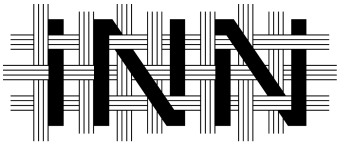

Høgskolen
i Innlandet

Handelshøgskolen i Innlandet - fakultet for økonomi og samfunnsvitenskap

Ole Eskild Billington, Jostein Thunæs Kråkemo og Eirik Strømmen Engum

Masteroppgave

Digital sikkerhet i sivil sektor

Hovedtendenser og utfordringer

Cybersecurity in the civilian sector:

Tendencies and challenges

Master i offentlig ledelse og styring - erfaringsbasert

MPABR4901

2023

Forord

Vi startet på studiet i 2019 med et ønske om å utvikle oss som ledere for å ruste oss for videre karriere. Studiet har gitt oss rikelig med påfyll, og gjort oss til mer reflekterte mennesker. Mye har skjedd i perioden fra vi startet på studiet og frem til innlevering av denne oppgaven. I første omgang ble vi et halvt år inn i studiet truffet av koronapandemien som førte til omstilling av studiehverdagen fra obligatorisk oppmøte på studiesamlinger til nettundervisning.

På et mer personlig nivå har Jostein byttet stilling innad i Forsvaret flere ganger. Han har gått fra Gardermoen via Rygge til Nederland, hvor han fortsatt arbeider. Eirik valgte å forlate Forsvaret og satser på en karriere innen cybersikkerhet, noe som førte til at han flyttet til Oslo. Ole Eskild besluttet også å si farvel til sin tid i Forsvaret og jobber nå sammen med Eirik. I mellomtiden ble Ole Eskild pappa, noe som har beriket hans liv ytterligere. Til tross for store endringer, noen forsinkelser, og en global pandemi, så har vi endelig fått levert en oppgave vi er stolte av. Oppgaven er et resultat av utallige diskusjoner om problemstillinger og metoder, og tusenvis av små eller store endringer. Resultatet er i et snevert perspektiv en oppgave som endelig er levert, men i et bredere perspektiv er oppgaven et resultat at vi er mer reflekterte og kunnskapsrike mennesker enn da vi startet. Vi er alle fornøyde med å ha startet på studiet, men også fornøyd med å være ferdige. I neste omgang gleder vi oss til å anvende kunnskapen i arbeidslivet spesielt, og i livet generelt.

Avslutningsvis må vi rette en stor takk til en gruppe mennesker som har støttet oss, motivert oss, og hjulpet oss med å prioritere studiene i en ellers hektisk hverdag. Våre bedre halvdeler: Hanna, Guro og Charlotte. Vi vil også rette en takk til lærerne ved Høgskolen i Innlandet som har gjort fagmaterialet forståelig, samtidig som det har vært underholdende i forelesninger.

"*Kunnskapen er det høyeste av alle goder, for ingen kan klare å stjele den, og ingen kan måle dens verdi eller ødelegge den"* - Hitopadesha

Takk for oss!

Oslo 15.05.2023
Ole Eskild Billington, Jostein Thunæs Kråkemo og Eirik Strømmen Engum

Sammendrag

Norge digitaliseres stadig mer, og er i dag et av verdens mest digitaliserte land. De aller fleste arbeidstakere i Norge må utføre deler av eller hele sin jobb ved hjelp av digitale systemer. Den stadig økende digitaliseringen gir mange muligheter for automatisering og effektivisering, men skaper også utfordringer. Digitale angrep omtales jevnlig i media, og den siste tiden har det vært en økning i frekvens. Aktører som ønsker å skade norske virksomheter, kan nå gjøre dette fra hvor som helst i verden, og de kan gjøre dette skjult og i stor grad uten risiko. I lys av den raske digitale utviklingen i Norge, har denne masteroppgaven gjennomført dokumentstudier av norske myndigheters styrende dokumenter for digital sikkerhet, for å avdekke utviklingstrender i disse dokumentene. Oppgavens har valgt fire styrende dokumenter som grunnlag for dokumentanalysen, disse er: NOU:2015 kjent som Lysneutvalgets rapport (2015), Stortingsmelding 38 (2016-2017) kjent under navnet *IKT-sikkerhet – et felles ansvar*, *Nasjonal Strategi for Digital Sikkerhet* (2019) og lov om nasjonal sikkerhet (2019). Oppgaven analyserer først disse styrende dokumentene hver for seg ved hjelp av Asdal og Reinertsen (2020) sitt verktøy for dokumentanalyse og Carol Bacchis (2009) metode for analyse av policydokumenter. Oppgaven benytter så disse identifiserte trendene til å peke på mulige utfordringer med implementeringen av ulike tiltak for å bedre den digitale sikkerheten i norske virksomheter.

Generelt oppleves de styrende dokumentene som relativt samkjørte i sine prioriteringer, og at endringene kun unntaksvis endres fra dokument til dokument. Det oppleves imidlertid som at dokumentene blir mer operasjonaliserte og konkrete i sine anbefalinger, jo senere de er publisert. Dette kan ha en sammenheng med at virksomhetene selv får mer ansvar for å strukturere sitt arbeid med digital sikkerhet. Av oppgavens analyser fremkommer det at området digital sikkerhetskultur er generelt lite prioritert gjennom alle de analyserte dokumentene, og at økning av kompetanse på IKT-sikkerhet er en vedvarende prioritet.

Oppgaven har videre pekt på at digital sikkerhet er et gjenstridig problem som ikke kan løses permanent. Samordning synes å være den største utfordringen for myndighetenes arbeid med digital sikkerhet. Dette kommer til syne gjennom Justis- og beredskapsdepartementets manglende informasjon om nasjonens digitale sikkerhetssituasjon og en generell mangel på IKT-sikkerhetskompetanse i Norge. Intra-organisatoriske faktorer som tydelig ansvarliggjøring, gjensidig tillit mellom virksomheter og myndigheter, og god kommunikasjon vil være viktig for fremtidig samordning av arbeidet.

Abstract

Norway is one of the most digititalized countries on the planet. Just about every organization is relying on digital systems to support their processes and achieve their objectives. Unfortunately, the increasingly rapid transfer into digital systems comes at a price. Organizations are threatened by increasingly creative adversaries that seek to exploit the organizations weaknesses through the gathering of information, interrupting processes and potentially challenging the very existence of the targeted organization. In light of this, our master thesis seeks to explore the governing public documents regulating Norway's policy on cybersecurity. This has been done through analyzing the following documents: NOU:2015, know as the report of the "Lysne" public committee (2015), Stortingsmelding 38 (2016-2017), known to be called "IKT-security – a shared responsibility", *Norwegian strategy for digital security* (2019) and Law of national security (Sikkerhetsloven) (2019). This thesis has analyzed these documents by using Asdal and Reinertsen's (2020) theory on document studies, and Carol Bacchi's (2009) method for analyzing policy documents.

The main findings of this thesis has been that the governing documents generally seem to be synchronized in terms of priorities throughout the period between 2015 and 2019. The changes we see are that the priorities get gradually more operationalized over the years. A possible cause to this could be the increased responsibility that the organizations themselves are given in order to structure their own work with digital security. We can also see from the analysis that culture aspects linked to digital security have not been prioritized, and that the general lack of qualified people with IT and cybersecurity education and background persists.

The thesis also points out that cybersecurity seems to be a so-called "wicked problem", which cannot be solved permanently. This means that work to improve cybersecurity within organizations is a never ending process. Furthermore, collaboration and synchronization of cybersecurity work across all sectors of the country continues to be a challenge. The Department of Justice and Public Security are not fulfilling their responsibilities as the coordinating department, which is visible through the lack of shared information regarding the general status of cybersecurity in Norway. Intra-organizational factors such as responsibilities, mutual trust between government and organizations, and communication will continue to be important factors in the future work of coordinating and organizing cybersecurity in Norway.

Innholdsfortegnelse

1 Innledning

I en tid der teknologien utvikler seg i et lynraskt tempo, har det aldri vært viktigere å ha solid digital sikkerhet. Digitalisering i norsk offentlig sektor er på god vei, og det ser ikke ut til at prosessen vil sakke ned med det første. I 2022 rykket Norge opp på femteplass i det uoffisielle EM i digitalisering basert på tall fra EU om EU/EØS-land sin digitale modenhet (European Commission, 2022). Utviklingen omfatter en rekke aspekter, fra elektroniske tjenester og kommunikasjon til automatisering av ulike administrasjonsprosesser. Dette bidrar til økt effektivitet, reduserte kostnader og forbedret informasjonsflyt mellom ulike offentlige etater og innbyggerne (European Commission, 2022). Digitaliseringen medfører imidlertid ikke utelukkende positive effekter, noe som blir tydeliggjort gjennom den betydelige økningen av digital kriminalitet (Politiet, 2023). Selv om potensielle utfordringer kan oppstå, knyttet til sikkerhet og personvern, fortsetter innsatsen for å digitalisere den offentlige sektoren i Norge med stor entusiasme og engasjement fra både myndigheter og befolkning.

Digitaliseringen av samfunnet er teknologidrevet, som mye annen utvikling i samfunnet. Ny teknologi innføres raskere enn hva menneskene antas å kunne håndtere, og måten man håndterer teknologien bærer preg av dette. Et eksempel på et lignende scenario er fra da biler ble allemannseie, førte dette til en ekstrem økning i trafikkulykker på 50- og 60-tallet. Teknologien var tilgjengelig, men man hadde ikke tilstrekkelige sikkerhetssystemer tilgjengelig for å benytte teknologien på en trygg nok måte til at man unngikk uønskede hendelser, herunder ulykker med og uten døden til følge. Dagens teknologi er på samme måte utviklet og gjort tilgjengelig, men tilstrekkelige sikkerhetsmekanismer er ikke etablert, særlig knyttet til de menneskelige aspektene ved digitaliseringen. Det finnes gode råd for organisasjoner som ønsker å styrke seg innen digital sikkerhet, men disse kan være vanskelige å følge opp og tilpasse til egen organisasjon. Det er derfor betimelig at myndighetene involverer seg, og bidrar til å øke nivået på den digitale sikkerheten, på samme måte som myndighetene har bidratt til økt trafikksikkerhet.

2 Problemstilling / forskningsspørsmål

Krav til sikkerhet er ikke et nytt fenomen i organisasjoner og virksomheter i Norge. Sikkerhet har lenge vært et viktig tema, og man ser i mange etablerte organisasjoner som opererer med risiko at sikkerhet har hatt høy prioritet. I det klassiske helse, miljø og sikkerhets-perspektivet

(HMS) ser man at det er skapt sterke kulturer, gode rutiner og metoder for kunnskapsdeling og risikostyring som sørger for lav forekomst av ulykker. Mange av kravene som stilles til HMS-arbeidet er pålagt gjennom lover og forskrifter. Når det gjelder digital sikkerhet så ser man i større utstrekning at dette perspektivet fortsatt oppleves nytt. I tillegg vanskeliggjøres det for virksomheter fordi cyberdomenet kan være svært teknisk og for de aller fleste uten spesiell interesse eller utdanning innen fagfeltet kan det også fremstå som utilgjengelig. Cyberdomenet endrer seg også raskt. En trussel i det digitale domenet forholder seg svært sjeldent lik over lang tid. Dette kan man se i utviklingen av forskjellig skadelig programvare, herunder opprettelsen av stadig nye skadelige programvarer. Innføringen av digitale sikkerhetskrav har likhetstrekk med tidligere teknologidrevet utvikling. I flybransjen så man eksempelvis at den teknologiske utviklingen gjorde flygning mulig under mer krevende forhold og over lengre avstander. Dette medførte imidlertid økte krav til personellet som opererte flyene. Det ble tydelig at ved økt bruk av fly som transportmiddel, og omfanget av hver enkelt ulykke, så måtte det stilles strenge krav til sikkerhet for å ivareta det flyvende personellet og passasjerenes sikkerhet. Paralleller kan trekkes til digitalisering i samfunnet. Det behandles etter hvert enorme mengder data for å kunne levere de nødvendige offentlige tjenestene til publikum, og på en rekke mer eller mindre kritiske systemer i de forskjellige offentlige sektorene. Både informasjon og tilgang til systemer kan utnyttes av trusselaktører for å oppnå forskjellige mål, herunder økonomisk vinning, aktivistiske mål, sabotasje eller etterretningsmål. Etter hvert som digitalisering har skutt fart og gitt mer effektive tjenester, har imidlertid også sårbarheten for at noen utnytter dette økt. Det har blitt gjennomført tiltak fra myndighetene for å forsøke å bøte på sårbarhetene gjennom forskrifter, strategier og opprettelse av offentlige organer som skal styrke motstandsdyktigheten. Samtidig som digitalisering skjer, er derfor et viktig suksesskriterium å utvikle motstandsdyktigheten, slik at mennesker og organisasjoner unngår uønskede hendelser og de ønskede effektene av digitalisering kan oppnås.

Oppgavens problemstilling gjøres videre dagsaktuell ved at stadige nyhetssaker om hendelser i cyberdomenet, hvor de potensielle tapene har gått fra tusenlapper til hundremillionersklassen, både for offentlige og private virksomheter. Dette har ført til at flere og flere får øynene opp for risikoene digitalisering medfører, og følgelig innfører tiltak for å motvirke dette. Det eksisterer allerede krav, strategier og rammeverk som er lagd for offentlige virksomheter fra styresmaktene, så hvorfor inntreffer angrep likevel ofte, og med tidvis enorm suksess for den angripende part? Med dette bakteppet vil det derfor være

interessant å undersøke hvilke endringer som har forekommet i offentlige myndigheters styrende dokumenter for arbeidet med styrking av digital sikkerhet i sivil sektor. Viser dokumentene endringer i tilnærmingen til digital sikkerhet, eller er det liten endring i hvordan myndighetene ønsker å sikre det digitale Norge? Vår hypotese er at på grunn av stor utvikling i trusselbildet og økning i hendelser, bør prioriteringene for digital sikkerhet endre seg i takt med dette. I neste omgang ønsker vi å diskutere hvilke utfordringer myndighetene står overfor i et instrumentelt organisatorisk perspektiv når de skal sette disse prioriteringene ut i praksis. Vår problemstilling blir derfor følgende: "**Hvilke hovedtendenser fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet og hvilke utfordringer står de overfor når det gjelder å sette disse prioriteringene ut i praksis?**". Vi vil besvare oppgavens problemstilling ved å se nærmere på følgende forskningsspørsmål:

1. Hvilke hovedtendenser fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet?
2. Hvilke utfordringer står Justis- og beredskapsdepartementet ovenfor når det gjelder å sette prioriteringene ut i praksis?

Denne oppgaven vil ta for seg problemstillingen ved å utføre en dokumentanalyse av relevant dokumentasjon. Dette vil bidra til å identifisere hovedtendenser og endringer knyttet til norske myndigheters prioriteringer i arbeidet med å styrke digital sikkerhet. Videre vil oppgaven drøfte hvilke utfordringer myndighetene kan møte når de implementerer disse prioriteringene i praksis. Oppgaven vil sette søkelyset på digital sikkerhet i Norge, med fokus på myndighetenes gjeldende dokumenter, perspektiver og strategier for styrking av digital sikkerhet, og utfordringene de trolig vil måtte overkomme for å oppnå den ønskede effekten.

2.1 Avgrensning

Oppgaven undersøker hvilke hovedtendenser som fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet. Vi har valgt å avgrense oppgaven til å kun analysere og undersøke et utvalg av dokumenter produsert i perioden 2015 til 2019. Årsaken til dette er at det vil være vanskeligere å kunne se effekten av arbeidet med implementering for dokumentasjon som er av nyere dato, og vil kunne bidra til å gjøre resultatene mindre troverdige.

Dokumentasjonen som er utvalgt som datagrunnlag er videre avgrenset til å være av eller for Justis- og beredskapsdepartementet. Dette departementet vil være det mest brukte eksempelet i våre drøftinger og konklusjoner.

I kraft av studiets faglige innretting, vil denne masteroppgaven undersøke aspekter knyttet til offentlig ledelse og styring, og gjennom det undersøke styrende dokumenter for digital sikkerhet i Norge. For mange vil de tekniske og teknologiske aspektene være de mest åpenbare diskursene innen digital sikkerhet, gjerne på nivået som handler om konkrete tiltak for å bedre den digitale sikkerheten. Denne oppgaven ønsker å forske på myndighetenes styrende dokumenter innen digital sikkerhet, da disse vil legge premissene for den videre retningen arbeidet med digital sikkerhet vil ta i norske virksomheter. Vi vil ikke redegjøre for, eller diskutere, tekniske aspekter ved digital sikkerhet.

3 Bakgrunn

Digital Economy and Society Index-rapporten (DESI) utgitt av Europakommisjonen har i flere år vurdert europeiske land på deres digitale konkurranseevne og innsats innen digitalisering. Norge rangeres høyt i flere kategorier, herunder bruk av digital teknologi og innovasjon (European Commission, 2022). Norge er også anerkjent som et av de ledende landene i Europa når det gjelder implementering og utnyttelse av ny teknologi (European Commission, 2022). I denne sammenheng bærer norske politikere et betydelig ansvar for å sikre at befolkningen drar nytte av ressursene som brukes på fellesskapets beste. Det innebærer en forpliktelse fra myndighetenes side til å fremme bruken av digitale løsninger innen både offentlige og private virksomheter. Digitalisering har potensial til å bringe betydelige fordeler, inkludert økt effektivitet, konkurransekraft og skapelsen av nye arbeidsplasser. Ved å integrere innovative teknologier i ulike sektorer kan man oppnå reduserte kostnader, forbedret kommunikasjon og samhandling mellom ulike aktører, samt økt fleksibilitet og tilpasningsevne i møte med endringer i markedet.

For å realisere disse målene er det viktig at politiske beslutningstakere utvikler strategier og investerer i infrastruktur som legger til rette for digital omstilling. Dette kan blant annet innebære støtte til forskning og utvikling, opplæring av arbeidskraft i nye ferdigheter samt tverrfaglig samarbeid mellom offentlig sektor, næringslivet, akademiske institusjoner og det sivile samfunnet. Samtidig må myndighetene være oppmerksomme på potensielle

utfordringer knyttet til digitalisering, som for eksempel sikkerhet og personvern. Det er derfor avgjørende å etablere robuste juridiske og regulatoriske rammeverk som beskytter enkeltpersoners rettigheter og interesser samt samfunnets samlede velferd. Ved å ta en aktiv rolle i digitaliseringen kan norske politikere bidra til en bærekraftig utvikling av landet, hvor både offentlige og private virksomheter drar nytte av teknologiens muligheter på en ansvarlig måte. Dette vil igjen føre til økt livskvalitet for den norske befolkningen og styrke Norges posisjon som et innovativt og fremgangsrikt samfunn på global arena.

Digitaliseringen av det norske samfunnet representerer samtidig en betydelig utfordring, ettersom den medfører økt kompleksitet og integrasjon av digital infrastruktur og systemer. Dette skaper avhengigheter og sårbarheter på tvers av ansvarsområder, sektorer og nasjoner, noe som krever en gjennomgående tilnærming for å sikre digital sikkerhet og personvern. Tilgjengelighet av digitale tjenester er også en forventning i dagens samfunn, hvilket legger ytterligere press på å ivareta sikkerheten i disse løsningene.

Norges første nasjonale strategi for digital sikkerhet ble introdusert i 2003, noe som gjorde landet til en pioner innen dette området (Departementene, 2019, s. 3). I tråd med endringer i trussellandskapet har denne strategien blitt revidert flere ganger – senest i 2019 (Departementene, 2019, s.). I 2015 utarbeidet Digitalt sårbarhetsutvalg (Lysneutvalget) en rapport kalt *Digital sikkerhet - sårbart samfunn – Beskytte enkeltmennesker og samfunn i en digitalisert verden* som analyserte digitale sårbarheter i det norske samfunnet (Departementene, 2019, s. 3). Denne rapporten la grunnlaget for Norges første stortingsmelding om digital sikkerhet, som ble publisert i 2017 under navnet *IKT-sikkerhet – et felles ansvar* (Justis- og beredskapsdepartementet, 2017). Dette markerte et skifte der temaet ikke lenger var begrenset til spesielt interesserte, men heller noe som angikk alle samfunnsaktører.

Norske myndigheter lanserte i 2019 den fjerde utgaven av *Nasjonal strategi for digital sikkerhet*, som tar høyde for utfordringene knyttet til den raske og omfattende digitaliseringen av samfunnet (Departementene, 2019, s. 3). Denne strategien bygger videre på tidligere versjoner og understreker behovet for et styrket samarbeid mellom offentlige og private aktører, både nasjonalt og internasjonalt. Hovedmålgruppen er myndigheter og virksomheter i privat og offentlig sektor, inkludert kommuner, men strategien har også som mål å øke

kunnskap og risikoforståelse hos privatpersoner for at de skal kunne benytte seg av teknologi på en trygg måte (Departementene, 2019, s. 3).

For å oppnå vellykket digitalisering er det essensielt at løsningene ivaretar krav til sikkerhet og personvern, slik at brukerne kan ha tillit til at de digitale tjenestene fungerer som de skal. Gjennom kontinuerlig utvikling av nasjonale strategier og tverrsektorielt samarbeid kan Norge bli bedre rustet til å møte de utfordringene som følger med digitaliseringen av samfunnet.

3.1 Myndighetenes arbeid med digital sikkerhet

I 2017 ble det oppnevnt et utvalg ved kongelig resolusjon som skulle utrede organisering og regulering av nasjonal IKT-sikkerhet. Utvalget kartla over nasjonale 150 lover og forskrifter som potensielt angikk IKT-sikkerhet på nasjonalt plan, men kun et mindretall av dem stilte eksplisitte IKT-sikkerhetskrav (Justis- og beredskapsdepartementet, 2018, s. 32). Enkelte lover og forskrifter, eksempelvis sikkerhetsloven og IKT-forskriften for finanssektoren, er omfattende og eksplisitte i bestemmelsene om IKT-sikkerhet. Av lover og forskrifter som er mer generelle i kravene om sikring finnes eksempelvis krav om internkontroll, produktsikkerhet og taushetsplikt, som indirekte regulerer IKT-sikkerhet (Justis- og beredskapsdepartementet, 2018, s. 32). I tillegg er det få eksempler på tverrsektorielle lover som inneholder krav om IKT-sikkerhet. Primært er det sikkerhetsloven, personopplysningsloven, lov om elektroniske tillitstjenester og forvaltningsloven. Disse stiller derimot krav om IKT-sikkerhet på ulik måte. Det må også nevnes at de fleste sektorene i Norge har regelverk som inneholder krav om IKT-sikkerhet, men det er store variasjoner mellom de sektorvise lovene og forskriftene (Justis- og beredskapsdepartementet, 2018, s. 33). Et godt eksempel på dette beskrives i utvalgets utredning; kravene for IKT-sikkerhet i regelverkene for petroleumssektoren og kraftsektoren er utformet på ulike måter. Olje- og gassindustrien har et funksjonsbasert regelverk innenfor helse, miljø og sikkerhet (Justis- og beredskapsdepartementet, 2018, s. 33). Petroleumsloven stiller krav om sikkerhet og forsvarlig petroleumsvirksomhet, men regelverket legger til grunn at virksomhetene selv vurderer risiko, setter akseptkriterier og beslutter relevante tiltak (Justis- og beredskapsdepartementet, 2018, s. 33). Videre beskriver utredningen at næringen har utarbeidet spesifikke retningslinjer for IKT-sikkerhet i prosesskontroll-, sikkerhets- og

støttesystemer som legges til grunn for arbeidet, basert på ISO 27000-serien (Justis- og beredskapsdepartementet, 2018, s. 33).

Når det kommer til hvordan kraftforsynings virksomheter forholder seg til IKT-sikkerhet stilles det omfattende krav av NVE gjennom deres reviderte forskrift for beredskap i kraftforsyningen. Dette er relativt omfattende krav om sikring av alle digitale informasjonssystemer hos virksomheter som er underlagt forskriften (Justis- og beredskapsdepartementet, 2018, s. 33). Den digitale grunnsikringen som virksomhetene er forpliktet til å opprettholde innebærer at de må sikre og ivareta deres digitale informasjonssystemers konfidensialitet, integritet og tilgjengelighet. Videre fremkommer det i forskriften at grunnsikringene skal være i henhold til anerkjente standarder og normer, deriblant krav om risiko- og sårbarhetsanalyser og sikkerhetskrav ved tjenesteutsetting (Justis- og beredskapsdepartementet, 2018, s. 33).

