UiT Norges arktiske universitet

Institutt for samfunnsvitenskap

Samarbeid om cybersikkerhet

En studie av håndtering av IKT-sikkerhetshendelser

Eskil Jakobsen

Masteroppgave i statsvitenskap – STV-3900 – Mai 2021

Forord

Cybersikkerhet er et tema som har betydning for alle mennesker som bruker datamaskiner og internett, enten de er klar over det eller ikke. Motivasjonen for valg av tematikk knyttet til cybersikkerhet som gjenstand for undersøkelse i denne masteroppgaven er todelt. Jeg har stor interesse for forholdet mellom mennesker og datateknologi, og jeg har en oppfatning av at temaet har blitt aktualisert gjennom mange alvorlige IKT-sikkerhetshendelser de siste årene. Gjennom arbeidet med denne oppgaven har jeg fått økt forståelse for hvor mange sårbarheter som eksisterer og hvor viktig det er å ha et bevisst forhold til sikkerhet i vår digitale hverdag.

Arbeidet med oppgaven har vært spennende, utfordrende og givende på samme tid. Jeg vil rette en stor takk til min veileder Hilde Bjørnå for sin tålmodighet og gode råd. Jeg vil også takke alle informantene som har deltatt i intervjuer. Deres innsikt og åpenhet har vært helt avgjørende for denne oppgaven. Jeg er også veldig takknemlig for seminarene som Beate og Sigbjørn har ledet gjennom arbeidsperioden hvor jeg har fått verdifulle innspill og råd fra Kristine, Øystein og andre. Jeg vil også si tusen takk til Mamma, Pappa, Hedda og Mormor som alltid støtter meg.

Sammendrag

Norge er et av verdens mest digitaliserte land og Lysne-utvalget slo i 2015 fast at dette gjør oss sårbare. En rekke alvorlige IKT-sikkerhetshendelser de senere år har vist oss at denne sårbarheten er reell. I 2019 lanserte norske myndigheter en nasjonal strategi for digital sikkerhet og to sentere ble opprettet for å styrke samfunnets evne til håndtere IKT-sikkerhetshendelser. Nasjonalt cybersikkerhetssenter (NCSC) og Kripos cyberkrimsenter NC3 arbeider begge med å beskytte innbyggere og virksomheter fra trusler i det digitale rom. Sentrene inngår i en såkalt *multistakeholdermodell* bestående av aktører fra det offentlige og det private som alle arbeider med å håndtere trusler og hendelser i det digitale rom. Hvordan nøkkelaktører i dette systemet samarbeider er temaet i denne masteroppgaven. Tverrsektorielt samarbeid mellom myndighetsaktører innenfor samfunnssikkerhet har helt siden innføringen av samvirkeprinsippet i 2012 vært et prioritert utviklingsområde. I den nasjonale strategien for digital sikkerhet er offentlig-privat samarbeid en grunnpilar. På bakgrunn av dette er følgende problemstilling utformet: *Hvordan fungerer samarbeid mellom aktører i norske myndigheters styringssystem for håndtering av IKT-sikkerhetshendelser?*

På grunnlag av dokumentanalyse og semistrukturerte kvalitative intervjuer med informanter fra NSM, Kripos NC3, HelseCERT og Østre Toten kommune beskrives samarbeid mellom nøkkelaktører innenfor håndtering av IKT-sikkerhetshendelser. Samarbeid analyseres i lys av to typologier om styring på cybersikkerhetsfeltet, en hierarkisk typologi og en multistakeholder-typologi (multistakeholdermodellen). Løsepengevirusangrepet som rammet Østre Toten kommune i januar 2021 benyttes som et illustrerende eksempel på hendelseshåndtering i praksis.

I studien avdekkes tilstedeværelse av forhold som kan signalisere overlappende ansvarsområder og interessekonflikt mellom de sektorovergripende aktørene NCSC og Kripos NC3. Det pekes også på utfordringer knyttet til manglende felles situasjonsforståelse av trusselbildet og relevante botemidler. Alvorlighetsgraden av konsekvensene til disse utfordringene oppfattes som motvirket av en rekke samarbeidsordninger og god kommunikasjon mellom aktørene i styringssystemet. Betydningen av åpenhet om IKT-sikkerhetshendelser tematiseres også i studien. Analysen tilsier at åpenhet fra rammede virksomheter styrker samfunnets evne til å håndtere IKT-sikkerhetshendelser gjennom bevisstgjøring og læringspunkter som kommer alle til gode.

Innholdsfortegnelse

Tabelliste

Figurliste

Vedlegg

Forkortelser

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DFØ	Direktoratet for forvaltning og økonomistyring
DIFI	Direktoratet for forvaltning og IKT (Digitaliseringsdirektoratet)
DSB	Direktoratet for samfunnssikkerhet og beredskap
DSSCERT	Departementenes sikkerhets- og serviceorganisasjon Computer Emergency Response Team
EKOM	Elektronisk kommunikasjon
ENISA	European Union Agency for Cybersecurity
FCKS	Felles cyberkoordineringssenter
FD	Forsvarsdepartementet
FFI	Forsvarets forskningsinstitutt
HF	Helseforetak
IKT	Informasjons- og kommunikasjonsteknologi
IRT	Incident Response Team
ISO	International Organization for Standardization
IT	Informasjonsteknologi
JD	Justis- og beredskapsdepartementet
NC3	Nasjonalt cyberkrimsenter
NCSC	Nasjonalt cybersikkerhetssenter
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NorSIS	Norsk senter for informasjonssikring
NOU	Norges offentlige utredninger
NSM	Nasjonal sikkerhetsmyndighet
PST	Politiets sikkerhetstjeneste
RHF	Regionalt helseforetak
SRM	Sektorvise responsmiljøer
VDI	Varslingssystem for digital infrastruktur

1.0 Introduksjon

Informasjonsteknologi og internettbasert kommunikasjon har de senere tiår fått enorm betydning i tilnærmet alle næringssektorer og alle deler av offentlig forvaltning. Inntreden av det såkalte cyberspace i samfunnet har blitt beskrevet som en informasjonsrevolusjon (Langø & Sandvik, 2013, s. 222). I kjølvannet av dette har sikkerhet innenfor dette nye domenet, ofte omtalt som cybersikkerhet, blitt vitalt for aktører i både offentlig og privat sektor. Økt grad av digitalisering i hele samfunnet har ført til økt sårbarhet for trusler som eksisterer i det digitale rom (NOU 2015:13, 2015, s. 15-16). Slike trusler har vist seg å ha stort skadepotensiale gjennom flere alvorlige IKT-sikkerhetshendelser som har rammet norske virksomheter og offentlige organer de senere år. Angrepet på Norsk Hydro i 2019 førte til et tap i størrelsesorden 550-650 millioner NOK etter langvarig produksjonsstans (Hydro, 2019). Dataangrepet mot Stortinget og en rekke andre offentlige og private aktører på sensommeren i 2020 førte til at trusselaktøren fikk tilgang til sensitiv informasjon om Norges folkevalgte (PST, 2021, s. 7; NRK, 2020). Østre Toten kommune ble i januar 2021 rammet av et dataangrep som gjorde det umulig å drifte kommunale helsetjenester etter etablerte prosedyrer (Helgestad, 2021).

Hvordan slike hendelser håndteres kan ha avgjørende betydning for hvor alvorlig skade som forvoldes den rammede virksomheten og i forlengelsen samfunnet forøvrig. I myndighetenes nasjonale strategi for digital sikkerhet som ble presentert i 2019 foreligger et tydelig fokus på samarbeid både mellom myndighetsaktører og mellom det offentlige og det private (Departementene, 2019a, s. 9). I 2019 ble også to sentere med ansvar innenfor håndtering av IKT-sikkerhetshendelser etablert, Nasjonalt cybersikkerhetssenter (NCSC) og Kripos cyberkrimsenter NC3. Hvordan disse sentrene og andre viktige aktører i myndighetenes system for styring av hendelseshåndtering evner å samarbeide fremstår som et viktig tema sett i lys av myndighetenes strategiske fokus på samarbeid. På bakgrunn av dette er temaet for denne masteroppgaven samarbeid mellom aktører i norske myndigheters styringssystem for håndtering av IKT-sikkerhetshendelser.

1.1 Problemstilling

Arbeidet som er gjort for å bedre tverrsektorielt samarbeid i staten siden innføringen av samvirkeprinsippet i 2012 og fokuset på offentlig-privat samarbeid i «Nasjonal strategi for digital sikkerhet» 2019 signaliserer denne tematikkens aktualitet. Jeg har på bakgrunn av dette utformet følgende problemstilling:

Hvordan fungerer samarbeid mellom aktører i norske myndigheters styringssystem for håndtering av IKT-sikkerhetshendelser?

For å understøtte problemstillingen og styrke utgangspunktet for analysen har jeg utformet disse to forskningsspørsmålene:

1. Hvordan tilrettelegger norske myndigheter for samarbeid om håndtering av IKT-sikkerhetshendelser?
2. Hvordan fungerer Nasjonalt cybersikkerhetssenters rolle som bindeledd mellom aktører i praksis?

1.2 Formål

Formålet med problemstillingen er å belyse norske myndigheters tilrettelegging for samarbeid på cybersikkerhetsfeltet og samarbeid om hendelseshåndtering i praksis. I forlengelsen av dette er ambisjonen å kunne beskrive hvilken betydning tverrsektorielt samarbeid og offentlig-privat samarbeid har som botemidler mot utfordringer som manglende felles situasjonsforståelse, overlappende ansvarsområder, interessekonflikter og «maktkamp» mellom det offentlige og det private.

1.3 Avgrensninger

Denne oppgaven omhandler cybersikkerhet i Norge og det norske styringssystemet for hendelseshåndtering. Cybersikkerhet i sikkerhetspolitisk forstand er kun relevant som et fenomen de norske aktørene må forholde seg til. Cyberforsvaret inngår ikke i analysen siden målet med oppgaven er å belyse sivil hendelseshåndtering. Etterretningstjenesten og Politiets sikkerhetstjeneste sine roller innenfor hendelseshåndtering omtales kun i forbindelse med deres posisjon i forhold til NSM og Kripos NC3. Årsaken til dette er at et hovedfokus på NSMs særegne rolle som bindeledd mellom sektorer og aktører fremstår som mest

formålstjenlig for problemstillingen. Aktører som tilhører privat sektor belyses kun gjennom samarbeid med offentlige etater og organer.

1.4 Operasjonalisering

Det overordnete systemet for håndtering av IKT-sikkerhetshendelser i Norge er omfattende og dets utforming preges av et stort antall aktører. For å operasjonalisere min problemstilling om samarbeid har jeg derfor valgt å definere et utvalg av aktører som et eget *styringssystem*. Jeg har utformet to kriterier for innlemmelse i dette konstruerte styringssystemet, tilstedeværelse av rolle som bistandsgiver til andre innenfor digital sikkerhet og formål som inkluderer håndtering av IKT-sikkerhetshendelser. For å unngå unødvendig kompleksitet i det konstruerte styringssystemet har jeg ikke gjennomført en altomfattende undersøkelse av aktører basert på de to kriteriene. Jeg har brukt dem som retningsgivende instrumenter og kartlagt de aktørene som fremstår som de viktigste for samarbeid vedrørende hendelseshåndtering i Norge.

I tråd med de ovennevnte vurderingene har jeg kommet frem til at styringssystemet for håndtering av IKT-sikkerhetshendelser kan defineres som bestående av følgende aktører: Alle *myndighetsaktører* med sektorovergripende ansvar og mandat som innebefatter bistand ved IKT-sikkerhetshendelser, *sektorvise responsmiljøer* med ansvar for offentlige organer og virksomheter (SRM-ene), samt *private selskaper* innenfor IT-sikkerhetsbransjen som har et formalisert forhold til offentlige organer vedrørende hendelseshåndtering. Formalisert forstås i denne sammenhengen som en etablert relasjon som er anerkjent av et offentlig organ, eksempelvis en bedrift som er kontrahert for å yte tjenester. Klassifiseringen av sektorovergripende aktører er gjort på grunnlag av opplysninger hentet fra myndighetenes strategi for digital sikkerhet og relevante stortingsmeldinger (Departementene, 2019, s. 22; Justis- og beredskapsdepartementet, 2020).

På grunnlag av problemstillingen og dens formål samt denne oppgavens omfang fremsto det som hensiktsmessig å fokusere på noen utvalgte aktører i dette styringssystemet. I utvelgelsen av aktører som skulle bli gjenstand for analyse var betydning for hendelseshåndtering i praksis det styrende kriteriet. Etter undersøkelse av aktørene som er definert inn i systemet valgte jeg ut NSM representert ved NCSC, Politiet representert ved Kripos NC3 og HelseCERT som representant for de sektorvise responsmiljøene (SRM-ene). Problemstillingen ble videre operasjonalisert ved å definere disse utvalgte aktørene som representanter for hvordan samarbeid knyttet til hendelseshåndtering foregår. Deretter ble

deres samarbeid med hverandre og andre aktører i styringssystemet undersøkt. Tanken bak denne tilnærmingen er at de utvalgte aktørenes samarbeid er så avgjørende for hvordan styringssystemet fungerer i sin helhet at hele styringssystemet blir tilstrekkelig belyst ved å analysere deres roller. Det fremstår som viktig å presisere at de utvalgte aktørene ikke skal danne grunnlag for representativitet i vitenskapsteoretisk forstand, men som nøkkelenheter som illustrerer hvordan systemet de tilhører fungerer. Nedenfor er styringssystemet presentert i en tabell. De utvalgte aktørene er markert i fet skrift.

Tabell 1 – Norske myndigheters styringssystem for håndtering av IKT-sikkerhetshendelser

Sektorovergripende
DSB - Etterretningstjenesten - FCKS - **Kripos NC3** - Kriserådet - Krisestøtteenheten - **NCSC (NSM)** - NSM - PST
Sektorvise responsmiljøer (SRM)
DSSCERT - EkomCERT - FinansCERT - **HelseCERT** - JustisCERT - Kommune-CSIRT* - KraftCERT - Landbruks- og matCERT - MilCERT - MiljøCERT - UninettCERT
Private virksomheter med formalisert forhold til offentlige organer
Atea - Defendable - KPMG** - Mnemonic - NETSecurity

*Kommune-CSIRT sin status som SRM er uavklart i skrivende stund.

**KPMG er inkludert som følge av sin bistandsgivning til Østre Toten kommune.

1.5 Oppgavens struktur

Oppgaven er inndelt i 6 kapitler. I dette første kapittelet presenteres tematikken sammen med problemstilling, forskningsspørsmål, formål, avgrensninger, operasjonalisering og struktur. Kapittel 2 omhandler bakgrunnsinformasjon jeg anser det som nødvendig for leseren å besitte for å forstå min analyse og diskusjon. Dette dreier seg primært om cybersikkerhetssituasjonen og det norske styringssystemet for hendelseshåndtering. I kapittel 3 presenterer jeg metodene som er brukt og grunnlaget for mine valg. Jeg redegjør også for utfordringer og avveininger som har preget arbeidet med oppgaven. I kapittel 4 beskrives teoretiske perspektiver på cybersikkerhetsfeltet og styring. Jeg legger også frem postulater som preger teoriutviklingen på feltet. I kapittel 5 analyseres empiri fra dokumentanalyse og semistrukturerte kvalitative intervjuer. Dette inkluderer empiri om IKT-sikkerhetshendelsen som rammet Østre Toten kommune i januar 2021 som jeg benytter som et illustrerende eksempel. Kapittel 6 inneholder

en oppsummerende diskusjon av empiri i lys av teori. Avslutningsvis oppsummeres prosjektets funn i en konklusjon etterfulgt av en redegjørelse av studiens begrensninger og refleksjoner om potensiell videre forskning.

2.0 Bakgrunn

Hvordan samarbeid mellom aktører i styringssystemet for hendelseshåndtering fungerer er sammenbundet med den samfunnsmessige konteksten samarbeidet foregår i. Hva slags tilnærming, planer, tiltak og ordninger norske myndigheter benytter i arbeidet med å tilrettelegge for samarbeid om håndtering av IKT-sikkerhetshendelser kan anses som avhengig av flere faktorer. Blant disse er forståelse av digitale sårbarheter og trusselaktørene som forårsaker IKT-sikkerhetshendelser. I det følgende vil jeg beskrive bakgrunnsinformasjon som jeg anser å være relevant for problemene styringssystemet er intendert å løse og myndighetenes tilnærming til disse. Kapittelet er også ment å gi relevant informasjon om cybersikkerhetssituasjonen i Norge.

2.1 Digitalisering og sårbarheter

I det moderne norske samfunnet har internett blitt en del av de aller fleste innbyggernes liv både i jobbsammenheng og privat. Samfunnskritiske tjenester som forsyning av strøm og vann, drift av livreddende verktøy i helsesektoren og bistand fra brannvesen og politi er i stor grad avhengig av IKT-systemer (Windvik, 2020, s. 19). Slik avhengighet kan danne grobunn for sårbarhet for både utilsiktede og tilsiktede uønskede hendelser. I juni 2014 ble «Lysne-utvalget» oppnevnt for å kartlegge digitale sårbarheter i Norge og komme med forslag til tiltak som kunne styrke beredskapen og redusere sårbarhetene (NOU 2015:13, 2015, s. 18). Utvalget pekte på en rekke sårbarheter og den som fremstår som viktigst på overordnet nivå er det norske samfunnets grad av digitalisering. Utvalget beskriver Norge som et av verdens mest digitaliserte land og at dette har både positive og negative sider. De fremste positive effektene er effektivisering- og moderniseringsgevinster. På den negative siden trekker utvalget frem at den høye graden av digitalisering har gjort at Norge har beveget seg lengre inn i et nytt sårbarhet- og risikobilde enn mange andre land. Som følge av dette kan det være vanskelig å høste relevante erfaringer fra andre. Utvalget kommenterer at situasjonen krever at det norske samfunnet må videreutvikle måtene det forholder seg til sårbarheter på (NOU 2015:13, 2015, s. 16).

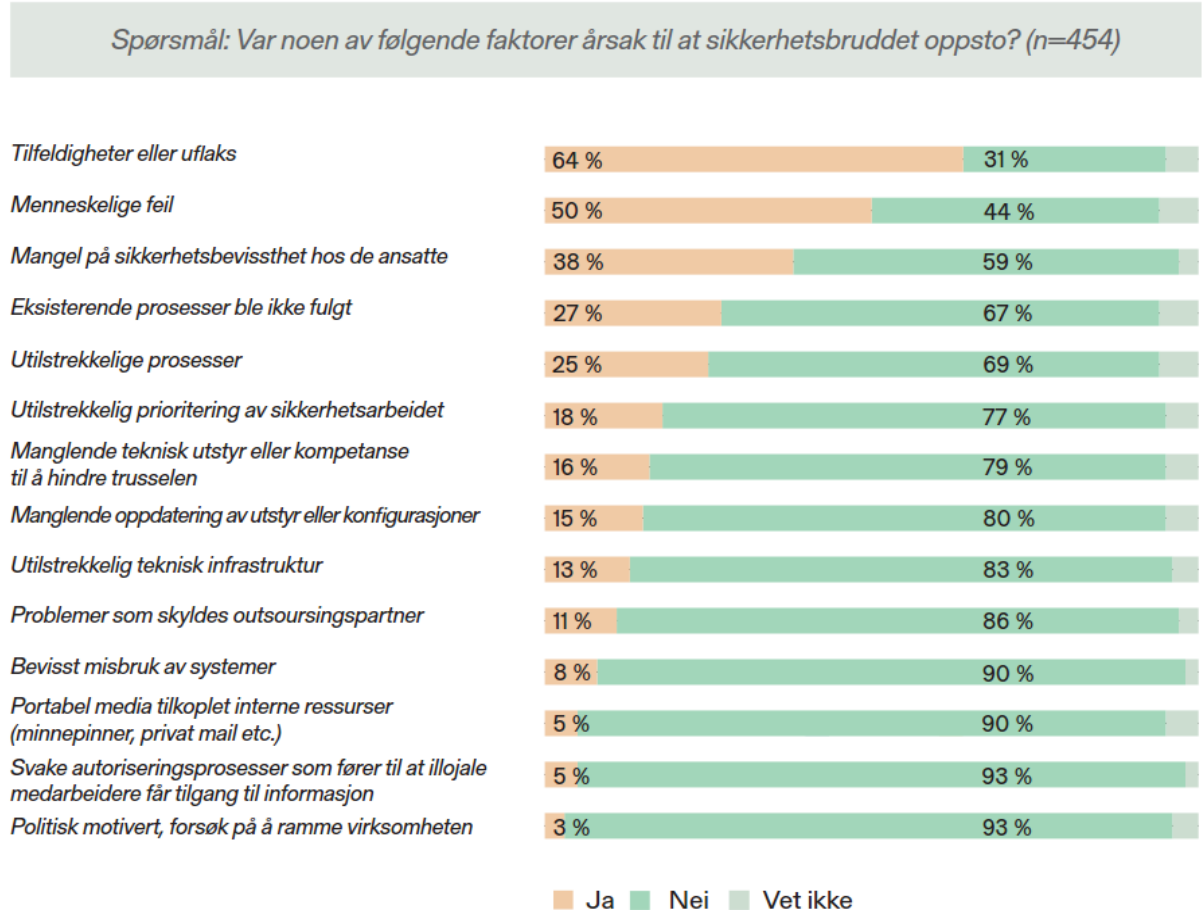
Det er mulig å forstå sårbarhet innenfor cybersikkerhetsfeltet som et tredelt fenomen bestående av menneskelige, teknologiske og organisatoriske sårbarheter. *Menneskelige* sårbarheter også omtalt som, personellsikkerhet, dreier seg om personer som kan bidra til å

skade en virksomhet gjennom kompromittering eller handling. Dette kan eksempelvis være en ansatt i en bedrift som utviser dårlig nettvett og ukritisk åpner alle vedlegg som dukker opp i sin e-post innboks. *Teknologiske* sårbarheter er som regel tilknyttet IKT-systemer og programvare. En datamaskin uten oppdatert operativsystem og fungerende brannmur er et eksempel på slik sårbarhet. *Organisatoriske* sårbarheter dreier seg om styring av en virksomhet og hvordan arbeid med menneskelige og tekniske sårbarheter foregår i den (Windvik, 2020, s. 20). Et eksempel på organisatorisk sårbarhet kan være en bedrift som har manglende rutiner for oppdatering av operativsystem og programvare i sine datasystemer.

Noen aktører i samfunnet har behov for å ha et mer bevisst forhold til digital sårbarhet enn andre. Dette behovet kan foreligge fordi de er mer utsatt for uønsket oppmerksomhet enn andre, eller at de besitter systemer og informasjon som er særlig viktig å beskytte. Blant dem som har et særlig behov for å operere med gode informasjonssikkerhetstiltak er virksomheter som ivaretar en grunnleggende nasjonal funksjon (GNF) direkte eller har leverandøransvar av materiell eller tjenester som bidrar til dette. Slike virksomheter vil ofte være underlagt egne bestemmelser og krav hjemlet i Sikkerhetsloven (Sikkerhetsloven, 2018, § 1-3; §6-1).

Koronapandemien har bidratt til økt bekymring for digitale sårbarheter blant deler av informasjonssikkerhetsmiljøet i Norge. Det faktum at bruk av hjemmekontor har økt betydelig i det private og det offentlige som følge av pandemien bidrar til at arbeidsoppgaver blir utført på maskinvare som kan ha for svake sikkerhetsinnstillinger og at kommunikasjon foregår over nettverk som er utilstrekkelig sikret (NSM, 2020c; Telenor, 2021). I Næringslivets sikkerhetsråds mørketallsundersøkelse for 2020, hvor informasjonssikkerhet i næringslivet og noen offentlige virksomheter undersøkes, ble det presentert data som tilsier at det ikke har vært noen betydelig økning i IKT-sikkerhetshendelser under koronapandemien (Næringslivets sikkerhetsråd, 2020, s. 40). Det ble også presentert data om hva slags type sårbarheter ansatte i næringslivet anser som årsak til at de ble rammet av IKT-sikkerhetshendelser i 2019. En oversikt hentet fra undersøkelsen følger under:

Figur 1 – Årsaksfaktorer bak IKT-sikkerhetshendelser



(Næringslivets sikkerhetsråd, 2020, s. 24)

Det fremgår av oversikten at årsaker forbundet med menneskelige, teknologiske og organisatoriske sårbarheter i varierende grad tolkes som avgjørende for at virksomheter ble rammet av en IKT-sikkerhetshendelse. Dette utvalget av representanter for norske virksomheter anser imidlertid tilfeldigheter eller uflaks som den fremste årsaken til at de ble rammet i 2019. Tilfeldigheter og uflaks kan være den opplevde årsaken for mange, men for at en IKT-sikkerhetshendelse skal oppstå må en aktør foreta seg tilsiktede handlinger som skaper uønsket aktivitet mot et IKT-system (NSM, 2017a, s. 1).

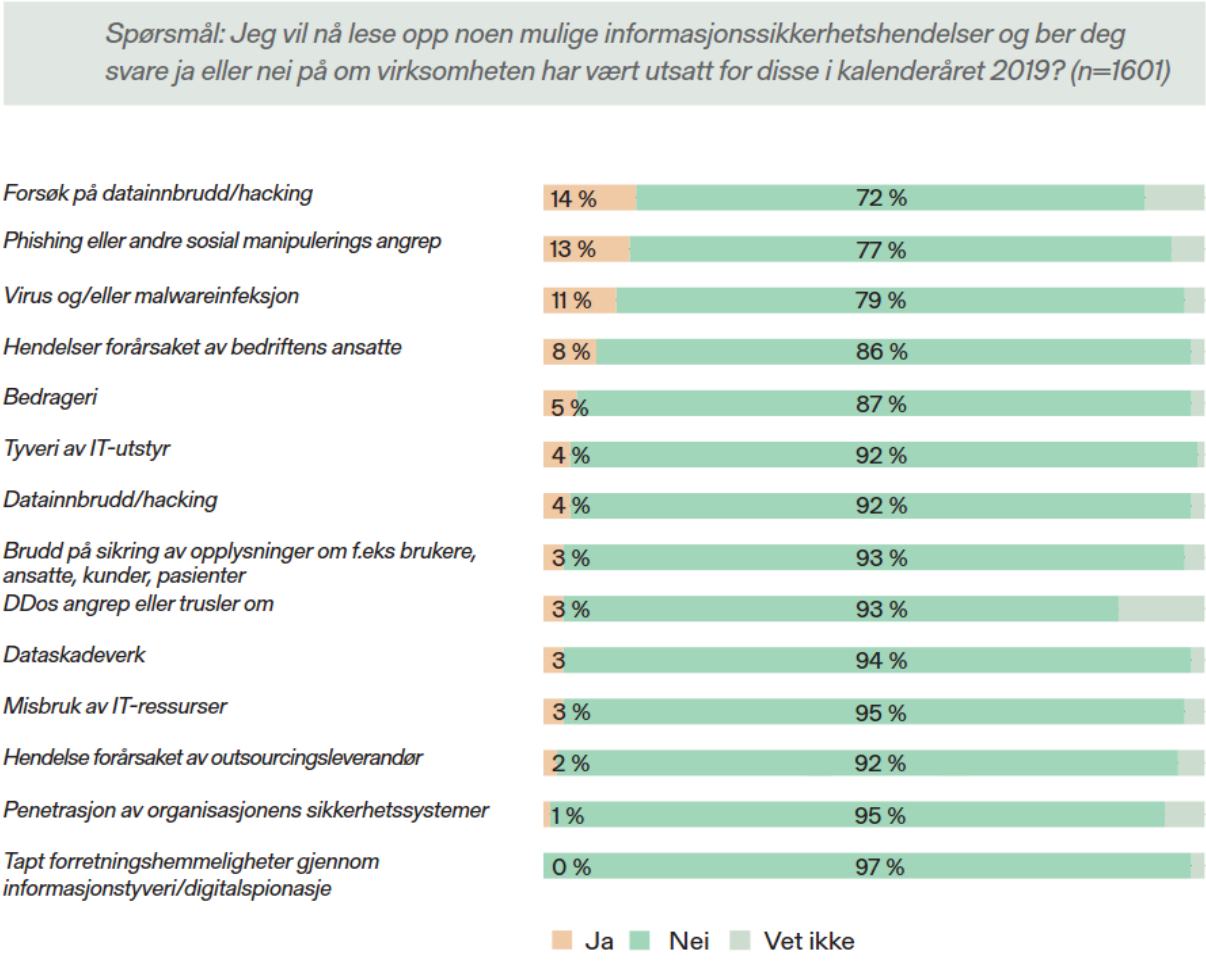
2.2 Trusselbildet

Det eksisterer mennesker og organisasjoner som ønsker å oppdage og utnytte sårbarheter for å utsette privatpersoner og virksomheter for uønskede hendelser. Disse omtales gjerne som trusselaktører og kan ha et vell av ulike motivasjoner for å benytte digitale sårbarheter til å

skade, sabotere, overvåke eller utnytte andre (Windvik, 2020, s. 20; Eie, 2020, s. 151-153). Slike aktører kan være alt fra en rebelsk tenåring med basiskunnskaper om programmering og nettverk til avanserte statlige aktører med tilgang til nyutviklet teknologi og kompetente informatikere (Muller, 2019, s. 289). Den samlede massen av slike truende aktører danner *trusselbildet* som personer, bedrifter og myndigheter må forholde seg til.

Hvert år publiseres det trusselvurderinger fra en rekke etater og organisasjoner som blant annet omhandler digital sikkerhet. Blant de mest betydningsfulle er Etterretningstjenesten, NSM og PST sine vurderinger. I 2021 presenterte disse sine trusselvurderinger samtidig (Regjeringen, 2021). Etterretningstjenesten og PST trekker i sine vurderinger frem nettverksoperasjoner mot norske mål fra kinesisk og russisk side som en viktig trussel. Nettverksoperasjonen som rammet Stortinget på sensommeren 2020 trekkes frem av begge som et eksempel på dette (Etteretningstjenesten, 2021, s. 21; PST, 2021, s. 7). NSM har et bredere fokus på digital sikkerhet enn Etterretningstjenesten og PST og trekker frem tre utviklingstrekk i risikobildet i sin vurdering for 2021; skjerpet risikobilde, tydeligere risiko knyttet til sammensatte trusler og forsterkning av risikobildet som følge av Covid-19 (NSM, 2021b, s. 7). Politiet har også publisert en trusselvurdering separat fra PST for 2021 som blant annet omhandler IKT-kriminalitet. I vurderingen for 2021 trekkes datainnbrudd med løsepengevirus frem som en meget aktuell risiko (Politiet, 2021, s. 22). I tillegg til de ovennevnte trusselvurderingene utgir Norsk senter for informasjonssikring (NorSIS) årlig en redegjørelse for trusler og trender. I vurderingen for 2021 trekker NorSIS i likhet med Politiet frem løsepengevirus som en aktuell trussel. De kommenterer at dataangrepet som rammet Østre Toten kommune, det illustrerende eksempelet i denne oppgaven, viser hvor alvorlige konsekvenser slike angrep kan få (NorSIS, 2021, s. 5). I Næringslivets sikkerhetsråds mørketallsundersøkelse for 2020 er det presentert data om ulike typer IKT-sikkerhetshendelser som rammet norsk næringsliv i 2019. En oversikt følger under:

Figur 2 – IKT-sikkerhetshendelser i næringslivet 2019



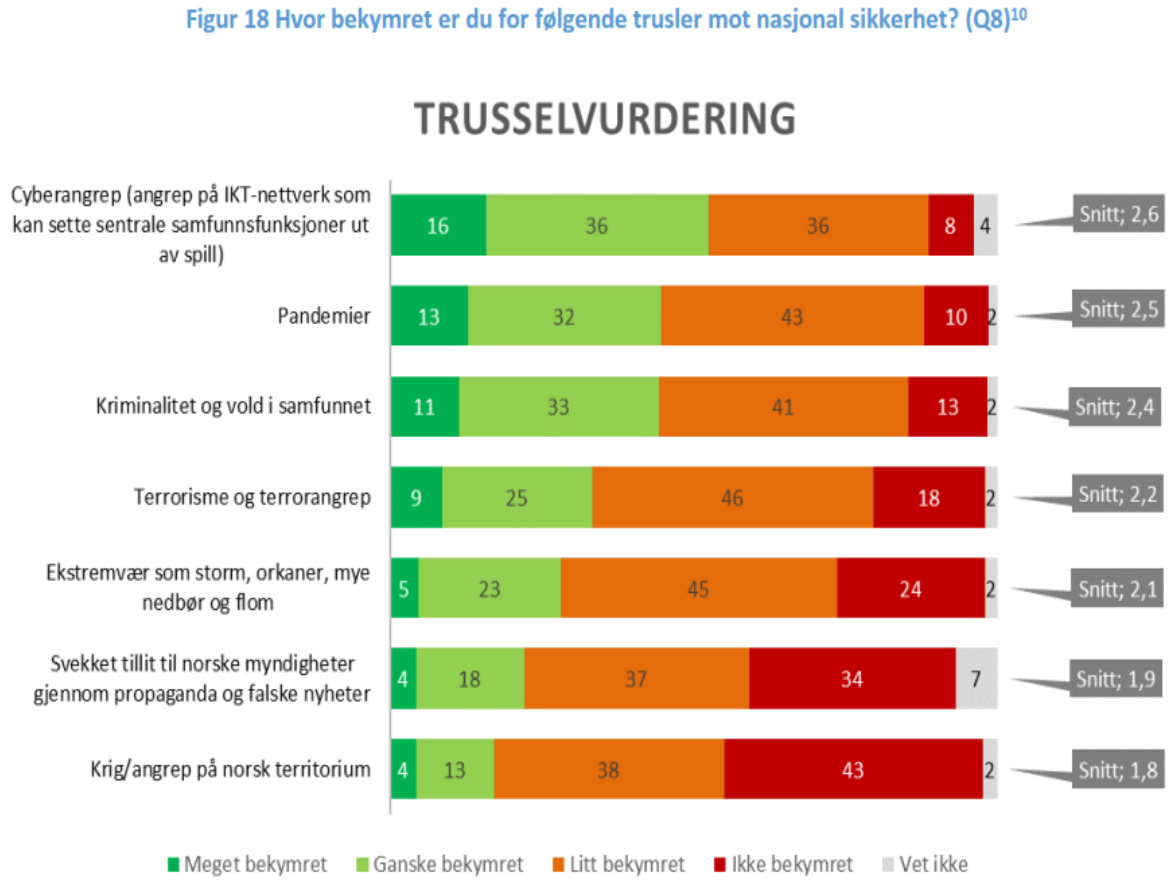
(Næringslivets sikkerhetsråd, 2020, s. 18)

Oversikten over selvrapporterte hendelser fra norsk næringsliv tyder på at det er mange ulike typer trusler som skaper problemer for en liten men betydelig del av virksomhetene. Flere enn 1 av 10 opplevde virus og/eller malwareinfeksjon i 2019. Dette er en type hendelse som kan få svært alvorlige konsekvenser for en rammet virksomhet (Norsk Hydro, 2020).

