Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2021 Åpen
Forfatter: Birgitte Bøe	
Fagansvarlig: Odd Einar Olsen **Veileder:** Odd Einar Olsen	
Tittel på masteroppgaven: Beredskap mot store cyberangrep. En studie av dagens status om beredskap mot store cyberangrep i organisasjoner som er ansvarlig for drift av kritisk infrastruktur. **Engelsk tittel:** Emergency preparedness towards large cyber attacks. A study of the status on preparedness in organisations that are responsible for critical infrastructure.	
Studiepoeng: 30	
Emneord: Cybersikkerhet, cyberangrep, digitalisering, trusler, beredskap, resiliens, redundans, risikovurdering, kritisk infrastruktur, kraftsektor, lufttransportsektor, vann- og avløpssektor, olje- og gassektor, SCADA, CERT.	Sidetall: 68 + vedlegg/annet: 85 Stavanger, 15. juni 2021

Forside for masteroppgaven

Det teknisk-naturvitenskapelige fakultet

Beredskap mot store cyberangrep

En studie av dagens status om beredskap mot store cyberangrep i organisasjoner som er ansvarlig for drift av kritisk infrastruktur

VG, 2018

Masteroppgave i samfunnssikkerhet

Universitetet i Stavanger

Birgitte Bøe

Våren 2021

Forord

Denne oppgaven er et resultat på et fullført masterstudie i samfunnssikkerhet ved Universitetet i Stavanger. Det har vært to svært innholdsrike år. Ved å knytte oppgaven opp til tematikken rundt cybersikkerhet har jeg fått muligheten til å studere et svært dagsaktuelt tema, noe som har vært svært spennende og interessant. Kunnskapen jeg har tilegnet meg gjennom denne oppgaven tar jeg med meg videre til arbeidslivet.

Tusen takk til alle informantene som tok seg tid til å stille til intervju. Uten dere ville ikke oppgaven vært like innholdsrik. Stor takk til professor og veileder Odd Einar Olsen, for gode veiledninger bestående av interessant diskusjon, gode tilbakemeldinger og mye oppmuntring. Det har gitt meg motivasjon og selvtillit til å gjennomføre oppgaven.

Underveis i skriveprosessen har jeg fått god hjelp og støtte av medstudenter, venner, familie og samboer. Det rettes en stor takk til min gode venninne og medstudent, Celine Iversen, som alltid har vært tilgjengelig for alle mine spørsmål, og for at du har lest korrektur av oppgaven. Takk til min kjære moster som har tatt seg av språkvasken. Det er et undervurdert arbeid. Ellers fortjener familie, venner og samboer en takk for å alltid ha kommet med motiverende taler når motivasjonen min har sviktet. Spesielt takk til min far som visste hva han skulle gjøre når jeg sølte vann over Macen min noen uker før innlevering. Dere alle har bidratt til at jeg herved leverer masteroppgaven min med stor stolthet.

God lesing!

Birgitte Bøe
Stavanger, 15. juni 2021.

Sammendrag

Den digitale utviklingen har satt store spor i samfunnet i løpet av de siste årene. Virksomheter har videreutviklet driftssystemer med digitale systemer, såkalt SCADA-systemer. Det har ført til at arbeidet kan utføres av færre mennesker, samtidig som at målet er at en får økt effektivitet og produktivitet. I takt med digitaliseringen øker de digitale sårbarhetene. PST sin nasjonale trusselvurdering fra 2021 påpeker at angrep i det digitale rom er den største trusselen for tiden, spesielt rettet mot norske virksomheter. Det krever en omstilling for enhver virksomheter i møte med de digitale truslene.

I denne oppgaven undersøkes det hvorfor beredskap mot cyberangrep har endret seg i sektorer som er ansvarlig for drift av kritisk infrastruktur. Slike sektorer som er ansvarlig for drift av kritisk infrastruktur er et mål for cyberangrep da det vil føre til større samfunnsmessige konsekvenser ved nedetid. Oppgaven tar utgangspunkt i fire selskaper fra ulike sektorer, kraftsektoren, lufttransportsektoren, vann- og avløpssektoren og olje- og gassektoren, for å se hvordan trusselbildet har endret seg, hvordan de foretar risikovurderinger og hvordan beredskapen har endret seg hos dem.

Det er flere årsaker til at beredskap mot cyberangrep har endret seg. Oppgaven viser at disse faktorene og årsakene kan sees på som sentrale:

- Det blir arbeidet kontinuerlig for å kartlegge trusselbildet hvor en aktivt søker og gir informasjon.
- Risikovurderinger skjer i samarbeid med andre aktører, eksempelvis CERTer.
- Beredskapen springer ut fra en strategi om å kunne motstå et cyberangrep fremfor å unngå cyberangrep. Dette med et fokus om å være resilient.

Trusselbildet har blitt større og mer komplisert. Sektorene som oppgaven tar utgangspunkt i, har i løpet av de siste årene fått et økt fokus rundt beredskap mot cyberangrep hvor praksis blir kontinuerlig vurdert i samarbeid med flere aktører. Empirien viser at sektorene har endret beredskapsplanleggingen sin med en holdning om at det er en dynamisk prosess hvor en aldri er ferdig med arbeidet. Beredskapen har dermed endret seg, og vil endre seg igjen og igjen så lenge digitale løsninger blir implementert.

Innholdsfortegnelse

Begreper ..... **vii**

Forkortelser ..... **viii**

Tabeller ..... **ix**

Figurer ..... **ix**

1.0 Innledning **1**

1.1 Bakgrunn 1

1.2 Problemstilling 2

1.3 Avgrensning 3

1.4 Tidligere forskning 3

1.5 Oppgavens struktur 6

2.0 Kontekst **7**

2.1 Digitalisering i kritisk infrastruktur 7

2.2 Cybersikkerhet 9

2.3 Cyberangrep 11

3.0 Teori **13**

3.1 Sikkerhetsforståelse i organisasjoner 13

Normal Accident Theory (NAT) 13

High Reliability Organisations (HRO) 15

Resiliens 18

Man-Made Disaster (MMD) 19

3.2 Oppsummering av teori 24

4.0 Metode **25**

4.1 Metodisk tilnærming 25

Forskningsdesign 25

Forskningsmetode 25

4.2 Forskningsprosess 25

Tabell over forskningsprosess 26

4.3 Datainnsamling 28

Dokumentanalyse 28

Informanter 29

Intervjuguide 31

Intervjuprosess 31

4.4 Kvalitetskriterier 31

Reliabilitet 32

Validitet 32

Overførbarhet 32
4.5 Styrker og svakheter ved valgt metode 32
5.0 Empiri 34
5.1 Presentasjon 34
Kraftsektoren 35
Lufttransportsektoren 36
Vann- og avløpssektoren 36
Olje- og gassektoren 36
Oppsummert 37
5.2 Hvordan har truslene endret seg? 37
Kraftsektoren 38
Lufttransportsektoren 39
Vann- og avløpssektoren 40
Olje- og gassektoren 41
Oppsummert 43
5.3 Hvordan blir risikovurderinger gjort? 43
Kraftsektoren 43
Lufttransportsektoren 44
Vann- og avløpssektoren 45
Olje- og gassektoren 46
Oppsummert 47
5.4 Hvordan har beredskapen endret seg? 48
Kraftsektoren 48
Luftransportsektoren 48
Vann- og avløpssektoren 49
Olje- og gassektoren 50
Oppsummert 51
5.5 Oppsummering 51
6.0 Diskusjon 52
6.1 Hvordan har truslene endret seg? 52
6.2 Hvordan blir risikovurderinger gjort? 58
6.3 Hvordan har beredskapen endret seg? 62
7.0 Konklusjon 66
7.1 Forslag til videre forskning 68
Referanseliste 69
Vedlegg 74
Vedlegg 1: Samtykkeerklæring 74
Vedlegg 2: Intervjuguide 75

Begreper

Risiko: Trefaktormodellen (trussel, verdi og sårbarhet) er en tilnærming til risiko, og er et uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen (NS 5830:2012, s. 5 i Bergsjø et al., 2020, s. 188).

Risikovurdering: Kartlegging og vurdering av det som kan true virksomheten, og en vurdering av hvilke konsekvenser dette kan få (Bergsjø et al., 2020, s. 187).

Trussel: Trussel kan være hva som helst, enten fysisk eller abstrakt, dersom det har potensialet til å negativt påvirke et objekt eller system (Bergsjø et al., 2020, s. 147).

Sårbarhet: Evnen virksomheten, systemet eller den samfunnskritiske funksjonen har til å være i stand til å møte trusselen med. Det vil si i hvilken grad en aktør kan utføre en uønsket handling uten å bli stanset (Njå et al., 2020, s. 258).

Beredskap: Beredskap omfatter alle tekniske, operasjonelle og organisatoriske tiltak som hindrer at en inntrådt faresituasjon utvikler seg til en ulykkessituasjon, eller som hindrer eller reduserer skadevirkningene av inntrådte ulykkessituasjoner (Aven et al., 2004, s. 121).

Krisehåndtering: Den umiddelbare og påfølgende responsen, forberedt eller ad-hoc, når en krise har manifestert seg (Engen et al., 2016, s. 300).

Kritisk infrastruktur: De anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner (NOU 2015: 13, s. 19).

Phishing: Innebærer å utnytte en ansatt for å skaffe seg uautorisert tilgang til en virksomhets IKT-systemer, for eksempel via epost (NSM, 2021, s. 38).

Resiliens: Et objekts evne til å gjenvinne sin opprinnelige form eller gjenopprette sin funksjon etter at det har blitt utsatt for en ytre påkjenning (Kongsvik et al., 2018, s. 88).

Forkortelser

PST	Politiets sikkerhetstjeneste
DSB	Direktoratet for Samfunnssikkerhet og Beredskap
NSM	Nasjonal sikkerhetsmyndighet
NOU	Norges Offentlige Utredninger
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
HRO	High Reliabilty Organization
NAT	Normal Accident Theory
MMD	Man-Made Disaster
Ptil	Petroleumstilsynet
SCADA	Supervisory Control And Data Acquisition
IKT	Informasjons- og kommunikasjonsteknologi

Tabeller

Tabell 1. Ulike kulturer for behandling av informasjon.....22
Tabell 2. Oversikt over prosessen i forskningsprosjektet.....26
Tabell 3. Oversikt over relasjoner til andre sektorer.....34

Figurer

Figur 1. Oppgavens oppbygging…….….6
Figur 2. Tidslinje av utviklingen når det gjelder fokus rundt cybersikkerhet.....9
Figur 3. Klassifisering av systemer som kategoriseres etter koplinger og interaksjoner.....14
Figur 4. Oversikt over kulturell dimensjon (Y-akse) og strukturell dimensjon (X-akse).....17
Figur 5. Faser i MMD-modellen.....20
Figur 6. Illustrasjon av NOU 2015: 13 sin betydning i senere arbeid.....28
Figur 7. Illustrasjon av oppsett i kapittel med fokus på hver sektor.....34
Figur 8. Illustrasjon av oppsett i kapittel med fokus på paraplybegrepet kritisk infrastruktur....52
Figur 9. Kategorisering av oppgavens sektorer etter koplinger og interaksjoner.....54
Figur 10. Hendelsesforløp i lys av MMD-modellen.....57
Figur 11. Syklus for cybersikkerhet.....61
Figur 12. Plassering av kritisk infrastruktur som en HRO.....64

1.0 Innledning

1.1 Bakgrunn

De siste tiårene har digitalisering ført til gjennomgripende samfunnsmessige endringer. Den har effektivisert arbeidshverdagen for de fleste av oss, slik at det samme arbeidet nå kan utføres av langt færre hender. Den har forandret måten vi styrer prosesser på, slik at komplekse operasjoner og infrastrukturer nå kan kontrolleres fra ett eller noen få sentrale steder (NOU 2015: 13, s. 15). Problemer rundt cyberangrep er like relevant for de fleste kritiske infrastrukturer, uavhengig hvilken sektor en hører til, og det må forskes mer på (Haanæs, 2020). Kritisk infrastruktur handler om de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner (NOU 2015: 13, s. 19). Derfor er det mulig å diskutere problemer rundt kritisk infrastruktur på et overordnet nivå da organisasjoner som kan kategoriseres som kritisk infrastruktur har den kritiske funksjonen til felles.

Den digitale utviklingen i samfunnet viser at cyberangrep mot bedrifter øker og at det fortsetter å øke i utbredelsen, samt at de blir mer sofistikerte og farligere (Roald, 2018). Maglaras et al. (2018) tar for seg sårbarhetene kritisk infrastruktur har når det gjelder cyberangrep, hvor driftssystemer ofte er utsatt. Et angrep på driftssystemer (også kalt for SCADA-systemer) kan forårsake mye skade, noe som også kan true menneskeliv. Dette er et problem for enhver organisasjon, men også nasjoner. Et viktig tiltak for å redusere risikoen for slike angrep, er at offentlig og privat sektor går sammen og utvikler omfattende og robuste sikkerhetsstrategier som er integrert i virksomheten (Umbach, 2012). Cybersikkerhet er et voksende fenomen, og det kommer nye oppdagelser med jevne mellomrom. Forskere rundt omkring i verden legger frem strategier for å kunne kartlegge trusselbildet, og dermed være bedre rustet til å tåle et cyberangrep. Stoddard (2016) tar for seg cybersikkerhet innenfor kritisk infrastruktur i Storbritannia, og påpeker hvor viktig det er med tiltak nasjonalt og globalt for å oppnå suksess med resiliens for cyberangrep. Skjelvik (2019) fant ut i sin masteroppgave hvordan risiko for cyberangrep så ut i finanssektoren. Funn viste at selv om det er en negativ utvikling i form av flere trusler og sårbarheter knyttet til cyberangrep, er finanssektoren en moden sektor når det gjelder cybersikkerhet. Likevel er konsekvensene katastrofale ved et digitalt angrep, til tross for lav sannsynlighet.

Det er allerede en del forskning rundt temaet cybersikkerhet med angrep på kritisk infrastruktur, og hva en bør gjøre for å være mer robuste til å tåle et slikt angrep. I og med at de digitale

utfordringene vokser i takt med den digitale utviklingen, vil en aldri komme til et punkt hvor det er nok forskning. PSTs nasjonale trusselvurdering for 2020 la frem at en av de mest alvorlige truslene er spionasje, digital kartlegging og sabotasje av kritisk infrastruktur (PST, 2020, s. 2). Trusselvurderingen for 2021 viser at trusler i det digitale rom fortsetter. De siste årene har andre lands etterretningstjenester lyktes med å bryte seg inn i de digitale nettverkene til norske myndigheter og private virksomheter. Det er en utvikling som påvirker trusselbildet på alle PSTs ansvarsområder (PST, 2021, s. 1). Fokus på angrep i det digitale rom må derfor få en større plass på dagsordenen.

1.2 Problemstilling

I og med at årlige rapporter belyser nødvendigheten av å ha et fokus på cybersikkerhet, viser det at det er et område i kontinuerlig endring. Det betyr at det holder ikke å ha én laminert beredskapsplan som skal gjelde i flere år og i flere organisasjoner. Den må oppdateres og justeres fortløpende så lenge den digitale utviklingen vokser. Med bakgrunn i dette vil det være interessant å ta et dypdykk i hvordan fokuset på cyberangrep har endret seg gjennom tidene, og hva som forårsaker det. Oppgavens problemstilling er som følger:

Hvorfor har beredskap mot cyberangrep endret seg i organisasjoner som er ansvarlig for drift av kritisk infrastruktur?

For å besvare problemstillingen er det utformet tre forskningsspørsmål som skal bidra til å besvare problemstillingen:

1. Hvordan har truslene endret seg?

For å forstå hvorfor beredskap for cyberangrep har endret seg, må en se på hvilke trusler en står overfor, og hvordan truslene har endret seg. Dette ved for eksempel å se på hvilke angrepsmetoder som blir brukt under et cyberangrep. Har det vært en endring i truslene gjennom tidene, så vil det medføre at beredskapen må endre seg deretter. Er truslene like uavhengig av hvilken organisasjon det er snakk om?

2. Hvordan blir risikovurderinger gjort?

Hvordan risikovurderinger blir gjort kan være avhengig av å følge med på nyhetsbildet og trekke erfaringer fra andre lignende aktører. Hva er de opptatt av? Hvor er fokuset? Hvem gjør

risikovurderinger? Blir det tatt hensyn til relasjoner med andre organisasjoner? På den måten kan en være proaktiv ved å håndtere de sårbarhetene den teknologiske utviklingen medfører, samtidig samarbeide på kryss og tvers for å få bedre kunnskap rundt sine risikovurderinger.

3. Hvordan har beredskapen endret seg?

Det siste forskningsspørsmålet går mer i dybden på selve beredskapsplanleggingen, og hva den er opptatt av. Hvordan møter beredskapen de truslene som nå ligger til grunn? Hvilken strategi bygger den på? Dette spørsmålet vil også se på om organisasjoner har iverksatt tiltak for å gjøre beredskapen mer oppdatert og robust internt, men også i samarbeid med andre sentrale aktører.

1.3 Avgrensning

Beredskap mot cyberangrep er et stort og omfattende tema. Oppgaven vil ta utgangspunkt i fire ulike sektorer som kan kategoriseres som kritisk infrastruktur; kraftsektoren, lufttransportsektoren, vann- og avløpssektoren og olje- og gassektoren. Grunnen til at kritisk infrastruktur er av interesse, er fordi det kan gå utover viktige funksjoner samfunnet er avhengig av. Dermed vil ikke oppgaven ta for seg det tekniske aspektet cyberangrep innebærer, men heller de samfunnsmessige konsekvensene. Problemstillingen handler om å se hvorfor beredskapen for cyberangrep har endret seg, og dermed vil det være hensiktsmessig å få et innblikk i viktige sentrale organisasjoner innenfor kritisk infrastruktur for å få et overordnet blikk på temaet. Med det kan en få en idé om cybersikkerheten i ulike kontekster. Er det forskjell på alvorlighetsgraden i de ulike sektorene? Oppgaven har ikke som formål å gjennomføre sammenligninger mellom sektorer, ei heller avdekke mangler og feil, men heller belyse et viktig tema for å bidra til et økt fokus. Med en slik avgrensning av oppgaven mister en muligheten til å gå i dybden i én sektor, men får heller et innblikk over flere – noe som bidrar til å belyse temaet innenfor et kritisk infrastruktur-perspektiv.

1.4 Tidligere forskning

I boken *Critical Energy Infrastructure at Risk of Cyber Attack* påpeker Frank Umbach (2012) at kritisk infrastruktur er i risiko for cyberangrep. Det er mye mer avansert enn hva eksperter trodde i 2010, og i de siste årene har cyberangrep og cyberkriminalitet vokst frem til å bli en massiv trussel. Cyberangrep utgjør en trussel til alt vi gjør siden verden i voksende grad blir avhengig av det digitale. Umbach (2012) beskriver kritisk infrastruktur som informasjonssystemer, telekommunikasjon, transportsektoren, energiforsyning, helse og

finanssystemer – for å nevne noen. Alle disse kritiske infrastrukturene er karakterisert med deres høye grad av interne kompleksitet og avhengighet, samt sårbarhet (Umbach, 2012, s. 38). Nødvendigheten for å beskytte kritisk infrastruktur som en potensiell nasjonal og internasjonal sikkerhetsrisiko, ble lagt frem allerede i midten av 1990-tallet. Det ble dog ikke tatt seriøst før etter 2001, som et resultat av internasjonal terrorisme og opprettelsen av Homeland Security i USA. I de senere år har fokuset skiftet fra fysiske terrorangrep til cyberangrep. Siden terrorangrepene 11. september 2001 har kritisk infrastruktur vært et mål under cyberangrep (Umbach, 2012, s. 38). Umbach konkluderer med at både offentlig og privat sektor må utvikle omfattende, redundante sikkerhetsstrategier som er integrert i daglig drift i virksomheten (Umbach, 2012, s. 64). Denne boken er interessant da den tar for seg holdningene rundt cybersikkerhet allerede i 2010, og når kritisk infrastruktur ble et mål for cyberkriminalitet. Boken bekrefter at risiko for cyberangrep innenfor kritisk infrastruktur har vært aktuell i flere år.

Kristan Stoddard (2016) har en artikkel hvor han tar for seg cybersikkerhet innenfor kritisk infrastruktur i Storbritannia. Han forklarer at med den raske digitale utviklingen som beveger seg i Storbritannia og i andre land, vil potensialet for ondsinnede handlinger bare øke (Stoddard, 2016, s. 1103). Volumet, typene og kompleksiteten innenfor cyberkriminalitet og cyberspionasje vil ikke endre seg med mindre robuste tiltak blir iverksatt (Stoddard, 2016, s. 1104). Stoddards artikkel ble skrevet for å hjelpe den britiske regjeringen med å beskytte Storbritannia mot cyberangrep på kritisk infrastruktur. Artikkelen legger frem anbefalinger slik som å bygge opp resiliens og redundans mot cyberangrep dersom det er nødvendig. For at det skal bli en suksess, er det nødvendig med tiltak på nasjonalt og globalt nivå. Land og private virksomheter må forstå trusselbildet og risikoen innenfor kritisk infrastruktur, og hvem som er ansvarlige for dem. Dette er kjente problemer for alle utviklende stater. Selv om artikkelen tar for seg cybersikkerheten i Storbritannia, så har den overføringsverdi til andre land. For å være robust til å håndtere cyberangrep er det viktig å trekke erfaringer fra andre selskaper, bransjer og land, noe Stoddard (2016) legger frem. Dermed er denne artikkelen svært relevant da en kan ta denne forskningen videre, og se hvordan fokuset er innenfor kritisk infrastruktur i Norge.

IT-selskapet ATEA har en artikkel angående cyberangrep mot bedrifter, hvor forfatteren forklarer hvordan cyberangrep fortsetter å øke i utbredelse, samt at de blir mer sofistikerte og farligere. Dette er angrep som handler om organiserte kriminelle som vil stjele finansiell informasjon, terrorister som lanserer løsepengevirus, samt statlig etterretning som er ute etter

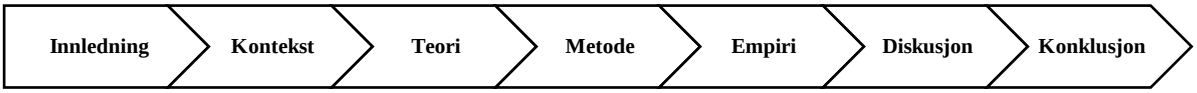
informasjonssystemer. Alle disse ulike angrepene jobber i det stille helt til de ser en mulighet som kan utnyttes ved sin tilstedeværelse. Bedrifter må dermed arbeide for å beskytte organisasjonen mot cyberangrep, ved å blant annet ha en kontinuerlig trening på bevissthet og beredskap rundt cybersikkerhet, samt ha sikkerhetsgjennomgang implementert i arbeidshverdagen (Roald, 2018).

I Maglaras et al. (2018) sin artikkel, tar forfatterne for seg de sårbarhetene kritisk infrastruktur står overfor, og kartlegger syklusen for cybersikkerhet som innebærer prediksjon, beskyttelse, oppdagelse og reaksjon. Under prediksjon må organisasjonen vurdere alle proaktive tiltak for å kunne identifisere truslene, gjennom eksempelsvis risikovurderinger. Gjennom beskyttelsesfasen må organisasjonen installere de nødvendige programvaretiltakene for å oppnå de sikkerhetsmålene en fikk ut av risikovurderingene fra forrige fase. I oppdagelsesfasen må organisasjonen ha implementert overvåkningsmekanismer, slik at de kan skille mellom normal og unormal oppførsel i nettverket. Siste fasen, reaksjonsfasen, inkluderer alle prosesser og metoder organisasjonen må ha på plass for å håndtere hendelsen, sammen med planer for gjenopprettelse (Maglaras et al., 2018, s. 2). Som nevnt innledningvis er SCADA-systemer et mål for cyberangrep. Dermed er det svært viktig at organisasjoner tar for seg de fasene nevnt ovenfor for å kunne være så godt forberdt som mulig.

En tidligere masteroppgave fra Universitetet i Stavanger tok for seg cyber-risiko i finanssektoren og hvorfor den har utviklet seg det siste tiåret. Forskingen viste at det har skjedd store endringer. Finanssektoren er avhengig av de digitale løsningene, noe som gjør systemet og infrastrukturen mer komplekst, som videre gjør det vanskelig å få en oversikt over sårbarheter. Med et trusselbilde som er i kontinuerlig utvikling hvor trusselaktører utvikler seg raskere enn de forebyggende tiltakene gjør, var det overraskende at sårbarheten betraktes som lavere selv om truslene, verdiene og konsekvensene av en uønsket digital hendelse er større i 2019 enn i 2009 (Skjelvik, 2019, s. III). Oppgavens konklusjon sier at selv om forskningen peker mot en negativ utvikling for risiko gjennom en økning i trusler og sårbarheter hvor flere verdier flyttes over på «cyberdomenet», så har finanssektoren en positiv utvikling ved at det ikke har skjedd noen alvorlige digitale hendelser. Utfordringen handler om at hvis det først skulle skjedd en uønsket hendelse, til tross for lav sannsynlighet, så vil konsekvensene være katastrofale (Skjelvik, 2019, s. 94).

Forskningsartiklene har bidratt til å øke forståelsen om når kritisk infrastruktur ble en målgruppe for angrep, både fysisk og digitalt, til hvilket type angrep bedrifter blir mest utsatt for, og hva organisasjoner bør gjøre for å bli mer robust i møte med cyberangrep.

1.5 Oppgavens struktur



Figur 1. Oppgavens oppbygging.

Oppgaven består av syv kapitler, hvor kapittel én introduserer oppgavens problemstilling og forskningsspørsmål, samt tidligere forskning. I kapittel to blir oppgavens kontekst lagt frem hvor rammeverket for studiet blir presentert. Digitalisering i kritisk infrastruktur, cybersikkerhet og cyberangrep vil bli forklart. Kapittel tre redegjør for oppgavens teoretiske rammeverk, hvor fire ulike teorier på sikkerhetsforståelse i organisasjoner blir presentert. Kapittel fire forklarer oppgavens metodiske fremgangsmåte hvor valg vil bli begrunnet. Kapittel fem legger frem funn fra empiri sektorvis, bestående av data fra både dokumentanalyse og intervjuer. I kapittel seks blir teori og empiri drøftet opp mot forskningsspørsmålene, hvor alle sektorene blir forklart samlet under paraplybegrepet «kritisk infrastruktur». Avslutningsvis i kapittel syv blir oppgavens konklusjon besvart, samt forslag til videre forskning.

