke var detaljert nok, at den ikke var oppdatert, eller at beredskapsplanen ikke var tuftet på en helhetlig og oppdatert ROS-analyse.

6.4 Omtalen av digitale uønskede hendelser i beredskapsplanverket

For å kunne svare på spørsmålet om hvordan beredskapsarbeidet i kommunene integrerer digitale uønskede hendelser, ønsket vi å spørre informantene om hvorvidt de var omtalt i beredskapsplanen i det hele tatt. Svarene vi fikk spriket stort. Likevel fant vi likheter mellom kommuner som var av samme størrelse. Presentasjonen av funnene gjenspeiler derfor dette, hvorpå vi har delt inn kapittelet etter kommunestørrelse.

6.4.1 I de små kommunene

Digitale uønskede hendelser ble ikke nevnt i beredskapsplanen til noen av de fire små kommunene.

To av fire (K1 og K3) brukte interkommunale selskap som fungerende IT-avdeling for kommunene. I begge disse kommunene fikk vi kun intervjuet beredskapsinformanten. Informanten fra K1 sa at kommunen «*i liten grad*» jobbet med digitale systemer selv, annet enn at det var omtalt noen digitale uønskede hendelser i den overordnede ROS-analysen i kommunen. Her var dermed kommunen helt avhengig av at de eksterne leverandørene hadde beredskapsplaner som fungerte for dem, dersom det skulle bli nødvendig.

Tilsvarende var tilfellet i K3, der det interkommunale samarbeidet startet i 2006. Det var også i denne kommunen at beredskapsplanen ikke var oppdatert på 10-11 år, og ROS-analysen fra samme tid var forsvunnet. Den overordnede beredskapsplanen, som var det eneste som fantes igjen av dokumentasjon, nevnte ikke noe om digitale uønskede hendelser.

> «Men om 1,5 år, hvis vi snakkes igjen da, så håper jeg vi kan presentere dere for hvordan vi har tenkt å løse den type utfordringer.» (K3, beredskap)

Bortfall av ekom som en digital uønsket hendelse var inkludert i ROS-analysen hos K4, men ikke i den overordnede beredskapsplanen. Dette fordi scenarioet som omhandlet bortfall av ekom ble rangert som nummer fem, av totalt ni hendelser, da de vurderte sannsynligheten for at scenarioene kunne inntreffe. Det var også bestemt på forhånd at beredskapsplanen kun skulle inneholde fire dimensjonerende hendelser. ROS-analysen lå likevel som et bilag til planen, og var utarbeidet i samarbeid med flere sektorer i kommunen, deriblant IT-avdelingen. IT-informanten i K4 hadde ikke kjennskap til beredskapsplanen i detalj, og kunne dermed ikke svare på om planen potensielt kunne fungere som et verktøy for å håndtere digitale hendelser.

I K2 var ikke digitale hendelser omtalt i beredskapsarbeidet i det hele tatt.

6.4.2 I de mellomstore kommunene

Også i K5 var det lite å se av digitale uønskede hendelser i beredskapsplanleggingen. Ifølge beredskapsinformanten ble tilfeller med bortfall av nett og kommunikasjon kun nevnt som bisetninger når det var snakk om *generell infrastruktur*. Hendelser som hacking ble ikke nevnt i det hele tatt. IT-informanten i K5, som var den eneste informanten vi snakket med fra et interkommunalt selskap, mente at digitale uønskede hendelser er i ferd med å bli såpass viktig at de vil havne i en egen kategori av beredskapsarbeidet. Vedkommende kunne imidlertid heller ikke si noe om digitale hendelser var inkludert i planen til kommunen.

Statsforvalteren gjennomførte et tilsyn med K6 sitt beredskapsarbeid i 2017. I rapporten ble det kommentert at kommunen i større grad måtte se på hvordan ulike risiko- og sårbarhetsfaktorer påvirket hverandre. Her ble bortfall av tele- og IKT-tjenester nevnt som et konkret eksempel som K6 måtte kartlegge bedre. Sannsynligvis er denne tilsynsrapporten en av grunnene til at K6 var blant de få kommunene som hadde inkludert digitale hendelser i beredskapsplanen. Planverket her tok for seg én hendelse som omhandlet bortfall av IKT og kommunikasjon som følge av strømbrudd, og én hendelse som omhandlet hacking. IT-informanten i denne kommunen understreket at:

> «Det er ingen som unngår det [digitale hendelser], det er bare noen som ikke ønsker å fortelle det. For alle blir rammet.» (K6, IT)

Kommunen vektla videre gode rutinebeskrivelser for å håndtere hendelser, og gode backup-løsninger som fungerer når det trengs, som viktige ting å ha på plass for å være i stand til å håndtere digitale uønskede hendelser.

6.4.3 I de store kommunene

Digitale uønskede hendelser var omtalt i beredskapsplanen hos kun halvparten av de fire store kommunene i utvalget. Disse var K8 og K10.

I K8 ble tre hendelser som gikk på det digitale inkludert: tilsiktede handlinger, bortfall av kraftforsyninger, og bortfall av kommunikasjon. Her fantes det både aksjonskort på strategisk nivå, i tillegg til lokale planer på virksomhetsnivå. Ifølge beredskapsinformanten hang dette tett sammen med den røde tråden kommunen fokuserte på å ha, der lokale planer skal tufte på, og henge sammen med, den overordnede beredskapsplanen. Selv om bortfall av kraftforsyning var inkludert som en digital hendelse, hadde ikke kommunen en løsning på hvordan opprettholde en funksjonell digital infrastruktur om denne hendelsen inntraff.

> «Det er ikke lagt opp til at vi skal kunne drifte, eller at vi kan ha serverne stående på, hvis vi mister strømmen» (K8, beredskap)

Beredskapsinformanten i K10 påpekte at planene lå hos de eksterne leverandørene som kommunen hadde outsourcet mye av IKT-tjenestene til. Kommunen selv hadde scenarioer for tap av ekom og tap av strøm, fordi kommunen mente det var disse scenarioene som ville resultere i samfunnskollaps etter få døgn. IT-informanten i K10 mente at planverket var ganske tynt, og at det hadde vært for lite fokus på IKT som et område som kan forårsake store konsekvenser for andre i kommunen. Denne oppfatningen gjenspeilet seg noe hos beredskapsinformanten da vedkommende sa at det gjenstod et ganske omfattende arbeid med å finne ut av nøyaktig hvor sårbar kommunen var for digitale uønskede hendelser.

I K9 ble det forklart at beredskapsplanen *«ikke er fersk»*, og at ingenting av det som var nevnt i den overordnede planen var knyttet til IT. I ROS-analysen var det likevel nevnt fem ulike IKT-hendelser: hendelser knyttet til server og utfall, skade/brudd på fiber og løse linjer, serverutfall på rådhuset, eksternt dataangrep og bortfall av kritisk infrastruktur i kommunen. At det var inkludert i ROS-analysen betød likevel ikke at det var tilstrekkelig. Dette ble bekreftet da vi spurte IT-informanten i kommunen om planverket var et nyttig verktøy for å håndtere digitale hendelser:

> «Nei. Vi er ikke der.» (K9, IT)

Beredskapsinformanten var riktignok overbevist om at det ville foretas en ny vurdering av de digitale hendelsene i neste evalueringsrunde.

Tilsvarende var tilfellet i K7. Her var et hacking-scenario gjennomgått i ROS-analysen, men likevel ikke nevnt i beredskapsplanen. IT-informanten kritiserte dermed egen plan for ikke å være presis nok når det kom til metodikken og tiltakene som burde iverksettes for å håndtere den aktuelle hendelsen. Planverket var bedre på selve organiseringen, å få riktig bemanning på plass, og å tydeliggjøre ansvarsområdene til enkeltpersoner. Da vi spurte informantene her om planverket kunne brukes til å håndtere en hendelse lik den i Østre Toten, ble det svart:

> «Nei, det gjør det ikke. (...) Men nå er det sånn at [kommunenavnet] er veldig godt beskyttet. En Østre Toten-hendelse vil aldri skje her.» (K7, IT)

Oppsummert er det syv av ti kommuner som ikke omtaler digitale uønskede hendelser i den overordnede beredskapsplanen. Dette gjelder *alle* de små kommunene (K1-K4), *én* av de to mellomstore (K5), og *halvparten* av de fire store (K7 og K9). Fire av dem påpekte riktignok at de har nevnt enkelte digitale hendelser i ROS-analysen, og én hadde nevnt det som bisetninger i planverket. For to av de seks IT-informantene som var inkludert i utvalget, var ikke innholdet i beredskapsplanen kjent for vedkommende. I de tre kommunene som hadde inkludert digitale hendelser, var det tydelig lagt mest fokus på hendelser som bortfall av strøm og bortfall av ekom, da dette var hendelser alle tre hadde inkludert i planverket. Dette var også de to hendelsene som var nevnt som bisetninger i planverket hos K5, uten at det forelå noen konkret plan for hendelsene. Det var kun de to kommunene på Østlandet som nevnte at de hadde inkludert hackerangrep som hendelse i beredskapsplanen.

En av årsakene til at digitale uønskede hendelser ikke er omtalt og beskrevet i de overordnede beredskapsplanene, kan finnes i Statsforvalterens tilsynsrapporter. Her fikk seks av kommunene avdekket avvik på at den overordnede beredskapsplanen ikke bygget på en oppdatert og helhetlig ROS-analyse. Disse var K2, K3, K4, K5, K6 og K9. K7 og K10 hadde også fått merknad på dette. Dette kan påvirke inkluderingen av digitale uønskede hendelser. Dersom beredskapsplanen ikke tufter på en oppdatert ROS-analyse, vil ikke risikoer som følger av digitaliseringen de siste årene gjenspeiles i planverket.

6.4.4 Forskjell i håndtering

Etter å ha vært innom de dimensjonerende hendelsene i planverket, spurte vi informantene om hvorvidt det er noen forskjell i håndteringen av digitale og fysiske uønskede hendelser. Med unntak av åpenbare forskjeller i de konkrete tiltakene som brukes i håndteringen, var nærmest

alle beredskapsinformantene enige om at det, rent prinsipielt, ikke er forskjell i håndteringen. Dette kan illustreres med de følgende sitater:

> «I prinsippet ikke, slik jeg ser det. Kriseledelsen håndterer saken og knytter sammen de fagfolkene man trenger for å løse hendelsene. Tiltakene blir jo annerledes da (...) Men sånn som vi angriper fra starten av så er det ikke noen store forskjeller på prinsippene.» (K1, Beredskap)

> «Nei. Det er jo et brudd i de daglige rutinene. Vi kan ikke opprettholde daglige rutiner. Vi må finne andre løsninger. Så prinsippene må jo være akkurat det samme.» (K3, Beredskap)

En beredskapsinformant hadde imidlertid et litt annet syn på forskjellene i håndtering av en digital uønsket hendelse versus fysiske:

> «I bunn og grunn blir det stort sett IT som er nødt til å håndtere det. Vi andre kan ikke gjøre noe, vi må jo bare skru av dataen.» (K2, Beredskap)

De fleste IT-informantene var også enige i at det ikke var store prinsipielle forskjeller i håndteringen av en digital versus fysisk uønsket hendelse. De trakk likevel frem noen forskjeller i håndtering, i større grad enn beredskapsinformantene. IT-informanten fra K4 henviste til at en spesiell utfordring med en digital uønsket hendelse er at det kan være store kommunikasjonsproblemer, fordi plattformer kan være nede. IT-informanten fra K9 henviste til at det ikke er store forskjeller fra kriseledelsens ståsted, men at de ikke hadde gode nok planer for blant annet *løsepengevirus*. En av årsakene til dette var at planverket var fragmentert. IT-informanten fra K10 var enda mer kritisk når det gjaldt forskjellen mellom håndtering av fysiske og digitale uønskede hendelser:

> «Ja [=stor forskjell], selv om jeg ikke har hatt så mange hendelser. Jeg tror vi er mer drillet på å håndtere tradisjonelle hendelser enn IKT-relaterte hendelser. Fordi de tradisjonelle hendelsene har eksistert litt lenger enn hendelser for IKT-området.» (K10, IT)

6.5 Samarbeidet mellom beredskap og IKT

Vi fikk mange ulike svar da vi stilte spørsmål om samarbeidet mellom beredskap- og IT-avdelingen. Det var gjennomgående at det var et godt samarbeid, men det var ulikt hvorvidt samarbeidet var formalisert, hvor ofte de hadde kontakt, samt i hvilken grad IT-miljøet ble inkludert i kommunens beredskapsarbeid. Det var for øvrig litt utfordrende fra vår side å forstå hvorvidt *godt samarbeid* betød at det var et *hyggelig* samarbeid, eller om det betød et godt

faglig samarbeid. Det må derfor påpekes at begrepet *godt* ikke nødvendigvis var et veldig forklarende begrep.

6.5.1 Fra beredskapsinformantens ståsted

Hovedoppfatningen vi satt igjen med var at beredskapsinformantene hadde et bedre inntrykk av samarbeidet mellom beredskap- og IT-miljøet enn det IT-informantene hadde. Fire av beredskapsinformantene påpekte at samarbeidet med IT-miljøet både er regelmessig og hensiktsmessig:

> «Jeg tror ikke samarbeidet er noe dårligere med [navn på interkommunalt IT-samarbeid] enn det er med våre egne etater.» (K1, beredskap)

> «IT ligger en del innunder mitt ansvarsområde. Jeg har en IT-sjef som rapporterer til meg.» (K6, beredskap)

> «Vi har et godt samarbeid grunnet organiseringen (...) Det som er så bra med den måten vi er organisert på nå i forhold til hvordan det var før er jo at vi har fått en stab som er mer dedikert til område, teknologi og innovasjon. Det hadde vi ikke før.» (K9, beredskap)

> «Samarbeidet er godt. Vi har jevnlige møter.» (K10, beredskap)

Sistnevnte utdypet imidlertid at samarbeidet med IT-miljøet var godt, ikke fordi det var et formalisert samarbeid, men fordi vedkommende var god venn og kollega med lederen av IT-avdelingen.

De seks andre beredskapsinformantene var i større grad kritiske til samarbeidet, og påpekte at samarbeidet ikke var særlig formalisert og faglig.

> «IT som interkommunalt samarbeid har jeg minimalt å gjøre med.» (K3, beredskap).

> «Ikke spesielt formelt samarbeid.» (K5, beredskap)

> «Det kan selvfølgelig bli bedre, det ser jeg.» (K7, beredskap)

6.5.2 Fra IT-informantens ståsted

IT-informantene var tilsynelatende mer kritiske til samarbeidet med beredskapsmiljøet.

> «Det er ingen formell inkludering av IT i beredskapsarbeidet.» (K4, IT)

> «Lite daglig samvirke (...) Det kunne hjulpet oss med å utvikle egne planer hvis det hadde vært tettere samarbeid mellom overordnede og vår virksomhet.» (K9, IT)

Flere påpekte blant annet at det var vanskelig å få gjennomslag for beredskapsarbeid på et såpass teknisk område, som ofte ble oppfattet som utilgjengelig av samfunnsviterne i beredskapsmiljøet. Dette handlet til syvende og sist om forståelse for hverandres fagfelt, noe vi kommer nærmere inn på nedenfor. På spørsmål om hvorvidt beredskapsmiljøet anser digital risiko som en naturlig del av beredskapsarbeidet svarte samme informant som overfor, følgende:

> «Det er nok noe som har måttet modnes over tid. Det har nok bedret seg, men det kunne nok fortsatt vært bedre.» (K4, IT)

Den mest kritiske kommentaren kom fra den største kommunen, som også viser at det ikke var noen korrelasjon mellom størrelse på kommunen og mengde samarbeid, samt kvalitet på samarbeidet.

