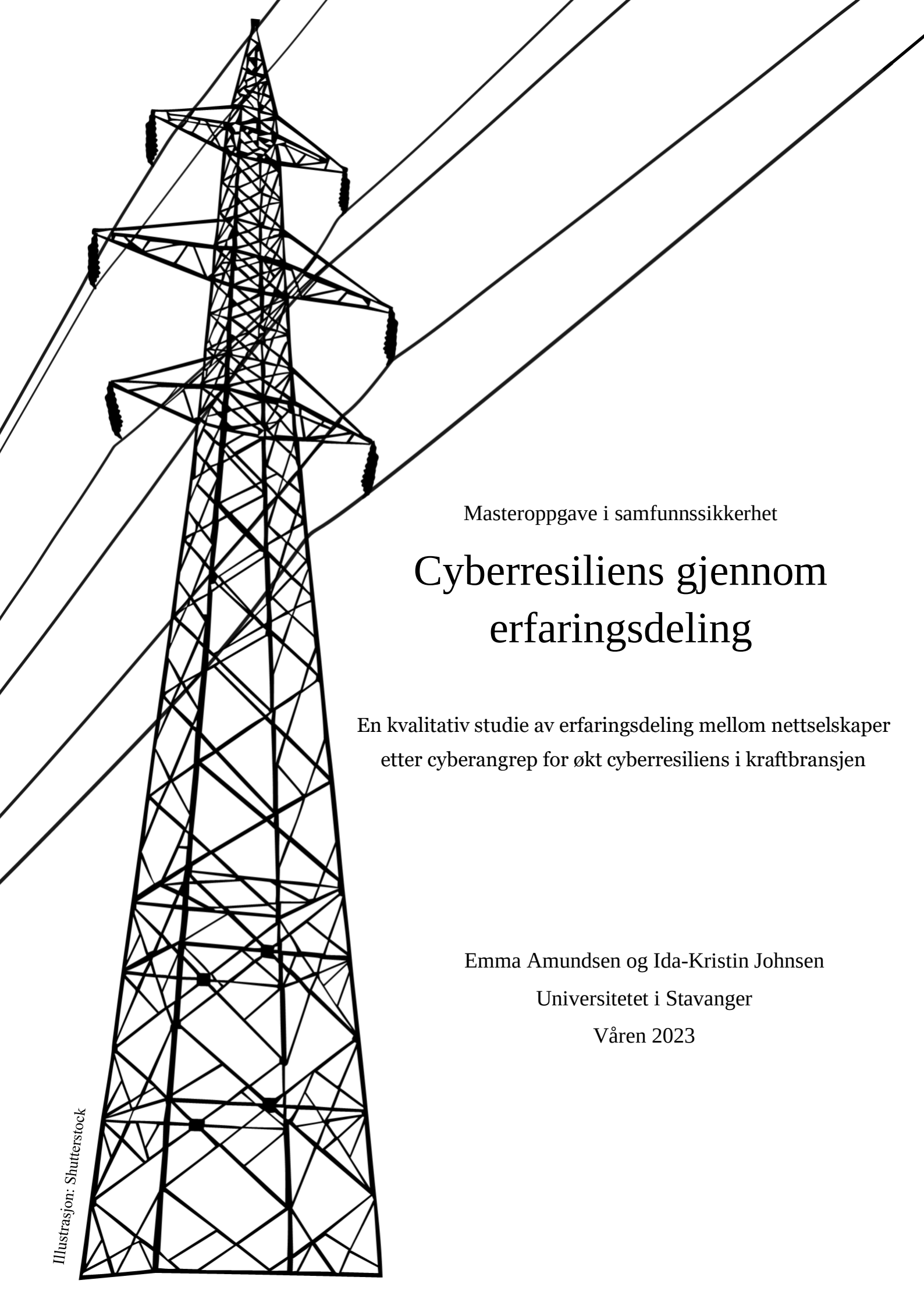
DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet	Vårsemesteret, 2023 Åpen / ~~Konfidensiell~~
Forfattere: Emma Amundsen og Ida-Kristin Johnsen	
Fagansvarlig ved UiS: Kenneth Arne Pettersen Gould Veileder: Kenneth Arne Pettersen Gould	
Tittel på masteroppgaven: Cyberresiliens gjennom erfaringsdeling Engelsk tittel: Cyber resilience through experience sharing	
Studiepoeng: 30	
Emneord: erfaringsdeling, cyberresiliens, cyberangrep, kraftbransjen, strømforsyning, smarte strømnett	Sidetall: 84 + vedlegg/annet: 108 Stavanger, 15.06.23



Illustrasjon: Shutterstock

Masteroppgave i samfunnssikkerhet

Cyberresiliens gjennom erfaringsdeling

En kvalitativ studie av erfaringsdeling mellom nettselskaper etter cyberangrep for økt cyberresiliens i kraftbransjen

Emma Amundsen og Ida-Kristin Johnsen

Universitetet i Stavanger

Våren 2023

Forord

Denne oppgaven markerer avslutningen på en fullført mastergrad i samfunnssikkerhet ved Universitetet i Stavanger. Det har vært to spennende år med mye sosialt og faglig påfyll. Arbeidet med masteroppgaven har vært en krevende, men lærerik prosess. Den har gitt oss mulighet til å utvikle vår kunnskap og kompetanse innenfor samfunnssikkerhet.