3.2 Forsvarlig nasjonal IKT-sikkerhet

Digitalisering kan sees på som et globalt fenomen. Digital utvikling har blitt helt essensielt for verdiskapning og vekst, men det kan også føre til at nye sårbarheter og utfordringer oppstår. I et digitalt samfunn hvor stadig flere systemer og enheter integreres og kobles sammen, medfører dette også at de samfunnsmessige sårbarhetene utvides (Justis- og beredskapsdepartementet, 2018). Dette kan forklares ved at eksempelvis et system, infrastruktur eller en verdikjede blir utsatt for en hendelse som kan få negative konsekvenser for en enkelt virksomhet. Dersom virksomheten er integrert eller koblet på systemer som andre virksomheter også benytter, kan dette utgjøre en strukturell sårbarhet hvor "alt henger sammen med alt" (Justis- og beredskapsdepartementet, 2018, s. 19). Dette kan i verste fall påvirke samfunnet i sin helhet, ved at tjenester, systemer, virksomheter og infrastruktur kan arve sårbarheter av hverandre. Ifølge Lysneutvalget (NOU 2015:13, 2015) er det ingen virksomheter som har full oversikt over egne sårbarheter på grunn av de digitale verdikjedene. En verdikjede kan utsettes for flere typer hendelser: bevisste handlinger hvor noen forsøker å sabotere eller ødelegge, eller ubevisste handlinger som skyldes feil eller ulykker. En enkel feil som oppstår på grunn av en enkeltperson kan plutselig føre til bortfall av en viktig digital tjeneste hos for eksempel pasientjournalene på et sykehus. I ytterste konsekvens kan gjensidige avhengigheter og sårbarheter påvirke samfunns- og statssikkerheten (Justis- og beredskapsdepartementet, 2018).

Samfunnssikkerhet blir i Stortingsmelding 10 (2016-2017) definert som "samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare" (Justis- og beredskapsdepartementet, 2016, s. 9). Videre forklares det hvordan slike hendelser kan oppstå og at "hendelser" kan være utløst av naturen, være et utslag av tekniske- eller menneskelige feil, eller bevisste handlinger" (Justis- og beredskapsdepartementet, 2016, s. 9). Økende globalisering innebærer også at sårbarheter kan ha sin opprinnelse utenfor Norges landegrenser og dermed utenfor norsk kontroll. Lysneutvalget beskriver ekomsektoren som et godt eksempel på dette, ved at de er en av de mest kritiske sektorene i et digitalisert samfunn. Nkom skriver i deres årlige risikovurdering at tap av nasjonal kontroll over kritisk tjenesteproduksjon og en uforutsigbar sikkerhetspolitisk situasjon utgjør en økt risiko innen elektronisk kommunikasjon for Norge (Nasjonal kommunikasjonsmyndighet, 2019). Produksjonen av elektroniske kommunikasjonsløsninger for norske virksomheter er i stor grad avhengig av både fysisk infrastruktur og bidrag fra internasjonale leverandører.

Utredningen *IKT-sikkerhet i alle ledd* (NOU 2018:14) tar for seg en helhetlig tilnærming til nasjonal IKT-sikkerhet. Utvalget legger vekt på at bruken av begrepet "nasjonal" i denne konteksten innebærer at det er gjeldende for all IKT-sikkerhet som har betydning for samfunnet som helhet. Dette inkluderer blant annet viktigheten av å beskytte både offentlige og private sektorer, ettersom "nasjonal" refererer til sikkerhetsaspekter som påvirker hele samfunnet (Justis- og beredskapsdepartementet, 2018). Med begrepet "forsvarlig" har de forstått det til at sikkerhetsnivået skal være på et minimum, men hva som skal til for å oppnå et minimumsnivå er derimot ikke definert til å være entydig. Utvalget uttrykker at forsvarlig IKT-sikkerhet kommer godt til uttrykk i NSMs grunnprinsipper for IKT-sikkerhet, som bygger på anerkjente nasjonale og internasjonale standarder og rammeverk. Grunnprinsippene beskriver hva en virksomhet bør gjøre for å sikre sine IKT-systemer og at en virksomhet som etterlever prinsippene vil ha en forsvarlig IKT-sikkerhet. NSMs grunnprinsipp deles inn i fire hovedkategorier: 1. Identifisere og kartlegge, herunder gjøre risikovurderinger. 2. Beskytte, sikring av virksomhetens verdier. 3. Opprettholde og oppdage; være bevisst egne sårbarheter og trusler. 4. Håndtere og gjenopprette; lære av utfordringene som virksomheten blir utsatt for (Nasjonal sikkerhetsmyndighet, 2020). Grunnprinsippene har underliggende teknologiske og organisatoriske sikringstiltak som beskriver i detalj hva virksomhetene bør gjøre for å både implementere og etterleve de (Nasjonal sikkerhetsmyndighet, 2020).

3.3 Risikobildet, cyberangrep og konsekvenser

Digitale sikkerhetstrusler mot samfunnet har lenge vært en viktig del av den offentlige debatten, og nasjonale myndigheter har jobbet med å både identifisere og forstå truslene man står overfor. Årlige nasjonale vurderinger fra Nasjonal sikkerhetsmyndighet, Politiets sikkerhetstjeneste og Etterretningstjenesten bidrar til å gi innsikt i de aktuelle sikkerhetstruslene mot Norge. I tillegg bidrar offentlige og private virksomheter med å synliggjøre sikkerhetsutfordringer som enkeltpersoner og samfunnet for øvrig må håndtere.
Cyberangrep utgjør en økende trussel mot norske interesser, virksomheter og privatpersoner. Med stadig mer sofistikerte og aggressive angrepsteknikker, kan disse angrepene føre til sikkerhetsmessige, økonomiske og sosiale konsekvenser. Identifisering av slike hendelser kan være krevende, og konsekvensene kan være ødeleggende. Dette har ført til økt oppmerksomhet og interesse fra både offentlige og private virksomheter for å forbedre deres digitale sikkerhet. Ifølge en rapport fra Nasjonal sikkerhetsmyndighet "... har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Antallet alvorlige og svært alvorlige hendelser har i 2022 holdt seg på et tilsvarende nivå som i 2021" (NSM, 2023, s.18). Nasjonal sikkerhetsmyndighet skriver videre i *Sikkerhetsfaglig råd - Et motstandsdyktig Norge*, at det er behov for å øke den digitale motstandskraften i hele samfunnet – fra nasjonalt nivå til kommuner, bedrifter og enkeltpersoner (NSM, 2023).

En trusselaktør kan ha som mål å skade en motpart ved å påvirke, redusere eller ødelegge funksjonaliteten i produksjonssystemer, stjele privat informasjon fra enkeltpersoner eller skaffe seg informasjon om stats- og forretningshemmeligheter, forskningsresultater eller teknologiske nyvinninger fra kommersielle bedrifter (NSM, 2023). Det er også stadig flere angrep rettet mot grunnleggende verdier og demokratiske funksjoner i samfunnet, gjennom desinformasjon og påvirkningskampanjer. Cyberangrep kan kategoriseres etter ulike formål, eksempelvis økonomisk vinning, politisk innflytelse, sabotasje eller spionasje. Økonomisk motiverte angrep gjennomføres vanligst i form av løsepengevirus som kan kryptere virksomhetens data, deretter vil trusselaktøren kreve betaling for at virksomheten skal få tilbake deres tilgang. Andre former kan være endring av eksempelvis kontoinformasjon i legitime fakturaer etter å ha kompromittert e-postsystemet til en virksomhet. Politisk motiverte angrep kan inkludere alt fra hacking av offentlige nettsider til innblanding i valgprosesser. Sabotasje kan involvere hacking av kritisk infrastruktur som energi- eller

transportnettverk, men spionasje kan inkludere stjeling av konfidensiell informasjon fra offentlige virksomheter, organisasjoner eller bedrifter.

Flere norske virksomheter har blitt rammet av alvorlige cyberangrep de siste årene. For å nevne noen opplevde Rec Silicon i 2022 å bli utsatt for et ransomware-angrep som hindret tilgangen til systemene deres (Rec Silicon, 2020). Stortinget ble i 2020 utsatt for et avansert og sannsynligvis statsstøttet angrep (NSM, 2021, s. 18). I 2019 ble Norsk Hydro utsatt for et omfattende cyberangrep som påvirket deres operasjoner (Hydro, 2020). Alle ble rammet av datainnbrudd som ga angriperne tilgang til blant annet sensitiv informasjon. Nasjonal sikkerhetsmyndighet uttrykker bekymring for en økende grad av ondsinnede cyberoperasjoner og skriver følgende i rapport *Risiko 2023 - Økt uforutsigbarhet krever høyere beredskap*: "Tar vi ikke inn over oss de økte verdiene og komplekse sårbarhetene i cyberdomenet, øker risikoen for at Kina, Russland og andre trusselaktører skaffer seg tilgang til systemer tilknyttet grunnleggende nasjonale funksjoner uten at vi er klar over det" (NSM, 2023, s.19).

Konsekvensene av cyberangrep kan være alvorlige og omfattende. Hacking av kritisk infrastruktur, for eksempel transportnettverk, vannforsyning eller kraftverk, kan påvirke sivilsamfunnets sikkerhet, trygghet og velvære. NSM har i sin rapport *Helhetlig IKT-risikobilde* identifisert at underleverandører og kontraktører i økende grad utsettes for målrettede operasjoner (NSM, 2022). Videre blir også tilfeldige systemer i økende grad utsatt for kompromittering. Dette kan føre til at de kompromitterte systemene utnyttes av trusselaktøren for videre nettverksoperasjoner mot andre mål. I prinsippet kan dette være et hvilket som helst IKT-system som ikke er et mål i seg selv, men det vil fungere som en mellomstasjon mellom en angriper og det faktiske målet.

4 Begrepsavklaring og teoretisk rammeverk

Sikkerhet som samlebetegnelse omfatter mye, og kan variere mellom alt fra personellsikkerhet til objekt- eller digital sikkerhet. Felles for alle dimensjoner av sikkerhet er at de søker å avverge uønskede hendelser, enten forårsaket av ulykker eller målrettede angrep som truer en verdi som man søker å beskytte. Denne oppgaven begrenser seg til digital sikkerhet, som handler om å beskytte informasjonsverdiene: *integritet, tilgjengelighet* eller *konfidensialitet.* Integritet betyr at informasjonen man behandler er riktig og fullstendig,

tilgjengelighet betyr at informasjonen er tilgjengelig når brukeren trenger den, og konfidensialitet handler om at informasjonen kun skal være tilgjengelig for de som er autorisert for tilgang til den.

Videre vil dette kapittelet presentere oppgavens teorigrunnlag. Innledningsvis presenteres teori om arbeid med sikkerhet, teori om tverretatlig samordning og relevant organisasjonsteori. Teorikapittelet danner grunnlaget for forståelse, analyser og diskusjoner av dokumentene som er utvalgt for å besvare problemstillingen.

4.1 Arbeid med sikkerhet

Moderne sikkerhetsarbeid har i løpet av de siste tiårene endret karakter og fokus. Det har blitt lagt til flere perspektiv for å kunne forstå ulike sider av hva som påvirker sikkerheten og med det også tiltak for å minimere risiko. Rundt 1960-tallet var det tekniske løsninger og utstyrsforbedring som var i fokus. Videre ut på 1970-tallet ble fokuset i større grad dreid mot de menneskelige faktorene– herunder feilhandlinger, informasjonsprosessering og hvordan individ handler i samspill med andre og med de systemene de skulle operere (Kongsvik et al., 2018, 21). På 1990-tallet ble det økt fokus på hvordan organisatoriske forhold påvirker sikkerhetsarbeid. Dette gikk i stor grad ut på å forstå hvordan kultur, holdninger og verdier i organisasjonen kunne påvirke sikkerheten. I dag er fokuset derimot en kombinasjon av alle de tidligere nevnte perspektivene og det blir gjerne omtalt som MTO-perspektivet (menneske, teknologi og organisasjon) (Kongsvik et al., 2018, 21). Ved å integrere en kombinasjon av nevnte perspektiv, får man en større forståelse for hvordan de kan påvirke hverandre, samt sikkerhetsnivået i organisasjonen.

Sikkerhetsarbeid kan være spennende, og det engasjerer ofte mennesker fra flere ulike fagområder. På grunn av sikkerhetsfagets relevans innenfor de aller fleste yrker bidrar dette også til et stort mangfold av meninger og forståelser. Det faglige mangfoldet kan først og fremst anses å være en styrke. Å arbeide med mennesker fra ulike fagretninger kan gjerne sørge for nye perspektiver som igjen kan føre til utvikling. Dette kan bidra til en tryggere arbeidshverdag og utviklingen kan videre redusere potensiell unødig risiko. En mulig utfordring med et bredt faglig mangfold er at det kan føre til konkurrerende forståelser for hva som er riktig og gyldig kunnskap (Kongsvik et al., 2018, s. 17). Sikkerhetsarbeid kan være veldig komplekst ved at det kan omfatte detaljerte arbeidsprosedyrer, dyrebare investeringer som krever omfattende sikkerhetstiltak eller høyteknologiske sikkerhetssystem

som kan være innført for å unngå uønskede hendelser. Samtidig kan arbeid med sikkerhet også være så enkelt som å henge opp en boks med plaster på arbeidsplassen for behandling av små skader som et konsekvensreduserende tiltak.

Hvis en ønsker å forstå hvordan sikkerhetsbegrepet benyttes i arbeidsorganisasjoner, kan en skille mellom to mer grunnleggende forskjellige perspektiver. Det første knytter sikkerhet til fravær av noe, nærmere bestemt fravær av risiko, men det andre perspektivet ser på sikkerhet som nærvær av spesielle organisatoriske egenskaper (Kongsvik et al., 2018, 21).

4.1.1 Fravær av uakseptabel risiko

Sikkerhet som fravær av uakseptabel risiko handler i stor grad om tapsforebygging. Ifølge Hovden (1998) går dette ut på å opprette et forsvar mot trusler og farer. Dette kan gjøres to på ulike måter (Kongsvik et al., 2018, 22):

1. Ved å hindre at uønskede hendelser oppstår i utgangspunktet.

2. Ved å etablere barrierer som beskytter det man oppfatter som verdifullt (liv, helse, miljø og materielle verdier), dersom det likevel skulle oppstå en uønsket hendelse.

Et eksempel på dette kan være et digitalt innbrudd hos en organisasjon. Et tiltak kan være å etablere strenge krav til nettverkssikkerheten. Dersom det digitale innbruddet likevel skulle oppstå, kan kryptering av filer og tilgangsstyring minimere skaden og omfanget for organisasjonen. Basert på dette kan man trolig si at sikkerhet kan knyttes til risiko og at sikkerhet og risiko betraktes som to sider av samme sak. Ifølge Rausand og Utne (2009) kan en definere risiko ved å si at risiko er en funksjon av sannsynlighet og konsekvens. En kombinasjon av sannsynlighet for at det skjer og den mulige konsekvensen hendelsen har, er med på å predikere risikonivået for hendelsen. En reduksjon av risiko vil derfor kunne sies å være en reduksjon av sannsynlighet og/eller konsekvensen av hendelsen (Kongsvik et al., 2018, 22). Hvis en ser på dette opp imot det tidligere nevnte eksempelet kan en si at begge tiltakene, økt krav til nettverkssikkerhet og kryptering av filer og tilgangsstyring, bidrar til økt sikkerhet og redusert risiko for at skadeomfanget blir omfattende. På bakgrunn av dette kan man si at sikkerhet er ensbetydende med fravær av risiko (Kongsvik et al., 2018, 22). En kan imidlertid ikke eliminere all risiko fullt ut. Sannsynligheten for at uønskede hendelser oppstår kan være tilnærmet null og potensielle konsekvenser kan forebygges i stor grad, men det fører likevel ikke til at risikoen blir totalt fraværende. Med bakgrunn i dette innføres tiltak

i den hensikt å redusere risikoen til å være så lav som mulig, slik at den kan anses å være akseptabel innenfor gitte rammer. Dette omtales innenfor risikoanalysetradisjonen som ALARP-prinsippet ("as low as reasonably practicable") (Kongsvik et al., 2018, 22). Denne tilnærmingen til sikkerhet er mer praktisk og realistisk og ifølge Hollnagel (2008) kan en omtale det som "fravær av uakseptabel risiko".

4.1.2 Nærvær av organisatoriske egenskaper

Det andre perspektivet, sikkerhet som nærvær av organisatoriske egenskaper, omhandler hvordan organisatoriske forhold påvirker sikkerheten. Dette perspektivet har både et positivt og negativt syn på hvordan systemulykker kan unngås. Det negative synet innen dette perspektivet, "normal accident theory" (NAT), fokuserer på hvordan et nærvær av teknologiske egenskaper fører til ulykker. Det positive synet, "High reliability organizations" (HRO), legger vekt på hvordan et nærvær av spesielle organisatoriske egenskaper bidrar til å skape sikkerhet (Kongsvik et al., 2018, 23).

4.1.2.1 Normal accident theory

Teorien er utviklet av Charles Perrow og bidrar til å skape en forståelse av ulykker i komplekse og teknologiske systemer. Hovedpoenget med teorien går ut på at enkelte systemer er konstruert og opererer på en slik måte at ulykker er uunngåelige eller "normale" (Kongsvik et al., 2018, 78). Perrow omtaler dette som systemulykker og at de har sin forklaring i to ulike årsaker. Den første går på at feil som oppstår kan virke sammen i et komplekst system, slik at konsekvensen blir annerledes enn om det bare er enkeltkomponenter som svikter. Den andre årsaken går ut på hvordan systemene er oppbygde, og med det settes hele systemet i fare. Perrow (1999) fremhever at mange store ulykker begynner med "småfeil". Ved å identifisere systemkompleksitet og koblinger som kjennetegner risikoutsatte systemer gir "normal accident"-teorien mulige retningslinjer for arbeidet med risikoreduksjon som kan nyttes i teknisk design og utvikling av styringssystemer (Kongsvik et al., 2018, 79). Perrows teori er i utgangspunktet utviklet med bakgrunn i virksomheter med høy grad av teknisk kompleksitet. Til tross for dette er det teorien like gyldig for virksomheter med høy grad av organisatorisk kompleksitet. Denne kompleksiteten kan dreie seg om forhold som antall aktører, informasjonsstrømmer, beslutningsprosesser, fordeling av ansvar og myndighet (Kongsvik et al., 2018, 80).

4.1.2.2 Høypålitelige organisasjoner

"High reliability organizations" (HRO) kan ifølge LaPorte og Consolini (1991) være "NAT"-organisasjoner som evner å håndtere komplekse systemer og som åpenbart fremstår som trygge. Et eksempel på dette er:

> "Et atomdrevet hangarskip der fly tar av og lander på et begrenset areal mens skipet er i fart også i mørket og under vanskelige værforhold. Organisasjonen om bord håndterer også høyradioaktivt materiale, store mengder lettantennelig flydrivstoff, våpen og eksplosiver. Fra hangarskipet gjennomføres også løpende operasjoner med høyt farepotensial. Supplybåter leverer alt fra post til mat og drivstoff til hangarskipet. De to skipene kjører parallelt med en fart på tolv knop (22 km/t). Hvis det ene skipet går raskere enn det andre, brytes forbindelsene. Kommer de for nær hverandre, vil de kollidere. Kommer de for langt fra hverandre, kan de miste lasten og sette personalet i fare. Når de to skipene er fortøyd til hverandre, er de mindre manøvreringsdyktige og mulige mål for fiendtlige angrep." (Kongsvik et al., 2018, 80).

Dette eksempelet viser hvordan organisasjoner håndterer komplekse, krevende teknologier på en måte som gjør at de opererer uten å bli utsatt for alvorlige ulykker, samtidig som de opprettholder operativ evne og produksjonskapasitet (Rochlin et al., 1987). Høypålitelige organisasjoner kan beskrives med flere kjennetegn, eksempelvis har de en redundans, evne til rekonfigurering og "mindfulness" (Kongsvik et al., 2018, 80). Organisatorisk redundans handler om å ha ansatte i organisasjonen med overlappende kompetanse. Hensikten med dette er å forsikre seg om at organisasjonen evner å løse oppdrag til tross for fravær. Videre er det essensielt for organisasjonen at de ansatte evner og har vilje til å utveksle informasjon, gi tilbakemeldinger og revurdere beslutninger. Ved rekonfigurering så menes det at i kritiske situasjoner fraviker man fra det normale organisatoriske hierarkiet og en forholder seg i mye større grad til kunnskap og erfaring for å håndtere situasjonen fremfor hvem for har høyest grad/stilling (Kongsvik et al., 2018, 80). "Mindfulness" er i denne sammenhengen viktigheten av at de ansatte i organisasjonen har en mental tilstedeværelse, kontinuerlig oppmerksomhet og årvåkenhet overfor potensielle feil og avvik (Weick & Sutcliffe, 2007, 9).

4.1.3 Barrieresvikt - Reasons sveitserostmodell

James Reasons (1997) modell på barrieresvikt og forsvar i dybden (swiss cheese model) tar utgangspunkt i tre begrep: fare, forsvar og tap. I denne modellen benyttes begrepet "fare" for

å beskrive hva som kan utløse en ulykke eller uønsket hendelse. Tap er de uønskede konsekvensene av hendelsen, mens forsvaret i modellen de etablerte barrierene som skal forhindre at et tap oppstår (Kongsvik et al., 2018, 76). De etablerte barrierene skal ha til hensikt å kompensere for hverandre slik at faren ikke kommer gjennom forsvaret. Det vil si at dersom den første barrieren ikke evner å hindre at den uønskede hendelsen oppstår, skal neste barriere sørge for dette, med andre ord forsvar i dybden. Modellen beskriver godt hvordan uønskede hendelser likevel kan oppstå til tross for et forsvar i dybden. Sveitserosten har gjerne mange hull og de hullene symboliserer i denne modellen mulige barrieresvikter. Dersom det er flere barrieresvikter i forsvaret vil dette medføre at faren ikke blir håndtert og det kan derfor utvikle seg til en ulykke. Årsaken til de ulike barrieresviktene kan være mange; det kan være faktiske feilhandlinger som tabber og prosedyrebrudd eller det kan være skjulte feil som utstyrssvikt, manglende kompetanse eller lite erfaring (Kongsvik et al., 2018, 77).

4.2 Gjenstridige problemer og tverretatlig samordning: Et analytisk rammeverk

Som en motreaksjon på New Public Managements fokus på en-oppgave organisasjoner og større autonomi for organisasjoner, herunder økt "*silozation"* og *"pillarization"*, har fokuset endret seg til å legge økt vekt på samordning på tvers av offentlige etater for å håndtere gjenstridige problemer som klima og miljø, fattigdom, arbeidslivskriminalitet og samfunnssikkerhet. Digital sikkerhet er et tema underlagt samfunnssikkerhet.

Nesheim m.fl. (2019) har etablert et analytisk rammeverk for ikke-hierarkisk samordning i staten, basert på instrumentelt organisasjonsfaglig perspektiv. Det instrumentelle perspektiver handler om å se organisasjoner som maskiner, fremfor en slags levende organisme. Sagt med andre ord, så ser man på en organisasjon både som et instrument til å oppnå noe spesielt, og som et styringsorgan for de ansatte (Christensen et al., 2010).

Det analytiske rammeverket består av fire dimensjoner. Hovedteorien til Nesheim m.fl. (2019) er at desto større avstand det er mellom de deltakende organisasjonene på de fire dimensjonene, desto mer krevende er det å få til en god tverretatlig samordning. Den første dimensjonen, oppgaver og avhengigheter, handler om å forstå at et problem eller et sett med oppgaver treffer flere etater og/eller forvaltningsnivåer. Ut fra et instrumentelt perspektiv så bør berørte etater samordne sitt arbeid basert på en tilpasning til egenskapene ved de

oppgavene som skal håndteres og de avhengigheter som finnes mellom etatene. Viktige variabler og dimensjoner ved dette er listet opp under "spesifikke mekanismer" i tabellen under. Den andre dimensjonen, distanse mellom organisasjoner, omhandler utfordringer knyttet til å oppnå samordning på tvers av organisasjoner som et produkt av ulike *distanser* mellom de deltakende organisasjonene. Nesheim m.fl. (2019) påpeker at økt distanse innen en av de fire distansedimensjonene, kan bidra til økte utfordringer med god tverretatlig samordning. De fire distansedimensjonene er geografisk-, kognitiv-, strukturell-, og maktdistanse. Nesheim m.fl. (2019) påpeker at graden av symmetri i makt er viktig for prosessene i samarbeidet, men de støtter ikke hypotesen om at asymmetri nødvendigvis er skadelig for samordningen. De mener det heller handler om at det er avgjørende å bygge opp styringsstrukturer og mekanismer for samordning som er i *samsvar* med makt- og avhengighetsforhold knyttet til de aktuelle oppgavene (Nesheim et al., 2019).

De to neste dimensjonene handler om intra- og inter-organisatoriske tiltak. Hvilke tiltak som gjennomføres internt i organisasjonen for å støtte opp under samarbeidet, og hvilke organisatoriske tiltak som gjennomføres for å styrke samarbeidet med øvrige deltakende etater og organisasjoner. Alle dimensjoner og spesifikke mekanismer tilknyttet disse er oppsummert i tabellen (Figur 1) under:

Dimensjoner	**Spesifikke mekanismer**
a) Oppgaver og avhengigheter	Myndighetsutøvelse eller tjenesteyting? Nærhet til etatens kjernevirksomhet Avhengigheter mellom etatene Hva er aktuelle oppgaver på ulike organisatoriske nivåer, og hvilke etater og enheter er aktuelle deltakere i disse? Oppgaver på operativt nivå: løpende, sporadiske eller tidsbegrensede?
b) Distanse mellom organisasjoner	Geografisk distanse Kognitiv distanse Strukturell distanse Maktdistanse
c) Intra-organisatoriske tiltak	Har etaten en strategi for feltet det samarbeides om? Intern organisering for samarbeid Intern styring (mål, ressurser med mer) for samarbeid Innslag av interne spenninger Er strategien forstått og kommunisert i etaten?
d) Inter-organisatoriske tiltak	Samarbeidshierarkiet: Sekundærorganisasjon med tiltak på ulike nivå Har man et ledende departement/ledende etat? Prosjekt eller varig tiltak? Styringsmekanismer: Formalisering vs. tillit Fase og grad av institusjonalisering Ledelse av samarbeidstiltak

Figur 1: Analytisk rammeverk for ikke-hierarkisk samordning i staten (Nesheim et al., 2019, s. 38).