Hvordan trusselbildet oppfattes i befolkningen kan ha betydning for hvilke forventninger borgerne har til Staten når det gjelder implementering av sikringstiltak og utvikling av botemidler mot trusler i det digitale rom. I sin årlige undersøkelse av holdninger og oppfatninger kartlegger Forsvaret hvordan befolkningen oppfatter dem og i forlengelsen tematikk med implikasjoner for nasjonal sikkerhet. Et av spørsmålene som er del av undersøkelsen hvert år omhandler en liste med trusler og respondenten spørres om grad av bekymring for disse. I undersøkelsen som ble gjennomført i 2020 var cyberangrep den trusselen befolkningen var mest bekymret for. I figuren nedenfor er oversikten over svar på

spørsmålet om trusler fra undersøkelsen. Tallene fra 2020 er basert på svar fra 4036 respondenter som ble avgitt mellom 30. april og 1. juni 2020 (Kantar, 2020, s. 9).

Figur 3 – Innbyggernes bekymring for trusler mot nasjonal sikkerhet

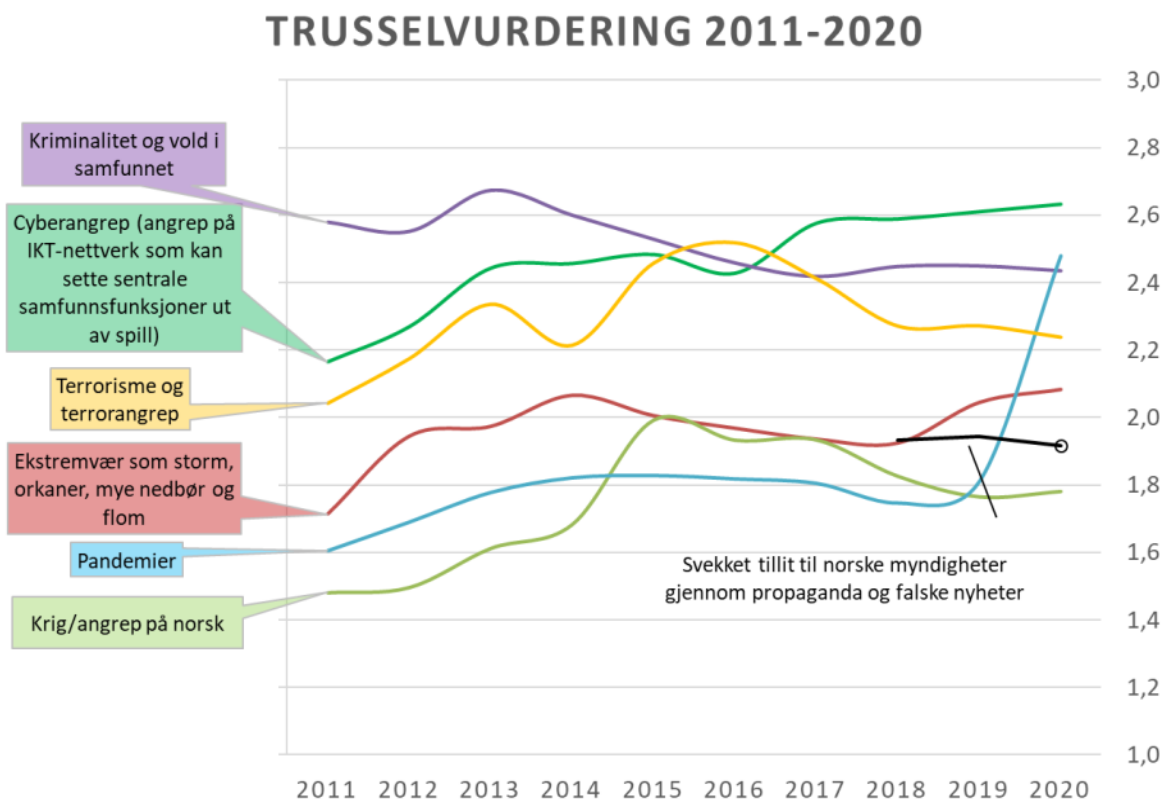


(Kantar – Forsvarets innbyggerundersøkelse 2020, 2020, s. 25)

Utfra disse tallene fremstår det som tydelig at den norske befolkningen er bekymret for cyberangrep. Pandemien forårsaket av Covid-19 begynte for alvor i Norge i mars 2020 og hadde pågått i rundt to måneder da respondentene avga sine svar. På tross av dette oppfatter dette utvalget cyberangrep som en større grunn til bekymring enn pandemier. I undersøkelsen presenteres også en graf som viser oppfatninger av truslene mot nasjonal sikkerhet over tid. Den er videreformidlet under:

Figur 4 – Innbyggernes bekymring for trusler mot nasjonal sikkerhet over tid

Figur 19 Trusselvurdering: 2011-2020[11]



(Kantar – Forsvarets innbyggerundersøkelse 2020, 2020, s. 26)

Basert på disse dataene kan det utledes at det har vært en økning i bekymring for cyberangrep siden 2011. Siden 2017 har denne trusselen vært vurdert som den mest bekymringsverdige av de som ble presentert for respondenter i Forsvarets innbyggerundersøkelse. På grunnlag av den påviste bekymringen for cyberangrep i befolkningen fremstår det som sannsynlig at norske innbyggere har forventninger til Staten innenfor dette samfunnssikkerhetsområdet.

2.3 Myndighetenes arbeid med digital sikkerhet

I Norge har Staten påtatt seg en rolle innenfor arbeidet med digital sikkerhet, ikke bare på vegne av seg selv og sine egne sikringsverdige systemer og informasjon, men også for sikring av personer og virksomheter i samfunnet for øvrig (Departementene, 2019a, forord). Norske myndigheter har siden begynnelsen av 2000-tallet etablert og utviklet strategier for ivaretakelse av informasjonssikkerhet i samfunnet (Justis- og politidepartementet, 2004, s.

43). Den første strategien kom i 2003 og hadde et overordnet fokus på en helhetlig tilnærming til myndighetenes arbeid med informasjonssikkerhet og koordinering mellom myndighetsorganer (Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet, 2003, s. 3). I 2012 ble en oppdatert strategi presentert med lignende formål som den første, men med en rekke nye mål inkludert. Blant disse var sikring av samfunnets evne til å oppdage, varsle og håndtere alvorlige IKT-sikkerhetshendelser og evne til å forebygge, avdekke og etterforske datakriminalitet (Departementene, 2012, s. 21-22). Den ferskeste strategien ble publisert i 2019 og har et særlig fokus på offentlig-privat samarbeid og koordinering mellom myndighetsetater (Departementene, 2019a, s. 6, s. 9). I september 2017 ble «Holte-utvalget» oppnevnt for å undersøke status på IKT-sikkerhet i Norge og utredning av hvordan fremtidig regulering og tiltak knyttet til IKT-sikkerhet burde utformes. Blant deres anbefalinger var utarbeidelse av en ny lov om IKT-sikkerhet som stiller krav til sikkerhetsnivå for samfunnskritiske virksomheter og forvaltning. Loven bør ifølge utvalget også gjennomføre NIS-direktivet som omhandler informasjonssikkerhet i EU og EØS (NOU 2018:14, 2018, s. 9; EU, 2016, s. 1)

Det er dessverre slik at noen trusselaktører har tilstrekkelig kunnskap og ressurser til å trenge gjennom sikringstiltak og påføre skade. Derfor må privatpersoner og virksomheter også være forberedt på å håndtere IKT-sikkerhetshendelser (Departementene, 2019a, s. 7). De siste par årene har det skjedd betydningsfulle endringer i organiseringen av offentlige etater med ansvar for håndtering av IKT-sikkerhetshendelser. Nasjonal sikkerhetsmyndighet (NSM) har gått fra å være administrativt underlagt Forsvarsdepartementet til Justis- og beredskapsdepartementet (Regjeringen, 2019). Nasjonalt cybersikkerhetssenter (NCSC) og Kripos nasjonale cyberkrimsenter (NC3) ble begge formelt opprettet i 2019. De to sentrene og de sektorvise responsmiljøene (SRM) er de fremste myndighetsaktørene innenfor operativ hendelseshåndtering i Norge (Justis- og beredskapsdepartementet, 2020, s. 84; NSM, 2017c, s. 11). Hvordan disse sentrene samarbeider med hverandre og andre aktører i det jeg har definert som styringssystemet for hendelseshåndtering er sentralt for min problemstilling.

2.4 De utvalgte aktørene i styringssystemet for hendelseshåndtering

Som nevnt i operasjonaliseringen undersøker jeg tre utvalgte aktører i det konstruerte styringssystemet for hendelseshåndtering. Disse er NCSC, Kripos NC3 og HelseCERT. Nedenfor følger beskrivelser av disse aktørene. For å beskrive NCSC sin rolle og virkemåte i

tilstrekkelig grad fremstår det som viktig og også inkludere en redegjørelse for deres moderetat, Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet (NSM) er Norges fagmyndighet for forebyggende nasjonal sikkerhet. Dette innebærer at de har tilsynsmyndighet vedrørende sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning (NSM, 2021b, s. 2). NSM er administrativt underlagt Justis- og beredskapsdepartementet (JD), men har et sektorovergripende ansvar for arbeid med nasjonal sikkerhet på vegne av JD og Forsvarsdepartementet (FD) (Regjeringen, 2019; Justis- og beredskapsdepartementet, 2020, s. 72).

Nasjonalt cybersikkerhetssenter (NCSC), underlagt NSM, ble etablert høsten 2019 og er et knutepunkt for informasjonsdeling, kompetanseutvikling og tverrsektorielt samarbeid. Senteret ivaretar også nasjonal responsfunksjon for alvorlige digitale angrep (Justis- og beredskapsdepartementet, 2020, s. 7, s. 8, s. 83). NCSC har blitt omtalt som et sentralt verktøy for økt samarbeid fra myndighetshold (Justis- og beredskapsdepartementet, 2020, s. 80).

Kripos NC3 som er en del av politiet ble formelt opprettet 25. januar 2019 og er et cyberkrimsenter med formål å være norske myndigheters fremste kapasitet innenfor forebygging mot og etterforskning av kriminalitet i det digitale rom (Politiet, 2021a; Justis- og beredskapsdepartementet, 2020, s. 84). Senteret er ment å være en nøkkelaktør i arbeidet med å sikre det digitale rom for befolkningen og virksomheter. I dette arbeidet skal det tilrettelegge for informasjonsdeling mellom myndighetene og det private. En viktig målsetning er å være blant de fremste aktørene innenfor deteksjon og håndtering av trusler og kriminalitet i det digitale rom, både nasjonalt og internasjonalt (Politiet, 2021a)

HelseCERT er et Computer emergency response team (CERT)* som arbeider med forebygging, overvåkning, varsling og hendelseshåndtering i helsesektoren. Gjennom dette arbeidet oppfyller de sin rolle som sektorvist responsmiljø (SRM)** for helsesektoren (NSM, 2017b, s. 2). HelseCERT drifter Nasjonalt beskyttelsesprogram for helse- og omsorgssektoren (NBP) som er en kostnadsfri tjeneste som muliggjør automatisk og kontinuerlig skanning av

systemer og tjenester for sårbarheter. Tjenesten tilbys alle aktører i helsesektoren og muliggjør også bistand fra HelseCERT til aktørene ved alvorlige IKT-sikkerhetshendelser (HelseCERT, 2021).

*CERT står for Computer emergency response team og er en gruppe personell som arbeider med forebygging, overvåkning, varsling og hendelseshåndtering innenfor IKT-sikkerhet. Det eksisterer CERTer i privat sektor og innenfor ulike sektorer i Staten. CERTer innenfor statlige sektorer utgjør sektorvise responsmiljøer (SRM). CERT er en lisenspliktig benevnelse (NSM, 2017a, s. 1)

**Sektorvise responsmiljøer er grupper med ansvar for ivaretakelse av digital sikkerhet og bistand til hendelseshåndtering til virksomheter og aktører innenfor de ulike departementenes myndighetsområder (sektorer) (NSM, 2017c, s. 7).

3.0 Teoretisk rammeverk

Det er et hurtig voksende tilfang av forskning og teoretisering på cybersikkerhetsfeltet og teorimassen preges av kontinuerlig utvikling av trusselbildet, teknologiske kapasiteter og organisering av styring (Cavelty, 2018, s. 148; Schia, 2019, s. 223-224). Den tradisjonelle forskningen på feltet har i stor grad blitt gjort innenfor tekniske disipliner som informasjonssikkerhetsutvikling og kryptografi utøvd av informatikere og ingeniører. Blant de fremste temaene disse teoretikerne har behandlet er metodologier for sårbarhetsvurderinger, sikkerhetsløsninger og botemidler mot cybertrusler på teknisk nivå (Cavelty, 2018, s. 149-151). Erkjennelsen av at sårbarheter innenfor digital infrastruktur og cyberspace også dreier seg om hvordan mennesker interagerer med teknologien har gjort at samfunnsvitenskapelig forskning på feltet har vokst frem. Samspillet mellom mennesker og teknologi har blitt omtalt som den *sosio-tekniske* tilnærmingen (Jaatun, Albrechtsen, Line, Tøndel & Longva, 2009, s. 34-35)

Innenfor statsvitenskapen har cybersikkerhet særlig blitt tematisert innenfor studier av internasjonal politikk (Langø, 2013, s. 238). Det har blitt postulert at det eksisterer tre distinkte skoler innen akademiske studier av cybersikkerhet med fokus på internasjonal politikk. Forskere tilhørende de respektive skolene kalles revolusjonister, tradisjonalister og økologer. Et sentralt element innenfor alle retningene er forståelsen av cybersikkerhet i relasjon til konflikt og makt (Langø, 2013, s. 229, s. 235-236). Disse retningene og deres kjennetegn er kun indirekte relevant for min problemstilling siden den ikke hovedsakelig omhandler mellomstatlige forhold. Min problemstilling om norske myndigheters styringssystem for hendelseshåndtering knytter seg i hovedsak til teoretiske perspektiver og tilnærminger til governance og ulike former for samarbeid. Hvordan ulike aktører samarbeider for å sikre cyberspace i praksis er kjernen av mitt prosjekt. Teoretiske perspektiver på samarbeid har vist seg å ofte være tilknyttet teorier om governance og koordineringsmekanismer (Bouckaert, Peters & Verhoest, 2010, s. 43-44; Weber & Khademian, 2008, s. 334).

I det følgende vil jeg beskrive litteraturgjennomgangen med fokus på den litteraturen som ligger tematisk nærmest kjernen i min problemstilling og dens formål. Deretter vil jeg redegjøre for de teorikonseptene jeg anser som nødvendige for å etablere et teoretisk rammeverk for analyse av samarbeid på cybersikkerhetsfeltet, særlig vedrørende hendelseshåndtering. Først behandler jeg teoretiske perspektiver om *governance* på

overordnet nivå. Deretter beskriver jeg perspektiver som gjør seg gjeldende i studier av cybersikkerhet. Avslutningsvis presenterer jeg teoretiske perspektiver som er særlig relevante for styring innenfor cybersikkerhetsfeltet i Norge. Herunder utvalgte postulater som er direkte relevante for formålet med min problemstilling – hvordan sektorbasert styring og nettverksstyring påvirker hverandre.

3.1 Litteraturgjennomgang

Majoriteten av litteraturen jeg har gjennomgått er funnet gjennom søk i Oria-portalen, Google og databasene til offentlige biblioteker. Jeg har også blitt anbefalt litteratur og kilder til informasjon av fagpersoner og informanter. Utgangspunktet for søk har vært relevans for min problemstilling og dens formål. I denne litteraturgjennomgangen presenterer jeg de teoretikerne og verkene som knytter seg tematisk tettest opp mot problemstillingen og de som har hatt størst betydning for mitt arbeid. Når det gjelder litteratur om cybersikkerhet som fagfelt har jeg bevisst søkt etter verker som omhandler cybersikkerhetspolitikk og cybersikkerhetsstyring fremfor cybersikkerhet på overordnet nivå. Denne innsnevringen har fremstått som hensiktsmessig siden den hovedsakelig har ledet meg til samfunnsvitenskapelige arbeider. Jeg har også gjennomgått litteratur av mer teknisk karakter der det har virket formålstjenlig. Antologiverket «Digital sikkerhet – en innføring» (2020) har vært et nyttig hjelpemiddel for bakgrunnsinformasjon om de tekniske aspektene ved fagfeltet.

Jakten på litteratur om styring på overordnet nivå begynte med den anerkjente teoretikeren Mark Bevir og hans perspektiver på governance. I hans antologiverk «The SAGE Handbook of Governance» (2011) er en rekke teoretikere samlet for å belyse ulike typer governance og perspektiver på dem. Dette verket fungerte som et utgangspunkt for videre lesning om governance innenfor cybersikkerhetsfeltet. En teoretiker som har arbeidet mye med governance og cybersikkerhet er Jacqueline Eggenschwiler. Hun har presentert ulike typologier av cybersikkerhetsstyring og utfordringer forbundet med disse på en oversiktlig og tydelig måte. Hennes arbeid på feltet har derfor vært retningsgivende for denne oppgaven.

Det finnes flere forskningsmiljøer som fokuserer på cybersikkerhet i Norge (SINTEF, 2021, NUPI, 2021). SINTEF har i en årrekke publisert omtaler av ny forskning på feltet, både samfunnsvitenskapelig og teknologisk. Jeg har funnet flere arbeider her som har vært gode kilder til bakgrunnsinformasjon, informasjon om hendelseshåndtering og utgangspunkt for videre lesning. De mest fremtredende er en systematisk litteraturgjennomgang om prosedyrer for håndtering av IKT-sikkerhetshendelser, en case-studie av hendelseshåndtering i

kraftsektoren og en studie av hendelseshåndtering i petroleumssektoren (Jaatun et al, 2009, s. 26; Line, 2015, s. 5; Tøndel, Line & Jaatun, 2014, s. 42). I tidsskriftet «Internasjonal politikk» utgitt av NUPI har det tidvis blitt publisert svært interessante artikler som omhandler styring og samarbeid på cybersikkerhetsfeltet. To artikler har vist seg å være særlig relevante for min problemstilling. Artikkelen «Makt og avmakt i cyberspace: hvordan styre det digitale rom?» (2016), forfattet av Lilly Pijnenburg Muller, omhandler multistakeholdermodellen i norsk kontekst med et særlig fokus på NSM sin rolle i offentlig-privat samarbeid. Mikkel Storm Jensen belyser sektorprinsippets betydning i nordiske land i artikkelen «Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer» (2019).

Gjennom mine søk har det blitt tydelig at det eksisterer litteratur om styring og samarbeid på andre politikkområder som også er relevant på cybersikkerhetsfeltet. I en undersøkelse av nettverksstyring innenfor norsk vannforvaltning har jeg funnet mange fellestrekk med cybersikkerhetsfeltet (Hanssen, Hovik & Hundere, 2014, s. 155). Et sentralt fellestrekk omhandler perspektivet om *insitusjonell lagdeling* og ulike *styringsnivåer* (Hanssen et al, 2014, s. 156). Artikkelen som denne undersøkelsen er presentert i har vært en verdifull ledesnor både for valg av teoretisk tilnærming og som kilde til postulater om styring. Det viktigste elementet i mitt prosjekt inspirert av artikkelen er fokus på hvordan tradisjonell sektorbasert styring interagerer med multistakeholdermodellen.

Det er skrevet en rekke masteroppgaver og avhandlinger om samarbeid på cybersikkerhetsfeltet. Mange av disse er forfattet av studenter innenfor samfunnssikkerhet. En masteroppgave som har klare likhetstrekk med min ble levert ved Universitetet i Stavanger av Ingrid Skjørland og Renate Thoreid i 2018. Oppgaven omhandler samvirkeprinsippet og hvordan DSB og NSM etterlever dette. Det pekes på en positiv utvikling av samvirket, men også utfordringer i samarbeidet mellom de to etatene. Deres definisjoner av samvirke og samarbeid samt grensedragningene mellom dem er direkte relevant for min problemstilling. Oppgaven skiller seg imidlertid fra min gjennom sitt fokus på to sektorovergripende aktører og forholdet mellom dem. Målet med min oppgave er å beskrive samarbeid på tvers av nivåer.

3.2 Governance

Såkalt governance-teori har blitt en viktig teoritradisjon innenfor flere fagdisipliner de senere tiår og særlig innenfor statsvitenskap (Bevir, 2011, s. 3). Governance dreier seg om styring og hvordan den utøves. Et sentralt element er at styring ikke oppfattes som bundet til hierarkier eller maktforhold, men kan utøves av et vell av forskjellige aktører på tvers av offentlig og

privat sektor (Bevir, 2012, s. 3). Aktører som yter innflytelse på styringen innenfor et politikkområde omtales gjerne som stakeholders, eller interessenter. Disse kan ha svært ulike motivasjoner og roller i styringen avhengig av hva slags organisasjon det dreier seg om. Det har blitt postulert at økende mangfold blant interessenter innenfor noen områder har vært med å drive frem nye typer organisering og former for samarbeid, herunder offentlig-privat samarbeid (Bevir, 2011, s. 2).

Noen teoretikere oppfatter grupperinger av relevante deltakere i styringen av et politikkområde som egne nettverk (Bevir, 2011, s. 3; Enroth, 2011, s. 19). Det eksisterer ulike tilnærminger til nettverk og deres betydning for styring, blant andre policy-nettverk og governance-nettverk (Sørensen & Torfing, 2011, s. 1030; Enroth, 2011, s. 19). Studier av policy-nettverk tar ofte sikte på å forklare hvordan nettverk av interessenter sammen bidrar til å utforme politikk (Enroth, 2011, s. 23). Denne tilnærmingen virker velegnet til å analysere hvordan politisk endring og utvikling inntreffer, men ikke til å beskrive hvordan nettverk gjør seg gjeldende i konkret styring av hendelseshåndtering. Governance-nettverk innebærer samarbeid mellom flere interessenter innenfor et politikkområde som bidrar til å løse en oppgave med betydning for samfunnet. Det er vanlig å betrakte felles målsetninger som en avgjørende faktor for hvorvidt en gruppe interessenter kan betraktes som et governance-nettverk (Sørensen & Tofring, 2011, s. 1030-1031). Det er en forholdsvis etablert praksis å benytte begrepet *nettverk* i betydningen governance-nettverk (Hanssen et al, 2014, s. 155; Bouckaert, Peters & Verhoest, 2010, s. 43-44). Styring gjennom nettverk fremstår som høyst anvendelig for å forstå noen typer samarbeid på cybersikkerhetsfeltet i Norge. Grunnlaget for denne oppfatningen er samarbeidet mellom myndighetsaktører og andre gjennom offentlig-private initiativer (Muller, 2014, s. 14-15). Forholdet mellom tradisjonell (hierarkisk) styring og nettverksstyring belyses ytterligere i punkt 3.9.

3.3 Cyberspace

Ethvert teoretisk rammeverk for analyse av styring på cybersikkerhetsfeltet krever en definisjon av begrepet *cyberspace*. Det finnes forskjellige måter å definere dette fenomenet på, men et gjennomgående likhetstrekk mellom definisjoner er at cyberspace er en arena som skapes gjennom kommunikasjon mellom digitale enheter (Choucri & Clark, 2012, s. 3; Langø og Sandvik, 2013, s. 221-222; Kremling & Parker, 2018, s.47). Statsviteren Nazli Choucri og informatikeren David D. Clark har utformet en detaljert definisjon av cyberspace med det globale internett som utgangspunkt. De beskriver cyberspace som et nivådelt fenomen med

fire forskjellige dimensjoner; det fysiske fundamentet, den logiske dimensjonen, informasjonsdimensjonen og brukerdimensjonen. Det fysiske fundamentet omhandler maskinvaren som gjør digital kommunikasjon mulig, herunder dataservere, fiberoptiske kabler, datamaskiner og mobiltelefoner. Den logiske dimensjonen dreier seg om programvare og digitale tekniske løsninger som kjøres på maskinvare, blant annet internett-protokoller, domener og programmer. Informasjonsdimensjonen er data som lagres, sendes og tilvirkes digitalt. Slike data kan eksempelvis være tekst, bilder eller videomateriale. Den siste dimensjonen til Choucri og Clark er brukerdimensjonen som omhandler hvordan mennesker og organisasjoner bruker teknologi til å skape opplevelsen av cyberspace. Denne dimensjonen innebefatter et bredt spekter av menneskelig atferd fra forskjellige måter å dele informasjon til utøvelse av handlinger i det digitale rom (Choucri & Clark, 2012, s. 2-3). Det fremstår som hensiktsmessig å oppfatte brukerdimensjonen som en del av grunnlaget for tanken om det sosio-tekniske aspektet ved cybersikkerhet (Jaatun et al, 2009, s. 34-35).

Det å benytte internett som utgangspunkt for forståelse av cyberspace fremstår som svært hensiktsmessig dersom man tar sikte på å analysere problemstillinger innenfor cybersikkerhet. Dette fordi de fremste og mest aktuelle digitale truslene mot personer og virksomheter oppstår gjennom tilkobling til internett (Cavelty, 2018, s. 146). Regulering og styring av cyberspace skjer på flere nivåer og teoretikere benytter gjerne paraplybegrepene *Cyber governance* og *Internet governance* i sine analyser. Felles for begge disse er at de omhandler styring og regulering av internett på teknisk og administrativt nivå (Bayuk, 2012, s. 86, s. 94-95).

3.4 Cybersikkerhet

Det er en utbredt oppfatning at cybersikkerhet må sees i sammenheng med cyber-governance, men det eksisterer ulike måter å definere begrepet på (Cavelty, 2018 s. 146-147; Bayuk, 2012, s. 1; Windvik, 2020, s. 18). En definisjon som harmonerer svært godt med NSMs klassifiseringspraksis vedrørende IKT-sikkerhetshendelser er den såkalte CIA-triaden. Den beskriver cybersikkerhet som teknologier, prosesser og prosedyrer utformet for å beskytte nettverk, datamaskiner, programvare og data fra angrep, skade eller uautorisert adgang, i tråd med allmenne mål om informasjonssikkerhet: Ivaretakelse av konfidensialitet, integritet og tilgjengelighet (NSM, 2017b, s. 1; Cavelty, 2018, s. 146; Windvik, 2020, s. 21-23). Det er verdt å merke seg at denne definisjonen tilsynelatende ikke anser internettilkobling som avgjørende for om et objekt eller mål skal anses som en del av cybersikkerhetstenkning.

Cyber-begrepet er mangefasettert og benyttes tidvis som en benevnelse som favner bredere enn andre mer presise begreper (Svenungsen, 2019, s. 2). Siden definisjonen forankret i målene om informasjonssikkerhet har blitt omtalt som gjeldende for både cybersikkerhet og *digital sikkerhet* benyttes disse begrepene om hverandre avhengig av kontekst i min analyse (Cavelty, 2018, s. 146; Windvik, 2020, s. 21). Grunnen til dette er at teoretikere og myndighetsaktører ofte bruker ulike begrepsapparat. Det er en forholdsvis etablert praksis å benytte begrepet digital sikkerhet fremfor cybersikkerhet i norsk sammenheng og det *digitale rom* brukes gjerne som benevnelse for cyberspace (Departementene, 2019, s. 6; Svenungsen, 2019, s. 2). Begrepene *datasikkerhet* og *IKT-sikkerhet* benyttes også tidvis synonymt med digital sikkerhet (Windvik, 2020, s. 18). Begrepet *IKT-sikkerhetshendelse* er det foretrukne begrepet blant flere myndighetsaktører for å beskrive uønskede hendelser i cyberspace (NSM, 2017c, s. 3; Justis- og beredskapsdepartementet, 2017, s. 66). NSM definerer IKT-sikkerhetshendelser som: «Situasjoner der IKT-systemer blir utsatt for tilsiktede handlinger» (NSM, 2017a, s. 1). Denne definisjonen favner svært bredt og vil inkludere begreper som cyberangrep, dataangrep, datainnbrudd og digitalt angrep som tidvis benyttes for å beskrive hendelser. Som følge av dette er IKT-sikkerhetshendelse det foretrukne begrepet i mine analyser.

3.5 Cybersikkerhetsstyring

Perspektivene på governance, cyberspace og cybersikkerhet danner et fundament for forståelse av styring på cybersikkerhetsfeltet. Governance i cyberspace har blitt omtalt som et fragmentert fenomen preget av et vell av aktører og ulike former for samarbeid (Bayuk, 2012, s. 4-5). Et samlebegrep som noen teoretikere benytter er *Cybersecurity governance*, heretter cybersikkerhetsstyring (Ellis & Mohan, 2019, introduksjon s. 2). Av praktiske språklige hensyn velger jeg her å benytte det norske ordet *styring* som ensbetydende med governance. Grunnlaget for dette er at jeg anser styring som et mer velegnet begrep for norske lesere i denne sammenhengen. Det er vanlig å betrakte cybersikkerhetsstyring som en underkategori av Internet Governance (Raymond & DeNardis, 2015, s. 588-589). Enkelte teoretikere er imidlertid kritiske til denne kategoriseringen på grunnlag av at den ikke bidrar til utvikling av forståelse for hvordan styring utøves digitalt i det moderne cyberspace. Kritikerne ser cybersikkerhetsstyring som et bredere og mer komplekst fenomen med vidstrakte sosiale, politiske og økonomiske implikasjoner (Eggenschwiler, 2019, s. 82-83; Ellis & Mohan, 2019, introduksjon s. 2-3). Cybersikkerhetsfeltet har også blitt omtalt som komplekst som følge av

de vidstrakte implikasjonene det har for regulering av forskjellige typer virksomheter og etater (Gundersen, 2020, s. 109-110).

Med utgangspunkt i Choucri og Clarks forståelse av cyberspace har det blitt anført at styring på cybersikkerhetsfeltet kan deles inn i tre ulike typologier av styringsformer; hierarkiske, multistakeholder-baserte og markedsbaserte (Eggenschwiler, 2018, s. 72). Den hierarkiske typologien kjennetegnes av myndighetsutøvelse og definerte kommandolinjer innenfor offentlig sektor. Multistakeholder-typologien, heretter multistakeholdermodellen, omhandler samarbeid mellom interessenter i det digitale rom på tvers av offentlig og privat sektor. Markedstypologien dreier seg om aktører og sikkerhetsløsninger tilhørende privat sektor (Eggenschwiler, 2018, s. 72-73). Disse typologiene er i det vesentlige identiske med de tre allmenne såkalte koordinasjonsmekanismene for styring i samfunnet; hierarki, nettverk og marked (Bouckaert, Peters & Verhoest, 2010, s. 6; Verhoest, Peters, Beuselinck, Meyers & Bouckaert, 2005, s. 4). I mine analyser har jeg valgt å benytte begrepet multistakeholder fremfor nettverk når jeg omtaler interaksjon mellom det offentlige og det private under hendelseshåndtering. Bakgrunnen for dette valget er at multistakeholder-begrepet fremstår som det foretrukne blant de teoretikerne innenfor cybersikkerhet som jeg har fokusert på i mitt arbeid (Eggenscwhiler, 2018, s. 73; Muller, 2016, s. 2).

Tabell 2 – Typologier av cybersikkerhetsstyring

	Hierarkisk	Marked	Multistakeholder
Problemområder	Kriser, katastrofer, problemer som kan løses gjennom myndighetsutøvelse	Rutineutfordringer, ikke sensitive problemstillinger	Komplekse og ustrukturerte multi-aktør problemer
Typer arbeid og resultater	Lover, reguleringer, kontroll, prosedyrer, tilsyn	Tjenester, produkter, frivillig samarbeid, allianser	Konsensus, avtaler, sosiale interaksjoner, prinsipper
Typiske svakheter	Ineffektivitet, tungroddhet	Ineffektivitet, markedssvikt	Uendelig kommunikasjon, manglende beslutningsdyktighet
Hovedaktører	Statlige aktører	Ikke-statlige aktører, selskaper	Statlige og ikke-statlige aktører

(Eggenschwiler, 2018, s. 72 – Oversatt)

De tre typologiene og deres egenskaper fremstår som et nyttig verktøy for å organisere aktører og typer samarbeid på cybersikkerhetsfeltet. De kan også betraktes som en slags idealtype som dokumentanalyse og analyse av intervjusvar kan utføres i lys av (Bratberg, 2018, s. 90-91). Siden min problemstilling omhandler myndighetenes styringssystem for håndtering av IKT-sikkerhetshendelser er typologiene hierarki og multistakeholdermodellen mest relevante. Aktører tilhørende markedstypologien er viktige innenfor hendelseshåndtering i Norge, men for min problemstilling er kun de virksomhetene som samarbeider med etater eller offentlige organer relevante. Disse utgjør en del av multistakeholdermodellen, og analyse av deres rolle i styringssystemet kan formodentlig anses som forankret i denne.

3.6 Sektoransvarsprinsippet

Den hierarkiske typologien inkluderer alle offentlige organiserte enheter som har en rolle innenfor arbeid med cybersikkerhet (Eggenschwiler, 2018, s. 72). Som følge av det grunnleggende utgangspunktet for styring av cybersikkerhet i Staten, *sektoransvarsprinsippet*, har alle offentlige etater og virksomheter i Norge som bruker IKT-teknologi en rolle innen cybersikkerhet og hendelseshåndtering. Sektoransvarsprinsippet, heretter sektorprinsippet, innebærer at hvert enkelt departement har ansvar for arbeid som foregår i sin sektor. Dette gjelder i forlengelsen alle organiserte enheter som er underlagt departementet (DIFI & DFØ, 2019, s. 9; Smith, 2015, s. 259). En av grunntankene som understøtter prinsippet er at hvert enkelt departement kjenner sitt politikkområde godt og følgelig er best egnet til å innføre politikk og tiltak innenfor sitt felt (Jensen, 2019, s. 268; Smith, 2015, s. 258-259). Sektorprinsippet kan oppfattes som hovedgrunnen for opprettelsen av de sektorvise responsmiljøene (SRM) som utgjør en vital del av styringssystemet for hendelseshåndtering.