Vi ønsker å benytte anledningen til å takke alle informantene som tok seg tid til å stille til intervju. Kunnskapen og innsikten deres har vært uvurderlig for vår forståelse av et svært interessant tema. Det har gjort oppgaven til et relevant bidrag for videre diskusjon.

En spesiell takk går til Kenneth Arne Pettersen Gould for gode råd og innspill. Oppgaven hadde ikke vært den samme uten din veiledning. Du har fått oss til å reflektere, være kritiske, og din positivitet har oppmuntret oss til å se nye muligheter i oppgaven.

Sist, men ikke minst, må vi takke hverandre for et produktivt, lattermildt og fint samarbeid. Vi kom oss helskinnet gjennom, og sammen leverer vi stolt fra oss masteroppgaven vår.

God lesing!

Emma Amundsen og Ida-Kristin Johnsen
Stavanger, 15. juni 2023

Sammendrag

Kraftforsyning er et grunnvilkår for opprettholdelsen av et moderne og komplekst samfunn. Samfunnets avhengighet av en pålitelig strømforsyning krever stadig mer benyttelse av ny teknologi for å utvikle innovative løsninger og øke effektivitet. Samtidig kan implementeringen av smartere strømnett føre til økt sårbarhet for cyberangrep mot kraftbransjen. For å imøtekomme et dynamisk risiko- og trusselbilde, er økt motstandsdyktighet nøkkelen.

Masteroppgaven undersøker hvordan erfaringsdeling mellom nettselskaper etter cyberangrep kan bidra til økt cyberresiliens for å sikre norsk strømforsyning. I den forbindelse har det vært viktig å kartlegge insentiver og utfordringer knyttet til erfaringsdeling. Det har videre vært sentralt for å undersøke hvordan erfaringsdeling kan bidra til strukturell resiliens i nettselskaper, og om det er overførbart til systemisk resiliens på bransjenivå. Studien har tatt utgangspunkt i intervjuer og dokumentanalyse. Intervjuene er gjennomført med sentrale informanter i kraftbransjen, herunder store nettselskaper og ulike samarbeidsorganisasjoner.

Resultatene av studien viser at erfaringsdeling mellom nettselskaper etter cyberangrep kan bidra til økt cyberresiliens basert på tre hovedinsentiver. Disse er gjensidig utbytte, tillit og delt forståelse. Nettselskaper bygger strukturell cyberresiliens gjennom å dele erfaringer med hverandre, og ved å forankre delte erfaringer i eget selskap. Strukturell cyberresiliens i nettselskaper er til en viss grad overførbart til systemisk cyberresiliens, ettersom nettselskapene er en del av en større helhet. For å oppnå systemisk cyberresiliens kreves overførbarhet fra strukturell cyberresiliens, men også en delt forståelse av felles trusler, sårbarheter og verdier. Erfaringsdeling bidrar til å oppnå systemisk cyberresiliens, og systemisk cyberresiliens kan sikre en helhetlig og pålitelig strømforsyning i kraftbransjen. Det vil derfor hevdes at nettselskaper og praksisfelleskap bør legge et solid grunnlag for erfaringsdeling i dag, da dette vil være til deres fordel i møte med fremtidig utvikling av trusselbildet i smarte strømnett.

Innholdsfortegnelse

Liste over figurer og tabeller

1 Innledning

Det norske samfunnet er avhengig av en strømforsyning som er pålitelig, fri for avbrudd, og som opererer med høyest mulig kvalitet. I Norge er andel elektrisitet i energibruken betydelig høyere enn i andre land (Meld. St. 14 (2011-2012)). Veksten i strømforbruket forsterkes av blant annet ny kraftkrevende industri, samt mer utbredt bruk av klimaanlegg og elektriske kjøretøy (Spilde, Hodge, Magnussen, Hole, Buvik & Horne, 2019). Dette stiller enda større krav til strømforsyningen. Sikkerhets- og beredskapsarbeidet i selskaper er derfor essensielt for forsyningssikkerheten (Norges vassdrags- og energidirektorat [NVE], 2023). Utviklingen og økningen av strømforbruk krever et smartere strømnett som kan håndtere og sikre forsyning av strøm. De innovative systemene, som er en sammensmelting av internett og kraftnett, øker effektiviteten og påliteligheten til strømnettet. Samtidig introduseres nye komplekse risikoer, avhengigheter, og sårbarheter (Tøien, Fagermyr, Treider & Remvang, 2021; Pléta, Tvaronavičiené, Casa & Agafonov, 2020). Denne trenden gjør samfunnet sårbart, selv ved mindre bortfall av strømforsyning.