2.0 Kontekst

I dette kapitlet vil digitalisering i kritisk infrastruktur bli introdusert, samt relevante aktører innenfor kartlegging av sårbarheter. I tillegg vil cybersikkerhet bli knyttet opp til kritisk infrastruktur, hvordan det har utviklet seg, og hvordan det ser ut i dag. Til slutt vil cyberangrep forklares sammen med en redegjørelse av de typiske cyberangrepene oppgavens problemstilling tar utgangspunkt i.

2.1 Digitalisering i kritisk infrastruktur

Ulike norske virksomheter kan kategoriseres som kritisk infrastruktur, som for eksempel virksomheter innenfor kraftsektoren, lufttransportsektoren, vann- og avløpssektoren og olje- og gassektoren. Som nevnt tidligere kan kritisk infrastruktur forklares som de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner (NOU 2015: 13, s. 19). Det som gjør en digital trussel mot kritisk infrastruktur mer alvorlig enn mot andre infrastrukturer, er at konsekvensene går ut over nødvendige anlegg og systemer som trengs for å opprettholde samfunnets kritiske funksjoner. NOU 2015: 13 presenterer elektronisk kommunikasjon, satellittbaserte tjenester, energiforsyning, olje og gass, vannforsyning, finansielle tjenester, helse og omsorg, og transport som de infrastrukturene som er kritiske for samfunnet. For å sørge for at kritisk infrastruktur er mer robust for digital trussel, har regjeringen lagt frem en nasjonal strategi for digital sikkerhet (Regjerningen, 2019). Et av målene handler om cybersikkerhet i kritiske samfunnsfunksjoner, hvor de skal være understøttet av en robust og pålitelig digital infrastruktur. Samfunnet er avhengig av at kritiske samfunnsfunksjoner opprettholdes, og det forutsettes at de digitale infrastrukturene som understøtter dem, virker overalt og hele tiden. Dette krever også et samarbeid på tvers av de ulike digitale infrastrukturene. En hendelse kan oppstå i én digital infrastruktur, og gi konsekvenser i en annen (Regjeringen, 2019, s. 3). Dermed kan problemet med cyberangrep sees på som tverrsektoriell.

Aktører

Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og politiet er noen sikkerhetsorganer som jobber kontinuerlig for å kartlegge risikobildet rundt digitalisering. NSM har i flere år rapportert at det er kjente sårbarheter som benyttes for å gi uautorisert tilgang til systemer og nettverk, og at det fortsatt preger det digitale risikobildet (NSM, 2020, s. 5). Videre i rapporten påpeker NSM at mange virksomheter fortsatt mangler risikoreduserende

tiltak helt eller delvis, noe som utgjør en bekymring. Samtidig har flere virksomheter begynt å prioritere arbeid med cybersikkerhet, noe som øker samfunnets totale robusthet mot sikkerhetstruende hendelser. Cybersikkerhet er et felles ansvar, og det må tas på alvor (NSM, 2020, s. 5). Politiets trusselvurdering for 2021 inneholder et utvalg av kriminalitetstrusler, blant annet datainnbrudd med løsepengevirus. Politiet fastslår at det er stor sannsynlighet at slike datainnbrudd vil øke, også rettet mot virksomheter med samfunnskritiske funksjoner (Politiet, 2021, s. 5). Når anerkjente sikkerhetsmyndigheter som PST, NSM og politiet fastslår at den digitale trusselen må tas på alvor, er det ingen tvil om at det er en alvorlig samfunnsutvikling.

For å minimere risikoer som oppstår ved digitalisering, er det nødvendig med et fellesskap hvor myndighetene er på banen, samt at flere aktører samarbeider på kryss og tvers. Digitalisering er sektorovergripende, som vil si at sektorene ikke kan løse digitale problemer hver for seg, og et samvirke er dermed nødvendig (Meld. St. 27 (2015-2016), s. 11). Regjeringen har lagt til grunn at alle sikkerhetstiltak skal iverksettes basert på en risikovurdering. Dette må virksomhetene selv vurdere, noe som er i tråd med ansvarsprinsippet. De må sørge for at informasjon og systemer er godt nok sikret i forhold til gjeldende regelverk, har et oppdatert trussel- og risikobilde, samt oversikt over kjente sårbarheter (Meld. St. 27 (2015-2016), s. 150). Her kommer de årlige rapportene fra PST, NSM og politiet inn som nyttige veivisere innenfor trusselbildet. Rapportene er oppdaterte på nyhetsbildet både nasjonalt og internasjonalt. Det kan tas med videre som inspirasjon til hva det må rettes fokus på, slik at hver virksomhet kan handle proaktivt. Den nye sikkerhetsloven (2018) bidrar også til et bedre fundament for å gjennomføre bedre risikovurderinger. Den nye sikkerhetsloven (2018) erstattet en 20 år gammel sikkerhetslov. Mens den gamle sikkerhetsloven la stor vekt på beskyttelse av gradert informasjon, omfatter den nye loven i tillegg informasjonssystemer, infrastruktur og objekter av sentral betydning for nasjonal sikkerhet (KPMG, u.å.). Den nye sikkerhetsloven (2018) legger dermed krav om at den enkelte virksomheten selv må sørge for gode risikovurderinger som passer til deres funksjon.

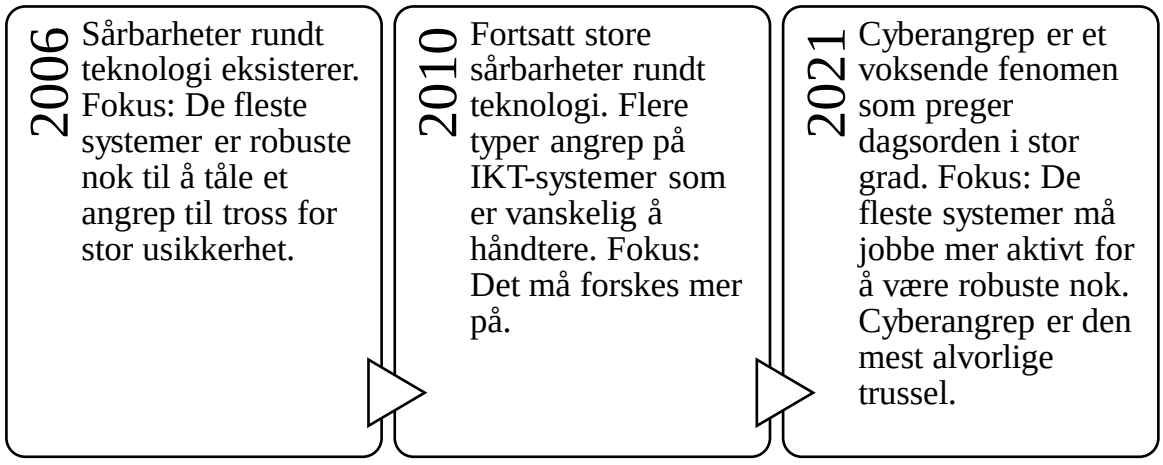
I tillegg til arbeidet PST, NSM og politiet gjør med årlige trusselvurderinger, har CERTer blitt opprettet som et tiltak for å være mer robuste i hendelseshåndtering ved cyberangrep. CERT står for Computer Emergency Response Team, og er en gruppe eksperter på informasjonssikkerhet som er ansvarlig for beskyttelse mot, påvisning av og respons overfor en organisasjons cybersikkerhetshendelser (Røislien, 2020, s. 205). De arbeider også for å øke offentlig bevissthet, samt drive forskning på å forbedre datasikkerhetssystemer (Røislien, 2020,

s. 205). Det finnes ulike fagspesifikke CERTer, alt ettersom hvilken sektor en går innunder. Videre i oppgaven er det primært KraftCERT og NorCERT som blir brukt. KraftCERT bistår kraftbransjen i sikring av driftssystemer for å motvirke cyberangrep (KraftCert, 2020). NorCERT ligger under NSM, og er sentrale med cybersikkerhetsarbeid og er et nasjonalt samlingspunkt (Røislien, 2020, s. 205). De er dermed ikke spesifikt knyttet til en sektor, men heller nasjonen Norge. Digitale trusler innenfor virksomheter er absolutt en virkelighet, og det er en stor nødvendighet å ha sikret robusthet mot digitale trusler i kritisk infrastruktur, da konsekvensene kan være omfattende og ødeleggende. Mye av robustheten består av kunnskap mot det uventede, noe en kan hente fra PST, NSM og politiet sine vurderinger, samt i samarbeid med tilhørende CERTer.

2.2 Cybersikkerhet

Digital sikkerhet handler om beskyttelse av «alt» som er sårbart, fordi det er koblet til eller på en annen måte er avhengig av informasjons- og kommunikasjonsteknologi (IKT) (Bergsjø et al., 2020, s. 18). Ulike begreper blir brukt om det digitale sikkerhetsarbeidet, blant annet informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet. I Norge er begrepene brukt om hverandre de siste årene (NOU 2015: 13, s. 34). I denne oppgaven er det begrepet cybersikkerhet som blir brukt.

Utvikling



Figur 2. Tidslinje av utviklingen når det gjelder fokus rundt cybersikkerhet. Inspirert av NOU (2006: 6), regjeringen (2010) og PST (2021).

Cybersikkerhet har vært et kjent fenomen i flere år. NOU 2006: 6 omhandler beskyttelse av kritiske infrastrukturer og kritiske samfunnsfunksjoner. Den tar for seg sikkerhetsutfordringer,

blant annet ved bruk av ny elektronisk kommunikasjon som åpner muligheter for å forårsake skade, både tilsiktet og utilsiktet. Den viser at sårbarheten har utviklet seg fra et systemnivå til et individnivå (NOU 2006: 6, s. 44). Sårbarheter rundt bruk av teknologi ble først da introdusert som et nytt og voksende fenomen. Det ble fremstilt at det var stor usikkerhet rundt det potensielle skadeomfanget et cyberangrep kan ha, men at de fleste systemer er robuste nok til å tåle et dataangrep, og at gjenopprettelse vil skje relativt raskt (NOU 2006: 6, s. 45). I 2010 utarbeidet PST, E-tjenesten og NSM en felles rapport om cybersikkerhet. Rapporten la frem digitale sårbarheter som er like aktuelle den dag i dag. Det dreide seg om spionasje, angrep på IKT-systemer, angrep på nett som lammer/påvirker kritiske samfunnsfunksjoner, nettkriminalitet og generelt alvorlige cyberhendelser som går utover store virksomheter, tjenesteleverandører, toppledere i både offentlig og privat sektor (Regjerningen, 2010, s. 3). Videre står det at sammenlignet med tradisjonelle konvensjonelle trusler, er det imidlertid svært vanskelig å beskrive, vurdere og håndtere cybertrusler. Grunnene til det er at trusselaktøren er i stor grad anonym, det er politiske og geografiske utfordringer, det er en hurtig teknologisk utvikling som kan utnytte de oppdagede sårbarhetene, det er «billig» å utføre et angrep, og at angrepene er blitt mer automatiserte (Regjeringen, 2010, s. 9). De to rapportene fra 2006 og 2010 viser at det på noen få år har gått fra å være et nyoppdaget fenomen, til å plutselig prege dagsorden i en mye større grad. Trusselvurderingene fra 2010 og frem til 2021 poengterer at sårbarheter og trusler vokser enda mer. Det bekrefter at fokuset har økt.

Sikkerhetsmål

Innenfor cybersikkerhet finnes det noen sikkerhetsmål med fokus på sikring av IKT-systemer for å unngå at uvedkommende får tilgang til driftssystemet. Det handler om sikring av konfidensialitet, integritet og tilgjengelighet. Konfidensialitet handler om at informasjonen kun er tilgjengelig for den som har autorisert tilgang. Tap av konfidensialitet kan være at hackere får tilgang til hemmelig informasjon. Integritet handler om at informasjonen og metodene er nøyaktige og fullstendige. Tap av integritet kan være et resultat av at uvedkommende endrer informasjon. Tilgjengelighet handler om at autoriserte brukere har tilgang til informasjon og nødvendige ressurser ved behov. Tap av tilgjengelighet kan være at driftsoperatører ikke får tilgang til driftssystemet (NOU 2015: 13, s. 162). Det er en balansegang mellom disse sikkerhetsmålene. For å oppnå full konfidensialitet kan informasjon låses ned, men det vil gå utover tilgjengeligheten som videre kan føre til mindre effektivitet. Høy grad av tilgjengelighet kan øke risikoen for at klassifisert informasjon kommer på avveie (NOU 2015: 13, s. 35). Sikkerhetsmålene må balanseres alt ettersom hva som er viktige verdier for virksomheten som

skal utføre dem. Dette er i tråd med den nye sikkerhetsloven (2018) ved at virksomheten selv må avgjøre hva som er gode nok risikovurderinger.

2.3 Cyberangrep

Innenfor cybersikkerhet ligger potensialet for cyberangrep. Cyberangrep handler om å forstyrre eller skade et datasystem gjennom ulike metoder, og er et fenomen som har vokst frem de siste årene i takt med digitaliseringen. I 2018 gjennomførte Direktoratet for samfunnssikkerhet og beredskap (DSB) en stor befolkningsundersøkelse om hva nordmenn tenkte rundt cyberangrep. Hele 42 % av innbyggerne er bekymret for at cyberangrep skal slå ut viktige driftssystemer de kommende fem årene. Nesten like mange, 37 %, er bekymret for terrorangrep i Norge (DSB, 2018). Dette er i tråd med PST sin trusselvurdering for 2021, hvor det blir lagt frem at digitale trusler er de største truslene Norge står ovenfor (PST, 2021, s. 1).

Utvikling

Cyberangrep utvikler seg kontinuerlig, det samme gjør de ulike typene av cyberangrep. En artikkel fra Teknisk Ukeblad legger frem en oversikt over 16 spektakulære cyberangrep gjennom tidene. Utviklingen viser at trenden gikk fra store ødeleggelser, til spionasje, videre til dataorm hvor datamaskinene blir infisert med virus, til zero-day angrep hvor sikkerhetssårbarheten ikke er kjent før selve angrepsdagen (Hamnes, 2012). Nå er det ikke lenger kun store ødeleggelser hvor hele systemet blir lammet permanent, men mer angrep hvor angriperne i tillegg kan få en økonomisk og politisk vinning.

Dagens trusler

De viktigste truslene er løsepengevirus og statlig etterretningsvirksomhet. Løsepengevirus er et type angrep som ikke kan holdes skjult av den enkelte bedrift da de kan føre til at driftssystemet får nedetid. Det blir offentliggjort uten at de kan kontrollere det selv. Hackerne får tilgang til datasystemene for å hente ut informasjon, og deretter truer med å publisere informasjonen om de ikke får løsepengekravet innfridd (Vollan, 2021). Dette ved å bruke for eksempel metoden «phishing», som innebærer en sosial manipulering via epost, utnyttelse av svakheter i programvare eller gjetting av passord (Politiet, 2021, s. 22). NSM og Kripos har utarbeidet en rapport hvor det oppsummeres at løsepengevirus er den største trusselen. Antallet registrerte tilfeller av løsepengevirus globalt har økt hvert år siden 2013, og økningen er rettet mot bedrifter og virksomheter med større betalingskraft enn enkeltpersoner (NSM & Kripos, 2020). Et

eksempel på et løsepengevirus er angrepet som rammet Norsk Hydro i 2019. Denne hendelsen vil bli beskrevet i delkapittel 5.3.

I PSTs trusselvurdering fra 2021 står det at flere lands etterretningstjenester vil det kommende året bruke store ressurser på etterretningsaktivitet i Norge, hvor russiske og kinesiske tjenester vil utgjøre den største trusselen (PST, 2021, s. 2). Fremmede stater vil kartlegge norsk infrastruktur, hvor de er ute etter informasjon og innflytelse som Norge ikke er interessert i at de får (PST, 2021, s. 2). Kartlegging av infrastruktur handler om at andre stater vil avdekke funksjoner og sårbarheter i Norges kritiske infrastruktur. Dette gjøres blant annet ved bruk av teknisk overvåkning (PST, 2021, s. 9). Eksempel på en slik hendelse er nettverksoperasjonen mot Stortinget høsten 2020 og våren 2021. I angrepet mot Stortinget høsten 2020 var det den russiske militære etterretningstjenesten «GRU» som sto bak. Formålet bak angrepet var å innhente grunnleggende informasjon om norske forhold som kan brukes i etterretningstjenester. GRU lyktes med å stjele sensitiv informasjon fra ulike epost-kontoer (PST, 2021, s. 7). Våren 2021 ble Stortinget utsatt for et nytt angrep, som opplevdes som større enn det som var tilfellet høsten 2020. Det ble omtalt som et angrep mot demokratiet, og de vet fortsatt ikke hvem som sto bak (Aftenposten, 2021).

3.0 Teori

I dette kapittelet vil oppgavens teoretiske rammeverk bli redegjort. Teorikapitlet består av flere teorier som sammen skal bidra til å besvare problemstillingen og forskningsspørsmålene. Avslutningsvis vil det være en oppsummering av hva disse teoriene har til felles for oppgavens problemstilling, og hva som vil bli tatt med videre.

3.1 Sikkerhetsforståelse i organisasjoner

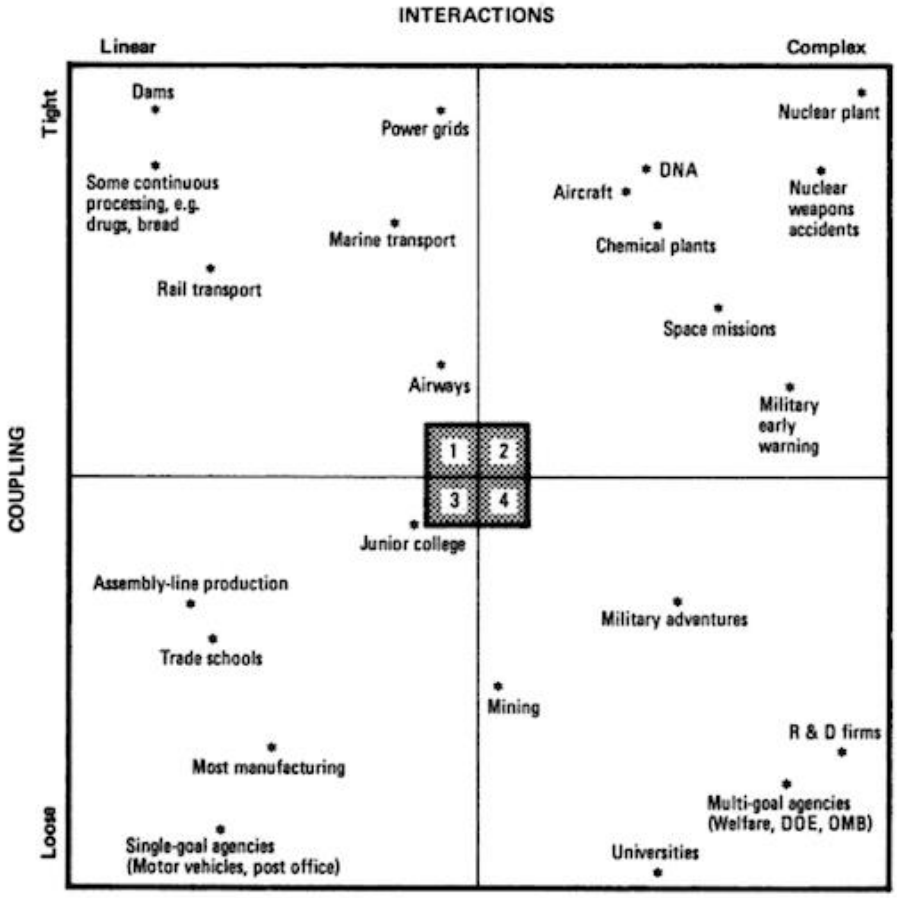
I dette kapitlet vil fire sentrale teorier innenfor forebygging av systemulykker bli presentert. Det blir lagt hovedvekt på teorien om High Reliability Organisations og Man-Made Disasters, da de kan bli sett på som kontraster. Teorien om Resiliens og Normal Accidents vil bli kort redegjort, da de har interessante momenter som kan trekke linjer til oppgavens problemstilling og forskningsspørsmål.

Normal Accident Theory (NAT)

Teorien om NAT er basert på Perrow (1984) sin forståelse av Three Mile Island ulykken, og hvorfor denne ulykken ikke kan ses på som uvanlig (Perrow, 1984, s. 31). Perrow (1984) sitt hovedpoeng er at komplekse og høyteknologiske systemer er konstruert på en slik måte at ulykker er uunngåelige og derfor «normale». Dette er basert på hvordan feilene interagerer, slik at effekten blir større og annerledes enn hvis det er en enkeltkomponent som svikter. I tillegg handler det også om hvordan systemet er bygget opp, og hvordan systemet tåler uforutsette kjedereaksjoner som setter systemet i fare for en ulykke (Perrow, 1984, s. 4).

Perrow (1984) mener at det er egne karakteristikker i systemene som fører til at ulykker er normale. Han skiller mellom kompleks og lineær interaksjon, og mellom tette og løse koplinger. Dette handler om hvordan ulike deler i systemet er koblet sammen og hvordan de samhandler, og hvor mye slakk det er i systemet. Systemer med tett kopling og høy grad av kompleksitet, slik som høyteknologiske systemer, vil oppleve ulykker under normal drift (Perrow, 1984, s. 72). Komplekse interaksjoner åpner for uventede feil, samtidig som tette koplinger kan føre til at det eskalerer, som videre fører til manglende kontroll og manglende evne til å forstå hva som skjer. En endring i hvor tett koblet og hvor komplekst systemet er, vil redusere risikoen for katastrofale feil. Redundans kan ofte være en løsning på å redusere risiko for katastrofale feil, men det må være designet inn i systemet på forhånd, og ikke etter at risikoen for ulykke er oppdaget og kjent. Det kan ofte gjøre vondt verre, da ulykken blir vanskeligere å forutse selv

om en har innført tiltak som var ment for å redusere risikoen etter at den ble oppdaget (Perrow, 1984, s. 368).



Figur 3. Klassifisering av systemer som kategoriseres etter koplinger og interaksjoner (Perrow, 1984, s. 97).

Figur 3 viser hvordan Perrow (1984) kategoriserer ulike systemer, fra lineær til kompleks interaksjon, og fra løs til tett kopling. Ifølge Perrow (1984) er det systemene som er plassert i øverste høyre hjørne, slik som atomkraftverk, som er mest utsatt for normale ulykker. De systemene som er plassert i figur 3 er i noen grad utdatert i og med at figuren ble laget på 80-tallet. Det digitale spekteret er ikke tatt med i betraktning når Perrow (1984) plasserte de ulike systemene i figuren, da digitale løsninger ikke dominerte i like stor grad da som nå. I dag kan en hel del nye systemer plasseres i figuren. Kraftsektoren, luftransportsektoren, vann- og avløpssektoren og olje- og gassektoren, kan alle plasseres inn i denne figuren i og med at alle kategoriseres som kritisk infrastruktur. Dette vil automatisk føre til en grad av tett kopling, og en grad av kompleks interaksjon, grunnet relasjoner på kryss og tvers av ulike infrastrukturer. Faraj et al. (2021) påpeker også hvordan den tette koblingen i systemer øker sannsynligheten for at feil blir forplantet til andre systemer og dermed forsterket. Dette blir presentert med covid-19 som eksempel og hvordan pandemien har avslørt sårbarheter i digitaliseringen. Resultatet er

dog det samme da sårbarheter ligger ukontrollert ved digitalisering, noe Faraj et al. (2021) også poengtere med å trekke linjer til Perrow (1984) sin forklaring av normale ulykker. En ulykke i en kritisk infrastruktur kan få ringvirkninger i en annen, noe som bidrar til å gjøre det mer kompleks. Dette blir tatt opp igjen i kapittel seks.

High Reliability Organisations (HRO)

Teorien om NAT har et mer pessimistisk syn på systemulykker, hvor det er umulig å designe en organisasjon som kan håndtere kompleks interaksjon og tett kopling. Den konklusjonen ble utfordret av en gruppe forskere som opprettet teorien om HRO (Rosness et al., 2004, s. 29). Teorien om HRO handler om hvordan ulykker, i eksempelvis høyteknologiske systemer, kan forebygges. Høyteknologiske systemer i denne sammenheng kan være i de organisasjoner hvor det meste av driftssystemer foregår via teknologi. De fleste organisasjoner i dag bruker en stor grad av teknologi i sine driftssystemer, og dermed kan teorien om HRO trekke linjer til flere organisasjoner som kan kategoriseres som kritisk infrastruktur. Teorien antyder at kombinasjonen av stabile kognitive prosesser og variasjoner i handlingsmønstre gjør det mulig for en HRO å håndtere uventende hendelser effektivt (Weick et al., 2008, s. 38). Weick et al. (2008) presenterer fem grunnleggende HRO-prinsipper som skal redusere sannsynligheten for svikt som kan føre til katastrofale utfall. I denne oppgaven vil fire av de fem prinsippene bli tatt med videre da de er mest relevante til oppgavens problemstilling. De er som følger:

1. Kontinuerlig fokus på mulige feil, som på sikt kan forhindre at feilene utvikler seg til katastrofale ulykker (Weick et al., 2008, s. 39). Det innebærer at det oppmuntres til rapportering av feil slik at en får mest mulig ut av de oppdagede feilene. Det vil videre føre til kontinuerlige vurderinger og revurderinger av praksis. Dette kan sees i sammenheng med den teknologiske utviklingen hvor en må ha et kontinuerlig fokus på sårbarheter, samtidig som en oppmuntrer til åpen dialog internt og eksternt for å få mest ut av de oppdagede feilene som fører til sårbarheter.
2. Skepsis til å forenkle for mye, da forenklinger øker sannsynligheten for at eventuelle faresignaler kan bli oversett (Weick et al., 2008, s. 41). I en HRO kan forenklinger fører til at sannsynligheten for overraskelser øker ved at det blir mindre oppmerksomhet på uregelmessigheter og dermed vanskeligere å se for seg potensialet for uønskede hendelser. Dette er en kjent problemstilling ved implementering av digitale løsninger, hvor formålet er å forenkle og effektivisere praksis, men som samtidig åpner for faresignaler som er vanskelige å oppdage fordi en ikke vet hva en skal se etter.