> «Jeg vil være veldig ærlige med dere nå, jeg prøver ikke å rosemale dette. Det er ikke så veldig god 'connection' mellom hverdagen og det som er overordnet. (...) Jeg opplever det som to veldig separate prosesser, som egentlig lever hvert sitt liv.» (K10, IT)

Utfordringer og manglende formalisering hva gjelder samordning og samarbeid kan underbygges av Statsforvalterens tilsyn med kommunal beredskapsplikt. Seks av kommunene hadde fått avvik eller merknad på beskrivelsen av samordningen av ressurser, eller sammenhengen mellom overordnet og etatsspesifikke planer. Kommunene med avvik var K3 og K5, mens K1, K6, K7 og K9 hadde fått merknad. Dette passer overens med de utfordringene informantene ytret hva gjaldt samordning mellom ulike fagressurser i kommunen.

6.5.3 Tverrfaglig forståelse

I de tilfellene det ble påpekt at de to miljøene samarbeidet lite, ble forståelse for hverandres fagfelt trukket frem som både en utfordring og en forklaring. Dette ble også trukket frem som en utfordring hos de kommunene som beskrev samarbeidet som velfungerende og godt. Faktum at IT- og beredskapsarbeid er to svært forskjellige fagfelt legger tilsynelatende noen begrensninger på det tverrfaglige samarbeidet. Følgende sitater illustrerer hva de fleste IT-informantene mente om tverrfaglig forståelse:

> «Det som kanskje er den store sårbarheten i en stor organisasjon, er at det ikke er alle som tenker sikkerhet og sitt ansvar som databehandler i alle tjenesteområdene.» (K6, IT)

> «Jeg skulle ønske at ledere på andre sektorer, og innenfor helsesektoren, kunne vært dyktigere på IKT, og hatt mer forståelse.» (K7, IT)

> «Vi tenker nok altfor tradisjonelt og si, litt gammeldags i forhold til det her. (...) Det er altfor lite forståelse for IKT-komponenters rolle i ulike ting.» (K10, IT).

Enkelte beredskapsinformanter problematiserte det samme, nemlig mangel på IKT-kompetanse i beredskapsmiljøet.

> «Kanskje få en forståelse opp i ledelsen om at dette [IT] er beredskapsarbeid. Ofte tenker vi på beredskap som et ras eller værhendelse (...) Så man har kanskje ikke hatt en tradisjon for å tenke om dette på samme måte.» (K7, Beredskap)

> «Vi har forbedringspotensial. Jeg tror at stadig flere områder og sektorer blir digitalisert. Med den digitaliseringen følger en økt sårbarhet. Det er så mye stammespråk ute og går, at det kan skape en fremmedgjøring og distanse hos kommunale toppledere som ikke har digital bakgrunn.» (K10, beredskap)

Det virket derfor utfordrende for beredskapsmiljøet å behandle digitale uønskede hendelser og digital risiko på lik linje med andre risikomomenter, fordi de manglet kompetanse på området. Utfordringen var imidlertid ikke kun at beredskapsmiljøet manglet IKT-kompetanse, men også motsatt. Flere beredskapsinformanter påpekte nemlig et behov for å utvikle IT-miljøets forståelse av beredskap.

> «IT kan sitt område. Beredskap, når det gjelder hele kommunen, har ikke IT kompetansen på.» (K3, Beredskap)

> «IT har mye å lære på beredskapsarbeid (...) veldig lite tradisjon å jobbe med det.» (K9, Beredskap)

6.6 Mest hensiktsmessig måte å håndtere digital risiko

Da vi spurte informantene om hva de anså som den mest hensiktsmessige måten å håndtere digital risiko på, var det gjennomgående i alle intervjuene at svarene gjerne kom i stikkordsform. Eksempelvis som i intervjuet med en av de store kommunene:

> «Gode ROS-analyser, tydeligere avklaringer av roller – det er ekstremt viktig, gode tiltakskort, altså gode forberedelser i beredskapsplanen. Rolleavklaring, varslingsliste, alt det der. Og det jeg sa i stad: øving, øving, øving.» (K9, beredskap)

Dermed så vi muligheten til å sette opp disse stikkordsvarene i en tabell, med fokus på de punktene som gikk igjen i flere av intervjuene. Tabellen er ikke ment som en rangering av de beste svarene, men det gir en indikasjon på hvilke tiltak som lå intuitivt hos informantene. At

visse punkt ble utelatt av enkelte kommuner betyr med andre ord ikke nødvendigvis at det ikke var viktig for kommunen, da vi ikke stilte oppfølgingsspørsmål vedrørende dette.

	K1 S	K2 N	K3 V	K4 M	K5 S	K6 Ø	K7 N	K8 Ø	K9 V	K10 M
ROS-analyser, planverk	x		x	x		x			x	
Tydelig avklaring av roller								x	x	
Tiltakskort						x		x	x	
Gode forberedelser					x	x	x		x	
Øving							x		x	x
Felles/delt situasjonsbilde							x		x	x
Involvere ledelsen				x					x	
Opplæring av ansatte					x		x			x
Anskaffelser					x	x				
Intern dialog		x	x	x			x	x		x
Ekstern dialog	x					x	x	x		x
Interkontroll/oppfølging					x	x				
Jobbe kontinuerlig	x			x		x		x		
Gode etablerte rutiner				x		x				x
Se system i sammenheng		x	x	x				x		

Tabell 6.1: Mest hensiktsmessig måte å håndtere digital risiko, i stikkordsform

Tabell 6.1 gir også en rask repetisjon av størrelsen til kommunen (markert i farger), og hvilken landsdel kommunen ligger i (S, N, V, M, Ø). Som vi ser, er det ingen spesiell korrelasjon knyttet til kommunenes svar og landsdelen kommunen ligger i. Den eneste korrelasjon vi fant mellom kommunestørrelsen og svaret de kom med, var at de større kommunene hadde en tendens til å ramse opp flere punkter enn de mindre.

Felles for flere av kommunene var vektleggelsen av samarbeid, både internt og eksternt. I tabellen ser vi at det er dette punktet som oftest ble nevnt. Flere så her et behov for å gå sammen i kommunen for å se hvordan systemene påvirker hverandre, for å få et fokus på hvordan alle sektorene i kommunen er en del av et større og mer komplekst bilde. Tilsvarende ble det da også viktig at man fikk frem det ansvaret alle de ansatte i kommunen hadde for å ta hensyn til dette, og den medfølgende sårbarheten. Å jobbe kontinuerlig og proaktivt var et nøkkelord hos mange, uten at det ble utdypet noe særlig. Det var også enkelte av de små kommunene som viste tydelig tegn til usikkerhet rundt dette spørsmålet. Noen påpekte at det ikke fantes en "beste" måte for å håndtere digital risiko på, mens andre sa de kunne lite for lite om feltet.

> «Jeg har jobbet for lite med det (...), men jeg ser helt klart at fagområdene IT og beredskap må arbeide tettere sammen.» (K3, beredskap)

> «Det vil jeg gjerne henvise til IT, det er ikke et fagfelt jeg kan noe om.» (K4, beredskap)

I K4 svarte også IT-informanten:

> «Jeg tenker jo at det er en del kompetansehull rundt omkring, folk skjønner kanskje ikke helt hvordan det henger sammen.» (K4, IT)

Denne usikkerheten og mangelen på kompetanse på området belyser behovet for intern dialog, opplæring og samarbeid, som ble påpekt av flere informanter. Flere nevnte viktigheten av å få ledelsen til å forstå hvor viktig beredskapsarbeidet var for kommunen, slik at dette fokuset kunne spre seg videre til de forskjellige sektorene som skulle utforme lokale beredskapsplaner på eget felt. Syv av ti kommuner sa de syntes det hadde vært utfordrende å få ledelsen til å forstå viktigheten av å jobbe kontinuerlig med beredskapsarbeidet. Fire av ti sa de syntes det var vanskelig å få de øvrige ansatte i kommunen til å se viktigheten av at også de tenkte på sikkerheten. Samtlige sa riktignok at de jobbet med å spre denne forståelsen.

Å få med ledelsen på laget ble også trukket frem som et viktig tiltak for å skaffe mer ressurser til å jobbe med beredskap, som flere av de mellomstore og store kommunene nevnte som utfordrende. Som nevnt i 6.1.1 var det kun én ansatt i K10 som jobbet med beredskap. IT-informanten i denne kommunen påpekte at det var lite økonomiske midler som ble avsatt til å gjennomføre analyser og øve på aktuelle hendelser som kunne ramme kommunen.

> «Det er lite ressurser og midler, ikke sant. Det finnes ikke budsjett for noe på det området der. Det må håndteres innenfor de vanlige, andre, budsjettpostene, hvis ansvar er fordelt rundt om i kommunen. Det brukes veldig lite penger og ressurser på beredskapsarbeidet i kommunen.» (K10, IT)

Når det gjaldt økonomiske midler for å håndtere digitale hendelser, hadde K6 riktignok funnet en løsning de mente fungerte godt for dem. Når budsjettene til kommunen utarbeides, settes det av en pott til digitalisering som et felles satsingsområde for kommunen. Dersom IT-avdelingen senere skulle ha behov for å iverksette sikkerhetstiltak som krevde økonomiske midler, ble det tatt av denne potten. Selv om ikke informantene nevnte noe om hvorvidt potten var stor nok for behovet, var det et tydelig forebyggende tiltak kommunen gjorde for å imøtekomme den digitale sårbarheten.

6.6.1 Tanker om eksterne samarbeid

Av alle de ti kommunene vi snakket med, var det hele syv av dem som nevnte at de allerede var med i et større interkommunalt samarbeid med andre kommuner, eller benyttet seg av eksterne leverandører. De syv var K1, K3, K4, K5, K8, K9 og K10. K6 var også i gang med å

vurdere en slik løsning. Med andre ord gjaldt dette kommuner av både liten, mellomstor og stor størrelse, fra alle landsdeler – med unntak av de to kommunene fra Nord-Norge. IT-informanten fra K5, som jobbet i et slikt IKS, trakk frem flere fordeler med å være en del av et større samarbeid. Blant annet ble det sagt at:

> «Fordelen med et interkommunalt selskap er at du kan få tilgang til et større fagmiljø. Mange små kommuner kan ikke sette av ressurser som er nødvendig for å få dette til å gå rundt på en bra måte. (...) Når du blir mindre enn [navn på annen kommune med cirka 20 000 innbyggere], koster det mer enn du føler du får tilbake. Da vil du alltid ha kampen om omsorgsplasser, skoleplasser, og lignende.» (K5, IT)

Likevel virker det ikke som at det bare er de små kommunene som vil ha fordel av å samarbeide om IKT-sikkerheten.

> «Jeg tror nok hvert fall store kommuner i fremtiden blir helt avhengig av å kunne kjøpe tjenester, være en del av et høyteknologisk miljø for å forebygge, avverge og ha bistand til å håndtere IT-hendelser i fremtiden.» (K10, beredskap)

IT-informanten i K10 ga riktignok ikke inntrykk for å være helt enig med kollegaen sin. På spørsmålet om hva vedkommende mente var den mest hensiktsmessige måten å håndtere digital risiko, ble det svart:

> «Det går i hvert fall ikke an å outsource, eller overlate til noen andre. Det er viktig budskap. (...) Det er vi som må ha ansvaret, enten vi vil eller ei (...). Den eneste måten vi kan leve opp til å ha et sånt ansvar, er at vi er kompetente nok. Og at vi har rom i hverdagen innenfor relevante domene så man faktisk får jobbet med det.» (K10, IT)

Samtidig som disse to utsagnene fra informantene i K10 illustrerer diskusjonen rundt interkommunale samarbeid, tydeliggjør de også behovet for å ha en felles forståelse av kommunens risikobilde.

6.7 Egenopplevde digitale uønskede hendelser

Responsen vi fikk på spørsmål om hvorvidt kommunen hadde opplevd noen digitale uønskede hendelser, viste tydelig at dette ikke var et fremmed konsept for informantene. Samtlige informanter påpekte at de hadde hatt digitale uønskede hendelser, men med ulik alvorlighetsgrad. Konseptet *digitale uønskede hendelser* favner bredt, ettersom det ble redegjort for svært mange forskjellige hendelser. Det var også bemerkelsesverdig at alle beredskapsinformantene, med unntak av én, hadde kunnskap om digitale uønskede hendelser som hadde inntruffet tidligere. Dette gir en indikasjon på at digitale hendelser ikke er helt

avgrenset til IT-avdelingen. Ingen av kommunene hadde imidlertid opplevd digitale uønskede hendelser der den kommunale kriseledelsen hadde blitt satt, og således hadde alle hendelsene blitt håndtert av IT-miljøet. Flere indikerte likevel at om hendelsene hadde manifestert seg med sitt fulle potensiale kunne konsekvensene blitt langt mer alvorlig.

Tabellen under viser hvilke hendelser kommunene refererte til, og viser også hvor mange forskjellige hendelser som kan kategoriseres som en digital uønsket hendelse.

	Svar	**Hendelser**
K1	JA	Langvarig strømbrudd, og mistet tilgangen til digitale verktøy. Mobiltelefonsystemet falt ut, men det var Telenors ansvar.
K2	JA	Ett hacking-tilfelle, og flere phishing-forsøk. Et annet tilfelle der lavspenning førte til at serveren skrudde seg av og på og kortsluttet.
K3	JA	Ansatt klikket på ondsinnet e-post, fikk kryptert filer. Krevde mye ressurser.
K4	JA	Kryptovirus som har hindret digitalt arbeid i opptil en dag. Én hendelse i 2018 og én 2019. Rammet hovedsakelig de tekniske områdene, og brannsystemer.
K5	JA	Fiberbrudd, uten nett i 18 timer. Telenor håndterte det, ikke IT-miljøet. Et par hundre forsøk på ondsinnede innlogginger i døgnet, særlig rundt Microsofts 'Patch Tuesday' (se kapittel 7.1).
K6	JA	Virusangrep i 2017, mange systemer nede. Oppstod etter at en ansatt hadde glemt å logge av før påske, slik at alle systemer hadde stått åpent. Flere daglige forsøk på å komme seg inn i kommunens sikkerhetsanordninger.
K7	JA	Mistet en minnepenn i posten, mange sensitive opplysninger på avveie. Ganske alvorlig virushendelse før jul, men IT-informanten husket ikke hva det gjaldt.
K8	JA	Flere strømbrudd der nettverket i kommunen har rast sammen. Flere virus som har trengt seg gjennom kommunens brannmurer.
K9	JA	'Solar Wind' Flere titalls brudd på personvern, som har måtte meldes inn til Datatilsynet.
K10	JA	Mange 'CEO-fraud' og 'DdoS'-angrep. Mange tusen forsøk på angrep i døgnet

Tabell 6.2: Oversikt over opplevde digitale uønskede hendelser

De aller fleste hendelsene som ble henvist til var tilsiktede handlinger i cyber-domenet, som i stor grad ble håndtert av IT-miljøet. Konsekvensene av disse hendelsene, som flere av informantene påpekte, er at man mister tilgang til de digitale systemene. Fire av informantene beskrev også strømbrudd eller strømrelaterte problemer som en digital uønskede hendelse, med tilnærmet like konsekvenser som ved tilsiktede hendelser.