Det har blitt forfektet at det å benytte sektorprinsippet som utgangspunkt for styring har noen potensielle svakheter. Blant svakhetene som har blitt påpekt er varierende grad av innsats, ulike tilnærminger til tiltaksimplementering og manglende samordning (Jensen, 2019, s. 268-269; Kaarbø, 2019, s. 2; Smith, 2015, s. 258). En postulert svakhet jeg anser som særlig relevant for cybersikkerhetsfeltet er sektorprinsippets mangler i møte med problemer som er så omfattende og komplekse at det krever *tverrsektoriell styring* for å nå målsetninger (Lie & Mydske, 2018, s. 56-57). Dette kan sees i sammenheng med såkalte *wicked problems*

som er sammensatte problemområder som ikke kan løses av enkeltsektorer eller aktører (Hanssen et al, 2014, s. 156; Rittel & Webber, 1973, s. 155). Det er flere teoretikere som anser cybersikkerhet for å være et slikt wicked problem (Clemente, 2011, s. 16; E. F. Malone & M. J. Malone, 2013, s. 170). Det faktum at det i utgangspunktet angår alle personer og organisasjoner som bruker IKT-systemer, og det mangefasetterte trusselbildet som er i konstant endring har blitt trukket frem som årsaker (Clemente, 2011, s. 15-16). Wicked problems har blitt koblet til nettverksstyring gjennom denne koordinasjonsmekanismens potensielle verdi som en løsning (Weber & Khademian, 2008, s. 334). Det fremstår som hensiktsmessig å betrakte cybersikkerhetsfeltet som et wicked problem grunnet dets kompleksitet vedrørende trusselbildet, antall brukere av cyberspace, antall ulike typer sårbarheter og den konstante utviklingen av programvare og teknologi.

3.7 Tverrsektorielt samarbeid

Etter terroranslagene mot Regjeringskvartalet og Utøya 22. juli 2011 ble samarbeid på tvers av sektorer innenfor samfunnssikkerhet og beredskap et viktig tema (NOU 2012:14, 2012, s. 76). Fenomenet ble igjen aktualisert gjennom Koronakommisjonens gjennomgang av krisehåndteringen i begynnelsen av Koronapandemien. Kommisjonen påpekte at når hver enkelt sektor fokuserer på sin egen agenda uten tilstrekkelig koordinering med andre kan det oppstå situasjoner hvor beslutninger som tas i én sektor får uventede konsekvenser i andre (NOU 2021:6, 2021, s. 214). Dette fremstår som relevant for hendelseshåndtering på cybersikkerhetsfeltet siden alvorlige og vidtrekkende IKT-sikkerhetshendelser kan ramme mange ulike aktører samtidig. Angrepet som rammet Stortinget og en rekke andre offentlige og private aktører sommeren 2020 eksemplifiserer dette (NRK, 2020). Under håndteringen av slike hendelser har felles situasjonsforståelse hos ansvarlige myndigheter blitt beskrevet som viktig (NOU 2015:13, 2015, s. 244). Opprettelsen av NCSC og deres tilrettelegging for offentlig-privat samarbeid har blitt beskrevet som styrkende for evne til å etablere slik situasjonsforståelse (Justis- og beredskapsdepartementet, 2020, s. 83).

Som følge av utfordringene forbundet med mangel på tverrsektoriell styring ble *samvirkeprinsippet* introdusert som et fjerde grunnprinsipp for arbeid med samfunnssikkerhet og beredskap ved kongelig resolusjon i 2012 (DSB, 2012, s. 5). De fire prinsippene for samfunnssikkerhet, ansvar, likhet, nærhet og samvirke benyttes av myndighetene også innenfor arbeidet med IKT-sikkerhet (NOU 2015:13, 2015, s. 61). *Ansvarsprinsippet* innebærer at den aktøren som har ansvar for et område i en normalsituasjon også har ansvar

for å håndtere uforutsette hendelser innenfor dette. *Likhetsprinsippet* betyr at struktur og organisering i krisesituasjoner skal være mest mulig lik den som gjelder under vanlige omstendigheter. *Nærhetsprinsippet* tilsier at kriser skal håndteres på lavest mulig nivå. *Samvirkeprinsippet* innebærer at alle offentlige myndigheter, virksomheter og etater plikter å arbeide for å oppnå best mulig samvirke med relevante aktører vedrørende forebygging, beredskap og krisehåndtering (Justis- og beredskapsdepartementet, 2020, s. 35).

Begrepet *samarbeid* har svært lignende betydning som begrepene *samvirke* og *samhandling*. Et definerende element er at det dreier seg om en prosess hvor aktører arbeider sammen for et bestemt mål eller formål (Skjorland & Thoreid, 2018, s. 28). Jeg velger å konsekvent benytte begrepet samarbeid i mine analyser. Grunnlaget for denne tilnærmingen er at samarbeidet som beskrives i denne oppgaven i stor grad skjer mellom sektorovergripende aktører som koordinerer og deler informasjon tverrsektorielt ved hendelseshåndtering. Denne typen samarbeid skiller seg fra samarbeid én-til-én mellom SRM-er som vil kunne oppfattes som *samvirke* i henhold til myndighetenes definisjon av begrepet. Det kan forstås som tverrsektorielt samarbeid i form av koordinering og informasjonsdeling på tvers av *alle* sektorer. Utgangspunktet for dette resonnementet er rollen Justis- og beredskapsdepartementet har for samordning og koordinering mellom sektorer. Samt NSM sin definerte rolle som ansvarlig for tverrsektoriell koordinering (NOU 2018:14, 2018, s. 26-27).

I henhold til den hierarkiske typologien av cybersikkerhetsstyring, som tverrsektorielt samarbeid kan oppfattes som del av, vil ineffektivitet kunne være en typisk svakhet. Slik ineffektivitet kan sees i sammenheng med perspektiver på ansvarsområder og ansvarsfordeling. Det har blitt postulert at kompleksitet, antallet interessenter og mangfold av ulike roller i cyberspace gjør at ansvarsfordeling innenfor ulike saksfelt kan bli uklart (Eggenschwiler, 2017, s. 7-8). Denne mekanismen kan sees i sammenheng med tidligere påpekt uklarhet om ansvarsplassering som følge av sektorprinsippets virkemåte på cybersikkerhetsfeltet i Norge (Jensen, 2019, s. 269-270). Dette kan oppfattes som en form for *fragmentert ansvarsfordeling*. Mangel på tydelig ansvarsfordeling har også blitt omtalt som grobunn for uklar rollefordeling og interessekonflikter blant myndighetsaktører (Muller, 2016, s. 17). Det fremstår som logisk å betrakte tverrsektorielt samarbeid som et virkemiddel som potensielt kan motvirke dette fenomenets negative effekter. Hvorvidt en slik sammenheng foreligger vil belyses i min analyse og diskusjon i kapittel 5 og 6.

3.8 Offentlig-privat samarbeid

Offentlig-privat samarbeid er en grunnpilar i Regjeringens strategi for digital sikkerhet (Departementene, 2019, s. 2). Innenfor teoretisering på cybersikkerhetsfeltet oppfattes gjerne slikt samarbeid som del av den tidligere omtalte multistakeholdermodellen (Multistakeholder-typologien). Modellen har blitt beskrevet som en kombinasjon av den hierarkiske typologien og markedstypologien. Den innebefatter som regel et stort antall offentlige og private interessenter (stakeholders) og interaksjon mellom disse oppfattes gjerne som tuftet på gjensidig tillit og konsensusbaserte beslutningsprosesser (Eggenschwiler, 2018, s. 73). Grunntanken bak multistakeholdermodellen er at samarbeid mellom offentlige og private aktører gir best mulig styring og sikring av aktivitet i cyberspace (Muller, 2016, s. 2). Multistakeholder-initiativer har blitt beskrevet som en neo-liberalistisk tilnærming til samarbeid med målsetning om økt effektivitet (Muller, 2016, s. 11). Norge har blitt trukket frem som et foregangsland vedrørende implementering av multistakeholder-initiativer. Dette grunnet forholdet mellom NSM og private aktører vedrørende deteksjon og varsling av IKT-sikkerhetshendelser gjennom Varslingssystem for digital infrastruktur (VDI) (Muller, 2016, s. 14-15). Norske myndigheter tilrettelegger for multistakeholder-initiativer både formelt og uformelt (Muller, 2016, s. 6). Tenkning assosiert med modellen kan oppfattes som en del av grunnlaget for opprettelsen av NCSC og økt grad av offentlig-privat samarbeid vedrørende håndtering av IKT-sikkerhetshendelser i Norge.

Det har blitt postulert at multistakeholdermodellen har betydelige svakheter grunnet maktdynamikk representert ved «maktkamp» mellom myndighetsaktører og privat sektor, og internt i Staten (Muller, 2016, s. 20). Kamp om innflytelse på cybersikkerhetsfeltet mellom det offentlige og det private har blitt beskrevet som å springe ut fra neo-liberal tankegang om frislipp av kontroll på et politikkområde med manglende tydelighet i lovgivning og regulering (Muller, 2016, s. 16). Det har også blitt anført at Staten og det privates arbeid med cybersikkerhet foregår ukoordinert (Muller, 2016, s. 18). Gjennom tidligere forskning på styringsnettverk har det blitt påpekt et spenningsforhold mellom hierarkisk koordinasjon og nettverkskoordinasjon (multistakeholder). Såkalt institusjonell lagdeling har blitt trukket frem som et perspektiv som kan forklare slike spenningsforhold. Et eksisterende institusjonelt lag, fortrinnsvis myndighetsaktører, kan dominere styringen på et felt i så stor grad at nye institusjonelle lag som er nettverksbaserte ikke fungerer så effektivt som det potensielt kunne (Hanssen et al, 2015, s. 175). De postulerte svakhetene i multistakeholdermodellen kan sees i sammenheng med dette spenningsforholdet. Som nevnt tidligere foregår det kontinuerlig

utvikling innenfor cybersikkerhetsfeltet, både hva gjelder den teknologiske siden og styringssiden. Det fremstår derfor som viktig å tolke perspektiver og postulater om utfordringer på feltet i lys av situasjonen på analysetidspunkt. Likevel virker det hensiktsmessig å benytte utvalgte postulater i mitt analysearbeid siden det kan fungere som et verktøy for å beskrive utvikling.

3.9 Hierakisk koordinering og multistakeholdermodellen

Forholdet mellom hierarkisk koordinasjon og nettverkskoordinasjon (multistakeholder) fremstår som svært relevant for styringssystemet for håndtering av IKT-sikkerhetshendelser fordi det preges av begge logikkene. Samarbeid mellom aktørene foregår horisontalt og vertikalt mellom flere nivåer i ulike spor. Samarbeid mellom sektorovergripende aktører som NSM og Kripos NC3 kan oppfattes som horisontalt-hierarkisk. Samarbeid mellom disse og SRM-ene kan betraktes som vertikalt-hierarkisk. Prosedyrer for tverrsektorielt samarbeid mellom SRM-ene som koordineres av sektorovergripende etater som NCSC kan oppfattes som vertikalt og horisontalt-hierarkisk. Både NCSC og Kripos NC3 har også til dels formaliserte former for samarbeid med virksomheter tilhørende privat sektor som kan oppfattes som vertikal-multistakeholder. Slike klassifiseringer fremstår som lite formålstjenlig siden det kan bli unødvendig komplisert når samarbeid på tvers av sektorer og mellom det offentlige og private i styringssystemet skal analyseres. Siden multistakeholder-typologien fanger opp både hierarkisk koordinering og koordinering mellom det offentlige og private i en form for nettverk fremstår det som mest hensiktsmessig å benytte multistakeholdermodellen som et paraplybegrep. Jeg velger å fortrinnsvis benytte dette begrepet i mine analyser av empiri sett i lys av multistakeholder-typologien. Når elementer i analysen dreier seg om kun statlige aktører vil jeg beskrive dem som tilhørende den *hierarkiske delen av multistakeholdermodellen*.

3.10 Håndtering av IKT-sikkerhetshendelser

Håndtering av IKT-sikkerhetshendelser har blitt definert som: «Defensive prosesser og tiltak for å detektere (avdekke) og stanse alvorlige IKT-sikkerhetshendelser, samt å gjenopprette sikker tilstand for berørte systemer, skadevurdere og skadebegrense (NSM, 2017c, s. 3). Det eksisterer fire fremtredende standarder for håndtering av IKT-sikkerhetshendelser som gjør seg gjeldende internasjonalt; International Organization for Standardization (ISO)-27035,

National Institute of Standards and Technology (NIST)-800-61, SANS Incident Handler's Handbook og European Union Agency for Cybersecurity (ENISA) Good Practice Guide for Incident Management. I en kartleggingsstudie av praksis under hendelseshåndtering gjennomført i 2014 beskrives det at det er betydningsfulle likheter mellom disse standardene (Tøndel et al, 2014, s. 43). ISO-27035-standarden har blitt omtalt som den mest omfattende og anerkjente internasjonalt (Line, 2015, s. 12). Denne standarden er oppdelt i 5 faser; Planlegge og forberede, deteksjon og varsling, vurdering og beslutning, tiltak og læring av hendelsen (Tøndel et al, 2014, s. 44). Disse elementene er alle tilstede i den fremste kilden til prosedyrer for hendelseshåndtering i Norge «Rammeverk for håndtering av IKT-sikkerhetshendelser» (2017). Samarbeid spiller en sentral rolle i det norske rammeverket siden samhandling mellom NSM og SRM-er nedfelt i det (NSM, 2017c, s. 7-8).

Det siste punktet i både ISO-27035 og Rammeverk for håndtering av IKT-sikkerhetshendelser omhandler læring av den inntrufne hendelsen (Tøndel et al, 2014, s. 44; NSM, 2017c, s. 19). Det har blitt postulert at det ofte ikke fokuseres tilstrekkelig på læring etter hendelser i virksomheter som har blitt rammet (Ahmad, Hadgkiss & Ruighaver, 2012, s. 651). En måte allmennheten kan lære om risikoen IKT-sikkerhetshendelser representerer og hvordan det er mulig å håndtere dem er gjennom åpenhet fra rammede virksomheter. Det er som regel den rammede virksomheten som treffer en beslutning om hvorvidt informasjon om en hendelse skal offentliggjøres. Det har blitt påvist bekymring blant ledere for at offentliggjøring av informasjon om hendelser kan medføre omdømmetap for deres virksomhet (Bergsjø, 2020, s. 275). Tilstedeværelse av åpenhet om IKT-sikkerhetshendelser fremstår som viktig for samfunnet og offentlighetens muligheter for å opparbeide forståelse av risikoen de representerer og i forlengelsen hvilke tiltak som bør implementeres for å styre risikoen til et akseptabelt nivå.

4.0 Metode

Metodene som er benyttet for å frembringe empiri i denne oppgaven er dokumentanalyse og semistrukturerte kvalitative intervjuer. For å belyse hendelseshåndtering i praksis benyttes løsepengeviruset som rammet Østre Toten kommune i januar 2021 som et illustrerende eksempel. I det følgende vil jeg redegjøre for valg av metode og tilnærming til datainnsamling. Jeg vil også beskrive hvordan datainnsamlingen ble gjennomført og redegjøre for avveininger jeg anser som betydningsfulle for oppgaven. Videre beskriver jeg utfordringer som har meldt seg underveis i prosjektet. Avslutningsvis kommenterer jeg validiteten og reliabiliteten i prosjektet.

4.1 Metodevalg

Samarbeid om hendelseshåndtering på cybersikkerhetsfeltet foregår mellom mange ulike aktører på ulike nivåer. Grad av formalisering av samarbeid strekker seg over et vidt spekter fra påbud hjemlet i lov til helt frivillig basis. Det foreligger en betydelig mengde dokumenter som beskriver hvordan samarbeid om hendelseshåndtering er intendert å foregå, og noe om hvordan det foregår i praksis. Dette inkluderer lover, forskrifter, stortingsmeldinger, utredninger, høringsuttalelser, standarder, rammeverk, planer, prosedyrer, rundskriv, notater, rapporter, evalueringer og skriftlig korrespondanse. På bakgrunn av alle disse tilgjengelige datakildene kom jeg frem til at dokumentanalyse er en velegnet metode for å produsere empiri som kan bidra til å besvare min problemstilling. Dokumentanalyse er også en metode jeg er komfortabel med å benytte.

Selv om IKT-sikkerhetshendelser rent teknisk rammer maskinvare, programvare og nettverk er det mennesker som sanser deres konsekvenser og treffer beslutninger under håndteringen av dem. Dette *sosio-tekniske* aspektet er en viktig del av hvordan samarbeid om hendelseshåndtering foregår i praksis (Jaatun et al, 2009, s. 34-35). På tross av alle planverk og prosedyrer er det i de aller fleste scenarier mennesker som skal omsette føringer til handling når krisen inntreffer. Hvordan ansatte med ansvar for hendelseshåndtering tenker, kommuniserer og handler fremstår derfor som svært viktig for hvordan samarbeid foregår, og i forlengelsen hvor effektivt aktører løser problemer. Dette er hovedgrunnen for mitt valg om å gjennomføre semistrukturerte intervjuer som et supplement til dokumentanalysen. Utover

dette har jeg erfart en opplevelse av økt forståelse for tematikken denne oppgaven omhandler gjennom intervjuene med informanter som arbeider med hendelseshåndtering.

4.2.0 Dokumentanalyse

Dokumentanalyse er undersøkelser av språk som er fiksert i tekst og tid (Lynggaard, 2012, s. 154). Idéanalyse er en tilnærming til slike undersøkelser som innebærer granskning av meningsbærende budskap i en tekst. Den har blitt definert som: «…kvalitativ analyse av ideers tilstedeværelse i tekst der fortolkning er en vesentlig side ved analysen (Bratberg, 2018, s. 67). Min tilnærming til dokumentanalyse harmonerer i stor grad med denne definisjonen og i min analyse har jeg brukt mye tid på å tolke meningsinnholdet som kommuniseres i ulike typer dokumenter. Jeg har også forsøkt å se meningsinnhold i et dokument i sammenheng med innhold i andre beslektede eller lignende dokumenter.

Oversikten nedenfor viser alle de dokumentbaserte kildene som har blitt analysert etter kategori. Dette innebærer at de, i varierende grad, har blitt benyttet i produksjonen av empirien. Tanken bak oversikten er å gi et innblikk i den type dokumenter som har vært viktigst under mitt arbeid. Kategorien «planverk» består av dokumenter som er utformet som strategier, tiltaksbeskrivelser, rammeverk eller instrukser som i en eller annen form etablerer plan eller prosedyre for handling. Tre særlig viktige dokumenter i analysen tilhører denne kategorien, «Nasjonal strategi for digital sikkerhet» (2019), «Tiltaksoversikt til nasjonal strategi for digital sikkerhet» (2019) og «Rammeverk for håndtering av IKT-sikkerhetshendelser» (2017). Kategorien «korrespondanse» beskriver brev og e-poster fremskaffet gjennom innsynsbegjæringer. Kategorien «andre» inkluderer ulike typer skriv og skjemaer tilegnet gjennom innsynsbegjæringer og materiale publisert på nett.

Tabell 3 – Oversikt over datagrunnlag for dokumentanalyse

	NOU-er	Meld.St	Rapporter	Planverk	Notater	Korrespondanse	Andre
Planlegging	2	3	1	3		5	3
Tilrettelegging	1	3		2		2	5
Praksis		1	3	3	2	3	5
Hendelse: Østre Toten kommune			1		2	3	1

4.2.1 Datainnsamling - Offentliggjorte dokumenter

De styrende kriteriene for søk og utvelgelse av dokumenter har vært *relevans for de utvalgte aktørenes* (NSM-NCSC, Kripos NC3, HelseCERT, Østre Toten kommune) *samarbeid med andre aktører i styringssystemet* og *håndtering av IKT-sikkerhetshendelser*. I tråd med mitt første forskningsspørsmål som omhandler myndighetenes tilrettelegging for samarbeid har dokumenter tilvirket av eller på oppdrag fra myndighetene vært den desidert viktigste kategorien av dokumenter som inngår i analysen. Utredninger (NOU-er) og stortingsmeldinger om samfunnssikkerhet og digital sikkerhet spiller en avgjørende rolle i analysen. Stortingsmeldingene i større grad enn utredningene fordi de formelt kommuniserer Regjeringens tiltak og intensjoner.

Datainnsamlingen har foregått mer eller mindre kontinuerlig gjennom hele arbeidsperioden. Jeg har gjort søk etter dokumenter i Google, oppdaget dokumenter gjennom manøvrering på nettsider og blitt tipset om dokumenter med jevne mellomrom. Etter hvert som prosjektet har skredet frem har jeg fått bedre grunnlag for å gjøre gode og presise søk. Jeg har også oppdaget nye interessante dokumenter gjennom lesning av tidligere oppdrevne dokumenter og referanser i dem. Denne tilnærmingen har blitt beskrevet som «snøballmetoden» (Lynggaard, 2012, s. 158). Jeg har ikke arbeidet med en definert tidsavgrensning under innsamlingen av dokumentene, men jeg har foretrukket dokumenter tilvirket etter innføringen av samvirkeprinsippet i 2012.

4.2.2 Datainnsamling - Innsynsbegjærte dokumenter

Jeg valgte en bred tilnærming til søk i Statens verktøy for innsyn i dokumenter fra forvaltningen, eInnsyn. Grunnen til dette var at jeg innledningsvis tenkte at det kunne være relevant informasjon i dokumenter som ikke i utgangspunktet hadde noen kobling til de utvalgte aktørene. Tilnærmingen besto i å gjennomføre søk på en rekke begreper assosiert med cybersikkerhet og tilnærmet alle aktørene som inngår i styringssystemet for hendelseshåndtering. Jeg gjorde også søk basert på ulike IKT-sikkerhetshendelser fra de senere år. Herunder angrepet på Norsk Hydro, Helse Sør-Øst RHF, Stortinget og Østre Toten kommune.

Utvelgelsen av dokumenter jeg søkte innsynsbegjæring for ble gjort etter samme kriterier som i utvelgelsen av offentliggjorte dokumenter, relevans for samarbeid og hendelseshåndtering. Jeg begjærte imidlertid også innsyn i noen dokumenter som ikke nødvendigvis svarte til kriteriene. I de fleste av disse tilfellene var årsaken til at jeg valgte å begjære innsyn at dokumentet hadde en tittel som gjorde at det fremsto som relevant for andre viktige aktører i styringssystemet eller interessant som kilde til bakgrunnsinformasjon. I noen tilfeller valgte jeg å begjære innsyn på grunnlag av hvem som var avsender eller mottaker. Noen av begjæringene jeg sendte basert på denne tankegangen viste seg å være helt irrelevante for cybersikkerhet. Jeg fikk blant annet innsyn i dokumenter om utpeking av samfunnskritiske virksomheter i forbindelse med unntaksbestemmelser fra koronaforskrifter. Dette berodde på at jeg misforsto rollen begrepet «samfunnskritisk» spilte i dokumentene. Jeg sendte totalt 122 innsynsbegjæringer fordelt på to runder med forespørsler to uker fra hverandre i tid. Jeg fikk helt eller delvis innsyn i rundt 60% av tilfellene. Alle innsynsbegjæringene er dokumentert i vedlegg 1.

4.2.3 Utfordringer

Skjerming for innsyn av interessante dokumenter har vært en utfordring i datainnsamlingsfasen av dokumentanalysen. Det er forståelig at store deler av dokumentmassen som omhandler status på sikkerheten innen IKT i offentlig forvaltning tilbakeholdes fra offentligheten. Dette var også en problemstilling jeg var klar over før jeg startet prosjektet. Vurderingen min da var at graderte og skjermingsverdige dokumenter ikke var nødvendige for å belyse problemstillingen med tilstrekkelig datagrunnlag. Det er også min vurdering nå. Min oppfatning er at manglende innsyn i enkelte dokumenter ikke svekker min dokumentanalyse vesentlig siden de dokumentene jeg har analysert fremstår som svært

troverdige og velbeskrivende for de tematiske elementene som er relevant for min problemstilling.

4.3.0 Semistrukturerte intervjuer

Semistrukturerte intervjuer gjennomføres ofte som en samtale mellom forsker og informant. Det har blitt anført at det er nødvendig å gjennomføre forarbeid for å opparbeide en grad av forståelse av tematikken intervjuet skal omhandle før det gjennomføres (Tanggaard & Brinkmann, 2012, s. 27). Det er vanlig å gjennomføre semistrukturerte intervjuer med utgangspunkt i en intervjuguide som i varierende grad er styrende for selve intervjuet (Tanggaard & Brinkmann, 2012, s. 28). Etter forberedende lesning om cybersikkerhet i Norge var jeg blitt klar over NSM sin vitale rolle innenfor hendelseshåndtering gjennom NCSC og planleggingen av de kvalitative intervjuene begynte med utforming av en intervjuguide for intervjuer med informanter fra NSM. Parallelt med dette begynte jeg å undersøke søknadsprosessen hos Norsk senter for forskningsdata (NSD). Denne prosessen skulle vise seg å være mer omfattende enn jeg antok i utgangspunktet grunnet den pågående koronapandemien.

På grunn av pandemien fremsto det som svært krevende å realisere fysiske intervjuer med informanter. Jeg besluttet derfor tidlig at intervjuene skulle gjennomføres via digital videokommunikasjon i Universitetet i Tromsøs Zoom-klient. De potensielle truslene som eksisterer i det digitale rom ble i denne sammenhengen relevante for selve gjennomføringen av prosjektet. Problemstillinger knyttet til informasjonssikkerhet og ivaretakelse av informantenes anonymitet dukket opp siden enhver maskinvare tilknyttet nettverk kan være sårbar. Jeg utformet derfor en forholdsvis detaljert datahåndteringsplan for å ivareta informasjonssikkerheten under datainnsamlingen. Planen innebar blant annet oppbevaring av opptaksfiler og gjennomføring av transkripsjon på en datamaskin uten nettverkskort. Datahåndteringsplanen og en godkjenning fra instituttledelsen om gjennomføring av digitale intervjuer ble lastet opp i NSD-søknaden sammen med annen påkrevd dokumentasjon i begynnelsen av januar 2021. Under to uker etterpå mottok jeg beskjed om at søknaden var godkjent og jeg kunne begynne å kontakte potensielle informanter.

4.3.1 Informantene

Utvelgelse av informanter ble gjort basert på undersøkelser av de viktigste aktørene innenfor håndtering av IKT-sikkerhetshendelser i Norge. Gjennom forberedende lesning var det blitt tydelig at NSM har en særegen rolle innenfor myndighetenes tilrettelegging for både tverrsektorielt samarbeid og offentlig-privat samarbeid. På grunnlag av dette valgte jeg å kontakte en leder i organisasjonen gjennom en felles bekjent og forhørte meg på telefon om de hadde mulighet til å delta med informanter. Det hadde de mulighet til og lederen satte meg i kontakt med en annen leder som tok kontakt med informantene. Grunnen til at jeg har 2 informanter fra NSM og kun 1 fra de andre utvalgte aktørene er den vitale rollen NCSC har innenfor tilrettelegging for samarbeid og koordinering ved hendelseshåndtering.

Kripos NC3 innehar en særegen rolle i styringssystemet gjennom sitt ansvar for etterforskning og påtale ved IKT-kriminalitet. Jeg var klar over dette da jeg begynte planleggingen av intervjuene, men jeg visste ikke hvor viktige de er i praksis før jeg hadde gjennomført intervjuet med Informant 5 ansatt i Østre Toten kommune. Gjennom det intervjuet forsto jeg hvor viktig Kripos NC3 sin rolle er og fikk kontakt med en ansatt hos dem gjennom en felles bekjent. Vedkommende ble informert om prosjektet og samtykket til å delta.

SRM-nivået er viktig for de enkelte sektorenes evne til god hendelseshåndtering. Derfor var det åpenbart fra begynnelsen av planleggingen at en representant for et SRM ville utgjøre en verdifull informant. Jeg vurderte på et tidspunkt å forespørre alle SRM-ene om deltakelse, men slo dette fort fra meg da jeg forsto at ved positiv tilbakemelding fra alle ville jeg endt opp med å måtte gjennomføre 15 intervjuer totalt. Gjennom undersøkelse av ulike SRM-er fremsto HelseCERT som det mest spennende grunnet den enorme sektoren de har ansvar for og den alvorlige IKT-sikkerhetshendelsen som rammet Helse Sør-Øst RHF i 2018 som de var instrumentelle i å håndtere. Jeg kontaktet HelseCERT gjennom e-postadressen de hadde publisert på sine nettsider og forespurte en informant. Jeg sendte informasjonsskrivet og kort tid etter fikk jeg et svar fra en ansatt som hadde anledning til å delta. Jeg forespurte også et annet SRM om deltakelse, men fikk aldri svar på min henvendelse.

Jeg ønsket i utgangspunktet å benytte 4 ulike illustrerende eksempler på hendelseshåndtering i praksis og intervjue en representant fra hvert av dem. Jeg fikk imidlertid avslag fra 2 av disse og måtte revurdere planen. Det ble etterhvert som prosjektet skred frem også tydelig at dette var overambisiøst med tanke på oppgavens omfang. Jeg hadde fulgt med på dataangrepet som rammet Østre Toten kommune i januar 2021 og

alvorlighetsgraden av konsekvensene var oppsiktsvekkende. Etter avslagene fra rammede virksomheter jeg hadde fått tidligere var jeg på jakt etter et illustrerende eksempel og tok kontakt med kommunen gjennom deres publiserte e-postadresse. En ansatt med kunnskap om dataangrepet hadde anledning til å stille som informant og intervjuet ble avtalt. Etter 3 avslag og ett frafall grunnet sykdom endte jeg opp med følgende informanter:

Informant 1 - Ansatt i NSM

Informant 2 - Ansatt i NSM

Informant 3 - Ansatt i Kripos NC3

Informant 4 - Ansatt i HelseCERT

Informant 5 - Ansatt i Østre Toten kommune

4.3.2 Gjennomføring av intervjuene

Intervjuene ble gjennomført via Zoom-klient for videokommunikasjon i tidsrommet mellom 18. mars og 12. mai 2021. De ble så transkribert og analysert. Alle informantene ønsket innsyn i hvordan deres svar ville bli brukt i oppgaven og sitatsjekk har blitt gjennomført med dem alle. Intervjuene med informantene fra NSM og Kripos NC3 hadde en planlagt varighet på 45 minutter. Intervjuene med informantene fra HelseCERT og Østre Toten kommune hadde planlagt varighet på 30 minutter. Alle intervjuene endte opp med å vare i over 40 minutter grunnet interessant tematikk jeg ønsket å stille oppfølgingsspørsmål til og rause informanter.

Under det første intervjuet med Informant 1 fra NSM ble det tydelig at intervjuguiden ikke var optimalt utformet. Den var for innholdsrik og flere av spørsmålene bidro i for liten grad til svar som hadde direkte relevans for problemstillingen. Dette ble imidlertid ikke ødeleggende for intervjuet siden jeg raskt innså at mange spørsmål var overflødige og fokuserte på intervjuet som en fri samtale.

I det andre intervjuet var jeg betraktelig bedre forberedt til å stille spørsmål med relevans for problemstillingen og gode oppfølgingsspørsmål. Jeg hadde understreket spørsmålene i intervjuguiden som hadde gitt interessante svar tidligere. Jeg hadde også inkludert noen nye spørsmål på grunnlag av interessante svar fra det første intervjuet.

Majoriteten av intervju 2 foregikk som en fri samtale og det var kun tidvis nødvendig å støtte seg til intervjuguiden.

Intervju 3 fikk en katastrofal start siden Zoom-klienten ikke fikk kontakt med kameraet på min datamaskin. Etter gjentatte forsøk på å løse problemet som endte med at klienten sluttet å svare besluttet jeg og Informanten å utsette intervjustart i 10 minutter. Dette var 10 meget stressende minutter hvor jeg febrilsk logget inn og startet opp et nytt møte på en annen datamaskin. Kameraet på denne maskinen viste seg å fungere og intervjuet gikk strålende helt frem til internettilkoblingen ble brutt. Dette inntraff over 40 minutter inn i intervjuet og jeg hadde fått gode svar på alle områdene jeg var interessert i. Jeg takket derfor Informanten for deltakelsen på telefon.

I det fjerde intervjuet hadde brikkene falt på plass både vedrørende utforming av intervjuguide og det tekniske oppsettet. Jeg hadde også blitt mer vant til å gjennomføre intervjuer via Zoom og var komfortabel i intervjuer-rollen. Intervjuet gikk bra uten nevneverdige utfordringer.

I likhet med intervju 4 gikk gjennomføringen av intervju 5 bra. Det var i all hovedsak en fri samtale og intervjuguiden ble kun benyttet tidvis for å sikre at de viktigste spørsmålene var blitt stilt. Intervjuet endte opp med å vare i nærmere en time grunnet mange interessante poenger som krevde oppfølgingsspørsmål.

4.3.3 Anonymisering

Anonymisering er en essensiell del av de forskningsetiske vurderingene som må foretas når kvalitative intervjuer benyttes som metode. Det å beskytte informanters identitet kan være avgjørende for tillitsforholdet som eksisterer mellom informant og forsker. Det kan imidlertid også gjøre det vanskeligere å undersøke forskningsarbeidet og vurdere resultaters gyldighet (De nasjonale forskningsetiske komiteene, 2015). Det eksisterer utfordringer forbundet med anonymisering når informanter tilhører små fag- og arbeidsmiljøer som i mitt prosjekt. Det kan være en risiko for at noen som tilhører arbeidsmiljøene til mine informanter kan sannsynliggjøre hvem noen er basert på språkbruk eller oppfatninger. Skadepotensialet som ligger i denne risikoen kan imidlertid oppfattes som mindre alvorlig siden tematikken jeg har intervjuet informantene om primært omhandler organisatoriske forhold og samarbeid. Dersom temaet hadde vært eksempelvis forhold til ledelse eller enkeltkolleger ville det potensielle skadepotensialet ved identifisering i deres krets vært mer alvorlig.