4.3 Organisasjonsteoretiske perspektiver

I arbeidet med å forstå ulike strategidokumenter og deres bakgrunn, er det relevant å også forstå de offentlige organisasjonene disse styrende dokumentene har blitt til i. Det er videre relevant å benytte organisasjonsteori rundt det å forstå hvordan organisasjoner fungerer når det gjelder endring og endringsprosesser. Christensen et al. (2015) diskuterer ulike perspektiver i analyse av offentlige organisasjoner i den hensikt å forstå hvordan organisasjonene fungerer. I oppgaven med å forstå ulike styrende dokumenter som myndighetene har gitt ut, vil det være nyttig å danne seg et bilde av organisasjonene som disse dokumentene har blitt til i. Den videre hensikten med dette er å forsøke å forstå hvilke mål og verdier organisasjonene legger til grunn for arbeidet, hvordan ledelse og styring påvirker utarbeidelsen av dokumentene. Det er interessant å se på hvilke tanker organisasjonene gjør seg om reformer og endring, da oppgavens tema i stor grad handler om å endre nåværende praksis til noe annet. Effekter og implikasjoner i organisasjonene er også interessante perspektiver knyttet til det å forstå disse organisasjonene (Christensen et al., 2015).

Christensen et al. (2015) beskriver tre ulike perspektiver å benytte for å analysere eller forstå organisasjoner. Disse er instrumentelt perspektiv, kulturperspektivet og myteperspektivet. Det instrumentelle perspektivet handler om at man ser på organisasjoner som instrumenter eller redskaper som er til for å oppnå organisasjonens mål. Perspektivet legger til grunn at organisasjonen er bygget opp på grunnlag av mål-middel vurderinger, og at organisasjonene derfor er designet for å oppnå spesifikke mål (Christensen et al., 2015, 34). Teorien om det instrumentelle perspektivet legger til grunn at det finnes to ulike måter å se på organisasjoner som instrumenter på. Den hierarkiske varianten legger til grunn at organisasjoner er hierarkisk innrettet, der det legges vekt på kunnskap om mål-middel sammenhenger hos ledelsen i organisasjonen. Ledelsen har oversikt over organisasjonens målsettinger, og oppnår disse gjennom å benytte sin organisasjon gjennom bruk av makt (Christensen et al., 2015, 35). Det andre perspektivet kalles forhandlingsvarianten. I denne varianten forstår man at organisasjoner er sammensatt av ulike avdelinger og underenheter som har ulike mål, som enkelte ganger er motstridende. Kunnskap og interesser er også i mange tilfeller ulike. Denne varianten legger til grunn at organisasjonens målsettinger oppnås gjennom forhandling og kompromiss mellom de involverte aktørene (Christensen et al., 2015, 35).

Der det instrumentelle perspektivet representerer de formelle normene og strukturene i organisasjonen, søker kulturperspektivet å forklare de uformelle normene og verdiene som finnes i organisasjonen. Når en organisasjon har utviklet et spesielt sett normer og verdier, som er særegent for akkurat denne organisasjonen, snakker vi gjerne om institusjonaliserte organisasjoner (Christensen et al., 2015, 52). I en institusjonalisert organisasjon handler organisasjonsmedlemmene i tråd med organisasjonens uformelle normer og verdier, og som nyansatt får man innsikt i disse fenomenene etter hvert som man blir inkludert og integrert i organisasjonen over tid (Christensen et al., 2015, 53). I en slik kultur vil gjerne de ansatte handle ut fra logikken om "passende atferd" (Christensen et al., 2015, 54). Dette innebærer at de ansatte ikke primært handler utelukkende rasjonelt ut fra instrumentelle perspektiver, ei heller egeninteresse eller konsekvensene av handlingene. Vedkommende vil også vurdere hvilke handlingsmåter eller beslutninger som er innenfor organisasjonens akseptable adferd (Christensen et al., 2015, 54). Vedkommende handler derfor ut fra kulturbaserte handlingsregler i organisasjonen, og kobler dermed andre ønskede utfall med de kulturelle normene og verdiene som eksisterer i organisasjonen (Christensen et al., 2015, 54). Innenfor kulturperspektivet snakker man også om fenomenet stiavhengighet. Fenomenet handler om at en organisasjonskultur, et sett av uformelle verdier og normer, vil dannes i startfasen når en ny organisasjon startes. Disse normene og verdiene vil ofte ha stor betydning for hvordan organisasjonen utvikles videre, og startpunktet for organisasjonen vil derfor ha stor innvirkning på hvilken retning organisasjonen senere utvikles i (Christensen et al., 2015, 61).

Det tredje perspektivet Christensen et al. (2015) benytter for å forstå organisasjoner er myteperspektivet. Dette perspektivet legger til grunn at organisasjonene må tilpasse seg sosiale normer i samfunnet i de institusjonelle omgivelsene. Der kulturperspektivet legger til grunn normer og verdier innad i organisasjonene som har vokst frem over lang tid, handler myteperspektivet om verdier i omgivelsene, også kjent som myter (Christensen et al., 2015, 76). Disse mytene er gjerne sosialt konstruerte normer og oppskrifter på hvordan organisasjonene bør være utformet og hvordan de bør fungere. Mytene gjenspeiler ikke alltid hvordan organisasjonene faktisk fungerer, men ledere i organisasjonene må gjerne forsøke å oppfylle mytene gjennom ord og handlinger for å unngå (Christensen et al., 2015, 97).

5 Metode

5.1 Analyseformål

Denne oppgaven har til hensikt å belyse hovedtendensene i myndighetenes prioriteringer over tid knyttet til styrking av digital sikkerhet. Videre er formålet å diskutere hvilke utfordringer Justis- og beredskapsdepartementet står overfor når de skal sette prioriteringene ut i praksis som ansvarlig for samordning av digital sikkerhet i sivil sektor. Gjennom grundig analyse av utvalgte dokumenter vil vi vurdere både hva hovedtendensene er og hva som kan være årsakene til at de har oppstått. Forhåpentligvis vil dette synliggjøre utfordringer som må løses for å øke den digitale sikkerheten til et tilfredsstillende nivå.

Dette kapittelet beskriver hvilke metodiske grep og valg som er tatt for å kunne finne de resultatene som presenteres i oppgaven. Vi vil presentere fremgangsmåten for hvordan informasjon har blitt fremskaffet til bruk for å besvare oppgavens problemstilling. Denne oppgaven baserer seg på en dokumentstudie av relevante dokumenter knyttet til digital sikkerhet for å kunne belyse problemstillingen på en interessant og fornuftig måte.

5.2 Dokumentstudier

Oppgaven vil benytte seg av kvalitativ dokumentstudie som datagrunnlag for å besvare problemstillingen. Dette innebærer en innholdsanalyse av allerede eksisterende dokumentasjon som anses relevant for problemstillingen. Innholdet, herunder datagrunnlaget det representerer, analyseres for å belyse og fremstille sammenhenger mellom hva som var prioriteringene for digital sikkerhet og frem til hva de har blitt, som definert av myndighetene. Dokumentasjonen vil også danne et grunnlag for å diskutere hvilke utfordringer myndighetene står overfor for å få gjennomført de løsningene og tiltakene fra et samordningsperspektiv.

Valget av dokumentstudie som metode for datainnsamling har både fordeler og ulemper. Dokumentstudier er definert som en “ikke-påtrengende metode”, og innebærer at data som produseres blir gjort uten deltakelse eller involvering av “ikke-forskende” (Tjora, 2020, s.182). Kritikk mot dokumentstudie som forskningsmetode handler ofte om at dokumenter er et produkt av tiden det er skrevet i, som kan føre til at de blir raskt gjort utdatert hvis det ikke oppdateres jevnlig. Videre vil dokumentene gi innsikt som er farget av både sted, forventet

målgruppe, eller andre faktorer som kan påvirke innhold. En dokumentstudie må derfor gjøres med forståelse for at informasjonen man får fra dokumentene som analyseres er kontekstavhengige. Det er også viktig å være klar over at informasjonen som hentes fra dokumentene er farget av forfatterne, deres meninger, virkelighetsforståelse og beskrivelser av fakta. De aller fleste dokumenter kan nyttes ved dokumentstudie, men de vanligste er stortingsmeldinger, lover, utredninger, ulike rapporter eller andre offentlige dokumenter, men man kan også benytte eksempelvis artikler, blogger, brev eller private journaler (Johannesen et al., 2016, s. 97). Det er i hovedsak dokumenter som ikke er produsert med forskning som formål. Derfor brukes dokumentene som empiri fremfor teori.

Asdal og Reinertsen (2020) forklarer dokumentstudier som metodisk tilhørende kvalitative studier. De viser videre til en praksisorientert metode som består av seks verktøy som kan brukes for å forstå et dokument i en bredere kontekst. Asdal og Reinertsen argumenterer for at det ikke er nok å kun forstå innholdet av et dokument for å forstå det sanne omfang og effekt av dokumentet. Det innebærer at analyser og vurderinger må gjøres av dokumentenes egenskaper og kvaliteter, samt virkning på sakene de omhandler. Først når man også vurderer hvordan praksisfeltet dokumentet beveger seg innenfor fungerer, hvordan det blir lest og brukt, eller er opphav til tiltak og påvirker situasjoner, vil en fullstendig analyse og forståelse av dokumentet oppnås (Asdal & Reinertsen, 2020, s. 22). Dokumentenes sjanger er videre noe som har påvirkning på leseren. Dette betyr at leseren må være årvåken knyttet til hvordan man møter teksten, slik at man er bevisst egen forforståelse som igjen påvirker tolkning.

Dokumentstudier kan gjennomføres på forskjellige måter, og det er to metoder som vi ønsker å dra nytte av i denne oppgaven for å analysere dokumentene og belyse problemstillingen. Først vil vi gå gjennom Asdal og Reinertsen praksisorienterte metode, og deretter Carol Bacchis metodikk.

5.2.1 Dokumentstudier - en praksisorientert metode

Den praksisorienterte metoden er utarbeidet av Kristin Asdal og Hilde Reinertsen som et verktøy for å analysere dokumenter. Metoden skiller seg ut ved at den vektlegger hvordan dokumenter er noe rent tekstlig, men også noe mer materielt. Tilnærmingen er derfor bredere enn både tekstanalyse og diskursanalyse (Asdal & Reinertsen, 2020). I de følgende delene av

dette delkapittelet vil vi utdype hver av de seks metodiske grepene som Asdal og Reinertsen (2020) presenterer.

5.2.1.1 Dokumentsteder

Det analytiske grepet som Asdal og Reinertsen (2020) kaller *dokumentsteder* handler om å se på dokumentene som "steder der det skjer noe". Med andre ord, der det foregår handlinger som har betydning for saken, handler som påvirker presenterte løsninger eller spørsmålene som forsøkes besvart. Ved å konkretisere dokumenter som både bestemte former for tekst, men også gjenstander, vil det bidra til å la oss analysere hva som er spesielt og særegent ved disse. Dokumentsteder, som forklart av Asdal og Reinertsen (2020), innebærer at man må forstå hvordan dokumenter er komponert på ulikt vis, med organisasjoner og virksomheter som har forskjellige regler og retningslinjer for hvor mye endringer og omgjøringer de tillater. Eksempelvis vil Stortinget, departementer eller NATO være dokumentsteder hvor det foregår forhandlinger og endringer av dokumenter over tid.

I denne oppgaven benytter vi oss av dokumentasjon utarbeidet av forskjellige offentlige organer, for eksempel egne utvalg eller Justis- og beredskapsdepartementet. Et av disse dokumentene er "Nasjonal Strategi for Digital Sikkerhet" som er et dokument som søker å tilby løsninger og anbefale tiltak til både private og offentlige virksomheter for å øke sin digitale sikkerhet. Ved å se på det som et dokumentsted, kan vi tilføye en dimensjon hvor vi også ser på hvor det kommer fra og "hvordan det potensielt virker og intervenerer på steder langt utenfor selve etaten eller institusjonens kontorer og korridorer" (Asdal & Reinertsen, 2020 s.145). I Nasjonal Strategi for Digital Sikkerhet er det enkelt å se hvilken sammenheng og hvilke påvirkninger som har ført til både dokumentets opprettelse og dokumentets intenderte virkning - eksemplifisert ved at det står i selve dokumentet. Det står beskrevet at "strategien inngår i en større sammenheng av politiske og strategiske dokumenter som gir føringer for det nasjonale arbeidet med digital sikkerhet" (Departementene, 2019, s.24)

5.2.1.2 Dokumentverktøy

Dokumentverktøy som metodisk grep handler om å identifisere hvordan dokumentet som skal analyseres brukes for å oppnå, realisere, etablere eller skape noe (Asdal & Reinertsen, 2020, 146). Politikk og byråkrati, som er brukt som eksempel av Asdal og Reinertsen (2020), er avhengig av dokumenter som verktøy for hjelp til, og understøttelse av, sine aktiviteter. Dokumenter er viktige styringsverktøy, og det er mye man bør forsøke å identifisere som en

del av analysen. For å forstå hvordan dokumentene brukes som verktøy må man studere hvordan dokumentene brukes som verktøy for å oppnå noe, hva de gjør, hvordan de virker, hvem de innvirker på, hvem som eier dem og hvordan ulike aktører kan slippe til. Videre er det en viktig del av analysen å kartlegge hvilken sammenheng dokumentet inngår i, hvilke andre dokumenter som kan være sentrale for å forstå dokumentet vi analyserer, hvilket landskap og hvilken tidsperiode er dokumentene en del av. Andre spørsmål som er en del av analysen man bør forsøke å besvare er hvorfor dokumentet er utformet, hvilke effekter har dokumentet på verden og hvordan muliggjør dokumentet handling og endring? Når man benytter dokumentverktøy som et analytisk og metodisk grep er det viktig å være innforstått med at dokumenter ikke er nøytrale, men bidrar til å påvirke sakene de omhandler. De kan bidra til å forme og omforme saker etter hvert som tiden går. Benyttelse av dette analytiske og metodiske grepet kan være svært nyttig og interessant i denne oppgaven, med bakgrunn i dokumentutvalget.

5.2.1.3 Dokumentarbeid

Ifølge Asdal og Reinertsen (2020) handler dokumentarbeid om å forstå hva dokumentarbeidet består av, hva slags betydning det har, hvilke former for kompetanse og spesielle ferdigheter som behøves. Det handler videre om hvordan dokumentarbeidet påvirker utformingen av de ulike dokumentene, har innvirkning på dokumentstedene og de sakene og spørsmålene som diskuteres og forsøkes løst eller endret. Dokumentarbeid, som metodisk grep, handler om mer enn bare hvordan arbeid gjøres i teksten. Det handler også om hvordan grunnlagsinformasjon innhentes, hvordan teksten utarbeides, herunder om det er individuelt utformet eller produsert av et samarbeid. Også avgjørelser om hvem som skal skrive hva inkluderes (Asdal & Reinertsen, 2020).

Det er ikke alltid enkelt å kartlegge all denne informasjonen, og i mindre grad når man benytter ferdigutviklede dokumenter slik det gjøres i denne oppgaven. Dokumentarbeid som metodisk grep er å følge arbeidet helt konkret, som en del av et feltarbeid. Hva gjøres, hvordan gjøres det og hvordan utformes dokumentet. I denne oppgaven vil det være mer interessant å se på innholdet i tekstene, historikk og hovedtendenser i holdninger til digital sikkerhet, men det utelukkes ikke at enkelte aspekter innenfor dokumentarbeid vil kommenteres senere i oppgaven.

5.2.1.4 Dokumenttekster

Dette metodiske grepet, i motsetning til i 5.2.1.3, retter seg mer mot det retoriske apparatet til teksten. Med dette menes det at man vier oppmerksomheten mot layout, bilder, illustrasjoner, tabeller og grafer. I tillegg retter man oppmerksomheten mot argumentasjon og narrativ. Hva slås tydelig fast, hva er mindre prominent og hva står ikke i det hele tatt? Man skal analysere hvordan dokumentet forsøker å overtale sine lesere. Asdal og Reinertsen (2020) forklarer at dette kombinert utgjør dokumentets sjanger, som er avgjørende for hvordan dokumentet blir mottatt og hvilken betydning det får.

5.2.1.5 Dokumentsaker

Dokumentsaker handler om hvordan dokumentene som analyseres arbeider med saken, eller aktiviteten som foregår i teksten, med og på sakene, hvordan dette bidrar til å forme sakene. Man skal med andre ord analysere hvordan et dokument bidrar til å moderere, omformer eller radikalt transformerer saker. Asdal og Reinertsen (2020) forklarer at man kan analysere dette ved å se på flere dokumenter ved å sammenligne ulike måter å forme saksforhold på i ulike dokumenter, med spesielt fokus på dokumenter som kanskje følger hverandre. Dette vil være en aktuell metode for denne oppgaven, hvor vi analyserer tre dokumenter i kronologisk rekkefølge, hvor den neste bygger på den forrige for å kunne avdekke eventuelle endringer og tendenser.

5.2.1.6 Dokumentbevegelser

Det siste analytiske grepet, dokumentbevegelser, handler om hvordan dokumenter settes i bevegelse og hvordan de beveger seg. Med andre ord hvordan endringer eller andre ytre påvirkninger tas inn i dokumentet som videre kan muliggjøre hvordan de blir handlet på, og kan bevege seg videre.

Når det gjelder digital sikkerhet så er det en økende trend i omfang, både størrelse og hyppighet, av uønskede digitale sikkerhetshendelser som kan virke som drivende for myndighetenes ønske om å sikre Norges digitale infrastruktur. Det kan være interessant å se nærmere på om det digitale trussellandskapet og registrerte hendelser kan ha bidratt til å endre, eller skape bevegelse, innen området som kan være viktig å forstå for å kunne besvare problemstillingen.

5.2.2 Carol Bacchis *Analysing Policy: What's the problem represented to be*

Den andre analysemetoden benyttet i denne oppgaven er hentet fra Carol Bacchis (2009) bok *Analysing Policy: What's the problem represented to be*. Hun har laget en fremgangsmåte for å analysere offentlige styringsdokumenter ved å fokusere på problemforståelsen som ligger bakenfor dokumentet. Bacchi presenterer en analysemetode ved hjelp av seks spørsmål som skal hjelpe forskeren med å strukturere sin analyse av politikk, både løsninger og hva som presenteres som et problem.

Sentralt i Bacchis (2009) metode er forståelsen for at en annerledes beskrivelse av hva som er problemet, produserer en annen effekt, som må og bør forstås og vurderes. I Bacchis analysemetode må man forstå tre effekter/virkninger som er knyttet sammen. Den første er diskursive effekter som handler om å forstå både hva som er diskutert, men også hva som *ikke* er diskutert. Den neste er subjektiviserende effekter som handler om hvordan individer er oppfattet og hvordan de oppfatter seg selv. Til slutt er det en forståelse av effekten på livene til de som påvirkes av politikken. Bacchi (2009) argumenterer med at måten de forskjellige problemene er definert på, eller hvordan situasjoner er problematisert, er så avgjørende for hvordan vi lever livene våre på, så er vi i praksis mer styrt av problematiseringer enn av politikk. Bacchi konkluderer derfor med at kritisk fokus bør rettes mot problematiseringene og de problempresentasjonene de består av, snarere enn politikken som baseres på dem. Metoden er derfor et verktøy for å analysere hvordan bestemte måter å presentere *problemer* på spiller en svært stor rolle i hvordan regjering og andre myndigheter velger å styre og lede undergitte offentlige organisasjoner, herunder også styring av god digital sikkerhet.

De seks spørsmålene som Bacchi (2009) presenterer kan brukes til å forstå dokumenter som skal bidra til å skape endringer for både mennesker og organisasjoner:

1. Hva er problemet? Hva er de definerte målene svaret på?
2. Hvilke forutsetninger og antagelser ligger til grunn for denne fremstillingen av problemet?
3. Hvordan har denne presentasjonen av problemet oppstått?
4. Hva er utelatt i beskrivelsen? Kan problemet fremstilles på en annen måte?
5. Hvilke effekter har denne måten å presentere problemet på, herunder diskursiv, subjektiviserende, livene?

6. Hvordan/hvor er problemet formulert, formidlet og forsvart? Hvordan kan det settes spørsmålstegn ved, forstyrre og/eller erstattes?

Enkelte av disse spørsmålene vil danne grunnlaget for de analytiske spørsmålene vi anvender som en del av den metodiske tilnærmingen til analysen av de utvalgte dokumentene. Bacchis spørsmål bidrar til å belyse problemet som skal løses, og løsninger som er foreslått. Dette er en del av besvarelsen på et av forskningsspørsmålene om hvilke hovedtendenser man kan identifisere i myndighetenes prioriteringer innen digital sikkerhet.

5.2.3 Valg av metode

Forfatterne av denne oppgaven har vurdert at bruken av dokumentstudie som metode vil gi den mest verdifulle innsikten og forståelsen for å kunne besvare problemstillingen. Vi ønsker å undersøke hvilke hovedtendenser man kan identifisere i myndighetenes prioriteringer, og hvilke utfordringer det medfører å sette disse ut i praksis. Dette anslår vi at best kan forstås gjennom analyse av dokumentene som de offentlige virksomhetene må forholde seg til. Ved bruk av andre metoder, eksempelvis kvalitative intervjuer, vil vi trolig få bedre innsikt i hvordan enkeltindivider i ulike virksomheter forstår myndighetenes prioriteringer, men det er ikke det vi ønsker å belyse med denne oppgaven. Ved bruk av valgt metode, har vi anledning til å benytte allerede tilgjengelig informasjon, samt at valget belyser tematikken på en uvanlig måte, som kan bidra til økt innsikt i problemstillingen.

5.2.3.1 Kategorisering og koding

Når vi skal analysere kvalitative tekstdata, som i denne oppgaven består av data fra dokumenter, er det normalt å bruke en variant av koding og kategorisering av datamaterialet (Ringdal, 2018). Dette kalles for innholdsanalyse og er en samfunnsvitenskapelig metode for å analysere tekstdata. En definisjon av innholdsanalyse lyder: *"*Innholdsanalyse er en samfunnsvitenskapelig metode for analyse av innhold i skriftlige eller muntlige tekster, samt bilder, videoer eller filmer*"* (Grønnmo, 2020).

For å kunne analysere flere dokumenter på en måte som gir troverdige svar, og som gir en økt likhet i analysen av flere dokumenter, så velger vi å benytte oss av kategorisering. Disse kategoriene er basert på og tar utgangspunkt i forfatternes forskningsspørsmål. Følgende kategorier vil benyttes:

1	2	3	4	5	6
Bakgrunn for at dokumentet er utviklet	Hvem har lagd dokumentet	Beskrivelse av sentrale mål med dokumentet / prioriteringer	Problemer som skal løses	Løsninger som foreslås	Utforming av løsningene

Figur 2: Kategorier benyttet for innholdsanalyse

Problemstillingen som skal undersøkes handler om hvilke hovedtendenser som fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet. Den utvalgte dokumentasjonen strekker seg over flere år, og det er naturlig å anta at det vil ha skjedd endringer i hva som prioriteres av offentlige myndigheter. For å kunne forklare hva forskjellene er, må vi gjennomføre analyser som gir oss et sammenligningsgrunnlag. For å oppnå dette har vi valgt å benytte oss av kategoriene i tabellen over for å sørge for at vi søker å besvare de samme spørsmålene i alle analysene vi gjennomfører. Alle kategoriene er valgt for å belyse forskjellige karakteristikker ved dokumentene for å få et bredere bilde på hvilke hovedtendenser som fremkommer av prioriteringene innen digital sikkerhet.

Spørsmål 1 til 3 er basert på metodikken til Asdal og Reinertsen (2020). Å klarlegge bakgrunnen for hvorfor de ulike dokumentene er utviklet kan bidra til å skape en forståelse for de samfunnsmessige forhold som rådet på det aktuelle tidspunkt. Skulle det vise seg at det har skjedd endringer i bakgrunnen for hvorfor dokumentene er utviklet, kan det være en forklaring på hvorfor prioriteringer har endret seg. Det neste spørsmålet, hvem som har lagd dokumentet, er viktig å få klarlagt for å forstå om det er noen interessenter som har påvirket eventuelle endringer i prioriteringene. Videre vil beskrivelse av sentrale mål med dokumentet gi ytterligere konkretisering av hva som kommuniseres som viktig å oppnå innen digital sikkerhet.

Spørsmål 4 og 5 er basert på Bacchis (2009) metode for dokumentanalyse, og skal bidra til forståelse for hvordan dokumentet og løsningene er begrunnet og forstått. I følge Bacchi (2009) så handler det om at forståelsen av det vi foreslår å gjøre noe med avslører hva vi mener er viktig å endre på, og derav hva vi mener er problemet egentlig er. Med andre ord, forslagene som presenteres gir sterke føringer for tolkninger av hva problemet egentlig er.