I en forlengelse av beskrivelsen av opplevde hendelser, var det flere informanter som belyste hva som kunne bli potensialet av slike hendelser. Det var naturligvis gjennomgående at

potensialet var langt mer alvorlig enn hvordan den reelle hendelsen utspilte seg. Det var likevel litt ulik tilnærming til dette med hendelsespotensialet. IT-informanten fra K10 belyste utfordringen med at det er uvisst hvordan en hendelse hadde blitt håndtert om den hadde utviklet seg til en krisesituasjon:

> «Men jeg vet ikke hvor godt vi hadde håndtert det i en krisesituasjon, for det øver vi ikke så mye på. Når det har skjedd noe, så har det gått greit.» (K10, IT)

Beredskapsinformanten fra K5 snakket også om hendelsespotensiale i forbindelse med et fiberbrudd kommunen hadde opplevd. Informanten beskrev en uoversiktlig situasjon, der alt fra skipstrafikken, brannvakt og hjemmesykepleien til innflyvningssystemene for helikopteret ved det lokale sykehuset måtte sjekkes opp. Hovedutfordringen, ifølge informanten, var at det var uvisst hvordan en slik hendelse forplanter seg videre til andre deler av kommunen.

> «Jeg vet ikke hvordan alt fungerer, men alt var liksom avhengig av den kabelen, og vi stilte litt spørsmål til det. Ut fra det tenker jeg at vi hadde såpass mange erfaringer av dette bruddet at jeg ville hatt dette som en egen hendelse, altså en definert hendelse på lik linje med for eksempel at en bro blir dekka i en flom.» (K5, beredskap)

6.7.1 Effekten av angrepet på Østre Toten

Det var til dels enighet om at mange av de nevnte digitale uønskede hendelsene potensielt kunne fått store konsekvenser, men at dette ikke hadde hendt enda. Elleve av informantene henviste til angrepet på Østre Toten, og forklarte at dette hadde belyst hvor sårbare kommuner er overfor slike angrep. Hendelsen på Østre Toten ble blant annet omtalt slik:

> «Hvis vi får en Østre Toten-hendelse, for eksempel, er ikke det omtalt her [ROS-analyse]. Da må vi finne opp kruttet på nytt. Jeg har fått med et veldig godt tips inn i arbeidet med helhetlig ROS, der vi er nødt til å ta høyde for sånne hendelser.» (K3, beredskap)

> «Angrepet i Østre Toten kunne like gjerne skjedd her, sikkert.» (K5, beredskap)

> «IT-sjefen hos oss kommenterte, da det skjedde i Østre Toten, at det er ikke snakk om 'hvis' noe skjer, det er snakk om 'når'. Vi er såpass sårbare. Det å prøve å tenke i forkant er mye bedre enn å håndtere i etterkant.» (K6, beredskap)

Begge informantene fra K4 påpekte at hendelsen i Østre Toten gjorde at det nå var nødvendig å gjennomgå ROS-analysen på nytt. I tillegg sa IT-informanten fra K10 følgende om hvordan vedkommende anser kommuners forhold til omfattende digitale uønskede hendelser:

> «Jeg tror nok svært få i kommunal toppledelse hadde sett for seg at en kommune kunne bli slått ut sånn som Østre Toten.» (K10, IT)

Dette indikerer at det ikke nødvendigvis krever en hendelse i egen kommune for å få satt digital risiko på dagsorden. En av IT-informantene påpekte:

> «Østre Toten er jo veldig bra at kom. Det er jo synd for dem, men det løfter det frem.» (K7, IT)

6.8 Digital risiko i beredskapsarbeidet

Avslutningsvis beskrives hva informantene svarte på problemstillingen. Dette vil også fungere som en oppsummering av de viktigste funnene, da flere av informantene besvarte dette ved å ramse opp det de hadde fokusert mest på under intervjuet. Ettersom formuleringen av problemstillingen henvender seg veldig til kommunens egne løsninger, ble også svarene her nokså subjektive. Likevel ble det sett antydninger til likheter mellom flere.

Flere av IT-informantene stilte seg kritiske til at IKT ble behandlet som et separat fagområde.

> «Jeg tror det blir såpass viktig, at dette havner i en egen kategori. Du ser jo dette i Østre Toten, det tar jo seks måneder før de er oppe igjen. (...) De mangler alle [digitale] fagsystemer, så jeg tror absolutt at dette vil få økt oppmerksomhet.» (K5, IT)

> «Det burde nok være en litt tettere link. Som jeg har antydet tidligere burde nok beredskapsavdelingen være litt mer aktive pådrivere nedover». (K8, IT)

> «Man ser på det som ét område, som det kan skje noe på. Men man har vel ikke sett på det som et område som kan forårsake eller ha konsekvenser for de andre områdene. Man har sett på det som en separat greie, liksom.» (K10, IT)

Noen fremstod også som mer utilfreds med egne planverk, og kommunens evne til å henge med på den digitale utviklingen.

> «Den tar ikke hensyn til det. Det er ikke behandlet i vår beredskapsplan. Der er planen utdatert.» (K3, beredskap)

> «Det som er en av de største utfordringene til kommunen, er at man ikke henger med. Utfordringer i forhold til IKT-sikkerhet utvikler seg raskere enn det tradisjonelle beredskapsarbeidet i kommunene klarer å henge med. Det er et økende gap, og faren er jo at dette gapet kan bli større. (...) Det handler ikke bare om organisering og tiltakene man setter i gang, det handler også mye om økonomi, ha nok ressurser til å ha nok kompetanse i organisasjonen, men også kjøpe de sikkerhetstiltakene som man kan og bør sette til verks.» (K8, beredskap)

Økonomi ble også tatt opp som et problem hos andre kommuner:

> «Jeg tror viljen til å jobbe med digitalisering er kjempestor, men jeg tror det er lite penger.» (K7, IT)

Likevel stod det ikke bare dårlig til. Informantene i de to mellomstore kommunene, blant annet, stilte seg positive til egen kommunes håndtering av digitale uønskede hendelser. Andre kommuner påpekte også at situasjonen var i ferd med å endres, men at det muligens tok litt tid.

> «Kommunen, det er en stor båt som krever litt tid for å endre kurs. Vi har styringsfart, men det er jo en så stor masse, at ting tar tid.» (K4, beredskap)

7.0 Diskusjon

I dette kapittelet vil vi drøfte våre empiriske funn med de foregående kapitlene. Kapittelet er strukturert etter oppgavens fire forskningsspørsmål. Det første forskningsspørsmålet sammenligner informantenes synspunkt på eget beredskapsarbeid med det lovpålagte og styrende rammeverket for kommunalt beredskapsarbeid. Under det andre forskningsspørsmålet diskuteres det hvordan kommunene behandler digital risiko i beredskapsprosessen. Under det tredje forskningsspørsmålet diskuteres hvordan digitale uønskede hendelser beskrives i beredskapsplanen. I denne beskrivelsen ligger også en diskusjon av hvordan det kan og bør gjøres, og hvorfor det er slik. Under det fjerde forskningsspørsmålet vil det som fremstår som mest utfordrende for kommunene når det kommer til å inkludere digital risiko i beredskapsarbeidet diskuteres. Avslutningsvis følger en oppsummerende diskusjon i 7.5, der hvert enkelt forskningsspørsmål og dets hovedfunn vil oppsummeres.

Som et bakteppe til alle forskningsspørsmålene følger innledningsvis en beskrivelse av det vi anser som hovedtrekkene i kommunenes beredskapsarbeid, basert på empiri, teori og lovverk. Svært forenklet kan det argumenteres for at beredskapsarbeidet i kommuner består av tre hovedaktiviteter; mål og rammer, ROS-analyse og overordnet beredskapsplan. Alle disse tre aktiviteten vektlegges i forskrift om kommunal beredskapsplikt, og det var også noe alle informantene hadde fokus på under intervjuene. Mål og rammer handler om hvem og hva som omfattes av beredskapsarbeidet. Videre er kommuner pålagt å utvikle og gjennomføre en ROS-analyse. Dette kan også innebære kontinuerlige vurderinger av risiko og sårbarhet i det daglige arbeidet. Resultatet av det kontinuerlige arbeidet og ROS-analysen, skal reflekteres i den siste aktiviteten, overordnet beredskapsplan. Forenklet sett, er dette arbeidsprosessen for utvikling av beredskap i kommunene vi snakket med. Det er utfordrende å generalisere en mer konkret og detaljert arbeidsmetodikk på tvers av kommuner, fordi det er så store variasjoner i administrasjonsstørrelse, innbyggertall, geografi, økonomi og lignende. I tillegg er mange av kravene som stilles til kommunalt beredskapsarbeid resultatorienterte, ikke metodeorientert. Med dette menes at kravene rettes mot hva som skal oppnås, ikke hvordan det skal oppnås.

7.1 Hvordan oppfatter kommunene sitt eget beredskapsarbeid, i forhold til det lovpålagte og styrende rammeverket?

Med denne spørsmålsformuleringen ønsker vi å kartlegge hva som kjennetegner eventuelle gap mellom kommuners oppfatning av beredskapsarbeidet og det lovpålagte og styrende

rammeverket. I tillegg vil det diskuteres hvordan dette er avgjørende for beredskapsarbeidet i praksis, og om det eventuelt er noe som går igjen i flere av kommunene vi snakket med.

Etter å ha gått gjennom sivilbeskyttelsesloven, forskrift om kommunalt beredskapsarbeid, relevante veiledere for dette arbeidet, samt styrende prinsipper for samfunnssikkerhetsarbeidet i Norge, har vi blitt presentert for de mest grunnleggende lovpålagte praksisene som kommunene må følge i deres beredskapsarbeid. Kort oppsummert kan de viktigste oppgavene til kommunen sies å være å jobbe systematisk og helhetlig med sikkerhetsarbeidet på tvers av sektorene, for å redusere risikoen for tap av liv og skade, og å sørge for befolkningens sikkerhet og trygghet (se kapittel 3). For å gjøre dette må planene være samstemte og oppdaterte, og det må gjennomføres øvelser som kan teste ut planverket i praksis. Det synes som at de fleste kommunene i utvalget er gode på det som kan sies å være kjernen i det lovpålagte beredskapsarbeidet. Det kartlegges risikoer og sårbarheter, foretas en utvelgelse av de mest relevante hendelsene for kommunen, og etableres beredskap deretter. Kommunene virker også gode til å se relevansen av hendelser de ser at andre kommuner blir utsatt for, som eksempelvis dataangrepet på Østre Toten kommune. Avvikene og merknadene vi har funnet ved å gå gjennom de siste tilsynsrapportene til kommunene, tilsier riktignok at det finnes både utfordringer og forbedringspotensial.

I forkant av prosjektet forventet vi å finne at digital risiko utgjorde en større del av beredskapsarbeidet de siste årene, sett i lys av både resiliens og trusselen den digitale risikoen utgjør. DSBs analyse av digitale angrep (DSB, 2014a; DSB, 2019) burde også bidra til å økt bevissthet rundt digital risiko. Digitale uønskede hendelser kan både gå utover menneskers sikkerhet og trygghetsfølelse, samt føre til tap av liv eller skade. Pasienten som døde under et digitalt angrep på et sykehus i Tyskland, som ble nevnt i kapittel 1, er et spesielt tankevekkende eksempel på dette. Med andre ord kan digitale uønskede hendelser gå utover alt det forskriften om kommunalt beredskapsarbeid sier kommunen er pliktet til å ha en plan for å håndtere. Alle informantene sa seg enige i at det bør fokuseres på den digitale risikoen i beredskapsarbeidet, men likevel var det et fåtall som faktisk hadde gjort det. Hele åtte av ti kommuner påpekte at de hadde brukt tid på å innse at IT-hendelser måtte inn i det overordnede beredskapsarbeidet – og at det var en pågående prosess. Ifølge informantene var grunnen til dette at det er utfordrende å se egen sårbarhet, og forstå hvor sektorovergripende og lammende en digital uønskede hendelse kan være. Antakeligvis var dermed beredskapsavdelingens kunnskap om digital risiko

en av faktorene til at det var vanskelig å se digitale uønskede hendelser som en del av det overordnede beredskapsarbeidet.

Flere av informantene insinuerte at de synes det var utfordrende å oppdatere beredskapsplanverket såpass jevnlig som det lovverket krever. Å revidere beredskapsplanen én gang årlig, og gjennomføre ROS-analyser hvert fjerde år, var for mange vanskelig å få til. Som vi så eksempler på i kapittel 6.3.1, var det enkelte kommuner som etablerte beredskapen etter planer og analyser som var flere år gamle. Dette ble også underbygget av Statsforvalterens tilsynsrapporter, samt DSBs Kommuneundersøkelse 2021 (se kapittel 2.1.3). Knappe ressurser som tid, økonomi og personell, ble spesielt trukket frem som begrensninger i dette arbeidet. Det kan være flere grunner til at kommunene blir kneblet av disse knapphetene. Beredskapsarbeidet er blant annet noe som foregår i kulissene, og som ikke nødvendigvis er så lett å se effekten av. Dette er fordi sikkerhet blant annet handler om å forhindre at uønskede hendelser skjer, og det er når disse *ikke* skjer, at arbeidet er vellykket. Som en følge av dette syntes syv av kommunene det hadde vært vanskelig å få ledelsen til å innse behovet for beredskapsarbeidet. Som vi så i organisasjonsmodellen i kapittel 4.3.3, vil mangel på ressurser og engasjement fra ledelsen påvirke beredskapsplanverket negativt. Blant annet kan det føre til lav motivasjon og dårlige beslutninger, som igjen kan føre til nye avvik og merknader ved tilsyn fra Statsforvalteren. En kritisk tilsynsrapport kan være med på å ødelegge for kommunens ansikt utad, som igjen kan ødelegge kulturen innad. Dette gjør det også utfordrende å jobbe kontinuerlig med beredskapsarbeidet. Å få med ledelsen på arbeidet, og omprioritere ressursene i kommunen, vil dermed være essensielt for det kommunale beredskapsarbeidet.

De digitale systemene kompliserer kravet om det kontinuerlige beredskapsarbeidet ytterligere. Som ett av verdens mest digitaliserte land skal det godt gjøres å videreutvikle systemene samtidig som sikkerheten ivaretas. Selv om man kan komme langt med å gjennomføre ROS-analyser av de fysiske risikofaktorene hvert fjerde år, er det grunn til å diskutere om dette er altfor sjeldent for de digitale. Digitale systemer må nemlig oppdateres og vedlikeholdes svært ofte, for å kunne driftes på en trygg og forsvarlig måte. Et eksempel som underbygger dette er Microsoft som sikkerhetsoppdaterer systemene sine hver annen tirsdag i måneden, på en dag de kaller "Patch Tuesday" eller "Update Tuesday" (Microsoft Security Response Center, 2021). I tillegg erstattes gamle systemer med ny teknologi relativt ofte (DSB, 2019), som kan tenkes å medføre ganske store systemendringer. Slike endringer vil påvirke samspillet mellom digitale

og fysiske komponenter, og således føre til en endring i risikobildet. Disse endringene kan også oppfattes som komplekse og uforståelige for mange - og spesielt for personer uten digital kompetanse. Når det foretas endringer i digitale systemer, som for eksempel når ny teknologi tas i bruk, er det all grunn til å tro at den samlede kompleksiteten i systemet (les: kommunen) endrer seg. I forlengelsen av dette er det all grunn til å tro at en helhetlig ROS-analyse bør gjennomføres oftere enn fire år, nettopp for å avdekke nye risikoforhold som følge av teknologiske og digitale endringer. Dette understøttes av lovverket, ettersom sivilbeskyttelsesloven § 14 sier at ROS-analysen skal oppdateres *«i takt med endringer»* i risiko- og sårbarhetsbildet.