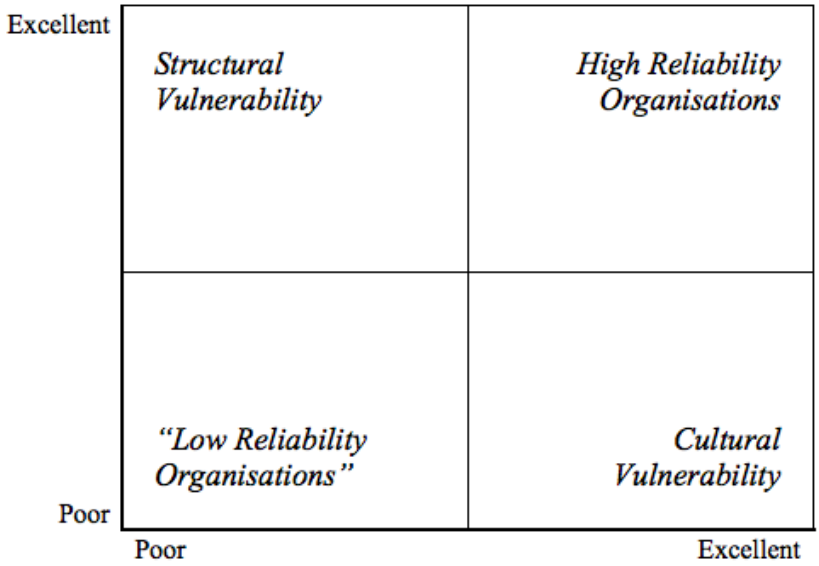
3. Oppmerksomhet på det operasjonelle, som innebærer situasjonsforståelse i den skarpe enden. Feil i den skarpe enden kan føre til katastrofale ulykker hvis det ikke oppdages (Weick et al., 2008, s. 43). Situasjoner må overvåkes i frontlinjen, og informasjon en finner der må videreføres tilbake til ledelsen og omvendt. Det må være et fokus på den nåværende situasjon og forutsetninger, som videre bidrar til et beslutningsgrunnlag. Cyberangrep kan ramme hvor som helst i organisasjonen. Dermed må de i den skarpe enden ha oppmerksomhet på cyberangrep da de har best situasjonsforståelse. Den situasjonsforståelsen må formidles tilbake til ledelsen slik at forebyggende tiltak kan vedtas.
4. Forpliktelse til resiliens handler om evne til å håndtere uventende forstyrrelser uten at en blir satt ut av spill (Weick et al., 2008, s. 46). Det innebærer en forståelse om at uventende hendelser vil oppstå, og at en dermed ikke kan unngå det i sin fulle helhet. I tillegg handler det om en evne til gjenopprettelse etter at forstyrrelsen har manifestert seg. Det er vanskelig å kunne motstå et cyberangrep. Dermed kan en bruke ressurser på å bygge seg såpass robust at konsekvensene kan bli mindre. Dette ved å gjennomføre gode risikovurderinger, ha øvelser, gode beredskapsplaner og lære av andre. Det er noen eksempler som kan bidrar til å være resilient i møte med et cyberangrep.
5. Fleksibilitet av strukturer, som vil si at beslutninger kan fattes uavhengig av den formelle hierarkiske strukturen, men heller basert på ekspertise og erfaringer (Weick et al., 2008, s. 49). Det kan sees i sammenheng med punkt tre hvor det må være en oppmerksomhet på den skarpe enden. Ofte er det de i den skarpe enden som har best ekspertise og erfaring til å forstå situasjonen, dermed kan det være lønnsomt å desentralisere beslutningsmyndigheten til det feltet. Da ser en bort i fra rangering og posisjon, og fokuserer heller på ekspertise. Systemoperatører er som regel først på å merke når systemet ikke virker som det skal, dermed må operatørene ha myndighet til å ta en beslutning, samt ha fått trening på å håndtere slikt. Eksempelvis dersom en operatør ser at systemet er komprimert av en inntrenger, må vedkommende ha myndighet til å stenge systemet inntil problemet er under kontroll.

Disse grunnleggende prinsippene har fokus på feil fremfor suksess, som gir en tilstand av oppmerksomhet. Denne oppmerksomheten gjør at en er kontinuerlig på jakt etter avvik som sammen med andre avvik kan føre til katastrofale ulykker (Weick et al., 2008, s. 61). Dette forklarer Weick og Sutcliffe (2007) med begrepet «mindfulness» som oppnås gjennom de fem prinsippene. De tre første prinsippene handler om forventningene om det uventede, mens de to

siste prinsippene handler om kapasitet til å tåle uventede hendelser (Weick & Sutcliffe, 2007, s. 9). De fem prinsippene vil dermed redusere sannsynligheten for svikt basert på arbeidet med å oppdage og kontrollere uventende hendelser som kan oppstå hvor som helst i organisasjonen. Med et slikt fokus kan en være forberedt på hendelser en aldri har erfart før. Grunntanken i teorien om HRO handler om at god planlegging vil gi et sikrere system og en sikrere organisasjon, slik at det uunngåelige forblir uunngåelig (Hollnagel, 2017).

Redundante løsninger

I motsetning til teorien om NAT, legger teorien om HRO stor vekt på redundante løsninger. Som nevnt tidligere, legger teorien om NAT vekt på at redundante løsninger kan gjøre vondt verre hvis de ikke blir opprettet på riktig måte og på riktig tidspunkt, mens teorien om HRO mener at det uansett kan gjøre et system sterkere. Rosness et al. (2004) presenterer organisatorisk redundans for å kunne bygge et pålitelig system fra mindre pålitelige komponenter. Det blir oppnådd ved å bygge inn ekstra komponenter som trer i kraft når de opprinnelige komponentene svikter, og dermed blir feilen som oppstår rettet på (Rosness et al., 2004, s. 29). Videre blir det presentert to dimensjoner av organisatorisk redundans. Den ene dimensjonen er kulturell dimensjon, og det handler om evne og vilje til å utveksle informasjon, gi tilbakemeldinger og revurdere beslutninger som en selv eller kollegaer har kommet med. Den andre dimensjonen er strukturell dimensjon, som innebærer muligheten for direkte observasjon, overlappende kompetanse, oppgaver eller ansvar (Rosness et al., 2004, s. 30-31).



Figur 4. Oversikt over kulturell dimensjon (Y-akse) og strukturell dimensjon (X-akse) (Rosness et al., 2004, s. 31).

Figur 4 viser de ulike dimensjonene fra utmerket til svake utfall. HROer er plassert under utmerket kulturell- og strukturell dimensjon hvor det både er evne og vilje til å utveksle informasjon, gi tilbakemeldinger og revurdere beslutninger, samt ha overlappende kompetanse, oppgaver og/eller ansvar. Innenfor digitalisering vil den kulturelle dimensjonen innebære at en har en åpen dialog, både internt og eksternt, om problemstillinger rundt digitalisering for å komme med gode beslutninger om forebyggende tiltak. Samtidig må en ha en forståelse for at trusselbildet er dynamisk, derfor må beslutninger revurderes kontinuerlig. I den strukturelle dimensjonen vil det være viktig å sørge for redundante løsninger slik at konsekvensene ved et cyberangrep blir mindre, ved for eksempel overlappende kompetanse, oppgaver og ansvar.

Resiliens

Resiliens handler om å være motstandsdyktig nok til å gjenopprette sin opprinnelige form etter å ha blitt utsatt for en ytre påkjenning (Kongsvik et al., 2018, s. 88). Resiliens skiller seg litt fra teorien om HRO ved at en heller vil være robust nok til å håndtere uventede hendelser i det daglige, fremfor å unngå slike hendelser helt (Hollnagel, 2017, s. 401). En resilient organisasjon fungerer som den skal både under normale og unormale forhold. Det kan trekkes paralleller mellom fokuset til en HRO og en resilient organisasjon, ved at organisasjonen skal fungere som den skal under alle forhold, og at ulykker ikke skal lamme dem. Løsningene til dette er derimot ulike. Mens teorien om HRO vil unngå ulykker i sin helhet, og streber etter å oppdage dem før dem skjer, «aksepterer» resiliente organisasjoner at ulykker skjer, men arbeider for å være robuste nok til å håndtere dem (Hollnagel, 2017, s. 402). Organisasjonen må gjøre mer enn å kun beskytte seg selv. Hollnagel legger frem fire grunnleggende egenskaper innenfor resiliente systemer (Hollnagel, 2017, s. 402; Kongsvik et al., 2018, s. 89):

- Evne til å respondere på forstyrrelser basert på kapasitet og ressurser
- Evne til å overvåke hvor en leter aktivt etter tegn på hva som kan skje
- Evne til å lære basert på erfaringer
- Evne til å forutse basert på forståelse av situasjonen

Resiliente systemer har da, i følge Hollnagel (2017), evne til å oppdage feil, og samtidig være robuste og motstandsdyktige til å håndtere feilene uten at systemet blir satt ut av spill.

Vogus og Sutcliffe (2007) definerer resiliens som et vedlikehold av positiv tilpasning under utfordrende forhold slik at organisasjonen kommer ut av de forholdene mer styrket og ressurssterke. I denne sammenhengen kan utfordrende forhold inkludere diskrete feil, skandaler, kriser og sjokk, forstyrrelser i rutiner, samt pågående risiko, stress og belastninger

(Vogus & Sutcliffe, 2007, s. 3418). Det vil si at organisasjonen skal komme styrket ut av enhver situasjon, alt i fra en unormal forstyrrelse til en krise. Å være resilient vil si å være forberedt på motgang som i sin tur krever en forbedring av kapasiteten som ligger til grunn, ved å lære og handle uten å vite i forkant hva som venter (Vogus & Sutcliffe, 2007, s. 3418). Det er to spesifikke forestillinger i resiliente organisasjoner. For det første behandler organisasjonene suksess lett, og er nysgjerrig på potensialet for det uventede. Det vil si at de resiliente organisasjonene er innforstått med at deres risikomodell trenger jevnlig oppdatering, beredskapen er ufullstendig, og deres forståelse av en sikker drift er skjør. Den andre forestillingen går ut på at resiliente organisasjoner har troen på at de kan takle et bredt spekter av uregelmessigheter, og at de kontinuerlig jobber for å utvide deres evner til å takle det. Det vil si at organisasjonene er klar over at de ikke er perfekte, men streber etter å kunne bli perfekt over en tid med lærdom fra hendelser og nesten-hendelser (Vogus & Sutcliffe, 2007, s. 3419).

I tillegg til Hollnagel (2017) og Vogus og Sutcliffe (2007) sine forståelser av resiliens, vektlegger Woods (2015, s. 6-8) fire konsepter for resiliens:

- Evne til å komme tilbake til en normaltilstand etter en forstyrrende hendelse.
- Evne til å tåle forstyrrelser.
- Evne til å håndtere hendelser som kommer som en overraskelse.
- Evne til å produsere vedvarende tilpasningsevner over lengre tid.

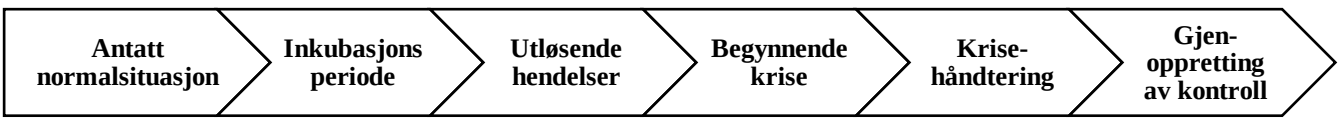
Det Hollnagel (2017), Vogus og Sutcliffe (2007) og Woods (2015) har til felles når det gjelder forståelsen rundt resiliente organisasjoner, er at det allerede foreligger en aksept for at en vil oppleve en forstyrrelse i en slags form, og at en streber etter en evne til å være robuste nok til å tåle forstyrrelsen. Det foreligger også en evne til å lære, hvor en alltid streber etter å bli bedre. Det er i tråd med oppfattelsen om at trusler er dynamiske, derfor må en arbeide dynamisk for å kunne håndtere det. Med et slikt fokus vil en på sikt utarbeide evner til å kunne tenke fremover og tilpasse seg deretter.

Man-Made Disaster (MMD)

Teorien om HRO legger vekt på hvorfor det går godt, mens teorien om MMD legger på vekt på hvorfor det går galt. Dermed kan denne teorien ses på som en kontrast av HRO-teorien. Teorien MMD ble opprettet av Barry Turner, og det enkle budskapet er at til tross for de beste intensjonene fra alle involverte, så kan målet om sikker drift av teknologiske systemer bli overkjørt av «normale» prosesser som oppstår i organisasjonen (Pidgeon & O´Leary, 2000, s.

16). Teorien om MMD ser på ulykker som et resultat av sammenbrudd i informasjonsflyten (Rosness et al., 2004, s. 37). Det er ofte flere årsaksfaktorer som ligger til grunn for en hendelse, men som ikke blir oppdaget før det er for sent. I ettertid av en hendelse kan en finne tegn eller informasjon som kunne indikere at noe var i ferd med å skje, men som det ikke ble tatt hensyn til. Det går under begrepet «informasjonssvikt», og kan foregå på fire ulike måter (Kongsvik et al., 2018, s. 81-82):

1. Informasjonen er fullstendig ukjent fordi den peker mot hendelser som aldri har inntruffet tidligere, og som en derfor heller ikke er oppmerksom på. Dette var nok et faktum når cyberangrep kom på agendaen hvor en ikke hadde erfart slike typer angrep tidligere, men måtte begynne å ta stilling til det.
2. Relevant informasjon er tilgjengelig, men blir oversett, for eksempel på grunn av høyt arbeidspress eller manglende sikkerhetsfokus. Manglende sikkerhetsfokus rundt det digitale kombinert med manglende forståelse av konseptet, gjør at en ikke får med seg relevant informasjon.
3. Informasjonselementer som sammenlagt indikerer at noe er i ferd med å utvikle seg, blir ikke kombinert eller sett i sammenheng. Et eksempel på dette kan være at en ikke ser sammenheng mellom å åpne eposter på arbeidsplassen, og at phishing-eposter kan være en inngangsport for hackere.
4. Informasjonen er tilgjengelig, men passer ikke inn i eksisterende fortolkningsrammer og blir derfor misforstått eller neglisjert. Dette kan sees i sammenheng med IT-avdelingers kompetanse rundt cybersikkerhet, men at det ikke har blitt tatt stilling til av resten av organisasjonen før cyberangrep ble satt på agendaen. Dermed har fokus rundt cybersikkerhet blitt neglisjert fordi en ikke har forstått alvoret. Årlige trusselvurderinger fra eksempelvis PST og NSM har bidratt til å få informasjonen til å passe inn i de eksisterende fortolkningsrammer.



Figur 5. Faser i MMD-modellen (Kongsvik et al, 2018, s. 82).

Modellen viser de ulike fasene i MMD, hvor første fase er normalsituasjonen hvor alt fungerer. I inkubasjonsperioden blir det utviklet én eller flere svakheter som ikke blir fanget opp i organisasjonen og det kan foregå misoppfatninger av faresignaler. Eksempel på en slik svakhet

er at en ansatt mottar en phishing-epost og åpner den. Hvis noen tar grep i signalene, kan det føre til «the decoy phenomen», som på norsk kan kalles lokkefenomenet. Det dreier seg om et tiltak som er tatt for å håndtere et oppfattet problem, men som en i ettertid ser var en distraksjon fra det aktuelle problemet som forårsaket en ulykkeshendelse. Lokkefenomenet tar oppmerksomheten bort fra de ekte faresignalene (Rosness et al., 2004, s. 37). Ved phishing-eksemplet kan det være at angriperen har forfalsket en epost som viser til informasjon som kunne vært reelt. Da blir mottaker oppmerksom og tenker seg ikke om før en går videre med eposten. Da «biter en på» distraksjonen til det aktuelle problemet, som i dette tilfellet er inngangsport til cyberangrep. I tredje fase skjer det noe som setter i gang en ulykkesskapende prosess, som utvikles til en krise hvis det ikke fanges opp (fjerde fase). I femte fase har hendelsen skjedd og må håndteres, og i sjette fase er hendelsen taklet og gjenopprettelse/oppbygging foregår sammen med eventuell læring og regulering (Kongsvik et al., 2018, s. 82). MMD-modellen går tilbake til rotårsakene for en ulykke i inkubasjonsperioden, og ser da på mangelen på informasjonen og misforståelser blant individene. I eksemplet med phishing-epost ville en da funnet ut at organisasjonen må informere og bevisstgjøre de ansatte om konseptet phishing. Utviklingen til ulykken må bli sett på som en prosess slik figur 5 presenterer (Rosness et al., 2004, s. 37).

Kultur for behandling av informasjon

Westrum (1993) har formulert begrepet «requisite imagination» som på norsk kan forklares som tilstrekkelig forestillingsevne. Dette begrepet kan trekkes linjer til MMD med tanke på at for å kunne legge merke til og håndtere informasjonen om mulige farer på en tilstrekkelig måte, må en være i stand til å forestille seg både hva som kan gå galt, og hvordan sammenhengene mellom årsaker og virkninger er. Det kan forklares som oppskriften på hvordan en skal kartlegge hvilken type informasjonssvikt det er, og hva en bør justere, samt hva en kan forvente. Det er vanskelig å forberede seg på, eller forestille seg noe en aldri har tenkt kunne skje, eller som aldri har skjedd tidligere (Kongsvik et al., 2018, s. 82). Organisasjoner må dermed oppmuntre individer og grupper til å observere, spørre, lage konklusjoner og gjøre dem kjent, innenfor viktige aspekter av systemet og for å aktivt gjøre ledelsen oppmerksom på dem. I tillegg må organisasjoner oppmuntre til åpenhet om tanker slik at avgjørelser blir tatt med full anerkjennelse av hva som kan være konsekvensene (Westrum, 1993, s. 402). For eksempel må organisasjoner være åpne rundt problemstillinger knyttet til cyberangrep da det er et fenomen som kan ramme på kryss og tvers av sektorer og landegrenser. På den måten kan en få mer informasjon og forståelse rundt konsekvenser enn hvis en holdt det for seg selv. Dermed har

organisasjoner muligheten til å bruke informasjonen, observasjoner og idéer innenfor systemet uten å ta hensyn til status og rangering til individet eller gruppen som kommer med det. For å kunne bruke det, må informasjonen bli oppdaget. Hvor godt denne informasjonsdelingen foregår blir knyttet opp til tre måter; patologiske, byråkratiske og generative måter (Westrum, 1993, s. 402).

	Patologiske	**Byråkratiske**	**Generative**
Ny informasjon	Vil ikke vite	Behøver ikke å finne ut	Søker aktivt etter informasjon
Budbringere	Budbringere blir skutt	Budbringere lyttes til dersom de dukker opp	Budbringere trenes
Ansvar	Ingen tar ansvar	Ansvar lagt til bestemte roller	Ansvar deles
Brobygging mellom enheter	Brobygging aksepteres ikke	Brobygging tillates, men informasjon blir oversett	Brobygging oppmuntres
Behandling av feil	Feil blir straffet eller skjult	Feilhandlinger vurderes rettferdig	Kontinuerlige vurderinger og endringer
Nye ideer	Nye ideer blir aktivt motarbeidet	Nye ideer presenterer problemer	Nye ideer ønskes velkommen

Tabell 1. Ulike kulturer for behandling av informasjon (Westrum, 1993, s. 402 i Kongsvik et al., 2018, s. 83).

Tabell 1 viser til kulturen innad i organisasjonen, og kan illustreres med hvordan en organisasjon bygger opp beredskap for et cyberangrep. Følger organisasjonen med på nyhetsbildet, trekker erfaringer fra andre lignende hendelser, jobber kontinuerlig med cybersikkerhet med andre aktører og inkludere hele bedriften i risikovurderinger, kan det trekkes linjer til en generativ kultur. Er ikke organisasjon villig til, eller har mulighet til, å prioritere cybersikkerhet på bakgrunn av eksempelvis mangel på ressurser og kunnskap, kan det trekkes linjer til en patologisk/byråkratisk kultur. Tar organisasjonen hensyn til cybersikkerheten, men kun konsentrert rundt en gruppe individer i for eksempel en avdeling som er adskilt fra resten av organisasjonen, kan det trekkes linjer til en byråkratisk kultur hvor ansvaret er lagt til bestemte roller, hvor en dermed ikke går utover de grensene. Samme gjelder det hvis en konstant holder seg til gamle rutiner og ikke vil oppdatere systemet. Da har en holdninger om at nye idéer fører til problemer, og at en tror det ikke er nødvendig å finne relevant informasjon.

Beredskapsplan som fantasidokument

Beredskapsplanlegging er et viktig verktøy som bør ligge til grunn når en kartlegger sikkerheten i en organisasjon. Det er dermed ikke en selvfølge at enhver beredskapsplan vil bidra til en positiv utvikling. Den kan bidra til misforståelser rundt faresignaler ved at den organisatoriske beredskapsplanleggingen bidrar til en beredskapsplan som heller kan forklares som et fantasidokument (Rosness et al., 2004, s. 39). Da vil organisasjonen tror blindt på fantasidokumentet, hvor erfaringer som kunne bidratt til å vise til at planen er unøyaktig blir ignorert. Det kan være at mange ulykker ikke allerede er dekket i planen, og hvis en ikke har øynene åpne for det så blir beredskapsplanen nettopp et fantasidokument. Da mister en oppmerksomheten til endringer og nye trusler som har oppstått i mellomtiden. Gjennom den pågående planleggingsprosessen kan dermed sårbarheter bli kartlagt, hvor en deretter implementerer det i beredskapsplanleggingen som videre gir en mer treffsikker beredskap (Perry & Lindell, 2003, s. 348).

Perry og Lindell (2003) har presentert ti retningslinjer for beredskapsplanlegging. Videre nevner de at en av de viktigste grunnegenskapen i effektiv beredskapsplanlegging er at det er en kontinuerlig prosess. Ingen effektiv plan er statisk. Det må forventes at planen må forbedres etter hver hendelse og etter trening og øvelser (Perry & Lindell, 2003, s. 346). Det kan knyttes opp til en generativ kultur (se tabell 1) hvor en arbeider aktivt med å hente inn informasjon, bygger broer med andre aktører som blir involvert i krisehåndteringen, ha kontinuerlige endringer og vurderinger, med mer. Cyberkulturen er i stadig endring, dermed må en være proaktiv med trening og øvelser, samt oppdatere planen alt ettersom. Trusselen er dynamisk, dermed må planen også være dynamisk, og ikke et fantasidokument.

Egenskaper for å håndtere informasjonsproblematikk

Woods (2006 i Kongsvik et al., 2018, s. 83) sier at en organisasjon som skal håndtere informasjonsproblematikken, må utvikle noen sentrale egenskaper som uavhengighet og involvering, og å være både informert og informativ. Uavhengighet handler om at organisasjonen oppmuntrer til selvstendige vurderinger, og at en kan utfordre konvensjonelle antagelser om risiko og sikkerhet, også oppover i organisasjonshierakiet. Det kan eksempelvis dreie seg om at ansatte innad i organisasjonen har en generativ kultur (se tabell 1). Involvering innebærer konstruktivt engasjement med tanke på både daglig drift og beslutningsprosesser. Det viser til at det er lik kultur i daglig drift og under beslutningsprosesser. Å være informert handler om at ansatte forstår hva som skjer, og vurderer denne informasjonen fortløpende, da

de er inkludert og oppdatert på hele sikkerhetsbildet. Å være informativ handler om hvordan organisasjonen benytter tilgjengelig informasjon for å vurdere og forbedre måten ting gjøres på, ved å for eksempel følge med på nyhetsbildet og trekke erfaringer fra andre hendelser. Dette viser til at en organisasjon ikke vil oppleve en MMD hvis de har disse sentrale egenskapene i grunn.

3.2 Oppsummering av teori

I dette kapitlet er oppgavens teoretiske rammeverk redegjort for. Innledningsvis i kapitlet ble det nevnt at det blir brukt flere teorier som sammen skal bidra til å belyse oppgavens problemstilling og forskningsspørsmål. Teoriene om HRO og MMD kan sees på som kontraster når det gjelder holdningen en har i møte med cyberangrep. En HRO vil arbeide for å unngå dem i sin helhet, mens teorien om MMD ser på hvorfor det går galt, og hva som kan gjøres for å unngå lignende igjen. Funn fra begge teoriene vil bli trukket frem i kapittel seks. Perrow (1984) sin kategorisering av systemer fra teorien om NAT vil også bli trukket frem i kapittel seks for kategorisering av sektorene oppgaven tar utgangspunkt i. Teorien om resiliens vil støtte opp de holdningene sektorene har når det gjelder motstandsdyktighet. Teoretiske bidrag vil bli diskutert om hverandre, da de belyser funn i oppgaven på hver sin måte når det gjelder arbeid rundt sikkerhet i organisasjoner.

4.0 Metode

I dette kapittelet vil oppgavens metodiske fremgangsmåte bli presentert. Valgt design og metode vil bli beskrevet og begrunnet. Deretter vil forskningsprosessen bli tydelig forklart før metodens kvalitetskriterier blir vurdert. Avslutningsvis vil metodens styrker og svakheter bli diskutert.