Trusselaktører har en evne til å tilpasse sine angrepsmetoder, og utnytte nye sårbarheter for å ramme strømforsyningen (Nasjonal sikkerhetsmyndighet [NSM], 2023). Mørketallsundersøkelsen (2022) viser hvordan det digitale trusselbildet i Norge har gjennomgått et taktskifte (Næringslivets sikkerhetsråd [NSR], 2022). Det skjer flere cyberangrep, og konsekvensene av angrepene har potensial til å bli enda mer omfattende på grunn av utviklingen av smarte strømnett (Tøien et al., 2021). Sikkerhetsarbeidet må derfor inkludere tiltak som forebygger mot uønskede hendelser, men også tiltak som muliggjør en god håndtering og gjenoppretting etter hendelser. Da vil eventuelle konsekvenser av nedetid reduseres i størst mulig grad. Et slikt fokus i sikkerhetsarbeidet vil bidra til å bygge motstandsdyktighet, også omtalt som resiliens. Regjeringen og NSM er aktører som påpeker viktigheten av å opparbeide resiliens i selskaper. Det kan blant annet gjøres gjennom åpenhet, og deling av informasjon og erfaringer (Meld. St. 38 (2016-2017); NSM, 2023).

Norske selskaper har gode forutsetninger for å håndtere dagens risikobilde, men samarbeid, åpenhet og erfaringsdeling i bransjen blir viktig for å imøtekomme cybertruslene (Meld. St. 38 (2016-2017); NSM, 2023). Dette er et satsingsområde for regjeringen, som mener selskaper og bransjer er avhengig av samvirke og samspill for å avdekke og håndtere cyberangrep (Meld. St. 38 (2016-2017)). Gjennom deling av erfaring etter cyberangrep, kan

selskaper samarbeide om å identifisere trusler og risikoer, samt iverksette nødvendige tiltak. Erfaringsdeling kan gi tilgang på informasjon, som kan føre til at lignende angrepsformer eller trusselaktører oppdages og forhindres (Rak, 2002). På den måten kan erfaringsdeling gi mulighet for økt resiliens i et selskap, ved at man både lærer om metoder for å forhindre angrep, men også metoder for å håndtere angrep som oppstår.

1.1 Bakgrunn

Det digitale domenet gir en ny og større angrepsflate for trusselaktører som har som hensikt å forstyrre eller ødelegge driften av samfunnskritisk infrastruktur. I 2015 gjennomførte russiske trusselaktører et cyberangrep mot kraftforsyningen i Ukraina (Pléta et al., 2020). Angrepet hadde omfattende, men relativt kortvarige konsekvenser. Hendelsen viser samtidig hvordan aktører kan få tilgang til kritisk infrastruktur, og på den måten ha mulighet til å ramme bredt i samfunnet. Det er derav et voksende behov for økt bevissthet, kompetanse og forståelse av cyberangrep mot kritisk infrastruktur (Pléta et al., 2020). En bidragsyter til dette behovet kan være erfaringsdeling i etterkant av cyberangrep.

Det finnes eksempler på cyberangrep hvor aktører på en vellykket måte har delt informasjon underveis og erfaringer i ettertid. I 2019 ble Hydro (2020) rammet av et omfattende cyberangrep, og de bestemte seg tidlig i hendelsesforløpet for å ha en åpen og hyppig kommunikasjon. Gjennom daglig kommunikasjon delte Hydro den informasjonen de kunne, om både utviklingen av angrepet og veien tilbake til normal drift. Eksterne aktører og interessenter responderte positivt på dette (Hydro, 2020). Hydros åpenhet kan sies å ha bidratt til økt bevissthet og forståelse for hva et cyberangrep kan føre til. I etterkant av angrepet har det også kommet fram at Hydros åpenhet trolig hindret nye angrep på andre virksomheter (Næringslivets Hovedorganisasjon, 2019). Eksempelet viser hvordan åpenhet om cyberangrep gjennom erfaringsdeling kan styrke integritet, tillit og omdømme til et selskap. Det viser også hvordan erfaringsdeling kan bidra til å styrke motstandsdyktighet i andre selskaper, og i beste fall forhindre nye cyberangrep.

1.2 Tidligere forskning

Utgangspunktet for våre litteratursøk har vært relevans til oppgavens problemstilling og formål. I gjennomgangen av tidligere forskning vil bidragene som knytter seg tematisk tettest mot problemstillingen bli presentert, da disse har hatt størst betydning for vår forståelse av de

ulike temaene diskutert i oppgaven. Hovedtemaene i oppgaven er erfaringsdeling og cyberresiliens.