Kommunalt beredskapsarbeid skal som nevnt tufte på de fire samfunnssikkerhetsprinsippene, nærhet-, likhet-, ansvar- og samvirkeprinsippet. Halvparten av kommunen omtalte disse prinsippene på eget initiativ. Dette ga oss et inntrykk av hvor sentrale disse prinsippene var for arbeidet. Spesielt nærhet- og likhetsprinsippet ble nevnt i forbindelse med beredskapsorganisasjonen til kommunen. I noen tilfeller ble disse prinsippene også henvist til da IT-informantene ble spurt om hvordan de gikk frem for å etablere beredskapen (se kapittel 6.3), eller da beredskapsinformantene ble spurt om beredskapen for digitale uønskede hendelser (se kapittel 6.4). Det er selvsagt ikke slik at man bør kunne forvente at alle de ansatte kan alt, i en så kompleks organisasjon som det kommunen kan sies å være. Det er derfor ikke så rart at flere forsøkte å henvise spørsmålet til andre i kommunen, som beredskapsinformanten i K4 gjorde i forbindelse med spørsmål om den mest hensiktsmessige måten å håndtere digital risiko. Likevel fremstod det, i enkelte tilfeller, som at disse prinsippene ble brukt som en unnskyldning for at de ikke kunne si noe om dette temaet. Dette er besynderlig. Hensikten med de fire nasjonale prinsippene er å fremme oversikt, kunnskap, samarbeid og gjennomføringskraft. I disse tilfellene virket det heller til å separere ansvarsoppgavene til den grad at de ikke kunne si noe om det arbeidet som, tross alt, overlappet en hel del med det de selv jobbet med. En IT-ansvarlig burde kunne forventes å kjenne til den overordnede beredskapsplanen som gjelder for hele kommunen. På lik linje burde en beredskapskoordinator ha kjennskap til hvordan IT-avdelingen jobber med beredskapen for digitale uønskede hendelser.

Dette funnet ble også støttet av tilsynsrapportene, der seks kommuner hadde fått merknad eller avvik for beskrivelsen av samordning av ressurser, eller sammenhengen mellom kommunens samlede beredskapsplanverk. Det er grunn til å stille spørsmål ved hvorvidt

samvirkeprinsippet, som kom på banen omtrentlig ti år etter de tre andre prinsippene, ikke er inkorporert nok i det kommunale arbeidet. Én ting er om kommunen har god kjennskap til Politiet, brannvesenet og helsepersonell; men hvor langt kommer man med kun disse samarbeidene, når det i fremtiden er de digitale systemene som blir angrepet? Her vil kommunen være tjent med å se mot andre aktører som kan hjelpe dem med det digitale, som for eksempel IT-avdelingen eller de nevnte aktørene i kapittel 2.2.3. Dette vil både være i tråd med samvirkeprinsippet, og gi kommunene kunnskapen som vi så i kapittel 6.4 og 6.6 at mange manglet for å etablere god beredskap.

7.2 Hvordan inngår digital risiko i den kommunale arbeidsprosessen for utvikling av beredskap?

Mens det første forskningsspørsmålet satt søkelys på kvaliteten av det kommunale beredskapsarbeidet, retter vi nå fokuset mot hvordan digital risiko inngår i kommunalt beredskapsarbeid. Her minner vi om forståelsen av beredskap som prosess, som vi var inne på i kapittel 4.2. Hensikten med spørsmålet er å diskutere hvordan digital risiko tas hensyn til i arbeidsprosessene knyttet til beredskap, som organisering, struktur og analyse. For å kunne diskutere dette vil vi se på hvordan kommunene vurderer risiko generelt, samt fire virkemidler kommunene bruker for å håndtere digital risiko. Avslutningsvis vil koblingen mellom ROS-analyse og digital risiko drøftes, samt noen virkemidler som kan styrke håndteringen av digital risiko.

Som forklart i kapittel 4.3.1, er risikopersepsjon den mest åpenbare av de faktorene som er med på å påvirke hva kommunene vurderer som risiko. For at et risikomoment skal betraktes som en reell risiko, og således inkluderes i beredskapsarbeidet, må det foreligge en idé om at dette er nødvendig. I tillegg kreves det kunnskap om den risikoen som undersøkes. En forutsetning for dette er fagkompetanse og tilgang til empirisk data og pålitelig informasjon. Hvorvidt en gitt risiko blir inkludert i beredskapsarbeidet vil dermed avhenge av blant annet hvordan man tolker og anser sannsynligheten for, og konsekvensen av, en risikokilde, samt hva slags objektiv og korrekt informasjon om risikokilden man har tilgjengelig.

Med utgangspunkt i dette, og hovedtrekkene i den kommunale beredskapsprosessen, kan vi se nærmere på hvordan kommunene håndterer digital risiko.

Først og fremst virket samtlige kommuner til å overlate ansvaret for den digitale risikoen til de som besitter mest kompetanse på området. Dette er i utgangspunkt ikke negativt, da dette også gjerne er tilfellet på andre områder, som blant annet helse. Det kan imidlertid virke som at risikomomentene i de andre fagområdene i større grad blir behandlet i det overordnede beredskapsarbeidet, enn det den digitale risikoen blir. På bakgrunn av hva informantene påpekte i kapittel 6.5, reises spørsmål om hvorvidt arbeidet med digital risiko i IT-miljøene har blitt oppfattet som beredskapsarbeid, både fra IT-miljøets og beredskapsmiljøets ståsted. Flere informanter påpekte at det har vært lite tradisjon for å tenke på digital sikkerhet som beredskap. Tilsvarende var det lite tradisjon å tenke beredskap i IT-miljøet (se kapittel 6.5.3). Her ser vi altså en tendens til å tenke på digital risiko som noe annet enn beredskap. Et nærliggende alternativ kan være kontinuitet, altså at digital sikkerhet er en del av det daglige arbeidet, og ikke er noe ekstraordinært. Denne tilnærmingen virker å passe godt overens med refleksjonene til flere av både IT- og beredskapsinformantene. Dette kan også forklare hvorfor ikke digital sikkerhet ilegges mer fokus på styrende dokumenter og lovverk, samt ROS-analyse. Dette kommer vi nærmere tilbake til.

Et annet viktig verktøy kommuner bruker for å håndtere digital risiko er bruken av eksternt samarbeid og eksterne tjenestetilbydere. Syv av kommunene var enten medlem av et IKS, eller brukte private IKT-selskaper for hendelseshåndtering og drift. Bruken av slike eksterne ressurser har en rekke fordeler, hovedsakelig knyttet til tilgangen på nødvendige ressurser, kapasiteter og kompetanse som kommunen ikke har tilgang til internt. Til tross for at denne løsningen har en del fordeler, kan det potensielt gjøre det utfordrende å inkludere digital risiko i beredskapsarbeidet innad i kommunen. Dette er fordi det kan føre til en tankegang om at digital risiko blir håndtert av noen andre, og derfor ikke trengs inkludert i verken ROS-analyser eller i den kommunale beredskapsplanen. Dette kan gjøre digital risiko mer utilgjengelig, spesielt om det ikke har vært tradisjon for å tenke på digital risiko som en del av det overordnede beredskapsarbeidet. Ni av ti kommuner indikerte likevel at kommunen var i en slags modningsfase. Forhåpentligvis betyr dette at måten man ser digital risiko i forhold til beredskapsarbeidet også er i endring, og at det sees et tydeligere behov for å inkludere digitale uønskede hendelser som dimensjonerende hendelser i beredskapsarbeidet.

Kjennskap til tidligere inntrufne hendelser virket til å være en tredje faktor som påvirket hvordan kommunene inkluderte digital risiko i beredskapsarbeidet. Dette gjaldt både hendelser som rammet noen andre, og hendelser kommunen selv hadde blitt offer for. En overvekt av

informantene henviste for eksempel til dataangrepet på Østre Toten, og påpekte at dette hadde medført et økt fokus på digital risiko i kommunen. Dette kan knyttes til risikopersepsjon, der mange av informantene påpekte at det var en tydeligere frykt relatert til digitale uønskede hendelser etter angrepet på Østre Toten. Frykten virket å øke bevisstheten rundt konsekvenser av slike hendelser, og således øke viljen for å inkludere det i det forebyggende og forberedende beredskapsarbeidet. Dette kan relateres til trinn 2 i Rake & Sommers beredskapshjul, der kartlegging av uønskede hendelser som kan inntreffe bør baseres på egne og andres tidligere erfaringer. Disse henvisningene viste at digital risiko kan undersøkes og avdekkes på lik linje med andre risikomomenter.

ROS-analyser virket å være det fjerde virkemiddelet i møte med digital risiko, og også det som var mest relatert til beredskap. Det var imidlertid store variasjoner hva gjelder hvilken grad digital risiko var involvert i ROS-analysene. En forklaring kan være at verken forskrift om kommunal beredskapsplikt, veileder til helhetlig ROS eller veileder til Statsforvalterens tilsyn med kommunal beredskapsplikt nevner digital risiko. Dette gjenspeiles også i tilsynsrapportene, der digital risiko kun nevnes i én av ti (K6). Hvis kommuner bruker disse dokumentene som veiledning, retningslinjer og inspirasjon vil de ikke få innspill til hvordan de kan inkludere digital risiko. En annen forklaring kan handle om at det ikke var nok fokus på den gjensidige avhengigheten mellom de digitale systemene og de andre systemene. En informant påpekte at ROS-analysen hadde som forutsetning at de digitale systemene fungerte. I et slikt tilfelle vil ROS-analysen påvirkes på to måter. For det første vil det påvirke analysen av gjensidige avhengigheter. Det virker sannsynlig at man ikke får avdekket konsekvensene av en digital uønsket hendelse i for eksempel skole- eller helsesektoren, dersom en forutsetning er at de digitale systemene fungerer. Spørsmålet som må stilles er dermed hvordan brudd i digitale systemer forplanter seg i andre deler av kommunen. For det andre vil det antakeligvis utelukke en analyse av digitale sårbarheter i kommunen, på samme måte som at ikke vil få analysert sårbarhetene tilknyttet brann hvis premisset er at det aldri brenner. Dette viser to ganske dramatiske konsekvenser av hva som kan skje dersom en slik forutsetning er lagt til grunn i ROS-analysen. En måte å løse dette på, er å fjerne premisset om at digitale systemer fungerer, og heller undersøke mulige hendelser som kan komme som et resultat av at de digitale systemene svikter.

Hva gjelder ROS-analyse og digital risiko var det lite som tydet på at ROS-analyser som inkluderte digital risiko ledet til beredskapsetablering for digitale uønskede hendelser. Med

andre ord stoppet det ofte opp med ROS-analysen. Det var imidlertid noen variasjoner mellom kommunene. Der K6 mente at analysene ble en del av den totale beredskapen, mente K10 at de i liten grad hadde etablert beredskapen for å svare på digitale utfordringer. Ifølge K10 var årsaken til at digital risiko ikke ble brukt som en dimensjonerende faktor i beredskapsetableringen at det eksterne apparatet hadde håndtert digitale hendelser godt. Slik informanten beskrev dette virket det overflødig å ha interne beredskapsressurser som skal håndtere digitale uønskede hendelser, når det eksterne apparatet håndterer det. Fra kommunens ståsted, fremstår dette som et fornuftig alternativ til å inkludere digital risiko i beredskapsarbeidet. Likevel påpekte informanten at det oppstår problemer hvis kommunen får interne digitale utfordringer, og hentydet videre at digital risiko *bør* inngå i den interne beredskapsprosessen.

Det er verdt å merke seg at bruken av disse fire virkemidlene synes å være et forsøk på å øke kommunens grad av resiliens for å kunne håndtere digitale uønskede hendelser. Til tross for dette var de fleste informantene i kapittel 6.4.4 enige i at det i prinsippet ikke er noe forskjell på håndteringen av digitale og fysiske uønskede hendelser. I den forstand kan det tenkes å være fordelaktig for kommunene å undersøke hvilke muligheter som ligger i å bruke det eksisterende beredskapsrammeverket for å håndtere digitale uønskede hendelser. Om dette er dimensjonert for å håndtere de fleste fysiske uønskede hendelsene, og det følgelig ikke er noe forskjell på håndteringen av digitale og fysiske uønskede hendelser, bør kommunene i utgangspunktet være bedre rustet enn de gir inntrykk av i blant annet kapittel 6.8. Det var, for ordens skyld, ingen informanter som reflekterte rundt denne sammenhengen.

Det finnes imidlertid noen metoder og tilnærminger som kan hjelpe kommunene med å forstå hvordan digitale risikoer bør være en naturlig del av det overordnede beredskapsarbeidet.

Forskriften om kommunal beredskapsplikt sier at kommunene skal analysere egen evne til å opprettholde virksomheten når den utsettes for en uønsket hendelse. Flere av informantene påpekte at digital risiko kan være utfordrende for beredskapsmiljøet, fordi det ofte anses som abstrakt, teknisk og komplisert. Dette stemmer overens med DSBs (2019) beskrivelse av digitale verdikjeder. Et virkemiddel som kan hjelpe med dette, kan være det Aven mfl. (2017) kaller operasjonalisering av risiko. En operasjonalisering av digital risiko innebærer å forstå digitale uønskede hendelser som forhold som kan påvirke den normale driftsituasjonen. Dette henger også sammen med kompetanseheving. Dette kan være et effektivt virkemiddel for å

plassere den digitale risikoen inn i et mer kjent rammeverk for risikostyring, for eksempel en risikomatrise (se kapittel 4.1.3), som flere av informantene henviste til. En operasjonalisering av digital risiko kunne dermed vært fordelaktig for å forstå digitale uønskede hendelser i sammenheng med for eksempel risikomatrisen.

En annen tilnærming som kan øke evnen til å forstå den underliggende og reelle risikoen i et digitalt system, er økt fokus på digital sikkerhetskultur. Fokus på optimisme for digitalisering kan bidra til å ha mer bevissthet rundt tilliten til digitale systemer. NorSIS (2019) viser som nevnt til at en persons holdninger til digitalisering påvirker måten man forholder seg til teknologi på. Hvis vi drar dette resonnementet litt lenger kan vi antyde at for høy tillit til digitale systemer kan bidra til å ikke forstå den underliggende risikoen. Hvis det er slik at beredskapsmiljøet i Norge har for høy tillit til digitale systemer, kan risikoen neglisjeres, fordi brukerne av systemene stoler på at de funker. Økt kompetanse på digital sårbarhet kan forhindre denne neglisjeringen. En annen nøkkelfaktor innen digital sikkerhetskultur, er interesse. Med interesse følger gjerne kompetanse, der økt interesse og kompetanse for digitale systemer kan øke kommunens evne til å forstå og avdekke digital risiko. Sett i lys av Lipshitz og Strauss' teori om usikkerhet, vil det også bidra til å redusere usikkerhet rundt vurderinger av egen sårbarhet, som følger av mangel på forståelse (se kapittel 4.1.1). Sett i sammenheng med organisasjonsmodellen i kapittel 4.3.3 vil også læring om digitale systemer påvirke de ansattes motivasjon. Dette vil påvirke beredskapsarbeidet som prosess, og beredskapsplanen som produkt.

