Rolle- og ansvarsfordelingen mellom NSM og politiet

-Vil en rolleendring endre den nasjonale evnen til å stå imot dataangrep?

Master i Samfunnssikkerhet

Universitetet i Stavanger

Klaus Aleksander Trapp

Våren 2018

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Våren 2018

FORFATTER:

Klaus Aleksander Trapp

VEILEDER:

Ole Andreas H. Engen

TITTEL PÅ MASTEROPPGAVE:

Rolle- og ansvarsfordelingen mellom NSM og Politiet

-Vil en rolleendring endre den nasjonale evnen til å stå imot dataangrep?

EMNEORD/STIKKORD:

NSM, NorCERT, Politiet, Kripos, IKT-sikkerhet, Dataangrep, Sikringsrisiko, Sikkerhet, Samfunnssikkerhet, Omstilling, Rolleendring

SIDETALL: 91

OSLO 01.11.2018

Sammendrag

Samfunnets avhengighet av dataløsninger har gjort oss sårbare. Dataangrep rammer det norske samfunn og trenden er økende. Samfunnets organisering av IKT-sikkerhet er derfor helt avgjørende for å sikre våre verdier på en god måte. Dataangrep innbefatter alt fra guttestreker med digitalt "hærverk" til statsaktører som ønsker å påvirke politiske prosesser.

NSM har det koordinerende ansvaret for håndteringen av alvorlige angrep mot kritisk infrastruktur, og politiet har det overordnede ansvaret med å bekjempe datakriminalitet. Dette gjør at politiets vide fullmakter overlapper flere av NSMs roller og ansvar innen IKT-sikkerhet. Problemstillingen lyder: *Hvordan påvirker en rolleendring mellom NSM-NorCERT og politiet den den nasjonale evnen til å håndtere dataangrep.* Oppgaven vil svare på dette gjennom tre teoretiske perspektiver: Samfunnssikkerhet og beredskap, sikringsrisiko og organisering av samfunnssikkerheten.

Datainnsamlingen foregikk i hovedsak ved innhenting av (styrende) offentlige dokumenter innen datasikkerhet og gjennom intervjuer. I tillegg ble det benyttet høringssvar og rapporter fra viktige samfunnsaktører for å illustrere ulike syn på rollefordelingen mellom sikkerhetsaktørene.

Ansvar og roller som NSM er pålagt gjennom lov overlapper de som også politiet er pålagt, men dette fordeler seg fint i praksis. Det er få saker NSM håndterer sammen med PST, da dette gjelder angrep med stort skadepotensial fra fremmede statsaktører som gjerne ikke berører politiet. Politiet håndterer alle saker som blir anmeldt; det er som regel saker knyttet til kriminalitet i det digitale domenet.

En rolleendring mellom NSM og politiet vil ikke styrke den nasjonale evnen til å håndtere dataangrep. Mer egnet til å styrke denne evnen er bedre informasjonsflyt mellom politiet og NSM. Politiet vil kunne ha stor nytte av overskuddsinformasjonen fra VDI-samarbeidet til NSM. Sikkerhetsaktørene bør se på løsninger på hvordan de kan gjøre denne informasjonen mindre formålsbegrenset, slik at politiet kan utnytte den.

Forord

Denne oppgaven utgjør avslutningen på min masteroppgave innen risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Dette har vært en særdeles krevende oppgave, da problemstillingen rører ved et ladet og omdiskutert tema innen IKT-sikkerhet. Informasjonen knyttet til mitt valg av problemstilling opplevdes sjelden som objektivt. Jeg valgte problemstilling etter innspill fra flere sentrale nasjonale aktører innen IKT-sikkerhet, som sitter utenfor EOS-miljøet. Med disse inngangsverdiene ble problemstillingen og forskningsspørsmålene utformet og testet gjennom oppgaven. Informasjonen jeg har brukt i oppgaven har jeg hentet fra offentlige dokumenter som berører temaet samt intervjuer med de absolutt mest aktuelle aktørene knyttet til problemstillingen. Kontrasten til hvordan jeg oppfattet problemstillingen før og etter oppgaven er stor; dette har vært en krevende og lærerik prosess.

Jeg vil gi en stor takk til min veileder Ole Andreas H. Engen, som har hjulpet meg med å forstå hvordan jeg skal strukturere oppgaven. Han har kommet med mange gode innspill som har bidratt til å løfte oppgaven. Videre ønsker jeg å takke alle informantene og spesielt sjef for NSM-NorCERT, Håkon Bergsjø, og Kripos' representant i Felles Cyber Koordinerings Senter (FCKS), Øystein Andreassen, for å stille til intervju.

Oslo, 01.11.2018

Klaus Aleksander Trapp

Innhold

Figuroversikt:

Tabelloversikt:

1 Innledning

Dataangrep er helt klart den hyppigste form for kriminalitet som individer og virksomheter (Appendiks A) i Norge blir utsatt for. Det er også den kriminalitetsformen som de færreste anmelder og som sjelden fører til påtale. Det er NSM-NorCERT i dag som har den nasjonale responsfunksjonen for dataangrep og ansvaret for å avdekke og koordinere bekjempelse av alvorlige angrep mot kritisk infrastruktur og samfunnsfunksjoner. Politiets bekjempelse av kriminalitet skal også gjelde i det digitale domenet. Flere samfunnsaktører, offentlige rapporter og utredninger peker på at det er berøringspunkter mellom NSM og politiet. Det er utfordringer knyttet til usikkerhet rundt aktørenes ansvars- og rollefordeling. Man kan løse dette gjennom dialog og styrket samhandling. Man kan også løse dette gjennom å gå vekk fra samhandling og heller vurdere kommandokontroll, der én aktør sitter med hele håndteringskjeden. En slik struktur har potensiale til å kunne viske vekk uklar ansvars- og rollefordeling samt styrke offentlighetens krav til tydelighet knyttet til aktørenes myndighetsområde.

Det finnes mange små og store aktører som må samvirke for å gjøre IKT-sikkerheten (Appendiks A) robust i Norge. I offentlige rapporter som omhandler IKT-sikkerhet knyttes det ofte usikkerhet til nasjonens samlede evne til samhandling, og om ansvars- og rollefordelingen mellom sikkerhetsaktørene er tydelig nok og hensiktsmessig fordelt. Det stilles spørsmål ved om den samlede kapasiteten sikkerhetsaktørene imellom er godt nok utnyttet. Dette spørsmålet er ofte knyttet til mangelfull kommunikasjon og uklare grensesnitt når det gjelder ansvar og oppgaver. Dette kan skyldes at myndighetsoppgavene til NSM overlapper politiets vide fullmakter. Lysne-utvalget (NOU 2015:13) tar opp flere viktige problemstillinger på dette området.

Norge er tjent med å samle de største aktørene rent geografisk for å få større kraft i samhandlingen. Gjennom samlokalisering kan man tenke seg at informasjonsutvekslingen blir raskere og mer presis. Formaliserte strukturerer med et tydelig grensesnitt for ansvar og oppgaver vil tvinge seg fram, og det vil føre til god

oversikt over hverandres kapasitet og ressurser. Dette kan -skape en mer effektiv ressursstyring.

En slik samlokalisering kan bli et nasjonalt senter for bekjempelse av digitale angrep.

Den andre problemstillingen er knyttet til om det er NSM eller politiet som bør ha en overordnet, koordinerende rolle og være navet i dette senteret. Her er utvalget (NOU 2015:13) delt i spørsmålet om hva som er mest hensiktsmessig. NSM har denne rollen i dag, og flertallet i utvalget mener denne strukturen bør bestå, mens mindretallet mener politiet bør ha denne rollen. I november 2017 skriver politiforum.no (Trædal, 2017) at det skal etableres et eget senter for cyberkriminalitet med 200 ansatte kalt NC3 (Norsk Cyber Crime Center). Sjef for dette senteret tiltrådte 1. september 2018. Til sammenligning har NorCERT ca. 40 ansatte. Med tanke på den kapasitetsøkningen politiet vil få, kan det intuitivt virke som mindretallutvalgets løsning vil gi en mer oversiktlig og klarere struktur.

Politiet har i henhold til lov om politivirksomhet (Politiloven) § 2 ansvar for å forebygge kriminalitet samt avdekke og stanse kriminell virksomhet og forfølge straffbare forhold. I henhold til Lov om forebyggende sikkerhetstjeneste (Sikkerhetsloven) § 9 driver NSM den nasjonale responsfunksjonen for alvorlige dataangrep mot kritisk infrastruktur og har et nasjonalt varslingssystem for digital infrastruktur. Det kommer klart fram at NSMs oppgave vil være å håndtere ulovlige angrep med et viss skadepotensiale mot samfunnskritiske strukturer og funksjoner. Det er derimot uklart om politiet kun skal håndtere IKT-kriminalitet av mindre betydning, eller om de også skal håndtere alvorlige hendelser. Her etterlyser offentligheten et tydeligere skille når det gjelder ansvar og oppgaver mellom NorCERT og politiet. Det er en utfordring at ansvar og oppgaver gitt NSM gjennom sikkerhetsloven overlapper politiets fullmakter etter politiloven. Det er også uklart hva sikkerhetsloven legger i begrepet responsfunksjon, da dette dimensjonerer NSMs oppgaver, både med tanke på hvor alvorlig noe må være før de tar tak i det og hvor langt de går i håndteringen av hendelsen.

IKT-beredskap består av forebygging, avdekking, håndtering og etterforskning. Både politiet og NorCERT har overlappende oppgaver i flere av leddene i denne

beredskapskjeden. NSM er en aktør som også berører kriminalitetsområder. Jeg vil se på om rollefordelingen er tydelig nok til klart å skille berøringspunktene mellom NSM og politiet og om en rolleendring av funksjoner vil styrke den nasjonale evnen til å bekjempe dataangrep.

NSM har bygget opp en tillit til norsk næringsliv i 15 år gjennom et samarbeid med offentlige og private virksomheter. Samarbeidet bygger på et sensorsystem som avdekker digitale angrep; dette varslingssystemet (VDI) er avhengig av samtykke og samarbeid mellom private virksomheter og NSM. NSM hevder i et høringssvar til Lysne-utvalget (NOU 2015:13) at "tilliten neppe vil la seg videreføre" hvis den funksjonen som avdekker angrep deles med eller plasseres hos politiet (NSM, 2016). Ordningen med VDI er basert på frivillighet og tillit mellom NSM og virksomhetene som har VDI-systemet. Samarbeidet er forankret i tilliten til at informasjonen som går gjennom sensorene eies av virksomheten, og at det er virksomheten som bestemmer hva informasjonen skal brukes til. Dette skaper en formålsbegrenset bruk av informasjonen og gir virksomhetene mulighet til å holde et ulovlig dataangrep skjult for politiet. Virksomheten vil av og til se seg tjent med at angrepet skal forbigås i stillhet, for å ikke avsløre at de er sårbare eller gjenstand for angrep som kan skade virksomhetens omdømme, som igjen kan få økonomiske konsekvenser.

VDI er et av de viktigste verktøyene norske myndigheter har for å avdekke ulovlige IKT-angrep mot virksomheter med samfunnskritisk infrastruktur og informasjon. NSM sammenfatter informasjon fra VDI for å kartlegge trusler og sårbarhet i den hensikt å drive forebyggende arbeid innen IKT-sikkerhet, noe de er pålagt etter sikkerhetsloven. En av hovedoppgavene til politiet er å forebygge kriminalitet. Politidirektoratet skriver selv at de ville hatt stor nytte av informasjonen fra VDI i dette arbeidet, forutsatt at de hadde hatt kapasitet til å behandle den (POD, 2015).

NSM er fag- og tilsynsmyndighet innen forebyggende sikkerhetstjenester og er forvalter av sikkerhetsloven. Når tilsyn og operativ virksomhet skal fungere i samme organisasjon, er det viktig å ha et klart skille mellom de to funksjonene. Et uklart grensesnitt mellom de to myndighetsfunksjonene vil svekke tilliten til både NSMs rolle som tilsynsmyndighet og som operativ enhet. Det kan være uheldig om tilsynsorganet er premissleverandør samtidig som det skal ha en god plattform for

samarbeid med tilsynsobjektet. I teorien kan et samarbeid mellom NSM og en virksomhet gi utslag i form av skeivfordeling av makt, dersom NSM i tillegg har en kontrollfunksjon for denne virksomheten. Stortingsmeldingen om statlig tilsyn (St.Meld 17, 2002-2003) er klar på at tilsynsrollen bør rendyrkes for å hindre at det stilles spørsmål ved deres legitimitet. Ut fra dette perspektivet kan man hevde at det vil være hensiktsmessig å gi den operative rollen NSM har i dag til politiet, slik at NSM i større grad kan rendyrke sin tilsynsrolle.

Det er først når oppgaven ikke lenger kan løses av én aktør at behovet for samvirke oppstår (Andersson, et al., 2014). Dagens løsning gir mange utfordringer: Uklare roller og ansvar, manglende samarbeid og informasjonsdeling, uklart skille mellom tilsyn og operativ virksomhet. I oppgaven vil jeg se på om en rolleendring, der politiet tar over noen av oppgavene og ansvaret gitt NorCERT, er hensiktsmessig. Jeg vil gjennom denne oppgaven drøfte om den nasjonale evnen til å bekjempe dataangrep blir styrket ved et bytte av myndighetsoppgaver mellom politiet og NSM.

2 Problemstilling og forskningsspørsmål

Følgende problemstilling er valgt for å gi et klarere grensesnitt mellom sikkerhetsaktørene NSM-NorCERT og politiet og om den nasjonale IKT-beredskapen er tjent med en rolleendring.

Hvordan påvirker en rolleendring mellom NSM-NorCERT og politiet den nasjonale evnen til å håndtere dataangrep?

Det snakkes og skrives mye om samvirke og koordinering og at dette må bli bedre for å styrke beredskapen innen IKT-hendelser. Dette er ikke unikt for IKT-sikkerhet. Samvirke og koordinering er utfordrende i en hvilken som helst beredskapskontekst. Ord som koordinering, samvirke, kommunikasjon gir ofte liten effekt uten formelle avtaler og tydelig ansvars- og rollefordeling. Oppgaven vil drøfte hvordan rollefordelingen er i dag og om man bør foreta en rolleendring for å legge til rette for at den samlede kapasiteten til sikkerhetsaktøren utnyttes mer hensiktsmessig.

Med dette vil oppgaven utrede problemstillingen ved å besvare følgende forskningsspørsmål:

1. Hva er de ulike sikkerhetsaktørenes ansvar og oppgaver?
2. Hva slags rolleutfordringer møter politiet og NSM i sin rolleutøvelse?
3. Bør politiet ha den nasjonale CERT-funksjonen?
4. Bør politiet ta over VDI-samarbeidet NorCERT har i dag?

Norges nasjonale evne til å bekjempe dataangrep kan forstås på ulike måter. Oppgaven forstår *nasjonal evne* som samfunnets institusjonelle kapasitet til å forebygge, håndtere og restituere ved ekstraordinære hendelser som går ut over den daglige driften (Kruke, 2012, p. 4). Denne oppgaven knytter Norges nasjonale evne til å håndtere dataangrep til samfunnets generelle evne til å følge de fire prinsippene innen samfunnssikkerhet, samt NSMs og politiets beredskapsarbeid og håndtering av IKT-angrep. Sikkerhetsaktørenes evne til å drive beredskap og håndtering av tilsiktede IKT hendelser blir påvirket av deres forståelse av egen og andres ansvar og roller knyttet til deres forvaltningsoppgaver.

2.1 Begrensning

2.1.1 Datakriminalitet og dataangrep

Digitale (Appendiks A) trusler, IKT-kriminalitet, cyberangrep, dataangrep, datakriminalitet er alle betegnelser på aktiviteter fra trusselaktører (Appendiks A) som ønsker å ramme våre verdier. E-tjenesten bruker i den årlige fokusrapporten begrepet digitale trusler og deler denne opp i tre kategorier: Etterretning (Appendiks A), sabotasje (Appendiks A) og påvirkningsopperasjoner (Appendiks A). Påvirkningsoperasjoner vil i denne oppgaven ikke bli karakterisert som digitale angrep. Selv om mye av det skjer i det digitale rom, kreves det en fundamentalt annen kapasitet av utøverne. NSM bruker begrepet dataangrep og bruker dette begrepet i tilknytning til alvorlige angrep mot kritisk infrastruktur (Appendiks A). Politiet bruker benevningen datakriminalitet og kategoriserer dette grovt i to kategorier: Kriminalitet der datautstyr blir benyttet som verktøy for å begå en kriminell handling, og angrep rettet mot data og selve datasystemet. I oppgaveteksten vil det

stå ***dataangrep*** når angrep rettet mot selve datasystemene er omtalt; begrepet vil dekke både alvorlige og ikke-alvorlige angrep. Eksempelvis vil ikke narkotikahandel eller spredning av barnepornografisk materiale på nettet omtales som dataangrep i denne oppgaven.

2.1.2 Begrenset tilgang til data

Utover offentlig tilgjengelig litteratur som behandler IKT-sikkerhet er det en stor utfordring knyttet til å samle relevante data til denne oppgaven. Det vil ligge i sikkerhetsaktørenes natur å ikke dele data fritt med offentligheten. Jeg har ikke fått all den informasjonen jeg trenger for å få et optimalt sanntidsbilde av utfordringene sikkerhetsaktørene har. Noe av denne informasjonen er gradert og blir ikke delt av hensyn til nasjonal sikkerhet.

2.1.3 Eldre dokumenter

Oppgaven vil ikke bruke kilder som omhandler utfordringen knyttet til rollefordelingen mellom NSM og politiet eldre enn 2015. Digitaliseringen og omstillingen skjer så raskt at dokumenter produsert før dette vil miste noe av sin relevans. Kilder knyttet til generell teori vil derimot kunne være noe eldre.

3 IKT-risikobilde

Norge er et av de mest digitaliserte land i verden (World Economic Forum, 2015). Det norske samfunn har tatt i bruk digitalisering for å effektivisere verdikjedene i nesten alle sektorer, både privat og offentlig. Dette har ført til innovasjon, bedre offentlige og private tjenester samt høyere levestandard. Meld. St 10 fra 2017; *Risiko i et trygt samfunn,* fremholder at digitalisering ikke lenger er et valg, men en forutsetning for et moderne og effektivt samfunn (Meld. St. 10, 2016-2017, p. 59).

I risikorapporten til NSM fra 2018 står det at risikoen for at norske interesser blir rammet av ondsinnede handlinger er økende og at det primært skyldes økende

sårbarhet innen digitale løsninger. Som et resultat av dette vil det øke konsekvensene for samfunnet. NSM har gjennom samarbeid med andre etterretnings- og sikkerhetsaktører avdekket et økende antall angrep fra fremmede statsaktører mot virksomheter med kritiske samfunnsfunksjoner. Intensjonen er å skaffe seg sensitiv informasjon. Samtidig avdekkes det også i større grad et økende antall rettede angrep fra statsaktører mot virksomheter som ikke har samfunnskritiske funksjoner. Dette gjør at skillet mellom ordinære virksomheter som ikke er underlagt sikkerhetsloven og samfunnssikkerhet viskes bort (NSM, 2018).

Fokusrapporten fra 2017, utgitt av Etterretningstjenesten, skriver at dataangrep mot Norge er økende og at den største trusselen kommer fra Russland og Kina. I november 2016 ble Abeiderpartiet forsøkt hacket. I 2017 ble mange norske bedrifter rammet av WannaCry, en ondsinnet kode som krypterer informasjonen brukeren har samlet på klienten, og krever løsepenger for å gi tilbake brukerens egen informasjon. I januar 2018 skal hackere ulovlig ha skaffet seg tilgang til flere av serverne brukt av Sykehuspartner og Helse Sør-Øst. I media blir det rapportert at det er russisk etterretning som trolig står bak det sistnevnte angrepet. Det blir anslått at individer og virksomheter i Norge blir tappet for 5 milliarder kroner årlig av kriminelle hackere. Til sammenligning ga Norges største bankran, Nokas-ranet, trusselaktørene et utbytte på ca 50 millioner kroner (Ruud, 2013).

Mørketallsundersøkelsen i 2016 rapporterer at 44 % av respondentene avstår fra nettjenester grunnet frykt for datakriminalitet og at 27 % av virksomhetene i undersøkelsen er blitt utsatt for ulovlige dataangrep i 2015 (NSR, 2016). Dataangrep øker i takt med den digitale utviklingen og de kriminelles evne og vilje til å bruke den. Det er en økt risiko for at sensitiv informasjon som vi deler over nettet kommer på avveie og misbrukes. Norge er et av de rikeste land i verden og samtidig et av de mest digitale. Denne kombinasjonen gjør oss veldig attraktive for kriminelle som opererer på nettet. Dette kan være alt fra fremmede statsmakter med spionasje eller sabotasje som agenda til enkeltindivider som driver "hærverk" i cyberdomenet fra gutterommet.

Datakriminalitet er ulovlige angrep som rammer alt fra individ og virksomhet til samfunnskritiske funksjoner. Dersom samfunnet skal bruke og nyttiggjøre seg

digitaliseringen, må tilliten fra brukerne være på plass. Vi må som samfunn beskytte oss mot disse angrepene for å gjøre oss robuste mot dataangrep. En god samlet innsats mot digitale angrep forutsetter god samhandling og en hensiktsmessig ansvars- og rollefordeling.

3.1 Sikkerhetsaktørenes ansvar og oppgaver

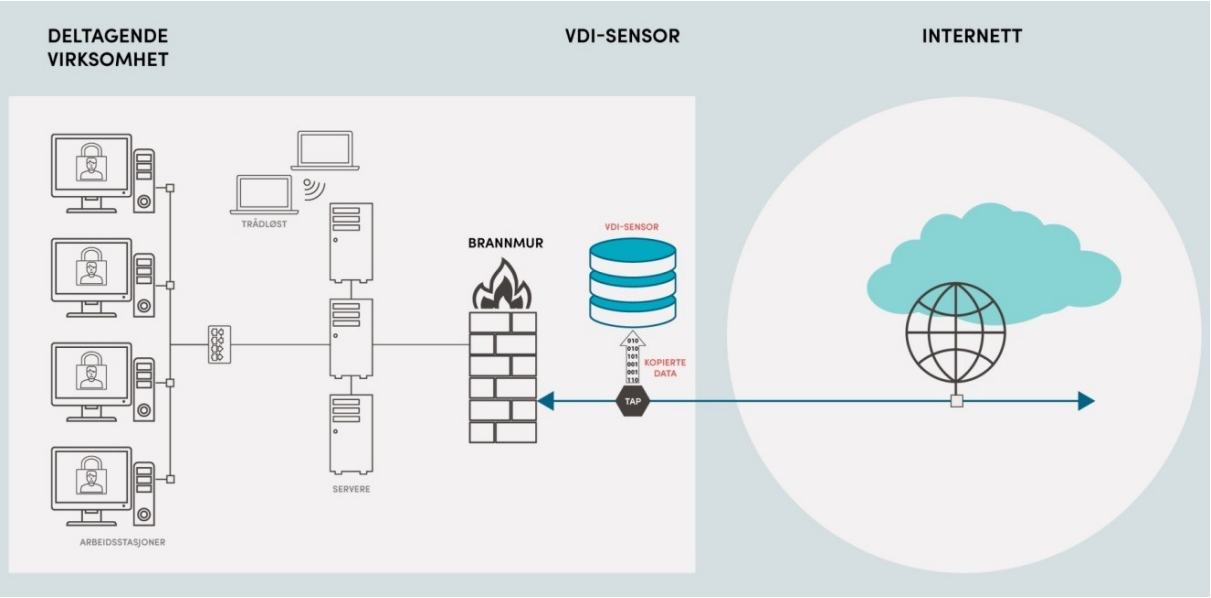
For bedre å forstå utfordringene knyttet til rolle- og ansvarsfordelingen vil oppgaven beskrive ansvarsområdet for de mest aktuelle sikkerhetsaktørene som sikrer samfunnsverdiene våre mot dataangrep.

3.1.1 Nasjonal sikkerhetsmyndighet (NSM)

NSM er underlagt Forsvarsdepartementet (FD) og rapporterer til FD i militære saker og til Justis- og beredskapsdepartementet (JD) i saker som faller inn under JDs fagområde i sivil sektor (NSM, 2014).

NSM skal detektere og varsle samt koordinere håndteringen av alvorlige dataangrep mot samfunnskritisk infrastruktur og funksjoner. NSM er forvalter av sikkerhetsloven og fører tilsyn med blant annet informasjon, objekter og infrastruktur blant virksomheter underlagt sikkerhetsloven. I den sammenheng gir de også ut veiledere og informasjon for å sikre at sikkerhetsforvaltningen ikke bryter med lover og forskrifter.

NSM har også ansvaret for det forebyggende arbeidet inn mot IKT-sikkerhet og har ansvaret for å drifte det nasjonale sensornettverket kalt Varslingssystem for digital infrastruktur (VDI). VDI består av mange sensorer som er utplassert hos virksomheter som har kritisk infrastruktur og/eller samfunnsfunksjon. Denne ordningen er frivillig og er forankret i tillit mellom virksomheten og NSM. Sensornettverket driftes av NorCERT, som også har det operative ansvaret for håndteringen av alvorlige angrep (NSM, 2014).