1.2.1 Erfaringsdeling

Det eksisterer lite tidligere forskning på erfaringsdeling i kritisk infrastruktur, så det er valgt å inkludere forskning på informasjonsdeling. Informasjonsdeling anses å ha lignende aspekter som erfaringsdeling, og det er dermed valgt å ta utgangspunkt i denne forskningen for å diskutere betydning av erfaringsdeling i kraftbransjen. Generelt beskrives informasjonsdeling som en bidragende faktor for å forstå cyberrisiko og øke IKT-sikkerhet blant aktører i kritisk infrastruktur (Aakre, 2020; Atkins & Lawson, 2021; Bodsberg, Hale, Dahl, Grøtan, Jaatun, Moe & Onshus, 2018; Gjesvik, 2019; Hausken, 2007; Rak, 2002).

Tidligere forskning har, først og fremst, gitt bidrag til forståelsen av insentiver for erfaringsdeling i kritisk infrastruktur. En NUPI-rapport fra 2018 påpeker at cybersikkerhet er spesielt viktig for beskyttelsen av kritisk infrastruktur, og at konsekvensene av svikt potensielt kan være katastrofale (Gjesvik, 2019). Gjensidig utbytte, tillit og delt forståelse er i rapporten identifisert som viktige insentiver for informasjonsdeling. Tillit er også nevnt i en SINTEF-rapport fra 2018, hvor tillit beskrives som viktig for å dele informasjon, og skapes gjennom personlige nettverk for informasjonsdeling (Bodsberg et al., 2018). Ifølge rapporten er det lettere å dele sensitiv informasjon med individer en har personlig kjennskap til. Rapporten trekker også frem bevissthet rundt hvilke kritiske verdier som krever beskyttelse for å oppnå god IKT-sikkerhet. En annen sentral publikasjon er Atkins og Lawson (2021), som skriver om samarbeid rundt cybersikkerhet i finanssektoren i USA. Viktige funn for oppgavens kontekst var at samarbeid ble akselerert i møte med risiko som truer systemet som helhet, og at regulatoriske myndighetenes innflytelse som pådriver for cybersikkerhet ikke var av større betydning enn de investeringene som aktørene gjorde selv (Atkins & Lawson, 2021). De presenterte faktorene har hatt betydning for hvordan vi har kategorisert ulike insentiver for erfaringsdeling mellom nettselskaper i kraftbransjen.

Tidligere forskning har i tillegg gitt bidrag til forståelsen av utfordringer med erfaringsdeling i kraftbransjen. Aakre (2020) sin artikkel om hvordan åpenhet kan bidra til å forstå cyberrisiko har i denne sammenheng vært viktig. I artikkelen beskriver hun hvordan informasjonsutveksling og kommunikasjon kan redusere det ukjente og gi bedre grunnlag for aktører til å arbeide med cybertrusler (Aakre, 2020). Å dele i etterkant av cyberangrep ble

likevel beskrevet som å kreve en villighet til å utgi seg selv på en måte som ellers ikke var ønskelig. Det ble trukket frem to hovedutfordringer tilknyttet informasjonsdeling; skam og redsel for hvordan informasjon kan brukes mot en. Rak (2002) trakk også fram lignende utfordringer i sin artikkel om informasjonsdeling i beskyttelsen av kritisk infrastruktur. Artikkelen definerte tre utfordringer for informasjonsdeling; mangel på tillit, bekymring over beskyttelsen av delt informasjon, og mangel på gjengjeldelse av deling. Ifølge Rak (2002) er det ønskelig med todelt deling, hvor en både føler at andre deler med deg, og at du selv deler med andre. For at todelt deling skal finne sted er det nødvendig at aktører har en forståelse av sårbarheter i egne systemer. I artikkelen til Hausken (2007), som omhandler informasjonsdeling mellom selskaper i møte med cyberangrep, presenteres det derimot et gratispassasjer-dilemma. Dilemmaet beskriver en utfordring hvor aktører ikke ser grunn til å dele informasjon med andre. I andre tilfeller har selve volumet av delt informasjon blitt sett som en utfordring for utbytte aktører har av informasjonsdeling (Gjesvik, 2019). Dette utfordrer følelsen av merverdi, som er viktig om informasjonsdeling skal oppleves som noe som gir gjensidig utbytte. De presenterte utfordringene har hatt betydning for hvordan vi har kategorisert ulike utfordringer mot erfaringsdeling mellom nettselskaper i kraftbransjen.

1.2.2 Cyberresiliens

Det finnes mye forskning på cyberresiliens, som er et viktig tema innenfor cybersikkerhet. I denne sammenheng blir det særlig relevant å se på cyberresiliens som begrep, og cyberresiliens i kritisk infrastruktur. Cyberresiliens har fått en sentral posisjon i måten organisasjoner kan forbedre sin evne til å forebygge og gjenopprette sin virksomhet etter cyberangrep. Begrepet cyberreiliens er noe omdiskutert, og ulike forfattere har påpekt viktigheten av å etablere en felles definisjon eller forståelse (Björck, Henkel, Stirna & Zdravkovic, 2015; Hausken, 2020). Björck et al. (2015) presenterer i kapittelet «Cyber resilience – fundamentals for a definition» en definisjon som handler om evnen til å opprettholde funksjonalitet og kontinuitet, selv under cyberangrep eller påvirkning. Videre vektlegger Björck et al. (2015) gjenoppretting og læring etter et angrep for å øke cyberresiliens mot fremtidige angrep. Forfatterne konkluderer med at dette er viktige elementer å ha med i en definisjon av cyberresiliens, og at redegjørelsen kan styrke arbeidet med cyberresiliens i selskaper og samfunnet. Samtidig påpeker Hausken (2020) viktigheten av å utvikle helhetlig tilnærming til cyberresiliens, hvor kombinasjonen av tekniske, organisatoriske og samfunnsmessige aspekter må tas i betraktning.