7.3 Hvordan beskrives digitale uønskede hendelser i beredskapsplanverket?

Hensikten med dette forskningsspørsmålet er å diskutere hvordan digitale uønskede hendelser beskrives i beredskapsplanene og ROS-analysene. I lys av dette vil vi også drøfte hvorvidt digitale uønskede hendelser bør beskrives, og hva som er fordelene med dette. Kapittel 7.3 må forstås i sammenheng med kapittel 7.2, der vi diskuterte hvordan digital risiko blir tatt hensyn til i beredskapsarbeidet. Premisset for forskningsspørsmålet er en tilnærming om at ROS-analysen og beredskapsplanen er et ferdig produkt i form av et dokument. For å undersøke hvordan kommuner håndterer digital risiko virker det nødvendig å se på hvordan digitale uønskede hendelser er beskrevet i sluttproduktet. Digital risiko kan for så vidt være inkludert i arbeidsprosessen uten å være beskrevet i sluttproduktet, og vice versa. Dette vil riktignok påvirke hvordan kommunene håndterer digital risiko, ettersom det er her informasjonen er

tilgjengelig. Som eksempel hadde flere informanter lest ROS-analysen og beredskapsplanen for å forberede seg til intervjuene, noe som indikerer at disse to dokumentene er sentrale kilder til informasjon. Når informantene snakket om digitale uønskede hendelser i planverket, var det disse to dokumentene det ble siktet til.

Før vi går videre er det nødvendig å minne om skillet mellom informasjonssikkerhet og digital sikkerhet, som vi gjennomgikk i kapittel 2.2.2. I dette delkapittelet, og i oppgaven for øvrig, legger vi vekt på digital sikkerhet. Mangel på digital sikkerhet kan føre til nedetid og bortfall på tilgang til digitale verktøy, som vi i kapittel 7.2 argumenterte for at kan utgjøre en vesentlig trussel for kommunen. Mangelen på digital sikkerhet vil også kunne kompromittere informasjonssikkerhet, som beskrevet i kapittel 2.2.2. Bruken av begrepet digital sikkerhet utelukker dermed ikke informasjonssikkerhet, og det oppfordres til å tolke digital sikkerhet til også å omfatte informasjonssikkerhet. En av grunnene til at vi aktivt ikke velger å skille på informasjonssikkerhet og digital sikkerhet er fordi det lovpålagte rammeverket ikke trekker dette skillet. Ettersom vi argumenterer for at digital sikkerhet er mest aktuelt for beredskapsarbeidet, forholder vi oss til det begrepet.

I kapittel 6.4 stilte vi spørsmål om hvordan digitale uønskede hendelser var omtalt og beskrevet i beredskapsplanen. Her påpekte flere at det var en svakhet at verken det overordnede eller de sektorspesifikke beredskapsplanene utenfor IT-sektoren tok for seg digitale uønskede hendelser. Et flertall av kommunene brukte som nevnt interkommunale IKT-selskap, og var dermed avhengig av at de eksterne aktørene hadde planer for å håndtere digitale uønskede hendelser. Blant de små og mellomstore kommunene var det lite konsekvent hvordan digitale hendelser var omtalt og beskrevet i beredskapsplanverket. Av de fire små kommunene var det ingen som hadde omtalt og beskrevet digitale uønskede hendelser i beredskapsplanverket. Dette kan skyldes at det ikke stilles noen konkrete krav på dette området, og at det dermed blir litt vilkårlig. Likevel bør det faktum at digital risiko løftes frem i rapportene til Etterretningstjenesten (2021), NSM (2021), NorSIS (2021) og Kommune-CSIRT (2021), samt i DSBs Veileder til helhetlig ROS (2014b), og som krisescenario i DSB (2019), fungere som et incentiv.

Det var også store variasjoner blant de større kommunene. Selv om digitale uønskede hendelser i større grad var beskrevet i planverket hos de større kommunene, virket det tilsynelatende å være litt tilfeldig. Etter å ha tolket resultatene fra intervjuene, er vi av den formening at graden

av inkludering av digitale uønskede hendelser i relativt stor grad beror på kompetansen hos de ansvarlige. Eksempelvis var den ene IT-informanten spesialisert innen sikkerhet, og det var tydelig at vedkommende hadde sterkere meninger om dette temaet enn hos de informantene som ikke besatt samme kompetanse. Det vil alltid være store variasjoner på tvers av kommuner i form av blant annet ulik fagkompetanse, fokusområder, økonomi og ressurser. Dette er viktig for at kommunene skal kunne imøtekomme ulike risikobilder. En viss form for standardisering og formalisering når det gjelder inkludering av digitale uønskede hendelser i beredskapsplanverket, virker likevel hensiktsmessig. Dette kan bidra til å utjevne ulikhetene som oppstår på grunn av ulik kompetanse i kommunen, og således gjøre det mindre tilfeldig hvorvidt digitale uønskede hendelser blir inkludert eller ikke.

En av utfordringene med å beskrive digitale uønskede hendelser, er det flytende skillet mellom digitale og fysiske trusler, som beskrevet i kapittel 2.2. Noen informanter trakk ekom-brudd og strømbrudd frem som digitale uønskede hendelser. Dette er gode eksempler på det intrikate forholdet mellom digitale og fysiske trusler, ettersom brudd i utgangspunktet er en fysisk hendelse som får digitale konsekvenser. Hackerangrep, som er å betrakte som en ren digital hendelse, ble kun beskrevet i to kommuner. Dette til tross for at Kommune-CSIRT (2021) og NorSIS (2021) trekker dette frem som en sentral del av risikobildet for offentlige virksomheter. Et fåtall av informantene reflekterte rundt ringvirkningene av digitale uønskede hendelser for fysiske systemer. Dette til tross for at forskrift om kommunal beredskapsplikt krever analyser av hvordan ulike risiko- og sårbarhetsfaktorer påvirker hverandre. En informant henviste for eksempel til at et fiberbrudd hadde slått ut kommunens datasystemer, der de videre ble nødt til å sjekke driftsstatus på innflyvningssystemene for helikopteret ved det lokale sykehuset. Dette var likevel ikke beskrevet i verken ROS-analyse eller beredskapsplanen. Kun én kommune hadde sett på denne gjensidige avhengigheten mellom digitale og fysiske systemer, etter å ha fått registrert avvik ved Statsforvalterens tilsyn.

Grunnen til at det er viktig å beskrive digital risiko og digitale uønskede hendelser, er for å klargjøre hva som kan inntreffe, og hva som skal kunne håndteres. Ut fra kapittel 4.2.1.1 om identifisering i beredskapsetableringen, kommer det frem at de dimensjonerende hendelsene må analyseres. Det virker nødvendig at disse hendelsene også må beskrives. Beskrivelser av scenarioer og hendelser er med andre ord en forutsetning for å kunne analysere dem. For å avgjøre om digitale uønskede hendelser bør tas i bruk og beskrives som dimensjonerende

hendelser i planverket, kan digital risiko knyttes til kapittel 4.2.1 Etablering av beredskap, kapittel 4.2.2 “God” beredskap og kravene i forskrift om kommunal beredskapsplikt.

Ifølge Lunde (2019) skal de hendelsene med antatt høyest risiko identifiseres i ROS-analysen. Sett i lys av risikodefinisjonen til Aven og Renn (2010) (se kapittel 4.1.1) kan det argumenteres for at risikoen er høy dersom en digital uønsket hendelse kan få alvorlige konsekvenser med hensyn til noe mennesker verdsetter, og det i tillegg følger usikkerhet med disse vurderingene. Basert på risikorapportene til Etterretningstjenesten (2021), NSM (2021), NorSIS (2021) og Kommune-CSIRT (2021) kan digitale uønskede hendelser argumenteres for å være blant de hendelsene med potensielt høyest risiko. Dermed bør disse inkluderes i ROS-analysene. Videre bør det gjennomføres en beredskapsanalyse av disse hendelsene, slik Rake & Sommer henviser til. En beredskapsanalyse er viktig av flere årsaker. For det første vil en beredskapsanalyse, som nevnt i kapittel 4.2.1.1, kunne avdekke ytelesrammer og ytelseskrav. Ytelesesrammene og ytelseskravene vil gi mer konkrete føringer for hvordan beredskapen skal dimensjoneres. For det andre vil dette gi noen konkrete mål for hvordan godheten av beredskapen kan måles. Gjennom å øve og trene beredskapsressursene opp mot ytelseskrav som beredskapen er ment for å håndtere, kan man få en forståelse av beredskapens "godhet". Dette legger videre til rette for å kunne evaluere og forbedre beredskapsressursene, slik både beredskapshjulet og beredskapsprosessen illustrerer (se kapittel 4.2.1.2). Hensikten med dette resonnementet er å vise at digitale uønskede hendelser passer inn i rammeverket til Lunde (2019) og Rake og Sommer (2018). Alle informantene var enige i at det er viktig å ha en beredskapsorganisasjon som kan håndtere en digital uønsket hendelse, men ingen henviste til denne måten å arbeide på. Vi er derfor av den formening at bruken av beredskapsanalyser vil øke kommuners evne til å håndtere uønskede hendelser - både fysiske og digitale.

Anbefalingen om å gjennomføre en beredskapsanalyse kan underbygges av kravene i forskrift om kommunal beredskapsplikt. Her pålegger § 2 kommunene å analysere eksisterende risiko- og sårbarhetsfaktorer i kommunen. I samme paragraf er også kommunene pålagt å analysere evnen til å opprettholde sin virksomhet når den utsettes for en uønsket hendelse. Dette står i sterk sammenheng med resonnementet over. Hvis digital risiko betraktes som en risiko- og sårbarhetsfaktor bør det være med i ROS-analysen fra start. Dersom det videre betraktes å ha *høy* risiko, bør det inkluderes videre i beredskapsanalysen som en dimensjonerende hendelse. Hvis man ikke analyserer og evaluerer håndteringsevnen av hendelser med høy risiko, vil det være utfordrende å måle, og oppfylle kriteriene for, god beredskap.

7.4 Hvilke utfordringer opplever kommunene i beredskapsarbeidet for å håndtere digitale uønskede hendelser?

Gjennom diskusjonen av de tre foregående spørsmålene, har vi vært innom flere utfordrende momenter ved beredskapsarbeidet. I det fjerde og siste spørsmålet diskuteres det som oppfattes som mest kritisk av utfordringene knyttet til beredskapsarbeidet for å håndtere digital risiko og digitale uønskede hendelser. Mulige løsninger til dette vil også diskuteres. Problemstillingene som tas opp her er utfordringer som kommunene selv påpekte, som for eksempel mangelfullt samarbeid mellom IT- og beredskapsavdelingen. I tillegg vil vi diskutere utfordringer som trolig fremstod tydeligere for oss, fra et utenfraperspektiv, enn for dem det gjaldt. Et eksempel på dette er informanter som undervurderte hvor sårbar kommunen faktisk var.

Flere av IT-informantene uttrykte at de så på IT- og beredskapsavdelingen som to veldig separate enheter som jobbet med hvert sitt område, og hadde lite formelt samvirke. Det ble også påpekt at det i enkelte tilfeller ble tatt for gitt at de digitale systemene fungerte. En av de nevnte årsakene til dette var at beredskapsavdelingen ikke hadde den tverrsektorielle forståelsen av hvordan digitale hendelser kunne ramme flere deler av virksomheten. I den forbindelse uttrykte flere i kapittel 6.6 et ønske om at både beredskapsavdelingen og ledelsen i kommunen skulle få en større forståelse for den digitale sikkerheten. Da ville de kunne innse hvor sårbare de egentlig var når det kom til digital risiko, og dermed få mer fokus på det i ROS-analysene og beredskapsplanverket.

Mer kompetanse på de digitale systemene og sårbarhetene var også noe vi så behovet for. Halvparten av kommunene trakk til stadighet frem andre kommuner og virksomheter som eksempler på det å være svært utsatt for digitale uønskede hendelser. Samtidig var det et fåtall som så den samme sårbarheten hos seg selv. Dette kan sees i sammenheng med det Brun (1997) kaller eksponeringsdimensjonen innenfor risikopersepsjon, der folk har en tendens til å tenke at hendelser er mer sannsynlig å ramme andre. Faktum at kun tre av kommunene hadde inkludert digitale uønskede hendelser i beredskapsplanen underbygger også behovet for mer kompetanse og forståelse for digital risiko. En tverrsektoriell forståelse av digital risiko ville for eksempel kunne ha vist hvordan konsekvensene av en digital uønsket hendelse kan være fatale, samtidig som det har en sannsynlighetsverdi som gjør det naivt og dumdristig å overse. I kapittel 6.7 kom det frem at kommunene til daglig opplever en eller annen form for digitale uønskede hendelser. Dette underbygger at sannsynligheten for at noe skal skje, er relativt stor.

Etter hendelsen i Østre Toten ser vi også at konsekvensene av slike hendelser kan bli alvorlige. Spørsmålet er om kommunene har råd til å overse den digitale risikoen. Likevel viser funn i dette prosjektet at det er flere som har neglisjert denne sårbarheten. I de kommende avsnittene vil vi diskutere hvorfor dette er tilfellet.

Fra kapittelet om risikopersepsjon vet vi at både nyhet-, eksponering- og styrkedimensjonen av risikopersepsjon påvirkes av kompetansen man har om risikoen. Kommunenes forsømmelse av digital risiko kan muligens forklares ut fra dette. Dersom risikoen var helt ukjent da vi pratet om det under intervjusituasjonen, ville antakeligvis konsekvensene og sannsynlighetene av risikoen blitt blåst opp av informantene vi snakket med. Det opplevde vi ikke at de gjorde. Antakeligvis var dette fordi den digitale risikoen ikke var helt ukjent for noen av informantene. Som diskutert i kapittel 7.2 var det IT-avdelingen, enten den var intern eller ekstern, som hadde hovedansvaret for å håndtere den digitale risikoen. En slik ansvarsfraskrivelse virket sannsynligvis betryggende for beredskapsinformantene, som selv ikke kunne noe særlig om dette temaet. Dette gjorde trolig at den digitale risikoen kommunen stod overfor ikke ble oppfattet som *så* stor, da den var kjent for alle, men ble håndtert av få. Slik kan nyhetsdimensjonen forklare hvorfor ikke beredskapsinformantene innså hvor sårbar egen kommune var for digitale hendelser.

Tilsvarende kan også eksponeringsdimensjonen forklare hvorfor det var slik. Denne dimensjonen snakker om hvordan folk har en tendens til å miskjenne sannsynligheten for at uønskede hendelser rammer en selv. Med økt kompetanse er det rimelig å anta at flere i kommunen vil innse at digitale uønskede hendelser rammer *alle*, slik IT-informanten fra K6 påpekte i kapittel 6.7.1. Mer kunnskap vil altså kunne rette opp i hvor eksponert kommunen selv mener de er. Helt avslutningsvis har vi styrkedimensjonen, som også henger sammen med de to andre. Her sies det at jo mer alvorlig de potensielle konsekvensene er, jo større oppleves risikoen. Dersom man imidlertid ikke kan nok om de potensielle konsekvensene, vil risikoen undervurderes, slik flere beredskapsinformanter gjorde da de ble utspurt om den digitale risikoen. Økt kompetanse vil trolig føre til at det innses hvor sektorovergripende uønskede hendelser i de digitale systemene er, som sannsynligvis vil gjøre at de potensielle konsekvensene oppleves som mer alvorlige og foruroligende.