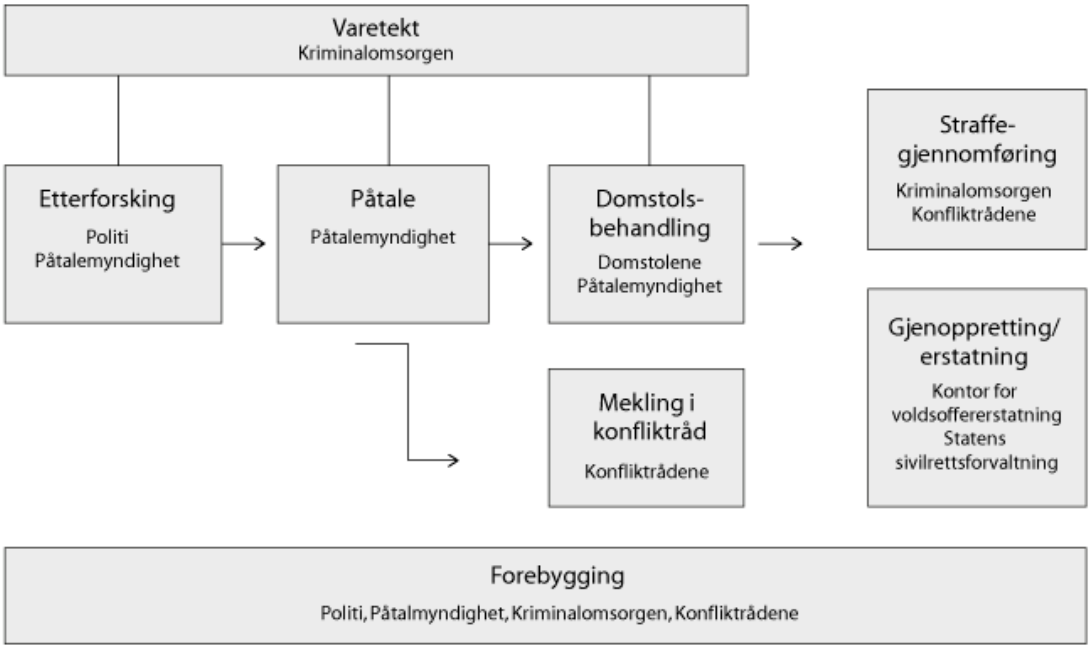


Figur 1: Prinsippet rundt VDI-samarbeidet

3.1.2 Politiet

Politiet skal etter politiloven § 2:
Forebygge, avdekke og stanse all kriminell virksomhet samt forfølge straffbare forhold.

Politiet og Forsvaret er de eneste maktmonopolene vi har i Norge, men politiet har enerett til å utøve makt overfor borgerne i fredstid. Politiet har handlingsrom til å gi forbud, pålegg og gjennomføre tvangstiltak. Handlingsrommet til politiet gjelder også i det digitale rom. Ved etterforskning har politiet ytterligere hjemler i straffeprosessloven til å drive sporsikring og samle informasjon; dette kan gjennomføres ved bruk av skjulte tvangsmidler. I spørsmål om påtale er politiet underlagt en overordnet påtalemyndighet. Både Kripos og PST er underlagt det nasjonale statsadvokatembetet (NAST) (NSM, 2017).



Figur 2: Fra etterforskning til straffegjennomføring (Prop. 1 S, (2016–2017))

3.1.3 Kripos

Kripos er underlagt politidirektoratet (POD) og er dets ekspertorgan for bekjempelse av organisert og alvorlig kriminalitet; datakriminalitet sorterer under dette. Kripos har en datakrimenhet med høy kompetanse innen kriminaletterretning og taktisk og teknisk etterforskning av datakriminalitet. Kripos har også en egen enhet som bistår med internettrelatert etterforskningsstøtte som elektronisk sporsikring av blant annet bevis på internett, utlevering fra tjenestetilbydere, ransaking og analyse av beslag (NSM, 2017). Kripos er også politiets koordinerende organ opp mot politi i utlandet samt Interpol og Europol, og ivaretar en rekke internasjonale forpliktelser (Politiet, 2018).

3.1.4 Politiets sikkerhetstjeneste (PST)

PST er direkte underlagt JD, men har politimyndighet på lik linje med politiet. Deres oppgaver er hjemlet i politiloven kapittel IIIa. De har ansvaret for å forebygge og håndtere overtredelser særlig knyttet til Norges selvstendighet og andre grunnleggende nasjonale interesser som ulovlig etterretning og sabotasje. PST er en del av EOS-miljøet og er Norges innenlandske sikkerhets- og etterretningstjeneste. PST samler informasjon og utarbeider analyser og trusselvurderinger til bruk i eget

forebyggende arbeid, samt at de bidrar til å spre risikobildet ut til andre virksomheter. PST har hjemler til å benytte seg av skjult informasjonsinnhenting i forebyggende saker (NSM, 2017).

3.1.5 Felles cyberkoordineringssenter (FCKS)

FCKS er en videreføring av Cyberkoordineringsgruppen (CKG). FCKS ble opprettet i 2017 og ledes av NSM og består av representanter fra NSM, E-tjenesten, PST og Kripos, som fysisk er lokalisert i bygget til NSM. FCKS ble opprettet for å styrke den nasjonale evnen til å håndtere digitale angrep. Senteret er et samlokalisert fagmiljø bestående av permanente representanter fra de fire partene. Senterets funksjon er å koordinere innsatsen til sikkerhetsaktørene ved håndtering av digitale hendelser. Dette vil kunne bidra til en bedre ressursstyring av nasjonale kapasiteter og bedre informasjonsdeling. FCKS fungerer som en samhandlingsplattform og har ingen egen beslutningsmyndighet. Senteret fungerer heller ikke som en kapasitet for andre virksomheter som ønsker bistand til håndtering (NSM, 2017).

4 Teoretisk rammeverk

For å drøfte hvordan en rolleendring mellom NSM-NorCERT og politiet vil påvirke den nasjonale evnen til å håndtere dataangrep, vil jeg i dette kapittelet anlegge tre teoretiske perspektiver: Samfunnssikkerhet, sikringsrisiko og organiseringen av samfunnssikkerheten. Disse tre perspektivene vil gi innsikt i faktorer som styrer den nasjonale evnen til å håndtere dataangrep og hvordan beredskapsaktørene bør organisere seg for å bekjempe trusselen mest mulig effektivt.

Kritiske samfunnsfunksjoner er en av bærebjelkene i det norske samfunn; bortfall av eksempelvis kraftforsyning, telekommunikasjon eller vannforsyning vil merkes umiddelbart (NOU 2006:6, p. 199). Sikkerhetsaktørenes arbeid med beredskap mot dataangrep er derfor en av de viktigste oppgavene innen samfunnssikkerhet. Teoridelen vil gi en oversikt over de viktigste aspektene i samfunnssikkerhet for

senere å kunne vurdere hvordan en ny fordeling av myndighetsoppgaver vil kunne endre den nasjonale evnen til å håndtere dataangrep.

Teori om sikringsrisiko vil gi perspektiver på hvordan sikkerhetsaktørene kan fordele roller forankret i risikoen. Sikkerhetsaktørens rolle vil utspille seg gjennom tiltak innenfor risikofaktorene verdi, trussel og sårbarhet. For å kunne vurdere en eventuell rolleendring må man først forstå hvordan myndighetsorganer vurderer risikoen for tilsiktede hendelser og hvordan sikkerhetsaktørenes forvaltningsoppgaver bidrar til å øke eller senke de tre faktorene.

Sikkerhetsaktørene har flere forvaltningsoppgaver. Dette kapittelet vil se på oppgavene hjemlet i et reguleringsregime. En oppgaveendring blant sikkerhetsaktørene vil potensielt kunne resultere i en lovendring. Teoridelen vil gi perspektiver på hvordan samfunnssikkerhet bør organiseres og samspillet mellom myndighetsoppgaver og regelverk. For at oppgaven skal kunne drøfte en rolleendring mellom sikkerhetsaktørene, må vi også se på premissene forvaltningen legger til grunn ved en eventuell oppgaveendring.

Til slutt vil oppgaven se på tilsyn som eget punkt. Tilsyn er et av samfunnets verktøy for å regulere risiko, men også et viktig punkt i oppgaven da akkurat dette er en potensiell sårbarhet knyttet til sikkerhetsaktørenes roller slik de står i dag.

4.1 Hva er samfunnssikkerhet?

Den nasjonale evnen til å bekjempe dataangrep er viktig for å opprettholde viktige samfunnsfunksjoner. Uten en robust IKT-infrastruktur vil vi til tider miste mange nødvendige og kritiske, private og offentlige funksjoner som borgerne er avhengige av. Samfunnssikkerhet er et bredt og sammensatt begrep; det har endret seg over tid og kan forstås på forskjellige måter.

For å få en dypere forståelse av hvordan IKT-beredskapen er knyttet til samfunnssikkerhet, vil oppgaven se på to overordnete aspekter som dikterer samfunnets generelle arbeid med å sikre samfunnsfunksjonene våre: Definisjonen av samfunnssikkerhet og samfunnssikkerhetskjeden.

4.1.1 Definisjonen av samfunnssikkerhet

Samfunnssikkerhet som begrep ble først tatt i bruk ved Universitet i Stavanger (Den gangen Høyskolen i Stavanger) på slutten av 90-tallet i forbindelse med et studium i sikkerhet og beredskap (Kristiansen, et al., 2017, p. 24). NOU 2000:24, kjent som Sårbarhetsutvalget, tok begrepet i bruk etter det og siden er det blitt etablert både som begrep og fagfelt. Samfunnssikkerhet er et flertydig begrep og har utviklet seg over tid. Begrepet kan forståes ulikt avhengig av kontekst. Oppgaven vil gjennom dette kapittelet komme frem til en begrepsforklaring rundt samfunnssikkerhet knyttet til IKT-sikkerhet og hvordan en rolleendring mellom NorCERT og politiet kan endre sikkerheten i samfunnet. Stortingsmelding nr 17 fra 2002 (St. Meld 17, 2001-2002) definerer begrepet slik:

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

Bjørn Ivar Kruke bruker også denne definisjonen i sitt Notat til 22. juli-kommisjonen. Kruke utreder hva som ligger i begrepet ”evne” (Kruke, 2012):

"Evne er den kapasiteten samfunnet har til å takle dets iboende sårbarhet ved forebyggende aktivitet, håndtering av kritiske situasjoner, og til restituering etter en slik svikt."

Kruke velger å forstå evne som samfunnets kapasitet til å dreie seg om tre ting: drive forebygging, håndtering og gjenopprette til normal eller ny tilstand.

En nyere definisjon av begrepet samfunnssikkerhet kom i Meld. St 10 (Meld. St. 10, 2016-2017). Oppgaven legger også denne definisjonen til grunn i beskrivelsen av samfunnssikkerhet**:**

"Samfunnssikkerhet er samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger."

Definisjonen over fra Meld. St 10 fra 2017 dekker bredere enn definisjonen fra 2002. Begge definisjonene tar i bruk ordet *funksjoner* samt *liv og helse*. Meld. St 10 fra 2017 har lagt til begrepet *"grunnleggende verdier"*. Dette begrepet er omfattende og vanskelig å definere, men i en samfunnssikkerhetskontekst kan forhold som personvern, ytringsfrihet og fri flyt av informasjon være med å forme det (Meld. St. 10, 2016-2017, p. 64). I tillegg har definisjonen fra 2017 tatt med eksempler på hva som kan utløse hendelser samfunnet skal verne seg mot. Eksemplene gjelder både tilsiktede og utilsiktede hendelser. Denne definisjonen sett opp mot tidligere definisjoner tydeliggjør behovet for det forebyggende arbeidet gjennom "verne seg mot", som er en av hovedoppgavene i en IKT-beredskapskontekst. Definisjonen har også med "grunnleggende verdier" som er viktig, da eksempelvis dataangrep fra en fremmed stat ikke nødvendigvis vil gå direkte på behov, liv og helse, men kan også kompromittere statshemmeligheter og påvirke valg. Av den grunn har oppgaven valgt og å ta i bruk denne definisjonen i det videre arbeidet.

Grunnleggende funksjoner kan forstås som samfunnskritiske funksjoner og institusjoner som ivaretar de viktigste oppgavene som skal sikre borgernes grunnleggende behov. Utredningen NOU 2006:6 *Når sikkerheten er viktigst* beskriver grunnleggende behov til å være fysiske behov og trygghet, og utvalget mener begrepet *kritisk samfunnsfunksjon* (Appendiks A) er det som sikrer borgerne de mest grunnleggende behov som mat, vann, ly, sikkerhet og beskyttelse. Direktoratet for samfunnssikkerhet og beredskap (DSB) har definert 14 kritiske samfunnsfunksjoner i en rapport fra 2016. Arbeidet med å definere kritiske samfunnsfunksjoner er viktig, da det kan betraktes som *"grunnpilarer for samfunnets robusthet"* og gir et godt utgangspunkt når man skal fordele ansvar og oppgaver (DSB, 2016).

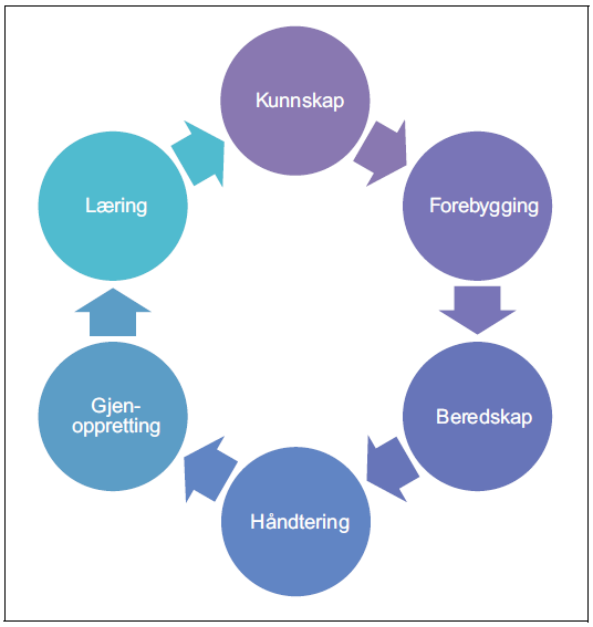
Befolkningens og samfunnets grunnleggende behov	Samfunnskritisk funksjon
Styringsevne og suverenitet	Styring og kriseledelse
	Forsvar
Befolkningens sikkerhet	Lov og orden
	Helse og omsorg
	Redningstjenester
	IKT-sikkerhet
	Natur og miljø
Samfunnets funksjonalitet	Forsyningssikkerhet
	Vann og avløp
	Finansielle tjenester
	Kraftforsyning
	Elektroniske kommunikasjonstjenester
	Transport
	Satellittbaserte tjenester

Tabell 1: DSBs definerte samfunnskritiske funksjoner

4.1.2 Samfunnssikkerhets- og beredskapskjeden

For å lettere å kunne få oversikt og sammenligne rollene til de ulike sikkerhetsaktørene innen samfunnssikkerhet knyttet til IKT-beredskap, vil jeg gjøre en fordeling av de ulike fasene i beredskapsarbeidet. NSM og politiet sitter med det samme ansvaret i noen av rollene og er alene om andre. Offentlige rapporter og utredninger peker på berøringspunkter i de ulike fasene. Teoridelen i dette kapittelet vil definere de fasene i beredskapsarbeidet som er best egnet som verktøy for å belyse rolleutfordringene mellom NorCERT og politiet.

Meld. St 10 fra 2017 beskriver en samfunnssikkerhetskjede i den hensikt å belyse alle leddene eller fasene man går gjennom i arbeidet med å sikre samfunnet.



Figur 3: Samfunnssikkerhet som kjede (Meld. St. 10, 2016-2017, p. 21)

Arbeidet med samfunnssikkerhet og beredskap bør forankres i *kunnskap* og erfaringer. Dette vil kunne gi informasjon om hvilket tiltak som kan fungere best. I dette arbeidet er det viktig å bruke gode metoder som gir kunnskap om risikoen som truer verdiene i samfunnet. Risikoanalyse vil være et godt verktøy til dette. I dette arbeidet må vi forstå hva eller hvem som truer de ulike verdiene, samt hvordan verdiene er sårbare og hvordan de påvirker hverandre.

Arbeidet med å redusere muligheten og konsekvensene av en potensiell hendelse er *forebygging*. Dette kan være alt fra rassikring til å installere sensorer på den digitale infrastrukturen slik NSM gjør. Å ha redundans kan også være forebyggende, eksempelvis å ha viktig informasjonen lagret på uavhengige medier.

Gjennom kunnskap og erfaringer skal alle virksomheter involvert i samfunnssikkerhet drive *beredskapsarbeid* og ha en plan for handling ved en uønsket hendelse. Planen skal ta høyde for de fire prinsippene for samfunnssikkerhet: ansvar, nærhet, likhet og samvirke. Virksomhetene involvert skal også ha tilgjengelig operativt personell og materiell for å bidra til håndtering av krisen.

Gjennom godt beredskapsarbeid skal man kunne *håndtere* krisen; det er viktig at personell satt av til å lede håndteringen har de fullmakter som er nødvendig for god krisehåndtering.

Når krisehåndteringen går mot slutten, skal fokus skifte på å *gjenopprette* samfunnsfunksjonene. I dette arbeidet kan funksjonen gjenopprettes til den samme tilstanden før krisen inntraff, eller så kan vi bruke kunnskapen vi har fått til å gjenopprette funksjonen til en ny tilstand som gir større evne til å tåle nye påkjenninger i fremtiden.

Læring får vi fra erfaringer ervervet gjennom øvelser og hendelser. Det er ikke noe automatikk i at vi lærer noe fra øvelser og hendelser, det er derfor viktig at vi setter det som et eget punkt i samfunnssikkerhetskjeden. Dette etterarbeidet gir kunnskap og er viktig når vi skal optimalisere det kontinuerlige fokuset vi skal ha på det forebyggende arbeidet.

4.1.2.1 Norges hovedprinsipper innen arbeid med samfunnssikkerhet

Den norske samfunnssikkerhetsmodellen bygger på fire prinsipper: *Ansvar, likhet, nærhet* og *samvirke*. Prinsippene kan forstås som et virkemiddel for å styre samfunnssikkerheten og fordele roller. Teoridelen vil vektlegge samvirkeprinsippet, da mye av suksesskriteriene for håndtering av dataangrep i dag hviler på dette prinsippet. Prinsippene *ansvar, likhet og nærhet* ble introdusert i en stortingsmelding i 2002 (St. Meld 17, 2001-2002). Disse er ikke unike for Norge, men brukes også av andre nasjoner vi kan sammenligne oss med, blant annet Sverige og Danmark. Samvirke som en del av en beredskapsmodell er derimot foreløpig unikt for Norge, og ble lagt til modellen som konsekvens av 22. juli-hendelsen (Kristiansen, et al., 2017). Samvirke har lenge vært kjent blant offentlige aktører, særlig mellom politi, brann og ambulanse, men ble satt på dagsorden av stortingsmelding nr 29 i 2002 i den hensikt å belyse regjeringens tverrsektorielle ansvar for samfunnssikkerhet og beredskap. For å utnytte ressursene best mulig på tvers av sektorene, må samfunnet ha et velfungerende samvirke mellom aktørene (Meld. St. 29, 2011-2012).

4.1.2.2 Samvirke

En av de største utfordringene knyttet til samfunnssikkerhet er selve den forvaltningsmessige organiseringen av aktører som skal drive hendelseshåndteringen. En trusselaktør vil ikke ta hensyn til om angrepet er sektoroverskridende eller ikke. Når den uønskede hendelsen kun treffer et departement, organisasjon eller etat, ser man at krisehåndteringen ofte fungerer bra (Engen, et al., 2016, p. 52). Fra dette perspektivet kan man si at samhandling er et nødvendig onde. Dette er en viktig årsak til at jeg drøfter om fordelingen av myndighetsoppgaver er hensiktsmessig fordelt med hensyn til den nasjonale evnen til å bekjempe dataangrep.

Som regel vil en større hendelse være sektoroverskridende og utløse et behov for samhandling med alle dets utfordringer (Engen, et al., 2016, p. 52). Kvaliteten på krisehåndteringen vil ofte være avhengig av forberedelsene gjennomført i forkant. For at krisehåndteringen skal fungere på tvers av sektorer, er det nødvendig med en entydig ansvars- og rollefordeling (Engen, et al., 2016, p. 283). Det er derfor viktig at de fire beredskapsprinsippene over følges av samtlige departementer med tilhørende underlagte virksomheter og at de gis oppmerksomhet under hele beredskapsarbeidet.

En beredskapsplan skal inneholde en tydelig rolle- og ansvarsfordeling for alle offentlige, private og frivillige aktører som er involvert. Effekten av hendelseshåndteringen er ofte styrt av effektiviteten i samvirket mellom beredskapsaktørene. Dette er en av hovedgrunnene til at samvirkeprinsippet kom inn som et sentralt prinsipp i beredskapsarbeid. Aktørene må kjenne til alle andres mandat, struktur, kapasitet og begrensninger inn mot hendelseshåndtering for å kunne styre mot den beste løsningen (Engen, et al., 2016, p. 290).

4.1.3 IKT-Beredskap

Beredskap i en IKT-kontekst kan gjelde alt fra virksomheters beredskapsplan for en lokal serverfeil til NSMs beredskapsarbeid med å sikre samfunnskritiske funksjoner. NOU 2000: 24 definerer beredskap slik *"Tiltak for å forebygge, begrense eller*

håndtere uønskede ekstraordinære hendelser". Fra denne begrepsforklaringen forstår vi forebygging og håndtering som en del av beredskap.

De ulike fasene i en IKT-beredskapsmodell er viktig å forstå, da oppgaven drøfter hvor i beredskapen berøringspunktene ligger mellom NSM og politiet. Beredskap i det digitale domenet er ikke det samme som beredskap i det fysiske. Eksempelvis vil punktet *avdekke* ha mye større tyngde i en cyberkontekst, da dette er en av hovedutfordringene til sikkerhetsaktørene. Til sammenligning vil ikke en krise som flom eller storm være noe man trenger å avdekke. Det finnes per dags dato ingen eksakt felles forståelse av hvordan en IKT-beredskapskjede ser ut. Rammeverk for håndtering av IKT-sikkerhetshendelser (Appendiks A) (NSM, 2017) bruker prosessen beskrevet i ISO-standard 27001: *Information security management systems — Requirements*. I denne kjeden har de med:

1. Planlegging og forberedelse
2. Deteksjon og vurdering av omfang og alvorlighetsgrad
3. Varsling av relevante parter
4. Iverksetting av prosesser og tiltak for å håndtere hendelsen
5. Situasjonsrapportering
6. Tilbakeføring og læring av hendelsen

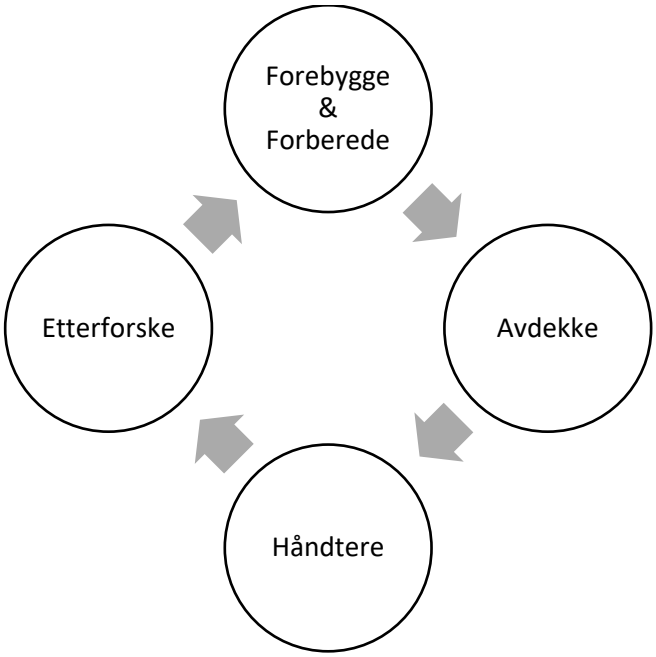
Lysne-utvalget ga selskapet Mnemonic i januar 2015 i oppdrag å samle innspill fra de operative miljøene i Norge med tanke på avdekking, håndtering og etterforskning knyttet til beredskapsarbeid mot cyberangrep (Mnemonic, 2015). Mnemonic har i sin rapport til Lysne-utvalget laget en modell (se figur 7) som tar for seg hvilke sikkerhetsaktører som har ansvar opp mot de tre siste fasene; avdekke, håndtere, etterforske. Modellen i rapporten tar ikke for seg forebygging (Mnemonic, 2015, p. 16), men legger til forberede og planlegge av de øvrige punktene som et eget punkt.