Det finnes videre et stort utvalg av artikler som omhandler resiliens og cyberresiliens i kritisk infrastruktur (Aoyama, Naruoka, Koshijima & Watanabe, 2015; Brown, Seville & Vargo, 2017; Salvi, Spagnoletti & Noori, 2022). Cyberresiliens har blitt en nøkkelegenskap for kritisk infrastruktur, som til enhver tid blir utsatt for cybertrusler. Cantelmi, Di Gravio og Patriarca (2021, s. 342, egen oversettelse) beskriver det på følgende måte: «å administrere kritisk infrastruktur, betyr å administrere kritisk infrastruktur sin resiliens». Artikkelen peker på det brede søkelyset med å identifisere cybersårbarheter og forhindre cyberangrep i tidligere forskning, men det har vært mindre oppmerksomhet rundt å forbedre cyberresiliens. De omtaler cyberresiliens som et underutviklet domene i moderne kritisk infrastruktur. Noe som gjør området ekstra utfordrende er raskt fremvoksende gjensidige avhengigheter i cyberfysiske systemene (Cantelmi et al., 2021).

En annen artikkel som også påpeker cyberresiliens sine forskningsmessige mangler, er Hausken (2020) i artikkelen «Cyber resilience in firms, organizations and societies». Avslutningsvis i artikkelen presenteres syv punkter som bør undersøkes nærmere i fremtidig forskning av cyberresiliens. Noen av punktene som nevnes er: (1) «fokus på å lære fra fortiden, tilpasse seg nåtiden og utvikle seg inn i fremtiden», (2) «samling av historiske data om cyberhendelser, og årsaker og konsekvenser av systemiske, menneskelige, organisatoriske og strategiske feil», og (3) «vurdere om cyberresiliente aktører potensielt kan bli bedre egnet til å håndtere ukjente ukjente» (Hausken, 2020, s. 7, egen oversettelse). Denne oppgaven vil særlig være en bidragsyter til det første punktet, ved å undersøke om erfaringsdeling gjennom læring fra fortiden kan bidra til økt cyberresiliens. Det vil både ha betydning for evnen til å tilpasse seg nåtiden, og utvikling for å imøtekomme trusselbildet i tiden fremover.

1.3 Problemstilling og forskningsspørsmål

Strømforsyning er et grunnvilkår for opprettholdelse av et moderne og komplekst samfunn, og blir i stadig større grad avhengig av ny teknologi for utvikling av innovative løsninger og økt effektivitet (NOU 2006: 6). Samtidig introduseres nye komplekse risikoer, avhengigheter, og sårbarheter. Disse kan utnyttes av trusselaktører som ønsker å ramme strømforsyning (Pléta et al., 2020). Økt motstandsdyktighet er nøkkelen for å imøtekomme risiko- og trusselbildet i kraftbransjen (NSM, 2023). Det blir dermed viktig at nettselskapene samarbeider for cyberresiliens i bransjen. Én måte å øke cyberresiliens på er gjennom deling av erfaringer etter cyberangrep.

Målet for denne oppgaven er å undersøke hvordan forskningsfeltene erfaringsdeling og cyberresiliens henger sammen. For å undersøke hvordan erfaringsdeling kan bidra til økt cyberresiliens, er følgende problemstilling utarbeidet:

Hvordan kan erfaringsdeling mellom nettselskaper etter cyberangrep bidra til økt cyberresiliens for å sikre norsk strømforsyning?