Som det har blitt påpekt opptil flere ganger, er det gjerne økt kompetanse som må til for at beredskapsinformantene og ledelsen i kommunene skal innse sårbarheten de står overfor når

det kommer til den digitale risikoen. Dette er et forventet funn i prosjektet, da det til stadighet var en av utfordringene som ble trukket frem av både IT- og beredskapsinformantene. Dermed er det heller ikke overraskende å se at kompetanseheving innad i kommunen heller ikke er så lett å få til. Dette kan underbygges av tilsynsrapportenes funn, der to kommuner (K3, K5) fikk avvik, og tre kommuner (K6, K9, K10) fikk merknad på mangelfulle systemer og rutiner for opplæring. Dette kan knyttes til kompetanseparadokset som ble nevnt i kapittel 4.2.3, der man på den ene siden er tvunget til å ha en viss digital kompetanse, men på den andre siden ikke har et godt system for hvordan man skal få en grunnleggende forståelse for det. I henhold til § 7 i forskrift om kommunal beredskap, er kommunene i utgangspunktet forpliktet til å gi nødvendig opplæring av de som innehar en rolle i kommunens krisehåndtering. I dette prosjektet er det ikke samlet inn tilstrekkelig data til å undersøke hvorvidt dette gjøres eller ei, men det er likevel nok data til å argumentere for at kompetansen ikke er tilstrekkelig. Om den hadde vært det, ville antakeligvis diskusjonen til nå vært helt annerledes. Da ville trolig den tverrfaglige forståelsen vært bedre, samarbeidet tettere, og digital risiko tatt mer hensyn til i analysene og beredskapsplanene. I stedet oppleves IT- og beredskapsavdelingene som mer segregerte, og planverkene som ikke inkluderer digital risiko, mer ufullstendige og utdaterte. Dette belyser et behov for en mer adekvat opplæring av kommunens ansatte som jobber med krisehåndtering.

I kapittel 7.1 diskuterte vi hvordan mangel på ressurser stod i veien for mye av beredskapsarbeidet. Dette gjør det vanskelig å jobbe kontinuerlig, å få ressurser til å gjennomføre øvelser, og å få nok personell til å dekke den nødvendige kompetansen. Trolig gjør også dette at det for mange kommuner oppleves som vanskelig å lære opp de ansatte i digital kompetanse. For mange kommuner strekker rett og slett ikke tid og penger til for å kunne gjøre beredskapsarbeidet skikkelig. I kapittel 6.1 så vi også hvordan mange som jobber med beredskap ofte har veldig mange andre ansvarsområder som også må prioriteres, i tillegg til beredskapsarbeidet. Dette gjaldt mest i de små og mellomstore kommunene. Tilsvarende slet de store kommunene med at beredskapsavdelingen var for liten i forhold til oppgavene som måtte gjøres. Disse utfordringene kan forklares med mangel på ressurser.

Et spørsmål verdt å stille i denne sammenheng, er hvorfor ikke IT- og beredskapsavdelingen da samarbeider mer om å ha det digitale beredskapsansvaret. Tidligere har vi sett hvordan digitale og fysiske uønskede hendelser overlapper hverandre, at tiden ikke strekker til, og at mangel på kunnskap og ressurser setter en stopper for beredskapsarbeidet. I lys av dette er det

rimelig å anta at et større samarbeid vil gjøre beredskapsarbeidet mer helhetlig, mer oppdatert og mer overkommelig for de som jobbet med det. Dette ville også løst problemer som at IT-avdelingen føler seg tilsidesatt, og utfordringer med at beredskapsavdelingen sliter med å spre budskapet om hvor viktig det er at alle de ansatte tenker sikkerhet. For å forsøke å forstå dette fra kommunens standpunkt har vi stilt oss selv spørsmål om hvorvidt det finnes noen fordeler med å holde prosessene separert. Det virker sannsynlig at en slik segregert modell oppfattes som enklere å administrere, og dermed mer oversiktlig. Kommuner er komplekse virksomheter, så løsningen med å plassere ulike kompetansemiljøer i avgrensede enheter kan virke både fordelaktig og effektivt. I den forstand er det forståelig at flere kommuner har valgt å separere IT-miljøet fra beredskapsmiljøet. Likevel mener vi det er overveiende sannsynlig at kommunene vil oppnå flere fordeler med en mer tverrfaglig organisering av håndtering av digital risiko og beredskapsarbeid.

Om ikke et tettere samarbeid skulle la seg gjennomføre, finnes det likevel mange ressurssterke institusjoner som kan hjelpe kommunene med opplæring på digital kompetanse og forståelse. Noen av disse ble nevnt i kapittel 2.2.3. Blant annet nevnes Datatilsynet som et rådgivende og kompetansebyggende organ, KommIT som rådgivende organ innen digitalisering, Kommune-CSIRT som ressurssenter, og NSM som det nasjonale fagmiljøet innen IKT-sikkerhet. Disse er alle statlige organer, som blant annet kan bidra med kompetanse, veiledning og rådgivning. Datagrunnlaget i dette prosjektet er ikke tilstrekkelig for å kunne si noe om nøyaktig hvor mye disse tilbudene tas i bruk av de forskjellige kommunene. Likevel er det viktig at disse tilbudene og ressursene blir løftet mer opp og frem, som løsningsforslag på utfordringer som mangel på digital kompetanse. Ifølge § 7 i forskrift om kommunal beredskap, er tross alt kommunene pliktet til å gi de ansatte *«nødvendig opplæring»*. I denne digitale tidsalderen er det all grunn til å argumentere for at digital kompetanse er *nødvendig* for å jobbe med krisehåndtering – uavhengig om man jobber i IT- eller beredskapsavdelingen. Det er derfor sentralt at bevisstheten rundt de eksterne ressursene kommunene har tilgjengelig økes, slik at de ansatte får mer kunnskap som kan styrke beredskapen.

7.5 Oppsummert diskusjon

Sammenlagt er forskningsspørsmålene i kapittel 7.1-7.4 ment å svare på hvordan digital risiko og digitale uønskede hendelser integreres i det kommunale beredskapsarbeidet. For å systematisere svarene, og tydeliggjøre konklusjonen, oppsummeres hovedfunnene her.

I det første forskningsspørsmålet diskuterte vi hvordan kommunene oppfattet sitt eget beredskapsarbeid, i forhold til det lovpålagte og styrende rammeverket. Til tross for at kommunene hadde god kjennskap til hva som forventes av dem, er det tydelig at det er utfordrende å oppfylle kravene i det lovpålagte rammeverket. Dette understøttes av funn både i tilsynsrapportene til Statsforvalteren, og kommuneundersøkelsen til DSB (2021). Flere informanter trakk frem hindringer som tid og penger, samt å få andre sektorer i kommunen til å jobbe med beredskap for sitt ansvarsområde. Det synes som at samvirkeprinsippet foreløpig ikke står sterkt nok i arbeidet, noe som er med på å gjøre det kommunale beredskapsarbeidet fraksjonert og uoversiktlig. Den digitale risikoen utfordrer beredskapsarbeidet ytterligere, da digitaliseringen øker behovet for risikoanalyser- og kartlegging. Vi har argumentert for at tidsintervallet for ROS-analyser bør skjerpes, fordi digitalisering medfører hyppigere endringer i risikobildet, samt at ulike risiko- og sårbarhetsfaktorer påvirker hverandre på nye måter.

I det andre forskningsspørsmålet så vi på hvordan digital risiko inngikk i prosessen for utvikling av beredskap. Vi satt her søkelys på fire virkemidler kommunene bruker for å håndtere digital risiko. For det første virker det utbredt å overlate arbeidet med digital risiko til de i kommunen som besitter nødvendig kompetanse, fremfor å styrke kompetansen i beredskapsavdelingen. Et annet virkemiddel er å tjenesteutsette IT-driften til eksterne fagmiljøer, enten det er interkommunale samarbeid eller private tjenestetilbydere. For det tredje virker kjennskap til enten selvopplevde eller andre digitale uønskede hendelser å øke fokuset på viktigheten av digital risiko. For det fjerde virker ROS-analysen å være et viktig verktøy, men at det varierer hvorvidt resultatet faktisk bidrar til økt fokus på digital risiko eller beredskapsetablering. Vi har også argumentert for hvordan operasjonalisering av risikobegrepet og økt fokus på sikkerhetskultur kan hjelpe kommuner med å se digital risiko som en del av den helhetlige beredskapen.

I det tredje forskningsspørsmålet så vi på hvordan digitale uønskede hendelser beskrives i beredskapsplanverket. Her viser funn at dette sjeldent gjøres. Totalt sett var det tre av ti kommuner i utvalget som hadde beskrevet digitale uønskede hendelser i beredskapsplanverket. Det kan synes som at det er utfordrende for de som ikke har beskrevet digitale uønskede hendelser å analysere håndteringsevnen for slike hendelser. Vi har argumentert for at det virker hensiktsmessig å gjennomføre beredskapsanalyser som også analyserer digitale uønskede hendelser, for å styrke håndteringsevnen til kommunen.

Det siste forskningsspørsmålet diskuterte utfordringer med beredskapsarbeidet. Funnene indikerte at kommunene sliter med å etablere en sikkerhetskultur der alle forstår viktigheten av å etablere "god" beredskap. I tillegg diskuterte vi hvordan mangel på tverrfaglig kompetanse gjør det vanskelig for IT- og beredskapsavdelingen å forstå hverandres fagfelt. Dette kan videre gjøre det vanskelig å etablere et godt samarbeid mellom avdelingene. Vi har derfor stilt spørsmålstegn ved hvorfor ikke flere IT- og beredskapsavdelinger jobber tettere sammen om sikkerheten. Vi har argumentert for at rådgivende og veiledende organ som Datatilsynet, NSM, Kommune-CSIRT og KommIT i større grad bør brukes som ressurser i de kommunene som har behov for det, for å oppfylle den kommunale beredskapsforskriftens § 7 om nødvendig opplæring. Etter all sannsynlighet vil dette også påvirke sikkerhetskulturen i kommunen, som etter organisasjonsmodellen til Jacobsen og Thorsvik (2013), vil kunne påvirke kvaliteten av beredskapsplanen som et sluttprodukt til det bedre.

I diskusjonskapittelet er det diskutert lite rundt hvordan kommunens geografi og innbyggertall påvirker integreringen av digital risiko i beredskapsarbeidet. Dette begrunnes med at studien ikke har avdekket pålitelige og tydelige sammenhenger på dette feltet. I stedet har vi argumentert for at kommunens evne til å integrere digital risiko i beredskapsarbeidet i større grad beror på andre faktorer. Disse faktorene omhandler blant annet ressurser, kompetanse og risikopersepsjon. I tillegg spiller det styrende og lovpålagte rammeverket en viktig rolle i hvordan kommunens beredskapsarbeid tilnærmer seg digital risiko.

I forlengelsen av dette kan vi gå over til oppgavens konklusjon, der diskusjonen brukes for å besvare problemstillingen.

8.0 Konklusjon

Gjennom prosjektet har hovedformålet vært å finne svaret på denne problemstillingen:

> *Hvordan integreres digital risiko og digitale uønskede hendelser i det kommunale beredskapsarbeidet?*

I lys av de empiriske funnene, og diskusjonene rundt disse, kan det virke som at kommunene sliter med å følge det lovpålagte og styrende beredskapsrammeverket i praksis. Flere av kommunene feiler blant annet i å oppfylle samvirkeprinsippet, ved at det ikke er et etablert et tilstrekkelig samarbeid mellom IT- og beredskapsavdelingen.

Det brukes tilsynelatende fire virkemidler for å håndtere digital risiko. Det første er å overlate håndteringen av den digitale risikoen til de med mest digital kompetanse, som ofte er IT-avdelingen i kommunen. Det andre er å tjenesteutsette både drift og risikohåndteringen til eksterne selskaper eller interkommunale samarbeid. Det tredje er å innføre risikoreduserende tiltak *etter* at en hendelse har inntruffet. Det fjerde er å vurdere digital risiko i ROS-analysene, for å kartlegge risikobildet til kommunen.

Overordnet sett er det kun de to siste virkemidlene som passer overens med teorien om beredskapsetablering. Problemet er imidlertid at arbeidet ofte stoppet med ROS-analyse, slik at det ikke ble etablert verken beredskap eller en plan for disse hendelsene. Kun tre kommuner hadde beskrevet digitale uønskede hendelser i beredskapsplanen, men ingen av disse henviste til verken beredskapsanalyser eller evalueringer av slike hendelser.

I dette henseende er svaret på problemstillingen at digital risiko *i liten grad* integreres i det kommunale beredskapsarbeidet.

8.1 Våre anbefalinger

Gjennom oppgaven har vi både henvist til, og argumentert for, at risikodefinisjoner, beredskapsdefinisjoner og lovpålagte krav *ikke* eksplisitt nevner digital risiko. Det er imidlertid ingen grunn til at det skal være slik. Dette er fordi en definert risikokilde utgjør en potensiell fare, uavhengig av hvilket adjektiv (digital eller fysisk) som blir brukt for å kategorisere den. Det er dermed påfallende at digitale risikoer i større grad bør betraktes som et kritisk element å håndtere i det kommunale beredskapsarbeidet. Kommuner bør bruke mer ressurser på å

kartlegge egen sårbarhet for at en sektorovergripende digital uønsket hendelse oppstår. For å få til dette bør kommunen bruke ressurser på lære opp de ansatte til å tenke sikkerhet, og se viktigheten av et helhetlig beredskapsarbeid. De nasjonale samfunnssikkerhetsprinsippene bør fortsette å prege beredskapsarbeidet i kommunen. Dette forutsetter at samvirkeprinsippet blir en mer integrert del av sikkerhetskulturen.

I en forlengelse av dette anbefaler vi kommuner å undersøke hvilke muligheter som ligger i et mer helhetlig beredskapsarbeid, og følgelig hvordan dette kan gjøres. I tillegg anbefaler vi å rette mer fokus på hvordan ulike risiko- og sårbarhetsfaktorer påvirker hverandre, spesielt rettet mot samspillet mellom digital og fysisk risiko. Videre anbefaler vi å arbeide mer aktivt med samvirkeprinsippet, herunder samarbeidet mellom beredskapsmiljøet og andre fagmiljøer i kommunen. Avslutningsvis anbefaler vi kommunene å i større grad vurdere hvilke muligheter som ligger i å styrke det tverrsektorielle samarbeidet med institusjoner som blant annet Datatilsynet, NorSIS, Kommune-CSIRT og NSM. Disse anbefalingene er generiske, og gjelder uavhengig av kommunens størrelse og geografiske beliggenhet.

8.2 Forslag til videre forskning

Masteroppgaven vår har belyst hvordan digital risiko integreres i kommunenes beredskapsarbeid. Av vår oppfatning har dette vært et lite utforsket område, som bør undersøkes mer. Vi ser blant annet et behov for en grundigere og mer omfattende kartlegging av hvordan kommuners beredskapsorganisasjoner håndterer digital risiko. For å kunne satse og investere på dette feltet er det avgjørende å ha et godt empirisk beslutningsgrunnlag. Videre bør det utforskes hvorvidt dagens lovverk er dimensjonert for digital risiko. Vi er av den formening at lovverket ikke utelukker digital risiko, men det bør grundigere undersøkes hvordan lovverket tolkes i praksis på dette feltet. I tillegg vil en interessant studie være hvordan kompetanse og ressurser påvirker kommuners evne til å håndtere digitale trusler. En slik studie vil kunne avdekke hvilke områder det må satses på. Til sist vil en interessant oppfølgning av dette prosjektet være å se på hvorvidt interkommunale samarbeid om IKT-sikkerhet styrker eller svekker det kommunale beredskapsarbeidet til de enkelte kommunene som er med. I vårt prosjekt har vi så vidt vært innom denne diskusjonen, men temaets omfang krever ytterligere utredninger og undersøkelser.