1. Forberede/planlegge
2. Avdekke
3. Håndtere
4. Etterforske

Lysne-utvalget (NOU 2015:13) beskriver ikke noen IKT-beredskapskjede, men en håndteringskjede med fire begreper som blir brukt til å beskrive de ulike faser:

1. Forebygge
2. Avdekke
3. Håndtere
4. Etterforske

Disse begrepene går igjen i flere offentlige rapporter og utredninger. Jeg vil bruke disse fire begrepene til å beskrive de ulike fasene i en IKT-beredskapskjede og knytte dem til sikkerhetsaktørenes berøringspunkter i deres respektive roller i de ulike fasene.



Figur 4: IKT-Beredskapskjeden

4.1.3.1 Forebygge

Forebygging er alle virksomheters sikkerhetsarbeid i forkant av en hendelse i den hensikt å redusere risiko for dataangrep. Beredskapsplan, deling av informasjon og sårbarhetskartlegging er avgjørende med tanke på forebygging.

Kripos gir ut årlige rapporter om trender og IKT-trusselen knyttet til organisert kriminalitet. Etterretningstjenesten og PST gir ut årlige trusselvurderinger som *Fokus 2018* og *Trusselvurdering 2018*. NSM gir ut årlige rapporter som *Helhetlig IKT-risikobilde* og *Risiko*. Offentlige og private virksomheter er avhengig av denne type

informasjon for å ta gode beslutninger rundt forebyggende tiltak mot dataangrep. I tillegg til offentlige rapporter utgitt av sikkerhetsaktørene, er det avgjørende at virksomheter som blir rammet deler denne informasjonen slik at sikkerhetsaktørene kan utnytte ressursene sine på en formålstjenlig måte (NOU 2015:13, p. 257).

Politiet benytter seg av flere virkemidler i sitt forebyggende arbeid. Et av dem er tilstedeværelse og patruljering på internett. Gjennom sosiale media gir de ut informasjon om alvorligheten av ulike handlinger, som eksempelvis deling av private bilder og personopplysninger. Dette er i seg selv preventivt, da det skaper bevissthet rundt kriminelle handlinger og deres konsekvenser for lovbrytere. Sikkerhetsaktørene forsøker i sitt forebyggende arbeid å gripe tidlig inn i planleggingsfasen der trusselaktører utvikler ondsinnede koder for å ramme virksomheter (POD, 2015, p. 15).

Å kartlegge sårbarheter et av de viktigste bidragene i det forebyggende arbeidet, for å kunne sette inn mer robuste løsninger der det trengs. NSM utfører varslet tilsyn og penetrasjonstesting mot virksomheters IKT-systemer underlagt sikkerhetsloven i den hensikt å finne sårbarheter. Denne tjenesten kalles Alvis NOR (NOU 2015:13, p. 258).

4.1.3.2 Avdekke

Avdekking er aktiviteter satt i system for å oppdage dataangrep. Her skiller kriser innen IKT seg fra annen type kriser. En IKT- krise utløst av et angrep er ikke en ulykke, men en tilsiktet handling. Trusselaktøren vil bruke en eller flere ondsinnede koder designet for å infisere mest mulig uten at det oppdages. Skal man i det hele tatt klare å løse krisen må man først finne den. Avdekking er et av fire sentrale punkter i IKT-beredskapskjeden. Et alvorlig dataangrep har som regel flere faser. Det begynner med rekognosering fra trusselaktørens side; angriperen forsøker å skaffe seg tilgang, eksempelvis gjennom phishing (Appendiks A), for så å stjele informasjon eller sabotere. Angrepet kan avdekkes i alle disse leddene. Virksomheter kan oppdage en rettet phishing-kampanje eller oppdage avvikende aktivitet på nettverket til klientene sine. NorCERT er pålagt det nasjonale ansvaret med å avdekke alvorlige angrep gjennom sensornettverket VDI (NOU 2015:13, p. 259).

4.1.3.3 Håndtere

Håndtering er knyttet til alle aktiviteter som dreier seg om analyse av årsak, minimerer skade, stoppe angrep, monitorere angrep eller gjenopprette til normaltilstand eller bedre. Analyse kan også være teknisk analyse der det drives "reverse enginering" av den skadelige koden for å avdekke angrepets intensjon. Ansvaret for håndteringen ligger hos virksomheten selv. Selve håndteringen av et dataangrep skjer som regel gjennom et samarbeid mellom virksomheten og en sikkerhetsaktør. Hvilken aktør som støtter virksomheten vil avhenge av omfanget av angrepet og hvilke sektorer som angripes. Hvis det for eksempel dreier det seg om organisert kriminalitet som rammer finanssektoren, vil det være naturlig at Kripos håndterer det. Er angrepet alvorlig og rettet mot kritiske samfunnsfunksjoner, vil det – slik rollefordelingen er i dag – være naturlig at NorCERT bistår i håndteringen av det. I 2017 ble Norge rammet av 22 000 dataangrep der 5 000 av disse ble prioritert og fulgt opp av NorCERT (NSM, 2017). Enkelte saker har en så høy alvorlighetsgrad at de løftes opp til FCKS. FCKS har ingen instruksjonsmyndighet overfor NorCERT, men den samlede kompetansen og informasjonen i gruppen kan bidra til å få et bedre bilde av situasjonen, som utløser en god fordeling av roller og ansvar for håndteringen. Den viktigste faktoren for fordeling av roller innen håndtering er angrepets skadepotensial og omfang (NOU 2015:13, p. 259).

4.1.3.4 Etterforske

Etterforskning er det punktet i beredskapskjeden som har en tydelig rolleavklaring. Oppgaven vil drøfte hvor det er berøringspunkter i rolleutøvelsen mellom sikkerhetsaktørene. Ingen av de offentlige rapportene eller utredningene i litteraturlisten behandler uklarhet i rolleforståelse innen etterforskning. Lysne-utvalget beskriver etterforskning som å være en aktivitet kun politiet og PST utfører og som kun er knyttet til arbeidet med å avdekke straffbare forhold. Andre aktører kan bistå i etterforskningen ved behov, men ansvaret ligger hos politiet og PST.

4.2 IKT-Sikringsrisiko

Sentral teori om sikringsrisikoanalyse vil være et godt verktøy for å avdekke verdi, trussel og sårbarhet som til sammen utgjør den totale sikringsrisikoen. Politiets og

NSMs roller er fastsatt i sikkerhets- og politiloven, og deres myndighetsoppgaver vil være grunnlaget for en avgrensning av disse rollene. Om en rolleendring mellom politiet og NSM fører til en bedre regulering av verdi, trussel og sårbarhet, vil dette endre den nasjonale evnen til å håndtere dataangrep.

Det vil være hensiktsmessig å ha en risikobasert tilnærming til samfunnssikkerhet, da det vil gi innsikt i hvor risikoen er størst. Dette vil gi de ansvarlige aktørene grunnlag for å drive god ressursstyring i arbeidet med å utarbeide en beredskapsplan. Man kan forstå det overordnede målet i arbeidet med samfunnssikkerhet og beredskap gjennom kunnskap om påvirkningsfaktorene verdi, trussel og sårbarhet (Meld. St. 10, 2016-2017, p. 19). Disse faktorene går igjen når man skal analysere risiko mot tilsiktede hendelser, der trusselen tiltrekkes av verdien og utnytter sårbarheten, og sårbarheten eksponerer verdien. Risikoanalyse vil være et godt verktøy i arbeidet med å systematisere den kunnskap og de erfaringer man bruker ved utarbeidelse og implementering av tiltak for å sikre verdiene våre mot dataangrep. For å forstå hvordan risiko er knyttet til tilsiktede handlinger i en IKT-kontekst, vil dette kapittelet gjennomgå begrepet risiko og hvordan sikkerhetsaktørene bruker risikomodeller knyttet til tilsiktede handlinger.

4.2.1 Risikobegrepet

Det finnes flere definisjoner av risiko, avhengig av kontekst. Generelt kan man si at risiko dreier seg om hva som kommer til å skje frem i tid. Man prøver å predikere risikoen ved å benytte informasjon om årsakssammenhenger i hendelser bak i tid. Historisk har man beskrevet og tallfestet risiko gjennom sannsynlighet ganger konsekvens, Risiko=P x C. Sannsynlighet og konsekvens er fortsatt to viktige faktorer, men vi må se mer helhetlig på risiko og tillegge usikkerhet mer tyngde når vi beskriver risiko (Aven & Renn, 2010). Aven skriver at man kan utrykke usikkerhet gjennom en kunnskapsbasert sannsynlighet der en henviser til den bakgrunnsinformasjonen som er brukt for å vurdere sannsynlighetsgrad (Aven, 2015). I den sammenheng er det også viktig å forstå at risiko alltid blir sett gjennom noens øyne og alltid vil være subjektiv (Aven, et al., 2004).

Aven definerer begrepet risiko slik (Aven & Renn, 2010) (FFI, 2017): *Risiko er en opptreden av hendelser med påfølgende konsekvenser og tilhørende usikkerhet*. Denne definisjonen gir en bred beskrivelse av begrepet risiko og dekker de fleste kontekster, også innen risiko knyttet til dataangrep. Selv om Avens definisjon av risiko også er dekkende for dataangrep, vil oppgaven velge definisjonen fra Norsk Standard 583x-serien, da denne er spesifikt knyttet til tilsiktede handlinger.

4.2.2 VTS-modellen

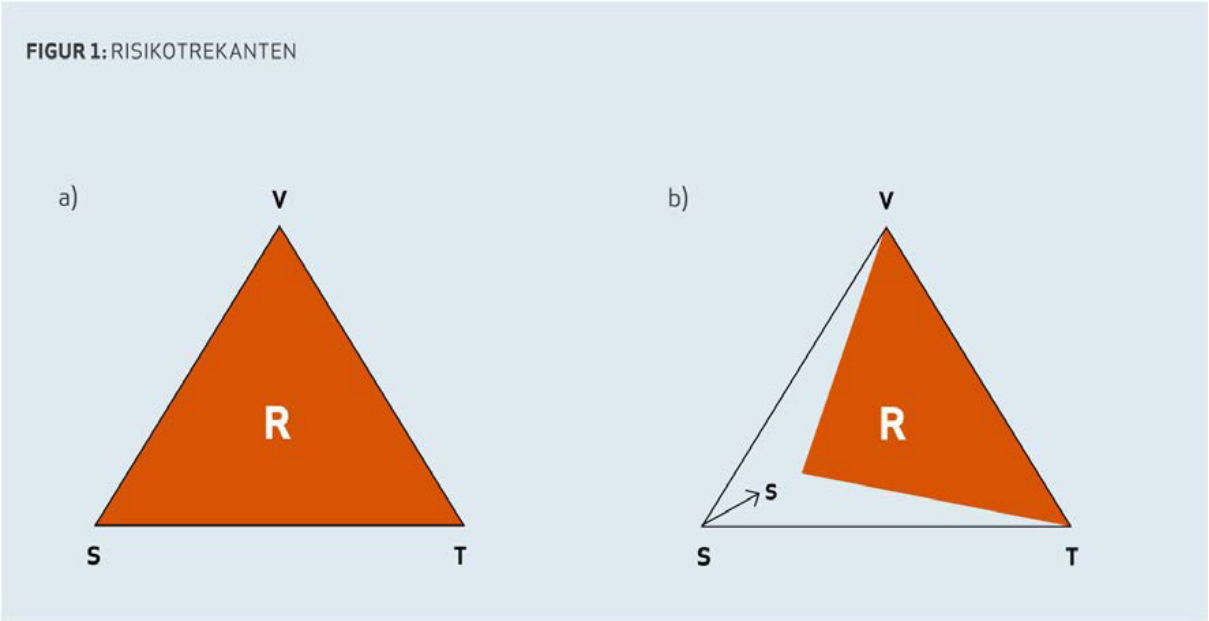
Norsk Standard (NS) 583x-serien er en standard som retter seg mot fagområdet sikring og knytter risiko opp mot *tilsiktet* uønskede handlinger. Standarden definerer risiko som:

"Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen."

Dette kalles trefaktor- eller VTS-modellen og består av parameterne: verdi-trussel-sårbarhet. Denne modellen er utelukkende utformet for å vurdere risiko opp mot tilsiktet uønskede handlinger. En tilsiktet uønsket handling defineres av NS 5830:2012 som *"en hendelse som forårsakes av en aktør som handler med hensikt."* Måloppnåelsen til aktøren kan være å fremme egne interesser eller skade en verdi (FFI, 2017). Standarden er bygd på at man ikke tallfester usikkerheten gjennom matematisk sannsynlighet, men i stedet bruker kunnskapsbasert sannsynlighet. Det finnes mye statistikk om dataangrep som gir et godt bilde av sann tid, men det gir ikke nødvendigvis gode prediksjoner for avanserte angrep frem i tid. Trusselaktører som spesialiserer seg på digitale angrep vil hele tiden prøve å finne nye sårbarheter og skrive nye koder for å penetrere systemene våre. Dette er en av grunnene til at man heller velger vekk statistikk i beslutningsgrunnlaget nå man vurderer sikringsrisiko (Barane, 2015). I stedet for å beregne sannsynligheten kvantitativt, benyttes det heller tilgjengelig bakgrunnskunnskap. Sannsynlighet utrykkes kvalitativt gjennom en skala, eksempelvis: svært sannsynlig – sannsynlig – lite sannsynlig.

Figur 5 viser en balanse mellom verdier, trusler og sårbarheter som brukes for å beskrive den aktuelle risikoen. I figuren under ser vi at arealet i trekanten

representerer den totale risikoen. I trekanten til venstre ser vi risikoen for et aktuelt scenario før tiltak, og i trekanten til høyre ser vi at risikoen er redusert som følge av sårbarhetsreduserende tiltak.



Figur 5: VTS modellen (NSM , 2015, p. 19)

4.2.2.1 Verdi

Målet for sikringen tar utgangspunkt i den verdi man ønsker å beskytte, uavhengig av de andre to faktorene. Veilederen for risikovurdering (NSM, 2016, p. 9) sier at sikringsrisikovurderinger som tar utgangspunkt i verdi er en god måte å drive sikkerhetsstyring på. Verdiene kan eksempelvis være materielle eller immaterielle; tap av renommé vil være et eksempel på en immateriell verdi. I arbeidet med å vurdere verdien, er det viktig å se verdi opp mot aktuelle konsekvenser (NSM, 2016, p. 11). Eksempelvis kan en virksomhet vurdere verdien av informasjonen på en server til å være høy eller lav ut fra hvilket skadeomfang det kan få om den går tapt, eksponert eller blir brukt av andre. Det er verdt å merke seg at om det ikke eksisterer noe skadepotensiale, vil det heller ikke finnes noe verdi. Er verdien null, finnes det heller ingen risiko. Virksomheter kan også redusere risiko gjennom å redusere verdi, men dette blir ofte lite hensiktsmessig, da virksomhetens formål som regel er å holde på eller øke verdien i sin egen virksomhet.

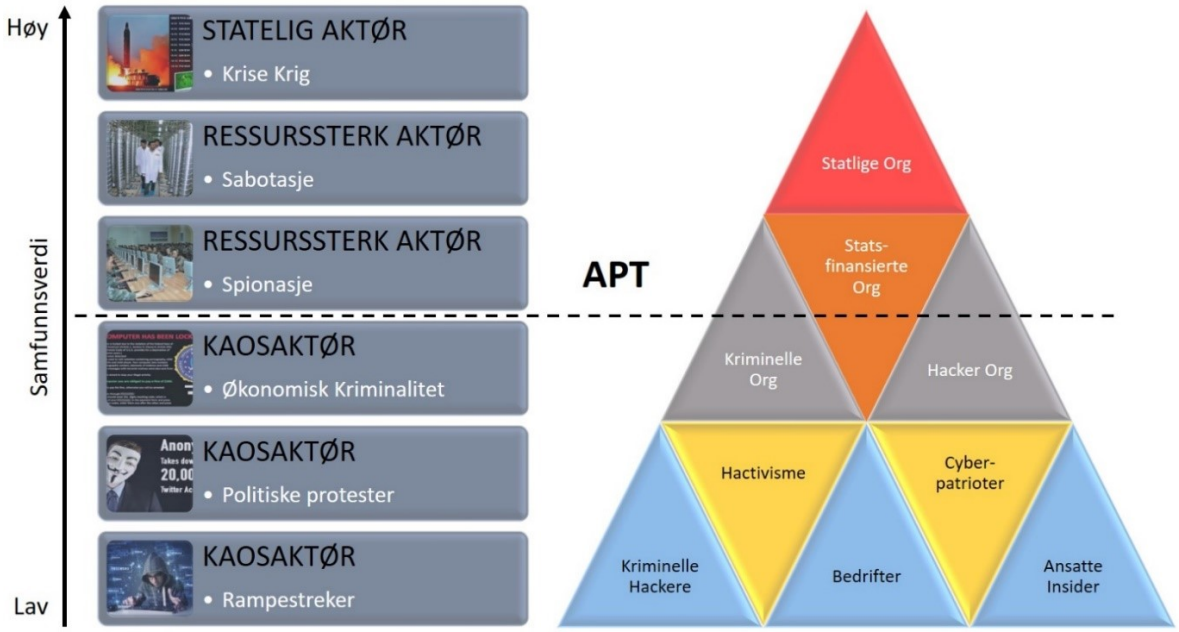
En klar rolle- og ansvarsfordeling mellom sikkerhetsaktørene vil gi god kunnskap om hvilke samfunnsfunksjoner (verdier) som skal beskyttes av de ulike aktørene. Verdiene bør kartlegges av den ansvarlige beredskapsaktøren for å se hvordan de påvirker hverandre. Eksempelvis vil et vellykket angrep mot kraftsektoren påvirke en rekke andre kritiske og ikke-kritiske samfunnsfunksjoner. Det er da viktig at man ikke etter hendelsen går i gang med å finne ut av hvem som har ansvaret for den rammede verdien, men at ansvaret er avklart i forkant.

4.2.2.2 Trussel

Når verdiene er identifisert og kvantifisert, skal man vurdere aktuelle trusler mot kartlagte verdier. Man ønsker her å kategorisere trusselen; dette kan gjøres på forskjellige måter. NSM (NSM, 2016, p. 14) anbefaler å dele opp truslene i de overordnede kategoriene spionasje, sabotasje, terrorhandlinger og annen alvorlig kriminalitet. Hvis man ser isolert på IKT-sikkerhetsrisiko, kan man kategorisere etter trusselaktør (se modell 8). VTS-modellen utrykker trusselen i hovedsak gjennom trusselaktørens intensjon og kapasitet (FFI, 2017, p. 27). Intensjonen med angrepet kan være hevn fra en misfornøyd medarbeider eller leilighetshandling til en statsaktør som ønsker å stjele teknologi.

En avklaring av hvilke sikkerhetsaktører som håndterer og har ansvar for å kartlegge ulike trusselaktører kan ha en betydning mht. hvilket ansvar og myndighet sikkerhetsaktøren har. Hvis for eksempel trusselaktøren er en fremmed stat, vil det være naturlig at en av etterretningsaktørene og ikke politiet håndterer angrepet. NSM og politiet produserer årlig rapporter om trusselbildet. Rapportene er utarbeidet på bakgrunn av den kunnskap som er oppnådd gjennom informasjonsdeling mellom offentlige og private virksomheter samt datainnsamling fra NSMs sensornettverk VDI. Dette gir et godt bilde av det nasjonale IKT-trusselbildet som ulike virksomheter kan legge til grunn når de gjennomfører tiltak for å redusere sårbarheter. I dag er det få tilfeller av dataangrep som blir etterforsket; dette fører til at trusselaktører ikke ser noe risiko i å utføre angrep. En økt risiko for å bli straffet kan i seg selv virke preventivt og være med på å redusere trusselen. Som ett ledd i å redusere IKT-*trusselen* kan politiet etterforske med sikte på å ta ut påtale. Straff er et effektivt

virkemiddel for å hindre trusselaktøren i å gjenta angrep og vil derfor kunne redusere trusselen (POD, 2015, p. 17).



Figur 6: APT-terskelen - Modellen er hentet fra NSM og sammenstilt av flere modeller

Når man analyserer risikoen iht. til NS 5832 vil man på bakgrunn av kartlagt informasjon om trusselaktør lage trusselscenarier relevante for den verdi man skal beskytte. Disse scenarier har til hensikt å belyse intensjon og kapasitet til de ulike trusselaktørene, som senere gir grunnlag for å vurder sårbarhet.

4.2.2.3 Sårbarhet

Med bakgrunn i potensielle trusselscenarier som kan ramme verdiene, ønsker man å belyse sårbarheten. NS 5830 utrykker sårbarhet som *manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønskede påvirkninger*. Sårbarheter er ofte et resultat av utilstrekkelig eller feil sikring av verdier, og har til hensikt å belyse et gap mellom allerede innførte sikringstiltak og trusselaktørens intensjon og kapasitet til å ramme verdien (NSM, 2016, p. 19). I en IKT sikringskontekst vil det ofte være snakk om å redusere logiske sårbarheter. Under er listet opp noen eksempler på IKT-sårbarheter hentet fra NSMs håndbok i risikovurdering:

• Manglende tilgangskontroll i systemer.
• Manglende oppgradering av program- og maskinvare.
• Manglende installasjon av sikkerhetsoppdateringer.
• Manglende registrering av datatrafikk og tiltak for å oppdage illegitime brukere.
• Sluttbrukere er tildelt administratorrettigheter.
• Brukere kan kjøre programvare som ikke er godkjent av virksomheten.
• Manglende herding av applikasjoner.
• Manglende bruk av klientbrannmurer.
• Manglende eller feil bruk av diskkryptering.
• Manglende oversikt over eget nettverk og egne systemer.
• Manglende bruk av sikkerhetssystemer og sikkerhetsprogrammer.
• Manglende evne til å oppdage uønsket aktivitet i nettverk

Skal virksomhetene sikre verdiene sine gjennom å redusere risikoen, er det som regel gjennom sårbarhetsreduserende tiltak (NSM, 2016). I henhold til sikkerhetsloven § 5 er det virksomheten selv som har hovedansvaret for å forebygge dataangrep. Departementene har ansvaret for å forebygge i sin sektor. I henhold til sikkerhetsloven § 8 skal NSM koordinere forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden på tvers av sektorer. Politiet skal forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet i henhold til politiloven § 2. Fra lovteksten kommer det fram at NSM og politiet har ansvaret for å utforme det forebyggende arbeidet nasjonalt.

4.3 Organisering av samfunnssikkerheten

Denne delen av teorien vil se på hva litteraturen mener om organiseringen av samfunnssikkerhet gjennom risikoregulering, offentlig omstilling og tilsynsforvaltning.

4.3.1 Risikoregulering

Samfunnets kontroll av risiko er kompleks og består av en rekke virkemidler. Det er en utfordring å ha en generisk organisering av samfunnssikkerhet som passer alle virksomheter uavhengig av roller og ansvarsområder. Man har derfor valgt å ta i bruk noen virkemidler for å håndtere organiseringen av samfunnssikkerhetsfeltet som gjør

det lettere å operasjonalisere den. Samfunnets regulering av risiko skjer på ulike nivåer, alt fra lovregulering med rettslige virkemidler til internreguleringer forankret i virksomhetens egne instrukser. I boken Perspektiver på samfunnssikkerhet (Engen, et al., 2016, p. 50) pekes det på ulike virkemidler for å organisere samfunnssikkerheten.

Reguleringsregime i en samfunnssikkerhetskontekst er en overordnet styring gjennom lover og regler der myndighetsorganet ser på selve risikoen og hvilke interessenter den treffer (Engen, et al., 2016, p. 228). Myndighetene har for eksempel gjennom sikkerhetsloven satt krav til virksomheter underlagt sikkerhetsloven om å ha et visst minimum av sikringstiltak mot intenderte handlinger. Skulle risikobildet endre seg, vil myndighetene med innspill fra flere samfunnsaktører regulere kravene opp eller ned for å treffe riktige tiltak i forhold til trusselnivå.

Samstyring er en ikke-hierarkisk prosess der offentlige og private aktører samarbeider om løsninger. Samstyring vektlegger særlig tre momenter: Aktørene har felles mål og stiller med ressurser til dette, det eksisterer en gjensidig avhengighet uten skeivfordeling av makt, og det er god organisering med relevante aktører som får velge strategi og virkemiddel (Engen, et al., 2016, p. 236). Eksempelvis vil det samarbeid innen VDI-løsningen som NSM har med private virksomheter være utarbeidet gjennom samstyring. Virksomheten øker sin egen IKT-sikkerhet og NSM får informasjon som bidrar i deres forebyggende arbeid. Målene til organisasjonene overlapper og dette bidrar til økt samfunnssikkerhet.

Best praksis blir utøvd når man følger en norm eller adferd myndighetene forventer at virksomheten skal følge innenfor rammer satt i loven (Engen, et al., 2016, p. 240). NSM gir ut veiledere for hvordan en kan tolke formålsbaserte regelverk som gjør det lettere for virksomhetene å følge best praksis. I tillegg til veiledninger og de aktuelle rettslig bindende lovene og forskriftene (se tabell 2), kan virksomheter velge om de vil følge standarder. Innen sikkerhetsarbeid finner vi nasjonale standarder som NS 583x-serien, som beskriver terminologi, best praksis for sikringsrisikoanalyse, sikringsrisikostyring og sikringstiltak for beskyttelse av bygg. NSM, etterretningstjenestene, PST og politiet bruker metodikken beskrevet i NS5832 når de skal utføre en sikringsrisikoanalyse (NSM , 2015). Virksomheten står fritt til å

velge å følge en standard, men samfunnet er tjent med at flest mulig følger de samme normene i den hensikt å oppnå felles forståelse og handlingsmønster.