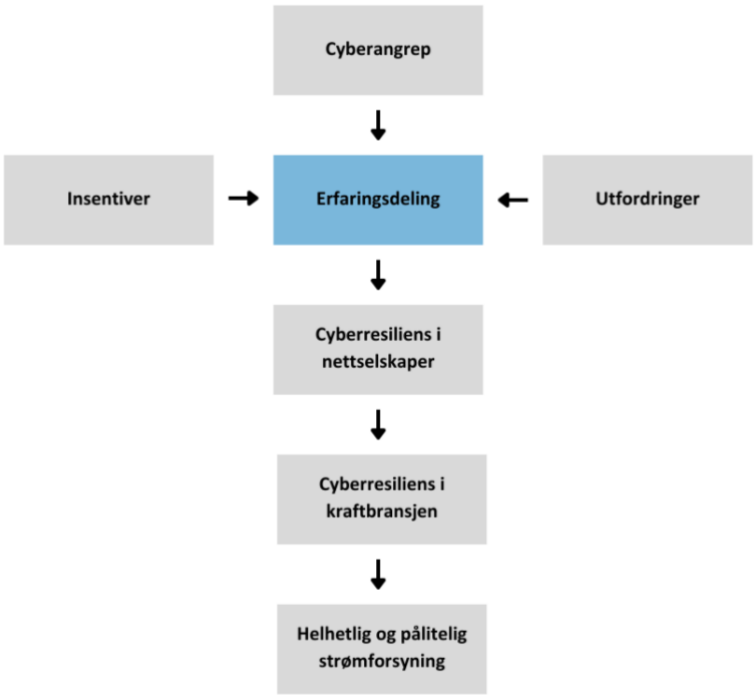
Følgende forskningsspørsmål er utformet for å besvare problemstillingen:
F1: *Hvilke insentiver og utfordringer knytter nettselskaper til erfaringsdeling etter cyberangrep, og hvordan påvirker disse faktorene erfaringsdeling mellom nettselskaper?*
For å besvare problemstillingen vil det være essensielt å utforske hvilke insentiver og utfordringer nettselskapene knytter til å dele erfaringer etter cyberangrep. Insentivene vil danne grunnlag for hvorfor nettselskaper velger å dele erfaringer med hverandre. Utfordringer vil undersøkes i forbindelse med insentiver, og det vil drøftes hvorvidt insentivene knyttet til erfaringsdeling svekkes av de identifiserte utfordringene. Basert på drøftingen vil det være mulig å svare på hvordan insentiver og utfordringer påvirker erfaringsdeling mellom nettselskapene.

F2: *Hvordan bidrar erfaringsdeling etter cyberangrep til å øke cyberresiliens i nettselskaper, og er cyberresiliens på selskapsnivå overførbart til cyberresiliens på bransjenivå?*
For å imøtekomme trusselen for cyberangrep og fremtidens smartere strømnett, bør både selskaper og bransjen øke cyberresiliens. Det vil dermed være hensiktsmessig å besvare hvordan nettselskaper kan bruke erfaringsdeling for å øke cyberresiliens etter cyberangrep. I den forbindelse vil det også være relevant å undersøke hvorvidt cyberresiliens på selskapsnivå kan være overførbart til cyberresiliens på bransjenivå.

Forskningsspørsmålene bidrar til å avgrense og tydeliggjøre fokuset i oppgaven. Spørsmålene skaper en målrettet tilnærming hvor erfaringsdeling vil bli sett i sammenheng med insentiver, utfordringer og cyberresiliens. Dette bidrar til å opprettholde fokus gjennom oppgaven og sikrer mulighet til å gå i dybden på de valgte forskningsspørsmålene. Det gir videre en klar ramme for empiri- og analysekapittelet, og spesielt drøftingskapittelet. Dette har vært formålstjenlig for oppgavens formidlingsevne og struktur.

1.3.1 Sammenheng mellom oppgavens temaer

Figur 1 visualiserer hvordan de sentrale temaene i oppgaven interagerer.



Figur 1: Sammenheng mellom oppgavens temaer

I figuren er cyberangrep plassert øverst som en utløsende hendelse. I etterkant av et cyberangrep deles erfaringer blant nettselskaper. Erfaringsdeling blir påvirket av både insentiver for å dele, samt utfordringer som knyttes til deling av erfaringer. Insentiver og utfordringer er dermed plassert i relasjon til erfaringsdeling. Videre kan erfaringsdeling bidra til cyberresiliens i nettselskaper ved å presentere nye og utbedrede metoder og praksiser for beskyttelse mot og gjenopprettelse etter cyberangrep. Ved å øke cyberresiliens gjennom erfaringsdeling i ett og ett nettselskap, kan erfaringsdeling være bidragende til å øke cyberresiliens på bransjenivå. Det kan ha betydning for evnen cyberresiliens på bransjenivå har til å sikre en helhetlig og pålitelig strømforsyning i Norge.

1.3.2 Avgrensning

I oppgaven er det foretatt noen avgrensninger for å oppnå dybde og klarhet i besvarelse av problemstillingen. I kraftbransjen eksisterer det mange aktører som er sentrale i ulike ledd. Oppgaven undersøker øking av cyberresiliens for å sikre norsk strømforsyning, og i den forbindelse er oppgaven avgrenset til nettselskaper, som har som hovedoppgave å drifte strømnettet. Fokuset er på forholdet mellom nettselskaper, og nettselskaper som en helhet på

bransjenivå. Når oppgaven omtaler *kraftbransjen,* er det dermed de aktørene som sikrer strømforsyning som står i fokus. Videre er det avgrenset til å intervjue kun store nettselskaper, og dermed ikke små eller mellomstore. Valget et tatt på bakgrunn av en antakelse om at store nettselskaper har tilgang til større ressurser, i form av tid og ansatte, for å delta i erfaringsdeling.