Kilder

Aker, K. S. (2020, 14. oktober). DSBs webinar Digital Sikkerhet 2020: *Sentral krisehåndtering og Justis- og beredskapsdepartementets ansvar ved digitale hendelser*. Innlegg presentert ved Justis- og beredskapsdepartementet. 14:45. Hentet fra: https://www.dsb.no/kurs-og-konferanser/andre/webinar-om-digital-sikkerhet/ [Sett: 14.10.2020]

Alvesson, M. and Deetz, S. (2000). *Doing Critical Management Research*. Sage, Thousand Oaks, CA.

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

Aven, T. & Renn. O. (2010). *Risk management and governance.* London: Springer-Verlag Berlin Heidelberg.

Aven, T., Renn, O. & Rosa, E. A. (2011). *The ontological status of the concept of risk*, Safety Science 49

Aven, T., Røed, W. & Wiencke, H. S. (2017). *Risikoanalyse* (2. Utg.). Oslo: Universitetsforlaget

Blaikie, N. (2010). *Designing social research: The logic of anticipation (2. Utg.)*. Cambridge: Polity Press.

Bergsjø, H., Windvik, R. og Øverlier, L. (2020). *Digital sikkerhet - En innføring.* Oslo: Universitetsforlaget

Brekke, A. & Gundersen, M. (2019, 21. mars). *Slik fungerte løsepengeviruset som rammet Hydro.* Norsk Rikskringkasting. Hentet fra: https://www.nrk.no/norge/slik-fungerer-losepengeviruset-som-rammet-hydro-1.14481782 [Lest: 14.06.2021]

Brun, W. (1997). *Subjektive determinanter for lekfolks risikovurderinger*. Nordisk Psykologi, 49(1), 1-11.

Bryman, A. (2004). *Social research methods* (2nd ed.). Oxford: Oxford University Press.

Boyesen, M. (2003). *Risikopersepsjon-En innføring i fagfeltet*. Direktoratet for sivilt beredskap.

Christensen, T., Egeberg, M., Lægreid, P. og Aars, J. (2014). *Forvaltning og politikk (4. utgave)*. Oslo: Universitetsforlaget

Clarke, L., & Perrow, C. (1996). *Prosaic Organizational Failure.* American Behavioral Scientist, 39 (8), 1040-1056.

Danermark, B., Ekström, M., Jakobsen, L., & Karlsson, J. C. (2002). *Explaining Society: Critical Realism in the Social Sciences*. London: Routledge.

Datatilsynet. (u.å.). *Datatilsynets oppgaver.* Hentet fra: https://www.datatilsynet.no/om-datatilsynet/oppgaver/ [Lest: 20.04.2021]

Departementene. (2019a). *Nasjonal strategi for digital sikkerhet*. Hentet fra: https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/ [Lest: 04.03.2021]

Departementene. (2019b). Nasjonal strategi for digital sikkerhetskompetanse. Hentet fra: https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf [lest: 27.04.2021]

Digdir. (2020). *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner.* Kunnskapgrunnlag – en dokumentstudie. Digitaliseringsdirektoratet. Oslo: Digitaliseringsdirektoratet.

Digdir. (u.å.). *Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål.* Digitaliseringsdirektoratet. Hentet fra: https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123#hva_handler_informasjonssikkerhet_om [Lest: 15.04.2021]

Digdir. (u.å.). *Kva er Digitaliseringsdirektoratet?.* Digitaliseringsdirektoratet. Hentet fra: https://www.digdir.no/om-oss/kva-er-digitaliseringsdirektoratet/703 [Lest: 15.04.2021]

DSB. (2014a). *Risikoanalyse av "Cyberangrep mot ekom-infrastruktur".* Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsb.no/globalassets/dokumenter/rapporter/risikoanalyse-av-cyberangrep-mot-ekom-infrastruktur.pdf

DSB. (2014b). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen.* Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/veileder-til-helhetlig-risiko-og-sarbarhetsanalyse-i-kommunen.pdf

DSB. (2015) *Veiledning for Fylkesmannens tilsyn med kommunal beredskapsplikt*. Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-

informasjonsmateriell/veiledere/veiledning_for_fylkesmannens_tilsyn_med_kommunal_beredskapsplikt.pdf

DSB. (2017) *DSB veileder: Samfunnssikkerhet i kommunenes arealplanlegging.* Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/samfunnssikkerhet_i_kommunens-arealplanlegging_metode-for-risiko_og_saarbarhetsanalyse.pdf

DSB. (2018) Veileder til forskrift om kommunal beredskapsplikt. Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsbinfo.no/DSBno/2018/tema/veileder-til-forskrift-om-kommunal-beredskapsplikt/

DSB. (2019) *Analyser av krisescenarioer*. Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra:https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf

DSB. (2020) *Høringsnotat – forslag til forskrift om organisering, bemanning og utrusting av brann- og redningsvesen og nødmeldesentralene (brann- og redningsforskriften).* Direktoratet for samfunnssikkerhet og beredskap. Hentet fra: https://hoering.dsb.no/Hoering/v2/1463

DSB. (2021). *Kommuneundersøkelsen 2021*. Direktoratet for samfunnssikkerhet og beredskap. Hentet fra: https://www.dsb.no/contentassets/2e46c5ab2c37436db36ba80a85cfbc51/kommuneundersokelsen-2021_publisert.pdf

DSB. (u.å.) *Ansvarsområder og roller*. Direktoratet for Samfunnssikkerhet og Beredskap. Hentet fra: https://www.dsb.no/menyartikler/om-dsb/ansvarsomrader-og-roller/

Engen, O., Kruke, B., Lindøe, P., Olsen, K., Olsen, O., & Pettersen, K. (2016). *Perspektiver på Samfunnssikkerhet*. Oslo: Cappelen Damm Akademisk.

Etterretningstjenesten. (2021) *Fokus 2021 - Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer.* Tilgjengelig fra: https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/fokus/rapporter/Fokus2021-web.pdf/_/attachment/inline/b9d52b53-0abe-4d1c-9c51-bf95796560bf:8dd66029b7efb38aab37d13e8b387d2e6ed0bd05/Fokus2021-web.pdf

FHI. (06.10.2020). *Trinn 5. Tiltaksvurdering.* Folkehelseinstituttet. Hentet fra: https://www.fhi.no/nettpub/overvaking-vurdering-og-handtering-av-covid-19-

epidemien-i-kommunen/ti-trinn2/7.-tiltaksvurdering/?term=&h=1#smitteverntiltak-som-kan-vurderes-ved-utbrudd

Forskrift om kommunal beredskapsplikt. (2011). Forskrift om kommunal beredskapsplikt (FOR-2011-08-22-894). Hentet fra https://lovdata.no/forskrift/2011-08-22-894

Hagen, S. M. (2020, 21. september). *Tysk kvinne døde etter ransomeware-angrep mot sykehus.* Computerworld. Hentet fra: https://www.cw.no/artikkel/hacking/tysk-kvinne-dode-etter-ransomeware-angrep-mot-sykehus [lest: 24.03.21]

Helgestad, B. (2021, 11. mars). NSMs Sikkerhetskonferanse 2021: *Trusler og trender innenfor digital sikkerhet i 2021 og felles digital grunnmur - et overblikk*. Innlegg presentert ved Østre Toten. 06:20. Hentet fra: https://nsm.no/kurs-og-konferanser/sikkerhetskonferansen/2021/program/trusler-og-trender-innenfor-digital-sikkerhet-i-2021-og-felles-digital-grunnmur-et-overblikk [Sett: 11.03.2021]

Instruks for dep. arbeid med samfunnssikkerhet mv. (2012). *Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering.* (FOR-2012-06-15-535). Hentet fra: https://lovdata.no/dokument/LTI/forskrift/2012-06-15-535

Jacobsen, D.I. (2009). *Perspektiver på kommune-Norge: en innføring i kommunalkunnskap*. Bergen: Fagbokforlaget.

Jacobsen, D. I., og Thorsvik, J. (2013). *Hvordan organisasjoner fungerer.* Bergen: Fagbokforlaget. (4. utgave)

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser?* Innføring i samfunnsvitenskapelig metode (3. utgave). Oslo: Cappelen Damm Akademisk.

Johannessen, A., Tufte, P. A., Christoffersen, Line. (2011). *Introduksjon til samfunnsvitenskapelig metode* (4. utgave) Oslo: Abstrakt Forlag AS.

Justis- og beredskapsdepartementet. (2017). *Risiko i et trygt samfunn - Samfunnssikkerhet.* (Meld. St. 10 (2016-2017)). Hentet fra: https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/no/pdfs/stm201620170010000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2021). *Samfunnssikkerhet i en usikker verden.* (Meld. St. 5 (2020-2021)). Hentet fra: https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf

Justis- og politidepartementet. (2002). *Samfunnssikkerhet. Veien til et mindre sårbart samfunn.* (Meld. St. 17 (2001-2002)). Hentet fra:

https://www.regjeringen.no/contentassets/ee63e1dd1a16409fa0bb737bfda9279a/no/pdfa/stm200120020017000dddpdfa.pdf

Justis- og politidepartementet. (2012). *Samfunnssikkerhet.* (Meld. St. 29 (2011-2012)). Hentet fra: https://www.regjeringen.no/contentassets/bc5cbb3720b14709a6bda1a175dc0f12/no/pdfs/stm201120120029000dddpdfs.pdf

Kartverket. (2021). *Norske fylker og kommunar.* Hentet fra: https://www.kartverket.no/til-lands/fakta-om-norge/norske-fylke-og-kommunar [lest: 25.03.21]

Kommunal- og moderniseringsdepartementet. (2021) *Vår felles digitale grunnmur – mobil-, bredbånds- og internettjenester*. (Meld. St. 28 (2020-2021)). Hentet fra: https://www.regjeringen.no/contentassets/e8441e5b035a4e18bbebf74737530c2f/no/pdfs/stm202020210028000dddpdfs.pdf

Kommune – CSIRT. (2021). *Digitalt situasjonsbilde - Rapport nr. 1 - 2021.* Tilgjengelig fra: https://kommunecsirt-no.offcenit.com/Digitalt-situasjonsbilde-K-CSIRT-no.1-2021.pdf

Kommune-CSIRT. (u.å.). *Kommune-CSIRT – et nasjonalt senter for kommuner og fylkeskommuner.* Hentet fra: https://kommunecsirt.no/om-oss

Kommuneloven. (2018). *Lov om kommuner og fylkeskommuner.* Lovdata. Hentet fra: https://lovdata.no/dokument/NL/lov/2018-06-22-83

KS. (2020, 16. desember). *KommIT-rådet.* Kommunesektorens Organisasjon. Hentet fra: https://www.ks.no/kommit [lest: 21. april 2021]

KS. (2021, 8. februar). *KS gir råd til kommuner for å redusere risiko for nye dataangrep.* Kommunesektorens Organisasjon. Hentet fra: https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/ks-gir-rad-til-kommuner-for-a-redusere-risiko-for-nye-dataangrep/ [lest: 06. mai 2021]

Kvale, S. (1997). Det kvalitative forskningsintervju. Oslo: Gyldendal Akademisk.

Lipshitz, R., & Strauss, O. (1997). Coping with Uncertainty: A Naturalistic Decision-Making Analysis. Organizational Behavior and Human Decision Processes, 69(2). 149-163.

Lunde, I. K. (2019). *Praktisk krise- og beredskapsledelse (2. utgave).* Oslo: Universitetsforlaget.

Microsoft Security Response Center. (2021, 13. april). *April 2021 Update Tuesday packages now available.* Hentet fra: https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/ [lest 19. april 2021].

Nappo, S. [StephaneNappo]. (2019, 27. oktober). The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: “Cyber security is much more than an IT topic”. #CyberResilience #Cybersecurity #CISO #ComprehensiveSecurity With @TopCyberNews. [Twitter]. Hentet fra: https://twitter.com/stephanenappo/status/1188574685983920129

Njå, O., Sommer, M., Rake, E., & Braut, G. (2020). *Samfunnssikkerhet: analyse, styring og evaluering.* Oslo: Universitetsforlaget.

NorSIS. (2019). *Nordmenn og digital sikkerhetskultur.* Norsk senter for informasjonssikring. Hentet fra: https://norsis.no/publikasjoner/

NorSIS. (2021) *Trusler og trender 2021.* Norsk senter for informasjonssikring. Tilgjengelig fra: https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

Norsk Hydro. (2020, 14. oktober). *Cyberangrep på Hydro*. Norsk Hydro. Hentet fra: https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/ [Lest: 14.06.2021]

NOU 2000:24. (2000). *Et sårbart samfunn.* Oslo: Justis- og beredskapsdepartementet.

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

NOU 2018:14. (2018). *IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.* Oslo: Justis- og beredskapsdepartementet.

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

NSM. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler.* Nasjonal Sikkerhetsmyndighet. Tilgjengelig fra: https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NSM. (u.å.). *Dette er NSM.* Nasjonal Sikkerhetsmyndighet. Hentet fra: https://nsm.no/om-oss/dette-er-nsm/

Perry, R. W., and Lindell, M. (2003). *Preparedness for Emergency Response: Guidelines for the Emergency Planning Process*. Disasters, 27(4), 336-350.

Pidgeon, N. F. & O’Leary. (2000). *Man-made disasters: why technology and organizations (sometimes) fail*. Safety Science 34 (2000) 15-30,

Politiet. (2020). *Krav og resultater for politiets responstid 1 tertial 2020.* Hentet fra https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/responstid/krav-og-resultater-for-politiets-responstid-1.-tertial-2020.pdf

Rake, E., & Sommer, M. (2018). *Beredskapsanalyse - En innføring*. Høgskulen på Vestlandet.

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

Renn, O. (2008). *Risk Governance – coping with Uncertainty in a Complex World*. London: Taylor & Francis LTD

Samfunnssikkerhetsinstruksen. (2017). Instruks for departementenes arbeid med samfunnssikkerhet (FOR-2017-09-01-1349). Hentet fra https://lovdata.no/forskrift/2017-09-01-1349)

SINTEF. (2016). *Kommunal beredskapsplikt – gir nye krav en bedre beredskapsevne?* Trondheim: SINTEF Teknologi og samfunn.

Sivilbeskyttelsesloven. (2010). Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (LOV-2010-06-25-45). From https://lovdata.no/lov/2010-06-25-45

Sovacool, B. K., Axsen, J. and Sorrell, S. (2018). *"Promoting novelty, rigor, and style in energy social science: Towards codes of practice for appropriate methods and research design."* Energy Research & Social Science, 45: 12–42.