Spørsmål 6 er valgt for å gi et sammenligningsgrunnlag på tvers av dokumentasjon knyttet til hvordan løsningene er utformet. Utforming kan trolig ha en påvirkning på prioritering på bakgrunn av kompleksitet.

5.3 Utvalg av dokumenter

I prosessen med å identifisere relevante dokumenter for vår studie, ble visse hovedelementer vektlagt i utvelgelsen av materiale. Gitt at oppgavens søkelys er på norske myndigheters forståelse av digital sikkerhet, var det logisk å undersøke de mest sentrale styringsdokumentene knyttet til dette temaet. Det overordnede tverrsektorielle dokumentet som danner grunnlaget for alt arbeid med digital sikkerhet i Norge er *Nasjonal strategi for digital sikkerhet*, utarbeidet av Justis- og beredskapsdepartementet. Dette dokumentet er naturlig å analysere da grunnlaget for alle sektorers arbeid med digital sikkerhet legges i dette dokumentet. For å identifisere hovedtendenser i prioriteringer, vil det videre være interessant å analysere ytterligere tre dokumenter som belyser problemstillingen. De to første dokumentene er direkte forgjengere til *Nasjonal Strategi for Digital Sikkerhet*. Man kan si at de danner grunnlaget for utarbeidelsen av strategien. Det første dokumentet er NOU 2015:13*,* en offentlig utredning laget av Lysneutvalget. Det andre dokumentet er *Melding til Stortinget nr. 38* av Justis- og beredskapsdepartementet, som beskriver departementets politikk for temaet med utgangspunkt i NOU 2015:13. Med bakgrunn i at samordningsansvaret for digital sikkerhet i sivil sektor ligger hos Justis- og beredskapsdepartementet, var det naturlig for oss å basere dokumentanalysen i stor grad på dokumenter med opphav hos Justis- og beredskapsdepartementet, herunder også Sikkerhetsloven (*Lov om nasjonal sikkerhet*) som står sentralt hva angår hvilke pålegg underlagte norske virksomheter har knyttet til digital sikkerhet. I tillegg tar den nye sikkerhetsloven av 2020 innover seg digital sikkerhet på en mer fleksibel måte sammenliknet med tidligere, og legger økt vekt på risikovurderingen som styrende for de sikkerhetstiltak virksomheten pålegges (NSM, 2020). Den overordnede hensikten med å velge ut disse dokumentene er å lete etter endringer i prioriteringer i dokumentene, og forsøke å beskrive hvilke utfordringer som følger av å sette prioriteringene ut i praksis.

5.3.1 NOU 2015:13 Digital Sårbarhet - sikkert samfunn

NOU 2015:13 er en norsk offentlig utredning gjennomført av Lysneutvalget i 2015. Den ble bestilt og skrevet med bakgrunn i de store endringene i det offentlige Norge knyttet til digitalisering. Utredningen er skrevet av anerkjente fagressurser med kunnskap om temaet, og skal gi anbefalinger til Justis- og beredskapsdepartementet om hvordan politikk bør utformes i møte med et økt digitalt trussel- og sårbarhetsbilde for sivil sektor. Justis- og beredskapsdepartementet har samordningsansvaret for arbeidet med digital sikkerhet. Utredningen er valgt som datakilde i denne oppgaven fordi det er den første offentlige utredningen om temaet som ble gjennomført etter at Justis- og beredskapsdepartementet fikk samordningsansvaret i 2013. Det antas at diskusjoner, konklusjoner og anbefalinger fra denne rapporten kan brukes som et godt utgangspunkt for å identifisere hvor myndighetenes prioriteringer kommer fra, og for å undersøke hvilke hovedtendenser man ser i prioriteringene.

5.3.2 Melding til Stortinget 38 (2016-2017)

Melding til Stortinget 38, også kjent under navnet "IKT-sikkerhet - Et felles ansvar", var den første stortingsmeldingen om digital sikkerhet. Etter at digitalt sårbarhetsutvalg (Lysneutvalget) gjorde sitt arbeid i 2015, og senere publiserte sine funn i NOU 2015:13 Digital sårbarhet - sikkert samfunn, gir stortingsmelding 38 en innsikt i regjeringens IKT-sikkerhetspolitikk. I tillegg gir stortingsmeldingen en oversikt over oppfølging av anbefalinger gitt i rapporten fra Lysneutvalgets arbeid. Stortingsmeldingen gir myndighetenes oppdaterte politikk knyttet til digital sikkerhet innenfor en rekke samfunnsområder. St. Meld. 38 består av fire deler. Del 1 er en introduksjon med bakgrunn, rammer, innhold relatert til IKT-sikkerhet presenteres. Del 2 av dokumentet omtaler sentrale områder av samfunnet der hvor digital sikkerhet bør inngå som en del av politikken. I denne delen legges det også frem konkrete tiltak innenfor en rekke sektorer. Tiltakene spenner fra organisatoriske grep, til politiske endringer og lovforslag. Del 3 omtaler Lysneutvalgets anbefalte tiltak og myndighetenes foreløpige arbeid med tiltakene. Den siste delen av dokumentet, del 4, diskuterer økonomiske og administrative konsekvenser knyttet til IKT-sikkerhet, implementering og organisering.

5.3.3 Nasjonal strategi for digital sikkerhet

Regjeringen ga i 2019 ut Norges strategi for digital sikkerhet (Departementene, 2019). Dette ble Norges fjerde strategi for digital sikkerhet gjennom historien, og la grunnlaget for det arbeidet som skal gjøres i tiden fremover, for å sikre norske offentlige og private aktørers digitale sikkerhet. Strategien er utarbeidet i den hensikt å dekke både private og digitale aktørers utfordringer og perspektiver, og ble utarbeidet gjennom en rekke workshops med deltakelse fra en rekke aktører, i tillegg til at det ble gjennomført en strategikonferanse.

Strategien legger til grunn myndighetenes 5 prioriterte områder for digital sikkerhet. Disse er (Departementene, 2019,): (1) Forebyggende digital sikkerhet, altså at norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser. (2) Digital sikkerhet i kritiske samfunnsfunksjoner, at kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur. (3) Kompetanse, at digital sikkerhetskompetanse styrkes i tråd med samfunnets behov. (4) Avdekke og håndtere digitale angrep, altså å øke samfunnets evne til å avdekke og håndtere digitale angrep. (5) Bekjempelse av data- og IKT-relatert kriminalitet, gjennom å styrke politiets evne til å bekjempe data- og IKT-kriminalitet. Videre beskriver strategien 10 konkrete tiltak alle virksomheter kan iverksette for å bedre sin egen evne til å motstå og håndtere digitale hendelser. Tiltakene er beskrevet gjennom en punktvis liste, som er utformet som en plakat virksomheten kan henge opp i sine lokaler. Se utsnitt av plakaten på neste side.

START-TIPS	✕ ✓	START-TIPS	✕ ✓
Etabler tilstrekkelig systematikk for sikkerhetsstyring, og sørg for at en fagperson støtter ledelsen i arbeidet.		Oppgrader program- og maskinvare. Fjern unødvendig kompleksitet og ubrukt funksjonalitet. Blokker kjøring av ikke-autoriserte programmer.	
Inkluder digital sikkerhet i virksomhetens risikoarbeid. Etabler tydelig ansvar i virksomheten, og effektive rapporteringslinjer til toppledelse og styre.		Installer sikkerhetsoppdateringer så raskt som mulig. Beskytt trådløse nettverk med sterke sikkerhetsmekanismer. Planlegg og dokumenter endringer. Slå på logging og gjennomgå viktige logger jevnlig.	
Lag en oversikt over virksomhetens sentrale mål, hvilke verdier og verdikjeder som inngår, hvor viktige data lagres og hvem som har tilgang til disse dataene.		Bruk kun siste versjon av nettlesere. Beskytt e-post med DMARC. Krypter viktig informasjon når det lagres på bærbare medier og når det sendes over nettet.	
Kartlegg virksomhetens sikkerhetskultur og identifiser hva som kan forbedres. Fastsett ønsket kultur og gjennomfør tilpasset, årlige treningsprogram for å fremme god sikkerhetskultur.		Endre standard passord og ikke tildel sluttbrukere administratorrettigheter. Bruk 2-faktorautentisering, eller som et minimum, sterke passord.	
Sats på god bestillerkompetanse og gjør en risikovurdering som forankres hos ledelsen.		Etabler en beredskapsplan for ulike typer hendelser og gjennomfør øvelser som tester planverket.	

Figur 3: Tiltak for økt digital sikkerhet i virksomheter (Departementene, 2019, s. 17).

5.3.4 Lov om Nasjonal Sikkerhet (Sikkerhetsloven)

Sikkerhetslovens overordnede formål er å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. Dette gjør loven gjennom forebygging, avdekking og å motvirke sikkerhetstruende virksomhet. Lovens hensikt er også å bidra til at sikkerhetstiltak beskrevet i loven gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.

Sikkerhetsloven er bygget opp av selve loven med forskrifter. Disse forskriftene regulerer ulike deler av samfunnet der sikkerhet er relevant. Eksempelvis har sikkerhetsloven forskrifter som dekker Dronning Mauds land, Svalbard og Jan Mayen. Dette er deler av norsk territorium som vil ha særskilte utfordringer knyttet til sikkerhet. Andre forskrifter inkluderer forskrift om sikkerhetsklarering, forskrifter om militære forbudssoner, forskrift om kryptosikkerhet og virksomhetsikkerhetsforskriften (Forsvarsdepartementet, 2018). Denne oppgaven vil ikke ta for seg lovens forskrifter, da dette anses som utenfor oppgavens søkelys. Denne oppgaven søker å klarlegge overordnede endringer i myndighetenes tilnærming til digital sikkerhet, og detaljer i alle forskrifter knyttet til sikkerhetsloven er derfor vurdert å ikke være relevante for oppgavens problemstilling.

Sikkerhetsloven ble revidert i 2019, der den forrige utgaven dateres tilbake til 1998 (Regjeringen, 2017). Bakgrunnen for revideringen var blant annet økt globalisering og økt digitalisering i samfunnet (NSM, 2023). Der den tidligere loven la mer vekt på sikkerhetsgradert informasjon, er den nye loven mer fleksibel i sin tilnærming, og legger i større grad opp til at virksomheten selv skal definere forsvarlige sikkerhetsnivåer ut fra et bredere spekter av verdier (NSM, 2023). Gjennom å kartlegge hvilke trusler som er relevante for sin organisasjon, er tanken at den nye sikkerhetsloven skal kunne benyttes fleksibelt i utarbeidelsen av mottiltak. Et annet viktig grep som direkte angår digital sikkerhet, er at den nye sikkerhetsloven nå forankrer NSM sitt ansvar for varslingssystem for digital sikkerhet (VDI) og NorCERT, som er den sentrale enheten for hendelseshåndtering knyttet til digitale hendelser.

Som styrende dokument representerer Sikkerhetsloven Norges dimensjonerende krav til norske offentlige virksomheter hva angår tiltak for å beskytte virksomheten og Norge mot sikkerhetstruende hendelser. Loven gjelder i utgangspunktet kun offentlige virksomheter, men vil etter beslutning kunne gjelde et hvert departement. Dersom virksomheten behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner, eller at virksomheten driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner, vil Sikkerhetsloven kunne gjelde (Forsvarsdepartementet, 2018, §1-3).
Når det gjelder digital sikkerhet, er lovens generelle krav til sikkerhet, herunder objektsikring og informasjonssikkerhet gjeldende for også digital sikkerhet i virksomhetene. I tillegg beskriver kapittel 6 i loven temaet "Informasjonssystemsikkerhet". Kapittelet beskriver krav til skjermingsverdige informasjonssystemer, herunder hvordan systemene skal beskyttes og godkjennes. Videre beskriver loven krav til informasjonssystemenes overvåkning og inntrengningstesting. Avslutningsvis beskriver kapittelet hvordan innholds- og kommunikasjonskontroll av informasjonssystemene skal drives (Forsvarsdepartementet, 2018, §6-6).

6 Analyse av dokumenter

6.1 Analyse av NOU 2015:13 Digital sårbarhet - sikkert samfunn

Digitalisering i Norge har vært rask og omfattende i det norske samfunnet. Norge er på verdenstoppen innen digitalisering og bruk av IKT. Det var allerede i 2015, da dokumentet ble utviklet, ingen grunnleggende nasjonale funksjoner i Norge som ikke var påvirket av digitalisering. Digitalisering har enorme fordeler for å øke både effektivitet og innovasjon i levering av tjenester til norske borgere. Det er imidlertid en skyggeside ved digitalisering som omhandler muligheten for uønskede hendelser som kan føre til tap av enten konfidensialitet, integritet eller tilgjengelighet på systemer og informasjon. Dette kan ha negative konsekvenser for både individet og staten. På bakgrunn av dette ble det oppnevnt et utvalg som skulle sørge for at sårbarhetene digitaliseringen medførte blir håndtert på en tilfredsstillende og sikker måte. Resultatet ble NOU 2015:13 *Digital sårbarhet - sikkert samfunn*, populært kalt Lysneutvalget er en norsk offentlig utredning som skulle bidra til å kartlegge digital sårbarhet i det norske samfunnet. Basert på kartleggingen ga Lysneutvalget anbefalinger til tiltak for å styrke og samordne Norges digitale beredskap. Lysneutvalget bestod av ni medlemmer, ledet av professor Olav Lysne fra Simula Research Laboratory.

Mandatet til utvalget er basert på et behov for en gjennomgang som kartlegger samfunnets digitale sårbarheter slik at det dannes et solid faglig grunnlag for å ytterligere styrke og samordne beredskapen. Resultatet som ble forventet var at det ble dannet et grunnlag for å vurdere tiltak som støtter opp om overordnede mål som å trygge liv og helse, økonomisk vekst og sosial utvikling, rettigheter og eiendom, sikre ivaretakelse av lov og orden, nasjonale sikkerhetsinteresser, rettsstatlige prinsipper, personvern og demokratisk styresett. Deretter peker mandatet på ti spesifikke områder som utvalget skal utrede. Mandatet er svært bredt, og kommenteres også av utvalget selv. På grunn av bredden i mandatet så kommenterer utvalget følgende angående begrensninger: “Begrensningene innebærer at det ikke har vært mulig med en omfattende analyse av hvert enkelt område. Det vil derfor være digitale sårbarheter i samfunnet vårt som ikke er omhandlet i tilstrekkelig grad i denne utredningen” (NOU 2015:13, s.19). Begrensningens konsekvenser med manglende mulighet til omfattende analyser er verdt å merke seg som noe som kan få betydning for anbefalingene som er gitt, eller løsningene som foreslås.

Problemet dokumentet er satt til å løse er at myndighetene ved Justis- og beredskapsdepartementet ikke har nok innsikt i det digitale sårbarhetsbildet, og har følgelig utnevnt Lysneutvalget til å kartlegge dette, samt anbefale tiltak for å redusere risiko tilknyttet disse. NOUer er bestillingsverk som skal bidra med et faglig fundament for politiske avgjørelser. De brukes, siteres og gjengis i stor grad i Meldinger til Stortinget som beskriver politikken som utøves av regjeringen. Drøftinger fra NOUer tillegges vekt av jurister som rettskilder og omtales også som lovforarbeider. Dokumentet skal videre, i mer spesifikk forstand, hjelpe Justis- og beredskapsdepartementet å sikre evne til å håndtere de kartlagte sårbarhetene og opprettholde funksjonalitet i kritisk infrastruktur for digitale tjenester tilhørende grunnleggende nasjonale funksjoner. Grunnleggende nasjonale funksjoner er definert som funksjoner som er grunnleggende for å opprettholde nasjonens sikkerhetsinteresser.

Løsningene som Lysneutvalget foreslår, er beskrevet som tverrsektorielle sårbarhetsreduserende tiltak. I selve dokumentet er utredningen delt opp etter sektorer, for eksempel olje og gass, og finansielle tjenester. Løsningene skal imidlertid være omforent og aggregert slik at anbefalingene til Justis- og beredskapsdepartementet skal fungere på tvers av disse. Løsningene, eller anbefalingene, består av åtte hovedtemaer, med enkelte underpunkter under noen av temaene. De viktigste anbefalingene er tatt med i sammendraget i starten av dokumentet - og bidrar til å beskrive hva Lysneutvalget mener bør være høyeste prioritet for Justis- og beredskapsdepartementets arbeid med digital sikkerhet. Disse ni tiltakene er (NOU 2015:13, 2015, s.16-17):

1. Redusere kritikaliteten av Telenors kjerneinfrastruktur
2. Sikre balansen mellom personvern og et sikrere samfunn gjennom utredninger og offentlig debatt.
3. Bruk av kryptografi bør ikke reguleres
4. Styrke Justis- og beredskapsdepartementets tverrsektorielle virkemidler på IKT-sikkerhetsområdet
5. Etablere et helhetlig rammeverk for digital hendelseshåndtering
6. Styrke politiets evne til å bekjempe IKT-kriminalitet
7. Tydeliggjøre et myndighetsansvar for norsk romvirksomhet
8. Styrke IKT-sikkerhetskompetansen i flere sektortilsyn
9. Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet

Av disse tiltakene så ser vi flere tverrsektorielle tiltak hvor to hovedtendenser skiller seg ut. Tre av tiltakene, (6, 8 og 9,) har elementer av fokus på kompetanse og/eller kapasitet. Tiltak 6 handler om å styrke politiets evne til å bekjempe IKT-kriminalitet. Årsaken til at denne anbefalingen er trukket frem er at det er lave forventninger til hvilken bistand politiet kan gi når man blir utsatt for IKT-kriminalitet. Dette henger sammen både med kompetanse- og kapasitetsutfordringer hos politiet. Tiltak 8 handler om at økende takt på digitalisering innenfor de fleste sektorer fører til at tilsynsmyndighetene vil til stadighet møte nye og komplekse utfordringer, og utvalget peker på behovet for utvikling av IKT-sikkerhetskompetanse hos sektorene og hos tilsynsmyndighetene. Tiltak 9 anbefaler å etablere en overordnet nasjonal kompetansestrategi som skal sikre IKT-sikkerhetskompetanse som de har sett mangler på de fleste nivåer i samfunnet.

Den andre hovedtendensen er at Lysneutvalget anbefaler tiltak som krever omorganisering og/eller tydeliggjøring av myndighet. Tiltak 4 handler om å styrke tverrsektorielle virkemidler på IKT-sikkerhetsområdet ved hjelp av utvidelse av virkemiddelapparatet ved tilsyn, herunder ved utvikling av mekanismer for gjennomføring av sektorovergripende løsninger. Dette oppnås ved å "sette Justis- og beredskapsdepartementet bedre i stand" (Justis- og beredskapsdepartementet, 2015, s.16) ved tydeliggjøring eller utvidelse av myndighet. Tiltak 8 handler om å tydeliggjøre myndighetsansvaret for norsk romvirksomhet. Dette har bakgrunn i at de fleste samfunnsområder, gjennom digitale verdikjeder, er avhengige av digitale satellittbaserte tjenester. Jurisdiksjon knyttet til romvirksomhet er imidlertid komplekst, og er regulert gjennom hjemler i mange ulike lover og forskrifter.

Lysneutvalgets rapport har totalt 78 anbefalinger, og har en utforming hvor anbefalingen er skrevet som en kort setning med påfølgende utbrodering, og avslutningsvis en anbefaling om hvem som bør gjennomføre tiltaket. I tilfeller hvor det er flere involverte i utførelsen av tiltaket, gir Lysneutvalget også anbefaling om hvem som bør lede arbeidet. Det er verdt å nevne at Justis- og beredskapsdepartementet er bestiller av NOUen, og de nevnes i mange av tiltakene. Dette må sees i sammenheng med samordningsansvaret departementet ble gitt i 2013 da det ble overført fra Fornyings-, administrasjons- og kirkedepartementet i Kongelig Resolusjon 22.03.2013 (Lovdata, 2013).

6.2 Analyse av Melding til Stortinget nr. 38 (2016-2017) IKT-sikkerhet - et felles ansvar

Stortingsmelding 38 (2016-2017) "IKT-sikkerhet - et felles ansvar" er Justis- og beredskapsdepartementets tilråding og presenterer regjeringens IKT-sikkerhetspolitikk. Meldingen ble utviklet som del av en respons på den stadig økende trusselen for cyberangrep rettet mot norske myndigheter og individ i samfunnet. Dokumentet er basert på Lysneutvalgets "NOU 2015:13 Digital sårbarhet - sikkert samfunn" og beskriver hvordan en kan arbeide mot å oppnå en helhetlig tilnærming til IKT-sikkerhet. Det er videre tydelig at stortingsmeldingen har til hensikt å fremme et samarbeid mellom offentlige og private sektorer om å beskytte norsk digital infrastruktur. Det fremkommer at alle virksomheter i Norge har ansvar for å ivareta egen IKT-sikkerhet. Samtidig har hver enkelt statsråd et overordnet ansvar for å ivareta IKT-sikkerheten i egen sektor, mens Justis- og beredskapsdepartementet er i tillegg tillagt et samordningsansvar. Videre er det kun Justis- og beredskapsdepartementet som har i oppdrag å utforme regjeringens politikk for IKT-sikkerhet, herunder etablere nasjonale krav og anbefalinger på IKT-sikkerhetsområdet for både offentlige og private virksomheter (Justis- og beredskapsdepartementet, 2017). Det fremkommer også at berørte fagdepartement, myndigheter og næringslivet skal involveres i dette arbeidet. Pålagte krav skal samtidig være hjemlet i lov og forskrifter.

I del én av stortingsmelding 38 beskrives bakgrunn, rammer, meldingens innhold, utviklingstrekk og betydning av IKT-sikkerhet og personvern. De sentrale målene med dokumentet er utviklet av Justis- og beredskapsdepartementet og ment som tilråding for Stortinget. En kan si at det er tre sentrale mål med stortingsmeldingen (Justis- og beredskapsdepartementet, 2017):

1. Beskytte viktige nasjonale IKT-systemer og infrastruktur mot cyberangrep
2. Styrke samarbeidet mellom offentlige og private sektorer for å forbedre IKT-sikkerheten i Norge
3. Fremme sikkerhetskultur og bevissthet om IKT-sikkerhet i hele samfunnet.

I del to av stortingsmeldingen beskrives generelle tiltak for å bedre nasjonal IKT-sikkerhet. Tiltakene er kategorisert i flere sentrale områder (Justis- og beredskapsdepartementet, 2017):

1. Et felles ansvar
2. Forebyggende IKT-sikkerhet

3. Avdekke og håndtere digitale angrep
4. IKT-sikkerhetskompetanse
5. Kritisk IT-infrastruktur

De overnevnte sentrale områdene brytes videre ned i 26 underkategorier. Denne fragmenteringen har trolig til hensikt å lette arbeidet med å identifisere hvem som er relevante i arbeidet med de anbefalte tiltakene, samt hvem som kan bli påvirket av deres effekt. En nedbryting av fem sentrale områder til 26 underkategorier kan også bidra til å identifisere nye området som eventuelt er ubevisst utelatt. Under kan man se hvordan de sentrale områdene er delt opp (Justis- og beredskapsdepartementet, 2017):

- **Et felles ansvar** inkluderer tre undergrupper: offentlig - privat samarbeid, internasjonalt samarbeid og sivil - militært samarbeid.
- **Forebyggende IKT-sikkerhet – virksomheters egen-evne** er delt opp i åtte grupper: rettslig regulering på IKT-sikkerhetsområdet, organisering av tverrsektorielt ansvar, systematisering og utvikling av anbefalinger og krav, tjenesteutsetting, inntrenging-tester, kunnskapsgrunnlag, kultur - ledelse og holdninger, personvern og forebyggende IKT-sikkerhet.
- **Avdekke og håndtere digitale angrep** er også delt inn i åtte grupper: Varslingssystemet for digital infrastruktur, rammeverk for digital hendelseshåndtering, informasjonsdeling, digitalt grenseforsvar, IKT-kriminalitet, koordinering mellom NSM, Etterretningstjenesten, PST og politiet for øvrig, åpenhet om digitale angrep og analysekapasitet.
- **IKT-sikkerhetskompetanse** er delt inn i syv grupper: Nasjonal kompetansestrategi for IKT-sikkerhet, grunnskole og videregående opplæring, høyere utdanning, forskning, etter- og videreutdanning, kompetansen i tilsyn og øvelser.
- **Kritisk IKT-infrastruktur** er delt inn i fem grupper: Alternative kjernenett og robusthet i de regionale transportnettene, utenlandsforbindelser, nød- og beredskapskommunikasjon, IKT-sikkerhet i styrings- og kontrollsystemer, personvern og kritisk IKT-infrastruktur - kommunikasjonsvern.