Internkontroll er en del av virksomhetens egenkontroll og skal sikre at det ikke skjer avvik fra lover og regelverkskrav. Internkontrollen kan beskrives som en kontroll av egen virksomhet med hensyn til rettslige og ikke-rettslige bestemmelser. Noe av hovedhensikten med internkontroll er å gi handlingsrom for løsninger tilpasset spesifikke virksomhetsområder (Engen, et al., 2016, p. 247). Eksempelvis vil forskrift om sikkerhetsadministrasjon i hovedsak tvinge på plass et krav om internkontroll ved utførelsen av tiltak, for å sikre at virksomhetens aktiviteter utføres og planlegges i henhold til krav satt av sikkerhetsloven (Forskrift om sikkerhetsadministrasjon, 2001).

Kategori	Hovedgruppe	Sikkerhet mot trusler
Rettslig bindene bestemmelser	Lover	• Internasjonal lovgivning • Sivilbeskyttelsesloven • Sikkerhetsloven • Politiloven
	Forskrifter	• Forskrift om kommunal beredskapsplikt • Forskrift om objektsikkerhet • Forskrift om personellsikkerhet • Forskrift om informasjonssikkerhet • Forskrift om sikkerhetsadministrasjon • Forskrift om sikkerhetsgraderte anskaffelser
Ikke rettslig bestemmelser	Veiledninger	• Veiledning i objektsikkerhet • Veileder i terrorsikring • Veiledning for sikkerhetsgraderte anskaffelser • Veiledning i verdivurdering • Veiledning i sikkerhetsstyring • Veiledning i sikkerhetsrevisjon • Veiledning i personellsikkerhet • Veiledning i sikring av industrielle automatiserte kontrollsystemer

		• Veiledning i fysisk sikring mot ulovlig inntrengning • Veiledning for sikring av kryptorom • Veiledning i sikring mot avlytting • Veiledning TEMPEST sikring av IKT-systemer
	Standarder	• NS 583x Serien - Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger • ISO 2700x Serien – Standarder innen informasjonssikkerhet

Tabell 2: Rettslige og ikke-rettslige bestemmelser - Matrisen er hentet fra (Engen et al., 2016, p. 239) og tilpasset

4.3.2 Rolleendring i forvaltningen

En rolleendring må gjøres i samsvar med god forvaltningsskikk. Forvaltningsloven og generelle forvaltningsprinsipper setter noe av rammeverket for en eventuell rolle- og oppgaveendring mellom sikkerhetsaktørene. For at oppgaven skal kunne drøfte endring av oppgaver mellom sikkerhetsaktørene, vil teoridelen se på ulike aspekter med hensyn til generell forvaltningspraksis innen offentlig omstilling. Et av fokusområdene til regjeringen er IKT-sikkerhet. Gjennom utredninger og rapporter har de avdekket sårbarheter og sett på hvordan vi nasjonalt er organisert for å stå imot dataangrep. Sårbarhetsutvalget (NOU 2015:13) anbefaler en omorganisering der de blant annet ser på samlokalisering, informasjonsdeling og rolleendringer. Statsforvaltningens oppgave er å sikre stabilitet, kontinuitet og tydelige rammer for et velfungerende samfunn. Skal det politiske system og demokratiske prinsipper fungere godt, må forvaltningen fungere godt. (St.Meld 19, 2008-2009)

Antall ansatte i forvaltningen i dag er fire ganger lavere enn i 1992, vi gikk fra 829 forvaltingsorganer i 1991 til 246 i 2008. Det har skjedd en betydelig rolle- og oppgaveendring i forvaltningen siden den gang. Styringssystemene er blitt videreutviklet og trenden viser at underliggende virksomheter har fått større frihet og mer handlingsrom. Bruk av digitalisering har endret måten forvaltningen arbeider på og har ført til relokalisering av statlige arbeidsplasser og nye tjenester.

Omorganisering i forvaltningen kan være et virkningsfullt og synlig tiltak for å nå de forvaltningspolitiske målene til regjeringen. Det kan bidra til å gi bedre ressursstyring, styrke samhandlingen mellom virksomheter og sikre bedre tjenester til befolkningen. Endring i rolle og oppgaver blir i forvaltningen ofte brukt for å sikre bedre måloppnåelse (St.Meld 19, 2008-2009). Rolle- og oppgavefordelingen vil ofte diktere hvordan oppdraget blir løst. Riksrevisjonens gjennomgang fra 2004-2005 viser til at omorganiseringen ikke alltid har hatt den predikerte gevinsten og at kostnaden av omorganiseringen ofte har vært undervurdert (Riksrevisjonen, 2004-2005). Erfaringen i etterkant viser at det kan ta en del år før man høster gevinst av en rolleendring. Skulle omorganiseringen skje på bakgrunn av feil kunnskapsgrunnlag, kan dette føre til en ny omorganisering.

4.3.2.1 En åpen forvaltning

For at staten skal sikre samfunnsutviklingen, bør forvaltningen legge til rette for en demokratisk og folkelig kontroll. Et viktig forvaltningsprinsipp er innsyn og åpenhet slik at offentligheten kan bruke sin demokratiske rett til å påvirke utviklingen i samfunnet samt føre tilsyn med hvordan fellesressursene blir brukt. Gjennom forvaltningen skal regjeringen dele kunnskap og lytte til synspunktene til de som blir berørt av avgjørelsene. Digitaliseringen av offentlig sektor må også legge til rette for at alle kan få innsyn (St.Meld 19, 2008-2009). Arbeidet regjeringen har lagt ned i å utrede samfunnets utfordringer knyttet til digitale sårbarhet er blitt iakttatt av offentligheten. Lysne-utvalgets utredning om digital sårbarhet ledet til nesten 90 høringssvar fra ulike offentlige og private virksomheter. Slike offentlige rapporter og utredninger forteller samfunnet hvilken informasjon som ligger til grunn når regjeringen skal fatte en beslutning.

4.3.2.2 Lett å finne fram

Et prinsipp i forvaltningen er at ansvar og rollefordelingen skal være tydelig, organiseringen skal være slik at det tydelig fremkommer hvem som er ansvarlig for hva og hvilke tjenester man faktisk kan få. Informasjonen skal være lett tilgjengelig og enkel (St.Meld 19, 2008-2009). Dette forvaltningsprinsippet blir utfordret av den uklare rollefordelingen mellom politiet og NSM-NorCERT. Etatene har overlappende

ansvar og oppgaver og det oppleves stor usikkerhet knyttet til om virksomheten får hjelp til å håndtere et digitalt angrep og hva slags hjelp de får. Noe av utfordringen NSM har i sin rolleutøvelse som nasjonalt koordinerende organ for digitale angrep, er at de også er en del av EOS-miljøet, der skjermet og gradert informasjon står sentralt innen kommunikasjon og informasjonsutveksling (POD, 2015).

4.3.2.3 God ressursbruk

Et annet prinsipp er at forvaltningen ikke skal bruke mer ressurser enn nødvendig for å løse sine oppgaver. Ressursene skal fordeles mellom de ulike sektorene og oppgavene i den hensikt å sikre de politiske målene regjeringen har satt. Forvaltningen bør ha en kritisk holdning til hvor ressursene allokeres. En feilaktig ressursfordeling kan føre til at vi ikke benytter potensialet i den offentlige arbeidskraften fullt ut (St.Meld 19, 2008-2009). Ser vi på IKT-beredskapens fire hovedpunkter– forebygging, avdekking, håndtering og etterforsking – finner vi at både NSM og politiet har roller med tilhørende oppgaver knyttet til alle hovedpunktene. Selv om NSMs oppgave er definert til kun å håndtere alvorlig digitale angrep mot samfunnskritisk infrastruktur, ser man tydelige eksempler på dupliserende kapasiteter, da politiets rolle ikke er definert vekk fra alvorlige angrep. Dette kan bryte med god forvaltningsskikk når det gjelder ressursbruk.

4.3.2.4 God styring og organisering

Alle virksomheter i forvaltningen har ansvar for å opptre samordnet og trekke sammen for å løse de store samfunnsutfordringene. Mål- og resultatstyring sammen med andre styringsinstrumenter skal sikre god samhandling. Virksomheten skal ikke sette egne sektormål foran gode fellesløsninger på tvers av sektorer (St.Meld 19, 2008-2009). Sikkerhetsaktørene prøver å etterfølge dette prinsippet og har fokus på samhandling. Som et ledd i å videreutvikle samarbeidet og styrke samhandlingen, etablerte NSM i 2017 Felles Cyber Koordinering Senter (FCKS) der de har forankret tilstedeværelsen av de fire sikkerhetsaktørene: Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet, Etterretningstjenesten og Kripos (Prop. 1 S, (2016–2017)).

4.3.3 Tilsyn, tjenestetilbyder og premissleverandør

Lysne-utvalget sammen med flere andre samfunnsaktører problematiserer tilsynsrollen til NSM, da denne rollen kan komme i konflikt med andre forvaltningsoppgaver. For at jeg senere i oppgaven skal kunne drøfte om dette stemmer, vil jeg se på hva som er god tilsynspraksis. Om det skulle vise seg at NSMs tilsynsrolle kommer i konflikt med andre forvaltningsoppgaver kan det være hensiktsmessig å vurdere om rollendringer kan løse dette.

Det finnes nesten førti statlige aktører som fører tilsyn med offentlige og private virksomheter i Norge. Stortingsmelding 17 fra 2003 forklarer begrepet slik (St.Meld 17, 2002-2003, p. 32):

"Tilsynsbegrepet kan i vid forstand forstås som et fellesbegrep for all aktivitet eller virkemiddelbruk som iverksettes for å følge opp et lovverks intensjoner. Kjernen i tilsynsrollen er imidlertid den konkrete kontrollen av pliktsubjektenes etterlevelse av en norm som allerede er fastsatt ved lov, forskrift eller enkeltvedtak, samt reaksjoner ved avvik."

Fra denne begrepsforklaringen ser vi at hovedintensjonen med å føre tilsyn er å kontrollere at virksomheters aktivitet følger de krav som er gitt i lover og forskrifter samt enkeltvedtak. Tilsynsmyndighetene har mandat til å søke informasjon for å fastslå om tilsynsobjektets aktiviteter avviker fra kravene. Forhåndsvarslet eller uanmeldte besøk med krav om innsyn er et av virkemidlene for dette. Ved funn av avvik kan tilsynsmyndigheten følge opp med en korrigerende reaksjon ovenfor tilsynsobjektet, eksempelvis veiledning, pålegg, stansing av aktivitet eller virksomhet, bøter m.m. i den hensikt å sikre at kravene blir overholdt. Et eksempel på dette kan være NSMs tilsyn med virksomheten i henhold til sikkerhetsloven, hvor de sender inspektører til virksomheten. Inspektørene utfører intervjuer med ledelse og ansatte og sjekker dokumentasjon mot faktiske forhold. Ved funn av avvik vil det bli gitt en forholdsmessig reaksjon som nevnt over. Tilsyn er en viktig samfunnsoppgave, da det avdekker regelbrudd som kan gi en konkurransemessig fordel foran andre virksomheter som ikke bryter reglene, samt at mangel på etterlevelse av regelverket kan utgjøre en risiko for eksempelvis liv og helse (St.Meld 17, 2002-2003).

4.3.3.1 Rollekonflikt i tilsynsforvaltningen

Rolle som generelt begrep kan beskrives som samtlige koblinger mellom en organisasjon eller virksomhet og dets oppgaver, samt utøvelse av roller og oppgaver som samfunnet forventer at virksomheten utfører (Lindøe, et al., 2015, p. 105).

Tilsynsmeldingen trekker fram forhold som utfordrer rolleavklaringen knyttet til selve tilsynsrollen. En av utfordringene er når de ulike tilsynsmyndighetene med tilsvarende formål har kontroll av samme tilsynsobjekt med forskjellig hjemmelsgrunnlag og virkemidler (St.Meld 17, 2002-2003). Eksempelvis vil NSM føre tilsyn etter sikkerhetsloven og objektsikkerhetsforskriften (alle skjermingsverdige objekter er underlagt sikkerhetsloven), mens det direkte tilsynet som kun omfatter den ugraderte ekominfrastrukturen i skjermingsverdige objekter føres av Nasjonal kommunikasjonsmyndighet (Nkom) etter ekomloven (NOU 2015:13, p. 103). Mye av arbeidet og hensikten med tilsyn etter objektsikkerhetsforskriften er effektivt å kunne motvirke trusler mot objektet, og fysisk sikring av ekominfrastrukturen er en del av dette (Sikkerhetsloven §1, 2001). Hovedmålet for begge tilsyn er forebyggende sikkerhet; dette kan føre til berøringspunkter og overlapping mellom tilsynene. Selv om det finnes eksempler der samarbeidsavtaler sikrer god saksbehandling, kan rollefordelingen oppfattes som uklar av tilsynsobjektene (St.Meld 17, 2002-2003, p. 9).

I stortingsmeldingen står det at regjeringen vurderer forvaltningstradisjonen i Norge til å være noe preget av uønskede rollekonflikter innen samme forvaltningsorgan. Det finnes mange tilsynsorganer som har flere roller. Blandingen av roller som tilsynsmyndighet, tjenesteprodusent og direktorat kan forekomme. Potensielt kan da den ene rollen påvirke utførelsen og utfallet av den andre. Samtidig kan det oppfattes som uryddig om et tilsyn også er tjenesteleverandør for en virksomhet den skal utføre kontrolloppgave på. Når samme organisasjon har motstridende formål kan dette svekke tilliten til at organet klarer å skille mellom de ulike rollene. En slik rollekonflikt kan også føre til at selve tilsynsrollen blir svekket. For å sikre tilliten til tilsynsmyndigheten bør det være klare skiller mellom tilsynsroller og andre forvaltningsroller. Meldingen påpeker at den mest åpenbare rollekonflikten er når tilsynsorganet står for kommersielle tjenester til tilsynsobjektet, ett eksempel på dette er VDI-samarbeidet NSM har med virksomheter. Denne rollekombinasjonen er utsatt

for å skape en uheldig kobling mellom funn avdekket av tilsyn og tjenestekjøp. Virksomheten underlagt tilsyn vil kunne oppleve at en straffereaksjon utløst av tilsynet vil påtvinge løsninger produsert av tilsynsmyndigheten (St.Meld 17, 2002-2003).

I Norge har vi hatt tradisjon for å prøve å unngå tette koplinger mellom forvaltningsoppgaver som myndighetsutøvelse og samfunnsstyring på den ene siden og næring og tjenesteyting på den andre. Myndighetsutøvelse og samfunnsstyring kan deles inn i seks oppgaver (Lindøe, et al., 2015, p. 106). NSM innehar alle disse rollene utenom "Forvaltning av tilskuddsordninger":

1. Utredning og analysearbeid
2. Forarbeid til overordnet lovgivning
3. Utforming av generelle forskrifter og normer
4. Kontroll med etterlevelse og vedtak i enkeltsaker, herunder vedtak i klagesaker
5. Veiledning og rådgivning i tilknytning til regeletterlevelse
6. Forvaltning av tilskuddsordninger

Rollekonflikter kan også oppstå når forvaltningsorganet går for langt i sin rolle med å gi faglig råd og veiledning, samtidig som de skal ivareta håndhevingsrollen. Det kan da virke uklart for virksomheten om det settes krav eller om det gis råd. Dette vil være spesielt utfordrende for tilsynsmyndigheten, fordi de har ansvaret for å velge gode løsninger som ivaretar reguleringsformålene. Eksempelvis vil da et faglig råd om en brukerbetalt løsning fra tilsynsmyndighetene kunne oppleves som et pålegg fra virksomhetens side. Samtidig er det viktig å ta hensyn til de positive sidene ved å ha flere roller under ett organ når det gjøres en vurdering av rolle og funksjonsinndeling til forvaltningen. Ved å samle flere funksjoner og roller vil dette styrke evnen til å opptre samordnet ovenfor målgruppen, samt at det kan bidra til å styrke sektor- og bransjemiljø (Lindøe, et al., 2015, p. 107).

5 Metode

Avhandlingen skal avdekke hvordan vi som nasjon beskytter oss mot hele spekteret av dataangrep mot selve datasystemene og hvordan man kan endre den nasjonale evnen til å utføre dette gjennom en rolleendring mellom NSM og politiet. Digitaliseringen i samfunnet har skjedd raskere enn forvaltningen har klart å omstille seg. Dette belyser Lysne-utvalget (NOU 2015:13) i sin utredning sammen med en rekke høringssvar og andre offentlige dokumenter. Samfunnssikkerheten innen datasikkerhet er i dag ikke organisert optimalt for å løse de utfordringene vi står overfor, og det er uenighet mellom ulike samfunnsaktører om hvordan ansvar og roller bør fordeles. Regjeringen tar tak i deler av problemstillingen ved å etablere et nytt cyber crime senter (NC3) i Kripos med ambisjon om 200 stillinger innen 2022 (Trædal, 2018), samt et nytt nasjonalt cyber sikkerhetssenter som en del av NSM i løpet av høsten 2018 (NSM, 2018). I lys av dette anses temaet som svært aktuelt både for arbeidet med organiseringen av samfunnssikkerheten innen IKT-sikkerhet og samfunnet for øvrig.

5.1 Datainnsamling

Data til oppgaven ble i hovedsak samlet inn gjennom offentlige dokumenter innen datasikkerhet, samt intervjuer. I tillegg ble det benyttet høringssvar og rapporter fra viktige samfunnsaktører for å illustrere ulike syn på rollefordelingen mellom sikkerhetsaktørene. Dokumentene utreder og mener noe om de største utfordringene knyttet til IKT-sikkerhet nasjonalt. Jeg har plukket ut det som er mest relevant knyttet til problemstillingen i oppgaven. Data fra dokumentene er sammenlignet med informasjonen fra intervjuobjektene.

Jeg har fått muligheten til å intervjue to betydelige nasjonale aktører innen IKT-sikkerhet. Den ene sjef for NorCERT, Håkon Bergsjø, og den andre er Kripos' representant for FCKS samarbeidet, Øystein Andreassen. Dette er to sentrale aktører direkte koblet opp mot nasjonal sikkerhet knyttet til dataangrep. Dette sikrer dataenes validitet. Jeg har nådd ut til flere aktører og har intervjuet to andre personer med tyngde innen nasjonal IKT-sikkerhet; dette er aktører som av ulike grunner

ønsker å være anonyme. De ville heller ikke at det skal opplyses om hvilken virksomhet de jobber i. Informasjon fra de anonyme intervjuene gir kun merverdi i form av kontekst, denne informasjonen vil ikke bli brukt direkte som empiri inn i oppgaven.

Det teoretiske referansematerialet for oppgaven består av litteratur om samfunnssikkerhet og risikoanalyse, samt offentlige dokumenter som beskriver best praksis innen forvaltningsprinsipper. Det teoretiske bakgrunnstoffet er ment å gi en grunnleggende forståelse rundt risiko og organiseringen av samfunnssikkerhet innen offentlig forvaltning i en IKT-beredskapskontekst. Dette legger grunnlaget for å drøfte om en rolleendring er hensiktsmessig både fra et operasjonelt og et forvaltningsmessig perspektiv.

5.2 Forskningsetikk

Kvalitativ forskning bør utarbeides ut fra tre etiske retningslinjer; informert samtykke, konfidensialitet og konsekvenser (Kvale & Brinkmann, 2015). Før intervjuet ble informantene informert om problemstillingen i oppgaven, samt bakgrunnen for valg av denne. Informantene har betydelige kunnskaper, men mye av denne kunnskapen er gradert informasjon grunnet nasjonal sikkerhet. Det er ikke alltid lett for en informant som har denne type informasjon å vurdere verdien av den informasjon de gir fra seg der og da. Av den grunn valgte jeg å gi informantene rett til å eie den informasjonen de hadde delt med meg, fram til innlevering av oppgaven, dvs. at de når som helst kunne legge til, trekke fra eller trekke seg fra intervjuet i sin helhet. Etter at intervjuet var transkribert, ble det sendt tilbake til informanten til godkjenning. Deretter sendte jeg drøftingen av oppgaven til informantene slik at de kunne kvalitetssikre at informasjonen de ga fra seg ikke var tatt ut av kontekst. Jeg anså at dette var avgjørende for å redusere muligheten for negative konsekvenser, både for intervjuobjektene og for den nasjonale sikkerheten. I tillegg vil dette sikre at informasjonen i oppgaven er så korrekt som mulig. Det ble tatt stilling til konfidensialitet der informasjonen fra de to anonyme intervjuene ikke ble tatt med. Grunnlaget for empirien fra denne informasjonen faller vekk, da jeg ikke kan henvise til en kilde. Sjef for NorCERT og Kripos' representant fra FCKS gir informasjon i kraft av sin stilling og kunnskap og skal derfor ikke være anonyme.

5.3 Gjennomføring av intervjuet

Intervjuet var semistrukturert både med spørsmål og temaer jeg ønsket en dialog rundt. Alle informantene ble gitt en egen intervjuguide ca. en uke i forveien. Dette ga informantene et bedre utgangspunkt til å forberede seg, slik at den informasjon de ga ble så korrekt som mulig. Før intervjuet startet, fikk de sine rettigheter lest opp. Det ble også foretatt begrepsavklaringer underveis i intervjuet når det var behov for det. Intervjuene av sjef for NorCERT og Kripos-representanten ble gjennomført hos den aktuelle virksomheten og intervjuene varte ca. to timer. Det ble ikke benyttet båndopptaker, da ingen av informantene ønsket dette. Transkriberingen ble foretatt fra notater under intervjuet.

Forskningsmetoden som ble benyttet er basert på forskningsmetodikk beskrevet av Berth Danermark, et al., (1997) (Danermark, et al., 1997). Valg av forskningsmetode var abduktiv, og jeg brukte teori og informasjon fra offentlige dokumenter som utgangspunkt. Teori om samfunnssikkerhet, sikringsrisiko og organisering av samfunnssikkerhet lå hele tiden som et rammeverk for innhenting av data fra dokumenter og intervjuer. Ved utarbeidelse av intervjuguide ble informasjon fra dokumentanalysen brukt som datagrunnlag, slik at intervjuet kunne avdekke de faktiske forhold som beskrevet i dokumentene. Ved å sammenligne denne informasjonen og sette den inn i et teoretisk rammeverk, kan jeg drøfte om en rolleendring vil kunne endre den nasjonale evnen til å håndtere dataangrep. Det må tas forbehold om kvaliteten på alle data som er samlet inn i denne oppgaven, da de er behandlet ut fra min subjektive forståelse og fortolkning (Blaikie, 2009).

5.4 Kunnskapshull

Jeg har forgjeves forsøkt å få sentrale aktører i virksomheter som samarbeider med NSM til å hjelpe meg med å få frem gode synsvinkler på min problemstilling. Spørsmålet om rolleendring mellom aktørene oppleves åpenbart som betent, og mange ønsker ikke å stå frem offentlig med sine syn. Bidrag fra disse personene kunne ha gitt flere og sikkert andre perspektiver på den problemstilling jeg ønsker å analysere.

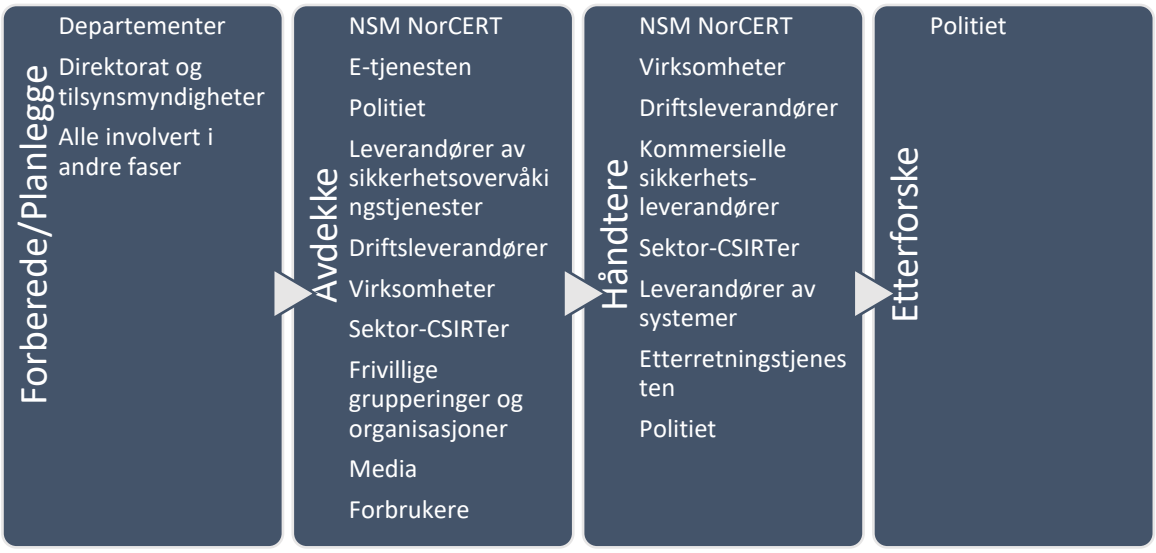
6 Empiri og analyse

Det er i utgangspunktet to overordnede rolleendringer jeg vil drøfte. Den ene er hvem som skal ha den nasjonale CERT-funksjonen og den andre er hvem som skal ha VDI-samarbeidet sammen med alle forvaltningsoppgavene som naturlig hører til disse to oppgavene. Analysen vil gjennom teoridelen, dokumentanalysen og intervjuene se på om det er hensiktsmessig med slik rolleendring. Problemstillingen blir drøftet systematisk gjennom de teoretiske perspektivene for samfunnssikkerhet og reguleringsregime sett i forhold til funn fra empirien. Empirien jeg har funnet om sikringsrisiko er skrevet inn der det er naturlig i forhold til de to andre perspektivene. Empirien er hentet fra analyser i offentlige rapporter og utredninger og intervjuer med sjef for NorCERT og Kripos' representant i FCKS.