4.1 Metodisk tilnærming

Forskningsdesign

I et forskningsdesign finnes det ulike forskningsstrategier en kan følge. Strategiene innebærer ulike sett av prosedyrer for å besvare forskningsspørsmålene (Blaikie & Priest, 2019, s. 21). I denne oppgaven blir det brukt dokumentanalyse og intervjuer for å besvare forskningsspørsmålene, noe som gjør at empirien leder arbeidet. Deretter ble teori hentet for å gi mening til innhentet data. Denne metoden kan plasseres under abduktiv forskningsstrategi. Blaikie og Priest (2019, s. 22) forklarer at hensikten med abduktiv forskningsstrategi er å forstå det sosiale liv innenfor sosiale aktørers meninger og motiver, gjennom for eksempel intervjuer. Det stemmer overens med forskningen min da jeg er ute etter å intervjue relevante aktører som kan representere sin sektor innenfor temaet beredskap mot cyberangrep. Selve prosessen i en abduktiv forskningsstrategi går ut på å oppdage hverdagslige meninger og motiver fra en informant, hvor teori deretter blir sluttproduktet i forskningen (Blaikie & Priest, 2019, s. 93). Blaikie og Priest (2019) sin fremstilling av abduktiv forskningsstrategi treffer den tilnærmingen jeg har hatt gjennom hele forskningsprosessen, hvor teorien blir spisset etter at all empiri er innhentet slik at teorien ikke leder vei.

Forskningsmetode

I denne oppgaven er det kvalitativ forskningsmetode som ligger til grunn ved bruk av dokumentanalyse og intervjuer. Hensikten med denne metoden er å bruke dokumentanalyse for å bygge opp en kunnskapsbase for å deretter intervjue nøkkelinformanter for å supplere med mer data, samt dekke eventuelle hull. Ved kvalitativ metode er opplegget fleksibelt, og de ulike fasene i forskningsprosessen overlapper hverandre (Halvorsen, 2008, s. 131).

4.2 Forskningsprosess

Oppgaven vil være casebasert, hvor det er noen få undersøkelsesenheter. Formålet er ikke å generalisere, men heller belyse. I dette casestudie er det prosesser om hvordan noe utvikler seg

som er i fokus, samt å utvikle en helhetsforståelse (Halvorsen, 2008, s. 105). Oppgaven tar utgangspunkt i fire selskaper fra ulike sektorer som kan kategoriseres som kritisk infrastruktur. Det blir studert hvordan og hvorfor beredskap mot cyberangrep har utviklet seg gjennom tidene hos dem, og hvordan det foregår i dag. Ingen av selskapene har opplevd et cyberangrep før, men de opplever digitale trusler og har endret praksis deretter. De er dermed relevante å ha med, sammenlignet med andre selskaper som kanskje har opplevd et cyberangrep. Ved å studere de fire selskapene i dybden bidrar de til en helhetsforståelse av hvordan fokuset har endret seg, samt belyser nødvendigheten med å være oppdatert på cybersikkerhet. Formålet med oppgaven er ikke å sammenligne de ulike selskapene, men heller belyse viktige momenter hos hver av dem. Det er i tråd med hva et casestudies mål er, hvor jeg oppnår en grad av helhetsforståelse.

Tabell over forskningsprosess

Når	Aktivitet	Formål	Resultat
Januar	Leste meg opp på temaet og utformet en klar problemstilling, samt forskningsspørsmål. Begynte på en skisse for innledningen. Startet med dokumentanalyse, samt tenkte ut hvordan jeg skulle skaffe informanter.	Ville komme i gang med oppgaven så tidlig som mulig, samt prosessen med å skaffe informanter for å unngå at det ville bli et stressmoment på et senere tidspunkt. Dokumentanalysen skulle skape et kunnskapsfundament for valg av informanter og intervjuspørsmål, samt øke min egen kunnskap om temaet.	Skaffet informanter allerede i uke 3 og 4. Spisset problemstilling og forskningsspørsmål flere ganger før endelig versjon. Dokumentanalysen startet tidlig. Skjelettet til oppgaven ble laget og innledningen ble påbegynt.
Februar	Gjorde ferdig innledning og lagde en skisse på kontekstkapittel. Fortsatte med dokumentanalyse, og noterte meg hvilke teorier som kan være av relevans. Begynte på metodekapittel. Prosessen med å hente inn flere informanter fortsatte.	Ved å gjøre ferdig innledning og kontekstkapittel, vil det gi tydelige føringer på hva jeg faktisk er ute etter.	Resten av informantene ble skaffet i løpet av uke 7. Da fant jeg ut at jeg hadde nok nøkkelinformanter. Første utgave av innledning og kontekstkapitlet ble ferdig, og lagt på vent.

Mars	Lagde intervjuguide og avtalte tidspunkt for intervjuer. Skisserte empirikapittelet, og fylte inn informasjon fra dokumentanalysen. Intervjuet 2/4 selskaper i slutten av måneden. Fylte inn data fra informantene fortløpende i empirikapittel.	Ivrig på å få innhentet så mye empiri som mulig slik at jeg kunne begynne prosessen med teorivalg.	Intervjuguiden ble ferdig, og intervjuer ble planlagt. De ble gjennomført i uke 11, 12, 14 og 15.
April	Gjennomførte siste runde med intervjuer. Skrev ferdig metodekapittel og empirikapittel samtidig som teorikapittel blir spisset. Sendte oppfølgingsspørsmål til informanter, samt avsnitt hvor det refereres til informanter til den respektive informant for «godkjenning».	Formålet med å hente inn all empiri før spissing av teorikapitlet er fordi da vet jeg hva jeg faktisk er ute etter, og jeg unngår at teori legger unødvendige føringer for empiriinnsamling, noe som samsvarer med en abduktiv forskningsstrategi. Å sende avsnittene hvor det refereres til informantene til informanten selv er for å sikre at det ikke er noen misforståelser, samtidig som det gir trygghet for begge parter.	Konkluderte med at jeg ikke trengte flere informanter, og at jeg hadde fått den informasjonen jeg var ute etter. Informantene godkjente teksten, og svarte på mine oppfølgingsspørsmål.
Mai	Ferdigstilte teorikapitlet, og fokuserte på diskusjonskapitlet. Putta på en presentasjonsdel om hver sektor innledningsvis i empirikapitlet slik at leseren får grunnforståelse om hver sektor innenfor temaet. Jobbet parallelt med diskusjonskapitlet og ferdigstilling av empirikapitlet. Skrev konklusjonen.	Fant ut at det var fordelaktig med en presentasjon av hver sektor i empirikapitlet slik at det er lettere å forstå informasjonen om sektorene relatert til hvert forskningsspørsmål. Ved å skrive diskusjonskapittel og ferdigstille empirikapitlet samtidig førte til at det ble lettere å se hvor jeg kan trekke linjer.	I slutten av måneden ble et første utkast av hele oppgaven ferdig.

Juni	Finleste og spisset hele oppgaven, gjennomførte språkvask, dobbeltsjekka referanser, tabeller og figurer.	Forsikret meg om at det er en rød tråd gjennom hele oppgaven, korrekt kildeføring og godt språk.	Oppgaven ble levert 15. juni 2021.

Tabell 2. Oversikt over prosessen i forskningsprosjektet.

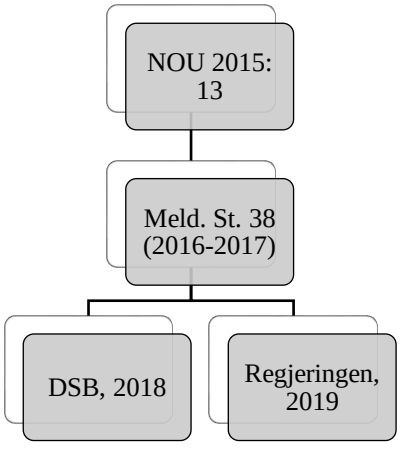
Tabell 2 er en grundig gjennomgang av forskningsprosessen. Den viser at det har vært en dynamisk prosess hvor jeg har gått frem og tilbake mellom ulike deler. Prosessen kan støttes av metodelitteraturen ved at det er en abduktiv forskningsstrategi som vises igjen, ved at empiri har lagt tydelige føringer for det teoretiske rammeverket. Teorikapitlet ble ikke ferdigstilt før etter all empiri var hentet inn.

4.3 Datainnsamling

I denne oppgaven er datainnsamlingen delt i to. Den første delen består av en dokumentanalyse, og den andre delen består av intervjuer. Hvordan de to ulike datainnsamlingene har foregått vil bli videre beskrevet.

Dokumentanalyse

Dokumentanalysen har vært grunnlaget for empiriinnsamlingen. Analysen består av ulike dokumenter slik som nasjonale trusselvurderinger utført av PST, NSM og politiet, NOUer, stortingsmeldinger, nyhetsartikler, forskningsrapporter, og rapporter fra de ulike sektorene angående risiko for cyberkriminalitet. NOU 2015: 13 *digital sårbarhet – sikkert samfunn* har lagt tydelige føringer for hva jeg er ute etter, da den belyser mange viktige momenter innenfor flere sektorer fra 2015, som gir meg mulighet til å se hvordan fokuset har endret seg.



Figur 6. Illustrasjon av NOU 2015: 13 sin betydning i senere arbeid inspirert av NOU 2015: 13, Meld. St. 38 (2016-2017), DSB (2020) og regjeringen (2019).

NOU 2015: 13 har vært et viktig kunnskapsgrunnlag i Meld. St. 38. (2016-2017) *IKT-sikkerhet – et felles ansvar*, som er den første Stortingsmeldingen som omhandler cybersikkerhet. Meld. St. 38 (2016-2017, s. 11) tok en oppfølging av de anbefalingene NOU 2015: 13 kom med angående cybersikkerhet. I 2018 fikk DSB i oppdrag å følge opp NOU 2015: 13 og Meld. St. 38., hvor de skulle etablere et nasjonalt rammeverk for myndighetene til å få en oversikt over digitale verdikjeder, samt en modell for virksomheter slik at de kan få en oversikt over slike verdikjeder selv. Det handlet om en kartleggelse av potensielle ringvirkninger som kan oppstå ved cyberangrep (DSB, 2020, s. 5). Regjeringens nasjonale strategi om digital sikkerhet fra 2019, bygger også videre på informasjon hentet fra NOU 2015: 13 og Meld. St. 38. (Regjeringen, 2019, s. 24). Dette viser at NOU 2015: 13 har vært en god kunnskapsbase og har bidratt til beslutninger tatt i senere tid i ulike rapporter, og kan dermed forsvares som et pålitelig hoveddokument i denne oppgaven, noe figur 6 viser.

Målet med dokumentanalysen har vært å innhente relevante funn om cybersikkerhet, både generelt i landet, men også internt i de ulike sektorene oppgaven tar utgangspunkt i. Dette har ført til en god kunnskapsbase som blir tatt med videre til intervjuene hvor eventuelle hull kan dekkes, samt få direkte uttalelser fra nøkkelinformanter med god kunnskap. Dermed ble det utviklet en generell dokumentanalyse som omhandlet temaet, og en individuell dokumentanalyse til hver sektor jeg studerte.

Grunnen til at dokumentanalysen la føringer for spørsmålene stilt i intervjuene, var for å gjøre intervjuene mer presise og direkte. Dataene fra intervjuene har også supplert dokumentanalysen med informasjon. Beredskap mot cyberangrep er et voksende tema, noe som har vist at informanter har vært interessert i å delta. Intervjuene ble dermed mer faglige og interessante ved at jeg som forsker hadde bygget opp en god grunnforståelse om temaet, basert på dokumentanalysen.

Informanter

I og med at oppgaven tar utgangspunkt i sektorer som kan kategoriseres som kritisk infrastruktur, snevret det noe inn utvalg av informanter. Jeg sendte epost til de selskapene jeg kom på som kan kategoriseres som kritisk infrastruktur. I tillegg tok jeg opp kontakten med bekjentskap som jeg visste jobbet innen et slikt selskap, samt informanter fra tidligere oppgaver gjennomført i studieløpet. I starten ble jeg videresendt fra bekjentskapet videre til de aktuelle nøkkelinformantene, noe som kan forklares som en snøballutvalgsmetode. Det bidrar til at jeg

som forsker får et innpass i et lukket miljø (Halvorsen, 2008, s. 164). På et senere tidspunkt svarte de ulike selskaper på epost. Denne prosessen foregikk relativt smertefritt. Jeg tror grunnen til det er basert på en genuin interesse i temaet hos de fleste informantene. Jeg endte opp med å få informanter fra selskaper som kunne representere kraftsektoren, lufttransportsektoren, vann- og avløpssektoren og olje- og gassektoren.

Informantene mine er nøkkelinformanter som antas å ha særlig god oversikt over og innsikt i de spørsmålene jeg som forsker ønsker å få belyst (Andersen, 2006, s. 279). Informanter og selskaper er anonymisert, og det er kun tilhørende sektor som vil bli presentert. Det er ikke avgjørende for oppgavens formål å inkludere navn på verken selskap eller informant. Etter ønske fra informantene blir heller ikke stillingstittel inkludert. Det var fem informanter som ble intervjuet til oppgaven, fordelt utover de fire selskapene oppgaven tar utgangspunkt i. I kapittel fem vil informantene bli referert som «informant» under tilhørende sektor integrert i tekst og i parentes. På den måten vil det bli en ryddig og oversiktlig presentasjon av data strukturert etter hver sektor. I kapittel seks vil dataene bli tatt med til videre diskusjon, men fremfor å presentere data sektorvis, vil de da bli presentert under paraplybegrepet «kritisk infrastruktur». Kapittel fem bidrar til en grunnforståelse i hver sektor, mens kapittel seks tar et steg tilbake og ser på det helhetlige da problemstillingen omhandler organisasjoner som kan kategoriseres under kritisk infrastruktur. For å støtte mine empiriske funn knyttet til kritisk infrastruktur, er det viktig at hver sektor blir presentert i dybden, basert på mine funn fra dokumentanalyser og intervjuer.

Det kan stilles spørsmål om olje- og gassektoren kan forsvares som kritisk infrastruktur da de ikke er direkte nødvendige for samfunnets kritiske funksjoner. NOU 2015: 13 presenterer sårbarheter i kritiske samfunnsfunksjoner, deriblant olje- og gassektor på lik linje med de andre sektorene. Det forklares med at i de senere år har det vært en økning i digitale trusler rettet mot den sektoren. Sektoren er svært viktig for norsk økonomisk bæreevne og for Norges internasjonale betydning og omdømme som olje- og gassleverandør (NOU 2015: 13, s. 146). Selv om samfunnet for øvrig ikke vil merke et angrep på olje- og gassektoren momentant, så vil det sette preg på Norges økonomi og relasjon til andre land. Dermed konkluderes det med at olje- og gassektoren kan forsvares som kritisk infrastruktur.

Intervjuguide

I forkant av intervjuene ble det utviklet en intervjuguide. Den ble utformet i tråd med oppgavens problemstilling, forskningsspørsmål og dokumentanalyse. Det ble først og fremst tatt utgangspunkt i intervjuguiden under intervjuene, men det var åpent for å stille spørsmål utenom hvis det ble sett på som nødvendig. Intervjuguiden kunne også justeres etter hvert intervju hvis det var behov, noe som kan forklares som semistrukturert intervju hvor det er åpent for fleksibilitet (Halvorsen, 2008, s. 137). Alle informantene fikk tilsendt den samme intervjuguiden sammen med samtykkeskjema i forkant av intervjuene. Jeg så på det som fordelaktig da informantene kunne forberede seg på det jeg håpte var konkrete og spisse nok spørsmål. I tillegg kunne informanten selv se om jeg burde snakke med en ekstra person innad i selskapet, og dermed tipse meg om det. Da blir det videre et strategisk utvalg hvor nøkkelinformanten sender meg videre til en annen nøkkelinformant. Denne metoden kan også kalles for snøballutvalgsmetode (Halvorsen, 2008, s. 164). Det viste seg at det ikke var nødvendig, da nøkkelinformantene satt med den kunnskapen jeg var ute etter.

Intervjuprosess

Semistrukturert intervju er en ofte brukt kvalitativ metode. Det foregår muntlig hvor intervjueren styrer samtalen så lite som mulig. Slike intervjuer er fordelaktig når forskeren vil studere noe som en ellers ikke har mulighet til å observere selv (Halvorsen, 2008, s. 137). I forkant av intervjuene hadde jeg et uforpliktet møte med hvert selskap hvor jeg fortalte om oppgavens tema og hva mine mål med oppgaven var. Deretter kunne selskapet selv avgjøre om de ville delta i studien eller ikke. Det skapte en fortrolighet mellom meg og informanten, noe som gjør det lettere å utføre dybdeintervju (Halvorsen, 2008, s. 138). I og med at alt av møter burde skje digitalt med tanke på covid-19, åpnet det muligheter for meg ved å nå informanter som sitter på kontor i en annen by, fremfor kun informanter som kan nås i Stavanger. Det så jeg på som fordelaktig, da jeg fikk snakke med selskaper plassert forskjellige steder i landet. For å sikre personvern ble data fra intervjuer kun registrert i form av notater underveis i intervjuet.

4.4 Kvalitetskriterier

I dette delkapitlet vil oppgavens kvalitetskriterier bli vurdert. Det handler om reliabilitet, validitet og overførbarhet.

Reliabilitet

Reliabilitet handler om dataens troverdighet og bekreftbarhet (Andersen, 2006, s. 291). Dataene består av både dokumentanalyse og intervjuer, noe som styrker reliabiliteten. Oppgaven tar derimot utgangspunkt i få informanter, noe som kan svekke reliabiliteten. Her bidrar dokumentanalysen til å rettferdiggjør antall informanter slik at oppgavens funn har troverdighet. Jeg som forsker har fått en grunnforståelse basert på flere offentlige dokumenter fra ulike organisasjoner, hvor jeg deretter får dataene bekreftet/avkreftet av nøkkelinformanter. Det gir en styrket reliabilitet til forskningens problemstilling.

Validitet

Validitet forteller oss hvor relevante dataene er for forskningens problemstilling (Halvorsen, 2008, s. 67). Dokumentanalysen består av anerkjente offentlige rapporter, samt artikler fra anerkjente selskaper, media og forskningsplattformer. De dataene ble videre supplert med intervjuer fra nøkkelinformanter. Nøkkelinformanter i denne settingen er de som jobber innenfor cybersikkerhet i sin bedrift, og som har god forståelse om temaet. I tillegg kjenner de sin bedrift godt, og dens utgangspunkt. Denne sammenhengen mellom dokumentanalyse og intervjuer styrker validiteten.

Overførbarhet

Overførbarhet går ut på om funnene kan overføres til andre sammenhenger (Halvorsen, 2008, s. 72). Oppgaven tar utgangspunkt i selskaper som er ansvarlig for drift av kritisk infrastruktur. Dermed er det brukt fire eksempler på slike selskaper som får samme intervjuguide og plass i oppgaven. Det begrenser overførbarheten ved at det kun er fire selskaper fra ulike sektorer som blir presentert, hvor en dermed ikke kan uttale seg om beredskap mot cyberangrep i andre sektorer. Siden det kun er tatt utgangspunkt i et selskap fra én sektor, utelukker det også andre selskaper av ulik størrelse. En kan ikke gå ut ifra at det er samme praksis i flere selskaper under hver sektor. Samtidig ser en at funnene fra sektorene er overførbare til hverandre da det er mye likheter, og dermed kan det påstås at det er en grad av overførbarhet innenfor sektorer som kategoriseres som kritisk infrastruktur, men ikke nok til å fastslå det.

4.5 Styrker og svakheter ved valgt metode

Kvalitativ metode innebærer både styrker og svakheter. En styrke er kombinasjonen med dokumentanalyse og intervjuer. Dokumentanalysen har fungert som en kunnskapsbase, hvor

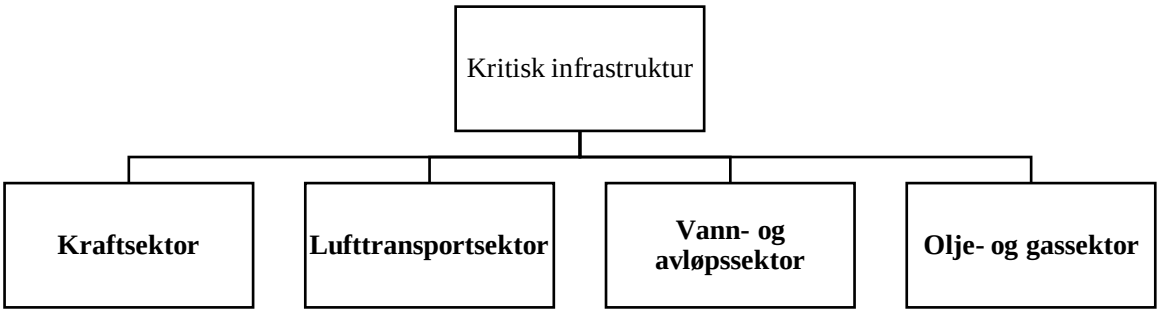
det deretter ble supplert med data fra intervjuer. Intervjuene ble gjennomført semistrukturert, noe som ga rom for at intervjuet foregikk som en faglig samtale. Før intervjuene ble det informert om at anonymitet sto sterkt, noe som både styrket forholdet mellom intervjuer og informant, og muligheten for at informantene ville stille opp. Oppgavens tema og problemstilling vekket en genuin interesse hos informantene, noe som også bidro til at de ville stille til intervju. Som nevnt tidligere, har covid-19 lagt føringer for at all intervju må foregå digitalt. Det har styrket oppgaven ved at jeg kunne nå ut til selskaper som holder til andre steder i landet, og ikke kun lokalt. Før covid-19 var det positivt og vanlig å stille opp til informantenes arbeidsplass, noe som hadde utelukket muligheten for å hente inn informanter fra andre steder da jeg helst skulle forholdt meg til lokale selskaper. Den digitale løsningen fikk meg til å tenke utenfor boksen, og ga meg flere muligheter ved å kontakte et bredere spekter av selskaper. Det betrakter jeg som en styrke i oppgavens empiriske data. I og med at jeg fikk tak i nøkkelinformanter i sine respektive selskaper, så har det også gitt meg god og viktig informasjon. Med en abduktiv forskningsstrategi har det styrket oppgaven ved at jeg er ute etter nøkkelinformantenes egne fortolkninger, som fremstås som svært troverdige.

Svakheter ved oppgavens metode er at det kunne vært ideelt og intervjuet flere selskaper i ulike størrelser innenfor samme sektor for å få en bedre helhetsforståelse av fenomenet. Et lite selskap vil nok ha større problemer med å ha et økt fokus når det gjelder beredskap mot cyberangrep sammenlignet med et stort selskap. Det påvirker også muligheten for å generalisere ved at jeg ikke har intervjuet flere selskaper av ulike størrelse. En annen svakhet ved valgt metode er at informanter kan pynte på sannheten, noe jeg som forsker ikke kan avdekke så lenge jeg forholder meg til noen få informanter. Dette forsvares ved at jeg ikke har som mål om å generalisere mine funn, dermed vil det ikke være et avgjørende faktum. Samtidig spiller dokumentanalysen inn og intervjuer med andre informanter, da det er en indikator på om informasjonen samstemmer eller ikke. Ellers kunne det vært interessant med metodetriangulering, hvor det blir foretatt både kvantitativ og kvalitativ metode (Halvorsen, 2008, s. 149). Da kunne jeg beholdt dybdeintervju med nøkkelinformanter, men også hatt en undersøkelse for å få inn data fra flere arbeidere i samme selskap.

Til tross for svakhetene med valgt metode så er det den mest egnede til dette forskningsprosjektet. Kvalitativ- og abduktiv metode har bidratt til at jeg kunne veksle mellom empiri og teori, som er en styrke for oppgaven i sin helhet.

5.0 Empiri

I dette kapitlet vil resultater fra datamaterialet bli presentert. Datamaterialet består av dokumentanalyser og intervjuer. Kapitlet er strukturert etter forskningsspørsmålene hvor det blir gjennomgang av hvert selskap under tilhørende sektor. Selskapene vil videre bli referert som den sektoren de tilhører. Hensikten med det er for å forenkle fremstillingen. Innledningsvis vil hver sektor bli presentert med hva som gjør de kritiske, relasjoner til andre kritiske infrastrukturer, og hvordan digitaliseringen ser ut hos dem. Etter hvert forskningsspørsmål vil det være en kort oppsummering. Avslutningsvis vil det være en oppsummering av hovedfunn fra hele kapitlet.



Figur 7. Illustrasjon av oppsett i kapittel med fokus på hver sektor. Det som er uthevet er i fokus.

5.1 Presentasjon

I dette delkapitlet vil hver sektor bli presentert med hva som gjør dem kritisk, hvordan digitaliseringen ser ut hos dem, og relasjoner til andre sektorer. Hva bruker de digitale systemer til? Og hva har det eventuelt erstattet? Tabell 3 gir en oversikt over relasjonene sektorene har.

Sektor	**Relasjon**
Kraftsektoren	Elektronisk kommunikasjon & Satellittbaserte tjenester
Lufttransportsektoren	Elektronisk kommunikasjon & Satellittbaserte tjenester
Vann- og avløpssektoren	Kraftsektor & Elektronisk kommunikasjon
Olje- og gassektoren	Kraftsektor, Elektronisk kommunikasjon & Satellittbaserte tjenester

Tabell 3. Oversikt over relasjoner til andre sektorer inspirert av NOU 2015: 13.

Tabellen viser at det ikke nødvendigvis er noen stor relasjon mellom sektorene denne oppgaven tar utgangspunkt i, utenom to relasjoner til kraftsektoren. Elektronisk kommunikasjon (heretter EKOM) og satellittbaserte tjenester går igjen hos de fleste. Derfor er de tatt med i oversikten slik at en får kartlagt hvilke relasjoner som er viktige å ha med i betraktning når en skal vurdere

trusselbildet, foreta risikovurderinger, samt lage beredskapsplan. EKOM og satellittbaserte tjenester er infrastrukturer som også har vokst frem og blitt større i lys av digitaliseringen grunnet deres funksjon, noe som kan sees på som et interessant funn med tanke på relasjoner og avhengighet.