To av informantene kommuniserte at de kunne stille med fullt navn. Jeg takket for dette tilbudet men kom frem til at det mest ryddige var å anonymisere alle og unngå en form for differensiering mellom dem. Grunnlaget for denne vurderingen var at det ved identifisering av enkelte informanter kunne oppfattes som at empirien som stammet fra dem hadde en annen verdi enn de andre, dette anså jeg som uheldig. Det var noen nødvendige avveininger knyttet til grad av anonymisering som potensielt har betydning for hvordan empirien bør tolkes. Disse dreide seg om informantenes stillingsbeskrivelser og roller i sine respektive organisasjoner. Jeg vurderte om jeg skulle forsøke å anonymisere denne informasjonen i så liten grad som mulig for å danne bedre forståelse av empiriens kontekst. Det ville potensielt hevet forståelsen av informantenes svar hvis mer informasjon om disse forholdene ble inkludert. Jeg anser imidlertid hensynet til ivaretakelse av informantenes anonymitet som mer tungtveiende enn denne potensielle gevinsten.

4.3.4 Utfordringer

Planlegging, gjennomføring og etterarbeid med de kvalitative intervjuene har vært en mer tidkrevende prosess enn det jeg hadde forestilt meg da jeg begynte arbeidet med dette prosjektet. Utforming av ulike intervjuguider, kommunikasjon i mange ledd for å avtale intervjuene og transkripsjon med flere runder sitatsjekk tar tid. Avslagene fra noen av de forespurte aktørene var også en forholdsvis stor utfordring siden det førte til at jeg måtte endre prosjektet. Kombinasjonen av disse har vært utfordrende siden det har forsinket progresjonen på andre deler av oppgaven. Jeg har vært avhengig av å vite hva som inngår i informasjonsgrunnlaget for analyse før jeg har kunnet ferdigstille de andre kapitlene.

4.4 Metodiske svakheter

Kvalitative metoder som dokumentanalyse basert på idéanalyse og semistrukturerte intervjuer er forbundet med svak mulighet for generalisering av funn. Semistrukturerte intervjuer som metode vil svært ofte lide av «liten-n»-problemet og dette forsterkes når så få informanter som fem er intervjuet. Intervjuene har også begrensninger knyttet til troverdighet siden kunnskapen som utledes fra dem kun er basert på det informantene velger å formidle. Det er ikke alltid samsvar mellom hva folk sier de gjør og hva de faktisk gjør i praksis. Jeg anser imidlertid alle mine informanter som troverdige kilder til informasjon. Målsetningen med intervjuene har vært å få perspektiver og informasjon om samarbeid som ikke eksisterer i

dokumentform og dette anser jeg å ha fått. I forlengelsen av dette dukker imidlertid en annen potensiell svakhet opp. Selv om intervjuene hele tiden har vært ment å være supplerende til dokumentanalysen har det vist seg at informantenes perspektiver og kunnskap gir så mye interessant innsikt i hvordan samarbeid foregår i praksis at intervjuene utgjør en større del av informasjonsgrunnlaget for analyse enn planlagt. Dette kan gå på bekostning av den formodentlig mer allmenngyldige empirien som kan oppdrives gjennom dokumentanalyse. I tråd med mitt ønske om å gjennomføre prosjektet med en utforskende tilnærming har jeg imidlertid kommet frem til at informantenes svar fortjener den plassen de har fått i analysekapittelet.

4.5 Validitet

Validitet omhandler gyldigheten til slutningene som trekkes om et fenomen som undersøkes. Dette kan forstås som hvorvidt det som er analysert (målt) faktisk beskriver det en problemstilling omhandler (Hellevik, 1980, s. 155). I dette tilfellet vil graden av validitet avhenge av hvordan de utvalgte dokumentene i dokumentanalysen og analysen av dem, samt svarene fra informantene er egnet til å gi reell kunnskap om hvordan samarbeid i styringssystemet fungerer. Dette vil formodentlig avhenge av flere faktorer som dokumentene og informantenes troverdighet, informantenes representativitet for sine roller, dokumentenes representativitet for fenomenet de benyttes for å analysere og både dokumenter og informanters relevans for hvordan samarbeid faktisk fungerer.

En utfordring knyttet til validiteten i denne oppgaven er begrepet «fungerer» som benyttes i problemstillingen. Siden begrepet kan forstås som både deskriptivt og normativt avhengig av konteksten det benyttes i må min analyse forstås utfra informasjonen som analyseres og dens kontekst. Dette er en utfordring for validiteten men en styrke for grad av åpenhet og frihet i analyse, diskusjon og konklusjon. Jeg verdsetter de sistnevnte elementene høyt og tror ikke validiteten blir alvorlig skadelidende som følge av tolkningsbehovet som begrepet «fungerer» frembringer. Det viktigste grepet jeg har implementert for å oppnå god validitet er grundighet i mitt arbeid med dokumentutvelgelse og utforming av intervjuguider.

4.6 Reliabilitet

Reliabilitet dreier seg om påliteligheten til en vitenskapelig studie. Dersom ulike undersøkelser fører til lignende konklusjoner vil høy grad av reliabilitet være oppnådd. Stor

grad av nøyaktighet under arbeid med vitenskapelige undersøkelser bidrar til høy reliabilitet (Hellevik, 1980, s. 155). I kvalitativ forskning som dokumentanalyse basert på idéanalyse og semistrukturerte intervjuer vil høy grad av reliabilitet være vanskelig å oppnå. I denne oppgaven fungerer multistakeholder-typologien som en form for idealtype og styringssystemet for hendelseshåndtering undersøkes i lys av den. Denne tilnærmingen har blitt beskrevet som en form for deduktiv idéanalyse. Grad av reliabilitet som kan oppnås med tilnærmingen har blitt beskrevet som avhengig av kriteriene som er benyttet og hvordan analyse gjennomføres (Bratberg, 2018, s. 90-91). Mine to kriterier for dokumentutvelgelse er bevisst formulert åpne for å muliggjøre oppdagelse av typer dokumenter og tematikk jeg ikke nødvendigvis har vært klar over på søketidspunkt. Dette vil sannsynligvis kunne oppfattes som svekkende for reliabiliteten i prosjektet.

Dersom multistakeholder-typologien hadde blitt fremholdt som en idealtype i snever forstand og samarbeid i styringssystemet for hendelseshåndtering som et fenomen avgrenset til å gjelde noen definerte parametere kunne potensielt høyere grad av reliabilitet blitt oppnådd. Dette ville imidlertid krevd en betraktelig mer stringent tilnærming til både dokumentanalysen og intervjuene som jeg ser det som sannsynlig at ville gått på bekostning av den åpne og utforskende tilnærmingen til samarbeid jeg har ønsket å benytte.

5.0 Analyse

Hvordan aktørene i styringssystemet for håndtering av IKT-sikkerhetshendelser i Norge samarbeider har vært den tematiske kjernen i min datainnsamling. I det følgende vil jeg presentere empiri fra dokumentanalysen og analysen av de semistrukturerte intervjuene. Jeg har valgt å presentere dataene sortert etter hvilken tematikk de omhandler. Grunnlaget for dette er den nevnte bruken av intervjuene som supplerende til dokumentanalysen. Presentasjonen er delt inn i tre tematiske kategorier utformet på grunnlag av problemstillingen og formålet med oppgaven. Disse er *planlegging* for samarbeid, *tilrettelegging* for samarbeid og samarbeid om *hendelseshåndtering i praksis*. Siden problemstillingen omhandler hvordan samarbeid i styringssystemet fungerer fremstår myndighetenes planlegging som et godt utgangspunkt for analysen. Det første forskningsspørsmålet dreier seg om tilrettelegging og dette kan oppfattes som planlegging implementert gjennom tiltak og prosedyrer. Praksis dreier seg om hvordan samarbeid om hendelseshåndtering faktisk foregår når en IKT-sikkerhetshendelse inntreffer.

Utvelgelsen av data har vært styrt av relevans for problemstillingen og forskningsspørsmålene. I kapittelet blir materialet presentert og fortløpende drøftet i lys av teori og problemstilling. Tre dokumenter har vist seg å være særlig relevante for problemstilling og formål, og spiller følgelig en sentral rolle i denne analysen. Dette gjelder «Nasjonal strategi for digital sikkerhet» (2019), «Tiltaksoversikt til nasjonal strategi for digital sikkerhet» (2019) og «Rammeverk for håndtering av IKT-sikkerhetshendelser» (2017) med vedlegg.

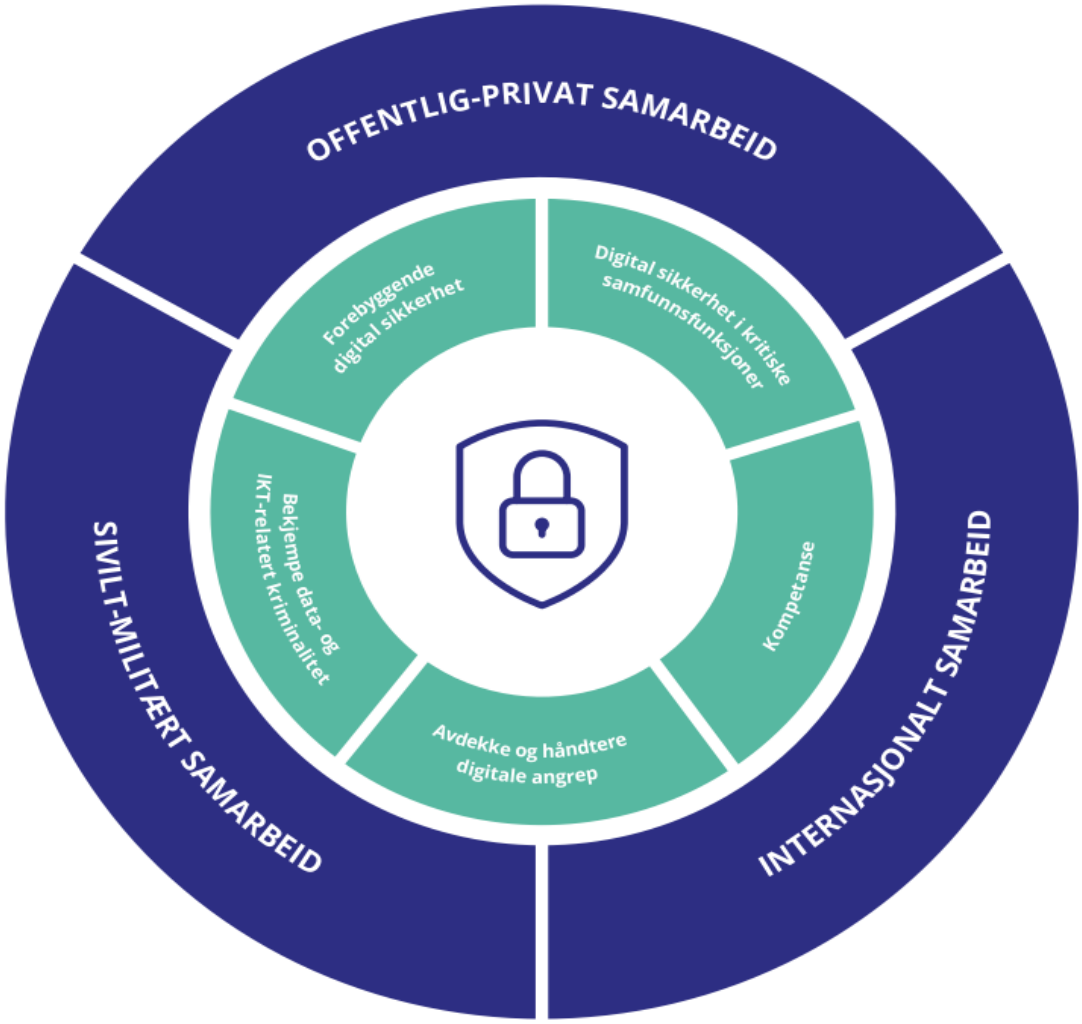
5.1 Planlegging for samarbeid

For å kunne oppnå forståelse av hvordan samarbeid i styringssystemet fungerer i henhold til intensjon er det viktig å forstå myndighetenes planlegging for tverrsektorielt og offentlig-privat samarbeid (multistakeholdermodellen). På overordnet nivå er myndighetenes strategi for oppnåelse av digital sikkerhet i samfunnet en tilsynelatende god indikator på dette. Gjennom analyse av strategien og følgedokumentet «Tiltaksoversikt til nasjonal strategi for digital sikkerhet» (2019) har jeg kartlagt myndighetenes planlegging og tilrettelegging for samarbeid om hendelseshåndtering. Nasjonal strategi for digital sikkerhet og tiltaksoversikten ble publisert av Departementene samlet i 2019. De er et resultat av en strategiprosess som har

foregått som et samarbeid mellom en rekke deltakere fra det offentlig og det private (Departementene, 2019a, forord). Kostnadsrammen for implementering av alle tiltakene som presenteres i dokumentene er anslått å være omkring 1,6 milliarder NOK over fire år (Justis- og beredskapsdepartementet, 2020, s. 82). Dette kan oppfattes som en betydelig satsning på opprustning av samfunnets evne til å forebygge og håndtere IKT-sikkerhetshendelser. Strategien retter seg mot aktører i offentlig og privat sektor, og omhandler digital sikkerhet i svært bred forstand. I tråd med sine sektorovergripende koordinasjonsroller har Justis- og beredskapsdepartementet (JD) og Forsvarsdepartementet (FD) ansvaret for oppfølging av strategien og tiltak (Departementene, 2019b, s. 1). Denne oppfølgingen foregår blant annet gjennom omfattende rapportering fra departementer og underliggende virksomheter til JD og FD (Helse- og omsorgsdepartementet, 2021; Arbeids- og sosialdepartementet, 2021; Kommunal- og moderniseringsdepartementet, 2021).

Offentlig-privat samarbeid er en essensiell del av strategien og er nedfelt i kjernen av myndighetenes strategiske tilnærming (Departementene, 2019a, s. 9). Dette er velillustrert i den såkalte plakaten for nasjonal strategi for digital sikkerhet som er inkludert i dokumentet og presentert under. Det er verdt å merke seg at begrepet *tverrsektorielt samarbeid* ikke benyttes i plakaten. Min analyse av dokumentet sett i sammenheng med analyse av utredninger og stortingsmeldinger før og etter publisering av strategien tilsier at myndighetene oppfatter tverrsektorielt samarbeid som en så naturlig del av arbeidet med digital sikkerhet at det ikke anses som nødvendig å inkludere det som en egen bolk i plakaten. Grunnlaget for denne analysen er det omfattende arbeidet som er gjort for å bedre tverrsektorielt samarbeid over tid og det massive fokuset på temaet i utredninger og stortingsmeldinger. (NOU 2015:13, 2015, s. 106, s. 238, s. 243; NOU 2018:14, 2018, s. 12, s. 15, s. 25; Justis- og beredskapsdepartementet, 2020, s. 8, s. 16, s. 72, s. 80). Det er imidlertid interessant at begrepet ikke inkluderes i plakaten med tanke på de ovennevnte elementene. Plakaten er gjengitt under:

Figur 5 – Plakat: Nasjonal strategi for digital sikkerhet.



(Departementene, 2019a, s. 11)

Myndighetene redegjør for grunnlaget for den sterke prioriteringen av offentlig-privat samarbeid og viktigheten av tverrsektoriell tenkning på flere nivåer på følgende vis:

> God digital sikkerhet er imidlertid ikke en målsetting myndighetene kan nå alene. Næringslivet har kompetansen og ressursene, og er en driver for digitalisering og innovasjon. Næringslivet er derfor en sentral del av løsningen. For å beskytte det digitale samfunnet må privatpersoner, virksomheter, sektorer og nasjoner se utover seg selv. Alle virksomheter har et ansvar for å ivareta sin egen digitale sikkerhet, men samfunnets

> digitale avhengighet gjør det nødvendig med et styrket samarbeid og partnerskap både internasjonalt og på tvers av samfunnet. (Departementene, 2019a, s. 9)

Disse betraktningene fremstår som en beskrivelse av myndighetenes overordnede tilnærming til samarbeid om oppnåelse av digital sikkerhet og i forlengelsen håndtering av IKT-sikkerhetshendelser. Næringslivets betydning trekkes frem sammen med andre sentrale aktører i samfunnet og internasjonalt. Sentimentet som utdraget tilkjennegir virker å være preget av verdsettelse av samarbeid utover det tverrsektorielle og offentlig-private siden aktører helt ned på individnivå nevnes. Dette harmonerer tilsynelatende svært godt med grunntanken bak multistakeholdermodellen som er at samarbeid på tvers av det offentlige og private gir best mulig styring og sikring av cyberspace (Muller, 2016, s. 2).

Punkt 3.4 i myndighetenes strategi omhandler hendelseshåndtering og inkluderer ett overordnet mål og seks delmål. Det overordnede målet lyder som følger: «Samfunnet har en bedre evne til å avdekke og håndtere digitale angrep.» (Departementene, 2019a, s. 19). I beskrivelsen av målet trekkes ansvarsprinsippet frem som det styrende for arbeidet med digital sikkerhet på følgende vis: «Det innebærer at virksomheter som har ansvaret i en normalsituasjon, også har ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser» (Departementene, 2019a, s. 19). Denne formuleringen harmonerer svært godt med ansvarsprinsippet og i forlengelsen sektorprinsippet. Betydningen av godt samarbeid understrekes imidlertid også i samme avsnitt på denne måten: «Det må være tilstrekkelig koordinering, samarbeid og deling av informasjon mellom sentrale aktører som har ansvar for å avdekke og håndtere alvorlige digitale angrep.» (Departementene, 2019a, s. 19). Denne formuleringen omhandler tilsynelatende samarbeid mellom aktører i styringssystemet for hendelseshåndtering og ikke en tenkt rammet virksomhet. Inkluderingen av den i beskrivelsen av det overordnete målet signaliserer at myndighetene verdsetter evne til helhetlig situasjonsforståelse blant de sektorovergripende aktørene. Dette inntrykket harmonerer godt med myndighetenes redegjørelser i Stortingsmeldinger også (Justis- og beredskapsdepartementet, 2017, s. 32; Justis og beredskapsdepartementet, 2020, s. 83).

Tverrsektoriell tenkning kommer til uttrykk i to av de seks delmålene. Delmål 1 lyder som følger: «Norske virksomheter tar ansvar for å håndtere digitale angrep i egen virksomhet, og for å dele informasjon om disse til myndighetene og andre relevante aktører.» (Departementene, 2019a, s. 19). Dette kan tolkes som et krav om informasjonseling med sikte på å bedre evne til forebygging av nye hendelser. Ordlyden i delmål 4 befester dette

inntrykket og lyder som følger: «Myndighetene legger til rette for informasjonsdeling og erfaringsoverføring mellom relevante aktører i samfunnet for å avdekke og håndtere alvorlige digitale angrep.» (Departementene, 2019a, s. 19). NCSC og Kripos NC3 har blitt trukket frem som sentrale aktører i slik tilrettelegging (Justis- og beredskapsdepartementet, 2020, s. 84).

5.2.0 Tilrettelegging for samarbeid

Tilrettelegging for tverrsektorielt og offentlig-privat samarbeid forstås her som ordninger og prosedyrer som er implementert for å legge til rette for samarbeid. Hvordan politikk og tiltak implementeres kan oppfattes å ha stor betydning for hvordan aktører i styringssystemet evner å håndtere IKT-sikkerhetshendelser. Informantenes verdsettelse av etablerte kommunikasjonskanaler og relasjoner understøtter dette resonnementet. Delmål 4 i kapittelet om hendelseshåndtering i myndighetenes strategi omhandler tilrettelegging for samarbeid og lyder som følger: «Myndighetene legger til rette for informasjonsdeling og erfaringsoverføring mellom relevante aktører i samfunnet for å avdekke og håndtere alvorlige digitale angrep.» (Departementene, 2019a, s. 19). Sett i lys av det tidligere beskrevne fokuset på offentlig-privat samarbeid og den generelle prioriteringen av tverrsektorielt samarbeid fremstår det som tydelig at relevante aktører her innebefatter alle aktører i styringssystemet for hendelseshåndtering. Tilrettelegging for offentlig-privat samarbeid nevnes også gjentatte ganger både i strategien og tiltaksoversikten. NCSC er utpekt som den viktigste aktøren for gjennomføring av slike multistakeholder-initiativer (Departementene, 2019a, s. 22; Departementene, 2019b, s. 10, s. 27).

I tiltaksoversikten som er publisert sammen med strategien presenteres 51 tiltak og 10 anbefalinger. Blant de mest omfattende tiltakene som også har en prominent plassering på listen er opprettelsen av NCSC og Kripos NC3. Om NCSC opplyses følgende: «Senteret skal styrke samarbeidet mellom de ulike IKT-sikkerhetsmiljøene slik at ulike aktører opererer i et felles risikobilde og med samme situasjonsforståelse. Etableringen er et viktig steg i videreutviklingen av det privat-offentlige samarbeidet innenfor IKT-sikkerhetsområdet.» (Departementene, 2019b, s. 10). Fokus på felles risikobilde og situasjonsforståelse ble trukket frem av begge informantene ansatt i NSM og omtalt som viktig. Begge NSM-informantene omtalte også etablerte relasjoner til andre i styringssystemet som en styrke vedrørende god kommunikasjon.

I tiltakspunktet som beskriver opprettelsen av NCSC kommenterer myndighetene også koordinering mellom NCSC og Kripos NC3. Det opplyses følgende: «For å sikre tydelig

ansvars- og rollefordeling er det viktig med et godt samarbeid mellom det nasjonale cybersikkerhetssenteret og politiets NC3-senter (se tiltak 4) for best mulig utnyttelse av samfunnets ressurser på området.» (Departementene, 2019b, s. 10). Begge informantene fra NSM beskriver samarbeidet med Kripos NC3 som godt. Informant 3 fra Kripos NC3 omtaler samarbeidet i positivt ordelag og kommenterer det slik: «Det funksjonelle samarbeidet er godt og samarbeid på ledernivå er også godt.» (Informant 3). Informant 2 trekker frem løsepengevirussaker som et saksfelt hvor det foregår koordinering mellom NCSC og Kripos NC3.

> Vi får mange løsepengevirussaker inn til oss. Disse blir videreformidlet til Kripos, men vi kartlegger de og gjør en vurdering ut fra vårt mandat. Er det noe spesielt med saken? Hvilken metode er benyttet? Hvilken virksomhet er rammet? Finnes det koblinger til andre saker vi jobber med? Ser vi noe som gjør at vi bør gå ut med et forebyggende varsel? (Informant 2)

Utfra Informant 2 sin beskrivelse kan det utledes at koordinering av innsats i løsepengevirussaker ikke er særlig utfordrende. Det virker også som at NCSC etterstreber å analysere hendelsers relevans for samfunnet. Informant 3 kommenterer at koordinasjonsarbeidet på området «fungerer stadig bedre». Vedkommende opplyser også at løsepengevirus er et voksende problem og at det er en kompleks og sammensatt type kriminalitet som i realiteten er fire lovbrudd i ett. Det er et innbrudd når en truende aktør tar seg inn i et system, skadeverk når de krypterer filer, tyveri når informasjon eksfiltreres og utpressing når det sendes krav om løsepenger. Informant 1 opplyser om samarbeid med Kripos NC3 som bidrar til å finne den beste kompetansen for en gitt problemstilling:

> …Ofte så finner vi ut at det sammen og velger den som har best kompetanse, kapasitet og er i stand til å utføre arbeidet. Slik kan vi benytte hverandre som hjelp. Kanskje har ikke vi den beste kompetansen og kunnskapen på dette området, kanskje ligger det hos en NCSC partner, SRM eller Kripos istedenfor, og da kan vi benytte hverandre. (Informant 1)

Informant 1 sin beskrivelse vitner om en form for koordinering av ressurser mellom etater gjennom ansvarsfordeling basert på en kartlegging av kompetanse. Dette harmonerer godt med myndighetenes intensjon om «best mulig utnyttelse av samfunnets ressurser på området» (Departementene, 2019b, s. 10). Informant 3 nevnte også ressursbruk som en faktor som har betydning for koordinering under hendelseshåndtering.

Kripos NC3 har en særegen rolle innenfor hendelseshåndtering grunnet sin politimyndighet og ansvar for etterforskning og påtale av IKT-kriminalitet (Justis- og beredskapsdepartementet, 2020, s. 84). Informant 3 beskriver politiets rolle i det digitale rom og Kripos NC3s posisjon i etaten slik:

> Politiet har et ansvar i det digitale rom som sammenfaller med det fysiske rom, men vi er fortsatt ikke på den kapasiteten vi skal ha for å håndtere det digitale domenet. Nå er det ikke kapasitet til å håndtere all den kriminaliteten som vi skulle ønske oss på noe område egentlig. Men vi skal i hvert fall opp på et nivå hvor ikke denne delen av kriminalitetsbekjempelsen skiller seg ut med underkapasitet. Og det er jo satsingen på NC3 som er politiets hovedsatsning. (Informant 3)

Det kan utfra dette utledes at informanten har en oppfatning av at politiet tidligere ikke har hatt tilstrekkelig tilstedeværelse i det digitale rom. Vedkommende beskriver også en tydelig målsetning om kapasitetsheving. Videre beskriver informanten cyberkrimsenterets rolle i styringssystemet for håndtering av IKT-sikkerhetshendelser slik:

> Det kan være lett for alle å huske at det er bare vi som etterforsker og hva det innebærer å etterforske noe. Da assisterer politiet påtalemyndigheten med å sikre spor og bevis og bygge sak. Og vi er da Riksadvokatens verktøy i Norge til å bygge sak som har med alvorlig kriminalitet å gjøre, sånn forenklet sagt. Og det er et helt eget fag som man ikke lærer om man har greie på cybersikkerhet eller kan noe om det vi kaller cyber-forensics, eller nettverks-forensics, eller device-forensics. (Informant 3)

Informanten redegjør her for Kripos' mandat og understreker viktigheten av Kripos NC3s kombinasjon av politifaglig og juridisk kompetanse og teknisk cyberkompetanse. I

forlengelsen av redegjørelsen for løsepengevirussaker utdyper Informant 3 betydningen av NC3 sin rolle:

> Det krever jo da en kompetanse, både til å forstå det og til å forebygge det og til å iretteføre eller etterforske om du vil. Slik virksomhet som det er det bare politiet som har og kommer til å ha fremover. Andre aktører er i stand til å beskrive problemet slik de ser det, avhengig av hva slags systemer som kan fortelle om nettaktiviteten. Men modus operandi på de kriminelle det finner du ikke noe fornuftig ut av annet enn i generelle termer, med mindre du faktisk etterforsker for da finner du jo for hvert trinn i etterforskningen så lærer du mer om hvordan denne typen kriminalitet gjennomføres og man får current og relevant informasjon som kan brukes ut i forebygging. Man kan gå inn med mer spisset, målrettet forebygging enn den generelle. (Informant 3)

Utfra disse betraktningene kan det tolkes at informasjon om trusler som fremskaffes gjennom etterforskning i regi av NC3 kan spres til relevante aktører i styringssystemet og bidra til utvikling av mer effektive sikringstiltak. Dette vil i forlengelsen formodentlig gjøre aktørene bedre skikket til å håndtere lignende hendelser som de NC3 tidligere har etterforsket. Informanten understreker også at politiet har en særegen rolle som gjør dem i stand til å produsere nyttig etterretning om cyberkriminalitet. Informanten kommenterer senere i intervjuet at Kripos NC3 er opptatt av å bidra til økt kunnskap om kriminalitet i det digitale rom og mer presis begrepsbruk. Vedkommende formulerer det som følger:

> Vi prøver jo å bringe inn litt annet språk i dette. Vi snakker jo om bankran, det er jo lite av det om dagen, men det var ikke bankangrep. Bare å få språket til å harmonisere litt med resten av den kriminelle virkeligheten og at dette er en utvikling innenfor kriminaliteten. Det er ikke sånn at med cyber så begynte de kriminelle å drive med angrep hele tiden. Vi ser at datainnbrudd som begrep sakte men sikkert begynne å krype frem og det er viktig. Fordi det er viktig å få frem at dette er kriminelt først og fremst. Ikke først og fremst at det er noe truende og farlig. (Informant 3)

Disse betraktningene er interessante sett i lys av hvordan både teoretikere og den gjengse borger oppfatter IKT-sikkerhetshendelser. Hendelser omtales svært ofte som *angrep* og ikke

de mer presise begrepene *datainnbrudd* eller *dataskadeverk*. Fokuset på en form for normalisering av IKT-sikkerhetshendelser som lignende annen kriminell virksomhet harmonerer godt med Kripos NC3 sin målsetning om å gjøre politiet i stand til å fylle samme rolle i det digitale rom som i det fysiske. Etablering av felles begrepsapparat mellom aktører kan oppfattes som et ledd i forbedring av utgangspunkt for samarbeid. Dersom det anlegges en vid definisjon av begrepet *situasjonsforståelse* kan felles begrepsapparat også tolkes som noe som styrker den felles situasjonsforståelsen mellom aktører. Manglende grad av felles situasjonsforståelse har blitt omtalt som en svakhet ved sektorprinsippet (Jensen, 2019, s. 269-270).

5.2.1 Tilrettelegging gjennom NCSC

Varslingssystem for digital infrastruktur (VDI) er et viktig system i NCSCs operative arbeid og et sentralt element i både offentlig-privat samarbeid og samarbeid med myndighetsorganer (Justis- og beredskapsdepartementet, 2016b, s. 34; Justis- og beredskapsdepartementet, 2020, s. 34). Systemet fungerer gjennom at sensorer utplassert hos både offentlige og private virksomheter overvåker nettverkstrafikk og gir NCSC melding hvis unormal eller uønsket aktivitet inntreffer (Justis- og beredskapsdepartementet, 2016b, s. 24; Informant 1). NSM opplyser følgende på sine nettsider om kriterier for medlemskap i VDI: «Kriteriene for å bli medlem er at virksomheten er underlagt sikkerhetsloven, pekt ut som en Grunnleggende nasjonal funksjon (GNF) av sin tilhørende departement, tilhører en prioritert sektor eller av andre årsaker kan sees på som samfunnsviktige» (NSM, 2020). Det opplyses også at NSM ikke offentliggjør identiteten til medlemmer med mindre de samtykker til dette. Siden medlemslistene i utgangspunktet er skjermet fra offentligheten er det vanskelig å analysere hvordan NSM tolker kriteriene og beslutter hvem som slippes inn i ordningen. Det er imidlertid meget sannsynlig at en rekke bedrifter er medlem gjennom sin rettsstilling i henhold til sikkerhetsloven og potensielt en vurdering av dem som «samfunnsviktige» (Sikkerhetsloven, 2018, §1-3; DSB, 2020c, s. 22).

Beskrivelser av VDI i en NOU og meldinger til Stortinget indikerer også at en rekke private bedrifter er medlemmer (Justis- og beredskapsdepartementet, 2016b, s. 34; Justis- og beredskapsdepartementet, 2020, s. 34; NOU 2016:19, 2016, s. 125). En beskrivelse av forholdet mellom VDI-medlemmer og NSM foreligger i NOU 2016:19 - Samhandling for sikkerhet:

> Tilknytning til VDI er basert på frivillighet og tilbys etter en nærmere vurdering av virksomhetenes betydning for kritisk infrastruktur. NSM inngår en avtale med den enkelte deltaker, hvor partenes rettigheter og plikter i samarbeidet er nærmere regulert. Private virksomheter som deltar i VDI-samarbeidet, forplikter seg gjennom avtalen med NSM til å bidra til finansieringen av VDI og NorCERT gjennom et årlig vederlag. (NOU 2016:19, 2016, s. 125)

Som nevnt i teorikapittelet har VDI-ordningen blitt trukket frem som et eksempel på multistakeholder-samarbeid som er unikt grunnet den store graden av gjensidig tillit mellom det offentlige og det private som kreves for at slikt samarbeid skal fungere (Muller, 2016, s. 14). Når VDI-sensorer installeres hos en bedrift får myndighetene representert ved NSM tilgang til deres nettverkstrafikk og følgelig mulighet til å overvåke den for å detektere uønsket aktivitet. Det gir dem imidlertid også en hypotetisk mulighet til å overvåke innholdet i trafikken som for noen bedrifter vil kunne oppfattes som lite ønskelig. Grunnlaget for slik tankegang kan eksempelvis være ønske om vern av bedriftshemmeligheter, sensitiv informasjon om kunder eller klienter og potensielt frykt for oppdagelse av lovbrudd. NSM er tilsynelatende klar over denne problemstillingen og har publisert følgende beskrivelse av temaet på sine nettsider:

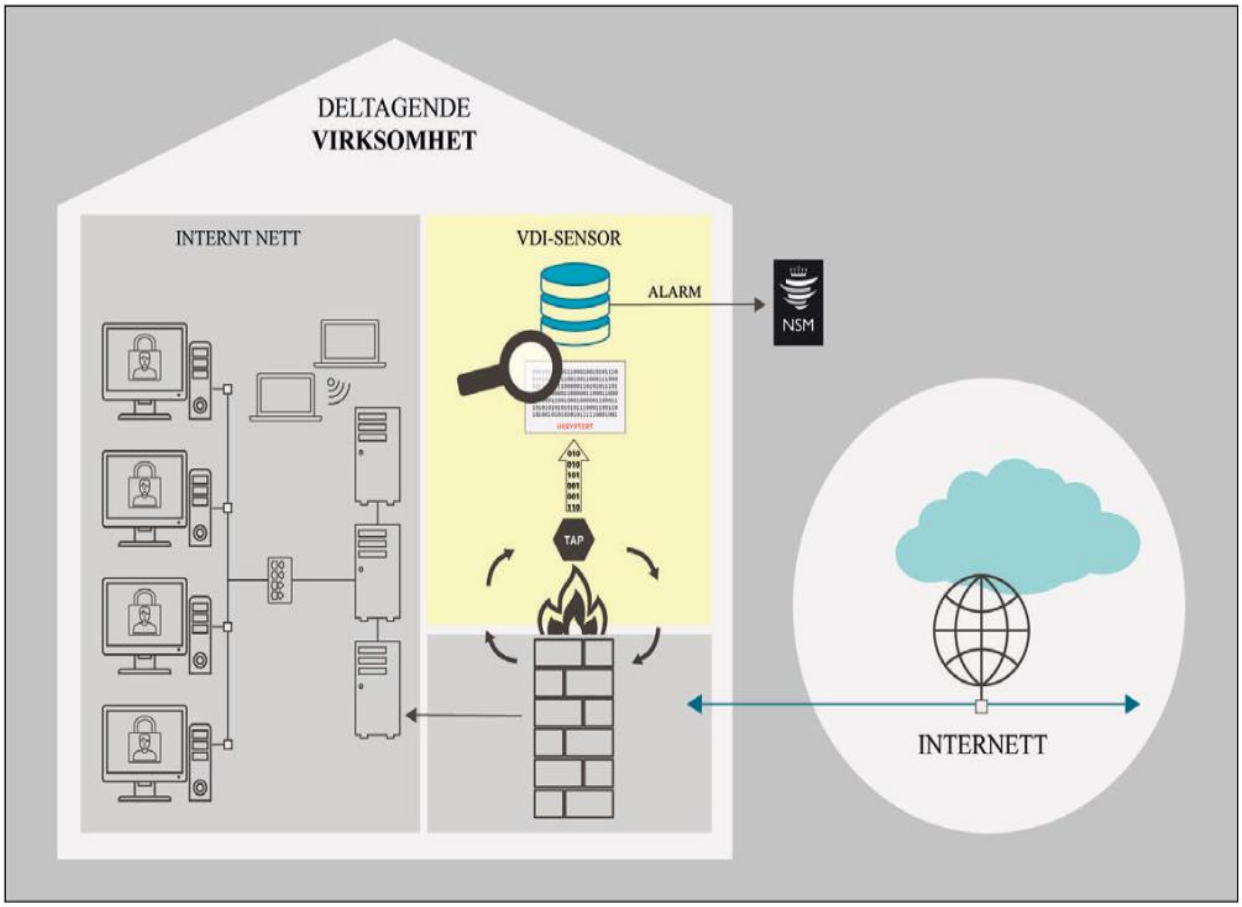
> VDI-samarbeidet er i stor grad basert åpenhet og tillit mellom NSM og deltagende bedrifter og etater. For den enkelte bedrift/etat er trafikkmengde, sikkerhetsmekanismer og fiendtlig aktivitet i egne datanettverk konfidensiell informasjon. Derfor blir også data fra VDI-sensorene behandlet konfidensielt. (NSM, 2020)

Denne redegjørelsen kan potensielt ha en beroligende virkning for noen bedrifter som vurderer om de skal søke VDI-medlemskap. Informant 2 tenker at NCSC sin rolle som sivil myndighet som skal skadebegrense bidrar til at de får tillit fra privat næringsliv.