6.1 Samfunnssikkerhet

I teoridelen om samfunnssikkerhet ble det presentert en IKT-beredskapskjede. Oppgaven vil bruke denne inndelingen av beredskapsfaser, da den skjelner godt mellom de ulike rollene til sikkerhetsaktørene og gjør det enklere å strukturere hvor berøringspunktene mellom politi og NSM ligger.

Modellen under er hentet fra rapporten og viser operative aktører involvert i arbeidet med digitale angrep (Mnemonic, 2015, p. 8).



Figur 7: Operative aktører involvert i arbeidet med digitale angrep

Mnemonic viser i denne figuren at det er overlappende myndighetsoppgaver innenfor de fire fasene i beredskapskjeden. Både NorCERT og politiet deler oppgaver innen forberedelse, avdekking og håndtering.

I dette kapittelet vil jeg bruke teorien sammen med empiri for å drøfte hvor berøringspunktene mellom politiet og NSM ligger i IKT-beredskapskjeden og hvordan en rolleendring potensielt kan bedre den nasjonale evnen til å bekjempe dataangrep.

6.1.1 Forebygge

"Det er nok forebygging til alle" (Sitat, Håkon Bergsjø, NorCert-sjef)

6.1.1.1 Mandat gitt i loven

Både NSM og politiet er gjennom loven pålagt å forebygge IKT-kriminalitet. Her vil jeg belyse berøringspunkter mellom NSM og politiet og drøfte om det kan være formålstjenlig for den nasjonale sikkerhet å bytte roller.

I sikkerhetsloven § 1 står det at formålet med loven er å *"motvirke trusler mot **rikets selvstendighet og sikkerhet** og andre vitale nasjonale sikkerhetsinteresser".* Sikkerhetsloven § 9 beskriver oppgavene NSM skal utføre i det forebyggende arbeidet som: *"innhente og vurdere informasjon av betydning for gjennomføringen av **forebyggende** sikkerhetstjeneste"* og tydeliggjør denne oppgaven gjennom å *"bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for **forebyggende** sikkerhetstjeneste".* Forarbeidet til sikkerhetsloven er beskrevet i Ot.prp.nr. 49 (Ot.prp.nr.49 (1996-1997)). Ot.prp. nr.49 beskriver arbeidet med forebygging som sikkerhetstiltak som skal være planlagt og implementert før et angrep finner sted. NSMs metodikk for å drive forebyggende arbeid er gjennom kontinuerlig arbeid med risikoanalyse, der sårbarheten vurderes opp mot trusselen. Behovet for sikkerhetstiltak vil være styrt av en løpende vurdering av verdi, trussel og sårbarhet. NSMs formål er rettet mot alvorlig angrep knyttet til spionasje, sabotasje og terrorhandlinger som kan ramme Norge eller allierte, og vil derfor ha fokus på

samfunnskritiske funksjoner og virksomheter som er underlagt sikkerhetsloven i sitt forebyggende arbeid (Ot.prp.nr.49 (1996-1997)).

Offentligheten har stilt spørsmål om politiets rolle ved datakriminalitet, da dette ikke har fremstått som en tydelig prioritert oppgave for politiet. Det kan skyldes at den teknologiske utviklingen har gått raskt frem og kapasiteten og fokuset i politiet har hengt etter utviklingen. Gjennom offentlige utredninger og rapporter kommer det tydelig fram at politiets oppgaver skal ikke diskriminerer mellom det fysiske og det digitale rom (POD, 2015) (NOU 2015:13) (NOU 2017:11). Politiet er lovpålagt å forebygge IKT-kriminalitet gjennom politiloven § 2: *"**forebygge** kriminalitet og andre krenkelser av den offentlige orden og sikkerhet"*. Forarbeidet til politiloven er beskrevet i Ot.prp. nr.22 (Ot.prp.nr.22 (1994-1995)). Proposisjonen (Ot.prp.nr.22 (1994-1995)) legger vekt på at *"offentlig sikkerhet"* handler om å verne om **rikets selvstendighet og sikkerhet**.

Både NSM og politiets arbeid med forebygging er pålagt gjennom lov. I forarbeidet til sikkerhetsloven (Ot.prp.nr.49 (1996-1997), 1997) og politiloven (Ot.prp.nr.22 (1994-1995), 1995) legger begge proposisjonene ***rikets sikkerhet*** til grunn for sikkerhetsaktørenes arbeid med forebygging. Man kan derfor si at oppgaven er definert likedan, selv om den er hjemlet i ulike lover om forebygging. Begrepet *rikets sikkerhet* er en rettslig standard og kan forandre seg med samfunnsutviklingen. I sikkerhetsloven brukes begrepet om indre og ytre sikkerhet (Ot.prp.nr.49 (1996-1997)) og straffelovkommisjonen (NOU 2003:18, 2003) skriver at innholdet i begrepet ikke er helt avklart, men at betydningen er knyttet til kontekst. Dette gir et handlingsrom til å utføre oppgaven på forskjellige måter med hensyn til samfunnsrollene.

6.1.1.2 Dokumentanalyse

Datakrimstrategien (POD, 2015, p. 16) legger vekt på at politiets virkemiddel å forebygge betinger at de har stor tilstedeværelse og kan patruljere på internett. Strategien innebærer også at straffeforfølgning vil være forebyggende. Begge sikkerhetsaktørene har i oppdrag å forebygge med tanke på rikets sikkerhet, men velger å løse oppdraget på forskjellige måter. Politiet løser oppgaven gjennom en

tilstedeværelse på internett som sprer bevissthet til befolkningen om risikoen for å bli straffeforfulgt i det digitale domenet. Dette alene dekker ikke bredden i arbeide med forebygging. På dette grunnlag kan man si at politiets innsats ikke gjenspeiler den rollen de er gitt etter politiloven, som pålegger dem å verne om rikets sikkerhet. NorCERTs oppgave med forebygging er mer knyttet til å danne seg et risikobilde, og samle informasjon om hvilke verdier som er sårbare og hvilke trusselaktører som potensielt kan angripe. NSM bruker denne informasjonen til å utvikle eller gi råd om endring av sikkerhetstiltak gjennom bindende og ikke-bindene rettslige reguleringer.

NSMs risikoanalyse vil også være knyttet til viktige samfunnsfunksjoner og trusselaktører med større skadepotensial. Politiets arbeid med forebygging pålegges av loven og dekker alle alvorlige og ikke-alvorlige trusler, mens det i praksis synes å være mer rettet mot individer og offentlige/private virksomheter. Politiet har i dag ikke stor nok kompetanse eller kapasitet til å drive med forebygging, selv om problemet med IKT-kriminalitet er økende. Kripos hadde i 2015 kapasitet til kun to til fem saker. Kapasitetsmangel er grunnen til at de ikke prioriterer forebyggende arbeid (POD, 2015).

Politiets oppgave med forebyggende arbeid i cyberdomenet er viktig, da det øker oppdagelsesevnen samt styrker evnen til å forfølge straffbare handlinger og etterforske. Det forebyggende arbeidet som politiet utfører i cyberdomenet er et virkemiddel for å redusere IKT-kriminaliteten (NOU 2017:11). Kapasiteten til å avdekke denne kriminaliteten styrer noe av evnen til å forebygge dataangrep.

6.1.1.3 Intervjuer

Hovedtyngden av sårbarhetsreduserende tiltak blir utført av NSM. I følge sjef for NorCERT er de Norges ekspertmiljø for forebygging innen IKT-sikkerhet. De samler inn mye informasjon om sårbarheter og leverer råd, veiledning og informasjon om tekniske løsninger til offentlige og private virksomheter.

Kripos' representant fra FCKS melder om at politiets hovedoppgave og innsats bør ligge på forebygging, da dette er en av deres hovedoppgaver. Kripos bør ha som mål å gi råd om hvordan man kan redusere sårbarheter, gi veiledning og informasjon til

virksomheter, dvs. mye av den oppgaven NSM har i dag innen forebygging. Det er lett å kritisere dette standpunktet, fordi det vil føre til dupliserende oppgaver, men politiet gjør dette allerede i det fysiske domenet eksempelvis med forsikringsselskaper osv. Det at to virksomhetet driver med forebygging kan gi en styrket total effekt, fordi den kan nå bredere ut og virke mer samkjørt når to sikkerhetsaktører gjør det samme. Kripos' representant legger også til at den rollen politiet har i dag innen forebygging ikke er adekvat, da den i hovedsak går ut på å patruljere internettet gjennom tilstedeværelse på sosiale medier og forumer samt i chatterom. Der politiet oppdager ytringer i chatterom som blir for ekstreme, kan de markere seg i chatterommet. Dette kan sammenlignes med å dempe ordensforstyrrelser på en fredag kveld i Oslo by.

6.1.1.4 Sårbarhetsreduksjon

De tre faktorene verdi, trussel og sårbarhet er godt forankret både innen samfunnssikkerhet og risiko. Det er i hovedsak disse tre faktorene som påvirker samfunnssikkerheten (Meld. St. 10, 2016-2017). NS 583X-serien beskriver sikringsrisiko gjennom disse faktorene. Summen av verdi, trussel og sårbarhet utgjør den totale risikoen, og målet er å redusere denne risikoen gjennom å redusere truslene og sårbarheten.

Å redusere sårbarheten er en stor del av forebyggingen. NS 5830 utrykker sårbarhet som *manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønskede påvirkninger*. Sårbarheter er ofte et resultat av utilstrekkelig eller feil sikring av verdier, og en kartlegging av sårbarhet har til hensikt å belyse et gap mellom allerede innførte sikringstiltak og trusselaktørens intensjon og kapasitet til å ramme verdien (NSM, 2016, p. 19).

6.1.1.5 Oppsummering

NSM er et nasjonalt kompetansesenter for IKT-sikkerhet og har den nasjonale CERT-funksjonen samt VDI-samarbeidet. Det vil være naturlig at den som har den nasjonale CERT-funksjonen har de forebyggende rollene som NSM har i dag, som er listet opp i tabell 1 med forbehold om hvorvidt tilsyn skal med eller ikke. Begge

aktørene har denne rollen i dag, men de utøver den på forskjellige måter. Mye av kartleggingen blir gjort gjennom tilsyn og penetrasjonstesting; det vil derfor være naturlig at den som har disse to oppgavene også har en større rolle innen forebygging. Ut fra dette perspektivet kan man si at det vil ikke være formålstjenlig å flytte denne rollen fra NSM over til politiet. Spørsmålet da er om politiet skal bygge opp en kapasitet rundt forebygging med flere oppgaver innen rådgivning, veiledning og informasjonsspredning, fordi det er noen av hovedfunksjonene til politiet. Ifølge Kripos' representant for FCKS, kan det også styrke det totale forebyggende arbeidet om begge aktørene driver med forebygging, da det kan gi et større nedslagsfelt.

Det er et viktig forvaltningsprinsipp at man samler flest mulig beslektede oppgaver under én etat, da dette gjør det enklere for offentligheten å finne frem, i tillegg til at det kan bli enklere å samkjøre ressursene og drive god styring og organisering (St.Meld 19, 2008-2009). Men det kan stride mot god forvaltningsskikk hvis en påtalemyndighet skulle treffe tiltak som skal fremme best praksis og veiledning innen ikke-rettslige bestemmelser, da dette kan oppfattes som pålegg mer enn som veiledning og oppfordring. Allikevel kan man ikke utelukke et større potensiale hvis politiet bygger opp en større rolle innen forebygging, så lenge dette ikke strider mot god forvaltningsskikk og oppgavene er samkjørt med NSM. Offentligheten er vant til at politiet har denne rollen i det fysiske rom, og det vil også bedre reflektere den oppgaven de er satt til å gjøre gjennom politiloven. Ut fra dette perspektivet kan man argumentere med at den nasjonale evne til å bekjempe IKT-kriminalitet vil styrkes hvis politiet tar på seg flere oppgaver innen forebygging.

Verktøy og oppgaver i det forebyggende arbeidet:

NSM	**Politiet**
Informasjon fra EOS-miljø	Informasjon fra tilsvarende organ i utlandet
Informasjon fra VDI	Har ikke denne rollen
Utgir veiledninger og rapporter	Har ikke denne rollen
Utfører tilsyn og penetrasjonstesting	Har ikke denne rollen
Innspill til forebyggende tiltak	Har ikke denne rollen
Har ikke denne rollen	Tilstedeværelse på internett
Informasjon fra andre private og offentlige virksomheter	Informasjon fra andre private og offentlige virksomheter

Tabell 3: Forebyggende Roller

6.1.2 Avdekke

6.1.2.1 Mandat gitt ved lov

NSMs pålagte oppgave med å drive avdekking er hjemlet i sikkerhetsloven § 9 e) *"drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur og* ***et nasjonalt varslingssystem for digital infrastruktur"***. Dette gir NSM rollen som forvalter av VDI-løsningen. Dette tilfører NSM et godt datagrunnlag til å drive god risikostyring, der de blant annet avdekker hvilke verdier som blir rammet. Politiet er også lovpålagt å avdekke kriminell virksomhet, ifølge politiloven § 2: ***"avdekke*** *og stanse kriminell virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov".* De pålagte rollene hjemlet i lov overlapper hverandre.

6.1.2.2 Dokumentanalyse

NSMs kapasitet til å avdekke alvorlige angrep overgår politiets, da de får mye informasjon fra andre EOS-miljøer samt fra VDI-samarbeidet. Politiet har et godt internasjonalt samarbeid med sikkerhetsaktører og tilsvarende etater i utlandet, men mangler et sensornettverk som VDI for effektivt å avdekke trusler og sårbarhet nasjonalt. Politiets evne til å avdekke er i dag sterkt knyttet til antall anmeldelser. Her

er det store mørketall, da antall anmeldelser ikke reflekteres i antall angrep. NSM melder om ca. 22 000 angrep i 2016 der 87 av dem resulterte i straffeforfølgelse (NSM, 2018) (SSB, 2017). Datakrimstrategien innebærer at virksomhetenes manglende vilje til å anmelde IKT-kriminalitet er et problem. Frykten for straffeforfølgning skyldes ofte uheldig eksponering av virksomheten samt ressursbruken i en slik prosess, som eksempelvis fremskaffelse av bevis og at man må stille til avhør og vitne (POD, 2015).

VDI-samarbeidet mellom NSM og virksomhetene legger en begrensning på bruk av informasjonen fra sensornettverket. Informasjonen kan kun benyttes til håndtering av alvorlige angrep og kan ikke deles med aktører utenfor FCKS. NSM utrykte en bekymring til Lysne-utvalget om at informasjonsdeling med politiet kan undergrave VDI-samarbeidet med virksomhetene, da dette bryter med avtalen de har om ikke å dele data med tredjepart (NOU 2015:13, p. 262).

I NSMs høringssvar til sårbarhetsutvalget skriver de at den norske modellen der NSM samarbeider med virksomheter gjennom VDI, virker attraktiv for samarbeidspartnere utenfor Norge, der man har fått til et godt samarbeid mellom de hemmelige tjenestene og virksomheter med samfunnskritiske funksjoner. Videre skriver de at denne tilliten sannsynligvis ikke vil la seg videreføre om VDI-løsningen blir overført til politiet (NSM, 2016). Mye av dette skyldes at ordningen er bygd på frivillighet og styrkes ved at virksomheten eier informasjonen. Terskelen for å dele informasjon med NSM er lavere enn med politiet, fordi det ikke trenger å resultere i en anmeldelse.

Strategigruppen (POD, 2015) eksemplifiserer en ordning FBI har i California med virksomheter hvor det ikke ville bli igangsatt straffeforfølgning uten med tillatelse fra virksomheten. Dette resulterte i godt samarbeid og en god informasjonsflyt fra virksomhetene som ga verdi i det forebyggende arbeidet. Politiet i Norge kan også dra nytte av en slik ordning, som vil være et godt virkemiddel for å bedre oversikten over datakriminaliteten som rammer Norge. Utfordringen er at en slik garantiordning betyr avvik fra påtalereglene med tanke på hvordan annen kriminalitet behandles påtalemessig.

En annen utfordring er begrepet "datakriminalitet". Det er diffust og kan brukes bredt. En garantiordning vil kunne omfatte andre saker som kun indirekte har med datakriminalitet å gjøre. En slik avtale må være klar på hva som faller inn under påtaleunnlatelse. Det kan også være tilfeller der det ligger en større samfunnsmessig interesse i å straffeforfølge hackere, særlig når den siktede er i varetekt og under etterforskning. Det vil være uheldig om henleggelse av en sak etter avtale med virksomheten fører til erstatning for siktede. Det er også utfordring at flere virksomheter kan være rammet av det samme dataangrepet, men har motstridende interesser (POD, 2015, p. 140). Det er formålstjenlig med flere anmeldelser av dataangrep, men kost-nytteeffekten av noen saker som ikke kan straffeforfølges kan av og til være negativ, eksempelvis når en statlig aktør står bak (Mnemonic, 2015).

Datakrimstrategien (POD, 2015) legger også vekt på at en fornuftig praktisering av opportunitetsprinsippet vil løse mange av de ovennevnte utfordringene. Straffeprosessloven § 62a lyder:

"Den offentlige påtalemyndighet skal påtale straffbare handlinger når ikke annet er bestemt ved lov. For overtredelse av straffebud med en ***strafferamme på 2 år eller lavere*** kan påtale unnlates hvis ikke allmenne hensyn tilsier påtale. ***Ved vurderingen av om allmenne hensyn foreligger, legges det blant annet vekt på*** overtredelsens grovhet, hensynet til den alminnelig lovlydighet og om ***den fornærmede, en annen som har lidt skade ved overtredelsen***, eller vedkommende berørte myndighet ***ønsker påtale***."

Datakriminalitet omtalt i straffeloven fra 2005, har for det meste strafferammer på under to år. Strategigruppen legger til at selv om straffesaker har en strafferamme på over to år, har påtalemyndigheten fortsatt et betydelig handlingsrom for å utvise skjønn. De legger også til at et alternativ er å innføre en egen påtale- eller saksbehandlingsregel for å styrke handlingsrommet for en eventuell ordning (POD, 2015).

Politiets utilstrekkelige evne til å avdekke dataangrep er et problem. Datakrimstrategien trekker fram at informasjonen fra VDI kan bli veldig begrenset for bruk av politiet, da den ikke deles med politiet og at politiet kunne dratt nytte av å ha

denne rollen eller et tilsvarende samarbeid med virksomhetene. "*Resultater fra VDI-systemet er et viktig informasjonsunderlag for IKT-risikobildet som NSM har et ansvar for å vedlikeholde. Indirekte vil informasjon som fremskaffes fra systemet kunne underbygge politiets vurderinger av den trusselen som datakriminalitet representerer.*" (POD, 2015, p. 78)

Fra sitatet over kan det virke som politiet ville dra nytte av informasjonen fra VDI-samarbeidet. Virksomhetene har i dag ingen reell avtale om påtaleunnlatelse, men unngår dette gjennom å ikke dele informasjon med politiet (POD, 2015).

6.1.2.3 Intervjuer

Ifølge sjef for NorCERT er den viktigste kilden til informasjon knyttet til avdekking, VDI og informasjon fra EOS-miljøet. VDI-samarbeidet er basert på at virksomhetene eier informasjonen og NorCERT kan dele informasjonen med E-tjenesten og PST; dette er kontraktsfestet med virksomheten. NorCERT vil ikke gå til politiet eller andre enn EOS-miljøet med informasjonen fra VDI, og virksomheten står fritt til å velge å anmelde angrepet til politiet. Kripos er en del av FCKS, og NorCERT har sendt ut en tilleggsavtale til de samarbeidende virksomhetene der de står fritt til å skrive under på om informasjonen også kan deles med Kripos. VDI er formålsbegrenset til å detektere alvorlige angrep og er ikke satt opp til å fange opp mindre alvorlige angrep. De angrepene NorCERT detekterer gjennom VDI-systemene er som regel alvorlige angrep knyttet til spionasje og sabotasje fra ressurssterke aktører som det mest sannsynlig ikke er mulig å ta ut påtale på. Denne type angrep er det NSM eller PST som håndterer og informasjonen fra slike angrep blir fort gradert.

Informasjon fra EOS-miljøet vil som regel dreie seg om alvorlige angrep knyttet til statlige trusselaktører. NorCERT får ofte informasjon fra andre EOS-miljøer nasjonalt og internasjonalt om signaturer de kan legge inn i VDI i den hensikt å detektere spesifikke cyberopperasjoner. Politiet har ikke de kanalene til utenlandske EOS-miljøer og har heller ingen klarering til å motta den type informasjon, som er gradert. Det er et viktig aspekt at informasjonen fra VDI er formålsbegrenset. Hvis politiet hadde hatt denne rollen, kunne de finne annen informasjon som kan være inkriminerende for virksomheten. Det er et viktig aspekt ved at NorCERT har denne

rollen at virksomhetene ikke frykter for å bli tatt for småkriminalitet. NorCERT har brukt mange år på å opparbeide seg denne tilliten.

Ifølge Kripos' representant i FCKS er det kun de mest alvorlige sakene som blir løftet opp til FCKS, og denne informasjonen faller ofte ikke under politiets mandat og er derfor heller ikke relevant for politiet. Et av hovedproblemene til politiet er mangel på deteksjonsevne. Det politiet avdekker kommer i hovedsak fra anmeldelser eller rapporteringer fra virksomheter eller privatpersoner. Det understrekes i intervjuet at Kripos kan dra nytte av informasjonene fra VDI-samarbeidet. VDI-samarbeidet er ikke bare knyttet til informasjonen som blir avdekket gjennom sensoren, men også informasjon virksomhetene deler med NorCERT. Selv om ikke all informasjonen fra VDI-sensoren berører politiet, vil det foreligge en del overskuddsinformasjon som Kripos vil kunne dratt nytte av, uavhengig av om angrepet er alvorlig eller ikke.

Kripos trenger ikke nødvendigvis å kjenne til hvilken virksomhet som blir rammet, men Kripos kan dra nytte av informasjon knyttet til generelle sårbarheter og systemer som blir forsøkt angrepet, modus, trender, konsekvenser osv. Denne informasjonen kan Kripos kryssjekke med annen informasjon for å danne seg et bedre situasjonsbilde. Her ligger det et urørt potensiale i å ha en bedre informasjonsflyt der Kripos får overskuddsinformasjon fra VDI-samarbeidet NorCERT har med virksomheten. En annen utfordring med avdekking er at virksomhetene har et aktivt og bevisst forhold til ikke å anmelde digital kriminalitet.

6.1.2.4 Oppsummering

Det er antatt at virksomheter ofte ikke ønsker å anmelde ulovlige forhold knyttet til dataangrep, da dette kan resultere i omdømmetap og binde opp virksomhetens ressurser ved å hjelpe politiet med å etterforske og ta ut påtale. En utfordring for politiet er virksomhetens behov for å stanse etterforskningen hvis den slår ufordelaktig ut for virksomheten. Dette kan være en medvirkende årsak til at det blir få anmeldelser.

I tillegg har politiet handlingsrom til å gi forbud, pålegg og gjennomføre tvangstiltak. Dette er også faktorer som kan bidra til å heve terskelen for å dele informasjon med politiet.

Ifølge informasjon fra sjef for NorCERT vil en løsning der politiet tar over driften av VDI, i tillegg til samarbeidet de har i dag med virksomhetene, ikke føre til større innsikt i IKT-kriminalitet. VDI er formålsbegrenset til å kun fange opp alvorlige trusler knyttet til spionasje og sabotasje. Den fanger ikke opp vanlig digital kriminalitet. Hvis politiet tar over VDI-løsningen slik den er konfigurert i dag, ville det ikke resultere i flere anmeldelser. Ved avdekking av et alvorlig angrep der politiet har den koordinerende rollen, måtte politiet mest sannsynlig ha gitt de fleste sakene avdekket av VDI over til NorCERT eller PST. Dette kan føre til at håndteringen blir stykkevis og delt. Mye av signaturene som blir lagt inn i VDI for å avdekke angrepene kommer fra EOS-miljøene; informasjon om slike signaturer vil ofte være gradert og utilgjengelig for politiet. Dette er også en av hovedgrunnene til at en i EOS-miljøet bør ha rollen som forvalter av VDI og sitte med samarbeidet med virksomhetene. Det sistnevnte støttes av Kripos' representant i FCKS.