Kraftsektoren

Kraftsektoren består av selskaper som driver med energiforsyning. Svikt i kraftsektoren som berører forsyningen av elektrisk kraft vil gi konsekvenser for alle samfunnssektorer, inkludert digitale systemer som samfunnet er avhengige av (NOU 2015: 13, s. 129). Grunnen til det er fordi de aller fleste avhenger av elektrisk kraft for å utføre nødvendig arbeid. Det betyr at det foreligger en tett relasjon mellom kraftsektoren og andre sektorer, noe tabell 3 viser. Kritiske infrastrukturer og samfunnsfunksjoner er avhengig av en stabil energiforsyning fra kraftsektoren. Den økte digitaliseringen gjør avhengigheten til kraftsektoren enda større, derfor stilles det større krav til kraftsektoren angående cybersikkerhet, da svekkelser kan føre til store ringvirkninger (NOU 2015: 13, s. 143).

Digitalisering i kraftsektoren innebærer blant annet IKT-systemer for å understøtte drift, samt overvåke og fjernstyre anleggene i energiforsyningen (NOU 2015: 13, s. 129). Dette kan også forklares som SCADA-systemer, som innebærer de driftssystemer som har blitt digitalisert (NOU 2015: 13, s. 41). Videre i oppgaven vil SCADA-systemer bli brukt som en generell betegnelse for driftssystemer som har blitt digitalisert. Dette fører til at IKT er en svært viktig og integrert del i dagens drift av energiforsyning. Det som tidligere var systemer som var uavhengige av andre IKT-systemer, er nå svært avhengige. Dette er forårsaket av å kunne tilfredsstille samfunnets krav til en effektiv drift av energiforsyning (NOU 2015: 13, s. 129). Hva er ulempen med å være avhengig av IKT-systemer? Den økte digitaliseringen og den tette sammenkoblingen av systemer og nettverk medfører at systemene er mer komplekse, og det kan være vanskelig å ha full oversikt. Har en ikke full oversikt, så har en heller ikke god nok kunnskap om hvordan samhandlingen mellom de ulike systemene fungerer. Dette fører til en økt risiko for teknisk feil, menneskelig svikt og uautorisert inntrenging i systemene (NOU 2015: 13, s. 136).

Lufttransportsektoren

NOU 2015: 13 presenterer transportsektoren med fire transportgreiner; luftfart, sjøtransport, veitrafikk og jernbane. Rapporten behandler transportgreinene på et overordnet nivå. Transportsektoren er kritisk for samfunnet da det er bindeleddet mellom a og b for mennesker og gods. IKT-systemer i transportsektoren (derav lufttransportsektoren) har effektivisert informasjonsflyten betydelig. Alle enheter i infrastrukturen under luftransportsektoren er avhengig av et fungerende kommunikasjonssystem for å kunne levere en sikker og effektiv tjeneste til passasjerene (NOU 2015: 13, s. 206). Det fører også til at sårbarheten blir større, ettersom det er en kritisk avhengighet av EKOM og satellittbaserte tjenester, hvor bortfall i de tjenestene vil redusere kapasiteten og effektiviteten betydelig (NOU 2015: 13, s. 201). Luftfart er en global industri, noe som krever at en må forholde seg til internasjonale regler og standarder innenfor for eksempel krav til cybersikkerhet. Det kan øke kompleksiteten.

Vann- og avløpssektoren

Vann- og avløpssektoren forsyner samfunnet med rent vann, samt håndterer avløpsvannet. De to systemene henger sammen da avløpssystemet er avhengig av vann, hvor svikt i vannforsyning vil føre til svikt i avløpssystemet (NOU 2015: 13, s. 159). Digitaliseringen i vann- og avløpssektoren handler om en økende bruk av SCADA-systemer, hvor en får bedre overvåking og styring, som videre fører til økt effektivisering, pålitelighet og produktivitet (NOU 2015: 13, s. 159). Derfor er sektoren avhengig av stabile og sikre digitale systemer da digitale sårbarheter vokser i takt med digitale løsninger (Vaforum, 2018). Det gjør at vann- og avløpssektoren er sårbar overfor svikt i de kritiske infrastrukturene kraftsektor og EKOM (se tabell 3). Et eksempel på et utfall hvor det er svikt i SCADA-systemer, kan være at noen bevisst har manipulert pumpestasjoner, ventiler og luker som videre fører til at en million liter ubehandlet avløpsvann renner ut i de nærliggende vassdragene (NOU 2015: 13, s. 161).

Olje- og gassektoren

Som nevnt tidligere (se delkapittel 4.3) er olje- og gassektoren en svært viktig sektor for Norge. Olje- og gassektoren har ført til at Norge har blitt et av verdens rikeste land, og setter oss på kartet i den internasjonale arena. Sikkerheten i olje- og gassektoren er for svak med tanke på viktigheten anlegg på norsk sokkel har for norsk økonomisk bæreevne, og for Norges internasjonale betydning og omdømme som olje- og gassleverandør. Det er ikke kun Norge selv som kan bli rammet, men også Norges kunder i utlandet. Anlegg på norsk sokkel har

betydning for vitale samfunnsinteresser og rikets sikkerhet, og derfor kan det ikke utelukkes at alvorlige hendelser kan inntreffe i fremtiden (NOU 2015: 13, s. 156-157).

Sektoren består av en omfattende infrastruktur, hvor en må sørge for en viss sanntidskommunikasjon mellom ulike deler av infrastruktur, både på land og på hav (NOU 2015: 13, s. 146). Den digitale trusselen mot sektoren innebærer blant annet innbrudd og integritetsangrep på SCADA-systemene. Når en kobler sammen SCADA-systemer med andre IKT-systemer over internett, vil det øke risikoen for angrep (NOU 2015: 13, s. 149). Tidligere var det vanlig å isolere ulike områder i systemene. Med et behov for overføring av data fra et system til et annet, i tillegg til fjernstyring, er det ikke lenger mulig med en full separasjon. Med en økende bruk av fjernstyring fra andre plattformer eller fra land, kreves det et felles kommunikasjonssystem og produksjonsutstyr som dermed kan være eksponert for IKT-sårbarheter (NOU 2015: 13, s. 150). Digitaliseringen har forbedret bindeleddet mellom hav og land, og muligheten for å styre systemene fra land, men det medbringer også sårbarheter. Relasjoner til andre sektorer er også en sårbarhet, hvor olje- og gassektoren er avhengig av blant annet kraftsektoren, EKOM og satellittbaserte tjenester (se tabell 3).

Oppsummert

Hver sektor har endret store deler av driftssystemet sitt til å være digitalisert for å øke produktivitet og effektivitet. Slike driftssystemer kalles også for SCADA-systemer. I lufttransportsektoren er det større fokus på digitale kommunikasjonssystemer enn SCADA-systemer. Det oppstår nye og flere sårbarheter ved denne digitaliseringen. I tillegg har hver sektor en relasjon til en annen sektor, hvor EKOM går igjen hos alle. Dette er faktorer som bidrar til større sårbarhet innenfor cybersikkerhet, som også bekrefter at digitale problemer er tverrsektorielle. Dette blir støttet av regjeringens nasjonale strategi, hvor målet er at kritiske samfunnsfunksjoner skal ha en robust og pålitelig digital infrastruktur hvor samarbeid også må stå sterkt (Regjeringen, 2019, s. 7).

5.2 Hvordan har truslene endret seg?

De siste årene har trusselbildet endret seg hos virksomheter, noe som har ført til at cyberangrep har fått en større plass i risikovurderinger og beredskapsplanlegging. Hva kan være grunnen til det? Videre vil de fire selskapene under tilhørende sektor bli presentert med deres oppfattelse av hvordan truslene har endret seg, hva de innebærer og hvordan deres worst-case scenario ser

ut. Det er verdt å nevne at ingen av selskapene som informantene representerer har blitt rammet av et alvorlig cyberangrep.

Kraftsektoren

Innenfor kraftsektoren har systemer som tidligere har eksistert bak lukkede nettverk, blitt koblet til internett for høyere tilgjengelighet, funksjonalitet og effektivitet, noe som påvirker trusselbildet i stor grad. Vellykkede cyberangrep på kraftsektoren er nå uunngåelige (Bratnes, 2020). Grunnen til det kan være fordi en ikke klarer å holde samme fart som utviklingen i trusselbildet. I kraftsektoren kunne informanten bekrefte at teknologiutviklingen har ført til nye løsninger som fører til effektivitet, men har også ført til nye trusler de må ta stilling til. Det er ikke valgfritt å ta del i digitaliseringen, det er noe en må gjøre for å ikke bli utdatert i bransjen. Mer og mer av systemene blir teknologidrevet og oppdatert deretter (informanten).

PST la frem i årets trusselvurdering at statlige etterretningstjenester lykkes i å bryte seg inn i norske virksomheter sine digitale nettverk (PST, 2021, s. 2). Dette er i tråd med hva som foregår i kraftsektoren. Informanten forklarte at typiske trusler de står overfor kan være alt fra angrep fra det typiske gutterommet til avanserte angrep fra statlige aktører, som for eksempel Russland og Kina. Videre forklarer informanten at det er cyberangrep fra statlige aktører en jobber mest med for å kunne motstå, samtidig som andre typer angrep blir inkludert i arbeidet (informanten).

Tidligere kunne cyberangrep ha en type karakter hvor målet var å lage støy og vise muskler. Nå ser en at trenden handler mer om penger, for eksempel løsepengevirus (NSM, 2015). Det å drive med cyberangrep har blitt «big business» ved at flere uvedkommende arbeider kontinuerlig for å finne måter å hacke seg inn på (informanten). I tillegg til løsepengevirus står infiltrering og spionasje høyt oppe på listen. Den beste hackeren vil ikke bli oppdaget lengre, den vil heller ha «bakdøren» åpen, og innhente så mye konfidensiell informasjon som mulig, og bruke det når det skader mest (informanten). Det vil føre til større konsekvenser å angripe en virksomhet når den er på det mest kritiske, og sannsynligheten for at de vil betale løsepenger er større på grunn av desperasjon.

Worst-case scenario

Informanten bekreftet at trusselen oppleves som større nå enn tidligere. PST legger frem i sine trusselvurderinger at det forventes at statlige aktører vil bruke ressurser på spionasje (se delkapittel 1.1), noe som bidrar til å sette det på dagsorden. I tillegg til spionasje og andre

metoder, frykter en også løsepengevirus (informanten). Informanten forklarte at et worst-case scenario i kraftsektoren handler om en hendelse som vil påvirker deres evne til å styre strømmen. En slik hendelse skjedde i Ukraina i 2015. Lille julaften mistet mange tusen innbyggere strømmen i flere timer. Flere kraftstasjoner ble koblet ut, og angrepet regnes som et av de første vellykka cyberangrepene mot kraftselskaper (Wernersen, 2020).

Lufttransportsektoren

På lik linje med andre sektorer og samfunnet for øvrig, er også lufttransportsektoren avhengig av den digitale utviklingen. Lufttransportsektoren innebærer ulike infrastrukturer, blant annet flyselskap, lufthavner og flysikring. De systemene som blir brukt hos de ulike infrastrukturer, er avhengig av datanettverk for å kunne fungere optimalt. Dette leder videre til at cyberangrep kan være en trussel mot disse systemene, som videre kan gi driftsforstyrrelser og potensielt alvorlige konsekvenser (Meld. St. 30 (2016-2017), s. 15). Typiske trusler lufttransportsektoren står overfor, innebærer alt fra hacking fra det typiske gutterommet til statlig etterretning hvor løsepengevirus og spionasje dominerer mest. Informanten fra lufttransportsektoren forklarte at hver uke opplever de utallige mange forsøk på hacking. De aller fleste blir luket bort ganske kjapt og utgjør ingen konsekvenser, mens noen blir undersøkt videre (informanten).

Et eksempel på et cyberangrep skjedde i 2018 på lufthavnen i Bristol. Lufthavnen ble utsatt for et løsepengevirus hvor alle informasjonsskjermene ble tatt offline. Det var et spekulativt forsøk snarere enn et målrettet angrep, men utfordret lufthavnen til å innføre midlertidige løsninger med penn og papir frem til problemet var håndtert (BBC, 2018). Dette eksemplet viser at nedetid i noen av systemene som brukes, kan skape problemer som kan gi videre ringvirkninger. Informanten fortalte at fokuset har lenge vært å unngå nedetid på systemet forårsaket av for eksempel løsepengevirus. Vi vil alltid jobbe hardt for at alle systemene våre skal fungere (informanten).

Nå handler truslene mer og mer om statlig etterretning som står bak, hvor de vil hente inn så mye informasjon som mulig (informanten). Det kan trekkes linjer til PST og NSM sine årlige trusselvurderinger. Samtidig tar vi også høyde for ikke-villede hendelser, hvor nedetid ofte kan være forårsaket av generelle tekniske feil (informanten). Luftrommet nord for Røros ble stengt januar 2020 på grunn av tekniske problemer. Systemet flygelederne bruker i avvikling av trafikk ble rammet, noe som førte til at all trafikk måtte stoppes. De avkreftet ryktet om at det var et cyberangrep (ABC nyheter, 2020). Tidligere har også såkalte tjenestenekt-angrep vært et

problem hos oss (informanten). Det er et angrep som innebærer at en blir hindret tilgang til systemet. Forsøk på tjenestenekt-angrep er så og si fraværende i dag, og det er uten tvil løsepengevirus og spionasje som er de mest dominerende angrepene. Med det sagt, så er ikke beredskapen for tjenestenekt-angrep lagt bort. En tar høyde for at det fortsatt kan skje, men det tar ikke like stor plass under radaren hos oss lengre (informanten). Det viser at trusselbildet er dynamisk.

I Luftfartstilsynets årsrapport fra 2014 ble fenomenet «digital sikkerhet» nevnt for første gang. Der blir det lagt frem at den digitale utviklingen har ført til at IKT er en sikkerhetsutfordring, og med den utviklingen samfunnet har må det forventes at det feltet vil kreve større oppmerksomhet i tiden som kommer (Luftfartstilsynet, 2014, s. 19). Informanten bekreftet at den digitale trusselen oppleves som større nå enn tidligere, dermed er det ingen tvil om at luftfartstilsynets spådom stemmer. Informanten fortalte at det foreligger en stor avhengighet til IKT-systemer, både nasjonalt og internasjonalt. Systemer er avhengige av eksterne leverandører noe som innebærer at cyberangrep er tverrsektorielle (informanten). Det vil si at cyberangrep rammer på tvers av sektorer, og kan gi store ringvirkninger.

Worst-case scenario

Informanten fortalte at et worst-case scenario i lufttransportsektoren handler generelt om nedetid i driftssystemene. Det foreligger reserveløsninger for å drive trafikkavviklingen selv om enkelte funksjoner ligger nede, men effektiviteten vil være svært lav (NOU 2015: 13, s. 208). Informanten bekreftet at det er etablert en del reserveløsninger, men de er ikke i nærheten av å ha samme kapasitet som systemet ellers. Eksempelvis kan et reservesystem på Oslo Lufthavn ha en kapasitet på fire fly i timen. Normalt er det en hel del flere flyvninger i timen (informanten). Ifølge Oslo Lufthavn sin hjemmeside er det i tidsrommet 16.00 - 17.00 på en ukedag, omtrent 25 flyvninger (Avinor, 2021). Et worst-case scenario hos lufttransportsektoren som omhandler nedetid, innebærer ikke tap av menneskeliv. Det handler mer om konsekvenser som går ut over næringslivet, det offentlige og den enkelte (NOU 2015: 13, s. 208).

Vann- og avløpssektoren

Samfunnet forventer at vannforsyningen er robust nok til å levere nok og godt vann selv om vannforsyningen utsettes for ulike typer trusler og påkjenninger, fra for eksempel cyberangrep (NOU 2015: 13, s. 159). Uten et fungerende vann- og avløpssystem vil samfunnet fort merke konsekvenser som kan gå utover liv og helse. Truslene vann- og avløpssektoren står overfor

innebærer blant annet innbrudd i SCADA-systemer hvor en mister kontrollen, som videre kan føre til at samfunnet blir rammet. Informanten fortalte at endringer innenfor trusselbildet handler om at det blir mer og mer sårbart alt ettersom hvor mye som blir knyttet opp til digitale løsninger, slik som SCADA-systemer er avhengige av for å fungere. Selve trusselaktørene har vært de samme gjennom tidene, men motivasjonen bak kan variere, samt at de har blitt mer profesjonelle. Motivasjonen kan være basert på økonomisk motiv slik som løsepengevirus, politisk motiv fra for eksempel statlig etterretning, eller tilfeldige grunner for å vise at «jeg kan hacke systemet» fra for eksempel det typiske gutterommet (informanten).

Worst-case scenario

PST og NSM sine årlige trusselvurderinger om cyberangrep er definitivt overførbare til vann- og avløpssektoren. Vi er en viktig infrastruktur som fort kan være et mål å angripe for å gjøre skade i samfunnet (informanten). Både løsepengevirus og statlig etterretning er aktuelt, men vi forbereder oss ikke noe særlig på hvilket type angrep det er, da konsekvensene ofte er det samme uavhengig om det er basert på et økonomisk, politisk eller tilfeldig motiv. Vi arbeider for å være robuste nok til å håndtere konsekvensene av angrepet (informanten). Et worst-case scenario innebærer at vi ikke er i stand til å levere vann, og at vannet ikke kan drikkes. Det er det vi vil forhindre (informanten). Et slikt scenario har ikke skjedd i Norge, men i andre land. I 2018 ble et fylke i USA rammet av et løsepengevirus hvor hackerne holdt vannsystemet i gissel, og krevde løsepenger for å gi det tilbake. Fylket nektet å betale løsepengene, og konstruerte heller et nytt vannsystem. Denne hendelsen ble satt på dagsorden i andre byer rundt omkring, for hvis hackere er i stand til å stenge systemet for å kreve penger, så kan de også forgifte vannsystemet (Heldahl & Pettersen, 2019).

Olje- og gassektoren

Den digitale utviklingen i olje- og gassektoren gir mange muligheter og fordeler, men sikkerheten må settes først. Det er viktig å forstå hvilke konsekvenser innføring av nye løsninger har for risikobildet. Tidligere måtte en ut til plattformen for å utføre arbeid, men nå kan mye fjernstyres fra land. Den økende digitaliseringen gjør olje- og gassektoren mer sårbar for blant annet digitale trusler (Midttun, 2019). Som nevnt tidligere er det de nye løsningene for bedre kommunikasjon mellom hav og land, samt fjernstyring som er sårbart. Dermed må en kartlegge trusler som er rettet mot de nye effektiviserende løsningene.

Olje- og gassektoren er et mål for trusselaktører på grunn av de store verdiene sektoren representerer, og for aktivister med idealistisk eller politisk motivasjon (Ptil, 2020, s. 1). I olje- og gassektoren kunne begge informantene bekrefte at den digitale utviklingen bidrar til nye trusler og sårbarheter som det må bli tatt stilling til. Cybertruslene omhandler alt fra løsepengevirus og spionasje, til stjeling av identitet til ansatte. Det er med andre ord mange ulike trusler de må forberede seg på (informant 1). Miljøaktivister blir også sett på som trusselaktører, hvor de har som formål å påvirke virksomheten gjennom cyberangrep, med eksempelvis tjenestenekt-angrep. Tidligere har ikke miljøaktivister hatt så mye ressurser og kunnskap til å påvirke oss digitalt, men det oppleves at de begynner å få mer kompetanse (informant 2). Det er ingen tvil om at trusselbildet har endret seg til å bli mer komplekst, hvor digitale trusler har fått en større og dominerende plass. Det er mye mer trusler i dag enn for noen år siden. Mye fordi det er en generell økning i hva og hvem som blir koblet til internett, men også fordi det er mer synlig. Et tiltak for å redusere konsekvenser av et cyberangrep er å foreta backup. Det er alltid viktig å ha en backup i tilfellet systemet blir angrepet, men nå er det også en strategi å angripe backup'en. Dette utfordrer oss til å tenke annerledes og ikke kun stole på et tiltak slik som backup, men også implementere andre risikoreduserende tiltak. Det er ingen tvil om at cyberangrep topper listen om trusselvurderinger innad i selskapet (informant 2).

Cybertrusler omhandler alt fra spionasje, løsepengevirus og sabotasje rettet mot SCADA-systemer, samt identitetstyveri av de ansatte. For selve selskapet er det løsepengevirus, og annen generell økonomisk vinning, som vil ødelegge mest av systemet i øyeblikket angrepet skjer. Spionasje fra statlige aktører vil prege samfunnet og sektoren i sin helhet, men kanskje ikke selskapet direkte der og da (informant 2). Det finnes utallige og uoppdagede inngangsporter og måter å angripe på, noe som viser at trusselaktørene åpenbart har blitt mer profesjonelle (informant 1 og 2).

Worst-case scenario

I olje- og gassektoren handler ikke et worst-case scenario nødvendigvis om nedetid i systemet, slik det gjør for de andre sektorene. Det handler mer om at det blir skapt ulykkessituasjoner som kan føre til tap av liv på anleggene. Hvis SCADA-systemene blir hacket så kan det i beste fall «kun» føre til at produksjonen blir stoppet. I verste fall utvikler det seg til ulykker offshore som følge av tap av strøm, angrep på helikoptertrafikken, angrep på sikkerhetssystemet med mer, som kan føre til ulykker hvor det blir katastrofale utfall for arbeiderne på anleggene. Det vil være det verste scenarioet (informant 1 og 2).

Oppsummert

Trusler rundt cyberangrep har vært et voksende fenomen på kort tid, og oppleves som større i dag enn tidligere. Det forklares med at store deler av driftssystemer, såkalt SCADA-systemer, har blitt digitalisert hvor målet er å øke effektivitet og produktivitet. Sårbarheter og trusler vokser i takt med den digitale utviklingen. Det er noe en ikke kan unngå å ta en del i da det er viktig for selskaper å være oppdatert digitalt for å effektivisere driften, samt holde seg konkurransedyktige i markedet. Trusler PST og NSM legger frem i sine årlige trusselvurderinger går igjen i alle sektorene. Både løsepengevirus og statlig etterretning er trusler de kjenner til, og noe de vil styrke seg mot. Hver sektor har tatt for seg hva som er deres worst-case scenario, og det varierer i noen grad alt ettersom hvilken sektor det er snakk om. Ikke alle innebærer tap av liv, men handler hovedsakelig om tap av kontroll. Truslene oppleves som større i dag enn tidligere, noe som går hånd-i-hånd med den digitale utviklingen. Det er dog de samme truslene som går igjen i de ulike sektorene, alt fra angrep fra det typiske gutterommet til statlig etterretning, men en merker at omfanget og graden av profesjonalitet har økt. Truslene har dermed endret seg til å være mer komplekse med et potensielt større skadeomfang.

5.3 Hvordan blir risikovurderinger gjort?

Hvilke trusler en står overfor vil påvirke hvordan en utfører risikovurderinger, og hvem som utfører dem. Er det egne folk i selskapet, eller en tjeneste en må få eksternt? Blir risikovurderinger basert på nyhetsbildet og/eller erfaringer fra andre hendelser? Blir det tatt hensyn til relasjoner til andre sektorer? NOU 2015: 13 påpeker nødvendigheten med å være medlem i en CERT. Hvilken CERT tilhører sektorene?

Kraftsektoren

Med en økning i trusselnivået, samt den økende kompleksiteten, ble KraftCERT etablert for å bistå med kompetanse til kraftforsyningsselskaper. KraftCERT skal bidra med håndtering og forebygging av angrep som skjer digitalt mot kraftsektoren (NOU 2015: 13, s. 134). I kraftsektoren kunne informanten bekrefte at i deres selskap er det egne folk som arbeider med cybersikkerhet, i tett dialog med KraftCERT. De arbeider også for å informere alle ansatte i selskapet slik at forståelsen rundt cybersikkerhet blir allmennkjent, og ikke lukket til en avdeling. Det er dog en balansegang da de andre ansatte selvsagt har andre arbeidsoppgaver også, og dermed ikke kan vie all sin tid på cybersikkerhet (informanten).

Informanten forklarte også at det blir trukket erfaring fra tidligere hendelser når de foretar risikovurderinger, for eksempel fra cyberangrepet i Ukraina (forklart i delkapittel 5.2) og Stuxnett. Stuxnett er en dataorm som er designet for å sabotere industriprosesser, eksempelvis i kritisk infrastruktur (NSM, 2010, s. 10-11). Vi følger kontinuerlig med i nyhetsbildet og årlige rapporter fra for eksempel NSM og PST (informanten). Det er verdifullt å bruke det en har rundt seg, samtidig som det også er viktig å dele informasjon med andre. Da kan andre også få lærdom og forberede sine løsninger deretter (informanten). Dette gjøres sammen med eksempelvis KraftCERT. Kompetansen KraftCERT bidrar med er sentral for å ha gode risikovurderinger, for da blir det lettere å vite hva en må se etter. I tillegg er cybersikkerhetsbegrepene integritet, konfidensialitet og tilgjengelighet sentrale i risikovurderingene våre (informanten). I tabell 3 blir det vist at det er tett relasjon med andre kritiske infrastrukturer, som fører til at cyberangrep hos kraftsektoren kan ramme tverrsektorielt. Derfor er det viktig at risikovurderinger tar hensyn til relasjoner til andre sektorer, da de kan bli preget hvis kraftsektoren blir utsatt for et cyberangrep. Bortfall av våre funksjoner gir raskt konsekvenser i samfunnet ellers (informanten). Dette viser at kraftsektoren er klar over avhengigheten andre sektorer har til dem, og dermed sørger for å ha et kontinuerlig fokus på cybersikkerhet.

Lufttransportsektoren

Lufttransportsektoren har egen responsgruppe som kalles for CSIRT som går innunder NorCERT (NOU 2015: 13, s. 206). I tillegg foregår det et stort samarbeid med andre CERTer i Norge og internasjonalt hvor en mottar og deler informasjon. På den måten blir en oppdatert på hendelser som skjer andre steder, slik at en kan gjøre seg robust til å håndtere et lignende angrep selv (informanten). Vi har egne folk i selskapet som arbeider med risikovurderinger i samarbeid med andre sentrale aktører, slik som CSIRT og andre CERTer. I tillegg er det etablert et samarbeidsforum for cybersikkerhet hvor alle transportgreinene er inkludert (luftfart, sjøtransport, veitrafikk og jernbane). Der kan de utveksle informasjon og erfaringer om cybersikkerhet generelt, samt det digitale trusselbildet (Meld. St. 38 (2016-2017), s. 62). Vi jobber også proaktiv med å inkludere og informere alle i selskapet om risikoer rundt cybersikkerhet (informanten). På den måten blir ikke avdelingen fremstått som en separert og lukket avdeling, men heller en åpen avdeling med fokus på informasjonsflyt. Risikovurderingene tar også utgangspunkt i cybersikkerhetsbegrepene tilgjengelighet, integritet og konfidensialitet. De begrepene står oss nært, hvor tilgjengelighet og integritet lenge har vært viktigst ofte på bekostning av konfidensialitet. Nå ser vi at konfidensialitet av informasjon må

være likeverdig med de andre begrepene, og dermed må vi bruke mer midler på å styrke det i våre risikovurderinger (informanten).