I tillegg til store nettselskaper har vi valgt å intervjue bransjespesifikke organisasjoner som tilrettelegger for informasjons- og erfaringsdeling. Det er gjort for å få oversikt over de ulike arenaene for samarbeid, samt en forståelse for hvordan de oppfatter og beskriver erfaringsdeling i sin organisasjon. Samtlige organisasjoner har IKT-sikkerhet som ett av sine fokusområder. Det er ikke foretatt noen avgrensninger i forbindelse med størrelse eller medlemsbase. Nasjonale organisasjoner på tvers av bransjer, er ikke inkludert i oppgaven.

1.4 Oppgavens struktur

I det første kapittelet presenteres oppgavens tema, tidligere forskning, problemstilling og forskningsspørsmål, samt en avgrensning av oppgaven.

I det andre kapittelet presenteres oppgavens kontekst, som inkluderer kraftforsyning som kritisk samfunnsfunksjon, kraftsystemet, rammeverk, og organisasjoner som tilrettelegger for erfaringsdeling i kraftbransjen.

I det tredje kapittelet vil det teoretiske rammeverket bli presentert. Teorien består av komplekse systemer, cyberangrep, resiliens, og erfaringsdeling.

I det fjerde kapittelet vil forskningsmetode bli redegjort og begrunnet. Styrker og svakheter ved oppgavens metodevalg vil også presenteres.

I det femte kapittelet vil empiriske funn presenteres. Hovedfunn er strukturert etter seks temaer valgt på bakgrunn av funn fra intervjuer og dokumentanalyse.

I det sjette kapittelet vil forskningsspørsmålene besvares basert på empiriske funn og det teoretiske rammeverk. Drøftingen vil gi grunnlag for å kunne besvare oppgavens problemstilling i konklusjonen, som er det avsluttende kapittelet.

2 Kontekst

2.1 Kraftforsyning som kritisk samfunnsfunksjon

Samfunnet er avhengig av en rekke samfunnsfunksjoner og infrastrukturer som kan kategoriseres som kritisk. De grunnleggende samfunnsbehovene blir dekket av kritiske samfunnsfunksjoner, som videre er avhengig av infrastrukturer for å fungere (NOU 2006: 6). Kritiske samfunnsfunksjoner kan inndeles i tre underkategorier som indikerer hvilken påvirkning svikt i den kritiske samfunnsfunksjonen kan ha for samfunnet og befolkningen. Underkategoriene er (1) styringsevne og suverenitet, (2) befolkningens sikkerhet, og (3) samfunnets funksjonalitet. Samfunnets funksjonalitet innebærer «kontinuitet i forsyninger og infrastrukturbaserte tjenester», og kraftforsyning inngår i denne kategorien (Direktoratet for samfunnssikkerhet og beredskap [DSB], 2016, s. 28). Kraftforsyning er et grunnvilkår for opprettholdelsen av et moderne og komplekst samfunn (NOU 2006: 6), og omfatter «de systemer og leveranser som er nødvendig for å ivareta samfunnets behov for elektrisk energi til oppvarming, husholdning, produksjon, transport med mer, og fjernvarme der slike anlegg er utbygd» (DSB, 2016, s. 86). Det er en gjensidig avhengighet og sammenkobling av kritiske samfunnsfunksjoner og infrastruktur, og i denne sammenheng er kraftforsyning avhengig av kritisk infrastruktur for å fungere (Rinaldi, Peerenboom & Kelly, 2001).

Kritisk infrastruktur kan defineres som «de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse» (NOU 2006: 6, s. 32). Forsyningsnettet er én kritisk infrastruktur som kraftforsyning er avhengig av, men det er også flere andre samfunnskritiske funksjoner i dagens samfunn som er avhengig av forsyning av strøm for å opprettholde sin funksjon. Samfunnets avhengighet av kraftforsyning er en av grunnene til at kraftsystemet er et attraktivt mål for trusselaktører. Det stilles større og større krav til leveringssikkerhet og funksjonalitet (Sørgard, Reiten & Bjella, 2014).

2.2 Det norske kraftsystemet

Kraftsystemet i Norge består av et mangfold av aktører innen produksjon, forsyning, forvaltning og tilsyn. Kraftsystemet er derfor en samlebetegnelse på alle de komponentene som sørger for at kraft produseres og overføres fra produksjonsanlegg til kraftstasjoner, og til slutt til forbrukeren (NVE, 2023). Den fysiske delen av kraftinfrastrukturen inkluderer alle fysiske installasjoner, anlegg og komponenter som bringer kraft rundt i Norge. Dette kan være

demninger, kraftstasjoner, kraftlinjer og transformatorer. For å styre de fysiske komponentene eksisterer det drifts- og styringssystemer som skal sørge for sikker og effektiv drift av kraftinfrastrukturen (NOU, 2006: 6). Det er behov for å styre strømmen gjennom slike systemer, ettersom kraftdistribusjon fungerer som et just-in-time-system. Strøm er nemlig en ferskvare som må brukes i samme sekund som den lages. Det må derfor eksistere en balanse mellom det som brukes og det som lages til enhver tid. Dette kalles momentan balanse (Statnett, 2018).