Samarbeidet mellom NorCERT og virksomhetene fungerer godt, og tilliten er bygd opp gjennom lang tid. Det er også en risiko for at samarbeidet delvis vil brytes ned hvis politiet tar over VDI-løsningen eller har fri tilgang til informasjonen. En rolleendring her forutsetter at politiet tar over samarbeidet NSM har bygd opp med de ulike virksomhetene og at virksomheten godtar et nytt samarbeid med politiet.

Det er lett å tenke at politiet er tjent med et sensornettverk som avdekker signaturene til vanlig IKT-kriminalitet. En av de mange utfordringene med dette er at denne tjenesten allerede finnes i det private markedet, og det ville vært uheldig om politiet skulle konkurrere med private virksomheter. Det er også en av årsakene til at VDI-løsningen til NorCERT kun er formålsbegrenset til å avdekke alvorlige angrep som kan true samfunnskritiske funksjoner og ikke ordinær digital kriminalitet.

Det er derimot et urørt potensiale i å la Kripos få ta del i overskuddsinformasjonen NorCERT får gjennom VDI-samarbeidet. Dette kommer tydelig frem gjennom datakrimstrategien og fra informasjonen fra Kripos' representant. Det er mye som

tyder på det vil styrke den nasjonale evnen til å bekjempe datakriminalitet hvis Kripos har en permanent tilstedeværelse i operasjonssenteret til NorCERT. De vil da kunne plukke ut relevant informasjon fra det som kommer inn av opplysninger og bruke dette i Kripos' eget arbeid. Hvordan dette samarbeidet vil se ut og hvordan det vil påvirke samarbeidet NorCERT har med virksomhetene er uvisst, men skal man styrke nasjonens evne til å bekjempe IKT-kriminalitet vil det være hensiktsmessig å utforske en slik løsning.

Verktøy for å avdekke IKT angrep:

NSM	Politiet
Analyse fra VDI	Har ikke denne rollen
Har ikke denne rollen	Anmeldelser
Informasjon fra EOS-miljø	Informasjon fra tilsvarende organ i utlandet
Har ikke denne rollen	Patruljerer internett
Informasjon fra andre private og offentlige virksomheter	Informasjon fra andre private og offentlige virksomheter

Tabell 4: Oppgaver med å Avdekke

6.1.3 Håndtere

To av utvalgsmedlemmer i Lysne-rapporten (NOU 2015:13, p. 274) mener at politiet bør ha den nasjonale CERT-funksjonen. Både Telenor, Kraft og FinansCERT er enig med mindretallsutvalget til NOU 2015:13 (KraftCERT, 2016) (Telenor, 2017). Den aktøren som har den nasjonale CERT-funksjonen vil få ansvaret for å koordinere håndteringen av dataangrep. I dette kapittelet vil jeg drøfte om nasjonen er tjent med en rollendring for denne oppgaven.

6.1.3.1 Mandat gitt i lov

NSM er pålagt å håndtere dataangrep gjennom sikkerhetsloven § 9 e) ***"drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur*** *og et nasjonalt varslingssystem for digital infrastruktur".* Her er oppdraget til NSM spesifikt rettet mot koordineringen av alvorlige dataangrep mot kritisk infrastruktur.

Politiets pålegg om å håndtere er hjemlet i politiloven § 2 *"yte borgerne hjelp og tjenester i faresituasjoner, i lovbestemte tilfeller og ellers når forholdene tilsier at bistand er påkrevet og naturlig"* og *"avdekke og stanse kriminell virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov".* Begge sikkerhetsaktørene skal håndtere digitale angrep. Rolleutfordringene er knyttet til at politiet har ansvar for både alvorlige og ikke-alvorlige angrep og vil derfor overlappe NSMs rolle som kun er rettet mot alvorlige angrep. Det er begges ansvar å håndtere alvorlige hendelser i det digitale rom rettet mot kritisk infrastruktur.

6.1.3.2 Dokumentanalyse

NorCERT er ansvarlig for å vurdere angrepene når de blir meldt inn av offentlige og private virksomheter eller avdekket av VDI, for så å koordinere håndteringen. Når NorCERT avdekker et IKT-angrep, vil det bli gjort en prioritering i operasjonssenteret deres med støtte fra FCKS. NorCERT vil fordele ansvar der det er behov for det (POD, 2015). Sakene blir prioritert etter de potensielle konsekvensene de kan gi. NorCERT har ikke håndtering som hovedoppgave, men kan bistå etter behov. Ifølge NorCert-sjef er det PST som velger hvilke saker de selv skal ta og hvilke saker NorCERT skal ta eller bistå i. Hvis angrepet ikke er alvorlig nok til å utløse håndtering, må politiet fortsatt vurdere om saken skal forfølges. I de tilfeller der det digitale angrepet gir en fysisk alvorlig konsekvens, vil det være naturlig at PST eller politiet står for koordineringen (POD, 2015). Det kan i starten være uklart hvem som skal ta saken, da dette ofte avgjøres basert på trusselaktører, eksempelvis om det gjelder statlig eller ikke-statlig industrispionasje.

Politiet har pr. dags dato ikke etablert noen god praksis med å rykke ut på slike hendelser, men Kripos hevder selv det er uheldig hvis de kommer for sent inn i saken da dette kan forsinke etterforskningen. Eksempelvis kan innsamling av bevis måtte gjøres på nytt, og bevis kan ødelegges eller går tapt dersom politiet kommer for sent inn i hendelsen (Mnemonic, 2015). Datakrimstrategien sier at idet et angrep oppstår, er det usikkerhet rundt omfanget av angrepet og hvem som står bak. Ved starten av angrepet er det viktig at alle aktørene raskt lokaliserer ansvaret og blir enige om rollefordelingen, slik at arbeidet med håndteringen kan begynne umiddelbart. Når det ikke er klart hvem som skal ta saken og det tar lang tid å komme i gang med

etterforskningen, kan dette føre til henleggelse (POD, 2015). Her påpekes det at samvirket må være så innarbeidet og sømløst at den ene aktøren ikke venter på at den andre myndigheten initierer arbeidet (POD, 2015).

Lysne-utvalget skriver at ansvarsdeling i en beredskapskontekst vanligvis bygger på forutsetningen om at man kjenner til hvem eller hva som står bak. Dette er ofte ikke tilfellet i det digitale rom. Kripos kunne den gangen vise til at saker ofte blir liggende for lenge i CKG til å være egnet for etterforskning når politiet fikk kjennskap til dem (NOU 2015:13, p. 261). Sjef NorCert sier også at det å ta over en hendelse fra en annen etat ikke vil være optimalt.

Politiet har en operativ rolle under et dataangrep, selv om den operative kapasiteten i dag er veldig begrenset. I det fysiske domenet vil den operative utelederen i politiet koordinere og lede ressursinnsatsen. Senere glir politiets rolle i håndteringen over i etterforskning, der de sikrer spor og samler informasjon. Kripos har et lite fagmiljø innen IKT-sikkerhet; dette fagmiljøet er nå under utbygging og et NC3-senter skal etableres (Antonsen, 2018). Ifølge Kripos' representant er ambisjonen et nytt NC3-senter med 200 ansatte innen 2022.

Det er en utfordring knyttet til retningslinjene for hvordan sikkerhetsaktørene skal sikre digitale spor før de overleveres til politiet. For sikring av logger og skadevare (Appendiks A) samt frysing av data bør det utarbeides en god praksis for NSM-NorCERT og andre CERTer før bevisene overleveres (POD, 2015). Ifølge NorCert-sjef bruker NorCERT og politiet de samme metodene for å sikre spor, dette støttes av Kripos' representant. NorCert-sjef legger til at i de sakene hvor det er en statsaktør som står bak er det ikke alltid like viktig å sikre sporene slik at politiet kan overta, da det ikke berører dem.

Tiltak sikkerhetsaktørene ønsker å iverksette kan noen ganger ikke gjennomføres fordi de ikke har de fullmaktene politiet har (POD, 2015). Datakrimstrategien (POD, 2015, p. 82) beskriver tvangsmidler som et viktig verktøy for håndtering og etterforskning og peker på at NorCERT ikke har dette verktøyet. NSM har ingen hjemler til å pålegge virksomheten å sette av ressurser, utlevere data eller la systemene stå og gå under et angrep i den hensikt å kartlegge trusselaktøren. I dag

etterlater trusselaktøren seg digitale spor i de fleste straffesaker (NOU 2015:13, p. 256). En rekke lovendringer trådde i kraft i 2016 for å styrke politiets evne til å etterforske hendelser. Lovendringene ga politiet et større handlingsrom til å ta i bruk skjulte tvangsmidler som dataavlesning, kameraovervåkning, hemmelig ransaking, romavlytting og kommunikasjonskontroll i den hensikt å forebygge, avverge og etterforske. Regjeringen la også fram et forslag til lovendring i 2017 som vil sikre politiet tilgang til datasystemer som nettbrett og mobiltelefoner slik at de kan åpnes ved biometrisk autentisering som for eksempel fingeravtrykk (NOU 2017:11).

6.1.3.3 Intervjuer

I følge NorCert-sjef er ikke behovet for tvangsmidler et reelt problem, da virksomhetene selv ønsker å bistå med å kartlegge innbruddets omfang. Dette er også i virksomhetens interesse, da gjenoppretting til sikker tilstand er et ledd i arbeidet med å sikre seg mot "bakdører". Når NorCERT avdekker angrepet har som regel trusselaktøren vært inne i lang tid, i snitt opptil flere hundre dager. Det vil sannsynligvis ikke øke skadeomfanget å monitorere angrepet noen dager lenger for å kartlegge trusselaktørens intensjon og skadens omfang. I noen tilfeller kan det være formålstjenlig å gå offline hvis det skulle være kritisk, men dette har NorCERT og virksomheten en god dialog om. Man må balansere hensynet med å kartlegge mot det å ikke miste kritiske data eller tjenester, da det kan være samfunnskritiske funksjoner som rammes. Det er virksomhetens ansvar å levere de tjenestene de gjør, noe NorCERT viser forståelse for.

Informasjonen fra Kripos tyder på at det ikke vil være formålstjenlig for Kripos å ta over rollen som nasjonalt CERT, spesielt med tanke på at mye av informasjonen som kommer fra sensornettverket slik avtale er nå ikke kan deles med politiet og signaturene som legges inn i det er gradert. I tillegg vil det kreve mye ressurser å drive vedlikehold og drift av systemet. NorCERT har brukt lang tid på å opparbeide seg dette samarbeidet, og det vil også kunne undergrave det samarbeidet NorCERT har med virksomheter hvis politiet tar over dette. På den andre siden har det norske politiet stor tillit i befolkningen, så ut fra dette perspektivet kan man si at det kunne ha vært gjennomførbart.

NorCERT kan ikke rekvirere tvangsmidler fra politiet for det vil helt klart gi en formålsutglidning, men politiet og NorCERT bistår hverandre med ulike former for tekniske analyser, da miljøet som driver med dette er relativt lite. Politiet har i enkelte tilfeller vært delaktige i å håndtere saker slik det fremstår i rammeverket, men da i saker de selv har avdekket. Politiet er da primært inne med tvangsmidler i samarbeid med private aktører som har bedre kompetanse til å bedrive selve håndteringen. Et slikt eksempel er at man har benyttet seg av tvangsmidler for å ta ned IKT-infrastruktur i forbindelse med et botnet (Appendiks A). Kripos har dog ikke mange eksempler på slik virksomhet.

6.1.3.4 Oppsummering

Utfordringen med dagens løsning er at det kan ta lang tid før man vet hvem som skal håndtere hendelsen. Frem til dette er avklart tar NorCERT seg av håndteringen. Av alle angrep som rammer samfunnet er det kun et fåtall som er rettet mot kritisk infrastruktur og samfunnsfunksjoner. Med dagens trusselbilde er det politiet som skal håndtere de aller fleste angrepene, da de er utført av kriminelle og ikke statsaktører. I realiteten håndterer NorCERT og PST kun få angrep, og de angrepene de håndterer er ofte av en slik karakter at de faller utenfor politiets mandat. Dette bekreftes av både NorCert-sjef og Kripos' representant i FCKS. Oppgaven med å forvalte den nasjonale CERTen (Appendiks A) er forbeholdt alvorlige angrep over APT-terskelen og beregnet på å stå imot angrep fra statsaktører det ikke er formålstjenlig eller i nasjonal interesse å ta ut påtale mot. Av den grunn er det vanskelig å se for seg en ordning der Kripos har denne rollen. Man kan argumentere med at PST kan ha rollen siden de er en del av EOS-miljøet, men det kan undergrave samarbeidet med virksomhetene da PST også har påtalemyndighet og handlingsrom for å gi pålegg og benytte tvangsmidler. Informasjon om at virksomheter ofte har et bevisst forhold til å ikke anmelde IKT-kriminalitet er med å støtte opp under dette.

Flere av dokumentene belyser utfordringen knyttet til NorCERTs manglende mandat til å benytte seg av tvangsmidler. Dette er ikke i samsvar med informasjonen fra intervjuene. Hverken sjef for NorCERT eller Kripos' representant opplever dette som et reelt problem og har ingen eksempler tilbake i tid der dette behovet har meldt seg.

Erfaringen er heller at virksomhetene ønsker å samarbeide, da det er i deres egen interesse.

6.1.4 Etterforske

Empirien er klar på at det kun er politiet som driver med etterforskning. Det vil allikevel være slik at håndtering glir over i etterforskning, og det kan også i denne fasen oppstå berøringspunkter. Etterforskning med påtale vil være et viktig verktøy for å redusere risikofaktoren trussel, da straff vil virke avskrekkende for trusselaktørene. Jeg vil i dette kapittelet også drøfte om en rolleendring vil føre til flere straffeutmålinger.

6.1.4.1 Mandat gitt i lov

Politiloven pålegger politiet å etterforske: § 2 *"avdekke og stanse kriminell virksomhet og* ***forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov".*** Kriminelle aktører i de fleste saker bruker i økende grad digitale verktøy for å gjennomføre sine kriminelle handlinger. Det å sikre digitale spor er blitt en integrert del av politiarbeidet på de fleste områder. Politiet må ofte spore IP-adresser og datatrafikk samt beslaglegge data og samarbeide med politi i andre land for å oppklare saker, selv i mindre alvorlige saker. Det som ofte tidligere var tradisjonell kriminalitet er nå blitt til digital kriminalitet, da de eneste sporene man kan sikre seg ofte er digitale. Svindel, menneskehandel, narkotikahandel osv. er eksempler på dette (NOU 2017:11, 2017).

6.1.4.2 Dokumentanalyse

Kripos er det nasjonale kompetansesenteret innen sporsikring og bekjempelse av IKT-kriminalitet. Kripos drar ut og bistår politidistriktene med å etterforske alvorlige og kompliserte saker. I 2016 bistå de politidistriktene 135 ganger med datatekniske undersøkelser på datamaskiner, nettbrett, mobiltelefoner, GPS osv. Kripos har spisskompetanse innen IKT-systemer på flere områder; på noen områder utmerker Kripos seg internasjonalt. Denne spisskompetansen har gjort Kripos til en attraktiv

samarbeidspartner internasjonalt og har dannet grunnlag for godt internasjonalt politiarbeid (NOU 2017:11, 2017).

Politiets arbeid med å etterforske dataangrep er ressurskrevende og sporene leder ofte ut av landet. Politiet er i den sammenheng avhengig av godt internasjonalt samarbeid. En annen utfordring er at nettleverandører ikke lagrer IP-adressene lenge nok til at politiet rekker å få dem utlevert, samt at trusselaktører bruker kryptering og tjenester som skjuler deres identitet (POD, 2015). Under ser vi data for anmeldelser og oppklaring av datakriminalitet fra 2016 hentet fra SSB.

2016	Alle avgjørelser	Uoppklart lovbr.	Oppklart lovbr.
Inntrengning i data- og kommunikasjonssystem	314	229	87
Prosent	100	73	27

Tabell 5: Etterforskede lovbrudd (SSB, 2017)

162 av de 229 uoppklarte lovbruddene skyldtes manglende opplysninger om gjerningspersonen. Politiet har også en utfordring knyttet til kapasitet. Lysne-utvalget skriver at det er bare Oslo politidistrikt med ca 20 ansatte som har tilstrekkelig kompetanse til å etterforske dataangrep, men de mangler kapasitet til effektivt å drive skadebegrensning, avdekking, håndtering (NOU 2015:13).

6.1.4.3 Intervjuer

I følge NorCert-sjef driver ikke NorCERT med etterforskning, men prøver alltid å kartlegge omfanget av et angrep. I dette inngår blant annet skadevareanalyse (Appendiks A) og kartlegging av trusselaktører. Håndteringen fordeler seg fint, da NorCERT ikke tar seg av kriminalitet. Det er veldig sjelden at politiet tar over saker NorCERT har avdekket, men NorCert-sjef er klar på at det aldri er optimalt å komme sent inn i håndteringen, og at samhandlingen kan alltid bli bedre.

I følge Kripos' representant i FCKS er det kun politiet som driver med etterforskning, men man kan få støtte fra NorCERT. Miljøene er såpass små at aktørene må hjelpe hverandre der man har ressurser og kunnskap. Kripos etterforsker på samme måte i

det digitale domenet som de gjøre i det fysiske, de sikrer spor, tolker sporene og setter dem i kontekst. Det finnes tidligere eksempler på at politiet tar over saker etter at NSM har håndtert en hendelse, og at politiet den gangen opplevde at man skulle ha vært koblet inn i saken på et tidligere tidspunkt. Etter at FCKS ble opprettet har ikke denne problemstillingen vært relevant. Kripos har overtatt saker etter at NorCERT har håndtert dem, men Kripos' representant har opplevd at NorCERT kontaktet politiet på et tidlig tidspunkt.

6.1.4.4 Trusselreduksjon

Årlig blir det etterforsket ca 20-30 datakrimsaker av Kripos, og de siste årene har fokus vært rettet mot saker med alvorlige konsekvenser, eksempelvis angrep mot finanssektoren. Institusjonene i finanssektoren er aktive med å anmelde saker. Kripos har grunnet utfordringer knyttet til kapasitet kun mulighet til å bistå i de mest alvorlige sakene. Det finnes eksempler der virksomheter har anmeldt dataangrep, men ikke fått den nødvendige bistand på grunn av kapasitetsmangel fra politiets side. Den raske teknologiutviklingen sammen med økt IKT-kriminalitet, både i kompleksitet og volum, har gitt politiet store kapasitetsutfordringer. Kun 9 % av virksomhetene anmelder IKT-kriminalitet (NSR, 2016), noe som i praksis betyr at angrep mot virksomheter i Norge som oftest går fri for straff. Trusselaktørene som gjennomfører IKT-kriminalitet vurderer risikoen og følger nøye med på hvilke land som er mest sårbare. De vil prioritere land der angrepet sannsynligvis ikke vil bli avdekket eller etterforsket. På sikt vil den økende IKT-kriminaliteten som ikke fører til konsekvenser for trusselaktører, undergrave tilliten til retts- og velferdsstaten (NOU 2017:11).

Ifølge NorCert-sjef blir ikke trusselen påvirket av arbeidet til NorCERT, da de driver med generell forebygging. De håndterer kun alvorlige angrep fra aktører som ofte har langsiktige strategiske mål, for eksempel statsaktører som ikke lar seg avskrekke av logiske barrierer og som har flere virkemidler å spille på, som plassering av innsidere eller "human intelligence" (Appendiks A). Disse aktørene vil ikke bry seg om hvilke nasjoner som er sårbare eller hvilke som er robuste når de velger mål, med mindre det dreier seg om NATO eller internasjonale organisasjoner som sitter med samme informasjon i flere land. Da kan de de rette angrepet mot den nasjonen som utgjør det svakeste ledd, og allikevel nå målene sine.

Den eneste aktøren som kan redusere trusselfaktoren er den som har voldsmonopol til å gjøre dette. Politiet kan gjennom økt fokus og rettet ressursbruk mot IKT-kriminalitet ha en avskrekkende effekt på en del trusselaktører. Her er det viktig å skille mellom statsaktører og aktører med betydelige ressurser som driver spionasje eller sabotasje som går inn under kategorien APT (Appendiks A), og andre trusselaktører som driver med kriminalitet i det digitale domenet. I utgangspunktet vil etterforskning med påtale kun bidra til å redusere trusselen mot det sistnevnte. Det vil alltid være lettere å gjemme seg enn å avdekke trusselaktøren, og oppgaven med å avdekke blir mer krevende ved angrep fra trusselaktører knyttet til fremmede stater.

6.1.4.5 Oppsummering

Det er allerede slått fast at en rolleendring der politiet tar over den nasjonale CERT-funksjonen eller VDI-samarbeidet ikke er formålstjenlig og heller ikke vil føre til flere straffeutmålinger. Fra dette perspektivet kan man si at å gjennomføre en rolleendring i den hensikt å redusere trusselen ikke er relevant. Datakrimstrategien og Lysne-utvalget fra 2015 har belyst en utfordring knyttet til at politiet kommer for sent inn i etterforskningen. Det er spesielt viktig i det digitale domenet at sporene er ferske, da de ofte har kortere levetid og de vil kunne anonymiseres eller slettes.

Håndteringskjeden kan også bli stykkevis og delt, og de forskjellige tilnærmingene til sporsikring kan forringe effekten av etterforskningen. Dokumentene er fra 2015, og informasjonen fra intervjuene tyder på at dette ikke er tilfelle lenger. Politiet tar sjelden over saker fra NorCERT og de gangene politiet gjør dette, kobles de inn tidlig. I tillegg er samarbeidet innen sporsikring godt samkjørt mellom politiet og NorCERT. Selv om det er en glidende overgang fra håndtering til etterforskning og det finnes berøringspunkter, kan det virke som om håndteringen fordeler seg fint.

6.2 Organiseringen av samfunnssikkerheten

Takten i digitaliseringen sammen med høy omstillingsevne blant trusselaktørene gjør det ikke enkelt å organisere samfunnssikkerheten. Digitale angrep var ikke en trussel for 30 år siden, og ulike nasjoner har landet på ulike løsninger. I Norge har vi valgt å

samle det generelle, forebyggende sikkerhetsarbeidet og koordineringen av alvorlige digitale angrep under NSM, sammen med en rekke andre myndighetsoppgaver. Fra teorien om reguleringsregime ser vi at forvaltningen må balansere mellom en tydelig rollefordeling der forvaltningsoppgaver på den ene side ikke konkurrerer mellom etater, og på den andre side samle flest mulig forvaltningsoppgaver under tilhørende etat. Ulike aktører bør ha minst mulig overlapp for å oppnå god ressursbruk og færrest mulig berøringspunkter for å gi tydelig ansvars- og rollefordeling. På disse punktene har politiet og NSM et forbedringspotensial. Datakrimstrategien slår fast at "Politiets vide fullmakter og ansvar etter politiloven overlapper fullmaktene til NSM" (POD, 2015, p. 124). I underkapitlene vil jeg se på hvor langt spennet er fra hvor den faktiske utøvelsen av forvaltningspraksis ligger til det teorien sier er den optimale etterlevelse av forvaltningsprinsipper. Jeg vil ut fra dette drøfte om det utgjør en faktisk eller teoretisk utfordring.

6.2.1 Risikoregulering

Risikoen i samfunnet reguleres gjennom et reguleringsregime der rettslige og ikke-rettslige regler justerer kravene til samfunnssikkerhet opp eller ned for å treffe riktig tiltak sett opp mot trusselnivået. Treffer man feil på tiltak, vil det potensielt kunne gi større ulemper enn fordeler. Hvis politiet for eksempel skal bygge opp sin kapasitet innen forebygging og gi ut ikke-rettslig bindende regelverk som veiledere, vil det kunne resultere i merarbeid fordi det vil sette strenge krav til samhandling. NorCert-sjef uttaler at det er nok forebygging for alle. Kripos' representant inn i FCKS uttaler at politiet bør ta mer ansvar for forebygging som berører den type forebygging NSM driver med i dag. Dette kan være problematisk; hvis aktørene kommuniserer to ulike former for best praksis vil dette skape forvirring blant befolkningen og vil kunne svekke tilliten til sikkerhetsaktørene; det kan oppfattes som om en av dem tar feil.

Det finnes en overlapp i det rettslig bindende regelverket i dag som kan gjøre det vanskelig å plassere myndighetsoppgaver, og det vil sannsynligvis ikke skape mindre forvirring hvis politiet tar over flere av oppgavene NSM har i dag knyttet til ikke-rettslig bindende regelverk (se tabell 6). Matrisen viser hvor sikkerhetsloven og politiloven overlapper hverandre og skaper berøringspunkter mellom politiet og NSM. Kolonnen

til venstre viser myndighetsoppgaver politiet og NSM er pålagt å gjennomføre ifølge henholdsvis sikkerhetsloven og politiloven.