NOU 2015: 13 legger frem at transportsektoren generelt må fokusere på eksisterende og kommende digitale sårbarheter, og gi de større oppmerksomhet (NOU 2015: 13, s. 215). I og med at sektoren i seg selv, men også cybersikkerhet, har en global karakter, er det viktig at det også fokuseres på internasjonalt samarbeid. Informanten bekreftet dette. I tabell 3 ser en at transportsektoren er avhengig av andre kritiske infrastrukturer, noe informanten også kunne bekrefte hvor relasjoner til andre sektorer blir tatt stilling til. Vi er avhengige av eksterne leverandører, blant annet innen EKOM. Det forholdet har vi med i planene våre (informanten). Nedetid i EKOM vil gi ringvirkninger i lufttransportsektoren, dermed må de se for seg slike scenarioer og inkludere det i sine risikovurderinger.

Vann- og avløpssektoren

NOU 2015: 13 påpekte at det ikke er et felles responsmiljø for vann- og avløpssektoren når det gjaldt hendelser knyttet til svikt i IKT, men at det var ønsket (NOU 2015: 13, s. 165). I dag har ikke vann- og avløpssektoren en egen CERT, men en avtale med KraftCERT (informanten). KraftCERT bidrar til å påvirke våre risikovurderinger, for eksempel ved å komme med rapporter fra hendelser som har skjedd andre steder slik at vi skal kunne ta stilling til om samme hendelse kunne skjedd hos oss, og om vi har tilsvarende rutiner (informanten). Vi har egne folk i selskapet som arbeider kontinuerlig med trusselbildet. Ansatte i andre avdelinger blir også bevisstgjort med hva de digitale sårbarhetene er, og hva en kan gjøre for å forhindre cyberangrep. Med det sagt, er det alltid en balansegang mellom sikkerhet og produktivitet. En kan ikke bruke alle ressurser på sikkerheten, dermed må det vurderes etter behov. Ved å implementere cybersikkerhetsbegrepene i våre risikovurderinger så kan det bidra til å få til en balansegang mellom sikring av integritet, konfidensialitet og tilgjengelighet. På den måten kan vi vurdere hva som er de viktigste verdiene for oss, og deretter balansere sikkerhet og produktivitet på en god måte (informanten).

Et eksempel på en hendelse hvor konfidensialiteten ikke var sikret nok, skjedde i et vannverk i Florida som ble hacket. Hackeren ville justere på mengden sodiumhyroksid som kan gi etseskader på hud og slimhinner. Operatøren som hadde vakt fikk med seg dette, og fikk stengt systemet før det ble gjort noen skade. Hackeren fikk tilgang til systemet etter et skjermbilde av driftskontrollsystemet som lå ute på produsentens hjemmesider, noe som svekker

konfidensialiteten (Seglesten, 2021). Denne rapporten fikk vi også tilsendt av KraftCERT i etterkant slik at vi kunne sjekke opp våre rutiner på tilsvarende (informanten).

I risikovurderingene blir det også tatt hensyn til relasjoner til andre sektorer, og at angrep ofte er tverrsektorielle. Vann- og avløpssektoren er eksempelvis avhengig av strømforsyning og EKOM (se tabell 3). Vi har backup-planer på hva vi må gjøre hvis tjenestene fra andre leverandører eller annen kritisk infrastruktur går ned. Ikke nødvendigvis knyttet til kun cyberangrep, men også basert på generell nedetid (informanten).

Olje- og gassektoren

Olje- og gassektoren tilhører NorCERT, og er et samarbeid som bidrar til å øke kompetansen for å kunne foreta gode risikovurderinger (NOU 2015: 13, s. 149). Informantene bekreftet at det er egne folk i sektoren som har i arbeidsoppgave å følge med på cybersikkerheten, ofte i samarbeid med NorCERT. Det blir jobbet aktivt for bevisstgjøring av cybersikkerhet innad i sektoren. Det foregår blant annet kampanjer for ansatte for opplæring i hvordan oppdage phishing (informant 1). Arbeidet med å informere om cybersikkerhet er ikke tilstrekkelig nok enda. Det er innenfor de gitte rammer, men en arbeider kontinuerlig for å øke bevisstheten enda mer i alle avdelinger (informant 2). I tillegg til samarbeid med NorCERT, er risikovurderingene sentrert rundt vurderingen av alle de tre cybersikkerhetsbegrepene; konfidensialitet, integritet og tilgjengelighet (informant 2). Samtidig blir det trukket erfaring fra hendelser som skjer andre steder for å være proaktive i trusselvurderinger.

Tidligere hendelser har gjort inntrykk, spesielt hendelsene som rammet Mærsk og Norsk Hydro. Vi tar med i betraktning at lignende hendelser kan ramme oss (informant 1). I 2017 ble Mærsk utsatt for et løsepengevirus som kostet dem rundt 2,5 milliarder kroner (Jørgenrud, 2017). I 2019 ble også Norsk Hydro utsatt for et løsepengevirus, og det kostet dem rundt 550-650 millioner kroner (Hydro, 2020). Informant 1 fortalte at ved slike hendelser trekker de erfaringer og ser hvordan et lignende scenario ville fått utspilt seg i deres virksomhet, og hva de bør gjøre for å motstå et lignende angrep. I tillegg til informasjon fra NorCERT, bidrar årlige rapporter fra for eksempel NSM, PST og Petroleumstilsynet (Ptil), samt nyhetsbildet, til å belyse trusselbildet. Det er også et eget nettverk internt i sektoren hvor en kan dele erfaringer. Det er mye mer fordelaktig å være åpen enn å holde informasjonen lukket. På den måten kan en styrke og hjelpe hverandre til å være best mulig forberedt på cyberangrep i fremtiden (informant 1 og 2).

Tabell 3 viser at olje- og gassektoren har relasjoner med kraftsektoren, EKOM og satellittbaserte tjenester. Når det gjelder relasjoner til andre sektorer, så er det noe vi kunne blitt flinkere til å ha med i betraktning når vi foretar risikovurderinger. Det blir til dels tatt med i betraktningen, men vi kunne vært flinkere (informant 2).

Oppsummert

I og med at digitale trusler har tatt større plass på dagsorden de siste årene, er det fordelaktig å ha egne folk internt som kontinuerlig arbeider for å kartlegge risikobildet. Det kunne alle informantene bekrefte at de hadde. Det er ikke en tjeneste de får eksternt. Dermed er det egen avdeling i selskapene som jobber regelmessig med cybersikkerhet. Ofte er det i samarbeid med en CERT, hvor både KraftCERT og NorCERT ble nevnt som sentrale og viktige aktører med mye kompetanse og ekspertise. Kraftsektoren og vann- og avløpssektoren tilhører KraftCERT, mens luftransportsektoren og olje- og gassektoren tilhører NorCERT. IT-avdelingene i selskapene arbeider også med å informere og inkludere alle ansatte i selskapet. På den måten bevisstgjør en trusselbildet slik at alle kan bidra til å unngå at fremmede aktører får innpass, for eksempel ved å informere om farene ved phishing. Alle informantene forklarte at det blir trukket erfaringer fra tidligere hendelser, samtidig som en holder seg oppdatert på årlige rapporter og nyhetsbildet. Informantene la også trykk på verdien av å dele informasjon videre slik at en kan bidra til at andre kan lære av sine egne oppdagelser. Det er en felles konsensus om at det ikke er noe vits i holde informasjon for seg selv.

Det at cyberangrep kan ramme tverrsektorielt, hvor en hendelse et sted kan gi ringvirkninger et annet sted, er noe sektorene har tatt stilling til – men i ulik grad. Olje- og gassektoren vet at det er et faktum, men har ikke inkludert det i ønskelig grad i sine risikovurderinger. For energisektoren går det henholdsvis én vei, da de fleste er avhengig av dem, og at de ikke nødvendigvis er like avhengig tilbake. Cybersikkerhet har fått større plass i risikovurderinger den siste tiden, som har økt det arbeidet betraktelig. Alle har tenkning etter cybersikkerhetsbegrepene konfidensialitet, integritet og tilgjengelighet. Med en holdning om at informasjon også må deles, får en inkludert erfaringer andre steder i sine egne risikovurderinger, samt kartlagt hvilke andre sektorer en kan være avhengig av slik at en kan ta en risikovurdering på det sammen. Dette er i tråd med budskapet fra Meld. St. 27 (2015-2016, s. 150) hvor samvirke er nødvendig da digitalisering er sektorovergripende, og at risikovurderinger må være oppdatert på trussel- og risikobildet.

5.4 Hvordan har beredskapen endret seg?

Dette forskningsspørsmålet går dypere inn i hvordan beredskapsplanleggingen foregår, og hvor fokuset ligger. Videre har hvert selskap besvart hvor fokuset er rundt beredskap for cyberangrep, hvilken strategi som ligger til grunn, om det foreligger et samarbeid med andre sentrale aktører, samt en egen sammenligning de siste årene på hvordan beredskapen har endret seg.

Kraftsektoren

I og med at trusselbildet har endret seg, og at cyberangrep er uunngåelig, trengs det gode beredskapsplaner. Avhengighet til leverandører øker og systemene blir mer komplekse, og derfor bør leverandører involveres i nettselskapene sin håndtering av cybersikkerhetshendelser (Bratnes, 2020). Dette viser at samarbeid er sentralt for å kunne håndtere cyberangrep med minst mulige konsekvenser. Informanten bekreftet at beredskapen innad i selskapet har uten tvil endret seg den siste tiden. Sammenligner en beredskapen flere år tilbake i tid var det lite spor av cyberhendelser. I dag, derimot, har cybersikkerhet en egen plass i beredskapsplanen og egne planer for håndtering (informanten). Dette er et resultat av den økende bevisstheten rundt cybersikkerhet fra nyhetsbildet, men også årlige vurderinger som blir gjort nasjonalt og internasjonalt.

Strategi

Strategien i beredskapen handler om å unngå angrep, samtidig å kunne motstå angrep. En kan aldri være hundre prosent sikret mot et angrep, derfor er det et økt fokus på evne til gjenopprettelse, redundans og være robust nok. I tillegg er det fokus på å øke beredskapen med andre aktører som en selv er avhengig av (informanten). Fokuset rundt cybersikkerhet har absolutt økt, noe som naturligvis spiller en rolle i beredskapsplanleggingen.

Luftransportsektoren

Digitaliseringen har skapt nye utfordringer for luftfarten. Mange av systemene som er knyttet til kommunikasjon og navigasjon er fra en tid hvor det var få tilfeller av cyberangrep. Med årene har det blitt flere kontaktpunkter mot andre nettverk, noe som øker sårbarheten for systemene (Haanæs, 2020). Dette krever at beredskapsplanleggingen er oppdatert på de utfordringene en står overfor. Informanten fortalte at trusselbildet og avhengigheten til digitaliseringen har endret seg i svært stor grad i løpet av de siste årene, noe som har påvirket

beredskapsplanleggingen. IT har i løpet av de siste årene fått en plass rundt bordet, og cybersikkerhet har fått en tydelig plass på beredskapsplanen. Konsernet har blitt mer og mer interessert i IT og hva vi driver med, noe som viser en modenhet i oppfattelsen rundt cybersikkerhet. Vi har et kontinuerlig fokus på trusselbildet med forbehold om at en aldri kan være helt forberedt på cyberangrep (informanten).

Strategi

Beredskapen bygger på en strategi hvor ønsket selvsagt er å kunne unngå angrep, men cyberangrep er umulig å kunne unngå i sin helhet. Dermed bygger strategien heller på å kunne tåle et angrep. Det å være robust nok til å motstå et angrep, samt oppnå normaltilstand så fort som mulig, er svært viktig for oss. Dette ved hjelp av å ha redundante løsninger, som for eksempel backup-planer (informanten). I tillegg er det fokus på å styrke beredskapen sammen med myndigheter og andre aktører. Informanten fortalte at de deler informasjon med NSM sin Nasjonale Cybersikkerhetssenter (NCSC), som videre anonymiserer informasjonen med andre aktører i samme partnerskap. På den måten gir en informasjon samtidig som en får verdifull informasjon tilbake innenfor cybersikkerhet. En slik deltagelse gir enklere tilgang til NSM og andre partnere sin kompetanse om cybersikkerhet (Luftfartstilsynet, 2019, s. 21). Beredskapsplanen gjennomgås årlig, og endringer forekommer av prosedyrearbeid basert på risikovurderinger (informanten).

Vann- og avløpssektoren

Spørsmål rundt cybersikkerhet var på et tidlig stadiet i modenhet i 2015, og NOU 2015: 13 la frem et ønske om at fokuset rundt cybersikkerhet må øke i sektoren, både hos ledelsen og hos de ansatte (NOU 2015: 13, s. 166). Fokuset rundt cybersikkerhet og cyberangrep er mye bedre i dag enn hva det var for noen år siden. Selvfølgelig skulle en alltids ønske at en kan gjøre mer, men vi har relativt god oversikt og kontroll (informanten). Vi arbeider for å lære alle ansatte om å gjøre de riktige tingene, et fokus som har økt betraktelig de siste årene. Vi i IT-avdelingen har også blitt mye mer involvert i det meste av planleggingen i selskapet, hvor vi får komme med premisser i forhold til cybersikkerhet (informanten). Dette er alle faktorer som påvirker beredskapen.

Strategi

Strategien vår handler om å være robust nok til å kunne motstå et angrep. Dette ved hjelp av gode backup-rutiner for å sørge for kjapp gjenopprettelse. Ønsket er jo helt klart å kunne unngå

angrep i sin helhet, men før eller siden vil en bli angrepet uansett, men vi vil at konsekvensene skal være så minimale som mulig (informanten). Vi utfører jevnlige risikovurderinger basert på nyhetsbildet og årlige rapporter fra eksempelvis PST og NSM, trener og øver, og reviderer beredskapsplanen deretter. Vi foretar kontinuerlige vurderinger i IT-bransjen, og sitter ikke og venter på at noe skal skje før vi innfører tiltak (informanten). I tillegg til et samarbeid med KraftCERT har vi også øvelser sammen med myndigheter, samt noe dialog med andre vann- og avløpsselskaper i landet. Med det sagt, skulle vi gjerne hatt en tettere dialog med andre selskaper som gjør det samme som oss (informanten).

Olje- og gassektoren

Informantene fortalte at cyberangrep har fått en mye større plass i beredskapsplanen nå, sammenlignet med de siste årene. Før var det et lite fokus på cyberangrep, mens nå blir det sakte, men sikkert, implementert mer og mer i beredskapsplanen. Vi har kommet langt med forståelsen av hvor viktig arbeid det er, og at det må få plass i beredskapsplanen på lik linje med andre hendelser (informant 1). Et slikt arbeid tar dessverre tid. Vi er langt i fra ferdig da det er mange som må inkluderes i prosessen. Alle må få en forståelse, samtidig som det er en balansegang mellom sikkerhet og produktivitet. Alle ressurser kan ikke bli lagt til sikkerhetsarbeid før det er vurdert hva som er nødvendig. Det må være knyttet til produktivitet (informant 2).

Strategi

Strategien bak beredskapen er selvsagt å kunne unngå angrep, men det er dessverre ikke mulig å kunne unngå det i sin helhet. En vil oppleve et cyberangrep en eller annen gang. Det er en «daglig krig», og bildet endrer seg hele tiden. Derfor må en være robust nok til å kunne motstå et angrep også. Dette med å ha fokus på redundans i en form av backup, samt ha god nok teknologi i bruk. Det er også et fokus på å styrke beredskapen med andre aktører og myndigheter, hvor Ptil spiller en stor rolle (informant 1). Ptil følger opp cybersikkerheten med en rekke tilsyn. De vil beskrive endringer og drivere som påvirker trussel- og risikobildet, samt identifisere områder hvor det trengs å gjøre mer for å hindre tilsiktede og utilsiktede handlinger (Midttun, 2019). Vi er også med i et nettverk med andre selskaper hvor det foregår en felles «brainstorming» av ulike forsvarsmekanismer en kan implementere (informant 2). Fokuset rundt cyberangrep har uten tvil økt det siste året, og begynner å ta større plass i beredskapen. Derfor er det svært viktig å ivareta samarbeidet med andre, samt kontinuerlig arbeide for å bevisstgjøre sårbarhetene en står overfor (informant 1).

Oppsummert

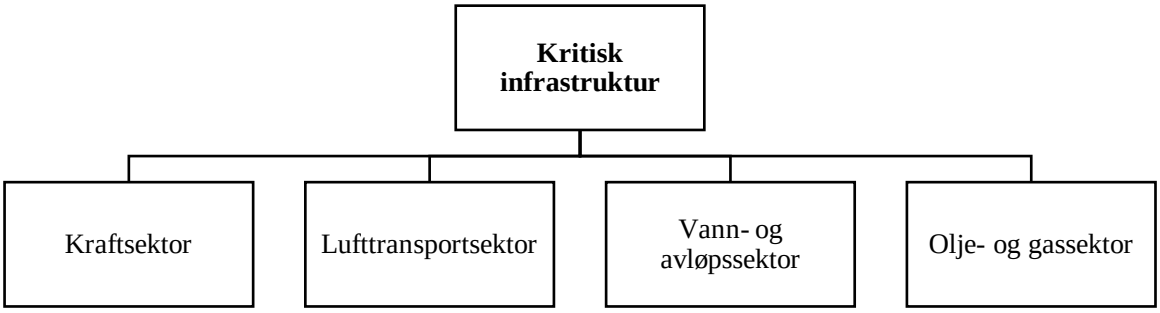
Det er ingen tvil om at cybersikkerhet har fått en større og dominerende plass på beredskapsplanen den siste tiden. IT og den kompetansen de har i selskapene har fått en plass rundt bordet, hvor ledelsen også har blitt mer engasjert. Informantene bekreftet at det er et økt fokus når det gjelder beredskap for cybersikkerhet, men at en aldri vil komme helt i mål. Det er en dynamisk prosess som krever at en arbeider jevnlig med å holde seg oppdatert på trusselbildet, noe hver informant bekreftet. Dermed vil en aldri være ferdig med et slikt arbeid. Selv om ønsket er å kunne unngå angrep i sin helhet, er de innforstått med at det ikke er fysisk mulig. Dermed er strategien bak beredskapen å kunne være robuste nok til å tåle et angrep. En vil bli rammet før eller siden, men en kan være med på å avgjøre hvor store konsekvensene vil bli. Beredskapen består også av et samarbeid med andre relevante aktører og myndigheter, i og med at cyberangrep kan ramme tverrsektorielt. Beredskapen har endret seg med at cyberangrep har fått en større plass de siste årene grunnet det økende omfanget av cyberangrep rettet mot virksomheter, og da særlig innenfor kritisk infrastruktur. Det å ha et kontinuerlig fokus på trusselbildet, ha et samarbeid med sentrale aktører og ha en strategi hvor en vil være så robust som mulig til å tåle et angrep, står sentralt i beredskapsplanleggingen og i beredskapsplanen. Dette er i tråd med regjeringens nasjonale strategi for digital sikkerhet hvor en i fellesskap har et mål om å styrke den digitale sikkerheten gjennom blant annet god beredskapsplanlegging (Regjeringen, 2019, s. 1).

5.5 Oppsummering

Etter en gjennomgang av hvordan truslene har endret seg, hvordan risikovurderinger blir gjort, og hvordan beredskapen har endret seg i de ulike sektorene, ser en at det er mer likheter enn ulikheter. Mye av informasjonen som NOU 2015: 13 la frem er videreført, noe som bekrefter at det er et økende fokus. Informasjonen de årlige rapportene til PST og NSM legger frem om trusselbildet, viser seg å samstemme med hva informantene fortalte, noe som bekrefter trusselbildet og det økende behovet for større fokus på cybersikkerhet.

6.0 Diskusjon

I dette kapitlet vil empiriske funn og teori flettes sammen. Tidligere forskning og informasjon fra kontekst vil også bli trukket inn der det er relevant. Kapitlet vil være strukturert etter forskningsspørsmålene slik som foregående kapittel. Her vil hver sektor gå samlet under paraplybegrepet «kritisk infrastruktur» og refereres som «sektorene». Noen av funnene vil bli nevnt flere steder, men med ulikt formål. Diskusjonen skal lede opp til et svar på problemstillingen i kapittel syv; Hvorfor har beredskap mot cyberangrep endret seg i organisasjoner som er ansvarlig for drift av kritisk infrastruktur?



Figur 8. Illustrasjon av oppsett i kapittel med fokus på paraplybegrepet «kritisk infrastruktur». Det som er uthevet er i fokus.

6.1 Hvordan har truslene endret seg?

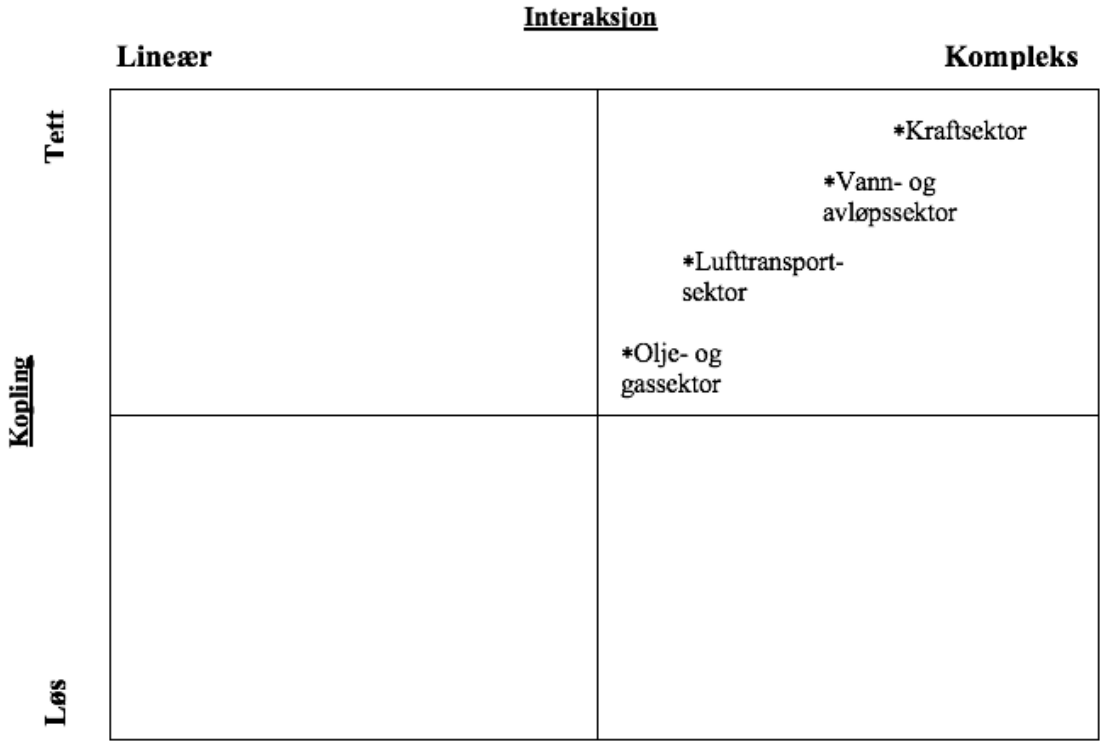
Funn fra intervjuer viser at trusler mot cybersikkerheten har økt betraktelig de siste årene i alle sektorene som blir studert. Dette samstemmer med funnene fra dokumentanalysen, hvor blant annet trusler i det digitale rom dominerer den nasjonale trusselvurderingen til PST for 2021. Trusler mot cybersikkerheten har gradvis manifestert seg med årene samtidig som truslene har blitt mer komplekse ved at de har økt i omfang, og trusselaktørene har blitt mer profesjonelle. Trusselaktørene har fått mer ressurser og kompetanse som har ført til at angrepsmåtene har blitt mer komplekse. Det finnes utallige måter å utføre et cyberangrep på, samt utallige trusselaktører med ulike motiv, men det er politiske og økonomiske motiv som er de største. Det fører til stor usikkerhet og utfordring å vite konkret hva en møter når en blir utsatt for en trussel.

Kritisk infrastruktur som høyteknologisk og komplekst system

Sektorene som blir studert i denne oppgaven kategoriseres som kritisk infrastruktur. Å være en kritisk infrastruktur innebærer de nødvendige anlegg og systemer som må fungere for å opprettholde samfunnets kritiske funksjoner (NOU 2015: 13, s. 19). Det øker kompleksiteten i stor grad da samfunnet for øvrig er avhengig av at ting skal fungere, hvor bortfall kan føre til

samfunnsmessige konsekvenser. Dette kan trekkes linjer til Perrow (1984) sitt hovedpoeng i teorien om NAT, som handler om at komplekse og høyteknologiske systemer ikke kan unngå systemulykker grunnet måten systemet er konstruert, med tette koplinger og komplekse interaksjoner. Kraftsektoren, lufttransportsektoren, vann- og avløpssektoren og olje- og gassektoren kan alle kategoriseres som komplekse og høyteknologiske systemer grunnet deres avhengighet til teknologi. Det innebærer blant annet deres avhengighet til digitale systemer, slik som SCADA-systemer, som er nødvendige for å opprettholde en produktivitet og effektivitet i sektoren. Samtidig handler det om at samfunnet og potensielt andre sektorer vil bli preget hvis systemene blir angrepet grunnet deres kritiske funksjon.