Informant 1 beskriver VDI som en «digital innbruddsalarm» og opplyser at de varsler virksomheter som er medlemmer hvis de oppdager mistenkelig aktivitet på deres sensor. Videre opplyses det at det oppdages en stor andel interessant trafikk og at det årlig sendes ut over 100 varsler. Dette inkluderer imidlertid også sårbarhetsvarsler, forebyggende meldinger og redegjørelser for trender. I 2018 registrerte NSM rundt 20000 alarmer om såkalte IKT-

hendelser og omkring 5000 av disse ble videre undersøkt (NSM, 2019, s. 10). Det fremstår som hensiktsmessig å her forstå begrepet *hendelse* som *interessant aktivitet som plukkes opp av sensorer*. Sett i lys av opplysningene fra informanten kan det utledes at det er en liten andel av den totale interessante aktiviteten som oppdages som fører til varsling av et VDI-medlem.

Figur 6 – Varslingssystem for digital infrastruktur



(Sylstad, NSM – Gjengitt fra Justis og beredskapsdepartementet, 2016a, s. 29).

Denne figuren fremstår som en god visuell fremstilling av hvordan VDI fungerer. Medlemsvirksomheten, her representert ved huset, har sin egen brannmur og VDI-sensoren installert for å fange opp all trafikk som kommer inn til nettverket fra internett og skybaserte tjenester. Sensoren fungerer ved å analysere trafikken og utløse alarm til NSM (NCSC) dersom noe unormalt eller uønsket oppdages.

Det har blitt besluttet at VDI skal oppgraderes. Oppgraderingen vil gi NSM ny analysefunksjonalitet som potensielt kan øke deres slagkraft og kapasitet vedrørende

hendelseshåndtering (Departementene, 2019b, s. 8; Justis- og beredskapsdepartementet, 2016b, s. 65). Oppgraderingen beskrives slik i Meld. St. 5 (2020-2021):

> Dagens varslingssystem for digital infrastruktur (VDI) har blitt brukt til å oppdage målrettede digitale angrep i snart 20 år. Nasjonal sikkerhetsmyndighet utvikler nå ny sensorteknologi som skal bygge videre på og erstatte dagens VDI-sensorer. Det skal utvikles en ny plattform som skal ta i bruk kunstig intelligens og maskinlæring på de dataene som samles inn. Plattformen skal gi mulighet for automatisk analyse av skadevare som oppdages, og automatisk deling av resultater. (Justis- og beredskapsdepartementet, 2020, s. 84)

Den positive omtalen av VDI og satsningen på oppgradering indikerer at myndighetene anser systemet som en viktig brikke i samfunnets evne til å oppdage og håndtere IKT-sikkerhetshendelser. Dette inntrykket befestes ytterligere gjennom den betydelige budsjettposten oppgradering av VDI representerer. Informant 2 opplyser at det er budsjettert for kostnader opp mot 500 millioner NOK i oppgraderingsarbeidet. Denne betydningsfulle investeringen kan tolkes som en bekreftelse av myndighetenes oppfatning av cybersikkerhetsfeltet som en prioritert del av arbeidet med samfunnssikkerhet i Norge.

En annen ordning som tilrettelegger for både offentlig-privat samarbeid og tverrsektorielt samarbeid er NCSCs partnersamarbeid. Informant 1 opplyser at dette partnersamarbeidet består av omkring 40 partnere fra privat næringsliv, IT-sikkerhetsbransjen, og forvaltningen. Disse har annenhver uke muligheten til å delta på såkalte NCSC-briefs hvor også SRM-ene deltar. Under disse briefene deles informasjon om status, hendelser, trender og indikatorer. Informant 1 beskriver dette samarbeidet slik:

> …Dette gjør at vi bygger tillitt til hverandre, vi holder hverandre oppdatert på hva som foregår, deler informasjon, møter hverandre på regelmessig basis, selv om det dessverre nå er digitalt. Men dette skaper helt klart bedre kommunikasjonsformer, gjennom å møtes og se hverandre, ha noe med hverandre å gjøre, nesten ukentlig. (Informant 1)

Informantens beskrivelse av samarbeidet vitner om at ordningen både bidrar til styrking av etablerte samarbeidsrelasjoner og fremmer felles situasjonsforståelse både tverrsektorielt

mellom SRM-er og mellom det offentlige og det private. Dette fremstår som en type tilrettelegging for samarbeid som foregår i tråd med myndighetenes intensjon om å etablere felles situasjonsforståelse på cybersikkerhetsfeltet (Departementene, 2019b, s. 10; Justis- og beredskapsdepartementet, 2020, s. 83). Det kan også oppfattes som en faktor som motvirker manglende grad av koordinering mellom sektorer (Jensen, 2019, s. 269-270).

Informant 4 som er ansatt i HelseCERT beskriver hvordan opprettelsen av NCSC og partnersamarbeidet har fostret nye typer samarbeid:

> I NCSC så har vi jo partnersamarbeid med en del aktører og de strekker seg også utover de sektorvise responsmiljøene, hvor også ulike private virksomheter deltar i det partnersamarbeidet. Så det har styrket den litt bredere samarbeidsplattformen i informasjonssikkerhetsmiljøet i Norge. Og det har også bidratt til å styrke de sektorvise responsmiljøene sitt samarbeid selv om vi også hadde de samarbeidsforumene og møteplassene før NCSC, i NorCERT regi men da var det nok kanskje ikke så mange andre partnere involvert i samarbeidet. (Informant 4)

Disse betraktningene vitner om at NCSC har inntatt en rolle som tilrettelegger både for tverrsektorielt samvirke og multistakeholder-initiativer. Informant 4 forklarer i forlengelsen av det ovennevnte sitatet at koronapandemien var ødeleggende for fysiske møter mellom aktører i styringssystemet hos NCSC på Langkaia i Oslo. Dette har imidlertid bidratt til hyppigere kontakt mellom aktører gjennom en lavere terskel for å ha møter via videokommunikasjon. Dette opplyses å være praktisk for de ansatte i HeleCERT som sitter i Trondheim.

NCSC har også en annen ordning som representerer en form for multistakeholder-initiativ mellom NSM og aktører i det private, den såkalte kvalitetsordningen for hendelseshåndtering. Informant 2 opplyser at private bedrifter som arbeider med informasjonssikkerhet og hendelseshåndtering kan søke et kvalitetsstempel fra NCSC som gir dem mulighet til å bli anbefalt som kompetent hendelseshåndteringsselskap dersom det er mangel på kapasitet. Målsetningen med denne ordningen er å heve kvaliteten på selskap som tilbyr tjenester innenfor hendelseshåndtering og oppnå økt slagkraft for styringssystemet samlet sett. Foreløpig er det fire selskaper som har fått et slikt kvalitetsstempel: Atea, Defendable, Mnemonic og NETSecurity. Informanten presiserer at det er åpent for alle å søke om godkjenning og at ordningen ikke skal virke konkurransevridende.

5.2.2 Tilrettelegging gjennom Kripos NC3

Kripos NC3 har også ordninger for samarbeid med aktører i det private. Informant 3 opplyser at de siden cyberkrimsenterets oppstart har hatt forbindelser til private aktører. De er også i ferd med å inngå intensjonsavtaler om samarbeid med IT-sikkerhetsselskaper. Informanten beskriver en type uheldig situasjon som kan oppstå mellom Kripos NC3 og andre aktører under hendelseshåndtering som det fremstår som naturlig å se i sammenheng med disse intensjonsavtalene. Informantens beskrivelse av denne type situasjon er svært relevant for utfordringer forbundet med Multistakeholdermodellen og er derfor inkludert i sin helhet under:

> Det som ikke er heldig er tilfeller der et selskap som er rammet av datakriminalitet leier inn en eller flere private sikkerhetsaktører, og med støtte fra for eksempel NSM gjennomfører sin hendelseshåndtering uten å bringe politiet inn i loopen i det hele tatt. Alternativt, at politiet involveres så sent at det hindrer sikring av spor og bevis, og at politiet må starte etterforskning på grunnlag av rapporter som er utarbeidet av en tredjepart. Det er slik og det kommer til å være slik at private og offentlige sikkerhetsaktører involveres. Det er ikke nødvendigvis et problem så lenge man kontakter politiet minst like tidlig som de andre aktørene. Da vil politiet koordinere innsatsen. Til sammenligning så kan man tenke seg en situasjon der lokalt politi rykker ut til et åsted etter tips fra publikum eller en fornærmet, med mistanke om drapsforsøk og drap. Politiet sikrer åstedet, setter opp sperrebånd, og avventer de lokale krimteknikerne samt støtte fra Kripos. Jeg tror det for de fleste er utenkelig at politiet i en slik situasjon ikke varsles, eller varsles så sent at de kommer til et åsted med sivilt personell i kjeledress som har satt opp eget sperrebånd og som er i full gang med det de kaller hendelseshåndtering når politiet kommer frem. Slik er det ofte i cyberkrimsaker, med fare for uforvarende bevisforspillelse av personell som mangler kompetanse og myndighet til å etterforske. (Informant 3)

Beskrivelsen av en slik situasjon hvor Politiet ikke involveres på gunstig tidspunkt og private aktører påtar seg en lederrolle innenfor arbeidet med håndtering fremstår som svært interessant i lys av de postulerte svakhetene i Multistakeholdermodellen forbundet med «maktkamp» mellom det offentlige og det private (Muller, 2016, s. 16). Situasjonen kan også oppfattes som relevant for tanken om et spenningsforhold mellom et eksisterende

institusjonelt lag bestående av myndighetsaktører og nye lag som har blitt koblet til nettverksstyring. Som tidligere nevnt har det blitt postulert at et institusjonelt lag bestående av myndighetsaktører kan dominere styringen på et felt i så stor grad at andre nettverksbaserte lag ikke fungerer så effektivt som mulig (Hanssen et al, 2014, s. 156). I situasjonen Informant 3 beskriver er imidlertid rollene snudd og IT-sikkerhetsbedriftene representerer det eksisterende institusjonelle laget og Kripos NC3 det nye. Dette fremstår som illustrerende for cybersikkerhetsfeltet i sin helhet og at det eksisterer behov for velfungerende samarbeid for å motvirke de negative effektene av «maktkamp».

Det faktum at hendelseshåndtering foretas av en rekke ulike aktører med ulike interesser gjør at koordinasjon kan oppfattes som essensielt. Denne oppfatningen deler tilsynelatende informanten. Informanten opplyser også at grunnlaget for intensjonsavtalene er et behov for en samarbeidskonstruksjon som sikrer at begge sider er godt informert på forhånd hvis en hendelse oppstår og de ender opp på samme åsted. Vedkommende poengterer også at avtalene er veldig viktige for arbeid med forebygging og kjennskap til kriminalitetsbildet. Informanten tilkjennegir sitt syn på Politiets rolle slik:

> Men det er for å fasilitere for et samarbeid mellom aktører som kommer til å treffe på hverandre før eller siden, slik at vi blir enige om hvordan dette skal gjøres på åstedet. Det er Politiet som leder og politiet som går først, og vi har det samme ansvaret i samfunnet på dette området som på alle andre områder. (Informant 3)

Det kan utledes fra disse formuleringene at informanten ser på intensjonsavtalene som et ledd i å etablere en prosedyre for hvordan aktører fra det private og Politiet skal samarbeide på et digitalt eller fysisk åsted. Informanten er også tydelig på at Politiets mandat og rolle gjør at det er naturlig at de tar styringen i arbeidet på åstedet. Dette harmonerer svært godt med Kripos NC3 sin målsetning om å ha tilsvarende myndighetsutøvelse i det digitale rom som i det fysiske. Det kan tenkes at intensjonsavtalene om samarbeid med private aktører kan motvirke effektene av interessekonflikt og «maktkamp» vedrørende hendelseshåndtering.

Informant 3 opplyser også om en kartleggingsfunksjon de har i cyberkrimsenteret som tar sikte på å kartlegge kapasiteter og ressurser som Politiet kan dra nytte av innenfor hendelseshåndtering:

> Og vi har en outreach-funksjon, eller en oppsøkende virksomhet som følger med på og skaper oversikt over de ulike aktørene, hva slags oppdrag de har, og hva de kan produsere. Det har vi brukt mye tid på de siste to årene med det enkle, men viktige formål at vi skal kunne mobilisere ressurser som ikke Politiet selv betaler for eller har i sine egne rekker for å løse problemer. Politiet støttes av Forsvaret, eller fra andre offentlige og private ressurser i samfunnet i andre situasjoner. Vi trenger ikke traktorer og transportfly selv, og vi kan heller ikke skaffe oss tilstrekkelig ekspertkompetanse selv innen alle aspektene ved bekjempelse av trusler eller kriminalitet i det digitale rom. (Informant 3)

Det kan utledes fra disse betraktningene at Politiet aktivt søker etter samarbeidspartnere som kan heve deres operative kapasitet og evne til å bekjempe kriminalitet i det digitale rom. Det er registrert 18 CERT/CSIRT-miljøer i Norge på listen til European Union Agency for Cybersecurity (ENISA) (ENISA, 2021). Dette er miljøer tilhørende det private og aktører i det offentlige som utfyller SRM-funksjon. Det er imidlertid ikke alle de norske SRM-ene som er registrert hos ENISA så det reelle antallet aktører er enda høyere. På grunnlag av dette store antallet potensielle samarbeidspartnere fremstår det som logisk at Kripos NC3 benytter ressurser og tid på å kartlegge og opprette samarbeid med nye partnere.

Informant 2 fra NSM kommenterte også det store antallet aktører i det norske informasjonssikkerhetsmiljøet: «Vi er et lite land med mange små fagmiljø. Distribuerte modeller har sine svakheter. Det krever mye å få oversikt. Det betinger godt samarbeid og klare kommunikasjonsplaner og rapporteringsrutiner.» (Informant 2). Informanten refererer her tilsynelatende til de 11 CERT/CSIRT-miljøer som fyller SRM-funksjon i styringssystemet. Betraktningene understøtter inntrykket av at gode plattformer for informasjonsdeling og god kommunikasjon er svært viktig i arbeidet med hendelseshåndtering. Det store antallet små miljøer på cybersikkerhetsfeltet kan forstås som en del av grunnlaget for utfordringer forbundet med fragmentert ansvarsfordeling (Eggenschwiler, 2019, s. 8).

5.2.3 Tilrettelegging på SRM-nivået

I delen av Departementenes tiltaksoversikt som omhandler avdekking og håndtering av digitale angrep er det første tiltaket de sektorvise responsmiljøene (SRM-ene). Det opplyses

følgende: «Ambisjonen med de sektorvise responsmiljøene er at disse skal kunne bistå sin sektor med kompetanse og være knutepunkt for informasjon og informasjonsflyt mellom virksomheter i sektoren, mellom sektorer og mellom sektor og nasjonalt nivå (NorCERT).» (Departementene, 2019b, s. 26). Denne formuleringen viser både myndighetenes benyttelse av sektorprinsippet og deres fokus på tverrsektorielt samarbeid. SRM-ene skal ha ansvar i sin sektor, men også kommunisere horisontalt på tvers av sektorer og vertikalt til de sektorovergripende aktørene. Det er verdt å merke seg at det er satt et likhetstegn mellom *nasjonalt nivå* og *NorCERT* som nå er en innbakt kapasitet i NCSC. Dette signaliserer at NCSC har en unik særstilling i styringssystemet som den fremste sektorovergripende aktøren innenfor hendelseshåndtering.

Informant 4 fra HelseCERT kommenterer at de har et veldig godt samarbeid horisontalt med andre SRM-er og at det er daglig kontakt på chat og faste ukentlige statusmøter mellom SRM-ene i regi av NCSC. Vedkommende synes samarbeidet fungerer godt og mener det har blitt bedre gjennom at ulike SRM-er har styrket seg de senere årene. Informanten trekker også frem samarbeid internasjonalt som viktig for HelseCERT. Dette innebærer blant annet kommunikasjon med responsmiljøer for helsesektorene i andre land. Det vertikale samarbeidet med tidligere NorCERT og nå NCSC opplyses også å ha gjennomgått en positiv utvikling de senere årene. Informant 1 fra NSM omtaler samarbeidet mellom dem og SRM-ene på følgende vis:

> Vi benytter de sektorvise responsmiljøene så mye som vi bare kan. Det er de som har oversikt over sin sektor. Altså, hypotetisk, skulle det skje en IKT-sikkerhetshendelse i helsesektoren, eller i forsknings- og utdanningssektoren, så har vi de sektorvise responsmiljøene som kjenner virksomhetene i sektoren bedre enn vi i NCSC gjør. NCSC har ikke kapasitet til å holde oversikt over enhver sektor, og derfor er det kjempebra og viktig at vi har et ledd rett under oss, de sektorvise responsmiljøene, som har god oversikt og forståelse for sin sektor. – Og det opplever jeg at de i stor grad har, det er selvfølgelig ulike nivåer på de ulike sektorvise responsmiljøene, det er noen som er relativt nyopprettede, men også flere som har drevet på i flere år. Så dette er veldig gode samarbeidspartnere vi drar stor nytte av. (Informant 1)

Informant 2 beskriver forholdet til SRM-ene slik: «I Nasjonalt cybersikkerhetssenter samarbeider NSM tett med SRM-ene, de har tilgang til våre lokaler og informasjon deles

digitalt. Det er et samhandlingsverktøy, som bidrar til å kompensere for en distribuert modell». Disse betraktningene kan sies å signalisere en opplevelse av velfungerende samarbeid med SRM-ene fra NSM sin side. Informant 1 peker imidlertid også på en utfordring som kan dukke opp knyttet til samarbeid med SRM-er grunnet forholdet mellom rammede virksomheter og deres SRM. Dersom en rammet virksomhet har liten kontakt med sin SRM kan arbeidet med hendelseshåndtering bli utfordrende. Informanten beskriver at et drømmescenario ville vært at alle virksomheter i sektorene hadde en veletablert tilknytning til sine SRM-er. Informant 4 opplyser at det er frivillig å koble seg til HelseCERT og Nasjonalt beskyttelsesprogram (NBP) som de drifter. Det opplyses i et notat at:

> Alle kommuner er tilknyttet og har en medlemsavtale med Norsk helsenett om helsenettilknytning og er medlem av helsenettet. Av disse så har 325 avtale med HelseCERT om deltakelse i NBP. De øvrige 31 kommuner har alle fått informasjon om NBP og tilbud om å delta, men har ikke respondert. Det er ingen kommuner som har gitt tilbakemelding om at de ikke ønsker å delta. (HelseCERT, 2021)

Dekningsgraden beskrevet i notatet virker god tatt i betraktning at primærhelsetjenesten i kommunene utgjør den største andelen av virksomheter i helsesektoren (Informant 4). Informant 3 beskriver SRM-ene og samarbeidet med dem som følger:

> CERTene er bra og det samles informasjon på et høyere nivå enn før. Det er lettere for oss å få tak i dem og samarbeide med dem. Vi utveksler informasjon, og de er kilder til vårt etterretningsarbeid. Det er et løpende samarbeid. (Informant 3)

Informanten beskriver her en heving av kvaliteten på arbeidet som gjøres i CERTene (SRM). Betraktningene om informasjonsutveksling og forbindelsen til Politiets etterretningsarbeid kan sees i sammenheng med målet om oppnåelse av felles situasjonsforståelse på tvers av sektorer. Dette kan tenkes å motvirke svakheten assosiert med sektorprinsippet vedrørende manglende felles situasjonsforståelse (Jensen, 2019, s. 269-270).

5.2.4 Tilrettelegging gjennom mekanisme

Tiltak 43 i myndighetenes tiltaksoversikt omhandler opprettelsen av Felles cyberkoordineringssenter (FCKS). FCKS er en samhandlingsmekanisme opprettet for å koordinere innsats mellom etater bestående av representanter fra Etterretningstjenesten, Kripos NC3, NSM og PST (Justis- og beredskapsdepartementet, 2020, s. 85). I tiltaksoversikten beskrives FCKS som følger: «FCKS skal bidra til å øke den nasjonale evnen til å motstå alvorlige digitale angrep og understøtte strategisk analyseproduksjon og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom.» (Departementene, 2019b, s. 28). Videre opplyses det at FCKS ikke er et selvstendig organ med egen beslutningsmyndighet. Begge informantene fra NSM og informanten fra Kripos NC3 beskrev samarbeidet og koordineringen som foregår i FCKS som velfungerende.

Informant 2 beskriver FCKS som en samhandlingsmekanisme som bidrar til å koordinere innsats mellom fire parter med ulike mandater og interesser innenfor hendelseshåndtering. Informanten beskriver også hvordan interessekonflikt kan komme til uttrykk under hendelseshåndtering. Ifølge informanten ønsker Etterretningstjenesten i tråd med sitt mandat å kartlegge informasjon, sammenfatte den og rapportere. Dette fører gjerne til en oppfatning av at det lureste å gjøre er å ikke intervenere hurtig for å løse problemet, men heller fokusere på informasjonsinnhenting. Politiet, i FCKS-sammenheng Kripos NC3 og PST, ønsker å etterforske hendelsen for å kunne stille noen til rette for den. Et sentralt element i dette er å samle inn bevis og sikre spor gjennom informasjonsinnhenting og potensielt analyse av maskinvare. NSM sine oppfatninger av hva som er lurt å gjøre vil som regel være tuftet på analyse av hva som best bidrar til å begrense skaden hendelsen forårsaker. Informant 2 beskriver at i noen tilfeller kan dette bety å anbefale nedstenging av systemer. I andre tilfeller kan anbefalingen være å la systemer forbli oppe for å kartlegge hva en truende aktør har fått tilgang til. Informant 2 kommenterte også at disse interessekonfliktene forsterkes når kritiske samfunnsfunksjoner rammes av IKT-sikkerhetshendelser og at FCKS i slike tilfeller blir enda viktigere som samhandlingsmekanisme.

Informant 2 sin oppfatning av interessekonflikt vedrørende hendelseshåndtering er svært interessant sett i lys av den postulerte svakheten i den hierarkiske delen av multistakeholdermodellen knyttet til fragmentert ansvarsfordeling (Eggenschwiler, 2019, s. 8; Jensen, 2019, s. 269-270). På spørsmål om en form for «maktkamp» mellom myndighetsaktører grunnet interessekonflikt svarer Informant 2 at det kan oppfattes slik, men at etatenes ulike mandat naturlig og ønskelig trigger ulike vinklinger inn i en problemstilling.

Denne oppfatningen av overlappende ansvarsområder kan sies å representere et alternativt perspektiv på utfordringen med fragmentert ansvarsfordeling. I stedet for å oppfatte det som negativt at ansvarsområder ikke er stringent definert ser informanten noe positivt som kan komme ut av det. På spørsmål om tilstedeværelse av «maktkamp» svarer Informant 1 at det ikke er noe vedkommende kjenner seg igjen i. Informanten opplever at etatene har sine roller, men at det noen ganger kan oppstå en grad av usikkerhet om hvem som bør ta styringen under en hendelse. Dette anses imidlertid ikke å utgjøre noe stort problem siden de gjennom god kommunikasjon finner ut hva slags anbefalinger som bør gis rammede virksomheter.

Informant 3 fra Kripos NC3 anerkjenner tilstedeværelse av interessekonflikt, men understreker at alternativet med totalt fravær av overlappende ansvarsområder ville gi hull hvor noen typer hendelser ikke vil bli håndtert tilfredsstillende. Informanten beskriver at overlapp mellom ansvarsområder er vanlig innenfor samfunnssikkerhetsfeltet og at dette kan være et gode så lenge det ikke fører til for ineffektiv ressursbruk. Om koordinering mellom aktører og politiets rolle i styringssystemet forklarer informanten følgende:

> Det vil være et vedvarende arbeid å koordinere, synkronisere og harmonisere innsats internt i Justis og mellom alle parter. Politiet vil alltid bidra med det vi kan innenfor kapasitet og ta vår rolle innenfor dette området som de andre samfunnssikkerhetsområdene. (Informant 3)

Informantens beskrivelse av et vedvarende arbeid med å koordinere, synkronisere og harmonisere innsats mellom alle parter fremstår som svært relevant både for multistakeholdermodellens virkemåte i styringssystemet og utfordringer knyttet til fragmentert ansvarsfordeling innenfor den hierarkiske koordinasjonsmekanismen (Eggenschwiler, 2019, s. 8; Jensen, 2019, s. 269-270). Alle aktører uavhengig av sektortilhørighet eller virksomhetstype kommuniserer og deler informasjon for å oppnå best mulig hendelseshåndtering. Selv om jeg har valgt å ikke definere styringssystemet som et nettverk i teoretisk forstand gir disse elementene assosiasjoner til et nettverk av aktører som utøver styring innenfor et samfunnssikkerhetsområde. Informant 4 fra HelseCERT kommenterer potensiell fragmentert ansvarsfordeling slik:

> Den multistakeholder-utfordringen er jo absolutt til stede. Det som er viktig er jo på en måte ansvarslinjene her. De må være tydelige, det kan ikke være tvil. Det tenker jeg er viktig. Og når de som skal gjøre jobben operativt snakker sammen så fungerer ting ofte veldig bra. (Informant 4)

Utfra disse betraktningene kan det tolkes at informanten, i likhet med flere av de andre informantene, anser god kommunikasjon som en motvirkende kraft mot den potensielle ineffektiviteten som fragmentert ansvarsfordeling og interessekonflikt kan medføre.

5.2.6 Tilrettelegging gjennom øving

Tilrettelegging for samarbeid gjøres ikke kun gjennom permanente ordninger og prosedyrer som de som er belyst så langt. Øvelser på hendelseshåndtering og samarbeid kan også oppfattes som en form for tilrettelegging siden de ofte tar sikte på å styrke funksjonaliteten til instrukser og prosedyrer. I myndighetenes tiltaksoversikt er DSB designert som ansvarlig for kursing av offentlige virksomheter i planlegging og gjennomføring av øvelser innen digital sikkerhet med støtte fra DIFI (nå Digitaliseringsdirektoratet) (Departementene, 2019b, s. 11). De ble også utpekt som ansvarlig for planlegging av en stor nasjonal øvelse på IKT-sikkerhet i nært samarbeid med blant annet NSM i tiltaksoversikten (Departementene, 2019b, s. 27-28). Myndighetene beskriver øvelsen på følgende vis:

> Det skal gjennomføres en ny nasjonal IKT-sikkerhetsøvelse med formål å styrke sivil-militært, offentlig-privat og internasjonalt samarbeid for hendelseshåndtering. En ny nasjonal øvelse vil spesielt ta utgangspunkt i et styrket offentlig-privat samarbeid, og vil derfor inkludere private virksomheter i planlegging, utforming og gjennomføring av øvelsen. (Departementene, 2019b, s. 27).

Inntrykket av at myndighetene anser offentlig-privat samarbeid som essensielt på cybersikkerhetsfeltet styrkes av deres beskrivelse av den nasjonale øvelsen. Den store nasjonale øvelsen ble gitt navnet «Digital 2020» og ble omtalt som en «nasjonal tverrsektoriell øvelse» av DSB (DSB, 2019). Under planleggingen av øvelsen ble den beskrevet som følger:

> Øvelsen skal planlegges, gjennomføres og evalueres i tett samarbeid med relevante offentlige og private virksomheter. Den overordnede hensikten med Øvelse Digital 2020 er å redusere samfunnets risiko for digitale angrep gjennom å forbedre evnen til å forebygge, avdekke og håndtere digitale hendelser. Øvelsen vil ta opp i seg de overordnede prioriterte områdene i Nasjonal strategi for digital sikkerhet; forebyggende digital sikkerhet, digital sikkerhet i kritiske samfunnsfunksjoner og evne til å avdekke og håndtere digitale angrep. Kompetanseheving vil være et integrert formål i hele øvelsesplanleggingen. Det vil også utarbeides egne ferdige øvingspakker som kan brukes av virksomhetene selv. Selve øvelsen vil ha hovedfokus på håndtering av et komplekst tverrsektoriell digitalt angrep i Norge. (DSB, 2019)

I tråd med beskrivelsen i tiltaksoversikten ble planleggingen iverksatt med deltakere fra det offentlige og det private. Det beskrevne hovedscenarioet harmonerer også godt med myndighetenes fokus på tverrsektorielt samarbeid. Etter en lang planleggingsprosess skulle det imidlertid vise seg at håndteringen av Covid-19 var så krevende at det ble besluttet å nedskalere øvelsen. DSB beskriver situasjonen slik i et brev om rapporteringsskjema:

> Håndteringen av Covid-19 har ført til omfattende utfordringer for mange av aktørene som er involvert i planleggingen og gjennomføringen av Øvelse Digital 2020. Det er nært opp til øvelsen besluttet å gjennomføre Digital 2020 som en to timers diskusjonsøvelse i stedet for spilløvelsen som det opprinnelig var planlagt med. Evalueringsarbeidet er justert deretter. (DSB, 2020a)

På tross av den reduserte øvingsverdien og mindre omfattende evalueringen forårsaket av Covid-19 fremstår Øvelse Digital 2020 som interessant i lys av myndighetenes tilrettelegging for samarbeid. Det faktum at øvelsen ble omtalt som en «tverrsektoriell øvelse» i kombinasjon med dens planlagte fokus på offentlig-privat samarbeid kan tolkes som en indikasjon på multistakeholder-tenkning. I henhold til tradisjonell tenkning vil begrepet *tverrsektoriell* kun benyttes for å beskrive samarbeid (samvirke) mellom sektorer i Staten. Det fremstår imidlertid som utfordrende å benytte begrepene gjennomgående presist dersom det konsekvent må skilles mellom typer samarbeid når de omtales samlet, slik som i omtalen av øvelsen. Det eksisterer tilsynelatende ikke noe etablert begrep for å beskrive både

tverrsektorielt samarbeid og offentlig-privat samarbeid samlet. *Sektoroverskridende* fremstår som en potensiell kandidat.

5.3.0 Samarbeid om hendelseshåndtering i praksis

Når en IKT-sikkerhetshendelse inntreffer kan mange ukjente faktorer påvirke evne til å håndtere hendelsen og situasjonsbildet kan være uavklart. Ansvaret for håndtering ligger som kjent hos den rammede virksomhet enten den tilhører det offentlige eller det private i henhold til ansvarsprinsippet. Dersom den rammede virksomheten har et bevisst forhold til IKT-sikkerhet kan det tenkes at de har lest og forholder seg til «Rammeverk for håndtering av IKT-sikkerhetshendelser» (2017). Dette dokumentet er spesielt viktig for hendelseshåndtering siden det er utpekt som den viktigste instruksen av myndighetene (Departementene, 2019b, s. 27; Justis- og beredskapsdepartementet, 2020, s. 80). Informant 2 beskriver rammeverkets betydning i praksis slik:

> Rammeverk for digital hendelseshåndtering er et veldig viktig redskap i samordning mellom sektorer. Nasjonalt cybersikkerhetssenter i NSM er navet, men kjerneprinsippet i rammeverket er at hver sektor skal ha kapasiteter gjennom sektorvise responsmiljø. (Informant 2)

På grunnlag av informantens beskrivelse kan rammeverket tolkes som en bidragsyter til felles forståelse av prosedyrer under hendelseshåndtering og følgelig et godt utgangspunkt for tverrsektorielt samarbeid.

Rammeverket harmonerer i svært stor grad med del 4 i dokumentet «NSMs grunnprinsipper for IKT-sikkerhet» (2020) som omhandler *håndtering og gjenoppretting*. De fire punktene i del 4 av grunnprinsippene, forberede, vurdere og klassifisere, kontrollere og håndtere og evaluering er alle tilstede i rammeverket. Utover disse er også *varsling* og *situasjonsrapportering* egne punkter. Prosedyrer for varsling er særlig relevant for samarbeid om hendelseshåndtering siden det er en av de fremste måtene aktører i styringssystemet blir involvert gjennom (Informant 1). Situasjonsrapportering fremstår også som svært relevant for hvordan samarbeid under hendelseshåndtering foregår grunnet informantenes vektlegging av god kommunikasjon som essensielt.