Speed, J. (2020, 11. august). *Da nett-kriminelle stjal 100 norske bistandsmillioner.* Bistandsaktuelt. Hentet fra: https://www.bistandsaktuelt.no/nyheter/2020/norfund-da-nett-kriminelle-stjal-100-norske-bistandsmillioner/ [Lest: 14.06.2021]

Staurheim, A. (2013). *IKT-sikkerhet og beredskap i tre fylkeskommuner* (Masteroppgave, Universitetet i Stavanger). Hentet fra: https://uis.brage.unit.no/uis-xmlui/handle/11250/184893

Stortinget. (2020, 1. september). *IT-angrep mot Stortinget.* Stortinget. Hentet fra. https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2019-2020/it-angrep-mot-stortinget/ [Lest: 14.06.2021]

Stortinget. (2021, 19. mars). *Stortinget utsatt for IT-angrep.* Stortinget. Hentet fra: https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Hva-skjer-nyheter/2020-2021/stortinget-utsatt-for-it-angrep/ [Lest: 14.06.2021]

Sutcliffe, K.M & Vogus, T.J. (2007). *Organizational Resilience: Towards a theory and research agenda.* Innlegg presentert på IEEE International Conference on Systems, Man and Cybernetics. Hentet fra

https://www.researchgate.net/publication/220756654_Organizational_Resilience_Towards_a_Theory_and_Research_Agenda

SSB. (2020). 11342: *Areal og befolkning i kommuner, fylker og hele landet (K) 2007-2020.* Statistisk Sentralbyrå. Hentet fra: https://www.ssb.no/statbank/table/11342/tableViewLayout1/

SSB. (2021). *07459: Alders- og kjønnsfordeling i kommuner, fylker og hele landets befolkning (K) 1986-2021.* Statistisk Sentralbyrå. Hentet fra: https://www.ssb.no/statbank/table/07459/tableViewSorted/

Thommesen, J., K. (2021, 13. mai). *Nettangrep ga drivstoffmangel – viktig oljeledning delvis gjenåpnet.* Norsk Rikskringkasting. Hentet fra: https://www.nrk.no/urix/nettangrep-ga-drivstoffmangel-_-viktig-oljeledning-delvis-gjenapnet-1.15495436 [Lest: 25.05.2021]

Tomter, L., Kampevoll, F., Wergeland, P., Sandholt, R. K., Norum, H., Næss, O. H. (2020, 31. desember). *Jeg advarte kommunen*. Norsk Rikskringkasting. Hentet fra: https://www.nrk.no/norge/_-jeg-advarte-kommunen-1.15309066 [lest 08.03.2021]

Tjora, A. (2021). *Kvalitative forskningsmetoder i praksis (4. utgave).* Oslo: Gyldendal Akademisk.

Turton, W. & Mehrotra, K. (2021, 4. juni). *Hackers breached Colonial Pipeline using compromised password.* Bloomberg. Hentet fra: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Lest: 14.06.2021]

Vigsnæs, M., K., Døvik, O. & Carlsen, H. (2018, 5. desember). *Beredskapsplaner, pasientinformasjon og forskning kan være stjålet fra Helse Sør-Øst.* Norsk Rikskringkasting. Hentet fra: https://www.nrk.no/norge/beredskapsplaner_-pasientinformasjon-og-forskning-kan-vaere-stjalet-fra-helse-sor-ost-1.14325823 [Lest: 14.06.2021]

Woods, D. D. (2006). *Essential characteristics of resilience.* I E. Hollnagel, D. Woods, & N. Leveson, Resilience Engineering: Concepts and Precepts (s. 21-34). London: Ashgate.

Vedlegg 1: Forenklet intervjuguide til utsending

Introduksjonsrunde: En liten presentasjonsrunde av oss selv og oppgaven vår, der vi vil gå gjennom formålet med prosjektet, og høre litt om ansvarsområdet til informanten.

1. Hvordan er beredskapsorganisasjonen i kommunen strukturert?

2. Hvordan går dere frem for å etablere og endre beredskapen?

3. Hvordan er digitale uønskede hendelser omtalt/beskrevet i den kommunale beredskapsplanen?

4. Beskriv samarbeidet mellom IT- og beredskapsmiljøet?

5. Hva mener du er den mest hensiktsmessige måten å jobbe med å håndtere digital risiko?

6. Har dere opplevd digitale uønskede hendelser i kommunen?

Vedlegg 2: Intervjuguide

Introduksjonsrunde: En liten presentasjonsrunde av oss selv og oppgaven vår, der vi vil gå gjennom formålet med prosjektet, og høre litt om ansvarsområdet til informanten.

Formålet med å prosjektet er å undersøke hvordan norsk kommunal sektor tar hensyn til digitale uønskede hendelser og digital risiko i sitt beredskapsarbeid. I den forbindelse undersøker vi hvordan beredskaps- og IT-miljøer arbeider sammen. Utgangspunktet for studien er en hypotese om at kommuner er svært kompetente, og nyter lang og omfattende erfaringer på beredskapsområde knyttet til mer tradisjonelle risikoer, men at digitaliseringen har ført til en endring i risikobilde, og følgelig nye utfordringer for beredskapsarbeidet. Denne studien gjennomføres ved å intervjue et lite, ca. 10, kommuner og stille spørsmål vedrørende beredskapsarbeidet.

- *Husk å spørre om båndopptak*

1. Hvordan er beredskapsorganisasjonen i kommunen strukturert?

2. Hvordan går dere frem for å etablere og endre beredskapen?
Egne beredskapsplaner?

3. Hvordan er digitale uønskede hendelser omtalt/beskrevet i den kommunale beredskapsplanen? Evt. mer konkret: Hvordan er digitale uønskede hendelser inkludert i den kommunale beredskapsplanen?

a. Hvordan skal slike hendelser håndteres ifølge planen?
b. Er det noen forskjell i håndteringen av digitale uønskede hendelser versus andre typer uønskede hendelser?

4. Beskriv samarbeidet mellom IT- og beredskapsmiljøet?
a. Er det noen utfordringer knyttet til samarbeidet mellom den samfunnsfaglige og den tekniske delen av beredskapsarbeidet?

5. Hva mener du er den mest hensiktsmessige måten å jobbe med å håndtere digital risiko?

6. Har dere opplevd digitale uønskede hendelser i kommunen?

Presentere problemstilling, og spørre om de har noe annet de har å tilføye

Avslutning:
- *Spør om de vil ha tilsendt transkribert versjon*
- *Husk å signere samtykkeskjema*
- *Har du noen spørsmål?*
- *Takk og farvel*

Vedlegg 3: Informasjonsskriv om prosjektet

Vil du delta i forskningsprosjektet:
Beredskap for digitale hendelser – hva kan vi, og hva må vi lære?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt der formålet er å avdekke muligheter og utfordringer knyttet til beredskapsarbeid for digitale uønskede hendelser i kommunal sektor. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

I vårt masterprosjekt undersøker vi hvordan den kommunale beredskapsplanleggingen tar hensyn til digitale uønskede hendelser.

Hvem er ansvarlig for forskningsprosjektet?
Universitetet i Stavanger er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Du får spørsmål om å delta fordi vi ønsker å undersøke hvordan den kommunale beredskapsplanleggingen tar hensyn til digitale uønskede hendelser. I tillegg ønsker vi å undersøke hvordan digitale risikoer kan passe inn i det etablerte og, kall det gjerne tradisjonelle, rammeverket for beredskapsarbeid i norske kommuner. I den forbindelse anser vi deg og din rolle for å være en relevant og hensiktsmessig kilde på dette fagområdet.

Når vi skulle velge ut ti av landets 356 kommuner bestemte vi oss for å utelukke kommuner med mindre enn 3000 innbyggere, samt Oslo kommune. Vi gjorde dermed et strategisk utvalg av ti kommuner med ulikt innbyggertall, i størrelsesorden fra omtrent 3500 innbyggere til 200 000 innbyggere.

For ordens skyld ønsker vi å opplyse om at vi fikk din kontaktinformasjon etter å ha tatt kontakt med sentralbordet til kommunen.

Hva innebærer det for deg å delta?

I dette forskningsopplegget tar vi sikte på å gjennomføre et semi-strukturert intervju i løpet av siste halvdel av februar, med en tentativ varighet på omtrent 30 minutter. Intervjuet vil omhandle utfordringer og problemstillinger knyttet til beredskapsarbeid med digitale risikoer. Videre vil vi fokusere på potensielle barrierer mellom det tekniske og samfunnsfaglige beredskapsarbeidet, samt hvordan digitale risikoer kan inkluderes i det øvrige beredskapsarbeidet i kommuner. Denne tematikken vil naturligvis bli konkretisert under intervjuet.

Opplysningene som samles inn under intervjuet vil behandles anonymt under hele prosjektarbeidet, og eventuelle personopplysninger som måtte fremkomme under intervjuet vil bli slettet. Det er verdt å påpeke at det er den faglige tematikken som står i fokus, ikke hvordan kommunen konkret jobber. 2

Til informasjon vil det bli tatt lydopptak av intervjuet for å kunne verifisere utsagn, om dette godkjennes av deg. All data fra intervjuet som anvendes i studien vil bli sendt til deg for sitatsjekk og/eller godkjenning.

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.
Du og dine svar vil ikke kunne gjenkjennes i publikasjonen.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 15.06.2021. Lydopptak fra intervju vil bli slettet etter prosjektslutt.

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

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

Hva gir oss rett til å behandle personopplysinger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.
På oppdrag fra Universitetet i Stavanger har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

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

- Universitetet i Stavanger ved Eivind Lars Rake - 91336270
- Vårt personvernombud: personvernombud@uis.no

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

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

Med vennlig hilsen

Eivind Lars Rake
(Forsker/veileder)

Nora Sande & Jo Lindberg Augestad
(Studenter/forfattere)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet [Beredskap for digitale hendelser- hva kan vi, og hva må vi lære?], og har fått anledning til å stille spørsmål. Jeg samtykker til:

☐ Å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 4: Godkjenning NSD

Behandlingen av personopplysninger er vurdert av NSD. Vurderingen er:

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 26.01.2021, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

DEL PROSJEKTET MED PROSJEKTANSVARLIG
Det er obligatorisk for studenter å dele meldeskjemaet med prosjektansvarlig (veileder). Det gjøres ved å trykke på "Del prosjekt" i meldeskjemaet.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 15.06.2021.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Nvivo er databehandler i prosjektet. NSD legger til grunn at behandlingen oppfyller kravene til bruk av databehandler, jf. art 28 og 29.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET NSD
vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Vedlegg 5: Beskrivelse av digitale angrepsmetoder

Phishing: Phishing, eller "nettfiske", er en metode der en ondsinnet aktør forsøker å lure til seg sensitiv informasjon, som for eksempel kredittopplysninger, personopplysninger eller annen informasjon som kan bruker til et spesifikt formål. Vanlige metoder innebærer å sende en falsk e-post, eller ringe.

DDoS: DdoS, eller "distribuert tjenestenektangrep" er en form for digitale angrep der en ondsinnet aktør bruker et nett av datamaskiner for å oversvømme eller overbelaste en ressurs på internett. Et eksempel kan være om en ondsinnet aktør skaper så mye trafikk på et nettsted at nettstedet blir utilgjengelig. Formålet kan gjerne være å kreve betaling for å avslutte angrepet. Et slikt angrep kan også brukes i samspill med andre metoder for å tilegne seg informasjon.

CEO-fraud: CEO-fraud, eller "direktørsvindel" er en metode der en ondsinnet aktør tar i bruk e-post eller tekstmelding og utgir seg for å være sjefen til vedkommende som blir kontaktet, eventuelt en kollega. Formålet er å tilegne seg sensitiv informasjon, ved å utgi seg for å være en offeret kjenner. Et eksempel kan være at offeret får beskjed av sin sjef om at du må sende betalingsdetaljer på nytt i forbindelse med utbetaling av lønn.

Solar Wind: Solar Wind Orion-plattformen er et system for overvåking, analyse og administrering av IT-systemer eksternt. Det var svært mange selskaper som brukte denne plattformen. Noen måneder før angrepet hadde noen på vellykket vis hacket plattformen og installert en bakdør, noe som gjorde at angriperne fikk tilgang til mange av de IT-systemene som brukerne av plattformen hadde.

Løsepengevirus: Løsepengevirus, eller "ransomeware", er digitale angrep der hensikten er å kreve penger for å avslutte angrepet, eller gi tilbake filer og informasjon som gjerne er kryptert under angrepet. I Norge har det vært flere store hendelser med løsepengevirus, der blant annet Norsk Hydro og Helse Sør-Øst har blitt utsatt for alvorlige angrep.

Kryptovirus: Kryptovirus er en type digitalt angrep der hensikten er å kryptere filer, slik at informasjon blir utilgjengelig for den som er utsatt. Kryptovirus skjer ofte i form av løsepengevirus, der det må betales for å få tilgang til filene igjen.

Vedlegg 6: Beskrivelse av tidligere digitale uønskede hendelser

Colonial Pipeline:

Colonial Pipeline er et selskap som drifter den største drivstoffrørledningen i USA. Selskapet ble i april 2021 utsatt for et digitalt angrep, som fikk voldsomme konsekvenser for selskapets tilbud av drivstoff på USAs østkyst. Angrepet skal tilsynelatende ha skjedd som følge at et enkelt passord på avveie. I tillegg til å sette store deler av driften ut av spill, ble en stor mengde informasjon stjålet og kryptert. Selskapet betalte hackergruppen 4,4 millioner dollar kort tid etter angrepet (Turton & Mehrotra, 2021).

Helse Sør-Øst:

I januar 2018 ble Helse Sør-Øst, som sørger for spesialhelsetjenester til omtrent tre millioner nordmenn, utsatt for et omfattende digitalt datainnbrudd. Det er fortsatt uvisst konkret hva angriperne fikk med seg, men ettersom de hadde fått administratortilgang hadde de potensielt tilgang til hele nettverket. Her ligger pasientdata, beredskapsplaner og forskningsdata. PST måtte til slutt henlegge saken, da det visste seg utfordrende å finne gjerningspersonene (Vigsnæs, Døvik og Carlsen, 2018).

Norfund:

Gjennom nettfiske og direktørsvindel klarte ondsinnede aktører å skaffe nødvendig kontaktinformasjon mellom Norfund og en partner i Bangkok. Norfund skulle betale ut en betydelig sum i bistandpenger til et prosjekt i Asia, men en ondsinnet aktør plukket opp dialogen, og fungerte som et mellomledd i kommunikasjonen mellom Norfund og partneren i Asia i flere måneder. Angrepet resulterte i at 10 millioner dollar ble overført fra Norfund til den ondsinnede aktøren, i stedet for at pengene gikk til partneren som avtalt. Angriperen hadde manipulert samtalene, som medførte at betalingsdetaljene Norfund trodde tilhørte partneren, i realiteten tilhørte angriperen (Speed, 2020).

Norsk Hydro:

En stor digital hendelse forårsaket av viruset «LockerGoga». Med dette viruset kunne aktørene som stod bak angrepet blant annet endre passordene til brukerne av systemet, og således kaste dem ut. Viruset låste videre filer og sikkerhetskopier, mens de ansatte var utestengt av systemet

(Brekke & Gundersen, 2019). Aktørene krevde at Hydro skulle betale løsepenger i form av kryptovaluta for at de skulle få tilgang til systemene igjen. Hydro betalte ingenting, men angrepet kostet dem likevel om lag 600 millioner kroner i form av tapt inntekt, ifølge dem selv (Norsk Hydro, 2020).

Stortinget:

Stortinget ble i august 2020, og i mars 2021, utsatt for flere digitale angrep. Det ble registrert innbrudd på epostkontoene til flere stortingsrepresentanter og ansatte (Stortinget, 2020). I det siste angripet var det sårbarheter i Microsoft Exchange som ble utnyttet. I verste fall kunne angrepet fått konsekvenser for demokratiske prosesser (Stortinget, 2021).

Sykehuset i Tyskland:

Universitetssykehuset i Düsseldorf ble utsatt for et løsepengevirusangrep, som rammet en rekke av sykehusets IT-systemer. Angrepet førte til at sykehuset vurderte det som for risikabelt å skrive inn nye pasienter. Dermed måtte blant annet en ung kvinne fraktes til et sykehus som lå en halvtime unna. Kvinnen døde i løpet av tiden den ekstra kjøreturen til det andre sykehuset tok (Hagen, 2020).