I Perrow (1984) sin klassifisering av systemer vil alle sektorene bli plassert under kompleks interaksjon, men med en varierende grad av tette koplinger. De hører til under kompleks interaksjon grunnet sin status som kritisk infrastruktur. Hvor tett koplet de er kan avgjøres av graden av relasjoner til andre sektorer. I denne forklaringen blir sektorene plassert ettersom hvor komplekse og tett koplede de er etter at et cyberangrep har skjedd. Plasseringen vil være annerledes enn hvis de skulle blitt kategorisert etter hvordan systemene fungerer i daglig drift. I det daglige kan de digitale løsningene som er implementert bli sett på som lineære og løst koplede, da det forenkler og effektiviserer driften av systemet. Når en blir utsatt for et angrep kan det oppstå kompleksitet fordi det er da en muligens finner ut at en ikke hadde god nok oversikt over alle sårbarhetene som følger med digitale løsninger. Dermed blir sektorene plassert ettersom hvor komplekst og tett koplet de er etter at et angrep har skjedd.



Figur 9. Kategorisering av oppgavens sektorer etter koplinger og interaksjoner inspirert av Perrow (1984).

Empirien viser at de fleste systemer er avhengig av kraftsektoren, noe som fører til at kraftsektoren kan plasseres som den med tettest kopling. Deretter er vann- og avløp en sektor med stor grad av tett kopling i og med at samfunnet for øvrig er avhengig av rent vann og et godt avløpssystem. Nedetid i sektoren kan medføre store helsemessige konsekvenser i samfunnet i løpet av kort tid. Lufttransportsektoren byr ikke på konsekvenser som truer helsen, men har tett kopling grunnet relasjon til andre sektorer. Stans i lufttransporten medfører ringvirkninger i ulike retninger som kan medføre store økonomiske tap med konsekvenser for næringslivet, det offentlige og den enkelte (NOU 2015: 13, s. 208). Som nevnt i kapittel fire, må det argumenteres for om olje- og gassektoren kan kategoriseres som kritisk infrastruktur. I denne oppgaven er det naturlig at sektoren får den kategoriseringen grunnet sektorens store økonomiske vekst, som har en stor betydning for velferdsstaten Norge. Ser en på selskaper i olje- og gassektoren alene, vil ikke samfunnet for øvrig merke om et selskap blir rammet av et cyberangrep. De konsekvensene vil oftest være interne i det aktuelle selskapet og i sektoren. Dermed kan olje- og gassektoren være den med minst tett kopling sammenlignet med de andre nevnte sektorene. Skjelvik (2019) har tatt for seg hvordan finanssektoren kan knyttes opp til Perrow (1984) sin figur. Finanssektoren blir forklart med høy grad av kompleksitet og tett

kopling grunnet ringvirkninger sektoren kan gi ved svikt, men da selvsagt ikke på bekostning av liv og helse. Dermed kan finanssektoren også bli plassert i samme bolk som de andre. I bolkene under lineær interaksjon og løst kopling vil sektorer som ikke går under kategorien kritisk infrastruktur bli plassert. Grunnen til det er fordi et angrep i en slik sektor ikke vil merkes på samfunnet for øvrig, men heller merkes lokalt og internt uten katastrofale konsekvenser for samfunnet. Det kan eksempelvis være hotell- og restaurantbransjen. Denne tolkningen av sektorenes kompleksitet og tette koplinger samstemmer med Faraj et al. (2021) sin forståelse, hvor digitalisering fører til sårbarheter som kan forplante seg til andre systemer.

Kartlegging av graden om kompleksitet og kopling er et første steg på å få en oversikt over hvilke konsekvenser som ligger til grunn ved en ulykke. Blir en kategorisert som et system med høy grad av kompleksitet og tett kopling kan det være et stort mål for trusselaktører å angripe, da det gir større sannsynlighet for katastrofale utfall grunnet status som kritisk infrastruktur. Det stemmer også med Umbach (2012) sin kategorisering av kritisk infrastruktur (se delkapittel 1.4) hvor kritiske infrastrukturer kjennetegnes med en høy grad av intern kompleksitet og avhengighet, samt sårbarhet for cyberangrep. Alle sektorene plasseres i bolken med høy grad av kompleksitet og tette koplinger, noe som krever at kartlegging av hva som er trusler, og at et kontinuerlig arbeid med det, er svært nødvendig for å unngå katastrofale utfall.

Redusere risikoen for angrep i et høyteknologisk og komplekst system

Empirien samstemmer delvis med Perrow (1984) sitt budskap, men motstrider med tanke på at ulykker ikke blir betraktet som normale. Sektorene er innforstått med deres kritiske status, og at relasjoner til andre kan gi ringvirkninger ved et angrep. Det faktum at ulykker er normale er ikke en holdning som går igjen i deres tenkning. Det faktum at ulykker er uunngåelige er derimot noe som kan bekreftes. Empirien viser til en felles tenkning hvor cyberangrep ikke kan unngås, og dermed må en bygge opp resiliens for å heller tåle et cyberangrep. Med det blir ikke cyberangrep normalisert, men heller akseptert med et kontinuerlig forebyggende arbeid som motstand.

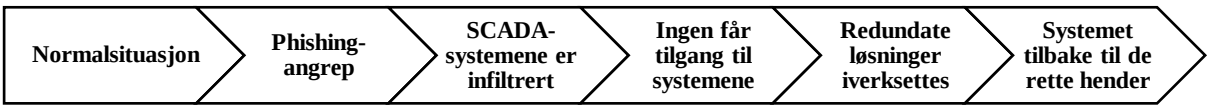
Innenfor cybersikkerhet i sektorene blir det jevnlig vurdert hva som er angrepsmetoder, og deretter kartlagt hvilken praksis som kan føre til at en trusselaktør får et smutthull og deretter infiltrerer systemet. Dermed er det viktig å ha et økt fokus på hva som forårsaker dette, for eksempel ved å informere og teste ansatte om konseptet phishing, og deretter justere praksis ved behov. Det er også viktig at oppmerksomheten er på de som er i den skarpe enden. Det

nytter ikke at det kun er ledelsen i organisasjonen sitter med kunnskapen om cybersikkerheten, og hva en bør/ikke bør gjøre. Informasjonen og praksisen må helt ned til den skarpe enden da det er de som ofte har situasjonsforståelsen. Det er også her erfaringer og kompetanse ofte ligger, og den informasjonen må tilbake til ledelsen. I empirien ble det forklart at det ikke lenger er klare skiller mellom de som arbeider med cybersikkerhet og de som arbeider i andre avdelinger i selskapet, noe som viser at de som arbeider med cybersikkerhet har fått en større plass rundt bordet. På den måten skaper det bedre forutsetninger for gode beslutninger da deres kompetanse blir tatt med i betraktning helt fra start. Evne til å faktisk tåle uventede forstyrrelser er også noe som står sterkt hos sektorene. Dette ved hjelp av redundante løsninger i ulike varianter. Redundante løsninger er viktig for å kunne tåle et angrep, og er dermed bygget inn i vanlig praksis. Backup-systemer blir nevnt som en første prioritet på en redundant løsning (dette blir videre forklart i delkapittel 6.3). Det er også viktig å gå bort i fra den hierarkiske strukturen, og la beslutninger fattes basert på ekspertise og erfaringer. Dette kan trekkes linjer til at IT-avdelinger og deres kompetanse har fått en større plass rundt bordet med ledelsen de siste årene. Ledelsen har sett at de trenger den kompetansen ved implementering av nye systemer, fremfor å inkludere dem etter at nye systemer er satt i gang. De holdningene empirien viser til, kan trekkes linjer til Weick et al. (2008) sine prinsipper om HRO-tenkning hvor ulykker kan forebygges. Fire av de fem prinsippene går igjen i empirien, hvor det handler om et kontinuerlig fokus på mulige feil, oppmerksomhet på det operasjonelle, forpliktelse til resiliens og fleksibilitet av strukturer. Ved en slik holdning og ved et slikt fokus på feil, kan en redusere risikoen for svikt i systemet etter et cyberangrep.

En slik tankegang med å alltid være på jakt etter feil for å redusere svikt i systemet, samstemmer med en generativ kultur. Westrum (1993) forklarer en generativ kultur med at en aktivt søker etter informasjon, noe en må gjøre for å holde seg oppdatert på hva som er trusler, og hva som er produktive tiltak å gjøre for å minimere risikoen for å bli utsatt for en slik trussel. Dette bekreftes av empirien hvor det er et økende fokus rundt å dele informasjonen en selv har, da en ikke ser noe poeng i holde informasjonen kun for seg selv. Det er stor verdi i å dele informasjon. I tillegg foregår det blant annet kontinuerlige vurderinger og endringer ved behandling av feil, noe en aktivt må gjøre da trusselbildet stadig endres.

Før cybersikkerhet fikk det fokuset det har i dag, var det enda mer usikkerhet rundt hva som faktisk var trusler, grunnen for hvorfor de oppsto, og hvilke konsekvenser de forårsaket. Ved en slik uvitenhet kan det skape flere årsaksfaktorer for en hendelse som en ikke vet om før det

er for sent. Cyberangrep er et relativt nytt fenomen, i hvert fall måten cyberangrep blir utført på i dag. For eksempel så skal en ikke gå langt tilbake i tid før phishing var en fremmed metode å bli angrepet på, og en dermed ikke visste at å «bite på» en slik metode kan føre til at systemet en opererer i kan bli utsatt for et cyberangrep. Det samstemmer med teorien om MMD hvor Rosness et al. (2004) forklarer at en type informasjonssvikt handler om at informasjonen en opererer med er fullstendig ukjent, da den peker mot hendelser som en aldri har erfart tidligere, og derfor ikke er oppmerksom på. Ved å være kontinuerlig på jakt etter informasjon knyttet til cybersikkerhet reduserer en risikoen for at informasjonssvikt er faktoren som gjør at en blir ekstra sårbar for en digital hendelse.



Figur 10. Hendelsesforløp i lys av MMD-modellen, inspirert av Rosness et al. (2004).

Med eksempelet ovenfor ser en at det skal ikke mer til enn at én ansatt ikke har kjennskap til phishingangrep, og dermed blir et smutthull for angriperen. Samtidig er ikke konseptet phishing fullstendig ukjent for organisasjonen da de har en plan på hva en skal gjøre hvis systemet blir infiltrert. Selv om organisasjonen kanskje ikke har erfart noe lignende tidligere, så har de aktivt hentet inn nødvendig informasjon for å være robust nok til å tåle et slikt angrep. I dette tilfellet kan organisasjonen kartlegge hvor det foregikk en informasjonssvikt, som da ville vært den ansatte som «bet på» en phishing-epost, og dermed redusere risikoen for den trusselen ved å arbeide tettere med å informere alle ansatte om phishing.

Worst-case scenario

De største truslene i dag består av løsepengevirus og statlig etterretning, noe som viser en sammenheng mellom hva informantene fortalte og hva PST (2021) sin årlige trusselvurdering presenterte. Det er de truslene hver sektor fokuserer mest på i det daglige, samtidig som de har øyene åpne for andre trusler. Som nevnt innledningsvis i dette delkapitlet, så er det en utfordring å vite hva en møter når en forsøker å kartlegge trusler. Fremfor å bruke tid og ressurser på å kartlegge hvilke typer angrep en kan møte, kan det være viktigere å kartlegge hvordan et worst-case scenario ser ut. Da kan en bruke tid og ressurser på å sørge for at konsekvensene blir så minimale som mulig, med eksempelvis redundante løsninger (kommer tilbake til det i delkapittel 6.3). Et worst-case scenario kan skje uavhengig av hvordan hendelsen oppstår, om det er et løsepengevirus eller statlig etterretning. Empirien viser at hver sektor har tatt for seg

hvordan et worst-case scenario ser ut hos dem, slik at en kan arbeide for å gjøre seg robust nok til å tåle det hvis et slikt angrep skulle finne sted. Det er basert på hendelser som har skjedd andre steder. Det er ikke et felles worst-case scenario hos sektorene, det varierer avhengig av hvilken sektor det går innunder. Fellesfaktoren mellom sektorene sine worst-case scenarioer handler hovedsakelig om tap av kontroll som kan gi videre ringvirkninger til andre systemer.

Delkonklusjon

Trusler for cyberangrep har endret seg en del, både i omfang og type. Truslene oppleves som større i dag, noe som er i takt med den digitale utviklingen. Sektorene arbeider dog mer med cybersikkerhet i dag enn hva de gjorde tidligere. Dermed kan det fastslås at det er en økende utvikling i trusselbildet, samtidig som det er en økt oppmerksomhet i sektorene når det gjelder cybersikkerhetsarbeid. Her kan finanssektoren også trekkes inn på lik linje med de andre basert på Skjelvik (2019) sine funn. De holdningene og det fokuset som ligger til grunn i sektorene kan trekkes linjer til Weick et al. (2008) sine prinsipper når det gjelder forebyggelse av ulykker, samt Westrums (1993) generative kultur, hvor en aktivt søker og gir informasjon om trusselbildet.

6.2 Hvordan blir risikovurderinger gjort?

Empirien viser at risikovurderinger blir utført i tett samarbeid med sentrale aktører, samtidig som det blir basert på tidligere hendelser, nyhetsbildet og årlige rapporter utført av myndigheter. I tillegg blir alle ansatte innad i selskapet informert om hva som er risikofaktorene. På den måten blir alle inkludert i risikoreduserende arbeid. Relasjoner til andre sektorer er også viktig å ta hensyn til i og med at det innebærer kritiske infrastrukturer. Dette støtter opp regjerningens nasjonale strategi for digital sikkerhet, hvor relasjoner til andre kritiske infrastrukturer må tas hensyn til i arbeidet for å være robust i møte med digitale trusler (Regjeringen, 2019).

Informasjonsdeling

For å kunne utføre gode risikovurderinger er en avhengig av å ha relevant informasjon til grunn. Hvis ikke kan det bli falske og urealistiske vurderinger. Hvordan kan en sørge for å få tilgang til relevant informasjon? Empirien viser til at det å dele informasjon med hverandre er svært betydningsfullt for å kunne forberede seg, i den grad det er mulig, på et cyberangrep. Ikke bare til ansatte innad i selskapet, men også til andre i samme sektor, samt andre sektorer en har en relasjon til. Det kan være informasjon om tidligere erfaringer, kompetanse og kunnskap en har

innhentet, og oppdagede sårbarheter. Dette påpeker også Stoddard (2016) i sin forskning fra Storbritannia, hvor han forklarer at for å bygge opp en robusthet mot cyberangrep må en trekke erfaringer fra andre land og virksomheter. Rapporter fra PST, NSM og tilsynsmyndigheter bidrar også til å belyse viktige momenter en må se etter. En er ikke lenger alene om å bli rammet av et cyberangrep, særlig hvis en driver med arbeid innenfor kritisk infrastruktur. Dermed er det viktig å innhente informasjon samtidig som en gir informasjon. Dette spiller en stor rolle da cyberangrep kan ramme flere enn den som faktisk blir angrepet. Det er viktig at sektorer trekker erfaringer fra andre selskaper i samme sektor, andre sektorer og andre land. På den måten kan en sammen gjøre seg mer robust da cyberangrep kan være tverrsektorielle, samtidig som en må kartlegge hvordan ringvirkninger fra et cyberangrep, som skjer et annet sted, kan ramme en selv. En er ikke lenger alene om et angrep.

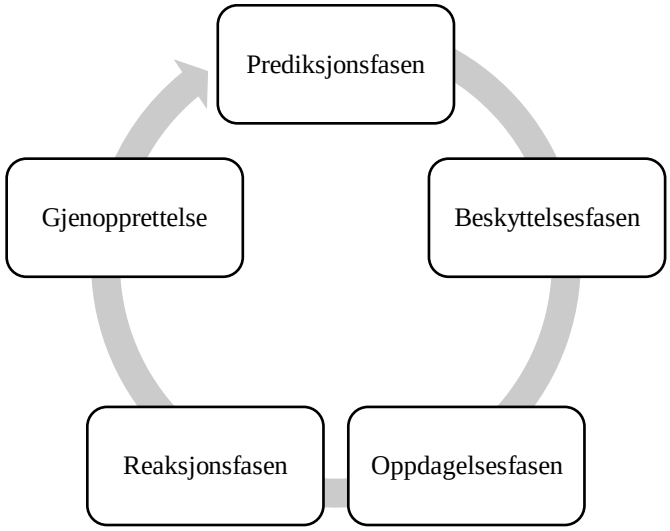
En må være åpen for at den oppfattelsen en har til grunn om cybersikkerhet kanskje ikke er tilstrekkelig nok, og dermed må oppdateres. Gode tiltak kan være å ha egne folk innad i sektoren som har i arbeidsoppgave å følge med på risikobildet og kontinuerlig vurdere nye tiltak som må til. KraftCERT og NorCERT er store aktører som kan bidra med kompetanse til tilhørende selskaper. I og med at cyberangrep kan ramme tverrsektorielt, er det viktig å ha flere planer for å håndtere det. Samarbeid på kryss og tvers, både private og offentlige virksomheter, kan gjøre en mer styrket i møte med utfordringer rundt digitalisering. Dette er noe Umbach (2012) også påpeker, hvor han legger frem at slike samarbeidsordninger vil gjøre en mer robust mot cyberangrep. Det er en kamp en må kjempe sammen. Holdninger rundt risikovurderinger må stamme fra et fokus hvor ingenting er statisk. Trusselbildet og sårbarheter endres stadig, dermed må en ha et dynamisk arbeid med en holdning om at en aldri er ferdig med å foreta risikovurderinger. Dette kan trekkes linjer til generativ kultur av Westrum (1993). En slik kultur går hånd-i-hånd med en forståelse om at risikovurderinger må gjøres kontinuerlig, da trusselbildet er dynamisk. Trusselbildet står aldri stille. Empirien påpekte at det har skjedd endringer i sektorene hvor IT-avdelingen har fått en større plass rundt bordet. Der deler de sin ekspertise før nye tiltak blir implementert, slik at fokus rundt cybersikkerhet blir tatt hensyn til helt fra start. Det viser at IT-avdelingene har fått et større ansvar, og at det har blitt en styrket relasjon mellom flere avdelinger hvor det tidligere var mer separert. Dette samstemmer med en generativ kultur hvor brobygging mellom enheter oppmuntres, og ansvar deles. På motsatt side av en slik praksis, er det snakk om en patologisk og byråkratisk kultur hvor skadeomfanget vil være mye større da en ikke har oppdaterte og nøyaktige risikoanalyser, ei heller god oversikt over organisasjonens evner til å tåle et cyberangrep.

Det er ikke nok å ha tilgang til en uendelig mengde informasjon, en må også vite hva en skal gjøre med informasjonen en besitter. Ifølge empirien er sektorene selvstendige nok til å foreta og vurdere risikovurderinger på egenhånd, samtidig som en benytter tilgjengelig informasjon fra eksempelvis CERTer, andre selskaper, nyhetsbildet og årlige rapporter fra PST og NSM. Den informasjonen bidrar til en kontinuerlig vurdering og eventuell justering av risikovurderinger, noe alle i selskapet kan være involvert i. Dette trekkes linjer til Woods (2006 i Kongsvik et al., 2018, s. 83) sine egenskaper uavhengighet, involvering, informert og informativ. Det er gode egenskaper som bidrar til at en vet hvordan en skal håndtere informasjonen som er tilgjengelig slik at en kan få mest mulig utbytte av den. I praksis vil det si at sektorene er uavhengige av andre, på den måten at de besitter ressurser til å hente inn nødvendig informasjon selv. De er involvert i arbeidet med cybersikkerhet, hvor det må tas like mye hensyn til som alt annet arbeid. Til slutt kan sektorene forklares med at de er informert og inkludert om trusselbildet, samt informative om tilgjengelig nyttig informasjon hentet fra ulike plattformer.

Den nye sikkerhetsloven (2018) er, som nevnt tidligere (se delkapittel 2.1), blitt oppdatert med blant annet et krav om at virksomheter må utføre gode nok risikovurderinger på egenhånd, fremfor å være pålagt å bruke et «ferdig formulert» oppsett. Sikkerhetsloven (2018) har bidratt til at det er et eget ansvar å ha et kontinuerlig fokus på risiko innad i virksomheten, noe som har endret måten risikovurderinger blir gjort på en forbedret måte, da enhver virksomhet må ta stilling til det arbeidet. Dette kan for eksempel gjøres ved å sørge for at cybersikkerhetsbegrepene blir ivaretatt. Empirien bekreftet at sikkerhetsbegrepene konfidensialitet, integritet og tilgjengelighet er sentrale når det gjelder risikovurderinger. Hvordan en sørger for at de ulike begrepene blir ivaretatt, er opp til hver virksomhet å vurdere. De må ta stilling til hvilken informasjon som ikke må komme på avveie, ei heller endres av uvedkommende, samt at systemet er tilgjengelig for de som til enhver tid må ha tilgang.

Risikovurderings betydning

Som påpekt tidligere er trusselbildet dynamisk, noe som krever en dynamisk fremgangsmåte når det gjelder risikovurderinger. De risikovurderingene som har blitt trukket frem i denne drøftingen er i tråd med en generativ kultur. De legger bedre føringer for hva en kan møte, og hvordan det blir møtt. Innledningsvis under delkapittel 1.4, ble Maglaras et al. (2018) sin cybersikkerhetssyklus presentert. Forskerne presenterte en syklus for god cybersikkerhet, hvor risikovurderingene legger viktige føringer for hvordan et angrep kan spille ut.



Figur 11. Syklus for cybersikkerhet inspirert av Maglaras et al. (2018).

Et tilstrekkelig fokus i forkant av et cyberangrep innebærer at sektorene vurderer alle mulige proaktive tiltak for å identifisere truslene en står overfor. Etter risikovurderingene må sektorene implementere de nødvendige tiltakene for beskyttelse, samt innføre tiltak for å gjøre seg mer robust i møte med et cyberangrep. Hvis ikke vil risikovurderingene kun være en aktivitet de er pålagt å gjennomføre, men ikke noe de går videre med. Når et cyberangrep er oppdaget, vil de prosessene og metodene en har kommet frem til, basert på risikovurderinger, bli iverksatt slik at en raskest mulig kan sørge for gjenopprettelse. Dette viser at fasene er sirkulære i tråd med et dynamisk bilde. Fokuset må aldri stoppe opp, da en aldri er i mål med å vurdere trusselbildet. Dermed er gode risikovurderinger nødvendig, noe empirien også bekreftet.

Delkonklusjon

Risikovurderinger spiller en stor rolle innenfor kritisk infrastruktur for å minimere risikoen for katastrofale utfall. Den nye sikkerhetsloven (2018) har bidratt til at risikovurderinger blir gjennomført på en bedre måte, med et økende fokus på å ha en dynamisk fremgangsmåte og tankegang. Vurderingene blir gjort internt i selskapet med et tett samarbeid med tilhørende CERT. Det er også et stort fokus på relasjoner til andre selskaper innad i samme sektor for å lære av hverandre. Årlige rapporter fra PST og NSM, samt tilhørende tilsynsorgan, spiller inn på hva en fokuserer på i trusselbildet. På denne måten klarer sektorene å sortere mye mengder informasjon til sin fordel. Dette springer ut fra en grunnforståelse om at det må være en kontinuerlig vurdering av risikoanalyser, noe som er i tråd med at trusler er dynamiske. En er aldri ferdig med et slikt arbeid, og en vil alltid kunne bli bedre. Hvordan risikovurderinger blir gjort innenfor sektorene kan trekkes linjer til en generativ kultur av Westrum (1993), og Woods

(2006 i Kongsvik et al., 2018) sine fire egenskaper for å håndtere mye mengde informasjon på best mulig måte.

6.3 Hvordan har beredskapen endret seg?

Empirien viser at i løpet av de siste årene har beredskapen endret seg for å møte utfordringene rundt cybersikkerhet. Tilsiktede hendelser i form av cyberangrep utgjør en større trussel i dag enn tidligere, noe som krever at beredskapsplanen må ta for seg slike scenarioer. Har cyberangrep fått større plass i beredskapsplaner i sektorer som er ansvarlig for drift av kritisk infrastruktur?

Resiliens

Informantene bekreftet at for å møte de utfordringene som truer cybersikkerheten, må strategien i beredskapsplanlegging være basert på en resilient tankegang hvor en vil være robust nok til å motstå et angrep, fremfor en holdning om å unngå angrep. En må akseptere at en vil bli rammet av cyberangrep uansett, og heller vurdere hvordan konsekvensene av et angrep vil ramme selskapet. Dette kan knyttes opp til Vogus og Sutcliffe (2007) sin teori om resiliens, hvor resiliente organisasjoner alltid er nysgjerrig på potensialet for det uventede. Da er en innforstått med at deres risikovurderinger trenger jevnlig oppdatering og at beredskapen som foreligger er ufullstendig. I tillegg har resiliente organisasjoner et fokus på å klare å takle et bredt spekter av uventede hendelser, samtidig som de jobber kontinuerlig for å forbedre deres evner til å takle de uventede hendelsene. Dette bekreftet empirien. Sektorene forklarte at det er umulig å være hundre prosent forberedt på et cyberangrep. Alle angrep er ulike og vanskelige å forutse. Derfor må en heller arbeide for å være robuste nok til å tåle et angrep. Dette ved hjelp av å innhente ekspertkunnskap og ha dialog med andre relevante aktører, trekke erfaringer fra andre steder og hendelser, og gjennomføre øvelser og trening internt for å kartlegge hva status er på kunnskap og kompetanse. Resultater av dette vil påvirke risikovurderingene og dermed føre til endringer i beredskapen. Oppdateringer i beredskapen skjer jevnlig, noe som er i tråd med at trusselbildet også endres jevnlig. Dette er også noe Stoddard (2016) trekker frem i sin artikkel, hvor resiliens og redundans må stå sterkt for å være mer robust i møte med cyberangrep.