Hva slags type virksomhet den rammede er og dens planer for hendelseshåndtering har betydning for hvem den bør henvende seg til for bistand. Virksomheter som har driftsavtaler for IT-systemer med eller kjøper sikkerhetstjenester fra aktører i privat sektor kan henvende seg til disse først. Dette skjedde i den tidlige fasen av løsepengevirusangrepet mot Østre Toten kommune (Informant 5). Dersom den rammede virksomheten er tilknyttet et SRM bør den vurdere å varsle det og hvis hendelsen har betydning for kritisk infrastruktur eller kritiske samfunnsfunksjoner bør SRM alltid varsles (NSM, 2017c, s. 15). Uavhengig av hvem den rammede velger å forespørre om bistand først kan hendelsen havne hos NCSC eller Kripos NC3 gjennom informasjonsdeling mellom aktører i styringssystemet. Slik informasjonsdeling skal gjøres i overensstemmelse med den/de som eier informasjonen om hendelsen, fortrinnsvis den rammede virksomheten, med mindre lovpålagte forhold tilsier noe annet (NSM, 2017c, s. 15). Delen av rammeverket som omhandler situasjonsrapportering legger føringer for hvordan informasjonsdeling skal foregå under hendelseshåndtering. Det opplyses følgende: «Situasjonsrapportering skal gå både fra virksomhets- og sektornivå til nasjonalt nivå, og fra nasjonalt nivå til sektor- og virksomhetsnivå.» (NSM, 2017c, s. 18). Vi ser her at informasjonsdeling i henhold til rammeverket skal foregå vertikalt begge veier. I praksis foregår informasjonsdelingen også horisontalt på alle nivåer (Informant 1; Informant 2; Informant 3; Informant 4).

5.3.1 Hendelseshåndtering hos NCSC

Informant 1 opplyser at NCSC har svært lav terskel for å bistå rammede virksomheter og at det i all hovedsak er tre måter de blir involvert i hendelseshåndtering på, oppdagelse av mistenkelig trafikk i VDI, varsling fra rammet virksomhet eller varsling fra en av samarbeidspartnerne. Informanten beskriver den videre prosessen slik:

> Innledningsvis i en hendelse undersøker vi omfang og forsøker å etablere et situasjonsbilde. Vi innleder kontakt med virksomheten og gir bistand til hendelseshåndtering. I første fase identifiserer vi hvilken type bistand virksomheten har behov for, det kan for eksempel være teknisk analyse. For å kunne utføre teknisk analyse er det helt avgjørende at virksomheten har gode logger, og at logging er påskrudd. Videre vil funn og resultater fra teknisk analyse sette oss i stand til å vurdere skadeomfang og hvilke risikoreduserende tiltak som bør implementeres. Dette gir oss et situasjonsbilde, slik at vi får forståelse for hvilken type hendelse vi står ovenfor. (Informant 1).

Informanten understreker betydningen av god logging av nettverksaktivitet hos virksomheter. Dette er også nedfelt i rammeverket for hendelseshåndtering i form av et punkt på listen over forventninger til virksomheter som lyder som følger: «Virksomheter forutsettes å ha systemer for loggføring av nettverkstrafikk.» (NSM, 2017c, s. 12). Logger er også et sentralt element i deteksjon og vurderingsfasen av hendelseshåndteringen og informasjon fra logger er oppført som en sentral del av analysearbeidet under en hendelse i rammeverket (NSM, 2017c, s. 14).

Informant 2 opplyser at NCSC skal analysere om en hendelse som rammer én virksomhet kan ha betydning for andre og kommunisere potensielle trusler til virksomheter som kan være sårbare. Denne analysevirksomheten på sektorovergripende nivå er nedfelt i sikkerhetsloven og rammeverket (Sikkerhetsloven, 2018, § 2-3; NSM, 2017c, s. 7). Informant 2 beskriver prosedyren på følgende vis:

> Men egentlig er vår aller viktigste oppgave å produsere et nasjonalt situasjonsbilde. Et nøkkelspørsmål er om hendelsen er noe som kan ramme andre i samfunnet og om varsling og forebyggende tiltak må iverksettes. Så da går vi inn i det med både teknisk og strategisk personell. (Informant 2)

Den ovennevnte beskrivelsen signaliserer at NSM tar sitt ansvar for helhetlig vurdering av trusselbildet på alvor og prioriterer å varsle andre når det er nødvendig i tråd med myndighetenes intensjon (Justis og beredskapsdepartementet, 2020, s. 72). Informanten opplyser at slik varsling av andre virksomheter noen ganger blir gjort etter såkalt samvirkekonferanse med DSB. Denne typen samarbeid kan oppfattes som kompenserende for den postulerte svakheten til sektorprinsippet vedrørende mangel på helhetlig situasjonsforståelse. Gjennom analyse og varsling av andre parallelt med et hendelsesforløp kan NCSC potensielt forhindre at en krises alvorlighetsgrad eskalerer. Dette kan oppfattes som motvirkende mot mangel på felles situasjonsforståelse som har blitt omtalt som en svakhet i sektorprinsippet (Jensen, 2019, s. 269-270).

5.3.2 Hendelseshåndtering på SRM-nivået

Rammeverket for håndtering av IKT-sikkerhetshendelser inneholder mange føringer for hva SRM-er skal foreta seg under hendelseshåndtering. Disse inkluderer blant annet

analysebistand til den rammede virksomheten (NSM, 2017c, s. 14) Informant 4 kommenterer verdien av rammeverket slik:

> Vi ble jo egentlig opprettet før det rammeverket var på plass og vi ser jo at vi er veldig compliant til det rammeverket. Men ikke nødvendigvis på grunn av det rammeverket for vi hadde jo egentlig mye på plass før det ble etablert. Så jeg tror det rammeverket for så vidt er nyttig for SRM-er som blir nyopprettet eller skal etablere seg. Og da ha et rammeverk å se til så tror jeg det hjelper. (Informant 4)

Det kan utledes fra disse betraktninger at informanten anser rammeverket for å være et godt redskap i håndtering av hendelser. Vedkommende beskriver at HelseCERT etterlever prosedyrene i det på en god måte. Senere i intervjuet trekker informanten frem en utfordring forbundet med rammeverket:

> Jeg tror det først og fremst er de to øverste nivåene som kjenner til det og forholder seg til det. Så du kan si at det er på en måte vår utfordring, SRM-nivået, og gjøre det kjent nedover til virksomhetene. Og da er det jo ikke sikkert at det er et mål å gjøre rammeverket i seg selv kjent, men først og fremst egentlig de kravene og forventningene som stilles til virksomhetene kjent for virksomhetene. Veldig mye av det vi gjør handler på en måte om å få virksomhetene til å få på plass mye av det som står i det rammeverket. Men ikke egentlig ved å sende ut rammeverket, det handler mer om å gi dem råd og anbefalinger om hva de bør gjøre. (Informant 4)

Informanten beskriver her varierende grad av kjennskap til rammeverket i virksomheter i helsesektoren. HelseCERT sitt fokus på krav og forventninger indikerer at de gir råd delvis for å gjøre virksomheter i stand til å samarbeide med dem og andre på en god måte under en eventuell hendelseshåndtering. Informanten kommenterer også at HelseCERT undersøker etterlevelse av rammeverket gjennom inntrengingstester hos virksomheter i helsesektoren for å se «om kart og terreng stemmer».

HelseCERT har også erfaring med håndtering av alvorlige hendelser i praksis. I 2018 bisto de Helse Sør-Øst RHF og deres undervirksomhet Sykehuspartner HF med å håndtere et angrep fra en avansert og profesjonell aktør (Sykehuset Innlandet HF, 2018, s. 1). Angrepet

ble gjennomført ved at trusselaktøren benyttet en sårbar applikasjon i et datasystem forvaltet av Sykehuspartner HF til å få tilgang til deres IT-infrastruktur (FFI, 2020, s. 29). HelseCERT varslet Sykehuspartner HF om at de hadde avdekket innbrudd i datasystemer den 8. januar 2018 og det ble satt krisestab dagen etter. I den innledende fasen av håndteringen bidro HelseCERT med analysestøtte (Sykehuset Innlandet HF, 2018, s. 1; FFI, 2020, s. 29).

Dataangrepet fikk store konsekvenser for IKT-systemene i flere helseregioner og en direkte alvorlig konsekvens var utfordringer med å utveksle pasientinformasjon mellom helseforetak. Denne utfordringen gjaldt blant annet radiografibilder (FFI, 2020, s. 29). Hendelsen ble anmeldt til politiet kort tid etter at den ble oppdaget og PST etterforsket innbruddet som mulig brudd på straffeloven § 121 *Etteretningsvirksomhet mot statshemmeligheter*. Saken ble imidlertid henlagt den 29. november 2018 grunnet manglende opplysninger om gjerningsperson (Sykehuset Innlandet HF, 2018, s. 1; FFI, 2020, s. 32). Informant 4 var med på den operative håndteringen av hendelsen og beskriver samarbeidet med Sykehuspartner HF slik:

> Vi kjente godt til Sykehuspartner, leverer tjenester til dem, har gjort inntrengningstesting og vi kjenner også miljøet og de som jobber operativt der. Så det var veldig lett å snakke sammen og begynne å jobbe sammen med den hendelsen. Så det samarbeidet der fungerte veldig bra. (Informant 4)

Utfra informantens beskrivelse av samarbeidet med Sykehuspartner HF kan det utledes at god kommunikasjon også er viktig mellom SRM-nivået og den rammede virksomheten. Etablerte relasjoner til ansatte virker også her å ha betydning for hvordan aktører i styringssystemet evner å håndtere hendelser.

Hendelsen som rammet Helse Sør-Øst RHF i 2018 ble grundig evaluert i etterkant og Forsvarets forskningsinstitutt (FFI) publiserte en rapport om hendelsen i 2020. Det ble også vedtatt at en evaluering av IKT-sikkerhet i helsesektoren i sin helhet skulle gjennomføres. Dette omtales også i myndighetenes tiltaksoversikt til «Nasjonal strategi for digital sikkerhet» 2019: «Det er bestemt at det etter datainnbruddet i Helse Sør-Øst i 2018, skal gjennomføres evalueringer i helsesektoren, NSM og JD. Videre bør større uønskede digitale hendelser evalueres. Myndighetene anbefaler at også private virksomheter evaluerer større hendelser og deler erfaringer.» (Departementene, 2019b, s. 29). Den beskrevne evalueringen av helsesektoren resulterte i en rapport utarbeidet av Riksrevisjonen i 2020. I den ble det påpekt

vesentlige svakheter i grunnleggende tekniske sikkerhetstiltak, samt utfordringer med helseregionenes sikkerhetsorganisering, styring og atferd blant helse- og IKT-personell (Riksrevisjonen, 2020, s. 71).

5.3.3 Hendelseshåndtering og åpenhet

Den siste delen av rammeverket for håndtering av IKT-sikkerhetshendelser omhandler *tilbakeføring og læring av hendelsen*. Et sentralt element er evaluering og læring av hendelser, samt deling av erfaringer. SRM-ene skal dele erfaringer med NSM som også deler læringspunkter ned igjen til dem (NSM, 2017c, s. 19). Etter alvorlige IKT-sikkerhetshendelser skal NSM dele læringspunkter med relevante myndigheter: «for å sikre at krav og anbefalinger er mest mulig hensiktsmessige og målrettede med hensyn til risikobildet» (NSM, 2017c, s. 19). Dette kan sees i sammenheng med åpenhet fra rammede virksomheter om deres erfaringer med IKT-sikkerhetshendelser. Multistakeholder-initiativer som VDI er som tidligere beskrevet avhengig av gjensidig åpenhet og tillit mellom myndigheter og virksomheter i privat sektor. Beslutningen om å være åpen om at man har blitt rammet av en IKT-sikkerhetshendelse i offentligheten er en annen type åpenhet. I myndighetenes tiltaksoversikt er det et eget punkt som omhandler åpenhet om IKT-sikkerhetshendelser. Det opplyses følgende:

> NSM har tidligere på oppdrag fra JD utarbeidet anbefalinger for hvordan offentlige og private virksomheter bør vurdere åpenhet om uønskede digitale hendelser. Anbefalingene er laget i samarbeid med DIFI, NorSIS, POD og Næringslivets sikkerhetsråd (NSR). Offentlige og private virksomheter oppfordres til å følge disse anbefalingene. (Departementene, 2019b, s. 29)

Utfra dette utdraget fremstår det som tydelig at myndighetene ser på åpenhet om IKT-sikkerhetshendelser som positivt så lenge det gjøres i henhold til etablerte prosedyrer. Myndighetenes syn på åpenhet belyses ytterligere i Meld. St. 38 (2016-2017) - IKT-sikkerhet:

> Åpenhet danner grunnlag for læring og bidrar til å sette virksomhetene bedre i stand til å forebygge, avdekke og håndtere hendelser. Det gir også virksomheter og myndigheter bedre forutsetninger for å forstå utfordringene i det digitale rommet. Samtidig må

> offentliggjøring og deling av informasjon praktiseres på en slik måte at taushetspliktbestemmelser ivaretas, og fordelene må vurderes opp mot mulige negative konsekvenser. Regjeringen oppfordrer både offentlige og private virksomheter til å følge anbefalingene om åpenhet. (Justis- og beredskapsdepartementet, 2016a, s. 32-33)

Formuleringene i dette utdraget tilsier at myndighetene ser på åpenhet om IKT-sikkerhetshendelser i offentligheten som viktig for læring på tvers av sektorer og mellom det offentlige og det private. Dette kan oppfattes som et ledd i den siste delen av håndteringen av en IKT-sikkerhetshendelse, læring av hendelsen (NSM, 2017c, s. 19). Det kan også sees i sammenheng med myndighetenes målsetning om utvikling av felles situasjonsforståelse siden felles forståelse av trusselbildet potensielt kan fremme bedre utgangspunkt for samarbeid (Justis- og beredskapsdepartementet, 2020, s. 63-64).

Informantene fra NSM sine oppfatninger av åpenhet belyser noen avveininger som en rammet virksomhet bør ta stilling til før beslutning om offentliggjøring av en hendelse fattes. Informant 1 beskriver åpenhet som et tosidig fenomen. På den ene siden er det veldig positivt å være åpen om IKT-sikkerhetshendelser siden det bidrar til at andre kan lære av hendelser. Informanten trekker frem at åpenhet om inngangsvektor for et angrep kan gjøre andre i stand til å implementere målrettede tiltak for å beskytte seg mot lignende trusler. På den andre siden så innebærer åpenhet at den ansvarlige for et angrep blir klar over at den er oppdaget. Dette kan ifølge informanten gjøre at de som arbeider med håndtering av hendelsen kan gå glipp av spor. Informant 2 forklarer at NSM ser på det som positivt når norske virksomheter er åpne om hendelser som rammer dem og at de oppfordrer dem til dette. Tidspunktet for offentliggjøring behøver imidlertid ikke å være umiddelbart etter at hendelsen er oppdaget. Informanten opplyser at for tidlig offentliggjøring kan være operasjonsskadelig og at «trusselaktører også leser avisen».

Selskapet Norsk Hydro ble natt til 19. mars 2019 utsatt for et alvorlig dataangrep i form av et løsepengevirus kalt LockerGoga som førte til store utfordringer med opprettholdelse av drift og produksjon. Under håndteringen av hendelsen arbeidet selskapet døgnet rundt med å analysere all maskinvare for skadelig programvare og gjenopprette kompromitterte maskiner ved bruk av ukompromitterte sikkerhetskopier (Norsk Hydro, 2020; NHO, 2019). Selskapet henvendte seg til NSM på morgenen av angrepsdagen og mottok bistand fra dem og Kripos. Norsk Hydro anslo høsten 2019 at angrepet hadde påført dem kostnader i størrelsesorden 550-650 millioner NOK (Informant 2; Justis- og

beredskapsdepartementet, 2020, s. 32; Norsk Hydro, 2020). Både under og i etterkant av angrepet utviste Norsk Hydro stor grad av åpenhet om det som foregikk. De formidlet informasjon om hendelsen til myndighetsaktører, kunder, andre selskaper og til offentligheten (Norsk Hydro, 2019). Det har blitt forfektet at denne åpenheten trolig hindret nye angrep på andre virksomheter (NHO, 2019). Norsk Hydro mottok «Åpenhetsprisen 2019» som deles ut av Kommunikasjonsforeningen for sin åpenhet og kommunikasjon om IKT-sikkerhetshendelsen til omverdenen. Deler av juryens begrunnelse fremstår som beskrivende for betydningen av åpenhet:

> Selskapets åpne kommunikasjon om hva som skjer når en bedrift rammes av et dataangrep har vakt internasjonal oppsikt. Deres åpenhet er i dette tilfelle av stor samfunnsmessig betydning, og bidrar til å øke bevisstheten og kunnskapen om hva dataangrep kan gjøre med en virksomhet og hvilke ringvirkninger det gir. Dataangrep er et økende samfunnsmessig problem, og kan være ødeleggende for bedrifter og institusjoner og i sin ytterste konsekvens samfunnet som helhet.
> (Kommunikasjonsforeningens jury, 2019 – Gjengitt fra Norsk Hydro, 2019)

Juryens beskrivelse av økt bevissthet om hvor alvorlige konsekvenser dataangrep kan få som følge av Norsk Hydros åpenhet virker treffende. Denne virkningen av åpenheten kan potensielt bidra til at virksomheter som har et likegyldig forhold til digital sikkerhet tar sårbarheter og risikobildet mer på alvor. Dette kan igjen føre til at de implementerer tiltak eller oppsøker samarbeid med andre for å bedre sin egen sikkerhetssituasjon. Informant 2 trekker også frem økt bevissthet om hvor alvorlig en IKT-sikkerhetshendelse kan bli som en konsekvens av Norsk Hydros åpenhet. Vedkommende trekker også frem at Hydro-saken har bidratt til økt forståelse for at når en slik hendelse inntreffer så er det ikke bare en *IT-krise*, det er en *virksomhetskrise*. De enorme skadevirkningene av hendelsen som rammet Norsk Hydro og åpenheten de utviste blir også kommentert i den siste stortingsmeldingen om samfunnssikkerhet:

> Konsekvensene påvirket hele Hydros globale organisasjon, og selskapet estimerte høsten 2019 den totale kostnaden til rundt 550–650 mill. kroner. Det er viktig at virksomheter som utsettes for digitale angrep varsler og anmelder forholdet. Deling av kunnskap

> styrker vår evne til å forebygge, oppdage, varsle og håndtere digitale hendelser. (Justis- og beredskapsdepartementet, 2020, s. 32)

Omtalen av hendelsen befester inntrykket av at myndighetene ser en sammenheng mellom tilstedeværelse av åpenhet om IKT-sikkerhetshendelser og styrking av evnen til å håndtere dem.

5.4 Hendelseshåndtering i praksis – Østre Toten kommune

Østre Toten kommune ble natt til 9. januar 2021 rammet av et dataangrep som skulle vise seg å få alvorlige konsekvenser for kommunens drift og tjenestetilbud. Angrepet ble gjennomført ved at en kriminell aktør med kallenavnet *PYSA* krypterte alle kommunens servere og slettet sikkerhetskopi av systemer. Dette ble gjort ved hjelp av et virus kalt *Mespinoza* som gir avsenderen mulighet til å kryptere innholdet på maskinvare (Kommune-CSIRT, 2021). Angrepet ble oppdaget da ansatte i den kommunale helsetjenesten opplevde manglende funksjonalitet i sine systemer (Helgestad, 2021). Det ble satt krisestab i kommunen på morgenen lørdag 9. januar (Informant 5).

Det inntraff en rekke direkte konsekvenser som følge av viruset. Den kommunale helsetjenesten mistet systemet som innlagte pasienter bruker for å tilkalle hjelp og måtte benytte bjeller for å varsle helsepersonell. Det ble også umulig å fjernstyre låsmekanismene på helsetjenestens dører (Helgestad, 2021). Store deler av administrativt arbeid måtte gjennomføres ved bruk av penn og papir (Kommune-CSIRT, 2021). Dette gjorde det blant annet vanskelig å kreve inn skatt for kommunen (Informant 5). Informant 5 ansatt i Østre Toten kommune opplyser også at det i kommunestyremøter har kommet frem at kostnadene som er blitt påført kommunen sannsynligvis overstiger 30 millioner NOK i direkte kostnader. Informanten kommenterer videre at dette vil få konsekvenser for innbyggerne og kommunens evne til tjenesteutvikling. Vedkommende forklarer også at angrepet hadde direkte konsekvenser for arbeidsområder med betydning for liv og helse: «Innenfor liv og helse så har du jo også barnevernstjenester som mistet alle sine data, hele systemet sitt og de ble prioritert som nummer én i gjenopprettingen.» (Informant 5).

Hendelseshåndteringen under og i etterkant av angrepet foregikk som et samarbeid mellom IT-staben i Østre Toten kommune og tre bedrifter, Atea, KPMG og Ikomm. Informant 5 opplyser at IT-sjefen i Østre Toten kommune tok kontakt med Atea IRT (Incident

response team) lørdag 9. januar og at det innledningsvis var kun Atea som bisto. Atea er definert som tilhørende styringssystemet for håndtering av IKT-sikkerhetshendelser som følge av deres deltakelse i NCSC sin kvalitetsordning. IT-staben og Atea arbeidet sammen for å etablere forståelse av situasjonsbildet og redde det som kunne reddes. Informanten opplyser at dette inkluderte et såkalt *snapshot* av noen systemer som har vært avgjørende for kommunens evne til å gjenopprette funksjonalitet i datasystemer. Etter hvert ble det tydelig at kommunen trengte ytterligere bistand for å håndtere hendelsen. Informanten opplyser at de gjennom korrespondanse med Kommunesektorens organisasjon (KS) ble oppmerksomme på at KPMG hadde ressurser og kompetanse som kunne bidra til å løse de mange problemene angrepet forårsaket. Etter etablering av kontakt med KPMG 18. januar ble de den viktigste samarbeidspartneren i det videre arbeidet med hendelseshåndtering. Informanten forklarer at det var delvis grunnet tilfeldigheter at de endte opp med å kontrahere KPMG til å bistå dem. Disse tilfeldighetene besto av at enkeltpersoner i KS kjente til personer ansatt i KPMG med relevant kompetanse.

Informanten opplyser at de holdt NCSC, Kripos NC3 og Kommune-CSIRT oppdatert om hvordan håndteringen gikk underveis. Informanten beskriver kommunikasjonen med Kommune-CSIRT som informasjonsdeling og at kontakten var av begrenset omfang. Informanten beskriver også en opplevd usikkerhet rundt hvorvidt det ville være riktig fremgangsmåte å be om bistand fra NCSC under hendelseshåndteringen. Gjennom innsynsbegjæringer har jeg fått tilgang til korrespondanse mellom Krisestøtteenheten underlagt Justis- og beredskapsdepartementet og Helse- og omsorgsdepartementets avdeling for kriseledelse fra angrepsdagen. I e-postene kommer det frem at NSM og Kommune-CSIRT sammen utformet et varsel om hendelsen som DSB sendte ut til landets Statsforvaltere for å gjøre andre kommuner i stand til å håndtere lignende angrep. Et utdrag fra korrespondansen følger under:

> For å gjøre andre kommuner i stand til å møte lignende angrep oversender DSB et felles varsel til Statsforvalterne, utarbeidet av NSM og Kommune-CSIRT, som skal distribueres til landets kommuner. Flere kommuner er også i prosess med å knytte seg til Kommune-CSIRT og dette vil bidra til økt robusthet på sikt. (Krisestøtteenheten, 2021).

Dette samarbeidet mellom NSM, Kommune-CSIRT og DSB illustrerer både vertikalt samarbeid mellom det sektorovergripende nivået og SRM-nivået, og horisontalt samarbeid på

det sektorovergripende nivået. Det er også beskrivende for NCSC sitt fokus på å analysere hendelsers relevans for samfunnet og helhetlig risikoanalyse. Kommune-CSIRT fylte i denne delen av hendelseshåndteringen tilsynelatende rollen som et SRM. De var imidlertid ikke offisielt anerkjent som SRM på dette tidspunktet. Informant 2 opplyser at NCSC brukte Kommune-CSIRT som et SRM under håndteringen av hendelsen. Vedkommende forklarer også at Kommune-CSIRT fra etableringstidspunkt har vært rettet mot kommuner i Mjøs-regionen og at dette bidro til deres rolle i hendelseshåndteringen. Videre opplyses det at det eksisterer usikkerhet om hvordan SRM-nivået i styringssystemet skal fungere i relasjon til landets kommuner. Informant 3 opplyser at Kripos NC3 bisto det lokale politidistriktet i den innledende etterforskningen av hendelsen. Vedkommende opplyser på generelt grunnlag at: «...når vi blir koblet på gjør vi som vi pleier å gjøre, nemlig hjelper dem raskt og godt i gang. Vi er nøye på nettopp det, å sørge for at de får en god start, både taktisk og teknisk (Informant 3). Informant 3 beskriver også en ordning hvor NC3 ansetter innsatsledere med kompetanse på cybersikkerhet som kan rykke raskt ut og bistå politidistriktene i den tidlige etterforskningsfasen av IKT-kriminalitet.

Flere måneder etter deteksjon og iverksetting av prosesser og tiltak for å håndtere hendelsen eskalerte alvorlighetsgraden av den betraktelig. Informant 5 forklarer utviklingen som følger:

> Vi var på et stadium like før påske, slutten av mars for å si det enkelt, der vi begynte å trappe ned det meste av aktivitet sammen med KPMG. Fordi vi har veldig gode ressurser på gjenoppretting av systemer internt sammen med ny driftspartner. Men så skjedde det jo da i påskeuka at det ble lekket data som var eksfiltrert fra systemene våre. Så da blusset jo aktiviteten med KPMG opp igjen fordi de var og er veldig godt kjent med hendelsen siden de har vært med og håndtert den. Pluss at de har riktige kapabiliteter for å analysere og jobbe med den type hendelser. (Informant 5)

Lekket data fra kommunens IT-systemer kan potensielt få alvorlige konsekvenser på lengre sikt. Disse har kommunen sammenfattet i to separate dokumenter som er rettet mot *alle innbyggere over 16 år* og *virksomheter som har hatt kontakt med Østre Toten kommune*. Begge dokumentene er beskrevet som varsler og er utformet med utgangspunkt i at kommunen 31. mars ble oppmerksomme på at dokumenter inneholdende personopplysninger og sensitive opplysninger var lagt ut på det mørke nettet (Østre Toten kommune, 2021a, s. 1;

Østre Toten kommune; 2021b, s. 1) I varselet adressert til innbyggere opplyses det om 10 mulige konsekvenser og potensielle metoder for misbruk av informasjon. Blant disse er fare for offentliggjøring av tjenestebenyttelse, helseopplysninger og fagforeningstilhørighet. I varselet til virksomheter kommuniseres fire mulige konsekvenser av informasjonssikkerhetsbruddet. Blant disse er tap av konkurransefortrinn som følge av misbruk av informasjon og offentliggjøring av avtaler og samarbeid med kommunen som er unntatt offentligheten.

Informant 5 opplyser at det er utfordrende å håndtere informasjonssikkerhetsbruddet og at det har krevd bistand fra flere kompetansefelt. Vedkommende trekker blant annet frem behovet for juridisk bistand i forbindelse med problemstillinger knyttet til informasjon på avveie og personvern. KPMG bisto kommunen også i denne delen av hendelseshåndteringen. Informanten beskriver sin opplevelse av samarbeidet med KPMG på følgende vis:

> KPMG har gjort en strålende jobb på alle områder sammen med oss. Du kan si at det er nok de som har i veldig stor grad gjort at vi har kommet på rett spor med mange ting. Det var jo også de som varslet at etter deres mening gikk i feil retning med å gjenopprette lokal infrastruktur i Østre Toten kommune på grunn av manglende evne og kapabilitet til å ivareta sikkerheten på en god nok måte som da gjorde at vi startet en prosess med å se på andre muligheter. (Informant 5)

Det opplyses her at kommunen i utgangspunktet planla å gjenopprette drift av IT-infrastrukturen lokalt og drifte sine egne systemer som de hadde gjort før hendelsen. Dette rådet KPMG dem til å revurdere og Informant 5 opplyser at de endte opp med å inngå en avtale med selskapet Ikomm som også er driftsansvarlig for IT-systemer for fem andre kommuner. Gjenopprettingsfasen av hendelseshåndteringen foregår i nært samarbeid med Ikomm og informanten beskriver at dette er en kompleks prosess:

> Kommuner er komplekse, både på infrastruktur og systemsiden. Vi har en master-systemliste som vi bruker som gjenopprettingsverktøy. Den har 240 linjer som da er systemer, integrasjoner og som er ting som må hensynstas og som skal gjenopprettes. … Vi har en 60-70 forskjellige mer eller mindre store datasystemer, fagsystemer og den slags og alt rundt det som skal få det til å funke ikke sant. Det er komplekst. Det sier seg

> selv. Og det er mye sammenhenger ikke sant, så når du begynner å jobbe etter prioritert liste så er det sånn, med Ikomms ord da. Det vi gjør nå, det er ting de bruker et og et halvt år på å planlegge og et år på å gjennomføre. … Det vi nå gjør på 8 måneder det bruker de 2 og et halvt år på. (Informant 5)

Kompleksiteten i gjenopprettingsfasen av hendelseshåndteringen som Informant 5 beskriver kan potensielt bidra til økt forståelse av skadepotensialet som ligger i IKT-sikkerhetshendelser. Denne hendelsen og håndteringen av den kan tenkes å inneholde mange viktige læringspunkter for både kommuner og andre virksomheter, i det offentlige og det private. Informant 5 trekker frem er viktig læringspunkt på følgende vis:

> En av tingene vi har lært er at rett og slett på grunn av manglende logging, eventuelt at logger ikke går langt nok tilbake i tid, at vi har for lite å gå på i de tekniske undersøkelsene. Hadde vi hatt mer logging og sporbarhet så hadde vi funnet langt mer enn det vi gjør nå. Logging er viktig, både i bredde, dybde og tid. (Informant 5)

Informanten beskriver her at bedre logging av nettverkstrafikk kunne gjort det enklere å finne spor etter trusselaktøren som angrep kommunen. Dette kan være et læringspunkt som andre kan dra nytte av i tråd med myndighetenes fokus på evaluering og læring av hendelser (Departementene, 2019b, s. 29).

De direkte konsekvensene, informasjonssikkerhetsbruddene og den komplekse gjenopprettingsfasen som angrepet mot Østre Toten forårsaket illustrerer skadepotensialet som ligger i IKT-sikkerhetshendelser. Håndteringen av hendelsen foregikk som et samarbeid mellom kommunen og de tre private aktørene, Atea, KPMG og Ikomm. NCSC og Kripos NC3 hadde også roller med betydning for hendelsens konsekvenser for samfunnet. Kripos NC3 bisto det lokale politidistriktet med kompetanse i den innledende etterforskningsfasen. De ble begge holdt orientert under hendelsesforløpet og NCSC samarbeidet med Kommune-CSIRT om utforming av varsel til Statsforvalterne utsendt av DSB. Denne operative beslutningen kan tolkes som betydningsfull for etablering av felles situasjonsforståelse på tvers av sektorer og følgelig en motvirkende kraft mot den postulerte svakheten til sektorprinsippet knyttet til dette (Jensen, 2019, s. 269-270).

Måten samarbeidet mellom aktørene i styringssystemet foregikk på under hendelsen som rammet Østre Toten kommune fremstår som i tråd med deres mandat og intenderte funksjon fra myndighetenes side, med unntak av rollen Kommune-CSIRT fikk. Mangfoldet av aktører og typer samarbeid som inntraff under hendelsen kan oppfattes som velillustrerende for hvordan multistakeholder-samarbeid foregår i praksis. Utfra den informasjonen jeg har samlet inn og analysert dukket det ikke opp utfordringer knyttet til interessekonflikter under håndteringen. Graden av åpenhet som Østre Toten kommune har utvist om hendelsen og håndteringen fremstår som beundringsverdig og potensielt svært verdifull som ledd i en læringsprosess for andre kommuner og virksomheter.

6.0 Oppsummering og konklusjon

I det følgende vil jeg oppsummere analysen og trekke frem det jeg anser som de mest relevante elementene for problemstillingen og forskningsspørsmålene. Deretter presenterer jeg studiens funn i en konklusjon. Helt til slutt kommenterer jeg oppgavens begrensninger og gir anbefalinger for videre forskning.

6.1 Oppsummering

Det er avdekket tilstedeværelse av interessekonflikter mellom de sektorovergripende aktørene NCSC og Kripos NC3 i analysen. NCSC vil som regel ha som førsteprioritet å begrense skaden en IKT-sikkerhetshendelse forvolder virksomheten som er rammet. Kripos NC3 vil innlede etterforskning og sikre spor før drastiske tiltak som nedstenging av systemer implementeres. God kommunikasjon mellom de to etatene motvirker tilsynelatende at interessekonflikten får alvorlige konsekvenser. Det er også avdekket at det foreligger overlapping på noen ansvarsområder mellom NCSC og Kripos NC3. Dette kan oppfattes som negativt fordi det kan resultere i ineffektivitet som følge av fragmentert ansvarsfordeling og uvettig ressursbruk.

Samhandlingsmekanismen FCKS bidrar ifølge informantene fra NSM og Kripos NC3 til å løse utfordringer forbundet med interessekonflikt gjennom kommunikasjon mellom de sektorovergripende etatene som er del av den. Verdien av mekanismen opplyses å være særlig stor under alvorlige hendelser som rammer mange virksomheter. De etablerte kommunikasjonskanalene mellom NCSC og NC3 blir omtalt som velfungerende av informantene og koordinerende virksomhet inntreffer ofte vedrørende løsepengevirusangrep. Alle de fire informantene som arbeider med hendelseshåndtering vektlegger god kommunikasjon med ansatte hos andre aktører i styringssystemet som en motvirkende kraft til utfordringer på feltet. En av informantene fra NSM og informanten fra HelseCERT opplyser også om uformelle relasjoner med ansatte hos andre aktører som gjør at det er lav terskel for å ta kontakt og løse problemer gjennom kommunikasjon.

Overlappende ansvarsområder har blitt omtalt som en svakhet ved sektorprinsippet (Jensen, 2019, s. 269). Informant 2 fra NSM og Informant 3 fra Kripos NC3 anerkjenner dette fenomenet men betrakter de ikke som et stort problem. Informant 2 fokuserer på at de ulike mandatene og interessene bidrar til ulike tilnærminger til problemstillinger som kan bidra til mer veloverveide beslutninger under hendelseshåndtering. Informant 3 beskriver at overlapp

kan sees på som noe positivt siden det vitner om tilstrekkelig kapasitet på et område. Det kan imidlertid representere en utfordring i form av uvettig ressursbruk.