	Sikkerhetsloven	Politiloven
IKT-beredskapskjeden	§ 9.Nærmere om oppgavene NSM skal	§ 2.Politiets oppgaver Politiet skal
Forebygge	a. innhente og vurdere informasjon av betydning for gjennomføringen av ***forebyggende*** sikkerhetstjeneste,	2 ***forebygge*** kriminalitet og andre krenkelser av den offentlige orden og sikkerhet
	d. bidra til at sikkerhetstiltak utvikles, herunder iverksette forskning og utvikling på områder av betydning for ***forebyggende*** sikkerhetstjeneste,	
Avdekke	e) drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur og ***et nasjonalt varslingssystem for digital infrastruktur***,	3 ***avdekke*** og stanse kriminell virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov
Håndtere	e) ***drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur*** og et nasjonalt	4 yte borgerne hjelp og tjenester i faresituasjoner, i lovbestemte tilfeller og ellers når forholdene tilsier at bistand er påkrevet og naturlig
		3 avdekke og ***stanse kriminell*** virksomhet og forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov
Etterforske		3 avdekke og stanse kriminell virksomhet og ***forfølge straffbare forhold i samsvar med regler gitt i eller i medhold av lov***
Bistå/Samhandle	b. søke internasjonalt samarbeid, herunder med andre lands og organisasjoners tilsvarende tjenester, når dette tjener norske interesser,	5 på anmodning yte andre offentlige myndigheter vern og bistand under deres tjenesteutøvelse når dette følger av lov eller sedvane
	f) gi informasjon, råd og veiledning til virksomheter.	6 samarbeide med andre myndigheter og organisasjoner tillagt

		oppgaver som berører politiets virkefelt så langt regler gitt i eller i medhold av lov ikke er til hinder for dette
Tilsyn	c. føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven her overholdes, og eventuelt gi pålegg om forbedringer,	

Tabell 6: Berøringspunkter mellom politiet og NSM

En ytterligere rolleendring der politiet driver forebygging på samme måte som NSM, vil også kunne bryte med sentrale prinsipper innen forvaltningspraksis. Fra teorien om god forvaltningspraksis kan man argumentere med at man er tjent med å samle flest mulig dupliserende oppgaver under én aktør; dette vil skape mindre tvetydighet rundt etterlevelse og forståelse av regelverket.

I de neste underkapitlene vil jeg gå gjennom de mest sentrale prinsippene innen forvaltning og se på om det er utfordringer knyttet til hvordan oppgavene har fordelt seg mellom sikkerhetsaktøren.

6.2.2 En åpen forvaltning

I dette underkapitlet vil jeg se om rolleutøvelsen til politiet og NorCERT følger de forvaltningsprinsippene vi har i henhold til stortingsmelding 19; Ei forvaltning for demokrati og fellesskap (St.Meld 19, 2008-2009) og krav til omstilling.

NSM utveksler informasjon med tilsvarende etterretnings- og sikkerhetstjenester i andre land. Denne informasjonen kommer ofte med distribusjonsrestriksjoner fra tjenesten som leverer den (NOU 2015:13, p. 262). Dette er en utfordring både for politiet og private virksomheter, da de ikke er klarert for å motta sikkerhetsgradert informasjon. NSM er en del av EOS-tjenesten og behovet for hemmelighold vil være naturlig for virksomheten. NSM er gjennom oppgavene de er pålagt en sentral og synlig aktør i den nasjonale bekjempelsen av dataangrep. NSMs behov for hemmelighold kan bryte med forvaltningsprinsippet om åpenhet og innsyn. NSM

anerkjenner utfordringen mellom behovet for gradert informasjon på den ene siden og samfunnets behov for åpenhet på den andre. Deling av gradert informasjon mellom EOS-miljøene kan komme samfunnet til gode, da informasjonen ofte omsettes til tiltak. NSM skriver i sitt høringssvar til Lysne-utvalget at tiltak basert på gradert informasjon kan forsvinne om ikke en av de hemmelige tjenestene er premissleverandør og har den nasjonale CERT-funksjonen. Det skal være fult mulig å vurdere informasjonen og dele etter behov, samtidig som de ivaretar rikets sikkerhet. NSM legger til at arenaen det deles på har utviklingspotensiale (NSM, 2016).

Trenden med spionasjesaker er økende. Håndteringen av disse hendelsene krever nært samarbeid mellom de hemmelige tjenestene og deling av gradert informasjon i henhold til sikkerhetsloven. Dette gjør det vanskelig å kommunisere og dele informasjon med ikke-klarert personell i andre organisasjoner. Det har også vært en kraftig økning i andre type IKT-hendelser, der ikke-statlige aktører står bak, eller der personer eller kriminelle nettverk har økonomiske motiver. Det er flere private og offentlige virksomheter som mener at NSM-NorCERT ikke er åpen nok; dette utfordrer samarbeid og informasjonsdeling. Det pekes på at en slik oppfatning er med på å svekke tilliten til NSM-NorCERT, som også har den nasjonale rollen med å koordinere og håndtere alvorlig angrep (Mnemonic, 2015).

Offentlighetens behov for å føre tilsyn med hvordan fellesressursene blir brukt er et viktig prinsipp, som kan komme i konflikt med NSMs behov for hemmelighold.

Ut fra dette perspektivet kan man argumentere med at om politiet tar over navet i oppgaven med å koordinere håndteringen, kan det føre til mer innsyn i informasjon og prosesser aktøren styrer mot og således bidra til en mer åpen forvaltning.

I følge NorCert-sjef må NorCERT, på lik linje med alle andre forvaltningsorganer, følge offentlighetsloven. NorCERT får mange innsynsbegjæringer og deler saksdokumenter, journaler og liknende registre for innsyn dersom de ikke er unntatt offentlighet eller gradert. Ut fra dette perspektivet kan man si at NSM fungerer som et hvilket som helst annet forvaltningsorgan som behandler gradert informasjon, og at

en rolleendring der politiet tar over flere av oppgavene til NorCERT ikke vil føre til en mer åpen forvaltning.

6.2.3 Lett å finne fram

Rollefordelingen mellom politiet og NSM skal være tydelig. Virksomheter og individer bør ikke være i tvil om hvilke sikkerhetsaktører som har ansvar for ulike oppgaver og hva de kan forvente av hjelp. Informasjonen rundt sikkerhetsaktørens rolleutøvelse skal være lett tilgjengelig og lettfattelig for offentligheten.

Det er flere tilfeller med saker som er meldt inn til NSM og oppfattet av virksomheten selv som samfunnskritisk uten å bli prioritert av NorCERT. Virksomhetene kan oppfatte prioriteringen som uforutsigbar, noe som igjen fører til usikkerhet om i hvilken grad NorCERT bistår i hendelseshåndteringen og med hva (Mnemonic, 2015). NSM har fokus på alvorlige angrep mot kritisk infrastruktur. Det er NorCERT som tar avgjørelsen om hvorvidt angrepet utløser bistand eller ikke. Mange angrep er ikke alvorlige, men allikevel ulovlige. Tar politiet over håndteringen, vil det aldri utspille seg noen tvil om at det er NSM eller politiet man skal melde sakene inn til. I tillegg vil politiet gi langt flere saker oppmerksomhet hvis angrepene er strafferettslige.

Lysne-utvalget har funn knyttet til samvirke. Utvalget mener at sikkerhetsaktørenes oppfatning av egen rolle er klar, men at rolleavklaringen og kapasiteten for andres organisasjoner er uavklart. Funnene tyder på at uklarheten kan være mer konstruert enn reell, og opplever friksjon mellom aktørene og at de mangler tillit til hverandre. Det stilles spørsmål til om sikkerhetsaktørene klarer å samhandle tilstrekkelig med en slik mangel på tillit. Utvalget mener at samarbeidsklimaet ikke er påvirket av uavklarte roller og ansvar, men heller av mangel på gode formelle strukturer (NOU 2015:13). Det er også usikkerhet knyttet til hvilke beredskapsroller de ulike aktørene har. Flere politiledere samt NSM peker på at det er utfordringer knyttet til ansvarsdeling og koordinering i det digitale domenet og at potensialet for samhandling er stort. Politiet peker på at behovet for definerte fullmakter er avgjørende for å løse kriser mer effektivt (NOU 2017:11).

Det er et klart tegn på uklare roller når sikkerhetsaktørene selv ikke kjenner til rollene og kapasitetene rundt andre aktører de skal samhandle med. Mye av dette skyldes overlappende myndighetsoppgaver som først og fremst er nedfelt i sikkerhetsloven og politiloven. Det er et viktig prinsipp innen forvaltning at borgeren skal enkelt kunne finne fram til hvilken aktør som utøver ulike myndighetsoppgaver. Det vil være hensiktsmessig å samle oppgavene der det er naturlig, samt tydeliggjøre rollefordelingen (St.Meld 19, 2008-2009). Utfordringen ligger i at politiet har det overordnede ansvaret med IKT-sikkerhet, men det er NSM som avdekker og koordinerer håndteringen av de mest alvorlige angrepene. Dette kan for mange oppleves som en tvetydig rollefordeling og skape usikkerhet knyttet hvor ansvaret ligger, ikke bare blant borgerne, men blant sikkerhetsaktørene selv. Usikkerhet blant virksomheter og privatpersoner er spesielt knyttet til om de skal rapportere til NSM eller anmelde til politiet og hvilken hjelp de kan forvente å få. NSM kan uansett ikke ta imot anmeldelser; skal det norske samfunnet ha én tydelig rapporteringskanal, må det av den grunn bli politiet som tar imot anmeldelser. Det er imidlertid ikke sikkert det er gjennomførbart å ha kun én rapporteringskanal, fordi samfunnet kan bli rammet av to forskjellige angrep, angrep over og under APT-terskelen, angrep der statsaktører står bak de mest alvorlige og de mindre alvorlige er knyttet til IKT-kriminalitet.

På bakgrunn av den forståelse virksomhetene og aktørene selv har, kan man argumentere for at dagens løsning bryter med prinsippet om krav til oversiktlig forvaltning. Jeg oppfatter at mye av kjernen i problemet er knyttet til begrepsbruken. Ordlyden *nasjonal responsfunksjon* kan bety at man håndterer angrep som rammer Norge og *alvorlig angrep* kan strengt tatt bety angrep fra hele trusselkjeden både over og under APT-linjen (se figur 6). Fra dette perspektivet kan man si at det som vil styrke nasjonal evne til å håndtere dataangrep ikke nødvendigvis er en rolleendring, men heller god kommunikasjon og en tydeliggjøring av hva oppgavene til NSM egentlig er, spesielt begrepene *nasjonal responsfunksjon* og *alvorlige data angrep.*

6.2.4 God ressursbruk

Forvaltningen skal ikke bruke mer ressurser enn nødvendig for å løse oppgavene sine. Dette er et viktig prinsipp for at borgerne skal få mest mulig igjen for det de

betaler inn til staten (St.Meld 19 2008-2009). Derfor er det viktig å se på om det finnes dupliserende oppgaver og kapasiteter mellom politiet og NSM. Samlokalisering er et verktøy som vil kunne bidra til et mer sømløst og friksjonsløst samarbeid mellom sikkerhetsaktørene. Det vil kunne gi bedre felles forståelse, bedre informasjonsdeling samt gi stordriftsfordeler ved å samle ressursene rundt hendelseshåndtering og forebygging. Det vil fungere som et senter for samarbeid mellom private og offentlige aktører samt gi et stort kompetansemiljø (NOU 2015:13). Lysne-utvalget er klar på at samlokalisering vil bidra til å øke den nasjonale evnen til å håndtere dataangrep, men er delt i synet på hvem som bør ha det øverste koordineringsansvaret i et slikt senter.

Begge sikkerhetsaktørene har roller knyttet til beredskapskjeden. Rollefordelingen mellom politiet og NSM i forebygging og avdekking er ulik, eksempelvis er det NSM som drifter VDI-løsningen og politiet som tar imot anmeldelser i oppgaven med å avdekke. Det finnes dupliserende oppgaver og kapasiteter i håndtering og etterforskning, der begge bistår den rammede med å analysere årsak, minimere skade, stoppe og monitorere angrepet osv.

En mulig løsning vil være å samle kapasitetene fysisk i ett bygg og styrke samhandling for å sikre god ressursbruk. En annen løsning vil være å dra noe av kapasiteten til NSM over til politiet, og sette en struktur der kun én avdeling har rollen med å håndtere og etterforske. Dette vil sikre god kontroll med ressursbruken. Utfordringen med det sistnevnte er at politiet ikke har klarering til drive håndtering av gradert informasjon, dette kan kun en aktør fra EOS-tjenesten utføre. Grovt sett kan man si at slik rollefordelingen er organisert i dag innen bistand til håndtering, tar NorCERT seg av angrep over ATP-linjen og politiet tar seg av de under (se figur 6).

En tredje løsning vil være å utvide samarbeidet mellom NorCERT og Kripos utover Kripos' tilstedeværelse i FCKS. Ifølge Kripos' representant og datakrimstrategien (POD, 2015) vil Kripos ha stor nytte av overskuddsinformasjonen NorCERT sitter med. I følge NorCert-sjef får operasjonssenteret inn ca. 21 000 angrep, der mange er automatisk behandlet og prosessert videre som varsler til dem det gjelder. De sakene som blir vurdert som viktige nok (ca. 5 000), blir fulgt opp manuelt. Kripos' representant har ingen kjennskap til hvilke saker som blir manuelt fulgt opp i

NorCERT. Ifølge NorCert-sjef er det kun 25 angrep som EOS-tjenestene håndterer, og da er det nærliggende å tro at Kripos vil ha stor nytte av informasjonen fra de 5 000.

Den mest effektive måten å gjennomføre en informasjonsutveksling på er å ha en Kripos-representant i operasjonssenteret til NorCERT. Dette vil i liten grad styrke NorCERTs oppgave, men vil være med på å styrke den nasjonale evnen til å bekjempe datakriminalitet under APT-terskelen. Samordnet bruk av virkemidler er et viktig forvaltningsprinsipp, der forvaltningsorganene må se utover sine egne ansvarsområder og sikre at egne mål ikke står i veien for gode løsninger på tvers av sektorene (St.Meld 19, 2008-2009, p. 9).

Løsning nummer tre kan kun gjennomføres under forutsetning av at en permanent tilstedeværelse av Kripos ikke vil ødelegge for VDI-samarbeidet med virksomhetene. En mulig løsning kan være å anonymisere informasjonen før Kripos' representant i operasjonssenteret deler den med egen avdeling. Det er usikkerhet knyttet til om virksomheter knyttet til VDI samarbeidet vil godta denne eller tilsvarende løsninger, men gevinsten vil sannsynligvis være at den nasjonale evnen til å bekjempe data-kriminalitet blir styrket, og av den grunn bør en slik løsning utredes.

6.2.5 God styring og organisering

Samfunnet har en forventning om at offentlige virksomheter opptrer samordnet og går sammen om å løse utfordringer. Virksomhetene skal ikke sette egne sektormål foran gode fellesløsninger på tvers av sektorer (St.Meld 19, 2008-2009).

Lysne-utvalget kommer med tre ulike forslag for å sikre god styring og bedre sikkerhetsaktørenes organisering. Samlokalisering, styrke NorCERTs koordineringsrolle eller gi rollen som koordinerende enhet til politiet. Hele utvalget er enig i at en samlokalisering vil styrke samordningen av sikkerhetsaktørene, men de er delt i synet på om det er politiet eller NSM som bør ha rollen som koordinerende enhet for IKT-hendelser.

Det er NorCERT som i dag har den koordinerende rollen ved større hendelser mot kritisk infrastruktur. Flertallet i utredningen (NOU 2015:13) mener at strukturen i dag, der NSM har den øverste koordinerende rollen, bør bestå, mens mindretallet mener det vil være formålstjenlig med en rolleendring der politiet overtar denne rollen. Høringssvarene til Lysne-utvalget viser at mindretallet har støtte fra flere sentrale virksomheter som er viktige for den nasjonale evnen til å håndtere dataangrep. Flertallet begrunner sin mening med at NSM allerede har etablert et godt samarbeid med de sivile aktørene. Videre mener de at dette sannsynligvis er et premiss for å sikre et godt samarbeid mellom EOS-tjenestene.

NSM er enig i Lysne-utvalgets vurdering av samlokalisering som virkemiddel til å bedre samarbeidet mellom sikkerhetsaktørene og styrke den nasjonale evnen til å bekjempe dataangrep. Videre mener NSM dette vil legge godt til rette for NSMs rolle med å koordinere IKT-hendelser. NSM er enig med flertallet i Lysne-utvalget i at man må videreutvikle den nåværende strukturen der NSM er det nasjonale navet (NSM, 2016).

Mindretallet mener at den gjeldende strukturen for kriminalitetsbekjempelse prinsipielt bør videreføres inn i det digitale rom. Samfunnets behov for åpenhet og informasjonsdeling gjør det ufordelaktig at en fra EOS-tjenestene skal være navet der behov for gradert informasjon og delingsbegrensninger ligger sentralt. Videre mangler de funn eller eksempler fra andre land, hvor de har lykkes med å drive et effektivt samarbeid og informasjonsdeling mellom etterretningssporet og samfunnssikkerhetssporet i samme organisasjon. Mindretallet foreslår en rolleendring der Kripos skal være den øverste, koordinerende sikkerhetsaktør (NOU 2015:13, p. 274). Kraft- og FinansCERT sier i sitt høringssvar til Lysne-utvalget seg enige med mindretallet (KraftCERT, 2016).

NSM er uenig med mindretallet i at politiet skal være navet i et nasjonalt cybersenter. De kan ikke se at dette vil løse de utfordringene Lysne-utvalget beskriver, og at det vil skape et skille mellom EOS-tjenestenes hendelseshåndtering utløst av gradert informasjon og den generelle samfunnssikkerheten. Dette skillet vil vanskeligjøre samarbeidet mellom EOS-tjenestene og øvrige aktører. NSM finner ingen eksempler fra andre land der politiet har det nasjonale ansvaret for hendelseshåndtering for

sikkerhetstruende digitale hendelser. NSM oppfatter handlingsrommet til politiet utilstrekkelig i rollen som nasjonal CERT. De mener det blir riktig å beholde rollestrukturen slik den er i dag, og heller styrke samarbeidet gjennom et helhetlig rammeverk for hendelseshåndtering (NSM, 2016).

Telenor Norge AS skriver i en rapport fra 2017 (Telenor, 2017) at politiet bør få det øverste ansvaret og får verktøyene og ressursene for å kunne bekjempe IKT-kriminalitet på samme måte som de (de? Telenor?) håndterer kriminalitet i den fysiske verden. Telenor skriver at det vil være hensiktsmessig for samfunnet om politiet får det helhetlige ansvaret for hele IKT-beredskapskjeden, og at de i mange år har etterspurt et «nasjonalt cyber crime center» i politiet – et såkalt NC3.

Finans og KraftCERT skriver i et felles høringssvar til NOU 2015:13 at de støtter mindretallets vurdering og at dette vil gi en bedre nasjonal evne til å respondere på dataangrep. Finans og KraftCERT skriver at det er politiet som bør ha det øverste koordinerende ansvaret, og deres erfaring tilsier at et privat-offentlig samarbeide fungerer best utenfor EOS-tjenestene, da dette bør skje på likeverdige premisser (KraftCERT, 2016).

Mange av oppgavene og ressursene vil naturlig følge den aktøren som har ansvaret for koordineringen. Eksempelvis vil VDI-rollen, som gir størst evne til å avdekke, være sterkt knyttet til koordinering av hendelser. Skal NSM fortsette i sin rolle med å koordinere håndteringen, vil den nasjonale evnen til å bekjempe IKT-kriminalitet testes av god samhandling. Om politiet tar over denne rollen, blir behovet for samhandling mindre og legger til rette for enklere organisering og styring, men dette er ikke hensiktsmessig, først og fremst fordi nasjonal CERT har behov for å jobbe med gradert informasjon. FCKS ble opprettet med representanter fra Kripos i den hensikt å sikre god samhandling. Det bør utredes om denne samhandlingen kan utvides til også å ha en representant i operasjonssenteret til NorCERT.

6.2.6 Tilsyn

NSM skal i henhold til sikkerhetsloven § 9c *"føre tilsyn med sikkerhetstilstanden i virksomheter, herunder kontrollere at den enkeltes plikter i eller i medhold av loven*

her overholdes, og eventuelt gi pålegg om forbedringer". Politiet har ingen tilsynsroller. Dette kapittelet vil besvare spørsmålet om tilsynsrollen til NSM ikke er skilt godt nok fra NorCERTs operative håndtering. Om det ikke skulle være tilfelle, vil det støtte opp under en rolleendring der politiet tar over flere av de operative oppgavene til NSM. Da vil NSM i større grad kunne rendyrke sin rolle som tilsynsforvalter.

NSM har det generelle tilsynet med forebyggende sikkerhet, mens tilsynsforvaltning innen IKT-sikkerhet er spredt mellom ulike tilsynsorganer og mangler ofte den tekniske kompetansen for å gjennomføre et godt tilsyn. Eksempelvis har petroleumstilsynet og finanstilsynet IKT-tilsyn for sin sektor. Som et ledd i å styrke kontroll og tilsyn med IKT sikkerhet, foreslår sikkerhetsrådet å øke driftsbudsjettet til NSM for å kunne etablere en større kapasitet for tilsynsstøtte til andre tilsynsmyndigheter (NSM, 2015). NSM skriver i høringssvaret til Lysne-utvalget at tilsynet med IKT-sikkerhetsarbeidet må økes. Erfaring fra tilsyn, digitale inntrengningsforsøk (penetrasjonstester fra NSM) og håndtering av hendelser avdekker store sårbarheter og avvik hos virksomheter. Av samfunnsøkonomiske hensyn mener NSM at tilsynsmyndighetene i de ulike sektorene bør innhente tilsynsstøtte innen IKT-sikkerhet fra NSM. Hvis de ulike tilsynsmyndighetene skaffer seg denne kompetansen internt, vil det føre til dublerende kompetansemiljøer (NSM, 2016).

NSM har mange roller og leverer tjenester som er delfinansiert ved brukerbetaling. NorCERT har fått ansvaret for å drifte VDI. Systemet består av sensorer som avdekker og varsler myndighetene om sikkerhetstruende dataangrep mot viktige virksomheter og kritisk infrastruktur i Norge. Dette er et samarbeid mellom NSM og virksomhetene som er basert på frivillig deltakelse og er delfinansiert av private aktører. NSM dekker kostnadene til selve infrastrukturen samt utvikling og drift, mens private virksomheter dekker kostnadene til selve sensoren. Offentlige virksomheter har ingen direkte kostnader knyttet til VDI.

Sikkerhetsfaglig råd har gjort en vurdering rundt en rollekonflikt mellom oppgavene og leveransene til NSM. De skriver at så lenge virksomhetene står fritt i å etterspørre tjenestene, vil ikke dette utløse en rollekonflikt, selv om noen av dem er

brukerfinansiert. NSMs tilsynsrolle er også begrenset til sikkerhetsloven, og mange av virksomhetene som etterspør tjenestene er unntatt denne, samt at NSM ikke fører tilsyn med ugraderte systemer (NSM, 2015, p. 28). Ut fra NSMs evnebeskrivelse i tabell 4, ser vi en rollekombinasjon som potensielt kan gi uklare signaler til både tilsynsobjekter og samarbeidspartnere.

NSM har flere roller i forhold til andre offentlige og private virksomheter innen forebygging, håndtering og kontroll. Tabell 4 viser en oversikt over NSMs roller.

FOREBYGGE	HÅNDTERE	KONTROLLERE
Evne til å styrke sikkerheten gjennom å redusere sårbarhet	**Evne til å redusere konsekvensene av en hendelse**	**Evne til å kontrollere at sikkerheten ivaretas**
Evne til: **E-f1** Råd, veiledning om forebyggende sikkerhet **E-f2** Person og virksomhets-klarering **E-f3** Kontroll med luftbårne sensorer **E-f4** Sertifisere informasjons-systemer **E-f5** Kryptosikkerhet **E-f6** IKT-sikkerhet **E-f7** Analyse, risiko-vurdering og tiltaksutvikling **E-f8** Kompetanse-bygging **E-f9** Tekniske undersøkelser **E-f10** Forskning og utvikling (FOU) - forebygge	Evne til: **E-h1** Opprettholdelse av sensornettverk **E-h2** Hendelses-håndtering og varsling **E-h3** Støtte ved hen-delsesrespons **E-h4** Teknisk analyse av skadevare **E-h6** Bidra med ressurser til tverrsektorielt nasjonalt samarbeid og nasjonal krise-håndtering **E-h7** Opprettholde og vedlikeholde handlefrihet og situasjons-forståelse i det digitale rom **E-h8** Forskning og utvikling(FoU) - håndtere	Evne til: **E-k1** Tilsyn **E-k2** Godkjenning av sikkerhets-graderte informasjons-systemer **E-k3** Forskning og utvikling (FoU) - kontrollere

Tabell 7: NSMs oppgaver (NSM, 2015, p. 21)

Når NSM i sin rolleutøvelse har både en asymmetrisk og symmetrisk maktrelasjon til virksomheter, kan rollene misforstås og de symmetriske relasjonene kan oppfattes

som asymmetriske. I tillegg vil ikke-rettslig bindende funksjonsrettede normkrav kunne oppleves som rettslig bindende.