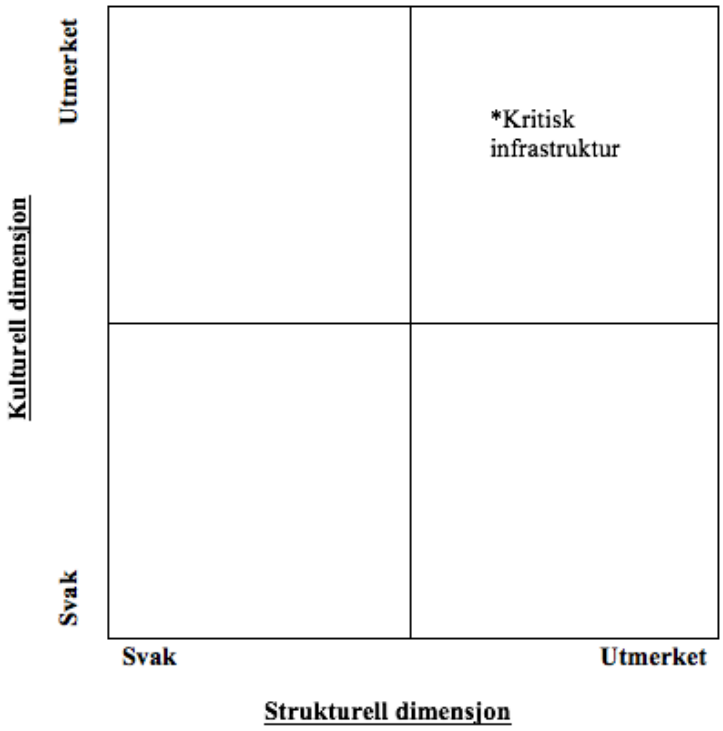
En resilient organisasjon gjenspeiler nødvendigheten med at beredskapsplanen må være en dynamisk prosess. Perry og Lindell (2003) påpeker at den viktigste egenskapen i effektiv beredskapsplanlegging er at det er en kontinuerlig prosess. Planen må endres etter erfaringer fra trening og øvelser, noe enhver informant bekreftet. Det springer ut fra en generativ kultur

fra Westrum (1993), hvor det aktivt søkes etter informasjon og det blir foretatt kontinuerlige vurderinger og endringer. Med en slik aktiv beredskapsplanlegging unngår en å havne i fellen hvor beredskapsplanen blir et fantasidokument.

Det ligger mye grunnarbeid i å være «god» på å håndtere cybertrusler. Dette er noe Haanæs (2020) også påpeker i sin forskningsartikkel hvor det er nødvendig å trene på ulike hendelser knyttet til cybersikkerhet. Ikke bare for å visualisere hvordan det vil se ut, men også for å vite hva en skal gjøre, hvem en skal kommunisere med, og hva en skal kommunisere. På den måten kan responsen bli mer effektiv og målrettet. Empirien viser til nettopp dette. For å gjøre denne prosessen mer innholdsrik bestående av gode erfaringer og kompetanse, er det åpen dialog med andre sentrale aktører og forum for å utveksle sine erfaringer og kompetanser. Dette viser at relasjoner til andre aktører er avgjørende i kampen mot å tåle cyberangrep. På den måten kan en på sikt få en beredskap som er robust nok til å tåle uforutsette cyberangrep, noe enhver sektor streber etter å ha.

Redundans

Redundante løsninger er et viktig tiltak for å redusere sannsynligheten for langvarig svikt. Som påpekt tidligere må strategien i møte med cyberangrep være å kunne motstå dem, ikke unngå dem. Empirien viser at redundante løsninger er svært viktig for å kunne være mer robust til å tåle et angrep. Det handlet om å ha redundans i form av backup-systemer slik at en kan oppnå en relativt normal drift nokså kjapt. Sektorene sin forståelse og fokus på redundans kan trekkes linjer til Rosness et al. (2004) sin forståelse av redundante løsninger, hvor en kan se på den kulturelle og strukturelle dimensjonen.



Figur 12. Plassering av kritisk infrastruktur som en HRO, inspirert av Rosness et al. (2004).

Sektorene viste til at utveksling av informasjon internt og eksternt står sterkt. I tillegg forklarte de at det foregår kontinuerlige vurderinger for nåværende praksis, og at en er innforstått med at beslutninger må revurderes etter behov. Sektorene påpekte at trusselbildet er dynamisk, og dermed må en være åpen for at nåværende praksis før eller siden bør endres på i møte med sårbarhetene en står overfor. Dette kan forklares som en del av å være redundant, noe som er i tråd med Rosness et al. (2004) sin kulturelle dimensjon. Sektorene la også vekt på redundante løsninger som backup-systemer, samt overlappende kompetanse og ansvar slik at et driftssystem ikke er avhengig av én som sitter med kontrollen, noe Rosness et al. (2004) også forklarer med strukturell dimensjon av redundante løsninger. Ved å innføre flere ulike redundante løsninger vil en sammenlagt være mer resilient i møte med cyberangrep, samt redusere sannsynligheten for langvarig svikt. Dermed kan sektorene forklares som HRO, hvor god planlegging og praksis fører til at en kan håndtere uventede hendelser effektivt. En slik praksis som fundament kan trekkes linjer til en generativ kultur av Westrum (1993).

Gode risikovurderinger handler blant annet om forventninger til det uventede. Etter å ha kartlagt risikoene en står overfor, er det viktig å bygge opp resiliens i form av redundante løsninger for å motstå et angrep som blir implementert i beredskapsplanleggingen. Dette forklarer Weick og

Sutcliffe (2007) med «mindfullness» hvor sannsynligheten for svikt blir redusert ved å gjøre gode risikovurderinger, som gir en evne til å tåle det uventende. Dette i tråd med HRO sin grunntanke om at god planlegging fører til sikrere system, noe som vises igjen i sektorene.

Delkonklusjon

Beredskapen har endret seg med at cybersikkerhet har fått en større plass i møte med det økende omfanget av cyberangrep rettet mot kritisk infrastruktur. Beredskapen spirer ut fra en strategi om å være resilient nok til å tåle et angrep, da det ikke er mulig å motstå et angrep. Samarbeid og relasjoner til andre aktører står sterkt i beredskapsplanlegging, da det er svært vanskelig å være alene om de utfordringene cyberangrep medfører. Beredskapsplanleggingen er dynamisk, noe som er i tråd med Perry og Lindell (2003) sine retningslinjer innenfor planlegging. Rosness et al. (2004) sin strukturelle- og kulturelle dimensjon av redundans er i tråd med Westrum (1993) sin generative kultur, hvor åpenhet og nysgjerrighet om det uvitende står sterkt.

7.0 Konklusjon

I dette kapitlet skal problemstillingen besvares basert på foregående drøfting av empiri og teori. Problemstillingen er som følger:

Hvorfor har beredskap mot cyberangrep endret seg i organisasjoner som er ansvarlig for drift av kritisk infrastruktur?

Oppgavens problemstilling åpner for flere svar, og det må sees i sammenheng med flere faktorer og årsaker. Basert på empiri er det mer likheter enn ulikheter mellom hver sektor og dermed kan funnene forklares samlet under kritisk infrastruktur. De faktorene og årsakene som sees på som relevante for oppgavens problemstilling er som følger:

- I hver sektor vises det til en økt bruk av digitale løsninger hvor målet er at det skal bidra til økt effektivitet og produktivitet. Samtidig oppstår det fremmede digitale trusler med stort omfang og en høy grad av kompleksitet som krever en omstilling for å redusere risiko for katastrofale utfall.
- PST og NSM sine årlige trusselvurderinger viser til en økning av cyberangrep mot virksomheter, noe sektorene bekreftet. Det viser en sammenheng mellom hva sektorene fortalte og hva PST og NSM fremlegger i sine trusselvurderinger.
- Tidligere handlet truslene mer om store ødeleggelser som lammet driftssystemet. I dag handler det mer om angrep hvor en kan få en økonomisk vinning slik som løsepengevirus, eller politisk vinning slik som statlig etterretning. Disse type angrep går igjen hos hver sektor, og krever en omstilling av beredskapsplanlegging.
- Ikke-villede hendelser blir også tatt med i betraktning når en vurderer trusselbildet, da menneskelig svikt også er en faktor for nedetid i et digitalisert driftssystem.
- Truslene er tverrsektorielle, som innebærer at et cyberangrep i én sektor kan gi ringvirkninger i en annen. Det blir tatt med i betraktning hos hver sektor.
- Sektorene arbeider mer med forebyggende arbeid innen cybersikkerhet enn hva de gjorde tidligere. Det vil si at sektorene er proaktive i møte med digitale utfordringer. Det foreligger et stort fokus angående cybersikkerhet hvor en aktiv søker etter informasjon for å være resilient i møte med cyberangrep.
- Risikovurderinger har endret seg i den grad at enhver sektor er mer selvstendig i sine vurderinger, som krever at en må kartlegge sine verdier og planlegge hvordan de skal beskyttes. IT-avdelinger har fått en større plass rundt bordet som innebærer at

sikkerhetsmessige tiltak blir implementert fra start. Det viser at øverste ledelse har blitt mer modne når det gjelder cybersikkerhet.

- Årlige rapporter fra PST og NSM, erfaring fra tidligere hendelser hos seg selv og andre, samt kunnskap hentet fra tilhørende CERTer bidrar i utførelsen av risikovurderinger. Det blir gjort risikovurderinger fortløpende, som viser at det er en dynamisk prosess. Det er viktig siden trusselbildet også er dynamisk.
- Cybersikkerhet har fått en større og dominerende plass i beredskapsplanen for å møte det økende omfanget av trusler i det digitale rom.
- Beredskapsstrategien handler om å evne til å kunne motstå et cyberangrep, da enhver sektor er innforstått med at det er umulig å kunne unngå et cyberangrep.
- Samarbeid med andre aktører og relasjoner med andre sektorer er svært viktig i arbeidet for å bli mer resilient i møte med digitale trusler, og derfor står det sterkt i beredskapsplanleggingen.
- I tråd med jevnlige risikovurderinger blir beredskapsplanen oppdatert deretter for å møte det dynamiske trusselbildet.

Det konkluderes med at beredskap mot cyberangrep har måttet endre seg for å møte de digitale truslene den digitale utviklingen medfører. Det viser at fokuset har økt betraktelig og at det foregår på en dynamisk måte. Det betyr at beredskapsarbeidet aldri er ferdig, og at det må vurderes og revurderes kontinuerlig. Hvis ikke risikerer en å falle bakpå, og beredskapsplanen blir et såkalt fantasidokument. Innenfor kritisk infrastruktur har cyberangrep fått et større fokus i løpet av kort tid, hvor nedetid i tjenester raskt kan gi samfunnsmessige konsekvenser. Diskusjonen viser at det er en økning i form av trusler med stor grad av kompleksitet, som også vokser for hver dag som går. Det kommer stadig nye måter å angripe på, da det å drive med cyberangrep har blitt en egen «virksomhet». Parallelt med det økende trusselbildet blir det også arbeidet kontinuerlig med forebyggende arbeid innenfor cybersikkerhet. Det er på dagsorden hos enhver sektor. IT-avdelinger har fått en større plass rundt bordet og øverste ledelse har blitt mer modne til det som angår cybersikkerhet. Et bevis på det er at ingen av selskapene i studien har foreløpig blitt utsatt for et alvorlig cyberangrep. Beredskapen har måttet endre seg for å møte dagens trusler rettet mot kritisk infrastruktur, og det er et arbeid som aldri blir ferdig så lenge cyberangrep er et faktum.

7.1 Forslag til videre forskning

Denne studien har tatt utgangspunkt i fire selskaper fra ulike sektorer, og hvordan deres arbeid i møte med digitale trusler foregår. Det kunne vært interessant og inkludert flere sektorer, som for eksempel helse og omsorg, EKOM og satellittbaserte tjenester. De to sistnevnte sektorene var de med flest relasjoner til de andre sektorene i oppgaven, derfor ville det vært interessant å sett hvordan de møter utfordringer knyttet til cybersikkerhet. Et slikt tema er stort nok i seg selv. Et ytterlige forslag ville vært og sammenlignet praksis i selskaper av ulik størrelse, innunder samme sektor. Det sier seg kanskje selv at de største selskapene har ressurser og midler nok til å ha et større fokus på cybersikkerhet, men hvordan ligger det an i mindre selskaper med færre ressurser og midler? Og hvilke tiltak kan de implementere for å gjøre seg mer resilient i møte med cyberangrep? Uansett er videre forskning av denne tematikken svært viktig for å holde tritt med den digitale utviklingen og sårbarheter den medfører.

Referanseliste

ABC nyheter. (2020, 29. januar). Radartrøbbel satte flytrafikken nord for Røros ut av spill. https://www.abcnyheter.no/nyheter/norge/2020/01/29/195645280/radartrobbel-satte-flytrafikken-nord-for-roros-ut-av-spill

Aftenposten. (2021, 10. mars). Stortinget utsatt for IT-angrep: «Et angrep på vårt demokrati». https://www.aftenposten.no/norge/i/PRnGRX/stortinget-utsatt-for-it-angrep-et-angrep-paa-vaart-demokrati

Andersen, S. S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift*, *22*(3), 278-298.

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

Avinor. (2021, 28. mai). *Oslo lufthavn: avgang & ankomst.* https://avinor.no/en/airport/oslo-airport/flight-times/departures/

BBC. (2018, 16. september). Cyber attack led to Bristol Airport blank screens. https://www.bbc.com/news/uk-england-bristol-45539841

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

Blaikie, N. & Priest, J. (2019). *Designing social research* (utg.3). Polity Press.

Bratnes, M. (2020). Sviktende beredskap mot hacking i strømnettet. *Sintef.* https://www.sintef.no/siste-nytt/2020/sviktende-beredskap-mot-hacking-i-stromnettet/

DSB. (2018, 7. februar). *Nordmenn mest bekymret for cyberangrep.* https://www.dsb.no/nyhetsarkiv/2018/nordmenn-mest-bekymret-for-cyberangrep/

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

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, E. O. & Pettersen, K. A. (2016). *Perspektiver på Samfunnssikkerhet*. Cappelen Damm AS.

Faraj, S., Renno, W. & Bhardwaj, A. (2021). Unto the breach: What the COVID-19 pandemic exposes about digitalization. *Information and Organization*. Vol. 31. 100337. https://doi.org/10.1016/j.infoandorg.2021.100337

Haanæs, Ø. R. (2020, 26. juli). Mennesker er like viktige som teknologi for å sikre fly mot cyberangrep. *Forskning.no.* https://forskning.no/de-regionale-forskningsfondene-

internett-luftfart/mennesker-er-like-viktige-som-teknologi-for-a-sikre-fly-mot-cyberangrep/1711003

Halvorsen, K. (2008). *Å forske på samfunnet. En innføring i samfunnsvitenskapelig metode.* Cappelen Akademiske Forlag.

Hamnes, L. (2012, 3. juni). 16. spektakulære cyberangrep. *Teknisk ukeblad.* https://www.tu.no/artikler/16-spektakulaere-cyberangrep/244245

Heldahl, H. Ø. & Pettersen, B. M. (2019, 31. oktober). Sykt godt drikkevann. *NRK.* https://www.nrk.no/nordland/xl/norsk-vann-renner-gjennom-eldgamle-ror-og-gjor-oss-syke-oftere-enn-vi-tror-1.14757385

Hollnagel, E. (2017). Å bli resilient: organisasjoner, sikkerhet og resiliens. I T. Hafting (Red.), *Krisehåndtering: planlegging og handling* (s. 401-412). Fagbokforlaget.

Hydro. (2020, 14. oktober). *Cyberangrep på Hydro.* https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Jørgenrud, M.B. (2017, 7. november). Mærsk tapte opptil 2,5 milliarder kroner på dataangrep. *Digi.no.* https://www.digi.no/artikler/maersk-tapte-opptil-2-5-milliarder-kroner-pa-dataangrep/411585

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

KPMG. (u.å.). *Flere private selskaper blir underlagt ny sikkerhetslov – er du klar?* Hentet 19. februar 2021 fra https://home.kpmg/no/nb/home/tjenester/radgivning/cybersikkerhet/flere-private-selskaper-vil-bli-underlagt-ny-sikkerhetslov.html

KraftCert. (2020, u.d.). *KraftCert.* https://www.kraftcert.no/

Luftfartstilsynet. (2014). *Årsrapport – 2014.* https://luftfartstilsynet.no/globalassets/dokumenter/arsrapporter/arsrapport-2014.pdf

Luftfartstilsynet. (2019). *Årsrapport – 2019.* https://luftfartstilsynet.no/globalassets/dokumenter/arsrapporter/arsrapport_2019.pdf

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., Janicke, H. & Rallis, S. (2018). Threats, countermeasures and attribution of cyber attacks on critical infrastructure. *EAI Endorsed Transactions on security and safety, 5*(16), Artikkel 155856. https://doi.org/10.4108/eai.15-10-2018.155856

Meld. St. 27 (2015-2016). *Digital agenda for Norge.* Kommunal- og moderniseringsdepartementet.

Meld. St. 30 (2016-2017). *Verksemda til Avinor AS.* Samferdselsdepartementet.

Meld. St. 38. (2016-2017). *IKT-sikkerhet – et felles ansvar.* Justis- og beredskapsdepartementet.

Midttun, Ø. (2019, 28. mars). Skjerpet innsats for IKT-sikkerhet. *Ptil.* https://www.ptil.no/fagstoff/utforsk-fagstoff/reportasjer/2019/skjerpet-innsats-for-ikt-sikkerhet/

NSM & Kripos. (2020). *Løsepengevirus: temarapport.* https://nsm.no/regelverk-og-hjelp/rapporter/felles-temarapport-med-kripos-losepengevirus/

NSM. (2010). *Sikkerhetskultur.* https://nsm.no/getfile.php/133379-1591858647/Demo/Dokumenter/Rapporter/arsmelding-nsm-2010web%20%281%29.pdf

NSM. (2015). *Helhetlig digitalt risikobilde 2015.* https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2019-og-tidligere/

NSM. (2020). *Helhetlig digitalt risikobilde 2020.* https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/

Njå, O., Sommer, M., Rake, E. L. & Braut, G. S. (2020). *Samfunnssikkerhet – Analyse, styring og evaluering.* Universitetsforlaget.

NOU 2006: 6. (2006). *Når sikkerheten er viktigst: beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Justis- og politidepartementet.

NOU 2015: 13. (2015). *Digital sårbarhet – sikkert samfunn.* Justis- og beredskapsdepartementet.

Perrow, C. (1984). *Normal accidents: living with high-risk technologies.* Princeton University Press.

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

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

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

PST. (2020). *Trusselvurdering 2020*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

PST. (2021). *Trusselvurdering 2021*. https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

Ptil. (2020). *IKT-sikkerhet – robusthet i petroleumssektoren: Trening og øvelse.* 2019-0823.

Regjeringen (2010, 6. januar). *Bakgrunnsnotat: Cybersikkerhet.* (2010/00719/430). https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

Regjeringen. (2019). *Nasjonal strategi for digital sikkerhet.* https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Roald, N. (2018, 17. oktober). *Slik bruker hackere ansatte til å få tilgang til selskapets datasystem.* ATEA. https://www.atea.no/siste-nytt/slik-bruker-hackere-ansatte-til-a-fa-tilgang-til-selskapets-datasystem/

Røislien, H. E. (2020). Cyberdomenet: Frihet med slagside. I G.L. Dyndal & A.K. Larssen (Red.), *Strategisk ledelse i krise og krig: det norske systemet* (s. 196-215). Universitetsforlaget.

Rosness, R., Guttormsen, G., Steiro, T., Tinmannsvik, R.K., & Herrera, I.A. (2004). *Organisational Accidents and Resilient Organisations: Five Perspectives*. SINTEF.

Seglesten, P. H. (2021, 12. februar). Vannverk ble hacket – skjermbilde av kontrollpanelet var brukt som reklame. *Digi.no.* https://www.digi.no/artikler/vannverk-ble-hacket-skjermbilde-av-kontrollpanelet-var-brukt-som-reklame/506719

Skjelvik, A. (2019). *Cyber-risiko i den norske finanssektor* [Masteroppgave]. Universitetet i Stavanger.

Stoddard, K. (2016). UK cyber security and critical national infrastructure protection. *International affairs (London), 92*(5),1079-1105.

Umbach, F. (2012). *Critical energy infrastructure at risk of cyber attack*. Konrad Adenauer Stiftung.

Vaforum. (2018, u.d.). Vannbransjen må etablere en god kultur for cybersikkerhet. https://vaforum.no/vaforum-artikler/vannbransjen-ma-etablere-en-god-kultur-for-cybersikkerhet/

VG. (2018, 2. februar). Smarte byer – hva er det egentlig? https://www.vg.no/annonsorinnhold/smart/komplett/472-smarte-byer-hva-er-det-egentlig

Vogus, T. J. & Sutcliffe, K. M. (2007). Organizational Resilience: Towards a Theory and Research Agenda. Presentert i IEEE International Conference on Systems, Man and Cybernetics.

Vollan, M. (2021, 12. januar). Kripos ser en økning i profesjonelle dataangrep. *NRK*. *https://www.nrk.no/innlandet/tre-alvorlige-dataangrep-den-siste-maneden_-kripos-ser-en-okning-i-profesjonelle-hackere-1.15324245*

Weick, K. E. & Sutcliffe, K. M. (2007). *Managing the unexpected: resilient performance in an age of uncertainty.* Jossey-Bass.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management*, *3*(1), 81-123.

Wernersen, C. (2020, 9. september). Ti store dataangrep: måtte rive ut ledningene til 22.000 datamaskiner. *NRK*. https://www.nrk.no/urix/ti-store-datangrep_-norge-var-blant-landene-som-ble-rammet-av-lospengeviruset-petya-1.15144202

Westrum, R. (1993). Cultures with requisite imagination. I J.A. Wise, V.D. Hopkin & P. Stager (Red.) *Verification and Validation of Complex Systems: Human Factors Issues* (s. 401-416). Springer-Verlag.

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, *141*, 5-9.

Vedlegg

Vedlegg 1: Samtykkeerklæring

Jeg skriver nå masteroppgave i samfunnssikkerhet ved Universitet i Stavanger hvor temaet mitt handler om beredskap mot cyberangrep i sektorer som kan kategoriseres som kritisk infrastruktur. I den forbindelse vil jeg intervjue ansatte som representerer ulike sektorer slik at jeg får et helhetlig bilde på hva som er dagens status. Spørsmålene vil være basert på forskningsspørsmålene mine, og vil omhandle hva som er trusler og hvordan de har endret seg, hvordan risikovurderinger blir gjort og hvordan beredskapen har endret seg.

Oppgaven vil bli offentliggjort, dermed vil alle selskaper og informanter anonymiseres. For å sikre personvern vil det kun bli tatt notater fremfor opptak av samtalen. Hvis det er ønskelig så kan dere få muligheten til å godkjenne teksten og sitater som blir brukt i oppgaven før den blir levert. Masteroppgaven skal levers 15.06.2021.

Ved å signere denne erklæringen samtykker du at opplysningene som blir gitt under intervjuet kan benyttes videre i oppgaven.

(Signatur informant, sted og dato)

Vedlegg 2: Intervjuguide

Del 1: Rammesetting, informasjon og innledning

- Informere kort om oppgaven og dens formål
- Informere om informantens anonymitet
- Informere om at det blir tatt notater underveis
- Spør om informanten kan presentere seg med stillingstittel og arbeidsoppgaver, samt deres bakgrunn
- Hva betyr cyber for deres sektor?
- På hvilken måte kan deres sektor kategoriseres som en kritisk infrastruktur?

Del 2: Intervjuet

Forskningsspørsmål 1: Hvordan har truslene endret seg?

1. Hvilke cybertrusler står dere overfor, og har dere opplevd et cyberangrep?
2. Ser dere en utvikling i hva som er trusler? Hva var «vanlig» før, og hva er det mest av nå?

   - PSTs årlige trusselvurderinger påpeker at andre lands etterretningstjenester lyktes med å bryte seg inn i de digitale nettverkene til norske myndigheter og private virksomheter. Er denne trusselen overførbar til deres sektor? I så fall, hvordan?
3. Har det skjedd en endring i hvem som er typiske trusselaktører? Blir ikke-villede hendelser kategorisert som trussel? Eventuelt hvorfor ikke?
4. Er motivasjonen bak angrep endret, med tanke på målet til hackerne (ødeleggelse eller penger)?
5. Hvorfor tror du trusselen for cyberangrep oppleves som større nå i 2021 enn de tidligere år?
6. Hvor aktuelt er løsepengevirus i deres sektor/selskap?
7. Hva er et worst-case cyberangrep for dere?

Forskningsspørsmål 2: Hvordan blir risikovurderinger gjort?

8. Har dere egne folk i selskapet som har arbeidsoppgave i å følge med på digitale trusler? Hva er prosedyrene? Er «alle» inkludert i risikovurderinger?
9. Trekker dere erfaringer fra hendelser som skjer andre steder som kunne skjedd hos dere for å være mer proaktive? Følger dere med på nyhetsbildet og årlige rapporter fra f.eks. NSM og PST? Bidrar det til å endre deres risikoanalyser?
10. Fører uønskede hendelser til endring i praksis?

11. Hvordan blir det tatt i betraktning med relasjoner til annen kritisk infrastruktur, hvor et cyberangrep i en kritisk infrastruktur kan gi ringvirkninger i en annen?

Forskningsspørsmål 3: Hvordan har beredskapen endret seg?

12. Den digitale utviklingen skjer i rekordfart, hvordan klarer dere å holde følge med utviklingen? Klarer dere å ha et tilstrekkelig fokus på trusler innad i selskapet?
13. Hvis dere sammenligner beredskapen mot cyberangrep i dag med 5 år siden, hvordan har bedriftens fokus på beredskap endret seg, og på hvilket grunnlag?
14. Hvilken strategi bygger beredskapen på? Unngå angrep eller motstå angrep, eller begge deler?
15. Hvilke prosedyrer har dere for å oppdatere beredskapsplanene? Er det basert på nyhetsbildet, årlige vurderinger, hendelser, m.m?
16. Har dere fokus på å styrke deres beredskap sammen med myndigheter og andre aktører i samfunnet?
17. Hvorfor har beredskap for cyberangrep endret seg (tror du)?

Del 3: Oppsummering

- Har jeg forstått informasjonen riktig?
- Er det noe informanten vil legge til?
- Har informanten tips til noen andre jeg burde snakke med?
- Er oppfølgingsspørsmål over epost/telefon aktuelt?
- Har informanten noen kilder, referanser eller prosedyre som de vil dele med meg i etterkant av intervjuet?