Gjennom analyse i samtid av IKT-sikkerhetshendelsers betydning for andre virksomheter både i det offentlige og det private bidrar NCSC til å motvirke den postulerte svakheten om manglende felles situasjonsforståelse som ligger i sektorprinsippet. Ved å produsere notater og varsler som distribueres til andre virksomheter som potensielt er sårbare for lignende IKT-sikkerhetshendelser som er pågående er NCSC bidragsyter til etablering av felles situasjonsforståelse av trusselbildet og risiko. Dette fenomenet illustreres av NSM, Kommune-CSIRT og DSBs operative beslutninger under håndteringen av dataangrepet mot Østre Toten kommune i januar 2021. Distribusjon av varsel til landets Statsforvaltere som så ble videreformidlet til andre kommuner kan tenkes å ha forhindret nye alvorlige angrep mot andre kommuner.

Løsepengevirusangrepet som rammet Østre Toten kommune illustrerer hvor alvorlige konsekvenser IKT-sikkerhetshendelser kan få. Manglende evne til å levere helt grunnleggende tjenester som helsehjelp viser hvorfor slike hendelser må tas på alvor. Samarbeidet mellom kommunen, Atea, KPMG og Ikomm ble beskrevet som velfungerende av Informant 5 ansatt i kommunen og viser hvordan private virksomheter kan spille en viktig rolle under hendelseshåndtering. Informasjonsdelingen fra kommunen til NCSC og Kommune-CSIRT dannet grunnlag for det tidligere beskrevne varselet og bidro således til å håndtere de potensielle negative konsekvensene av hendelsen i samfunnet for øvrig. Den langvarige og komplekse gjenopprettingsfasen av hendelseshåndteringen som kommunen har stått i siden deteksjon illustrerer at håndtering av IKT-sikkerhetshendelser er krevende.

6.2 Konklusjon

Det samlede inntrykket etter analyse av myndighetenes strategi, tiltak og prosedyrer i kombinasjon med informantenes svar om tiltakenes virkning i praksis er at det de senere år er påbegynt en betydelig satsning på tverrsektorielt og offentlig-privat samarbeid innenfor IKT-sikkerhet på overordnet nivå og hendelseshåndtering spesifikt. Dette samarbeidet foregår i flere spor på tvers av sektorer og mellom det offentlige og det private gjennom informasjonsdeling og koordinasjon av innsats. Navet i dette samarbeidet er Nasjonalt cybersikkerhetssenter som har inntatt sin intenderte rolle som tilrettelegger for informasjonsdeling og koordinering. Gjennom VDI-samarbeidet, partnersamarbeidet, partner-briefs, ordninger for SRM-samarbeid og kvalitetsordningen for IT-sikkerhetsselskaper

tilrettelegger NCSC for både tverrsektorielt og offentlig-privat samarbeid. Samarbeid mellom det sektorovergripende nivået i styringssystemet og SRM-nivået fremstår som velfungerende.

NCSC bidrar i samarbeid med alle de andre aktørene i styringssystemet også til etablering av en felles situasjonsforståelse av trussel- og risikobildet. Denne situasjonsforståelsen blir til gjennom informasjonsdeling mellom alle nivåene i systemet på tvers av det offentlige og det private. Gjennom samarbeid med andre sektorovergripende aktører som eksempelvis DSB kommuniseres situasjonsforståelsen ut til virksomheter og organer i samfunnet for øvrig når det anses som nødvendig. Slik praksis motvirker den postulerte svakheten som ligger i sektorprinsippet vedrørende manglende felles situasjonsforståelse (Jensen, 2019, s. 269-270).

Kripos NC3 har inntatt sin rolle som Politiet på internett og arbeider med å oppskalere sin kapasitet. Senteret bistår de lokale politidistriktene med innsatsledere og kompetanse for å gjøre dem bedre i stand til å etterforske og bringe IKT-kriminalitet til påtale. De samarbeider med NCSC gjennom koordinerende virksomhet og informasjonsdeling, de deler og mottar også informasjon med SRM-nivået. Det foreligger en overlapping av ansvarsområder mellom Kripos NC3 og NCSC. Dette kan potensielt føre til uvettig ressursbruk, men dette fenomenet er ikke påvist i noen særlig grad gjennom mine analyser.

I henhold til den den hierarkiske delen av multistakeholder-typologien for styring på cybersikkerhetsfeltet vil ineffektivitet og tungroddhet kunne prege myndighetsaktørers arbeid i cyberspace (Eggenschwiler, 2018, s. 72). Denne ineffektiviteten kan gjøre seg gjeldende som følge av interessekonflikt som hindrer effektivt samarbeid (Muller, 2016, s. 17). Tilstedeværelse av slik interessekonflikt har i denne studien blitt påvist mellom de sektorovergripende myndighetsaktørene NCSC og Kripos NC3. Alvorlighetsgraden av disse virker imidlertid å motvirkes betydelig av tre faktorer: Formelle kommunikasjonskanaler mellom aktører, etablerte uformelle relasjoner mellom ansatte og samhandlingsmekanismen FCKS. God kommunikasjon og kjennskap til ansatte i andre organisasjoner virker å styrke evne til godt samarbeid om hendelseshåndtering på tvers av nivåer.

Multistakeholder-typologien og i forlengelsen multistakeholder-initiativer har blitt koblet til svakheter gjennom uklar ansvarsfordeling og «maktkamp» mellom det offentlige og det private (Muller, 2016, s. 2-3). «Maktkamp» mellom det offentlige og det private er i denne studien kun påvist mellom Kripos NC3 og private IT-sikkerhetsselskaper på åsteder for IKT-kriminalitet. Kripos NC3 virker å ha en proaktiv innstilling til å løse slike «maktkamper» og er i prosess med å etablere en samarbeidskonstruksjon i form av intensjonsavtaler med IT-

sikkerhetsselskaper som skal etablere prosedyrer for hvordan hendelseshåndtering på åsteder fungerer.

Åpenhet fra dem som rammes av IKT-sikkerhetshendelser styrker samfunnets evne til å håndtere hendelser gjennom bevisstgjøring og læring som kommer alle til gode. Læringspunkter fra hendelser kan bidra til at andre aktører i samfunnet for øvrig blir bevisste på det store skadepotensialet som ligger i IKT-sikkerhetshendelser. Dette kan motivere til iverksettelse av prosesser for å bedre sin egen sikkerhetssituasjon. Åpenhet om hendelser bidrar til en form for samarbeid på tvers av alle institusjoner i samfunnet. Det bidrar til vår alles felles situasjonsforståelse av de mange sårbarhetene og truslene som vi står ovenfor i vår digitale hverdag.

6.3 Begrensninger

Denne studien har undersøkt samarbeid om håndtering av IKT-sikkerhetshendelser i svært vid forstand. Tilnærmingen til datainnsamling og analyse av empiri har vært preget av et ønske om å utforske cybersikkerhetsfeltet og oppdage ulike former for samarbeid og betydningen av dem. Dette gjør at funn og konklusjon bør tolkes som del av en form for kartleggingsstudie som ikke danner grunnlag for inngående teknisk forståelse av samarbeid om håndtering av IKT-sikkerhetshendelser.

Datagrunnlaget for analysen i denne oppgaven består av offentlig tilgjengelige dokumenter og dokumenter som kan erverves gjennom innsynsbegjæringer. Dette gjør at det potensielt kan være informasjon som er relevant for problemstilling og forskningsspørsmål som ikke har blitt analysert. Grunnet tematikkens sikkerhetsmessige betydning er en god del informasjon gradert.

Styringssystemet som er utformet som del av operasjonaliseringen i denne studien fanger ikke opp alle aktører som er betydningsfulle for hendelseshåndtering i Norge, kun de som fremstår som de viktigste. Derfor må funnene om samarbeidet mellom aktører og nivåer i systemet kun forstås som beskrivende for én del av samfunnets kapasitet til å håndtere IKT-sikkerhetshendelser. Det foregår omfattende og betydningsfullt arbeid med hendelseshåndtering i det private og samarbeid mellom private aktører kan tenkes å ha stor betydning for samfunnets overordnede evne til å håndtere IKT-sikkerhetshendelser.

6.4 Anbefalinger til videre forskning

Samarbeidet som er belyst i denne studien foregår både tverrsektorielt og mellom det offentlige og det private. Det kunne potensielt vært fruktbart å gjennomføre en studie av kun tverrsektorielt eller offentlig-privat samarbeid som går dypere inn i hvordan det arter seg isolert. Det fremstår som potensielt interessant å undersøke samarbeid på feltet med hovedfokus på de private aktørenes forhold til det offentlige og eventuelt gjennomføre intervjuer med representanter for IT-sikkerhetsbransjen. Det kunne også vært interessant å kartlegge samarbeid mellom IT-sikkerhetsselskaper i lys av markedstypologien for cybersikkerhetsstyring.

Den sektorovergripende koordineringen som foregår gjennom samhandlingsmekanismen FCKS fremstår også som svært interessant og relevant for hvordan myndigheter og samfunnet evner å møte trusler i det digitale rom. En tenkt studie kunne undersøkt hvordan koordineringen mellom Etterretningstjenesten, Kripos NC3, NSM og PST foregår og hvilke hensyn som har betydning for deres arbeid. Dette er også interessant sett i lys av utfordringene forbundet med interessekonflikt beskrevet i denne oppgaven.

Referanseliste

Ahmad, A., Hadgkiss, J. & Ruighaver, A. B. (2012). Incident response teams – Challenges in supporting the organizational security function. Computers & Security 31, 643-652.

Arbeids- og sosialdepartementet (2021, 23. mars). Oppfølging og rapportering på digital sikkerhet fra Arbeids- og sosialdepartementet. Brev til FD og JD (Innsynsbegjært).

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J. & Weiss, J. (2012). *Cyber Security Policy Guidebook*. New Jersey: Wiley.

Bergsjø, H. (2020). Hendelseshåndtering og opprydding. I H. Bergsjø., R. Windvik & L. Øverlier (Red.), *Digital sikkerhet – En innføring* (s. 267-278). Oslo: Universitetsforlaget.

Bevir, M. (2011). Governance as Theory, Practice and Dilemma. I M. Bevir (Red.), *The SAGE Handbook of Governance* (s. 1-16). London: SAGE Publications.

Bevir, M. (2012). *Governance: A Very Short Introduction*. Oxford: Oxford University Press.

Bouckaert, G., Peters, B. G. & Verhoest, K. (2010). *The Coordination of Public Sector Organizations: Shifting Patterns of Public Management*. London: Palgrave Macmillan.

Bratberg, Ø. (2018). *Tekstanalyse for samfunnsvitere* (2. utgave). Oslo: Cappelen Damm Akademisk.

Cavelty, M. D. (2018). Cybersecurity. I B. Warf (Red.), *The SAGE Encyclopedia of The Internet* (s. 146-153). London: SAGE Publications.

Choucri, N. & Clark, D. D. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. *MIT Political Science Department Research Paper 2012*(29).

Clemente, D. (2011). International Security: Cyber Security As A Wicked Problem. *The World Today 67*(10), 15-17.

De forskningsetiske komiteene. (2015, 16. juni). Ansvar for den enkelte. Hentet fra https://www.forskningsetikk.no/ressurser/fbib/personvern/ansvar-for-den-enkelte/ lest 23.05.2021.

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet*. Hentet fra https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

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

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

DIFI & DFØ. (2019). *Departementene i førersetet for omstilling? Rapport 2019*(3). Hentet fra https://dfo.no/filer/Fagomr%C3%A5der/Rapporter/Rapporter-Difi/departementene_i_forersetet_for_omstilling_-_difi-rapport_2019-3_et_samarbeidsprosjekt_med_dfo.pdf

DSB. (2012). Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering. Hentet fra https://www.dsb.no/globalassets/dokumenter/risiko-sarbarhet-og-beredskap/pdf-er/kongelig_resolusjon_15_06_2012.pdf

DSB. (2019). Digital 2020: Invitasjon til informasjonsmøte for private virksomheter. Brev. (Innsynsbegjært)

DSB. (2020a). Digital 2020: Rapportering fra virksomheter Digital 2020. Brev. (Innsynsbegjært)

DSB. (2020b). *Risikostyring i digitale verdikjeder*. Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/risikostyring-i-digitale-verdikjeder.pdf

Ellis, R. & Mohan, V. (2019). Introduction. I R. Ellis, V. Mohan (Red.), *Rewired: Cybersecurity Governance* (Introduksjon). Hoboken: Wiley.

Eggenschwiler, J. (2017). Accountability challenges confronting cyberspace governance. *Internet policy review 6*(3), 1-11.

Eggenschwiler, J. (2018). A Typology of Cybersecurity Governance Models. *St Anthony's International Review 13*(2), 64-78.

Eggenschwiler, J. (2019). An Incident-Based Conceptualization of Cybersecurity Governance. I R. Ellis, V. Mohan (Red.), *Rewired: Cybersecurity Governance* (s. 81-96). Hoboken: Wiley.

Eie, K., M. (2020). Trusler og etterretning. I H. Bergsjø., R. Windvik & Lasse Øverlier (Red.), *Digital sikkerhet – En innføring* (s. 145-183). Oslo: Universitetsforlaget.

ENISA. (2021). CSIRTs by Country - Interactive Map – Norway. Hentet fra https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Norway lest 14.05.2021.

Enroth, H. (2011). Policy Network Theory. I M. Bevir (Red.), *The SAGE Handbook of Governance* (s. 19-35). London: SAGE Publications.

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

EU. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Hentet fra https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&qid=1621690339474&from=EN

Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet. (2003). *Nasjonal strategi for informasjonssikkerhet: Utfordringer, prioriteringer og tiltak.* Hentet fra https://www.regjeringen.no/globalassets/upload/kilde/mod/red/2000/0002/ddd/pdfv/249054-nasjonal_strategi_for_informasjonssikkerhet.pdf

Forsvarets forskningsinstitutt. (2020). *Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene – en vurdering*. Hentet fra https://publications.ffi.no/nb/item/asset/dspace:6767/20-01560.pdf

Gundersen, G. (2020). Lover og ansvar. I H. Bergsjø., R. Windvik & L. Øverlier (Red.), *Digital sikkerhet – En innføring* (s. 109-126). Oslo: Universitetsforlaget.

Hanssen, G. S., Hovik, S. & Hundere, G. C. (2014). Den nye vannforvaltningen – Nettverksstyring i skyggen av hierarki. *Norsk statsvitenskapelig tidsskrift 2014*(3), 155-180.

Helgestad, B. (2021). Innlegg på Sikkerhetskonferansen 2020. Hentet fra https://www.youtube.com/watch?v=JSGuH0HAVQ4 5.32-8.45.

Hellevik, O. (1980). *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.

HelseCERT. (2021). Norsk Helsenett – HelseCERT, Helsenettet og Nasjonalt Beskyttelsesprogram. (Innsynsbegjært)

Helse- og omsorgsdepartementet. (2021, 26. mars). Oppfølging og rapportering på digital sikkerhet. Brev til JD (Innsynsbegjært).

Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I.-A. & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection 2*(1), 26-37.

Justis- og politidepartementet. (2004). *Samfunnssikkerhet og sivilt-militært samarbeid* (Meld. St. 39 (2003-2004)). Hentet fra https://www.regjeringen.no/contentassets/5f624a82750b4b14b3a7717e6bdb3516/no/pdfs/stm200320040039000dddpdfs.pdf

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

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

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

Kaarbø, A. (2019). Vil ha mer endring og samordning i departementene. *Stat & styring 2019*(2), 2-4.

Kantar. (2020). *Forsvarets innbyggerundersøkelse 2020*. Hentet fra https://www.forsvaret.no/aktuelt-og-presse/publikasjoner/forsvarets-innbyggerundersokelse/Forsvarets%20innbyggerunders%C3%B8kelse%202020.pdf/_/attachment/inline/d9829eb1-e2fd-475e-a86f-df6a4959a0f9:33c5ed6e623b2e14e7c7930bbd15c7ed3650ab3a/Forsvarets%20innbyggerunders%C3%B8kelse%202020.pdf

Kremling, J. & Parker A. M. S. (2018). *Cyberspace, Cybersecurity, and Cybercrime*. London: SAGE Publications.

Kommunal- og moderniseringsdepartementet. (2021, 26. mars). Rapportering på digital sikkerhet. Brev til Datatilsynet (Innsynsbegjært).

Kommune-CSIRT. (2021). *Digitalt situasjonsbilde: Rapport nr. 1 2021*. Hentet fra https://kommunecsirt-no.offcenit.com/Digitalt-situasjonsbilde-K-CSIRT-no.1-2021.pdf?mtime=20210415142639&focal=none

Krisestøtteenheten. (2021). Oppdatering: Kompromittering av IT-systemene i Østre Toten kommune. E-post til HOD-Krisestab. (Innsynsbegjært).

Langø, H.-I. (2013). Den akademiske debatten om cybersikkerhet. *Internasjonal politikk 71*(2), 229-240.

Langø, H.-I. & Sandvik, K. B. (2013). Cyberspace og sikkerhet. *Internasjonal politikk 71*(2), 221-228.

Lie, A. & Mydske, P. K. (2018). Virksomhetsstyring, etatsstyring og sektorstyring. *Stat & styring 2018*(3), 56-60.

Line, M. B. (2015). *Understanding Information Security Incident Management Practices: A Case Study in the Electric Power Industry* (Doktoravhandling, NTNU). Hentet fra https://infosec.sintef.no/wp-content/uploads/2015/09/2015-MBL-PhD-thesis-Part-1-2.pdf

Lyngaard, K. (2012). Dokumentanalyse. I S. Brinkmann &. og L. Tanggaard (Red.), *Kvalitative metoder: Empiri og teoriutvikling*. (s. 153-170). Oslo: Gyldendal.

Malone, E. F. & Malone, M. J. (2013). The "wicked problem" of cybersecurity policy: analysis of United States and Canadian policy response. *Canadian Foreign Policy Journal 19*(2), 158-177.

Muller, L. P. (2016). Makt og avmakt i cyberspace: hvordan styre det digitale rom? *Internasjonal politikk 74*(4), 1-23.

Muller, L. P. (2019). Inn i gråsonen: avskrekking som forsvar av cyberspace? *Internasjonal politikk 77*(3), 288-295.

NHO. (2019, 12. september). Åpenhet har hindret nye cyberangrep. Hentet fra https://www.nho.no/tema/offentlig-sektor-og-naeringslivet/artikler/apenhet-har-hindret-nye-cyberangrep/ lest 07.05.2021.

NorSIS. (2021). *Trusler og trender 2021*. Hentet fra https://norsis.no/wp-content/uploads/2021/03/NorSIS_Trusler_Trender_2021_Digital.pdf

Norsk Hydro. (2019, 20. september). Hydro tildeles pris for åpenhet etter cyberangrep. https://www.hydro.com/no-NO/media/news/2019/hydro-tildeles-pris-for-apenhet-etter-cyberangrep/ lest 07.05.2021

Norsk Hydro. (2020, 14. oktober). Cyberangrep på Hydro. Hentet fra https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/ lest 07.05.2021.

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

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn: Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo: Justis- og beredskapsdepartementet. Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2016: 19. (2016). *Samhandling for sikkerhet: Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Oslo: Forsvarsdepartementet. Hentet fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

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

NOU 2021: 6. (2021). *Myndighetenes håndtering av koronapandemien – Rapport fra Koronakommisjonen*. Oslo: Statsministerens kontor. Hentet fra https://www.koronakommisjonen.no/files/2021/04/Koronakommisjonens_rapport_NOU.pdf

NRK. (2020, 10. desember). Stortinget ikke alene: Massivt hackerangrep mot Norge. Hentet fra https://www.nrk.no/norge/stortinget-ikke-alene_-massivt-hackerangrep-mot-norge-1.15277734 lest 06.05.2021.

NSM. (2017a). Begrepsliste til bruk for rammeverk for håndtering av IKT-sikkerhetshendelser. I *Rammeverk for håndtering av IKT-sikkerhetshendelser* – Vedlegg 4. Hentet fra https://nsm.no/getfile.php/133863-1593022742/Demo/Dokumenter/vedlegg-4---begrepsliste.pdf

NSM. (2017b). Klassifisering av IKT-sikkerhetshendelser. I *Rammeverk for håndtering av IKT-sikkerhetshendelser* – Vedlegg 5. Hentet fra https://nsm.no/getfile.php/133866-1593022796/Demo/Dokumenter/vedlegg-5---klassifisering-av-ikt-sikkerhetshendelser.pdf

NSM. (2017c). *Rammeverk for håndtering av IKT-sikkerhetshendelser*. Hentet fra https://nsm.no/getfile.php/133853-1593022504/Demo/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

NSM. (2019). Risiko 2019: Krafttak for et sikrere Norge. Hentet fra https://nsm.no/getfile.php/133696-1592910347/Demo/Dokumenter/Rapporter/nsm_risiko_2019_final_enkeltside.pdf

NSM. (2020a). *NSMs grunnprinsipper for IKT-sikkerhet*. Hentet fra https://nsm.no/getfile.php/133735-1592917067/Demo/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

NSM. (2020b, 6. januar). Varslingssystem for digital infrastruktur (VDI) Hentet fra https://nsm.no/tjenester/varslingssystem-vdi/ lest 12.05.2021

NSM. (2020c). NCSC-varsel i forbindelse med koronaviruset. (Innsynsbegjært).

NSM. (2021a). Felles cyberkoordineringssenter (FCKS) etableres. Hentet fra https://nsm.no/om-oss/historien-om-nsm/felles-cyberkoordineringssenter-fcks-etableres lest 14.05.2021

NSM. (2021b). *RISIKO 2021 – helhetlig sikring mot sammensatte trusler*. Hentet fra https://nsm.no/getfile.php/136419-1616673370/Demo/Dokumenter/Rapporter/NSM_Risiko_2021_web_enkeltside_1203.pdf

NUPI. (2021). NUPI's Centre for Digitalization and Cyber Security Studies. Hentet fra https://www.nupi.no/nupi_eng/Our-research/Research-centres/NUPI-s-Centre-for-Digitalization-and-Cyber-Security-Studies lest 05.05.2021.

Næringslivets sikkerhetsråd. (2020). *Mørketallsundersøkelsen 2020*. Hentet fra https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Politiet. (2021a). National Cybercrime Centre (NC3). Hentet fra https://www.politiet.no/en/om/organisasjonen/specialist-agencies/kripos/key-roles-of-ncis/national-cybercrime-centre/ lest 19.05.2021.

Politiet. (2021). *Politiets trusselvurdering 2021*. Hentet fra https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/2021-02-12-o-ptv-2021.pdf

PST. (2021). *Nasjonal trusselvurdering 2021*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf

Raymond, M. & DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory 7*(3), 572-616.

Regjeringen. (2019, 3. mai). Nasjonal sikkerhetsmyndighet overføres til Justis- og beredskapsdepartementet. Hentet fra https://www.regjeringen.no/no/aktuelt/nasjonal-sikkerhetsmyndighet-overfores-til-justis--og-beredskapsdepartementetny-side/id2643809/ lest 19.05.2021.

Regjeringen. (2021, 3. februar). Felles fremlegging av trusselvurderinger. Hentet fra https://www.regjeringen.no/no/aktuelt/trusselvurderinger21/id2831242/ lest 19.05.2021.

Riksrevisjonen (2020). *Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer*. Hentet fra https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer.pdf

Rittel, H. W. J. & Webber, M. M. (1973). Dilemmas in a General Theory of Planning. Policy sciences 4(2), 155-169.

Schia, N. N. (2019). Forord: Cybersikkerhet. *Internasjonal politikk 77*(3), 223-224.

Sikkerhetsloven. (2018). Lov om nasjonal sikkerhet. (LOV-2018-06-01-24). Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24 lest 12.05.2021

SINTEF. (2021). Cybersecurity is our field of expertise. Hentet fra https://infosec.sintef.no/en/about-us/ lest 05.05.2021.

Skjørland, I. & Thoreid, R. (2018). *Hvordan evner sentrale aktører å samhandle ved IKT-hendelser* (Masteroppgave). Universitetet i Stavanger, Stavanger. Hentet fra https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2580427/Skjorland_Ingrid_Thoreid_Renate.pdf?sequence=1&isAllowed=y

Smith, E. (2015). "Ministerstyre" – Et hinder for samordning? *Nytt norsk tidsskrift 2015*(3), 258-266.

Svenungsen, B. (2019). *Vårt digitale fundament. IFS Insights 5*. Hentet fra https://fhs.brage.unit.no/fhsxmlui/bitstream/handle/11250/2614405/IFS%20Insight%205_2019.pdf

Sykehuset Innlandet H. 2018. Notat: Innbrudd i datasystemene til Sykehuspartner i Helse Sør-Øst. Hentet fra https://sykehuset-innlandet.no/seksjon/styret/Documents/2018/2018-01/007-2018%20Vedlegg%2003E%20Dataangrep%20i%20Helse%20S%C3%B8r-%C3%98st%20%20-%20bakgrunn%20og%20status.pdf

Sylstad, M. (2016). Figur: Varslingssystem for kritisk infrastruktur.

Sørensen, E. & Torfing, J. (2011). Governance Networks. I B. Badie., D. Berg-Schlosser & L. Morlino (Red.), *International Encyclopedia of Political Science* (s. 1029-1035). Los Angeles: SAGE Publications.

Tanggaard, L. & Brinkmann, S. (2012). Intervjuet: Samtalen som forskningsmetode. I S. Brinkmann &. og L. Tanggaard (Red.), *Kvalitative metoder: Empiri og teoriutvikling.* (s. 17-45). Oslo: Gyldendal.

Telenor. (2020). Slik bedrer du datasikkerheten på hjemmekontoret. Hentet fra https://www.telenor.no/bedrift/sikkerhet/hjemmekontor/ lest 19.05.2021.

Tøndel, I.-A., Line, M. B. & Jaatun, M. G. (2014). Information security incident management: Current practice as reported in the literature. *Computers & Security 45*, 42-57.

Verhoest, K., Peters, G. B., Beuselinck, E., Meyers, F. Bouckaert, G. (2005). *How coordination and control of public organizations by government interrelate: An analytical and empirical exploration.*

Weber, E. P. & Khademian, A. M. (2008). Wicked Problems, Knowledge Challenges, and Collaborative Capacity Builders in Network Settings. *Public administration review 68*(2), 334-349.

Windvik, R. (2020). Introduksjon til digital sikkerhet. I H. Bergsjø., R. Windvik & L. Øverlier (Red.), *Digital sikkerhet – En innføring* (s. 15-32). Oslo: Universitetsforlaget.

Østre Toten kommune. (2020a). Varsel om at foretakssensitive opplysninger kan være på avveie. Hentet fra https://www.ostre-toten.kommune.no/_f/p1/i5b3be1df-d2ff-4de4-a359-2dc5fe99bbbb/dataangrepet-massevarsling-naringsliv.pdf

Østre Toten kommune. (2020b). Varsel om at personopplysninger er på avveie. Hentet fra https://www.ostre-toten.kommune.no/_f/p1/i42329283-e953-4a69-b352-8cf19e344dd4/dataangrepet-varsling-massevarsling.pdf

Vedlegg

Vedlegg 1: Innsynsbegjæringer

Innsynsbegjæringer gjennom eInnsyn

13.04.2021 kl. 14:56 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2016/6093 180
13.04.2021 kl. 14:56 Varsel fra Nasjonalt Cybersikkerhetssenter - Etterregistrert Rapporteringer i forbindelse med Covid-19 2020/2019 5
13.04.2021 kl. 14:56 Kommune - CSIRT IKS - nasjonalt senter for informasjonssikkerhet i kommunesektoren Kommune-CSIRT IKS - nasjonalt senter for informasjonssikkerhet i kommunesektoren 2019/11403 1
13.04.2021 kl. 14:56 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for digital sikkerhet 2021/145 2
13.04.2021 kl. 14:56 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2016/6093 181
13.04.2021 kl. 14:56 Oppdatering: Kompromittering av IT-systemene i Østre Toten kommune Hendelser 2021 2021/28 6
13.04.2021 kl. 14:56 Samfunnssikkerhet - Digitale trusler Samfunnssikkerhet - Digitale trusler 2021/2099 1
13.04.2021 kl. 14:56 Oppdatering: Kompromittering av IT-systemene i Østre Toten kommune Hendelser 2021 2021/28 9
13.04.2021 kl. 14:56 Myndighetenes samordning av arbeidet med digital sikkerhet - oppstart av foranalyse Myndighetenes samordning av arbeidet med digital sikkerhet 2021/2042 1
13.04.2021 kl. 14:56 Rapportering på digital sikkerhet - Innspill Stortingsmelding 2017/787 18
13.04.2021 kl. 14:56 Oppfølging av ny sikkerhetslov - Justeringer i tidligere innrapportering Implementering av ny sikkerhetslov i ASDs sektor 2019/35 34
13.04.2021 kl. 14:56 Tilbud om plass i Nasjonalt cybersikkerhetssenter Nasjonalt cybersikkerhetssenter 2019/5393 6
13.04.2021 kl. 14:56 Rapportering på digital sikkerhet Statsbudsjettet 2021 - Datatilsynet - tildelingsbrev og etatsstyring 2020/4276 12
13.04.2021 kl. 14:56 Myndighetenes samordning av arbeidet med digital sikkerhet - oppstart av foranalyse Myndighetenes samordning av arbeidet med digital sikkerhet 2021/1996 1
13.04.2021 kl. 14:56 Rapportering på nasjonal strategi for digital sikkerhet Felles innsats - ny nasjonal strategi for digital sikkerhet 2019/8234 4
13.04.2021 kl. 14:56 Oppfølging og rapportering på digital sikkerhet Stortingsmelding 2017/787 19
13.04.2021 kl. 14:56 Status - digital sikkerhet i sivil sektor - 110800A mar 2021 Rapportering på samfunnskritiske funksjoner (KIKS) - Covid-19 2020/1854 818
13.04.2021 kl. 14:56 NSM - Status digital sikkerhet i sivil sektor 04032021 Rapportering på samfunnskritiske funksjoner (KIKS) - Covid-19 2020/1854 805
13.04.2021 kl. 14:56 Notater og refleksjoner - NCSS Nasjonalt cybersikkerhetssenter 2019/5393 3
13.04.2021 kl. 14:56 Oppfølging og rapportering i forbindelse med Nasjonal strategi for digital sikkerhet Stortingsmelding 2017/787 17
13.04.2021 kl. 14:56 Informasjon om nasjonal tverrsektoriell øvelse "Digital 2020" Nasjonal tverrsektoriell øvelse Digital 2020 2019/3403 1
13.04.2021 kl. 14:56 Kompromittering av IT-systemene i Østre Toten kommune Hendelser 2021 2021/28 7
26.04.2021 kl. 13:57 Statusmøte i utviklingen av FCKS Felles cyberkoordineringssenter FCKS 2017/2509 3
26.04.2021 kl. 13:57 Årsrapport Prosjekt: Datadrevne trusselvurderinger og -analyser 2020/196 3
26.04.2021 kl. 13:57 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for digital sikkerhet med tiltaksoversikt og nasjonal strategi for digital sikkerhetskompetanse 2018/89 35
26.04.2021 kl. 13:57 ASD sektor trekker sin deltakelse i Øvelse Digital 2020 Øvelse Seminar - ASD DSB Direktoratet for samfunnssikkerhet og beredskap Justis og beredskapsdepartementet JD - Øvelse Digital 2020 Digitalt kompetansehevingsseminar 2020/1251 1
26.04.2021 kl. 13:57 Plan for videre etablering av NC3 i Kripos Nasjonal strategi for bekjempelse av IKT-kriminalitet - Datakrimstrategi 2013/2063 41
26.04.2021 kl. 13:57 Høringsinnspill - Digital sårbarhet - sikkert samfunn Høring - Digital sårbarhet - sikkert samfunn 2015/4848 9
26.04.2021 kl. 13:57 Tjenestetilbud ENISA Nasjonal strategi for digital sikkerhet med tiltaksoversikt og nasjonal strategi for digital sikkerhetskompetanse 2018/89 36
26.04.2021 kl. 13:57 Signert avtale, NCSC, Luftfartstilsynet - Avskjermet 2019/10145 24