Matrisen under har to dimensjoner:
Den horisontale dimensjonen viser til rollen NSM har i forhold til offentlige og private virksomheter. Den vertikale viser til de rettslig bindende rollene NSM har i forhold til virksomhetene.

	Påvirkning av adferd		
	Tilsyn (Asymmetrisk maktrelasjon)	**Tjenesteyter (Asymmetrisk/symmetrisk maktrelasjon)**	**Tilrettelegger (Symmetrisk maktrelasjon)**
Rettslig bindende krav	1. Detaljkontroll med etterlevelse av lover og regler og reaksjon ved avvik	2. Koordinerende ansvar ved alvorlig angrep mot kritisk infrastruktur/ samfunnsfunksjon	3. Veiledningsplikt mht. til lover og regler
Ikke-rettslig bindende krav	4. Faglig skjønn mht. om normkrav er oppfylt	5. Samarbeid med virksomhet gjennom VDIløsning (Brukerbetaling)	6. Dialog og samarbeid om utvikling av forebyggende sikkerhet og beste praksis

Tabell 8: NSMs Rollekombinasjoner

I rute 3 og 4 vil det typisk vises faglig skjønn rettet mot funksjonskrav der det ofte tas i bruk rettslige standarder. NSMs forvaltningsrolle blir her å veilede og i de tilfeller der det sees på normkrav som standarder og regler som er ikke-rettslig bindende (rute 4), kan dette oppfattes som rettskrav. Utover virksomhetens feiltolkning av roller kan dette også føre til forvaltningsfeil der kontrolløren uten hjemmelsgrunnlag gir

sanksjoner til tilsynsobjektet. Der NSM opptrer som tjenesteyter (rute 2 og 5) og premissleverandør (rute 1), kan virksomheten komme til å oppfatte NSMs rolle som tjenesteyter som noe påtvunget, da de ønsker å unngå negative reaksjoner etter sikkerhetsloven fra tilsyn. Dette kan føre til at samarbeidet som skal basere seg på en symmetrisk maktrelasjon, blir oppfattet som asymmetrisk. Dette slår spesielt uheldig ut når tjenesten (rute 5) er pålagt brukerbetaling.

Et forvaltningsorgan som har flere roller, spesielt som premissleverandør og samarbeidspartner, vil potensielt kunne skape forvirring. Det bør være et prinsipielt skille mellom tilsyn og operativ enhet. NSM-NorCERT som operativ enhet er organisatorisk underlagt NSM, som fører tilsyn etter sikkerhetsloven. Dette kan innvirke på tilliten til virksomheter underlagt denne loven. Tilsyn og operativ enhet bør ikke være plassert i samme organisasjon (Mnemonic, 2015).

Utredningen trekker også fram at private aktører som er viktige for IKT-beredskapen oppfatter en asymmetrisk maktrelasjon mellom de private og offentlige aktørene, der de offentlige fungerer som premissleverandør, og at samvirke ikke er basert på likeverd. Misnøyen begrunnes med at informasjonsdelingen ofte går én vei, fra virksomhet til sikkerhetsaktør (NOU 2015:13).

I følge NorCert-sjef fører ikke NorCERT tilsyn. NSM har en egen kontrollavdeling som utfører tilsyn etter sikkerhetsloven. Det er kun virksomheter underlagt denne loven som har tilsyn fra NSM. Alle virksomheter som har graderte systemer er underlagt tilsyn, og virksomheter uten graderte systemer blir ikke vurdert på IKT-sikkerhet av NSM. Når en virksomhet ber om håndteringsstøtte I forbindelse med et angrep, skyldes dette ofte avvik fra best praksis eller i verste fall avvik fra sikkerhetsloven. NorCERT vil da aldri rapportere til tilsynsavdelingen om avviket. Rapportene vil bli sendt til staben i NSM, og det er en teoretisk mulighet for at tilsynsmyndighetene vil kunne finne avvik i de rapportene. Tilsynsavdelingen i NSM vil ha et tilsynsprogram som går ett år fram i tid uavhengig av hva NorCERT finner eller skriver i rapportene sine. I tillegg er NSM veldig klar på at de skal skille mellom forvaltningsoppgavene tilsyn og håndtering. NorCert-sjef bekrefter i intervjuet at han aldri har hørt om virksomheter som de har hjulpet eller de har et VDI-samarbeid med

uttrykke bekymring rundt tilsynsrollen til NSM, og han mener NSM balanserer dette bra.

Ut fra disse perspektivene kan man si at usikkerheten rundt forvaltningsrollen til NSM som organisasjon er knyttet til den organisatoriske distansen mellom den operative avdelingen NorCERT og kontrollavdelingen som fører tilsyn etter sikkerhetsloven. I tillegg er det spørsmål knyttet til om de faktisk klarer å skille tilsynsrollen og operativ virksomhet, og hvordan virksomhetene opplever dette. Teoridelen på tilsyn er klar på at det er uheldig for ett og samme forvaltningsorgan å være både tjenestetilbyder og premissleverandør. Informasjonen fra NorCert-sjef gir inntrykk av at NSM klarer å skille disse rollene. Funnene jeg har fra sentrale offentlige dokumenter og høringssvar knyttet til NSMs oppgaver, handler mer om det prinsipielle rundt tilsynsforvaltning og nevner ingen eksempler hvor dette er tilfelle. Jeg opplever at dette er en mer konstruert og ikke en faktisk utfordring. Fra perspektivene rundt samfunnets forvaltningsprinsipper kan man si at det er en styrke å samle flere beslektede oppgaver under én og samme organisasjon, da dette vil oppleves som mer oversiktlig for offentligheten.

Jeg har i kapittel 6 brukt teorien og empirien og drøftet de tre teoretiske perspektivene. IKT-beredskapskjeden sammen med trussel- og sårbarhetsreduksjon skjelner godt mellom rollene til sikkerhetsaktørene NorCERT og Kripos. Dette sammen med organisering av samfunnssikkerhet knyttet til digitale angrep har jeg utredet og drøftet ut fra problemstillingen og delspørsmålene.

7 Konklusjon

7.1 Innledning

Flere offentlige og private aktører er av den oppfatning at den nasjonale evnen til å bekjempe dataangrep vil styrkes gjennom en rolleendring der politiet har det øverste koordinerende ansvaret. Samhandling innen beredskap er et nødvendig onde og fører ofte til at håndteringen blir stykkevis og delt. Beredskapsteori og erfaringer fra

krisehåndtering forteller oss at det er først når oppgaven ikke lenger kan løses av én aktør, at behovet for samvirke oppstår (Andersson, et al., 2014), og at når krisen kun treffer ett ansvarsområde gir det størst sannsynlighet for god håndtering (Engen, et al., 2016, p. 52). Ut fra et beredskaps- og forvaltningsmessig perspektiv er det lett å tenke at den beste løsningen vil være at én aktør sitter med hele ansvaret, da dette sikrer en mer helhetlig håndtering og gir færrest mulig berøringspunkter. Jeg vil her svare på om en rolleendring mellom NorCERT og politiet vil endre den nasjonale evnen til å bekjempe dataangrep gjennom å svare på de fire innledende forskningsspørsmålene.

7.2 Ansvar og oppgaver

Utfordringen med dagens lovgivning er at politiets oppgaver favner bredt og omfatter alle angrep, også de alvorlige. Sikkerhetsloven er mer spesifikk og begrenser NSMs rolle til kun å omfatte alvorlige dataangrep. NSMs og politiets roller og ansvar overlapper kun ved de mest avanserte dataangrepene som rammer kritisk infrastruktur. Noe av utfordringen er at det ikke er spesifisert hva loven legger i oppgaven "å drive en nasjonal responsfunksjon for alvorlige dataangrep mot kritisk infrastruktur" og det er uklart hvor alvorlig et alvorlig angrepet er. Lovverket gir ingen tydeliggjøring av disse begrepene, noe som gir rom for feiltolkning. Dette står heller ikke beskrevet i forarbeidet til sikkerhetsloven (Ot.prp.nr.49 (1996-1997)). Funnene mine samsvarer med utredningen til Lysne-utvalget, der de skriver at sikkerhetsaktørene kjenner sin egen rolle, men at usikkerheten ligger i at aktørene ikke alltid kjenner de andre aktørenes rolle (NOU 2015:13, p. 273). Med unntak av NorCERT, kan det virke som om det er noe usikkerhet blant de andre sikkerhetsaktørene, virksomhetene og offentligheten om hva loven legger i *nasjonal responsfunksjon* og *alvorlige angrep.* En tydeliggjøring av disse begrepene kan føre til mindre usikkerhet rundt NSMs oppgaver og kan bidra til å synliggjøre dagens ansvarsfordeling som fornuftig.

Norge ble rammet av ca. 22 500 angrep i 2017. NorCERT avdekket og bisto PST med håndteringen av ca. 25 hendelser gjennom VDI-samarbeidet og informasjon fra EOS-miljøet. Man er gjennom sentrale dokumenter som NOU 2015 :13 og datakrimstrategien (POD, 2015) ledet til å tro at NorCERT avdekker, koordinerer og

håndterer langt flere og mindre alvorlige saker enn det som er tilfellet. Ifølge NorCert-sjef avdekker og bistår NorCERT med håndtering kun der trusselaktører driver spionasje og sabotasje i cyberdomenet. Den nasjonale responsfunksjonen, eller det NSM selv kaller den nasjonale CERT-funksjonen, omfatter ikke håndtering av ordinær IKT-kriminalitet, men avdekking og koordinering av angrep fra aktører med betydelige ressurser. Det er viktig å forstå at PST har politimyndighet og er som en del av EOS-miljøet ansvarlige for å håndtere de mest alvorlige dataangrepene og etterspør bistand fra NorCERT ved behov.

7.3 Bør politiet ha den nasjonale CERT-funksjonen

Den nasjonale CERT-funksjonen omfatter generell forebygging, avdekking av alvorlige angrep mot kritisk infrastruktur og bistand med håndteringen av disse. Utfordringen er at angrep fra fremmede statsmakter eller ressurssterke aktører ofte blir avdekket gjennom gradert informasjon fra EOS-miljøet eller gjennom VDI-samarbeidet med virksomheter som ikke ønsker å anmelde angrepet. Dette gjør at politiet blir skjermet fra informasjon om angrep med et viss skadepotensial. Mangel på slik informasjon vil vanskeligjøre etterforskning. Angrep fra ressurssterke aktører som angriper fra utsiden av landegrensen, vil sannsynligvis ikke bli identifisert. Selv om dette er ulovlige angrep og går inn under politiets ansvarsområde, vil det ikke være god utnyttelse av ressurser om disse sakene ble etterforsket, da det sannsynligvis ikke vil føre til påtale. Skulle politiet klare å identifisere trusselaktøren kan det i visse tilfeller av politiske grunner ikke lønne seg å ta ut påtale begrunnet nasjonale interesser. Ut fra disse perspektivene kan man konkludere med at politiet ikke bør ta over denne rollen, da den er begrenset til få spesielle saker som sannsynligvis ikke vil la seg løse.

7.4 Bør politiet ta over VDI-samarbeidet

Det er lett å se for seg at VDI-løsningen til NorCERT avdekker flere tusen angrep og at politiet blir skjermet for viktig informasjon. Dette stemmer ikke. NorCERT har VDI-samarbeidet med virksomhetene. VDI-løsningen er formålsbegrenset til kun å fange opp kjente signaturer NorCERT legger inn i VDI for å fange opp alvorlige angrep. Disse signaturene er gradert og kommer som regel fra andre EOS-miljøer, nasjonalt

og internasjonalt. NorCERT koordinerer få angrep i året som avdekkes gjennom VDI-samarbeidet og informasjon fra EOS-miljøet. Det kan være lett å kritisere ressursbruken til NorCERT når de kun håndterer 25 angrep, men dette er angrep som rammer Norge med et enormt skadepotensial. Driften av VDI-løsningen og samarbeidet med virksomhetene slik det ser ut i dag er ikke en rolle politiet kan ta over, da de er avhengige av gradert informasjon fra EOS-miljøene. Om man uansett skulle lande på en slik løsning, må politiet gi disse sakene videre til PST eller NSM, noe som kan føre til at håndteringen blir stykkevis og delt.

En rolleendring mellom NSM og politiet vil ikke styrke den nasjonale evnen til å håndtere dataangrep. Men en bedre informasjonsflyt mellom politiet og NSM vil kunne gjøre dette. Politiet vil kunne ha stor nytte av overskuddsinformasjonen fra VDI-samarbeidet. Dette kan være informasjon knyttet til trusselaktørens metoder, trender, generelle sårbarheter blant virksomheter og så videre. Utfordringen er at virksomhetene eier informasjonen. For å kunne gjennomføre en slik informasjonsutveksling, bør informasjonen NSM får fra VDI-samarbeidet bli gjort mindre formålsbegrenset, eksempelvis ved å anonymisere informasjonen fra den berørte virksomheten.

En god måte å løse dette på er å kopiere den fungerende samarbeidsmodellen i FCKS og ha en fast liaison fra Kripos i NorCERTs operasjonssenter. Her vil Kripos' representant kunne skille ut relevant overskuddsinformasjon for egen avdeling samt anonymisere den for å ivareta virksomhetens interesser. Dette er en løsning aktørene bør tilstrebe å få til, da samordnet bruk av virkemidler er et viktig forvaltningsprinsipp, der forvaltningsorganet må se utover sine egne ansvarsområder og sikre at egne mål ikke står i veien for gode løsninger på tvers av sektorene (St.Meld 19, 2008-2009, p. 9).

8 Referanser

Andersson, A., Carlstrom, E. D., Ahgren, B. & Berlin, J. M., 2014. Managing boundaries at the accident scene - a qualitative study of collaboration excercises. p. Volume 3 Issue 1 pp. 77.

Antonsen, R., 2018. Olav Skard Jørgensen blir ny leder for NC3. *Politiforum*.

Aven, T., 2015. *Risikostyring,* Oslo: Universitetsforlaget.

Aven, T. et al., 2004. *Samfunnsikkerhet,* Oslo: Universitetsforlaget.

Aven, T. & Renn, O., 2010. *Risk Management and Governance,* New York: Springer.

Aven, T., Røed, W. & Wiencke, H. S., 2008. *Risikoanalyse.* 2. opplag 2010 ed. Oslo: Universitetsforlaget.

Barane, J. E., 2015. La oss diskutere risikoanalyse uten hersketeknikk. *Digi.no*.

Blaikie, N., 2009. *Designing Social Research.* 2. opplag ed. Cambridge, UK: Polity Press.

Danermark, B., Ekstrom, M. & Karlsson, J., 1997. *Att förklara samhället.* 3 ed. Lund: Studentlitteratur.

DSB, 2016. *Samfunnets Kritiske Funksjoner,* Tønnsberg: Direktoratet for samfunnssikkerhet og beredskap.

Engen, O. A. H. et al., 2016. *Perspektiver på samfunnsikkerhet.* Oslo: Cappelen Damm Akademisk.

E-Tjenesten, 2017. *Fokus,* Oslo: Etteretningstjenesten.

E-Tjenesten, 2018. *Fokus,* Oslo: Etteretningstjenesten.

FFI, 2015. *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger,* Kjeller: Forsvarets forskningsinstitutt.

FFI, 2017. *Hvordan kan vi kommunisere det vi ikke vet?,* Kjeller: Forsvarets forskningsinstitutt.

Fimreite, A. L., Lango, P., Lægreid, P. & Rykkja, L. H., 2014. *Organisering, samfunnssikkerhet og krisehåndtering.* Oslo: Universitetsforlaget.

Forskrift om sikkerhetsadministrasjon, 2001. *Forskrift om sikkerhetsadministrasjon (FOR-2012-06-22-580),* Oslo: Hentet fra Lovdata.

KraftCERT, 2016. *Høring: "Digital sårbarhet - sikkert samfunn" (NOU 2015:13).*

Kristiansen, E., Magnussen, L. I. & Carlstrom, E., 2017. *Samvirke - en lærerbok i beredskap.* Oslo: Universitetsforlaget.

Kruke, B. I., 2012. *Notat: 7 /12 Samfunnssikkerhet og krisehåndtering: relevans for 22. juli 2011,* Oslo: 22. juli-kommisjonen.
Kvale, S. & Brinkmann, S., 2015. *Det kvalitative forskningsintervju.* 3 ed. Oslo: Gyldendal Norsk Forlag.
Lindøe, P. H., Kringen, J. & Braut, G. S., 2015. *Risiko og Tilsyn.* 2 ed. Oslo: Universitetsforlaget.
Meld. St. 10, 2016-2017. *Risiko i et trygt samfunn,* Oslo: Regjeringen.
Meld. St. 29, 2011-2012. *Samfunnssikkerhet,* Oslo: Regjeringen.
Mnemonic, 2015. *Avdekke, håndtere og etterforske digitale angrep - For Lysneutvalget,* Oslo: Mnemonic.
NOAB, 2018. *Det Norske Akademis ordbok,* Oslo: Kunskapsforlaget.
NOU 2003:18, 2003. *Rikets sikkerhet.*
NOU 2006:6, 2006. *Når sikkerheten er viktigst.*
NOU 2015:13, 2015. *Digital sårbarhet – Sikkert samfunn.*
NOU 2016:19, 2016. *Samhandling for sikkerhet.*
NOU 2017:11, 2017. *Bedre bistand. Bedre beredskap.*
NS-ISO 31000, 2018. *Risikostyring - Retningslinjer.*
NSM , 2015. *Terrorsikring.*
NSM, 2014. *Organisasjon.* [Online]
Available at: https://www.nsm.stat.no/om-nsm/organisasjon/
NSM, 2015. *Anbefalinger om åpenhet rundt IKT-hendelser.*
NSM, 2015. *Sikkerhetsfaglig råd.*
NSM, 2016. *Digital sårbarhet- Sikkert samfunn - Høringssvar fra Nasjonal sikkerhetsmyndighet.*
NSM, 2016. *Risikovurdering for sikring.*
NSM, 2017. *Helhetlig IKT-Risikobilde.*
NSM, 2017. *Rammeverk for håndtering av IKT-Sikkerhetshendelser.*
NSM, 2017. *Årsrapport.*
NSM, 2018. *NSM etablerer Nasjonalt cybersikkerhetssenter.* [Online]
Available at: https://nsm.stat.no/aktuelt/nsm-etablerer-nasjonalt-cybersikkerhetssenter/
NSM, 2018. *Risiko 2018.*
NSR, 2016. *Mørketalsundersøkelsen.*
Ot.prp.nr.22 (1994-1995), 1995. [Online].

Ot.prp.nr.49 (1996-1997), 1997. [Online].
POD, 2014. *Etterretningsdoktrine,* Oslo: Norengros Erik Tanche Nilssen AS.
POD, 2015. *Overordnet nasjonal strategi for bekjempelse av datakriminalitet - Datakrimstrategien.*
Politiet, 2018. *Politiet.no.* [Online]
Available at: https://www.politiet.no/om/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/
Prop. 1 S, (2016–2017). *For Budsjettåret 2017 — Utgiftskapitler: 61, 400–497 Inntektskapitler: 3400–3497.*
PST, 2018. *Trusselvurdering 2018.*
PWC Norge, 2017. *Cybercrime Survey.*
Riksrevisjonen, 2004-2005. *Riksrevisjonens undersøkelse av omorganiseringer som forvaltningspolitisk virkemiddel.*
Ruud, H.-M. T., 2013. Jeg vet ikke hvor NOKAS-pengene er. *Dagbladet*, 10 Desmeber, pp. https://www.dagbladet.no/nyheter/jeg-vet-ikke-hvor-nokas-pengene-er/61903830.
Sikkerhetsloven §1, 2001. *Lov om forbyggende sikkerhet.*
SSB, 2017. *Etterforskede lovbrudd.* [Online]
Available at: https://www.ssb.no/lovbrudde/
St. Meld 17, 2001-2002. *Samfunnssikkerhet-Veien til et mindre sårbart samfunn.*
St.Meld 17, 2002-2003. *Om statlig tilsyn.*
St.Meld 19, 2008-2009. *Ei forvaltning for demokrati og fellesskap.*
Telenor, 2017. *Digital Sikkerhet.*
Trædal, T. J., 2017. Nå får politiet sitt «NC3» - et eget senter for cyberkriminalitet. *Politiformu.no*, 16 November.
Trædal, T. J., 2018. Ny cybersjef på plass. *Politiforum.*
World Economic Forum, 2015. *Global Information Technology Report.*

Appendiks A

Definisjoner

APT: Avanserte vedvarende trusler (Advanced Persistent Threats). Vedvarende og målrettet angrep på systemer med formål å etablere bakdører, plante og spre skadevare og hente ut fortrolig informasjon. Angriperen er gjerne ressurssterk, bruker avansert skadevare og opererer langsiktig. Også betegnelse på aktøren bak et slikt angrep (NSM, 2017).

Botnet: Samling datamaskiner i nettverk som hackere har tatt robotaktig kontroll over (NOAB, 2018)

CERT: «Computer Emergency Response Team» er en koordinerende enhet for IKT-sikkerhet. CERT er en lisensbelagt tittel. I Norge eksisterer ulike CERT-miljøer. NorCERT er det nasjonale CERT-miljøet (NSM, 2017).

Cyber: Benyttes om alt som er på internett og digitalt. Cyberspace refererer til en verden av sammenkoblede datasystemer og informasjonsressurser. Betegnelsen blir ikke benyttet i rammeverk for digital hendelseshåndtering, men sidestilles i denne sammenheng med betegnelsen «IKT» (NSM, 2017).

Digital: Funksjoner som er bygget opp ved hjelp av det binære to-talls systemet, 0 eller 1, som refererer til av/ eller på-signal eller ikke signal. Det aller meste av datateknologi og informasjon på datamaskiner er digitalt (NSM, 2017).

Etterretning: Etterretning har til formål å innhente digitalt lagret, men ellers utilgjengelig informasjon, og utnytte denne i en systematisk bearbeidingsprosess. Etterretningsoperasjoner er i høy grad rettet mot politiske, militære, teknologiske og økonomiske mål i samsvar med nasjonalstatlige interesser. Etterretningstjenesten følger i særlig grad statlige eller statlig sponsede trusselaktører (E-Tjenesten, 2018).

Human Intelligence (HUMINT): Begrepet menneskebasert innhenting brukes om etterretning utledet av data og informasjon skaffet til veie gjennom interaksjon med

menneskelige kilder, for eksempel informantbehandler, spaner, avhører, m.m. (POD, 2014)

IKT: IKT forstås her som alle systemer som utfører sin funksjon gjennom å sende, motta, lagre, prosessere og konvertere informasjon fra andre systemer (NSM, 2017).

IKT-sikkerhet: Beskyttelse av informasjon og systemer som er sårbare fordi de er koblet til, eller på annen måte er avhengig av IKT (NSM, 2017).

IKT-sikkerhetshendelse: Situasjoner der IKT-systemer blir utsatt for tilsiktede handlinger (NSM, 2017).

Kritisk infrastruktur: De anlegg og systemer som er nødvendige for å opprettholde samfunnets kritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghet (NSM, 2017).

Kritisk samfunnsfunksjon: De funksjonene som må opprettholdes i samfunnet for å sikre trygghet og basale fysiske behov for befolkningen (NSM, 2017).

Phishing: Nettfisking, eller phishing på engelsk, er et samlebegrep som beskriver hvordan kriminelle lurer mennesker til å gi fra seg sensitiv informasjon eller penger på Internett.

Påvirkningsopperasjoner: Påvirkning vil si å bruke sosiale medier og nyhetsmedier til å undertrykke og manipulere virkelighetsoppfatningen gjennom fornektelse og desinformasjon. Målet vil være å diskreditere en stats myndigheter, forvirre befolkningen og eventuelt demoralisere militært personell. Den overordnede hensikten er å forme det strategiske handlingsrommet til egen fordel (E-Tjenesten, 2018).

Sabotasje: Sabotasje omfatter skade, ødeleggelse og forstyrrelser. Norge kan settes under press og tvang ved at fremmede stater retter trusler mot sivile mål som infrastruktur for elektrisk kraft, telekommunikasjon, transport og banktjenester. På det

militære området kan det rettes sabotasjehandlinger mot systemer for kommando og kontroll, kommunikasjon, navigasjon og overvåkning (E-Tjenesten, 2018).

Skadevare (malware): Skadelig programvare (fra engelsk malicious software) (NSM, 2017).

Skadevareanalyse: Analyse av det tekniske innholdet i skadevare (NSM, 2017).

Trusselaktør: En kjent eller ukjent aktør (person, organisasjon, land eller annen) som forbindes med en trussel (NS 5830:2012).

Virksomhet: Betegnelse for en organisatorisk enhet som eksempelvis kan være et departement, et direktorat, en etat, en organisasjon eller et privat foretak. For dette rammeverket må det skilles mellom departementet som sekretariat for politisk ledelse, departementet som en virksomhet som skal ivareta egen sikkerhet, og departementet som overordnet ansvarlig for sikkerhet i egen sektor (NSM, 2017).