I del tre av stortingsmeldingen presenteres en oversikt og gjennomgang av myndighetenes vurdering og oppfølging av Lysneutvalgets anbefalinger fra 2015, samt en oversikt over prioriterte tiltak og forbedringsområder for det videre oppfølgingsarbeidet. Det fremkommer i

denne delen behovet for en bred tilnærming til arbeidet med IKT-sikkerhet i tiden fremover. Meldingen beskriver også at flere sektorer arbeider med de samme utfordringene, men at det er et manglende tverrsektorielt samarbeid. Eksempelvis jobber flere sektorer med utvikling av kompetanse innen IKT-sikkerhet eller håndtering av alvorlige digitale hendelser, men det er delvis/ingen samarbeid som kan bidra til å lette det omfattende arbeidet. I Stortingsmeldingen blir grunnlaget for, og regjeringens prioriteringer med spesiell relevans for, nasjonal IKT-sikkerhet beskrevet. Departementet uttrykker at følgende prioriteringsområder er av særlig betydning for nasjonal IKT-sikkerhet: forebyggende IKT-sikkerhet, virksomheters egenevne, avdekke og håndtering av digitale angrep, IKT-sikkerhetskompetanse og kritisk IKT-infrastruktur. Oppfølgingen av Lysneutvalgets anbefalinger er delt inn i 13 kategorier: Elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, olje og gass, vannforsyning, finansielle tjenester, helse og omsorg, transport, kompetanse, styring og kriseledelse, digitale angrep, felleskomponenter og tverrsektorielle tiltak. Hver av de nevnte 13 kategoriene brytes videre ned i problembeskrivelser med henvisning til ulike punkter i Lysneutvalgets utredning. Totalt sett er det 59 tiltak som skulle følges opp som et resultat av Lysneutvalgets anbefalte tiltak i deres utredning. De anbefalte tiltakene er beskrevet på følgende måte: Nummerering, overordnet tittel, referanse til relevante punkt i NOU, generell beskrivelse av problem og generell status på tiltak. Nedenfor kan man se et eksempel på hvordan utformingen av en løsning er utformet (Justis- og beredskapsdepartementet, 2017):

> **“18.1 Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet**
> *Problembeskrivelse (NOU 2015: 13, punkt 19.8)*
> IKT-sikkerhetskompetanse er mangelvare i Norge, og det er nødvendig å iverksette både langsiktige og kortsiktige tiltak. I dag utdannes det for få innenfor IKT-fagene, spesielt innenfor IKT-sikkerhet. En nasjonal kompetansestrategi innenfor IKT-sikkerhet er nødvendig for å få langsiktighet i finansieringen og på den måten sørge for å bygge opp varige kompetansemiljøer. Skal Norge som nasjon være rustet til å møte den økende digitale sårbarheten i samfunnet, må kompetansen innenfor IKT-sikkerhet bygges gjennom hele utdanningsløpet.
>
> *Status på tiltak*
> Anbefalingen fra Lysneutvalget har bred støtte i høringsuttalelsene. Vektlegging av kompetansebehov for IKT og IKT-sikkerhet er også i tråd med regjeringens overordnede IKT-politikk slik denne er lagt fram i Meld. St. 23 (2015–2016) Digital

> agenda for Norge og Meld. St. 10 (2016–2017) Risiko i et trygt samfunn. Regjeringen vil i tiden fremover sette i verk flere tiltak for å styrke IKT-sikkerhetskompetansen i Norge, herunder utarbeide en nasjonal kompetansestrategi innenfor IKT-sikkerhet. Strategien vil legge føringer for kommende tiltak. Se en bredere omtale av tiltaket i punkt 8.1." (Justis- og beredskapsdepartementet, 2017, s. 65)

I del fire av stortingsmeldingen beskrives økonomiske og administrative konsekvensene av det foreslåtte IKT-sikkerhetsarbeidet. Omfanget av denne beskrivelsen er på en halv side, og beskriver i svært liten grad hvordan dette arbeidet skal utføres. Det anbefalte arbeid skal være en integrert del av den ordinære styringen og innenfor gjeldende budsjettrammer. Eventuelle tiltak som medfører en ekstrautgift for departementene i statsbudsjettet vil behandles i årlige budsjettforslag, og regjeringen vil komme tilbake til dette hvis relevant. Den siste delen av stortingsmeldingen er mangelfull, det fremkommer ingen tidfesting i når tiltak kan, bør eller må gjennomføres.

6.3 Analyse av Lov om nasjonal sikkerhet (Sikkerhetsloven)

Lov om nasjonal sikkerhet ble revidert i 2018, og ble endret med bakgrunn i endrede behov for ivaretakelse av norske virksomheters sikkerhet. Særlig gjorde økt globalisering og økt digitalisering det klart at behovet for en revidert lov var nødvendig (NSM, 2023). Den nye sikkerhetslovens hovedformål er beskrevet i første kapittel av loven. Loven skal "Trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser." Videre skal loven "Forebygge, avdekke og motvirke sikkerhetstruende virksomhet", og loven skal "Bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn" (Forsvarsdepartementet, 2018). Sikkerhetsloven skal altså først og fremst beskytte Norge, og gjennom dette sørge for at norske virksomheter strukturerer sitt sikkerhetsarbeid på en slik måte at eventuelle angripere ikke får muligheten til å påvirke noen av de nevnte formålene med dokumentet. Som dokument er sikkerhetsloven et regulerende dokument, som gir krav til norske virksomheter innen sikkerhetsarbeid. Loven gir videre grunnlag for å eventuelle dømme norske virksomheter som bevisst eller ubevisst bryter disse fastsatte reglene.

Sikkerhetsloven skiller seg grunnleggende i denne oppgaven fra de andre dokumentene i studien, da dokumentet er en lov. Sikkerhetsloven består av selve loven med en rekke

forskrifter. De andre dokumentene i analysen er policydokumenter, og vil i så måte kunne være mer vage og strategiske i sin ordlyd enn loven. Lover skal være presise og regulerende, og skal danne det juridiske grunnlaget for hvordan et spesifikt tema eller område reguleres av myndighetene. Sikkerhetsloven inngår blant Norges formelle lover (SNL, 2021). Formelle lover i Norge kan kun vedtas av den lovgivende makt, Stortinget, og krever flertall i Stortinget for å kunne vedtas, og denne versjonen av Sikkerhetsloven ble vedtatt i Stortinget og trådte i kraft 1. januar 2019 (Forsvarsdepartementet, 2018, §12-1).

Den nye sikkerhetsloven (2019) har flere fundamentale endringer sammenlignet med forgjengeren, lov om forebyggende sikkerhet av 1998 (NSM, 2023). De viktigste endringene inkluderer måten loven legger opp til at virksomhetene skal oppnå høy sikkerhet. Der den forrige loven i større grad beskrev hvordan virksomhetene skulle oppnå sikkerhet på, beskriver heller siste versjon krav til hva virksomhetene skal oppnå (NSM, 2019). Hovedhensikten med denne endringen er å gjøre de ulike virksomhetene i stand til å selv vurdere risiko, og tilpasse sikkerhetsarbeidet i takt med sikkerhetsutfordringene. Disse endringene gjennom økt ansvarliggjøring av virksomhetene selv, kommer på bakgrunn av de svært ulike kravene virksomhetene som arbeider med sikkerhet opplever. De rent konkrete endringene i loven er blant annet inndeling av fagområder. Lov om forebyggende sikkerhet (1998) var delt inn i fagområdene sikkerhetsadministrasjon, personellsikkerhet, sikkerhetsgraderte anskaffelser, objektsikkerhet og informasjonssikkerhet. Denne inndelingen var hensiktsmessig i den forrige utformingen, da loven fastsatte konkrete krav til virksomhetene innenfor disse kategoriene. En av utfordringene justis- og beredskapsdepartementet vurderte med denne tilnærmingen, var at loven la opp til at man at man skulle arbeide med sikkerhet avdelt i sitt respektive fagområde, heller enn å søke å strukturere virksomhetens sikkerhetsarbeid mer tverrfaglig. En av ideene med den nye inndelingen av sikkerhetsloven, er derfor at den nye strukturen i økende grad skal oppfordre virksomheter til å arbeide helhetlig med sikkerhet, heller enn å velge seg ut enkelte fagområder og tilpasse disse til lovens krav (Forsvarsdepartementet, 2018).

Endringen av sikkerhetsloven kommer som følge av endrede krav til sikkerhet i dagens samfunn, sammenlignet med sikkerhetssituasjonen som dannet grunnlaget for den forrige sikkerhetsloven. Vi kan forstå at myndighetene i Norge innså at den forrige sikkerhetsloven sto til hinder for å oppnå et høyere sikkerhetsnivå blant de omfattede virksomhetene, og en ny lov var i så måte nødvendig. Vi kan også forstå at myndighetene, gjennom hendelser som har

fått stor medieoppmerksomhet, sammen med et stadig økende fokus globalt på sikkerhetsarbeid, opplevde at en modernisering av lovverket var betimelig. Det er allikevel nødvendig å vurdere hvorvidt den nye loven har skapt økte muligheter for sikkerhetsarbeid i virksomhetene.

Et argument som taler mot den nye sikkerhetsloven, er den økte ansvarliggjøringen av virksomhetene selv i struktureringen av sitt sikkerhetsarbeid. Dette stiller nye krav til virksomhetene selv, og legger et økt press på kompetanseheving hos den enkelte virksomhet. Da sikkerhetsarbeid må struktureres for å møte de aktuelle truslene som finnes mot virksomhet, og at disse truslene i senere tid i stadig økende grad blir digitale, skapes et kompetansebehov som mange virksomheter sliter med å møte. I en rapport om IKT-sikkerhetskompetanse i Norge beskrev en artikkel i Norsk sosiologisk tidsskrift at Norge i skrivende stund manglet 2000 IT sikkerhetsfolk. Artikkelen anslo også at Norge vil mangle om lag 4100 mennesker med IKT-sikkerhetskompetanse i 2030 (NIFU, 2019). Utfordringer med sikkerhetskompetanse generelt, og IKT-sikkerhetskompetanse spesielt, kan virke å være en stor utfordring i å oppnå en god forvaltning av sikkerhet i virksomhetene som sikkerhetsloven regulerer. På den annen side er neppe sikkerhetslovens utforming kjerneproblemet i de utfordringer norske virksomheter har med bekjempelse av digitale trusler, og man kan si at IKT-sikkerhetskompetanse er noe som virksomhetene uansett må ha, uavhengig av hvilke krav sikkerhetsloven stiller til virksomhetene. Det virker likevel å være et poeng at sikkerhetslovens utforming ansvarliggjør virksomhetene selv i å strukturere sitt arbeid med digital sikkerhet i økt grad, noe som for virksomhetene mulig oppleves krevende å leve opp til, da kompetansekravet er stort og at mange virksomheter for tiden sliter med avvik hva angår digital sikkerhetskompetanse.

En annen viktig endring i ny sikkerhetslov, er økt samarbeid mellom privat og offentlig sektor i sikkerhetsarbeidet. Særlig gjennom sikkerhetslovens §2-4, som beskriver at regjeringen skal utpeke en myndighet med ansvar for: "... en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur" (Forsvarsdepartementet, 2018, §2-4). Ansvarlig myndighet for dette er utpekt til å være Nasjonal Sikkerhetsmyndighet (NSM), og etableringen av Nasjonalt Cybersikkerhetssenter (NCSC) ble gjennomført etter at loven kom ut, i 2019. En annen viktig endring som markerer et tydelig skille i retning av arbeidet med digital sikkerhet i sivil sektor, er skifte av ansvarlig departement for sikkerhetsloven. Den siste revisjonen av sikkerhetsloven ble utarbeidet av

Forsvarsdepartementet (Forsvarsdepartementet, 2018), og en av endringene i loven er at det fra loven ble satt i kraft, er Justis- og beredskapsdepartementet som har ansvar for videre utvikling av loven. Da Justis- og beredskapsdepartementet også har blitt pekt ut til å være departementet med ansvar for samordning av arbeidet med digital sikkerhet, markerer også endringen av ansvarshavende departement for sikkerhetsloven et tydelig skille mot ansvarliggjøringen av Justis- og beredskapsdepartementet.

6.4 Analyse av Nasjonal Strategi for Digital Sikkerhet

Ved analyse av dokumenter er det viktig å avdekke hvorfor et dokument er utviklet for å forstå innholdet i en bredere kontekst. *Nasjonal Strategi for Digital Sikkerhet* fra 2019 er den fjerde versjonen som er utarbeidet siden den første strategien kom i 2003. Årsaken til at den første strategien ble laget er beskrevet i forordet til den nåværende strategien som er signert av daværende statsminister Erna Solberg (2019, s.3):

> "Digitaliseringen av det norske samfunnet utfordrer oss også. Digitale infrastrukturer og systemer blir stadig mer komplekse, omfattende og integrerte. Det skapes avhengigheter og sårbarheter på tvers av ansvarsområder, sektorer og nasjoner. Det forventes at digitale tjenester skal være tilgjengelige til enhver tid. En vellykket digitalisering handler også om at løsningene ivaretar krav til sikkerhet og den enkeltes personvern på en god måte, og at vi kan ha tillit til at digitale løsninger fungerer slik de skal. Norges første nasjonale strategi for digital sikkerhet ble lansert allerede i 2003. Med denne ble Norge et av de aller første landene i verden som fikk en nasjonal strategi på området. I takt med utviklingen av trusselbildet ble den nasjonale strategien revidert i 2007 og 2012" (Departementene, 2019)

Videre kan vi se av sitatet at strategien må utvikles som følge av at trusselbildet forandrer seg. Utarbeidelsen av versjonen fra 2019 er et produkt av slik endring, og det var et økt behov for en strategi for å møte utfordringer som følger av rask og gjennomgående digitalisering av det norske samfunnet som var i tråd med tiden. Det blir beskrevet i dokumentet at det var et tydelig behov for økt offentlig-privat, sivilt-militært og internasjonalt samarbeid som også bidro til at strategien hadde behov for revisjon. Dette har trolig sammenheng med at digitaliseringen, som beskrevet i forordet av Erna Solberg, i økende grad har blitt mer knyttet

sammen som fører til at det ikke lenger er nok å ha kontroll i egen sektor. Kontrollen må strekke seg lenger.

I dokumentet så står det at utgiver av strategien er "Departementene", og ingen spesifikke departementer navngis. Det er imidlertid beskrevet i forordet av Erna Solberg (2019) følgende om utarbeidelsen:

> "I utarbeidelsen av strategien er det lagt vekt på inkludering av aktører i privat og offentlig sektor, for å sikre at strategien er relevant. Strategikonferansen med over 300 deltagere, skriftlige innspill og høy deltagelse i en rekke workshops viser at det er stor interesse for å finne felles løsninger" (Departementene, 2019).

Ved å inkludere så mange aktører fra både privat- og offentlig sektor, samtidig som fokuset har vært på felles løsninger kan man anta at en mer demokratisk prosess har blitt benyttet slik at strategien er et produkt som kan fungere hvis den blir fulgt opp tilstrekkelig. Dette kan bidra til å øke strategiens troverdighet og minimere sjansen for at det er spesielle interesser som har påvirket strategien til å fokusere i en spesiell retning.

Når man skal gjennomføre en dokumentanalyse er det viktig å forstå hvilke mål dokumentet har til hensikt å oppnå. Uten tydelig målformulering kan det være vanskelig å vite når implementering av foreslåtte løsninger er gjennomført, eller vite om man har oppnådd ønsket effekt av de gjennomførte endringene eller implementeringene. I *Nasjonal Strategi for Digital Sikkerhet* (2019) er det beskrevet fem hovedmål som søkes oppnådd ved å følge strategien:

1. Norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser.
2. Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur.
3. Styrket digital sikkerhetskompetanse i tråd med samfunnets behov.
4. Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.
5. Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.

Målene fungerer godt som overordnede beskrivelser av hva som ønskes oppnådd, men er mindre gode til å beskrive når ønsket sluttilstand er oppnådd. Disse målene vil være viktige for besvarelsen på problemstillingen, og vil adresseres senere i oppgaven når vi skal drøfte hvilke hovedtendenser vi ser i myndighetens prioriteringer innen digital sikkerhet.

Det er videre beskrevet i dokumentet at ivaretakelse av digital sikkerhet først og fremst er et virksomhetsansvar, hvor det påpekes at virksomhetsledere er ansvarlige for å få gjennomført risikovurderinger, og på bakgrunn av disse gjennomføre tilstrekkelige tiltak (Departementene, 2019, s.22). Hver enkelt statsråd har i tillegg et overordnet ansvar for ivaretakelse av digital sikkerhet i sin egen sektor. Det er imidlertid én aktør som har tverrsektorielt ansvar, Justis- og beredskapsdepartementet (JD). JD har ansvar for samordning i sivil sektor, og et generelt samordningsansvar for samfunnets sivile sikkerhet. Forsvarsdepartementet har på sin side ansvar for digital sikkerhet i forsvarssektoren. I denne oppgaven ønsker vi å vie spesiell oppmerksomhet mot JD og deres ansvar, og samordningsevne som verktøy for å øke digital sikkerhet i blant offentlige virksomheter i Norge.

Carol Bacchis metode for kritikk av policyer er lagt til grunn for analysespørsmålet knyttet til hva er problemet som skal løses. Bacchi (2009) beskriver viktigheten av å forstå både hva problemet er som det er beskrevet i dokumentet, men også hva som ikke er beskrevet og konsekvensen av det. I *Nasjonal Strategi for Digital Sikkerhet* så er det innledningsvis beskrevet at strategien er utviklet for å bidra til å oppnå et felles grunnlag for håndtering av digitale sikkerhetsutfordringer. Det er imidlertid ikke en problembeskrivelse, men heller en ønsket effekt av strategiens implementering. Det nevnes derimot noen sårbarheter som bidrar til å øke forståelsen for problemet som ligger til grunn for en ønsket endring i måten man jobber med digital sikkerhet på. Det første er en opplevd manglende enhetlig tilnærming til digital sikkerhet, og det andre er en påfølgende sårbarhet som manglende samordning og utnyttelse av ressurser på tvers av sektorer og virksomheter. Dette er utfordringer som strategien søker å løse, og det vil påvirke evnen til å håndtere digitale sikkerhetsutfordringer. Det som imidlertid fremstår som den problemformuleringen som treffer nærmest kjernen er at digital sikkerhet er en særlig viktig forutsetning for å opprettholde tilliten til offentlig sektors IKT-systemer, og offentlige digitale systemer. Av dette kan vi forstå at det ikke er trusselbildet i seg selv, eller konsekvensene av hendelser, som er driveren for ønsket om sterkere digital sikkerhet, men et ønske om å opprettholde tillit til systemer og løsninger. Tillit til systemer og løsninger henger til syvende og sist sammen med tillit til myndighetene.

Strategien gjør imidlertid en god jobb med å foreslå løsninger som skal sørge for opprettholdelse av denne tilliten. Det er utarbeidet fem mål, hvor alle har sine tilhørende delmål som varierer i antall fra to til åtte. Hvert overordnede mål er tilknyttet et prioritert område, eksempelvis "Forebyggende digital sikkerhet" og "Avdekke og håndtere digitale angrep". I tillegg følger det et vedlegg til strategien med mer konkrete tiltak som skal innføres knyttet til hvert av de fem prioriterte områdene som fungerer som en videre operasjonalisering. Totalt antall tiltak i vedlegget er 51, men det er også utarbeidet ti ekstra tiltak som har til hensikt å hjelpe virksomheter til å øke sin egenevne til å håndtere digitale utfordringer. Det er også utarbeidet ti "start-tips" i plakat-form, som en del av strategien. Antallet tiltak kan virke skremmende, men en konkretisering kan gjøre det enklere å forstå hvordan man skal gå frem for å heve den digitale sikkerheten.

Løsningene som foreslås er relativt konkrete. Hver løsning, eller tiltak, består av fire elementer. Tittel, beskrivelse, ansvarlig myndighet og tidspunkt for gjennomføring. Se eksempel på neste side (Departementene, 2019, s.17):

> "**Tiltak 18: Statens standardavtaler**
> (SSA) Statens standardavtaler brukes i stort omfang, ikke bare ved offentlige anskaffelser, men også mellom næringsdrivende. Nærings- og fiskeridepartementet har det overordnede ansvaret for standardavtalene. Mer utfyllende sikkerhetsklausuler, i første omgang i avtalene som brukes ved IKT-drift og skytjenester, kan potensielt ha stor positiv innvirkning på mange avtaler om tjenesteutsetting av IKT-tjenester. JD og KMD vil, i samarbeid med underlagte fagmiljøer, vurdere behovet for revisjon av sikkerhetsklausulene relevante for tjenesteutsetting.
>
> Ansvarlig virksomhet: JD og KMD, i samarbeid med Difi og NSM
> Gjennomføres: 2019"

Tiltakene er konkrete i hva som søkes endret eller oppnådd, og stiller krav til av hvem og når tiltakene skal gjennomføres. Tiltakene er likevel skrevet på en måte som gir en beskrivelse av hva som ønskes oppnådd, fremfor hva som skal gjøres. Det vil derfor være opp til den ansvarlige myndigheten å selv definere hvilke løsninger man rent praktisk ender opp med for å oppnå tiltaket som er beskrevet i den nasjonale strategien. Strategien kan derfor sies å være

bygd opp av en rekke mål eller effekter som skal oppnås, som er bygd i et hierarki, men uten å presentere faktiske løsninger for hvordan man går frem for å få innført de gjeldende tiltakene. I eksempelet over så handler dette om at man skal styrke sikkerhetsklausulene, men det gis ingen veiledning på hva klausulene bør inneholde for å kunne ansees som styrket. Det refereres heller ikke til andre publikasjoner eller veiledninger som kan bidra til å svare på dette.

Løsningene presentert i vedlegget (Tiltaksoversikten) er utformet på en todelt måte. Den første delen er kalt "sentrale tiltak" og må forstås som tiltak som skal løses eller følges opp av de departementene de enkelte tiltak er delegert til. Det er imidlertid fortsatt Justis- og beredskapsdepartementet som har samordningsansvaret og det overordnede ansvaret for å følge opp strategien sammen med Forsvarsdepartementet. Tiltakene i del én er tiltakene som blir pålagt virksomheter og etater. Dette innebærer også berørte private aktører. Del to er anbefalte tiltak til virksomheter som de på eget initiativ kan gjennomføre for å øke sin egen evne til å beskytte seg mot og håndtere uønskede digitale hendelser. Tiltakene er generelt utformet, og skal kunne benyttes av norske virksomheter uavhengig av størrelse, modenhet og kompetanse om digital sikkerhet.

6.5 Sammendrag av analyser

	1	2	3	4	5	6
Navn på dokumentet	**Bakgrunn for at dokumentet er utviklet**	**Hvem har lagd dokumentet**	**Beskrivelse av sentrale mål med dokumentet**	**Problem som skal løses**	**Løsninger som foreslås**	**Utforming av løsningene**
NOU 2015:13	Lysneutvalget er satt ned av Regjeringen for å kartlegge samfunnets digitale sårbarhet. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Behov for en gjennomgang som kartlegger samfunnets digitale sårbarheter slik at vi kan få et solid faglig grunnlag for ytterligere å styrke og samordne vår beredskap.	Lysneutvalget på bestilling fra JD	Gi et grunnlag for å vurdere tiltak som støtter opp om overordnede mål som å trygge liv og helse, økonomisk vekst og sosial utvikling, rettigheter og eiendom, sikre ivaretakelse av lov og orden, nasjonale sikkerhetsinteresser, rettsstatlige prinsipper, personvern og demokratisk styresett	Manglende innsikt og forståelse av omfanget av digitale sårbarheter. Problemet som skal løses er manglende evne til å håndtere sårbarheter og opprettholde funksjonalitet i kritisk infrastruktur for digitale tjenester til samfunnsviktige funksjoner, evnt grunnleggende nasjonale funksjoner	Løsningene som foreslås er beskrevet som tverrsektorielle sårbarhetsreduserende tiltak, Består av 8 hovedtemaer - med noen underpunkter under enkelte av temaene. Det totale antall anbefalinger er 78. Det er i sammendraget dratt frem de viktigste anbefalingene - totalt 9	Løsningene er utformet som tverrsektorielle tiltak - og gir anbefalte løsninger for hvordan Justis- og beredskapsdepartementet kan gjennomføre regulering og bestemmelse på tvers av sektorer for å redusere sårbarheter.
Stortings-melding 38	Utviklet som en respons på den stadig økende trusselen fra cyberangrep mot norske myndigheter, virksomheter og innbyggere. Dokumentet ble utviklet for å presentere en helhetlig tilnærming til IKT-sikkerhet og for å fremme et samarbeid mellom offentlige og private sektorer for å beskytte Norges digitale infrastruktur.	Justis- og beredskapsdepartementet	1. Beskytte viktige nasjonale IKT-systemer og infrastruktur mot cyberangrep 2. Styrke samarbeidet mellom offentlige og private sektorer for å forbedre IKT-sikkerheten 3. Fremme sikkerhetskultur og bevissthet om IKT-sikkerhet i hele samfunnet	Manglende samarbeid mellom offentlige og private sektorer i å beskytte Norges digitale infrastruktur. Svakheter i nasjonale IKT-systemer. Manglende bevissthet om IKT-sikkerhet i hele samfunnet.	Tiltakene består av en overordnet tittel og en kort beskrivelse på overordnet nivå. 1. Styrking av det offentliges ansvar for IKT-sikkerhet 2. Styrking av kravene til IKT-sikkerhet i offentlige anskaffelser 3. Fremme samarbeid mellom offentlige og private sektorer for å forbedre IKT-sikkerheten 4. Etablere en nasjonal IKT-sikkerhetsmyndighet 5. Styrke bevisstheten om IKT-sikkerhet i hele samfunnet	Foreslåtte løsninger er utformet for å: • Styrke det offentliges ansvar for IKT-sikkerhet • Øke kravene til IKT-sikkerhet i offentlige anskaffelser • Fremme samarbeid mellom offentlige og private sektorer • Etablere en nasjonal IKT-sikkerhetsmyndighet • Øke bevisstheten om IKT- sikkerhet i hele samfunnet. Dokumentet foreslår en rekke tiltak med en helhetlig tilnærming til IKT-sikkerhet og et samarbeid for å beskytte Norges digitale infrastruktur.