26.04.2021 kl. 13:57 Kontaktpunkter for DSB i de hovedansvarlige departementer - Ber om tilbakemelding Covid-19 - Hendelseshåndtering 2020 2020/593 63
26.04.2021 kl. 13:57 Årsrapport Prosjekt: Netsecurity Security Operations Center 2019/11141 3
26.04.2021 kl. 13:57 Evalueringsdirektiv - øvelse Digital 2020 Øvelse Digital 2020 2019/305 23
26.04.2021 kl. 13:57 Tilknytting til HelseCERT for virksomheter i BLDs sektor IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 6
26.04.2021 kl. 13:57 Avtale til signering - Avtale med HelseCERT Norsk Helsenett - HelseCERT 2018/56327 5
26.04.2021 kl. 13:57 Ferdig referat diskusjonsøvelse Digital 2020 - 03122020 Øvelse Digital 2020 2019/305 29
26.04.2021 kl. 13:57 Samordning av arbeidet med digital sikkerhet - informasjon Riksrevisjonen - Foranalyse om myndighetenes samordning av arbeidet med digital sikkerhet 2021/3107 2
26.04.2021 kl. 13:57 Øvelse Digital 2020 - Invitasjon til informasjonsmøte for departementene Krisestøtteenhet for departementsfellesskapet - KSE - Forum for beredskapsmedarbeidere - tidligere Regjeringens kriseråd - h.u. Kriserådet 2014/8936 57
26.04.2021 kl. 13:57 Etablering av Felles cyberkoordineringssenter FCKS - kopi av brev til NSM Felles cyberkoordineringssenter FCKS 2017/2509 2
26.04.2021 kl. 13:57 Invitasjon til planleggingskonferanse II for Øvelse Digital 2020 Øvelse Digital 2020 2019/3084 10
26.04.2021 kl. 13:57 Øvelse Digital 2020 - Informasjonsmøte for private virksomheter Krisestøtteenhet for departementsfellesskapet - KSE - Forum for beredskapsmedarbeidere - tidligere Regjeringens kriseråd - h.u. Kriserådet 2014/8936 56
26.04.2021 kl. 13:57 Invitasjon - Digital sikkerhet 2020 - De lange linjene Invitasjoner generelle - Direktør DSB - assisterende direktører 2020 2019/13789 22
26.04.2021 kl. 13:57 Evalueringsdirektiv - øvelse Digital 2020 Øvelse Digital 2020 2019/305 25
26.04.2021 kl. 13:57 Vedrørende fornyelse av medlemskap i NCSC partnersamarbeidet Tilbud om plass i Nasjonalt cybersikkerhetssenter 2019/2606 8
26.04.2021 kl. 13:57 Bekreftelse på plass i NCSCNSM / NorCERT - VDI og annet samarbeid 2017/23617 5
26.04.2021 kl. 13:57 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2016/6093 194
26.04.2021 kl. 13:57 Svar på oppfølging og rapportering på digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2018/70 32
26.04.2021 kl. 13:57 Høring av rapport avgitt av Lysne II-utvalget om digitalt grenseforsvar DGF Lysne II - høring 2016/2699 1
26.04.2021 kl. 13:57 FCKS temarapport med vedlegg NSM - FCKS temarapport 2019/2277 1
26.04.2021 kl. 13:57 Øvelse Digital 2020 - Invitasjon til digitalt kompetansehevingsseminar og oppfordring til bruk av øvingspakker i underlagte virksomheter Øvelse Digital 2020 2019/305 21
26.04.2021 kl. 13:57 Øvelse Digital 2020 - Sektordeltagelse og anbefalt scenariogrunnlag Øvelse Digital 2020 2019/305 8
26.04.2021 kl. 13:57 Utpeking av samfunnskritiske virksomheter Beredskap, krisehåndtering 2020/3452 6
26.04.2021 kl. 13:57 Styring og samhandling knyttet til JustisCERT JustisCERT 2021/1135 1
26.04.2021 kl. 13:57 Om signert avtale Nasjonalt cybersikkerhetssenter 2019/649 11
26.04.2021 kl. 13:57 FOU-prosjekt: IKT-sikkerhetstilstanden i kraftbransjen - Referat fra møte i dag FOU 80415 Sikkerhetstilstanden i norsk kraftforsyning 2021/4778 10
26.04.2021 kl. 13:57 FCKS halvårlig trussel og risikobilde 2018 FCKS rapport 2018/289 2
26.04.2021 kl. 13:57 Referat diskusjonsøvelse Digital 2020 3. desember Øvelse Digital 2020 - invitasjon til innledende møte 2019/135 8
26.04.2021 kl. 13:57 HelseCERT mulig tilknyting for Bufdir - kopi til BLD IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 10
26.04.2021 kl. 13:57 Arbeids- og sosialdepartementets sektor trekker sin deltakelse i Øvelse Digital 2020 Deltakelse i Øvelse Digital 2020 2020/15227 1
26.04.2021 kl. 13:57 Statusmøte i utviklingen av FCKS Videreutvikling av cyber- og IKT-områdene i forsvarssektoren 2017/458 9
26.04.2021 kl. 13:57 Kontaktpunkter for DSB i de hovedansvarlige departementer - Tilbakemelding Covid-19 - Hendelseshåndtering 2020 2020/593 76
26.04.2021 kl. 13:57 FCKS temarapport Felles cyberkoordineringssenter - FCKS 2017/4722 2
26.04.2021 kl. 13:57 ASDs sektor trekker sin deltakelse i Øvelse Digital 2020 Øvelse Digital 2020 2020/11221 1
26.04.2021 kl. 13:57 Cybersikkerhet i kraftbransjen FOU-Prosjekt 80411 Sikkerhet i digitale verdikjeder og komponenter i kraftforsyningen 2020/1197 38
26.04.2021 kl. 13:57 Oppfølging av nasjonal strategi for digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2018/70 34

26.04.2021 kl. 13:57 Informasjon fra JustisCERT KDI - Varslingsrutiner i Justissektoren - Nasjonal IKT øvelse 2018 2019/2225 1
26.04.2021 kl. 13:57 Oppfølging og rapportering på digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2018/70 3326.04.2021 kl. 13:57 Informasjon angåpende besøksforespørsler fra kinensiske delegasjoner Informasjon angående mistenkelig besøksforespørsel fra kinesiske delegasjoner 2019/1460 1
26.04.2021 kl. 13:57 Digital 2020 - Invitasjon til digitalt kompetansehevingsseminar Krisestøtteenhet for departementsfellesskapet - KSE - Forum for beredskapsmedarbeidere - tidligere Regjeringens kriseråd - h.u. Kriserådet 2014/8936 67
26.04.2021 kl. 13:57 Øvelsen Digital 2020 Øvelsen Digital 2020 2019/1000 3
26.04.2021 kl. 13:57 Nytt agendapunkt til planleggingskonferanse III B for Øvelse Digital 2020 Øvelse Digital 2020 - revidert fremdrifts- og gjennomføringsplan 2020/284 4
26.04.2021 kl. 13:57 Mulighet for tilknytting til HelseCERT for virksomheter i BLDs sektor - Forespørsel IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 5
26.04.2021 kl. 13:57 Oversendelse av tjenestetilbud fra European Agency for Cyber Security (ENISA) Nasjonal strategi for digital sikkerhet med tiltaksoversikt og nasjonal strategi for digital sikkerhetskompetanse 2018/1257 19
26.04.2021 kl. 13:57 Åpningen av Nasjonalt cyberkrimsenter (NC3) ved Kripos 25012019 Invitasjon til politidirektøren - Åpningen av Nasjonalt cyberkrimsenter (NC3) 2019/215 1
26.04.2021 kl. 13:57 Rapportering på nasjonal strategi for digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2016/6093 192
26.04.2021 kl. 13:57 UNIT Mandat for Uninett CERT som sektorvist responsmiljø Informasjonssikkerhet ved statlige universiteter og høyskoler 2017/1224 21
26.04.2021 kl. 13:57 Vedrørende fornyelse av medlemskap i NCSC partnersamarbeidet Tilbud om plass i Nasjonalt cybersikkerhetssenter 2019/2606 9
26.04.2021 kl. 13:57 Klage på avslag på søknad Prosjekt: BDO CERT 2017/9009 3
26.04.2021 kl. 13:57 PrepEx Øvelse Digital 2020 Øvelse Digital 2020 - revidert fremdrifts- og gjennomføringsplan 2020/284 5
26.04.2021 kl. 13:57 Tilknytting til HelseCERT for virksomheter i BLDs sektor - spørsmål om møte IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 7
26.04.2021 kl. 13:57 Tilknytting til HelseCERT for virksomheter i BLDs sektor - Forslag til tidspunkt for avklaringsmøte IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 8
26.04.2021 kl. 13:57 Evaluering av øvelse Digital 2020 Øvelse Digital 2020 2019/2431 21
26.04.2021 kl. 13:57 Informasjon om løsepengevirus - deling av temarapport Felles cyberkoordineringssenter FCKS 2017/2509 7
26.04.2021 kl. 13:57 Øvelse Digital 2020. Evaluering Øvelse Digital 2020 2019/2431 20
26.04.2021 kl. 13:57 Offentlig ph.d. til digital sikkerhet Nasjonal strategi for digital sikkerhetskompetanse - oppfølging 2019/680 24
26.04.2021 kl. 13:57 Oppdrag 14 - videreutvikling av JustisCERT JustisCERT 2021/20683 3
26.04.2021 kl. 13:57 Digital 2020 - Egne innspill og dreiebok Øvelse Digital 2020 2019/259 35
26.04.2021 kl. 13:57 Innsikt i HelseCERT Kommune-CSIRT IKS - Nasjonalt senter for informasjonssikkerhet i kommunesektoren 2019/5024 19
26.04.2021 kl. 13:57 Digital 2020 - Invitasjon til digitalt kompetansehevingsseminar Krisestøtteenhet for departementsfellesskapet - KSE - Forum for beredskapsmedarbeidere - tidligere Regjeringens kriseråd - h.u. Kriserådet 2014/8936 68
26.04.2021 kl. 13:57 Oppfølging og rapportering på digital sikkerhet fra Arbeids- og sosialdepartementet Nasjonal strategi for IKT-sikkerhet 2018/95 29
26.04.2021 kl. 13:57 Mandat for Uninett CERT som sektorvis responsmiljø (SRM) Mandat for Uninett CERT som sektorvist responsmiljø (SRM) 2020/647 2
26.04.2021 kl. 13:57 Tillegg til opprinnelig høringsinnspill - Digital sårbarhet - sikkert samfunn - KRIPOS Høring - Digital sårbarhet - sikkert samfunn 2015/4848 12
26.04.2021 kl. 13:57 Avslag på søknad Prosjekt: BDO CERT 2017/9009 2
26.04.2021 kl. 13:57 Oppdrag 6 - Øvelse Digital 2020 Statsbudsjettet og styringsdialogen 2020 - KMD - Leveranser og rapportering tildelingsbrev 2020/406 28
26.04.2021 kl. 13:57 Ugraderte videokonferanseløsninger - Oversendelse av vurdering fra NSM Nasjonal Sikkerhetsmyndighet Samfunnssikkerhet og beredskap - Korona / Covid-19 pandemi - 2020 2020/923 262
26.04.2021 kl. 13:57 Signert kontrakt og registreringsskjema - Avtale om nasjonalt cybersikkerhetssenter - Videre deltakelse i NCSN partnersamarbeid Invitasjon - Nasjonal sikkerhetsmyndighet NSM Nasjonalt cybersikkerhetssenter NCSC 2020/1864 8

26.04.2021 kl. 13:57 Vedrørende fornyelse av medlemskap i NCSC partnersamarbeidet Tilbud om plass i Nasjonalt cybersikkerhetssenter 2019/2606 7
26.04.2021 kl. 13:57 Kontaktpunkter for DSB i de hovedansvarlige departementer - Ber om tilbakemelding Covid-19 - Hendelseshåndtering 2020 2020/593 59
26.04.2021 kl. 13:57 Svar fra Kripos / NC3 på offentlig sektor- og nærings ph.d ordningen til digital sikkerhet Nasjonal strategi for digital sikkerhetskompetanse - oppfølging 2019/680 30
26.04.2021 kl. 13:57 Løsepengevirus - Temarapport FCKS Temarapporter 2019/2349 1
26.04.2021 kl. 13:57 HelseCERT mulig tilknyting for Bufdir - Foreløpig svar og orientering om prosess IKT-hendelser i Barne- og likestillingsdepartementets (BLDs) sektor - Kontaktpunkt 2017/2312 9
26.04.2021 kl. 13:57 Oppfølging av Nasjonal strategi for digital sikkerhet Nasjonal strategi for IKT-sikkerhet 2018/70 29
26.04.2021 kl. 13:57 Signert avtale for Partner i NCSC - Nasjonalt cybersikkerhetssenter Nasjonalt cybersikkerhetssenter 2019/649 10
26.04.2021 kl. 13:57 Brev til næringen - Testing av cybersikkerhet sendt fra Norges Bank Samarbeid med andre offentlige virksomheter 2019/11060 14
26.04.2021 kl. 13:57 Tjenestetilbud ENISA - Digital sikkerhet - Kopi Stortingsmelding 2017/787 20
26.04.2021 kl. 13:57 Vedrørende fornyelse av medlemskap i NCSC partnersamarbeidet Nødnett Cybersecurity Engagement 2019/11372 6
26.04.2021 kl. 13:57 Høring NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett Høring - NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett 2018/6579 34
26.04.2021 kl. 13:57 Oversendelse av samarbeidsavtale mellom EkomCERT og NSM NorCERT Samarbeidsavtale mellom EkomCERT og NSM NorCERT 2017/2761 1
26.04.2021 kl. 13:57 Orientering om høringssvar til JD - Digital sårbarhet - sikkert samfunn Høring - Digital sårbarhet - sikkert samfunn 2015/4848 24
26.04.2021 kl. 13:57 FOU-prosjekt IKT-sikkerhetstilstanden i kraftbransjen Oppsummering av møte FOU 80415 Sikkerhetstilstanden i norsk kraftforsyning 2021/4778 11
26.04.2021 kl. 13:57 Invitasjon til møte om tilknytting til HelseCERT for virksomheter i BLDs sektor 21.03.18. Invitasjon til møte om tilknytting til HelseCERT for virksomheter i BLDs sektor 2018/91 1
26.04.2021 kl. 13:57 HelseCERT KMD HelseCERT 2021/1589 4
26.04.2021 kl. 13:57 ASDs sektor trekker sin deltakelse i Øvelse Digital 2020 Øvelse Digital 2020 2019/1870 426.04.2021 kl. 13:57 Evalueringsdirektiv - Øvelse Digital 2020 Øvelse Digital 2020 2019/305 24
26.04.2021 kl. 13:57 Oversendelse av dokument - (UO) A03 - S-20-00283-1 2020-01-22 Deling av FCKS-rapport om utnyttelse av Citrix-sårbarhet med vedlegg Felles cyberkoordineringssenter FCKS 2017/2509 6
26.04.2021 kl. 13:57 Program for hendelseshåndtering i regi av UNINETT CERT - Styrking av evne til digital hendelseshåndtering ved statlige universiteter og høgskoler Styrking av evne til digital hendelseshåndtering ved statlige universiteter og høgskoler 2017/2034 1
26.04.2021 kl. 13:57 Felles cyberkoordineringssenter - presisering av oppdrag Felles cyberkoordineringssenter FCKS 2017/2509 4
26.04.2021 kl. 13:57 Referat 03.12.2020 diskusjonsøvelse Digital 2020 Øvelse Digital 2020 2019/3084 18
26.04.2021 kl. 13:57 Vedrørende fornyelse av medlemskap i NCSC partnersamarbeidet Tilbud om plass i Nasjonalt cybersikkerhetssenter 2019/2606 11
26.04.2021 kl. 13:57 ASDs sektor trekker sin deltakelse i Øvelse Digital 2020 ASDs sektor trekker sin deltakelse i Øvelse Digital 2020 2020/29016 1
26.04.2021 kl. 13:57 Øvelse Digital 2020 - informasjon - digitalt kompetansehevingsseminar Øvelse Digital 2020 planleggingskonferanse 2019/244 4
26.04.2021 kl. 13:57 Samordning av arbeidet med digital sikkerhet - forespørsel om informasjon Riksrevisjonen - Foranalyse om myndighetenes samordning av arbeidet med digital sikkerhet 2021/3107 1

Vedlegg 2: Informasjonsskriv til informanter

Vil du delta i forskningsprosjektet

Norske myndigheters styring på cybersikkerhetsfeltet?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å finne ut hvor funksjonelt det norske styringssystemet på cybersikkerhetsfeltet er. Dette skrivet inneholder informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
De siste årene har det skjedd betydningsfulle endringer i organiseringen av norske etater med ansvar på cybersikkerhetsfeltet. Nasjonalt cybersikkerhetssenter (NCSC) underlagt Nasjonal sikkerhetsmyndighet (NSM) ble formelt opprettet i 2019. Formålet med dette prosjektet er å finne ut hvordan det norske styringssystemet på cybersikkerhetsfeltet fungerer etter denne omorganiseringen. På bakgrunn av dette er følgende problemstilling utformet: Hvor formålstjenlig er norske myndigheters styringssystem for håndtering av IKT-sikkerhetshendelser? Prosjektet er en masteroppgave i statsvitenskap og har følgelig et begrenset omfang.

Hvem er ansvarlig for forskningsprosjektet?
Universitetet i Tromsø – Norges arktiske universitet er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Utvalg for dette prosjektet er trukket på bakgrunn av relevans for styring på cybersikkerhetsfeltet og roller i utvalgte IKT-sikkerhetshendelser. Dette innebefatter sentrale offentlige etater og virksomheter som har blitt rammet av IKT-sikkerhetshendelser. Henvendelser gjøres etter korrespondanse med de utvalgte etater og virksomheter. Du blir forespurt om deltakelse på bakgrunn av din rolle innen hendelseshåndtering.

Hva innebærer det for deg å delta?
Metoden som benyttes til informasjonsinnhenting er semistrukturerte kvalitative intervjuer. Dette innebærer at du som informant blir intervjuet om dine erfaringer med IKT-sikkerhetshendelser. Intervjuene er planlagt å vare i 30 minutter og gjennomføres via kryptert digital videokommunikasjon i programvaren Zoom (UIT-lisens). De vil bli spilt inn ved lyd-/videoopptak og transkribert i etterkant.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. På grunn av pandemisituasjonen forårsaket av Covid-19 vil samtykke gis muntlig før intervjustart. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan dine opplysninger oppbevares og benyttes
Opplysningene om deg vil kun benyttes til formålene som er omtalt i dette skrivet. Opplysningene behandles konfidensielt og i samsvar med personvernregelverket. Prosjektansvarlig er den eneste som har tilgang til opptak og transkripsjoner. Opplysninger om deg som person skal ikke kunne kobles til datamaterialet. Dette sikres gjennom en såkalt

kodenøkkel som beskriver informantene og som kun vil eksistere på fysisk papir. Din identitet vil bli anonymisert i transkripsjonen. Opptak og transkripsjoner vil bli oppbevart på en datamaskin uten nettverkskort under hele prosjektet med mindre du som informant ønsker innsyn.

Hva skjer med opplysningene dine når forskningsprosjektet avsluttes?
Lyd-/videoopptak slettes når transkripsjon er gjennomført, senest når oppgaven er godkjent, noe som etter planen skjer i slutten av juni 2021. Utklipp av muntlig samtykke vil oppbevares på kryptert harddisk også etter prosjektslutt. De anonymiserte transkripsjonene vil også kunne overføres til kryptert harddisk dersom arkivering for senere forskning fremstår som hensiktsmessig. Prosjektansvarlig vil da være den eneste med tilgang.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Tromsø – Norges arktiske universitet har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
Prosjektansvarlig - Eskil Jakobsen, UIT. E-post: eskil_jakobsen@hotmail.com. Telefon: 48181110.
Faglig veileder - Professor Hilde Bjørnå, UIT. E-post: hilde.bjorna@uit.no. Telefon: 77644338.

UITs personvernombud - Joakim Bakkevold. E-post: personvernombud@uit.no. Telefon: 77646322.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen
Eskil Jakobsen, masterstudent i statsvitenskap, UIT

Vedlegg 3: Datahåndteringsplan

Datahåndteringsplan

Prosjekt: Masteroppgave i statsvitenskap, Eskil Jakobsen, UIT

Veileder: Professor Hilde Bjørnå, UIT

Datatype: Digitale kvalitative intervjuer

Dataformat: Strømmefiler (Zoom, Teams), videofiler (MP4) / lydfiler (WAV, MP3), dokumentfiler (Docx, PDF)

Ansvarlig for oppbevaring: Eskil Jakobsen

Nødvendige ressurser: PC (Windows 10), Zoom-lisens (UIT), Teams-lisens (UIT), VPN (UIT), Minnepinne, PC uten nettverkskort, Kryptert harddisk

Organisering av data: Windows Explorer

Volum: 4 intervjuer à 45 minutter og 4 intervjuer à 30 minutter i MP4/WAV/MP3 format og transkribert til Docx/PDF

Oppbevaring i prosjektets levetid: PC uten nettverkskort og minnepinne

Oppbevaring på lang sikt: Lyd-/videofiler skal slettes, lydklipp av muntlig samtykke og transkripsjoner skal potensielt beholdes på kryptert harddisk eller i egnet sky

Plan for informasjonssikkerhet: Intervjuene skal gjennomføres fra min student-PC gjennom Zoom på UIT sin lisens. Denne plattformen åpner for kryptering av samtalen. Maskinen har 10. generasjons Intel prosessor og operativsystemet er Windows 10. I tillegg til Windows Defender er høyt rangert sikkerhetsprogramvare installert, samt UITs VPN-tjener. Opplysninger om informantene og deres formelle stillingsbeskrivelse skal tilegnes før opptak begynner. Lyd-/videoopptak startes i samråd med informanten. Videoopptak vil foretrekkes med mindre informanten ikke ønsker dette. Når intervjuet er over flyttes opptaksfilen til en dedikert minnepinne og overføres til en eldre PC uten nettverkskort (Dermed ingen mulighet for tilkobling til nett), såkalt *airgapping*. På denne maskinen gjennomføres transkribering av intervjuet og transkripsjonen kopieres *kun* hvis informanten ønsker den for gjennomlesning. Med denne tilnærmingen vil de eneste filene som befinner seg på en nettverkstilkoblet maskin være strømmefiler og opptaksfilene mens innspilling pågår.

Vedlegg 4: Intervjuguide: NSM

Intervjuguide – NSM-versjon

Introduksjon	Intervjuet omhandler dine erfaringer med håndtering av IKT-sikkerhetshendelser.
Anonymisering	Ditt navn vil bli anonymisert. Din stillingsbeskrivelse vil omtales i så vage ordelag som mulig.
Samtykke	Samtykke gis muntlig og kan når som helst trekkes tilbake.
Innsyn og redigering	Du kan når som helst be om innsyn i transkripsjon og få rettet/fjernet opplysninger. Dette gjøres gjennom henvendelse per e-post.
Gjennomføring	Intervjuet gjennomføres ved bruk av kryptert digital videokommunikasjon i Zoom (UIT-lisens).
Lydopptak	Lyd-/videoopptak vil bli gjennomført. Start av opptak vil gjøres i samråd med deg. Etter endt opptak vil filen flyttes til en datamaskin uten nettverkskort via minnepinne og transkribert. Transkripsjonen av intervjuet vil forbli på ovennevnte datamaskin med mindre du selv ønsker å lese den.
Tid	Intervjuet er planlagt å vare i 45 minutter.

Intervjuet

Mål	**Intervjuspørsmål**
Om informanten (før lydopptak).	Stillingsbeskrivelse og ansvarsområder.
Informantens rolle under IKT-sikkerhetshendelser.	Hvor ofte forekommer hendelser med stort samfunnsmessig skadepotensiale? Hva er din rolle under hendelseshåndtering? Er det noen hendelser du husker særlig godt?
Organisasjonens prosedyrer for hendelseshåndtering.	Hvordan foregår selekteringen av hendelser som dere velger å fokusere på? Følger dere kriterier for å avgjøre hvilke hendelser som blir prioritert? Bruker dere noen form for etablert standard i deres arbeid med hendelseshåndtering? Har dere ekspertgrupper internt i organisasjonen? Hvordan fungerer Varslingssystem for digital infrastruktur (VDI) i praksis?
Hendelseshåndtering i praksis.	Kan du nevne de viktigste oppgavene dere har under en prioritert hendelse? Hvilke taktiske grep er viktige for å sikre god hendelseshåndtering?

Samarbeid med rammede virksomheter.	Hvordan synes du samarbeidet med rammede virksomheter fungerer generelt? Kan åpenhet om hendelser i offentligheten være med å forhindre skadepotensiale fra en trussel? Hvilke hensyn er viktige i vurderinger knyttet til åpenhet om hendelser og angrep? Har dere noen generelle utfordringer knyttet til samarbeid med rammede virksomheter?
Samarbeid med andre etater.	Hvilke etater samarbeider dere tett med vedrørende hendelseshåndtering? Fungerer dette samarbeidet på en god måte? Hvordan fungerer samarbeidet med CERT/CSIRT-strukturen? Har dere noen generelle utfordringer knyttet til samarbeid med andre etater?
Konkrete hendelser.	Hendelser: Cyberangrepet mot Stortinget 08/2020, Cyberangrepet mot Østre Toten 01/2021, Cyberangrepet mot Norsk Hydro 03/2019, Cyberangrepet mot Sykehuspartner HF 01/2018. Hva slags bistand ga NSM/NCSC de rammede virksomhetene under disse hendelsene? Hvordan fungerte samarbeidet med den rammede virksomheten under hendelsen? Kunne/burde noe vært gjort annerledes under hendelsen? Har du gjort deg noen andre refleksjoner om hendelsen og deres respons?
Utfordringer knyttet til hendelseshåndtering.	Ser du noen generelle utfordringer knyttet til deres arbeid med hendelseshåndtering?
Styrker og svakheter ved styringssystemet for IKT-sikkerhetshendelser.	Synes du ansvarsfordelingen mellom etater med ansvar på cyberfeltet er tydelig nok? Synes du opprettelsen av Nasjonalt cybersikkerhetssenter har vært vellykket? Merker du noen forskjell i deres slagkraft etter opprettelsen? Ser du noen styrker ved det nåværende styringssystemet? Ser du noen svakheter ved det nåværende styringssystemet? Noen forskere har hevdet at det foregår en maktkamp mellom etater på cybersikkerhetsfeltet. Er dette en påstand du kjenner deg igjen i?
Trusselbildet og fremtiden.	Hva anser du som de fremste truslene mot digital sikkerhet i Norge? Synes du styringssystemet på cybersikkerhetsfeltet er godt utformet for å møte disse truslene? Hva slags rolle spiller sikkerhetskultur for samfunnets evne til å møte cybertrusler?

Vedlegg 5: Intervjuguide: Kripos NC3

Intervjuguide – Kripos NC3-versjon

Introduksjon	Intervjuet omhandler dine erfaringer med håndtering av IKT-sikkerhetshendelser.
Anonymisering	Ditt navn vil bli anonymisert. Din stillingsbeskrivelse vil omtales i så vage ordelag som mulig.
Samtykke	Samtykke gis muntlig og kan når som helst trekkes tilbake.
Innsyn og redigering	Du kan når som helst be om innsyn i transkripsjon og få rettet/fjernet opplysninger. Dette gjøres gjennom henvendelse per e-post.
Gjennomføring	Intervjuet gjennomføres ved bruk av kryptert digital videokommunikasjon i Zoom (UIT-lisens).
Lydopptak	Lydopptak vil bli gjennomført. Start av opptak vil gjøres i samråd med deg. Etter endt opptak vil lydfilen flyttes til en datamaskin uten nettverkskort via minnepinne og transkribert. Transkripsjonen av intervjuet vil forbli på ovennevnte datamaskin med mindre du selv ønsker å lese den.
Tid	Intervjuet er planlagt å vare i 45 minutter.

Intervjuet

Mål	**Intervjuspørsmål**
Om informanten (før lydopptak).	Stillingsbeskrivelse og ansvarsområder.
Organisasjonens rolle under IKT-sikkerhetshendelser.	Hva er deres rolle under hendelseshåndtering?
Organisasjonens prosedyrer for hendelseshåndtering.	Følger dere kriterier for å avgjøre hvilke hendelser som blir prioritert? Bruker dere noen form for etablert standard i deres arbeid med hendelseshåndtering? Spiller ISO 27000 serien noen rolle i deres arbeid? Har dere fokus på skadebegrensning eller sikring av spor? Tenker du at det eksisterer et spenningsforhold mellom skadebegrensning og god etterforskning? Hvor viktig er det å få saker til påtale?
Hendelseshåndtering i praksis.	Kan du nevne de viktigste oppgavene dere har under en prioritert hendelse?
Samarbeid med rammede virksomheter.	Hvordan synes du samarbeidet med rammede virksomheter fungerer generelt? Har dere noen generelle utfordringer knyttet til samarbeid med rammede virksomheter?

Samarbeid med andre etater.	Hvilke etater samarbeider dere tett med vedrørende hendelseshåndtering? Fungerer dette samarbeidet på en god måte? Hvordan fungerer samarbeidet med NSM og NCSC? Hvordan fungerer samarbeidet med CERT/CSIRT-strukturen? Hvordan synes du koordineringen i Felles cyberkoordineringssenter fungerer? Har dere noen generelle utfordringer knyttet til samarbeid med andre etater? Hvor ofte forekommer interessekonflikter mellom dere og andre etater?
Konkrete hendelser.	Hva slags rolle hadde dere under håndteringen av løsepengeviruset som rammet Østre Toten kommune? Hvordan fungerte samarbeidet med kommunen under hendelsen? Hvordan fungerte samarbeidet med andre aktører under hendelsen? Kunne/burde noe vært gjort annerledes under hendelsen? Har du gjort deg noen andre refleksjoner om hendelsen og deres respons?
Utfordringer knyttet til hendelseshåndtering.	Ser du noen generelle utfordringer knyttet til deres arbeid med hendelseshåndtering?
Styrker og svakheter ved styringssystemet for IKT-sikkerhetshendelser.	Synes du tverrsektorielt samarbeid på cybersikkerhetsfeltet er godt organisert? Synes du ansvarsfordelingen mellom etater med ansvar på cyberfeltet er tydelig nok? Ser du noen styrker ved det nåværende styringssystemet? Ser du noen svakheter ved det nåværende styringssystemet? Noen forskere har hevdet at det foregår en maktkamp mellom etater på cybersikkerhetsfeltet. Er dette en påstand du kjenner deg igjen i?
Trusselbildet og fremtiden (Hvis tid)	Hva anser du som de fremste truslene mot digital sikkerhet i Norge? Synes du styringssystemet på cybersikkerhetsfeltet er godt utformet for å møte disse truslene?

Vedlegg 6: Intervjuguide: HelseCERT

Intervjuguide – HelseCERT-versjon

Introduksjon	Intervjuet omhandler dine erfaringer med håndtering av IKT-sikkerhetshendelser.
Anonymisering	Ditt navn vil bli anonymisert. Din stillingsbeskrivelse vil omtales i så vage ordelag som mulig.
Samtykke	Samtykke gis muntlig og kan når som helst trekkes tilbake.
Innsyn og redigering	Du kan når som helst be om innsyn i transkripsjon og få rettet/fjernet opplysninger. Dette gjøres gjennom henvendelse per e-post.
Gjennomføring	Intervjuet gjennomføres ved bruk av kryptert digital videokommunikasjon i Zoom (UIT-lisens). Alternativt kan Teams (UIT-lisens) benyttes.
Lydopptak	Lydopptak vil bli gjennomført. Start av opptak vil gjøres i samråd med deg. Etter endt opptak vil lydfilen flyttes til en datamaskin uten nettverkskort via minnepinne og transkribert. Transkripsjonen av intervjuet vil forbli på ovennevnte datamaskin med mindre du selv ønsker å lese den.
Tid	Intervjuet er planlagt å vare i 30 minutter.

Intervjuet

Mål	**Intervjuspørsmål**
Om informanten (før lydopptak).	Stillingsbeskrivelse og ansvarsområder.
Informantens rolle under IKT-sikkerhetshendelser.	Hvor ofte forekommer hendelser med stort skadepotensiale?
Organisasjonens prosedyrer for hendelseshåndtering.	Hvordan foregår selekteringen av hendelser som dere velger å fokusere på? Bruker dere noen form for etablert standard i deres arbeid med hendelseshåndtering? Kan du forklare hvordan sensorplattformen i Nasjonalt beskyttelsesprogram fungerer?
Hendelseshåndtering i praksis.	Hvilke taktiske grep er viktige for å sikre god hendelseshåndtering?
Samarbeid med rammede virksomheter.	Har dere noen generelle utfordringer knyttet til samarbeid med rammede virksomheter?
Samarbeid med andre etater.	Fungerer samarbeidet med andre etater på cybersikkerhetsfeltet på en god måte? Fungerer samarbeidet med aktører i privat sektor på en god måte?

Konkrete hendelser.	Hvordan fungerte deres respons på IKT-sikkerhetshendelsen som rammet Helse Sør-Øst januar 2018? Sykehuspartner ble rammet på nytt i 2020 Hvordan fungerte samarbeidet med den rammede virksomheten under hendelsen? Hvordan fungerte samarbeidet med andre etater under hendelsen? Kunne/burde noe vært gjort annerledes under hendelsen? Har du gjort deg noen andre refleksjoner om hendelsen og deres respons?
Utfordringer knyttet til hendelseshåndtering.	Ser du noen generelle utfordringer knyttet til deres arbeid med hendelseshåndtering?
Styrker og svakheter ved styringssystemet for IKT-sikkerhetshendelser.	Hvordan synes du tverrsektorielt samarbeid om hendelseshåndtering fungerer? Noen forskere har hevdet at det foregår en maktkamp mellom etater på cybersikkerhetsfeltet. Er dette en påstand du kjenner deg igjen i?
Trusselbildet og fremtiden.	Synes du styringssystemet på cybersikkerhetsfeltet er godt utformet for å møte trusselbildet?

Vedlegg 7: Intervjuguide: Rammet virksomhet

Intervjuguide – Rammet virksomhet

Introduksjon	Intervjuet omhandler dine erfaringer med håndtering av IKT-sikkerhetshendelser.
Anonymisering	Ditt navn vil bli anonymisert. Din stillingsbeskrivelse vil omtales i så vage ordelag som mulig.
Samtykke	Samtykke gis muntlig og kan når som helst trekkes tilbake.
Innsyn og redigering	Du kan når som helst be om innsyn i transkripsjon og få rettet/fjernet opplysninger. Dette gjøres gjennom henvendelse per e-post.
Gjennomføring	Intervjuet gjennomføres ved bruk av kryptert digital videokommunikasjon i Zoom (UIT-lisens).
Lydopptak	Lydopptak vil bli gjennomført. Start av opptak vil gjøres i samråd med deg. Etter endt opptak vil lydfilen flyttes til en datamaskin uten nettverkskort via minnepinne og transkribert. Transkripsjonen av intervjuet vil forbli på ovennevnte datamaskin med mindre du selv ønsker å lese den.
Tid	Intervjuet er planlagt å vare i 30 minutter.

Intervjuet

Mål	**Intervjuspørsmål**
Om informanten (før lydopptak)	Stillingsbeskrivelse og ansvarsområder.
Informantens rolle under IKT-sikkerhetshendelser	Hva var din rolle under hendelsen?
Hendelseshåndtering i praksis	Hvordan ble dere oppmerksomme på hendelsen? Hvilke hensyn var viktige under vurderinger av taktikk under hendelseshåndteringen?
Samarbeid	Hvordan fungerte samarbeidet med myndighetsetater? Hvordan fungerte samarbeidet med aktører i det private?
Konkrete hendelser	Hvordan fungerte deres respons på hendelsen? Kunne/burde noe vært gjort annerledes under hendelsen? Har du gjort deg noen andre refleksjoner om hendelsen og deres respons?
Utfordringer knyttet til hendelseshåndtering.	Ser du noen generelle utfordringer knyttet til deres arbeid med hendelseshåndtering?

Styrker og svakheter ved styringssystemet for IKT-sikkerhetshendelser	Noen forskere har hevdet at det foregår en maktkamp mellom etater på cybersikkerhetsfeltet. Er dette en påstand du kjenner deg igjen i?
Trusselbildet og fremtiden	Synes du styringssystemet på cybersikkerhetsfeltet er godt utformet for å møte trusselbildet?