	1	2	3	4	5	6
Sikkerhetsloven	Loven har 3 hovedformål: 1.Trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser. 2.Forebygge, avdekke og motvirke sikkerhetstruende virksomhet. 3.Bidra til at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn.	Forsvars-departementet	Hensikten med sikkerhetsloven er å regulere norske virksomheters sikkerhetsarbeid. Dette inkluderer forebyggende sikkerhetsarbeid, tilsyn, informasjonssikkerhet, informasjonssystemsikkerhet, objekt- og infrastruktursikkerhet, personellsikkerhet og sikkerhetsgraderte anskaffelser. Loven regulerer også eierskap over virksomheter som er underlagt sikkerhetsloven.	Loven skal oppnå lovens formål gjennom universelle krav samtidig som den dekker de mange ulike områder som sikkerhetsloven dekker på en fleksibel måte. Revidert sikkerhetslov skal i større grad ta høyde for økt digitalisering og globalisering.	Loven ble vedtatt av Stortinget i 2018, og ikraftsatt 1. januar 2019. Loven er en utvikling av sikkerhetsloven av 1998, og tar i større grad høyde for samfunnets økte globalisering og digitalisering.	Sikkerhetsloven regulerer norske virksomheter som omfattes av loven gjennom lovkrav til de ulike temaene listet i dokumentbeskrivelsen. Særlig området hva angår virksomhetenes risikovurderinger er nå i større grad enn tidligere omgjort til å være opp til virksomhetene selv, med bakgrunn i at de er best egnet til å vite hvilke sårbarheter hos dere som er størst.
Nasjonal Strategi for Digital sikkerhet	Regjeringen ønsker et felles grunnlag for håndtering av digitale sikkerhets-utfordringer	Departementene	1. Norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser. 2. Kritiske samfunnsfunksjoner er understøttet av en robust og pålitelig digital infrastruktur. 3. Styrket digital sikkerhetskompetanse i tråd med samfunnets behov. 4. Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep. 5. Politiet har styrket sin evne til å bekjempe data- og IKT-relatert kriminalitet.	Manglende enhetlig tilnærming til digital sikkerhet Manglende samordning og utnyttelse av ressurser på tvers av sektorer og virksomheter Sikre vedvarende tillit til offentlig myndigheters evne til å beskytte sine ikt-systemer og sikre digitale tjenester	Det følger med en egen tiltaksoversikt som vedlegg til strategien. Den inneholder 51 tiltak som bygger opp under de 5 prioriterte områdene. I tillegg har den 10 tiltak som skal øke virksomheters egenevne til å motvirke digitale sikkerhetsutfordringer Tiltakene er utformet med tittel, kort beskrivelse på overordnet nivå, ansvarlig myndighet og tid for gjennomføring.	Løsningene er utformet på en måte som forteller ansvarlig myndighet *hva* som må gjøres, og *hvorfor.* Strategien beskriver imidlertid ikke *hvordan*.

Figur 4: Sammendrag av analyser

7 Diskusjon

I dette delkapittelet diskuteres resultatene av dokumentanalysen. Oppgaven har her sammenfattet alle funn fra dokumentanalysene, og gjennom en tabell sammenliknet hovedtendensene som finnes i myndighetenes styrende dokumenter for digital sikkerhet. I dette kapittelet vil de to forskningsspørsmålene stå sentralt, da disse bygger opp under oppgavens problemstilling. I diskusjonskapittelet vil vi først identifisere hovedtendenser som presenteres i delkapittel 7.1, og diskuteres mot relevant teori og litteratur. Hensikten med dette er å kartlegge hvilke tendenser som finnes i styrende dokumenter utgitt av norske myndigheter vedrørende digital sikkerhet i perioden 2015 til 2019. Oppgaven vil forsøke å komme inn på mulige årsaker til at disse tendensene fremkommer slik de gjør, og beskrive muligheter og utfordringer knyttet til disse. I neste delkapittel tar oppgaven for seg myndighetenes utfordringer med å sette sine prioriterte tiltak ut i virke. Med bakgrunn i tidligere nevnte utfordringer for myndighetene med å øke nivået for digital sikkerhet generelt i samfunnet raskt nok i forhold til trusselen samfunnet står opp mot, er det relevant å kartlegge hvilke utfordringer som finnes med implementeringen av prioriterte tiltak. Gjennom dette har oppgaven til hensikt å finne ut hva Justis- og beredskapsdepartementet bør fokusere på som samordningsansvarlig i et instrumentelt organisasjonsteoretisk perspektiv for å sikre fremdrift i arbeidet med styrke digital sikkerhet i sivil sektor.

7.1 Hvilke hovedtendenser fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet?

Hovedtendensene som presenteres i dette delkapittelet er kartlagt gjennom analyser av alle oppgavens dokumenter beskrevet i analysekapittelet. Gjennom kartlegging og sammenligning av dokumentene, har oppgaven funnet hovedtendenser innenfor fire kategorier. Disse kategoriene inkluderer: Organisatoriske perspektiver, myndighetenes prioriteringer, forankring av ansvar, og målsettinger og krav.

7.1.1 Organisatoriske perspektiver

Gjennom oppgavens analyserte dokumenter, har oppgaven funnet flere organisatoriske tendenser som går igjen i myndighetenes styrende dokumenter for digital sikkerhet. De styrende dokumentene beskriver flere organisasjonsteoretiske aspekter ved bedringen av den digitale sikkerheten i Norge, og dette delkapittelet vil forsøke å kaste lys over disse. Oppgaven vil diskutere disse tendensene i dokumentene opp mot relevant organisasjonsteori,

i den hensikt å kunne skape økt innsikt i disse aspektenes påvirkning på den digitale sikkerheten i virksomhetene.

Et viktig tema som i liten grad er inkludert i oppgavens dokumenter er kultur. Sikkerhetskultur nevnes riktignok enkelte ganger i alle de analyserte dokumentene, med unntak av Lov om nasjonal sikkerhet. Kultur beskrives i NOU:2015 rapporten som: "Utover intuitive sikkerhetstiltak og opplæring vil enkeltindividets holdninger til sikkerhetsarbeidet og sikkerhetskulturen i miljøet rundt påvirke sikkerhetsnivået" (NOU 2015:13, 2015, 53). Vi forstår at NOU-rapporten sier at sikkerhetskulturen vil, som en av flere faktorer, påvirke sikkerhetsnivået hos virksomheten. Kongsvik et al (2018) beskriver arbeid med sikkerhet som en etablering av en rekke barrierer, og sikkerhetskulturen i en virksomhet vil utgjøre en slik barriere (Kongsvik et al., 2018, s. 22). Vi leser videre i *Nasjonal Strategi for Digital Sikkerhet* (2019) at et delmål under kapittel 3.1 beskriver følgende: "Befolkningen har en god digital dømmekraft og god sikkerhetskultur". Delmålet skal bygge opp under det overordnede målet: "Norske virksomheter digitaliserer på en sikker og tillitsvekkende måte, og har bedre evne til egenbeskyttelse mot uønskede digitale hendelser" (Departementene, 2019, 13). Den nasjonale strategien foreslår også sikkerhetskultur som et av tiltakene virksomheter kan arbeide med, og foreslår å implementere et tilpasset årlig treningsprogram for å fremme digital sikkerhet i virksomheten (ibid, 15).

Selv om temaet kultur og digital sikkerhetskultur nevnes i flere av dokumentene, vil likevel denne oppgaven argumentere for at temaet er nedprioritert i alle styrende dokumenter utgitt av myndighetene. Organisasjonskulturen i en virksomhet forbindes med de uformelle normene og verdiene som vokser fram og har betydning for livet i og virksomheten til formelle organisasjoner (Christensen et al., 2015, 52). Det virker å være slik at digital sikkerhetskultur er et lite prioritert område, samtidig som det er kjent at kompetansen på digital sikkerhet er lav blant ansatte i de fleste virksomheter i Norge. Christensen et al. (2015) beskriver institusjonalisering i virksomheter som et fenomen som gjerne vokser frem over mange år (Christensen et al., 2015, 53). Fordelen med en institusjonalisert kultur i organisasjonen kan være at oppgaver kan løses bedre, eller at man utvikler et sterkere sosialt fellesskap (ibid). Ulempene kan være at organisasjonen blir mer kompleks og mindre fleksibel, og tilpasningsdyktighet overfor nye krav kan være utfordrende (ibid). Når myndighetene virker å være lite opptatt av å omtale det å bygge en digital sikkerhetskultur for å motstå digitale angrep, kan det ha flere mulige forklaringer. Det kan være at myndighetene

opplever det som krevende å komme med råd knyttet til det å bruke tid på å utvikle organisasjonskulturen, da virksomhetene som dekkes av de styrende dokumentene er mange og svært mangfoldige, og dokumentene skal dekke alle typer virksomheter. Det kan videre tenkes at myndighetene velger å fokusere dokumentene mot andre tiltak, slik som konkrete sikkerhetstiltak eller å bygge kompetanse innenfor digital sikkerhet. Om virksomhetene generelt innfører disse tiltakene, er det grunn til å tro at også kulturen i organisasjonen vil endre seg. Det vil likevel etter denne oppgavens syn være nyttig for myndighetene å i økt grad benytte kultur og kulturbygging som et verktøy for innføring av nye tiltak for økt digital sikkerhet.

Et annet viktig organisatorisk grep som er gjennomført og gjennomgående i alle analyserte dokumenter, er omstruktureringen til at Justis- og beredskapsdepartementet (JD) har samordningsansvar for alt arbeid med digital sikkerhet i virksomheter i Norge. JD har ansvaret for Lov om nasjonal sikkerhet, etter at ansvaret ble overført fra Forsvarsdepartementet (NSM, 2019), og innehar ansvaret som tilsynsmyndighet. Samordningsansvaret ble videre tildelt JD i 2013, og har siden da blitt stadig videreutviklet. Riksrevisjonens rapport fra 2023 påpeker likevel at dette arbeidet ikke har kommet langt nok. Gjennom fire hovedtemaer påpeker Riksrevisjonens rapport at JD har mangler knyttet til samordning av arbeidet med digital sikkerhet. Det første temaet handler om svak samordning av roller, ansvar og krav som videre gjør arbeidet med forebyggende digital sikkerhet krevende for virksomhetene. Det neste punktet som Riksrevisjonen påpekte, er at JD ikke har gitt god nok informasjon om den nasjonale digitale sikkerhetstilstanden i Norge. Rapporten pekte også på at JD ikke har sørget for god nok oppfølging av den nye nasjonale strategien for digital sikkerhet, og at de ikke har lagt godt nok til rette for god tverrsektoriell hendelseshåndtering (Riksrevisjonen, 2023). Det er derfor tydelig at JD til en viss grad har tatt ansvar for samordningen av arbeidet med digital sikkerhet i Norge, men at en del arbeid også gjenstår.

En annen viktig omorganisering er dreiningen mot å pålegge virksomhetene selv mer ansvar for risikovurdering og egensikring. Med bakgrunn i at virksomhetene som omfattes av oppgavens analyserte oppgaver, og at arbeidet med digital sikkerhet vil være svært ulikt ved ulike virksomheter, søker både sikkerhetsloven og de nasjonale strategiene å legge vekt på helhetlige løsninger for digital sikkerhet der virksomheten selv skal vurdere sine egne sårbarheter. Det fremkommer gjennom analysen i forrige kapittel at *Nasjonal Strategi for*

Digital Sikkerhet legger til grunn en tilnærming til digital sikkerhet der myndighetene beskriver hva som skal oppnås innen tiltak for digital sikkerhet, og hvorfor disse tiltakene er viktige. Myndighetene legger seg imidlertid ikke opp i *hvordan* dette gjøres. Denne tilnærmingen skaper frihet for virksomhetene til å selv utforme sine tiltak, og gir økt ansvarliggjøring i virksomhetene selv. I forordet i *Nasjonal Strategi for Digital Sikkerhet* beskriver statsminister Erna Solberg prosessen der strategidokumentet ble til. Gjennom en strategikonferanse med 300 deltakere, i tillegg til en rekke workshops skapte grunnlaget for selve strategien (Departementene, 2019). Det er oppgavens tydelige oppfatning at myndighetene her bevisst har valgt å involvere så mange parter som mulig i prosessen med å utarbeide den nye strategien. Årsakene til dette kan være flere. En mulig forklaring kan være at myndighetene opplever å mangle kompetanse og oversikt over behovene i de ulike virksomhetene i Norge når det gjelder digital sikkerhet. En sekundæreffekt av dette vil være at sterke stemmer i enkelte virksomheter mulig ble satt i en posisjon til å påvirke strategidokumentet i en retning som var i deres interesse. Kan det eksempelvis være i virksomhetenes interesse at strategi og lovgrunnlag organiseres på en måte som gir virksomhetene selv mer makt over tiltakene og dermed økt handlefrihet?

Om vi legger Christensen et. al (2015) sine perspektiver for analyse av organisasjoner til grunn, kan vi forstå myndighetenes organisering av arbeidet med å utarbeide en ny strategi som en forhandlingsvariant snarere enn en hierarkisk variant innenfor det instrumentelle perspektivet (Christensen et al., 2015, 35). Myndighetene involverer et bredt spekter av interessenter i utarbeidelsen, og lar de ulike aktørene få medbestemmelse. Sluttproduktet eller selve strategien vil i så måte være et kompromiss basert på alle innspill i prosessen. Det er allikevel klart at myndighetene har det siste ordet i prosessen med å utarbeide denne strategien, og de involverte aktørenes innspill vil i så måte ikke nødvendigvis inkluderes i sluttproduktet. Vi forstår derfor at det også gjennom det hierarkiske perspektivet er slik at myndighetene benytter sin makt overfor virksomhetene for å oppnå en strategi som er best mulig, og at arbeidsprosessen med strategidokumentet i så måte kun er til slik at arbeidsgruppen kan oppnå sitt mål om å lage en god strategi for digital sikkerhet i Norge. Organiseringen av arbeidet med utarbeidelse av strategidokumenter for digital sikkerhet i Norge virker derfor som en prosess der både bred involvering og tydelig ledelse har vært viktige aspekter.

7.1.2 Myndighetenes prioriteringer

I dette kapitlet vil vi drøfte endringer i myndighetenes prioriteringer innen digital sikkerhet, basert på fire offentlige dokumenter utarbeidet av norske myndigheter: Nasjonal strategi for digital sikkerhet (2019), NOU 2015:13 Digital sårbarhet - sikkert samfunn, Meld. St. 38 (2016-2017) IKT -sikkerhet - Et felles ansvar, og Lov om nasjonal sikkerhet (sikkerhetsloven). Basert på analysene av de nevnte dokumentene, kan vi se at kjerneelementene i myndighetenes prioriteringer forblir relativt stabile over tid og at det er liten grad av endring. Eksempelvis ser vi at tverrsektorielt samarbeid, håndtering av digitale sikkerhetshendelser, digital sikkerhetskompetanse og beskyttelse av kritisk infrastruktur og samfunnsfunksjoner er vedvarende prioriteringer.

Selv om prioriteringene bærer lite preg av endring, ser vi at det er en økende vektlegging på samarbeid mellom offentlig og privat sektor for å håndtere digitale trusler. Dette er særlig tydelig i NOU 2015:13 og Meld. St. 38, hvor samarbeid mellom staten, næringslivet og enkeltpersoner fremheves som et sentralt element i å styrke nasjonal IKT-sikkerhet. Internasjonalt samarbeid har også fått en større betydning i de senere dokumentene. Selv om dette beskrives i både NOU 2015:13 og Meld. St. 38, er det nå blitt enda mer fremtredende i den nasjonale strategien for digital sikkerhet. En mulig forklaring på hvorfor prioriteringen fremdeles er relevant kan være at truslene blir stadig mer avanserte og komplekse. En slik utvikling av trusselbildet vil være utfordrende for én organisasjon eller sektor å håndtere alene. Videre kan et samarbeid bidra til å utveksle beste praksis og erfaringer mellom organisasjoner, og på den måten forbedre sikkerhetspraksisen på en mer generell basis. En tredje forklaring på hvorfor et styrket samarbeid er en relevant prioritering er at det kan bidra til å øke bevisstheten og forståelsen av cybersikkerhet blant andre aktører i samfunnet. En forutsetning for et godt samarbeid på tvers av sektorer og landegrenser er likevel aspektet ved informasjonsdeling. For at et samarbeid med fokus på digital sikkerhet skal styrke den nasjonale sikkerheten er det essensielt med en god informasjonsflyt. Imidlertid kan det være flere utfordringer knyttet til informasjonsdeling, blant annet frykten for å eksponere konfidensiell informasjon, sårbarheter eller personopplysninger. En god tilnærming til å håndtere nevnte utfordring kan være en balansert tilnærming til informasjonsdeling som hensyntar både sikkerhets- og personvernrisikoer.

Det fremkommer også fra analysen av NOU 2015:13 en anbefaling om etablering av et nasjonalt cybersikkerhetssenter. Anbefalingen i seg selv viser en tydelig endring i

myndighetenes fokus på å styrke nasjonal kapasitet for å respondere på digitale sikkerhetshendelser. Det er likevel ikke en endring i prioritering av tiltak da effektene som ønskes oppnådd kan vurderes til å være de samme. Etableringen av nasjonalt cybersikkerhetssenter viser at norske myndigheter ser behovet å styrke landets evne til å oppdage og håndtere digitale sikkerhetshendelser i et digitalisert samfunn. Normal Accident Theory (Perrow, 1999) peker på at komplekse systemer og organisasjoner er utsatt for uforutsette og uunngåelige hendelser, og det er begrenset hvor mye man kan gjøre for å forhindre slike hendelser. Teorien understreker at organisasjoner må være forberedt på å håndtere uforutsette hendelser og ha en beredskapsplan på plass. I denne sammenhengen kan et nasjonalt cybersikkerhetssenter være en måte å øke beredskapen og evnen til å håndtere digitale sikkerhetshendelser på en effektiv måte. Videre kan vi si at teorien om høypålitelige organisasjoner påpeker viktigheten av en høy grad av pålitelighet og sikkerhet over tid. Dette krever en organisasjonskultur som vektlegger læring og kontinuerlig forbedring, samt en evne til å håndtere uforutsette hendelser og å tilpasse seg nye omstendigheter (Weick & Sutcliffe, 2007). Ved å etablere et nasjonalt cybersikkerhetssenter kan dette bidra til å fremme en slik organisasjonskultur og evne til å håndtere digitale sikkerhetshendelser. Begge teoriene peker på ulike sider ved nasjonal håndtering av digitale sikkerhetshendelser. Beslutningen om å etablere et nasjonalt cybersikkerhetssenter var trolig basert på flere faktorer enn det som er nevnt. Samtidig er det nærliggende å tro at prioriteringen om å etablere dette er tuftet på en helhetlig tilnærming til et økt nasjonalt digitalt forsvar.

Et tredje område som har fått økende oppmerksomhet, er knyttet til kompetanse og ferdigheter innen digital sikkerhet. I *Nasjonal Strategi for Digital Sikkerhet* (2019) fremheves grunnleggende digitale ferdigheter og kompetanse som et nøkkelelement for å styrke samfunnets evne til å forebygge, oppdage og håndtere digitale trusler. Selv om dette fokusområdet har fått mer oppmerksomhet siden 2019, har det vært en vedvarende prioritet i dokumentene vi har undersøkt. Dette kan tyde på at man både ser verdien av et kompetanseløft i samfunnet, men det kan også bety at det er utfordrende å adressere dette på kort sikt. Vi ser at regjeringen tenderer til å prioritere følgende områder når det kommer til utvikling av kompetanse og ferdigheter: god grunn kompetanse, tilstrekkelig spesialistkompetanse, bevisstgjørende tiltak, digital sikkerhet som en del av IT-relevante utdanninger og muligheter for etter- og videreutdanning (Departementene, 2019).

For å illustrere dette, har Justis- og beredskapsdepartementet i samarbeid med Kunnskapsdepartementet utarbeidet en nasjonal strategi for digital sikkerhetskompetanse. Denne strategien danner grunnlaget for utvikling av kompetanse i tråd med samfunnets, arbeidslivets og individets behov (Departementene, 2019, s. 4).

Beskyttelse av kritisk infrastruktur og samfunnsfunksjoner er et fjerde område som fremkommer i de styrende dokumentene vi har undersøkt. Arbeidet med å sikre digitale tjenester og infrastruktur som samfunnet er avhengig av sees på som en absolutt nødvendighet i samtlige av dokumentene. Det foreligger en forventning i samfunnet om at samfunnskritiske funksjoner og tjenester er redundante og resiliente. Dette fører også til at myndighetene må utvikle og håndheve lover og forskrifter som sikrer at virksomheter og organisasjoner har passende sikkerhetstiltak på plass for å beskytte systemer og data mot angrep. Videre er det også viktig at myndighetene håndhever etterlevelse og straffer brudd på stilte sikkerhetskrav for å vise at de tar sitt ansvar på alvor og at manglende etterlevelse kan medføre konsekvenser.

Den nye lov om nasjonal sikkerhet (sikkerhetsloven), som trådte i kraft 1. juli 2018 gir et mer helhetlig juridisk rammeverk for både digitale og fysiske trusler rettet mot nasjonal sikkerhet. Det vi ser er at den nye loven har et økt fokus på informasjonssikring, tydeligere ansvarsfordeling mellom offentlige myndigheter, virksomheter og enkeltpersoner, samt etablering av tilsyns- og kontrollmekanismer. De observerte endringene reflekterer en økende bevissthet om kompleksiteten knyttet til digital sikkerhet, samt et ønske om å styrke nasjonal evne til å forebygge, oppdage og håndtere digitale trusler. Vi ser at norske myndigheter forsøker å gjøre dette gjennom et bredt spekter av tiltak – fra lovverk til samarbeid mellom offentlig-private aktører.

7.1.3 Målsettinger og krav

Dokumentene kan alle sies å stille krav til offentlige virksomheter gjennom formulering av mål som skal oppnås ved hjelp av tiltak som presenteres i dokumentene. I kronologisk rekkefølge så er Lysneutvalget, i denne oppgaven, det første dokumentet som anbefaler tiltak som bør innføres for å styrke det offentlige Norges digitale sikkerhet. Disse er videre raffinert i Melding til Stortinget nr. 38, og videre operasjonalisert gjennom *Nasjonal Strategi for Digital Sikkerhet*.

Problemforståelsen i de forskjellige dokumentene er i stor grad uten endring, som heller understreker en omforent forståelse av hvorfor det er viktig å styrke den digitale sikkerheten. I NOU 2015:13 så beskrives problemet som at det er manglende enhetlig tilnærming til digital sikkerhet, manglende samordning og utnyttelse av ressurser på tvers av virksomheter og sektorer. Dette kan føre til en forringelse av tillit til offentlige tjenester som leveres ved hjelp av digitale hjelpemidler. Det kan forstås som at det ikke er noen tvil om viktigheten av digital sikkerhet, og problemet handler ikke om å sette dette på agendaen eller avdekke hva god digital sikkerhet er, men heller å øke effektiviteten av det arbeidet som er gjort ved hjelp av koordinering og samordning av innsats.

Denne forståelsen bringes videre inn i Meld. St. 38 (2017) som beskriver manglende samarbeid mellom offentlige og private sektorer for beskyttelse av Norges digitale infrastruktur som en utfordring. Det er imidlertid et noe mer operativt fokus i Meld. St. 38 (2017) ved at det i problemforståelsen også adresserer svakheter i nasjonale IKT-systemer, og manglende bevissthet om IKT-sikkerhet i hele samfunnet som grunnlag for utforming av ny politisk tilnærming til digital sikkerhet. Denne forståelsen blir igjen videre operasjonalisert gjennom Nasjonal Strategi for Digital sikkerhet som er mer fokusert mot innsikt og forståelse for omfanget av digitale sårbarheter, og manglende evne til å håndtere sårbarheter og opprettholde funksjonalitet i kritiske infrastruktur for digitale tjenester. Alle disse problemforståelsene handler i bunn og grunn om det samme, som er å forstå sårbarhetene og adressere dem på en mer helhetlig måte ved hjelp av økt tverrsektorielt samarbeid og samordning. I ny Sikkerhetslov av 2019 så kan det forstås som at den samme årsaken er lagt til grunn for utarbeidelse av ny lovtekst. Loven skal ta høyde for økt globalisering og digitalisering, og man kan forstå implisitt i dette at økt kompleksitet i verdikjeder er en årsak. Ved å gjøre kravene mindre spesifikke, og legge ansvaret på virksomheten for å forstå hva som er forsvarlig sikkerhetsnivå, så kan man legge til grunn at hurtig utvikling av trusselbildet og stadig utvikling av ny teknologi blir håndtert innenfor lovteksten. Dette fordrer økt tverrsektorielt samarbeid og enhetlig tilnærming til sikkerhet. Hovedtendensen i problemforståelsen kan derfor sees på som en dreining fra sikring av den enkelte virksomhets digitale systemer til å se det i en større sammenheng som startet ved Lysneutvalget, men som ble videre raffinert og operasjonalisert i de påfølgende dokumentene, men uten vesentlig avvik fra den opprinnelige forståelsen av problemet.

Hvis vi går inn på tiltakene som er foreslått for å bidra til å løse problemene som er beskrevet over, så er det tydeligere endringer som har forekommet etter hvert som dokumentene har blitt utviklet. Det er imidlertid viktig å huske på hvem som er målgruppen for tiltakene, fordi dette kan ha påvirkning på formuleringer. I Lysneutvalget er tiltakene laget som anbefalinger til regjeringen for hvordan de skal politisk tilnærme seg digital sikkerhet, mens stortingsmeldingen redegjør for hvordan regjeringen har bestemt seg for å tilnærme seg digital sikkerhet, og den nasjonale strategien er resultatet av dette som skal sørge for at målene nås. Sikkerhetsloven, som er relevant, men ligger litt på siden, understøtter dette ved å sette et økt press på underlagte virksomheter for å følge opp strategien.

Tiltakene er utformet som mål eller effekter som skal oppnås. Det innebærer en forklaring av *hva* og *hvorfor,* men ikke *hvordan.* Dette bidrar trolig til å holde tiltakene relevante over tid. Ved for konkrete beskrivelser av hvordan et tiltak skal gjennomføres, vil det fort bli snevert og vanskelig å gjøre relevant for forskjellige virksomheter og organisasjoner med bakgrunn i størrelse, modenhet, kompleksitet, infrastruktur og valgt teknologi. Det vil også være lite hensiktsmessig å forklare hvordan et tiltak skal løses, som kanskje er riktig i det øyeblikket tiltaket ble skrevet, men som bare seks måneder senere kan bli utdatert som følge av endringer i trusselbildet eller utviklingen av teknologi. I løpet av bare de siste månedene, når denne oppgaven skrives, har kunstig intelligens, gjennom eksempelvis ChatGPT, vist at teknologiske hjelpemidler, og kraften i disse, kan endres drastisk i løpet av kort tid.

I Lysneutvalgets utredning representerer tiltakene i alle dokumentene en dreining mot Perrows Normal Accident Theory (1999). For det første så er fokuset på det forbedring av det tverrsektorielle arbeidet med digital sikkerhet i tråd med Perrows teori hvor han påstår at fordi enkeltkomponentene, i dette tilfellet både de tekniske anleggene og systemene i virksomhetene, men også samhandling mellom virksomhetene, er satt sammen i komplekse systemer så vil konsekvensene være større enn hvis kun enkeltkomponenter feiler. Det andre argumentet for at dokumentet ser ut til å sammenfalle med Perrows teori er fokuset på reduksjon av både sannsynlighet og konsekvenser. Ved å fokusere utelukkende på sannsynlighet, så vil man kunne argumentere for at det rådende synet hadde vært at ulykker og uønskede hendelser ville vært mulig å forhindre fullstendig. Fokuset på reduksjon av konsekvenser er imidlertid et sterkere argument for at myndighetene heller har et syn som innebærer at det ikke vil være mulig å redusere sannsynligheten fullstendig.

Det er imidlertid ikke slik at målet ikke kan være en reduksjon av all risiko for ulykker eller uønskede hendelser. Dog ville det trolig vært et urealistisk mål all den tid digital sikkerhet ikke kun må ta høyde for tekniske feil eller menneskelig svikt, men også ondsinnede trusselaktører som stadig utvikler nye metoder, taktikker og teknikker for å utnytte teknologi til å nå sine mål. Den økende forekomsten av eksempelvis cyberangrep beskrevet tidligere i oppgaven bidrar til at teorien om at det vil være mulig å fjerne all risiko, virker fjern. I de ulike dokumentene som er analysert i oppgaven fremkommer det ingen større skift i denne forståelsen. Dette argumenterer for at prioriteringene, som i mer eller mindre grad har vært uendret gjennom tidsperioden for de analyserte dokumentenes opprinnelse, er fortsatt relevante.

En annen endring som er interessant i dokumentene som er analysert, er mengden tiltak som er produsert. Det har skjedd en gradvis reduksjon i antall tiltak i hvert av dokumentene etter hvert som de er utviklet. Som regel vil overordnede tiltak eller mål, operasjonaliseres gjennom å splitte de opp i flere mer konkrete og håndterbare oppgaver eller tiltak, som skal bidra til å sørge for at man klarer å oppnå målene. I de analyserte dokumentene, som vi allerede har etablert som pågående raffinering og operasjonalisering av det foregående dokument med opphav i Lysneutvalgets, så har imidlertid det motsatte skjedd. En årsak til dette kan være at digital sikkerhet er komplisert og vanskelig, og kompetanse er vanskelig å finne. En annen årsak kan være at det har vært en læringskurve også for Justis- og beredskapsdepartementet, som har ført til en mer konkret prioritering av innsats som følge av et ønske om mest mulig effekt per enhet innsats.

7.1.4 Oppsummering

Kapittelet har vurdert hvilke hovedtendenser man kan se i de utvalgte dokumentene knyttet til myndighetenes prioriteringer innen digital sikkerhet. Grunnforståelsen er at utfordringene var i stor grad kjent, selv om man ikke nødvendigvis hadde omforent forståelse av sårbarhetsbildet. Utviklingen har vært utløst av en økende trussel i kombinasjon med økt sårbarhet som følge av mer komplekse verdikjeder. Dokumentene understreker at prioriteringene som er satt ikke kan løses med en silobasert tilnærming, men at ønskede mål kun er oppnåelig med enhetlig tilnærming på tvers av sektorer.

I det organisatoriske perspektivet så er digital sikkerhetskultur et gjennomgående nedprioritert område, til tross for at mangel på kompetanse er identifisert som en utfordring. I

tillegg så har det skjedd endringer i rammene for samordning av digital sikkerhet i sivil sektor ved at Justis- og beredskapsdepartementet har fått et bredere ansvar, samtidig som de enkelte virksomheter har fått et større ansvar for risikovurdering og egensikring.

Når det gjelder myndighetenes prioriteringer så ser vi at det er liten grad av endring i prioriteringer. Det er imidlertid enkelte elementer som er tillagt en økende vektlegging, slik som kompetanse og ferdigheter, samarbeid mellom offentlig og sivil sektor, og beskyttelse av kritisk infrastruktur og samfunnsfunksjoner.

Dokumentenes krav og målsettinger er heller ikke underlagt store endringer, men det er en påviselig dreining som har skjedd fra NOU 2015:13 via Meld. St. 38 til *Nasjonal Strategi for Digital Sikkerhet* og ny sikkerhetslov av 2019, ved at antall tiltak som skal gjennomføres er redusert, og konkretisert i noen grad. En årsak til dette kan være at omfanget er for stort, eller at det var nødvendig med økt konkretisering for å skape forståelse blant virksomhetene som skal gjennomføre tiltakene.

Oppsummert ser vi at prioriteringene fra Lysneutvalget frem til *Nasjonal Strategi for Digital Sikkerhet* har holdt seg noenlunde like, og er fortsatt relevante. Det er imidlertid et tankekors at det ikke har vært større utvikling på området, og at anbefalingene fra 2015 er fortsatt gjeldende mange år senere.

7.2 Hvilke utfordringer står Justis- og beredskapsdepartementet ovenfor når det gjelder å sette prioriteringene ut i praksis?

Hovedtendensene knyttet til myndighetenes prioriteringer innen digital sikkerhet er diskutert i foregående kapittel. Disse prioriteringene har ikke endret seg nevneverdig fra Lysneutvalget til *Nasjonal Strategi for Digital Sikkerhet*, sett bort ifra at det har foregått en videre operasjonalisering av de anbefalte løsningene/tiltakene. Det kan være et tegn på et mer dyptgående problem som fører til at når løsningene skal settes til livs, og gjennomføres ute i virksomhetene, så er det noen mekanismer som fører til at dette arbeidet stopper helt eller delvis opp. Riksrevisjonen publiserte i en rapport om Justis- og beredskapsdepartementets samordning av digital sikkerhet i sivil sektor med nedslående konklusjon. Arbeidet med samordning under ansvar og ledelse av Justis- og beredskapsdepartementet ble omtalt som kritikkverdig. Manglende samordning kan føre til overlapp mellom ansvarsområder og blindsoner i regulering, oversikter og oppfølging. Effektiv samordning kan på sin side

redusere ressursbruken og forbedre effekten av tiltak og virkemidler (Trondal, 2017). I dette delkapittelet skal vi drøfte hvilke utfordringer som kan være gjeldende for Justis- og beredskapsdepartementet i et instrumentelt perspektiv basert på det analytiske rammeverket til Nesheim m.fl. fra 2019 for å sørge for at arbeidet med digital sikkerhet blir fulgt opp og gjennomført av virksomheter i sivil sektor.

7.2.1 Oppgaver og avhengigheter

Ifølge Nesheim et al (2019) så er det en grunnleggende forutsetning for god samordning at man forstår hva det tverrsektorielle samarbeidet skal håndtere. Dette innebærer at utforming av struktur og virkemidler for samordning bør tilpasses trekk ved oppgavene som skal løses. Inter-organisatorisk samarbeid, som digital sikkerhet krever, er ofte forbundet med gjenstridige problemer. Et gjenstridig problem er problemer som er komplekse, varige og ikke kan løses "en gang for alle"; de spenner typisk over organisatoriske grenser, forvaltningsområder og hierarkiske nivåer (Nesheim et al., 2019, s. 29).

I det analytiske rammeverket til Nesheim et al (2019) så er det viktig å avklare hvorvidt oppgavene handler om myndighetsutøvelse eller tjenesteyting. For digital sikkerhet kan dette være et vrient spørsmål å svare på. Dette har sammenheng med at digital sikkerhet handler om å sikre en sekundær prosess som støtter primære prosesser. Digitale hjelpemidler, eller IKT-ressurser, er noe som skal effektivisere tjenesteyting. Offentlige virksomheter har sitt utspring i politiske visjoner som er operasjonalisert til faglig, operativ oppgaveforståelse (Bastøe et al., 2002). Digitalisering av tjenester er det som har ført til et økt behov for digital sikkerhet, og handler om å sikre at tjenestene kan leveres på tross av at uønskede digitale hendelser oppstår, som for eksempel hackerangrep. Man kan derfor argumentere for at digital sikkerhet hverken treffer myndighetsutøvelse eller tjenesteyting i den rette forstand, men er mer og mer blitt en grunnleggende forutsetning for at virksomhetene kan levere tjenester. For Justis- og beredskapsdepartementet så faller dette imidlertid under myndighetsutøvelse og kontroll, ettersom de har ansvar for å samordne innsatsen på tvers av etater og sektorer. Dette bør legges til grunn for hvordan de velger å organisere seg for utøvelse av samordningsansvaret.

Når det gjelder nærhet til Justis- og beredskapsdepartementets kjernevirksomhet så kan man anta at det ligger relativt nært. Formålet til Justis- og beredskapsdepartementet er å legge føringer for hvordan virksomheter skal arbeide med sikkerhet. Et eksempel på dette er

arbeidet med å forebygge terrorangrep. Det burde i utgangspunktet tale for at de på forhånd skal være rigget til å ivareta ansvaret på en god måte. Likevel er arbeidet som er gjort karakterisert av Riksrevisjonen (2022/2023) som kritikkverdig. Dette har i hovedsak bakgrunn i at svak samordning av roller, ansvar og krav gjør arbeidet med forebyggende digital sikkerhet krevende for virksomhetene. Dette forklares med at sentrale samordningsarenaer er lite forpliktende for deltakerne og bidrar i varierende grad til samordning, tilsynsmyndighetene er lite samordnet og det eksisterer ikke en felles tilsynsmetodikk, og brukere opplever det krevende å holde oversikt over regelverk og veiledning. Dette er kritikk som er rettet direkte mot Justis- og beredskapsdepartementet, og fremstår som overraskende all den tid oppgavene knyttet til samordning antas å ligge så nært kjernevirksomheten. På den annen side så er Justis- og beredskapsdepartementet et departement med et vidt ansvarsområde, og det er sannsynlig at det er interne spenninger knyttet til viktigheten av samordning av andre fagområder innenfor sikkerhet og beredskap som kan føre til en bevisst eller ubevisst nedprioritering av samordningen av digital sikkerhet.

En annen utfordring som Justis- og beredskapsdepartementet står ovenfor, er spennet i oppgaver knyttet til ulike organisatoriske nivåer. Digital sikkerhet er viktig for omtrent alle offentlige virksomheter, og kan kun løses i samspillet mellom mennesker, prosesser og teknologi. Det innebærer i en enkelt organisasjon at man har nødvendige styringsmekanismer som ivaretar digital sikkerhet på et teknisk nivå hvor infrastrukturen er robust, at menneskene er informerte og kompetente, og kan utgjøre et ledd i forsvaret mot digitale trusler. I tillegg må virksomhetsprosessene være utviklet slik at digital sikkerhet ivaretas i utførelsen av deres primære oppgaver. Oppsummert så er alle organisatoriske nivåer i en enkelt virksomhet involvert i styrking av digital sikkerhet, og dette må videre aggregeres innenfor de enkelte sektorer, og deretter settes sammen i et helhetlig perspektiv. Riksrevisjonen (2023) har pekt på Justis- og beredskapsdepartementets manglende evne til å levere god nok informasjon om den nasjonale digitale sikkerhetstilstanden. Man kan argumentere for at et manglende bilde på sikkerhetstilstanden vanskeliggjør samordningen av digital sikkerhet ved at man muliggjør faren for økt ressursbruk og uteblivende effekt av tverrsektorielle tiltak og virkemidler som er forsøkt realisert.

7.2.2 Distanse mellom organisasjoner

I tråd med det analytiske rammeverket skal vi vurdere distansen mellom organisasjoner. Dette gjøres i fire dimensjoner; 1) geografisk distanse, 2) kognitiv distanse, 3) strukturell distanse

og 4) maktdistanse. Teorien tilsier at desto større distanse det er innen disse fire dimensjonene av distanse, desto vanskeligere blir det å få til god samordning.

I den første dimensjonen, geografisk distanse, så kan man anta at det ligger elementer til grunn her som kan argumentere for at geografisk distanse er en faktor som vanskeliggjør Justis- og beredskapsdepartementets samordningsansvar. For eksempel er hovedkontoret til Direktoratet for samfunnssikkerhet og beredskap (DSB) plassert i Tønsberg, mens departementet hører til i Oslo. Imidlertid så er det bare et eksempel, men digital sikkerhet er, som tidligere beskrevet, et tema som påvirker nært sagt alle offentlige virksomheter i Norge, og geografisk distanse vil påvirke mulighetene for å gjennomføre både ansikt-til-ansikt dialog og veiledning. Det er likevel vanskelig å tillegge dette særlig mye vekt som en hovedutfordring for Justis- og beredskapsdepartementet i arbeidet med samordning, da det trolig er andre utfordringer som i større grad vanskeliggjør arbeidet. Dette har bakgrunn i at det finnes digitale hjelpemidler som kan kutte ned den geografiske avstanden, men et kanskje enda sterkere argument er at omfanget av involverte er så stort, at gjennomføring av aktiviteter på fysisk lokasjon ikke kan imøtekomme antallet deltaker i den grad det er nødvendig og dermed mister mye av sin verdi.

Den andre dimensjonen, kognitiv distanse, handler om forskjeller i perspektiv og kunnskapsbase. Nesheim et al (2019) påpeker at økende kognitiv distanse påvirker evne til å forstå hverandre og samordne aktiviteter negativt. Dette er et interessant tema, fordi digital sikkerhet er både spesifikt, men også generelt. Det kan være store forskjeller i infrastrukturen til to forskjellige virksomheter, men prinsippene for sikring er i utgangspunktet de samme. Fordi digital sikkerhet er en sekundær prosess, så bør perspektivene blant aktørene i utgangspunktet ikke ha store forskjeller fra hverandre. Til syvende og sist bør alle virksomheter være interessert i å sikre sin evne til å fortsatt levere tjenester på tross av uønskede digitale hendelser. Den store forskjellen her kan imidlertid handle om kunnskapsbasen de ulike aktørene har å spille på. Det er allerede etablert at Norge mangler digital sikkerhetskompetanse, og har iverksatt strategier og tiltak for å bøte på dette. Dette kan spille seg ut i de ulike forståelse for oppgavene de er satt til å løse, og forsterke utfordringene. Dette er spesielt interessant sett i sammenheng med at både ny *Sikkerhetslov* og *Nasjonal Strategi for Digital Sikkerhet* legger opp til et større ansvar for virksomhetene selv å besørge risiko- og sårbarhetsvurderinger, samt egensikring.

Når det gjelder strukturell distanse så handler det om at ulike aktører kan ha ulike formelle trekk ved organisasjonen, som struktur, størrelse, beslutningsprosesser og ansvarsforhold. Det kan bidra til å skape utfordringer med hensyn til koordinering av oppgaver som må løses i fellesskap. På grunn av omfanget av sektorer som er underlagt Justis- og beredskapsdepartementets samordning, så er det rimelig å anta at det vil eksistere både større og mindre strukturelle avstander mellom aktørene og Justis- og beredskapsdepartementet. Spørsmålet i dette tilfellet er hvorvidt det egentlig trenger å ha noe å si. Et eksempel brukt av Nesheim et al (2019) er forskjellen mellom Politiet og Skatteetaten, hvor Politiet er vant med å "bygge straffesaker", som stiller andre krav til bevisførsel og prosedyre, enn "forvaltningssporet" som kanskje i større grad preger Skatteetaten. Fordi digital sikkerhet ikke er rettet mot verken Politiet eller Skatteetatens primærfunksjoner, så kan det være at strukturell distanse, selv om den er stor, ikke trenger å ha betydning for samordning. På den annen side, så snart det involveres beslutninger som skal tas, eller løsninger som skal utformes, vil man kunne anta at det vil være forskjellige måter å komme frem til disse på. Likevel, det er i hovedsak ikke den operative politimannen eller skattejuristen som er gitt hovedansvaret for digital sikkerhet i sine etater, men snarere fagressurser innen IT. Disse vil man i større grad kunne anta snakker samme språk selv om de er ansatt i forskjellige etater. Det er denne oppgavens oppfatning at samordningen likevel gjennomføres på en hierarkisk måte, hvor Justis- og beredskapsdepartementet kan gi veiledning og bidra med innspill for å redusere denne avstanden på tvers av sektorer.

Den siste dimensjonen innen distanse handler om makt. Asymmetri og maktforskjeller mellom de involverte aktørene kan bidra til begrensninger når det gjelder handlingsrom og beslutningstaking i situasjoner hvor det eksisterer ulike interesser og mål. Dette kan komme til uttrykk gjennom utfordringer knyttet til aktørenes forskjellige forhold til hensikter, mandater, ansvarsområder, og insentiver, og konkurranse om begrensede ressurser (Nesheim et al., 2019). Forskjeller i makt, herunder formell autoritet, ressurskontroll og diskursiv legitimitet, kan bidra til å vanskeliggjøre arbeidet med samordning for Justis- og beredskapsdepartementet. Antakeligvis er utfordringen todelt. I første instans så kan det være ulike aktører som motsetter seg å være underlagt Justis- og beredskapsdepartementets samordning. Dette kan ha bakgrunn i at man ikke ønsker å dele informasjon om sikkerhetstilstand, eller politisk motivert konkurranse, hvor en aktør har interesse av at Justis- og beredskapsdepartementet ikke oppnår de ønskede resultatene. Det andre aspektet kan være at Justis- og beredskapsdepartementet ikke evner å få de enkelte aktørene til å prioritere

arbeidet med digital sikkerhet. Dette aspektet kan forsterkes ved mangel på makt, hvor makt forstås som Justis- og beredskapsdepartementets evne til å påtvinge en aktør en spesifikk handling eller prioritet. De er i utgangspunktet tildelt en slik formell makt gjennom tilsynsmyndigheten, men som Riksrevisjonen påpeker i sin rapport så evner de ikke å utnytte det (Riksrevisjonen, 2023). Riksrevisjonen (2023, s.18) skriver:

> "Tilsyn er et sentralt virkemiddel som Justis- og beredskapsdepartementet og øvrige myndigheter kan bruke til å kontrollere at regelverket på det digitale sikkerhetsområdet implementeres og overholdes. Tilsyn skal bidra til å forbedre arbeidet med digital sikkerhet i virksomhetene. For myndighetene er tilsynsrapportene også en viktig kilde til innsikt i arbeidet på området – i hver enkelt sektor og i samfunnet som helhet. Mangelfull tilsynsvirksomhet kan føre til at den digitale sikkerheten får for lite oppmerksomhet i virksomheter og departementer. Dette kan svekke den digitale sikkerheten i samfunnet. Undersøkelsen viser at det gjennomføres forholdsvis få tilsyn med digital sikkerhet som tema."

Vi vil derfor argumentere for at et av de viktigste grepene Justis- og beredskapsdepartementet kan gjennomføre for å øke tempoet i arbeidet med digital sikkerhet blant involverte virksomheter, er å øke tilsynsaktiviteten, samt utvikle en felles tilsynsmetodikk. Dette handler i utgangspunktet mer om å utnytte maktforskjellen til sin fordel, fremfor å redusere maktavstanden slik som teorien i utgangspunktet forfekter. Nesheim et al. (2019) har et annet syn på det og argumenterer for at asymmetri i maktforholdet ikke nødvendigvis trenger å være til hinder for god samordning. Det er heller viktig å etablere rammer og styringsprosesser som tar høyde for ubalansen i makt. Dette kan oppnås ved å benytte seg av den tilsynsmyndigheten de er tillagt.

7.2.3 Intra-organisatoriske tiltak

Intra-organisatoriske tiltak handler om de grep som tas internt i den enkelte organisasjon som er med i det tverrsektorielle samarbeidet. Med andre ord, hvordan en organisasjon ruster seg for å delta i et samarbeid, og for at det samarbeidet skal lykkes. Det er flere motiver som kan ligge til grunn for at en virksomhet ønsker å delta i et tverrsektorielt samarbeid. Dette kan være økt kunnskap, utveksling av informasjon, samordning av offentlige tiltak og offentlige tjenester. For digital sikkerhet, som tidligere diskutert, så er dette et område som treffer de aller fleste virksomheter, og økt risiko knyttet til kompleksitet i verdikjeder fører til at det

ikke vil være praktisk mulig å sørge for et forsvarlig sikkerhetsnivå uten at arbeid samordnes på tvers av sektorer. En forutsetning for denne samordningen er hvordan de enkelte deltakerne organiserer seg internt for å bidra til at oppgavene og tiltakene løses. Vi ser nærmere på Justis- og beredskapsdepartementet.

I henhold til det analytiske rammeverket til Nesheim et al. (2019) så er det viktig å organisere seg internt for å få til samarbeid, og at man etablerer en strategi som bør være både forstått og kommunisert i etaten. Det har Justis- og beredskapsdepartementet etablert og publisert gjennom *Nasjonal Strategi for Digital Sikkerhet*. Dette er et viktig tiltak for å sørge for at både en selv og andre deltakende aktører vet hva som er forventet og hva som ønskes oppnådd. For Justis- og beredskapsdepartementet som har en ledende rolle i form av samordningsansvar, med en rekke underlagte enheter, vil det være spesielt viktig å vise støtte fra toppledernivået, gi tydelig informasjon, og bidra med klare styringssignaler. Dette vil trolig bidra til at Justis- og beredskapsdepartementet med underlagte enheter kan møte andre deltakende aktører på en tilnærmet lik måte, med like forventninger, som vil redusere risikoen for motstridende beskjeder og forståelser. Hvis Justis- og beredskapsdepartementet har fortolket en oppgave på en måte, mens Norsk Sikkerhetsmyndighet har tolket det på en annen måte, kan det føre til økt frustrasjon og motstand blant andre virksomheter som er gitt oppdrag om å gjennomføre oppgavene – rent praktisk.

Selv med god intern kommunikasjon, organisering og strategi, så kan man likevel oppleve utfordringer hvis man ikke identifiserer og adresserer et punkt til. Innslag av interne spenninger kan bidra til at arbeidet med samordningsoppgaver stopper helt eller delvis opp. Etter terrorhendelsen 22. juli ble det fattet vedtak om tiltak som skulle gjennomføres under ledelse av Justis- og beredskapsdepartementet. To avdelinger hadde imidlertid en pågående intern konflikt, som hadde vart i minst ti år, som førte til at arbeidet ble kraftig forsinket (Johnsen & Ertesvåg, 2014). Interne spenninger kan representere en stor utfordring for Justis- og beredskapsdepartementet. Basert på denne oppgavens datainnsamling har vi ikke grunnlag for å si at slike spenninger eksisterer i arbeidet med samordning av digital sikkerhet i sivil sektor. Riksrevisjonens rapport (2023), som er en nøye gjennomgang av Justis- og beredskapsdepartementets arbeid med samordning, peker heller ikke på store utfordringer knyttet til dette. Det er derfor rimelig å anta at Justis- og beredskapsdepartementet er relativt godt organisert for å ivareta sitt ansvar.

7.2.4 Inter-organisatoriske tiltak

Innen organisasjonsfaget er en sentral lærdom at utforming av struktur og samordningsmekanismer bør tilpasses egenskapene ved oppgavene som skal utføres (Nesheim et al., 2019, s. 33). For eksempel, hvis oppgavene er forutsigbare og forbindelsen mellom virkemidler og måloppnåelse er tydelig, anbefales detaljert planlegging og standardiserte arbeidsprosesser. Derimot, når det foreligger betydelig usikkerhet relatert til kunder, marked og oppgaveløsning, er tendensen å anvende organisasjonsstrukturer med lavere grad av byråkrati. Dersom organisasjonen arbeider med særegne oppgaver som har et tydelig start- og sluttpunkt, anbefales det å integrere prosjektenheter i strukturen (Nesheim et al., 2019, s. 33). Når Justis- og beredskapsdepartementet skal sette prioriteringen om tverrsektorielt samarbeid ut i praksis, står de overfor en rekke utfordringer. En av de største utfordringene kan være koordineringen av arbeidet på tvers av ulike sektorer. Oppgaven om å etablere et tverrsektorielt samarbeid kan vurderes til å være forutsigbar, men hvordan man bør gå frem for å oppnå dette kan være noe utydelig. Dette er en kompleks oppgave, da det gjerne er flere ulike aktører som skal samarbeide og som kan ha ulike interesser, prioriteringer og arbeidsmetoder. Sett i lys av teorien til Nesheim (2019) kan en prosjektbasert tilnærming til denne oppgaven være hensiktsmessig ettersom den berører flere organisasjoner og må håndteres gjennom et inter-organisatorisk samarbeid. Dette er en samarbeidsform som i offentlig sektor er forbundet med gjenstridige problemer. Ifølge Rittel og Webber (1973) kan gjenstridige problemer være komplekse, varige, kan ikke løses "en gang for alle" og de påvirker flere organisasjoner, forvaltningsområder og hierarkiske nivåer (Nesheim et al., 2019, s. 33).

Et effektivt samarbeid med andre offentlige instanser, privat sektor og internasjonale aktører vil være avgjørende for å lykkes med en sterk digital sikkerhet på et nasjonalt nivå. Dette krever klare ansvarsforhold, tillit og god kommunikasjon. Riksrevisjonens undersøkelse av Justis- og beredskapsdepartementets arbeid med digital sikkerhet konkluderer blant annet med at det er for svak samordning av roller, ansvar og krav, noe som gjør arbeidet med digital sikkerhet krevende (Riksrevisjonen, 2023, s. 8). Et viktig poeng å få fram er at ulike sektorer gjerne har ulike typer oppgaver. I offentlig sektor kan det trekkes et skille mellom oppgaver som omhandler kontroll og myndighetsutøvelse, og tjenesteyting i ulik form. I privat sektor vil derimot de fleste oppgavene være knyttet til tjenesteyting på en eller annen måte som omhandler å fremskaffe "goder" for andre virksomheter og innbyggere (Nesheim et al., 2019, s. 33).

En potensiell utfordring i samarbeidet mellom offentlige og private virksomheter er etablering av tillit, noe som kan være en kritisk faktor for et effektivt samarbeid, sikring av informasjonsdeling og ressursutnyttelse til fellesskapets beste. I dette tilfellet vil styringsmekanismer som formalisering og tillit spille en viktig rolle for samarbeidet. Formalisering innebærer å etablere formelle regler, prosedyrer og kontrakter for å koordinere aktiviteter mellom de ulike aktørene. Dette kan bidra til å redusere usikkerhet og friksjon. Videre vil det kunne skape klarhet rundt roller, ansvar og forventninger hos de involverte partene. Formalisering kan også bidra med å adressere potensielle interessekonflikter, ved å definere felles mål og retningslinjer som skal følges. Tillit derimot, bygger på gjensidig forståelse, respekt og troen på at andre aktører vil handle i samsvar med fellesskapets interesser. Gjennom transparent kommunikasjon, informasjonsdeling og dialog vil tillit kunne etableres. Samarbeid basert på tillit reduserer ofte behovet for omfattende formalisering og kontroll, samtidig som det fremmer utviklingen av "taus kunnskap" som kan gjøre det lettere å håndtere forhold som er utfordrende å formalisere (Nesheim et al., 2019, s. 44). Det er derfor viktig å finne en god balanse mellom formalisering og tillit i samarbeidet mellom offentlige og private virksomheter. En for sterk formalisering kan være et hinder for fleksibilitet og innovasjon, mens et for tillitsbasert samarbeid kan føre til manglende kontroll og ansvarliggjøring, noe som Justis- og beredskapsdepartementet har blitt kritisert for (Riksrevisjonen, 2023, s. 8). Å etablere et effektivt samarbeid krever derfor en kombinasjon av både formelle mekanismer og tillitsbyggende tiltak som sikrer at alle parters interesser ivaretas på en hensiktsmessig måte.

Iverksettelse og arbeid med tiltak krever ledelse, ifølge Rørvik (2007) er ledelse direkte og dialogbasert påvirkning av involverte aktører (Nesheim et al., 2019, s. 44). Innenfor en organisasjon baseres ledelse på et hierarkisk forhold mellom ledere og medarbeidere. Når tiltak derimot krever omfattende samordning mellom organisasjoner og sektorer, opererer man i en helt annen kontekst, med andre betingelser for utøvelse av ledelse (Nesheim et al., 2019, s. 44).

> "Sett fra deltakernes side vil man forholde seg både til a) egen moderorganisasjon og dens prioriteringer og målsetninger, og til b) en aktørkonstellasjon, hvor en aktør eventuelt kan ha en formell koordineringsrolle. Når man utvikler noe nytt i samarbeid mellom organisasjoner er det viktig å utøve endringsledelse" (jf. Sarapuu, Lægreid, Randma-Liiv & Rykkja, 2014).

Det vil være avgjørende å kommunisere strategi og tiltak på en god måte for å sikre at man setter riktig retning for de involverte aktørene. Stensaker og Haueng (2016) påpeker at det sentrale i denne formidlingen er å skape en tydelig retning og en felles overordnet målsetting (Nesheim et al., 2019, s. 45). For Justis- og beredskapsdepartementets del vil det å skape et samspill mellom det innholdsmessige og prosessuelle kunne være utfordrende i inter-organisatoriske relasjoner, og det nettopp det som kommer til syne i Riksrevisjonens kritikk av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.

Innen arbeidet med samordning av arbeidet med digital sikkerhet, er Nasjonalt Cybersikkerhetssenter (NCSC) et eksempel på et inter-organisatorisk tiltak som ble etablert i 2019 (NSM, 2023). Senteret skal ivareta arbeidet med nasjonalt og internasjonalt samarbeid med deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet (NSM, 2023). Vi kan se for oss en rekke utfordringer knyttet til flere av de nevnte utfordringene med inter-organisatorisk samarbeid mellom norske virksomheter og NCSC. En mulig utfordring er dette som handler om balansen mellom tillit og formalisering. Myndighetene vil mulig legge opp til lovpålagt rapportering av digitale hendelser i fremtiden, som antydet i lovforslaget til ny lov om digital sikkerhet (Regjeringen, 2023). I så måte er man avhengig av en etablert rapporteringskultur som har et tilstrekkelig nivå av tillit mellom rapporterende virksomhet og NSM. Dersom virksomheter opplever å bli hengt ut, anmeldt for manglende systemer for å håndtere digitale angrep eller på andre måter oppleve svekket tillit mellom seg selv og NSM, vil senterets funksjon være truet. Et tillitsbasert forhold mellom virksomhetene og NCSC virker derfor å være viktig for å oppnå den ønskede hensikten, nemlig å effektivt begrense risiko knyttet til digitale angrep på norske virksomheter.

8 Avslutning

8.1 Konklusjon

Oppgaven har hatt til hensikt å besvare følgende problemstilling: "**Hvilke hovedtendenser fremkommer i styrende dokumenter for offentlige myndigheters prioriteringer innen digital sikkerhet og hvilke utfordringer står de overfor når det gjelder å sette disse prioriteringene ut i praksis?**". Vi har belyst dette ved å analysere fire utvalgte dokumenter som omtaler digital sikkerhet produsert i perioden 2015 til 2019, for å se om det har vært et skifte i prioriteringer. Våre funn knyttet til prioriteringer viser at sikkerhetskultur er et gjennomgående nedprioritert område. Dette stiller vi oss undrende til, ettersom en sterk sikkerhetskultur kan være en katalysator for økt digital sikkerhet. Mangel på kompetanse er identifisert som en utfordring, og den prioriteringen har vedvart i alle dokumentene som er undersøkt. Fokuset på samordning har i perioden som er undersøkt blitt satt på agendaen, og legger grunnlaget for å kunne oppnå det nivået av digital sikkerhet som befolkningen forventer.

Analysene som er gjennomført har vist at det i utgangspunktet har vært mindre endringer i prioriteringene, men heller enkelte elementer som er vektet forskjellig fra dokument til dokument. Vår forståelse er at dokumentene har vært en videre raffinering og operasjonalisering av foregående dokument. Dette vises videre gjennom reduksjonen av antall tiltak som hvert av dokumentene presenterer. Dette kan ha sammenheng med at det har vært en dreining i ansvaret som pålegges virksomhetene for å sikre seg selv digitalt. Disse to endringene sammen kan være resultat av mangelen på kompetanse som i noen grad har fått økt vektlegging etterhvert som dokumentene har blitt produsert. Prioriteringene i perioden har i liten grad vært offer for store endringer. Det kan være bevis på relevans, men også et symptom på manglende fremdrift i arbeidet med styrking av digital sikkerhet.

Videre har oppgaven søkt å belyse hvilke utfordringer Justis- og beredskapsdepartementet som ansvarlig for samordning av digital sikkerhet i sivil sektor står ovenfor når disse prioritetene skal settes ut i praksis. Vi har valgt å se nærmere på dette i et instrumentelt perspektiv i en organisasjonsfaglig kontekst. Vi har basert våre diskusjoner om temaet på et analytisk rammeverk for tverretatlig samarbeid knyttet til gjenstridige problemer. Digital sikkerhet er et gjenstridig problem fordi det ikke kan løses permanent, men trenger

kontinuerlig oppfølging og utvikling for å holde tritt med truslene mot grunnleggende nasjonale funksjoner.

Justis- og beredskapsdepartementet møter blant annet på organisatoriske utfordringer når det kommer til digital sikkerhet. Samspillet mellom mennesker, prosesser og teknologi er utfordrende å ivareta, spesielt når det er et stort antall virksomheter fra offentlig og privat sektor som blir involvert. Manglende roller, ansvar og krav bidrar til svak samordning og vanskeliggjør arbeidet med forebyggende digital sikkerhet. Riksrevisjonen (2023) har videre kritisert departementet for manglende evne til å gi et klart bilde av nasjonal digital sikkerhetstilstand, noe som også vanskeliggjør en god samordning.

Oppgaven har videre diskutert fenomenet distanse mellom organisasjoner, og pekt på at den geografiske avstanden mellom virksomhetene JD regulerer er stor, men at dette ikke er en avgjørende faktor grunnet tilgang på digitale hjelpemidler og digital sikkerhet sin naturlige funksjon som sekundærfunksjon i virksomhetene. Det at digital sikkerhet er en sekundærfunksjon i virksomhetene gjør også at den strukturelle distansen er liten, gjennom det faktum at utfordringene er relativt like hos de ulike virksomhetene og at personell med IKT-kompetanse vil være en del av alle virksomheter. Når det gjelder kognitiv distanse, har oppgaven pekt på at kompetanse knyttet til digital sikkerhet er en utfordring gjennom det varierende faglige nivået generelt blant ansatte i norske virksomheter. Også kompetansemangel gjennom manglende personell med IKT-utdanning skaper en stor kognitiv distanse innen feltet digital sikkerhet. Den viktigste faktoren for distanse mellom organisasjoner identifisert i denne oppgaven er imidlertid makt-distansen Justis- og beredskapsdepartementet naturlig innehar som tilsynsmyndighet for digital sikkerhet for alle virksomheter i Norge. Denne oppgaven har funnet at JD i langt større grad bør utnytte denne maktdistansen gjennom økt hyppighet og strukturering av tilsyn. Dette vil av virksomhetene oppleves som økt kontroll fra tilsynsmyndighetens side, som videre vil føre et generelt høyere nivå av digital sikkerhet.

Når det gjelder intra-organisatoriske tiltak har oppgaven funnet at tydelig ledelse, klare prioriteringer og mål for arbeidet med digital sikkerhet vil gjøre virksomheten best mulig rustet for god samordning med andre virksomheter. Oppgaven har videre funnet at unngåelse av interne spenninger vil være en faktor som også vil ha innvirkning på virksomhetens suksess med samvirke med andre virksomheter. Oppgaven har ikke identifisert noen

inter-organisatoriske utfordringer knyttet til Justis- og beredskapsdepartementets interne organisering for arbeidet med digital sikkerhet.

Effektivt samarbeid mellom offentlige instanser og privat sektor er avgjørende for å styrke digital sikkerhet på nasjonalt nivå. Dette innebærer etablering av klare ansvarsforhold, gjensidig tillit og god kommunikasjon. Vi har drøftet utfordringer JD kan møte på når de skal samordne innsatsen om digital sikkerhet, herunder etablering av tillit, balanse mellom formalisering og fleksibilitet, samt ledelse i inter-organisatoriske relasjoner.

8.2 Oppgavens begrensninger og forslag til videre forskning

I sluttfasen av arbeidet med denne oppgaven, ble det fremsatt et lovforslag fra regjeringen om å innføre en egen lov om digital sikkerhet i Norge (Regjeringen, 2023). Lovforslaget søker å sette krav til virksomheter som har "særlig betydning for samfunnet", i den hensikt å sikre det norske velferdssamfunnet gjennom digitaliseringen av samfunnet (ibid). Som styrende dokument ville denne loven vært naturlig å inkludere i denne oppgaven, da den bidrar til tydeligere og høyere lovkrav til private og offentlige virksomheter innenfor digital sikkerhet.

Det er etter vårt syn ingen tvil om at mange virksomheter både på privat og offentlig side i Norge sliter med overgangen til stadig økt bruk av digitale verktøy samtidig som antall digitale angrep øker. Vi mener det vil være interessant å gå ytterligere inn i hvilke utfordringer som ligger i den tverrsektorielle koordineringen av arbeidet med digital sikkerhet, i den hensikt å forstå hvorfor endringen til mer digital sikkerhet i virksomhetene er krevende. I gjennomgangen av teori om tverrsektorielt og tverretatlig samarbeid har vi sett at det er forsket mye på inter-organisatoriske tiltak for samordning, men i mindre grad de intra-organisatoriske tiltakene og mekanisme som skiller god og dårlig samordning. Til syvende og sist vil dette kunne ha positive effekter for hvordan etater organiserer seg for å best mulig kunne oppnå ønskede mål ved samordnet innsats.

9 Litteraturliste

Antonsen, S., Heldal, F., & Kvalheim, S. A. (2017). *Sikkerhet og ledelse*. Gyldendal akademisk.

Asdal, K., & Reinertsen, H. (2020). *Hvordan gjøre dokumentanalyse: en praksisorientert metode*. Cappelen Damm akademisk.

Bacchi, C. (2009). *Analyzing Policy - What's the problem represented to be?* Pearson Australia.

Bastøe, P. Ø., Dahl, K., & Larsen, E. (2002). *Organisasjoner i utvikling og endring: Oppgaveløsning i en ny tid*. Gyldendal Akademisk.

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

Christensen, T., Egeberg, M., Lægreid, P., Roness, P. G., & Røvik, K. A. (2015). *Organisasjonsteori for offentlig sektor* (3rd ed.). Universitetsforl.

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

Departementene. (2019). *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*.

Departementene. (2019, January 30). *Nasjonal strategi for digital sikkerhetskompetanse - regjeringen.no*. Regjeringen.no. Hentet Mai 1, 2023, fra https://www.regjeringen.no/contentassets/8ed748d37e504a469874ce936551b4f8/nasjonal-strategi-for-digital-sikkerhetskompetanse.pdf

Digitaliseringsdirektoratet. (2022). *Digital sikkerhet*. Digdir. Hentet April 28, 2023, fra https://www.digdir.no/handlingsplanen/digital-sikkerhet/1263

European Commission. (2022). *Digital Economy and Society Index (DESI) 2022 - Norway*. Norway in the Digital Economy and Society Index. Hentet April 28, 2023, fra https://ec.europa.eu/newsroom/dae/redirection/document/88980

European Commission. (2022, July 28). *Norway in the Digital Economy and Society Index*. Shaping Europe's digital future. Hentet Mars 28, 2023, fra https://digital-strategy.ec.europa.eu/en/policies/desi-norway

Forsvarsdepartementet. (2018). *Lov om nasjonal sikkerhet (sikkerhetsloven)*. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Forsvarsdepartementet. (2018, July 2). *HØRINGSNOTAT - Forslag til forskrifter til ny sikkerhetslov*. Regjeringen.no. Hentet April 23, 2023, fra https://www.regjeringen.no/contentassets/61541372f9f74ed1982b0a4338d791f2/horingsnotat---forskrifter-til-sikkerhetsloven.pdf

Grønnmo, S. (2020, Oktober 5). *Innholdsanalyse*. Store norske leksikon. Hentet April 9, 2023, fra https://snl.no/innholdsanalyse

Hollnagel, E. (2008). *The changing nature of risks*. Ergonomics Australia Journal.

Hovden, J. (1998). *"Ethics and safety": "Mortal" questions for safety management*. Safety in Action, Melbourne, 25-28 Februar.

Hydro. (2020, Oktober 14). *Cyber-attack on Hydro*. Hydro.com. Hentet May 9, 2023, fra https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

Johannessen, A., Tufte, P. A., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utgave ed.). Abstrakt Forlag.

Johnsen, A. B., & Ertesvåg, F. (2014, Mai 17). Slakter beredskapen i Justisdepartementet. *VG*. https://www.vg.no/nyheter/innenriks/i/wlV8L/slakter-beredskapen-i-justisdepartementet

Justis- og beredskapsdepartementet. (2015). *Digital sårbarhet - sikkert samfunn*. Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet. (2016). *Meld. St. 10 (2016–2017)*. Meld. St. 10 (2016–2017) - regjeringen.no. Hentet Mai 1, 2023, fra https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/?ch=3

Justis- og beredskapsdepartementet. (2017, June 9). *Meld. St. 38 (2016–2017) "IKT-sikkerhet - Et felles ansvar"*. Regjeringen.no. Hentet April 28, 2023, fra https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2018, Desember 3). *NOU 2018: 14 IKT-sikkerhet i alle ledd — Organisering og regulering av nasjonal IKT-sikkerhet*. Regjeringen.no. Hentet Mai 1, 2023, fra

https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2019). *Veileder til samfunnssikkerhetsinstruksen*. Direktoratet for samfunnssikkerhet og beredskap. Hentet Februar 2, 2023, fra https://www.dsb.no/globalassets/dokumenter/veiledere-handboker-og-informasjonsmateriell/veiledere/veileder-til-samfunnssikkerhetsinstruksen.pdf

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I. A., Hovden, J., & Schiefloe, P. M. (2018). *Sikkerhet i arbeidslivet*. Fagbokforl.

LaPorte, T. R., & Consolini, P. M. (1991). *Working in Practice but Not in Theory: Theroretical Challenges of "High-Reliability Organizations"* (1st ed.). Journal of Public Administration Research and Theory: J-PART.

Lovdata. (2013, Mars 23). *Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet*. Lovdata. Hentet May 9, 2023, fra https://lovdata.no/dokument/DEL/forskrift/2013-03-22-296

Nasjonal kommunikasjonsmyndighet. (2019). *EkomROS 2019: Den digitale grunnmuren*. Nkom. Hentet Mai 1, 2023, fra https://www.nkom.no/rapporter-og-dokumenter/ekomros-2019/_/attachment/download/1d662520-d3e9-40e2-8950-ec63e084c014:158b4769643926c4d6be90247638e3c40a1c7f92/EkomROS%202019%20-%20Nkom.pdf

Nasjonal sikkerhetsmyndighet. (2020, Juni 5). *Grunnprinsipper for IKT-sikkerhet 2.0*. Nasjonal sikkerhetsmyndighet. Hentet Mai 1, 2023, fra https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/

Nasjonal sikkerhetsmyndighet. (2022, April 8). *Nasjonalt digitalt risikobilde 2022*. Nasjonal sikkerhetsmyndighet. Hentet Mai 1, 2023, fra https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf

Nesheim, T., Gressgård, L. J., Hansen, K., & Simon Neby. (2019). Gjenstridige problemer og tverretatlig samordning: Et analytisk rammeverk. *Norsk Vitenskapelig Tidsskrift*, *35*(1-2019), 28-50. https://doi.org/10.18261/issn.1504-2936-2019-01-02

NIFU. (2019, Juni 3). Leaving the windows open – Økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk sosiologisk tidsskrift*, *3*(3), 173-190. https://nifu.brage.unit.no/nifu-xmlui/handle/11250/2601787

NSM. (n.d.). *Nasjonalt cybersikkerhetssenter*. Nasjonal sikkerhetsmyndighet. Hentet Mai 7, 2023, fra https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/

NSM. (2019, Januar 1). *Introduksjon - Ny sikkerhetslov*. Nasjonal sikkerhetsmyndighet. Hentet April 17, 2023, fra https://nsm.no/regelverk-og-hjelp/sikkerhetsloven-og-forskrifter

NSM. (2021). *Nasjonalt digitalt risikobilde 2021*. Nasjonal sikkerhetsmyndighet. Hentet Mai 9, 2023, fra https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

NSM. (2023). *Risiko 2023 - Økt uforutsigbarhet krever høyere beredskap*. NSM.no. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

NSM. (2023). *Sikkerhetsfaglig råd - Et motstandsdyktig Norge*. Nasjonal sikkerhetsmyndighet. Hentet Mai 9, 2023, fra https://nsm.no/getfile.php/1312994-1683615611/NSM/Filer/Dokumenter/Rapporter/Sikkerhetsfaglig%20r%C3%A5d%20-%20Et%20motstandsdyktig%20Norge.pdf

NSM. (2023, April 17). *Ny tryggingslov trer i kraft*. Nasjonal sikkerhetsmyndighet. Hentet April 17, 2023, fra https://nsm.no/om-oss/historien-om-nsm/ny-sikkerhetslov-trer-i-kraft

NSM. (2023, Mai 7). *Nasjonalt cybertryggingssenter (NCSC) vert etablert*. Nasjonal sikkerhetsmyndighet. Hentet Mai 7, 2023, fra https://nsm.no/om-oss/historien-om-nsm/nasjonalt-cybersikkerhetssenter-apnes?instance=0

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press.

Politiet. (2023). *Cyberkriminalitet 2023*. Politiet. Hentet Mai 8, 2023, fra https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Rausand, M., & Utne, I. B. (2009). *Risikoanalyse - teori og metoder*. Tapir Akademisk Forlag.

Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate.

Rec Silicon. (2020, January 14). *REC Silicon Cyber Security Incident*. Recsilicon.com. Hentet Mai 9, 2023, fra https://storage.mfn.se/b429712c-632d-4b36-948b-a71324a20351/rec-silicon-cyber-security-incident.pdf?

Regjeringen. (2017, Juni 16). *Prop. 153 L (2016–2017) - regjeringen.no*. Regjeringen.no. Hentet Mai 10, 2023, fra https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/

Regjeringen. (2023, Mai 5). *Norge får sin første lov om digital sikkerhet*. Regjeringen.no. Hentet Mai 6, 2023, fra https://www.regjeringen.no/no/aktuelt/norge-far-sin-forste-lov-om-digital-sikkerhet/id2975757/

Regjeringen. (2023, Mai 5). *Norge får sin første lov om digital sikkerhet*. Regjeringen.no. Hentet Mai 7, 2023, fra https://www.regjeringen.no/no/aktuelt/norge-far-sin-forste-lov-om-digital-sikkerhet/id2975757/

Riksrevisjonen. (2023, Februar 2). *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*. Riksrevisjonen. Hentet Mai 4, 2023, fra https://www.riksrevisjonen.no/globalassets/rapporter/NO-2022-2023/myndighetenes-samordning-av-arbeidet-med-digital-sikkerhet-i-sivil-sektor.pdf

Ringdal, K. (2018). *Mangfold: Samfunnsvitenskapelig forskning og kvantitativ metode* (4th ed.). Fagbokforlaget.

Rochlin, G. I., La Porte, T. R., & Roberts, K. H. (1987). *The Self-Designing High-Reliability Organization: Aircraft Carrier Flight Operations at Sea*. U.S. Naval War College Digital Commons. Hentet Mai 6, 2023, fra

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=4373&context=nwc-review

Samfunnsøkonomisk analyse. (2021, Januar 20). *Norges behov for IKT- kompetanse i dag og framover*. Abelia. Hentet Mai 3, 2023, fra https://ikt-norge.no/wp-content/uploads/r1-2021-behov-for-og-tilbud-av-ikt-kompetanse-1.pdf

SNL. (2021, Juni 21). *Lov*. Store norske leksikon. Hentet April 17, 2023, fra https://snl.no/lov

Tjora, A. (2020). *Kvalitative forskningsmetoder i praksis* (3. utgave ed.). Gyldendal Norsk Forlag.

Trondal, J. (2017). *The Rise of Common Political Order*. Storbritannia: Edward Elgar Publishing.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected. Resilient Performance in an Age of Uncertainty*. Jossey-Bass.