Strømnettets balanse er selve ryggraden i kraftsystemet, og bindeleddet mellom produsent og forbruker. Regulering av den momentane balansen i strømnettet skjer på tre ulike nivåer; transmisjonsnettet, regionalnettet og distribusjonsnettet. Energi fra produksjon og import overføres via transmisjonsnettet på tvers av Norge. Dette er primært eid og forvaltet av Statnett, som er et statsforetak underlagt Olje- og energidepartementet (Statnett, 2018). Energien når ut til forbrukeren gjennom regional- og distribusjonsnett. Disse eies og forvaltes av nettselskaper, som igjen er eid av hovedsakelig kommuner og fylkeskommuner i områdene de driftes (Olje- og energidepartementet, 2022; Statnett, 2018).

2.2.1 Nettselskaper

Det er tre essensielle elementer som utgjør infrastrukturen i forsyningen av kraft; produksjon, overføring og omsetning (NOU 2022: 6). Overføringen av strøm til forbruker er i denne oppgaven svært relevant, og nettselskapene har en sentral rolle i dette arbeidet. I tillegg til å binde kraftproduksjon og forbruk sammen, har nettselskapene ansvar for en sikker drift og imøtekomme forespørselen av strøm (NOU 2022: 6). Et nettselskap er ansvarlig for å drifte strømnettet i et geografisk område, og nettselskapene har derfor naturlig monopol over strømnettet innen sitt geografiske område (Statnett, 2018).

Når forventninger til uavbrutt strømforsyning øker, øker også presset på de lokale nettselskapene (Meld. St. 25 (2015-2016)). Det enkelte nettselskapet må, i møte med forventningene, prioritere mellom kortsiktige og langsiktige investeringer. Kortsiktige investeringer omhandler drift og vedlikehold, og er aktiviteter som er nødvendig for å opprettholde infrastrukturen på et nivå som er tilfredsstillende sikkerhetsmessig, eller at systemet fungerer etter tiltenkt funksjon (NOU 2012: 9). Langsiktige investeringer omhandler utvikling og utbygging av infrastrukturen. Investeringer her kan være svært kompliserte og kostbare ettersom det krever store mengder ressurser i form av arbeidskraft, materialer og tid

(NOU 2012: 9). Det kreves derfor godt utarbeidede planer, både kortsiktig og langsiktig, for å sikre at nettselskaper evner å ta gode beslutninger knyttet til IKT-sikkerhet.

2.2.2 Smarte strømnett

Strømnettets evne til å håndtere dagens elektrifiserte samfunn må modnes i takt med samfunnsutviklingen (SINTEF, u.å). Det må derfor utvikles teknologier som gjør drift og planlegging av smarte strømnett, også kalt smartgrid, mer automatisert (Pléta et al., 2020). Smartgrid er samlebetegnelsen på en ny generasjon strømnett – «det vi kaller fremtidens digitaliserte, smarte strømnett» (SINTEF, u.å). Det finnes mange ulike definisjoner på hva smartgrid består av. Alle definisjonene innebærer en beskrivelse av økt grad av intelligens i strømnettet gjennom automatisering og digitalisering, med ønske om høyere grad av effektivitet, sikkerhet og samfunnsøkonomisk og miljømessig sparing. Kort sagt kan smartgrid beskrives som en sammensmelting av internett og kraftnett. Sammen utgjør dette et system hvor fjernstyring og observasjon av anlegg og komponenter er mulig gjennom internett. De mest sentrale elementene i smarte strømnett er automatiske måle- og styringssystemer (AMS), tingenes internett (IoT), operasjonelle driftssystemer (SCADA), bruk av stordata, og skybaserte tjenester (Pléta et al., 2020). Denne oppgaven har ikke som formål å gå dypere inn på de ulike elementene, men de nevnes for å understreke kompleksiteten som har oppstått i det norske kraftnettet.

Smarte strømnett fører til mer hensiktsmessig bruk av strøm for kunder, og kapasiteten i strømnettet utnyttes bedre gjennom raskere og mer effektiv tilgang til informasjon (SINTEF, u.å). Den konstante oppdateringen av nye systemer innen infrastruktur åpner på denne måten for mange nye muligheter. Et angrepsmål i vekst er bransjer med operasjonell teknologi (OT), slik som EKOM, vann- og avløp, og strømforsyning (NOU, 2012: 9). Sammensmeltingen av IT og OT i kritisk infrastruktur (IIoT) har økt sannsynligheten for å bli angrepet til et kritisk punkt (Pléta et al., 2020). Av den grunn har beskyttelse av kritisk infrastruktur blitt et mer relevant tema i møte med ny teknologisk utvikling.

2.2.3 IKT-sikkerhetstilstanden i norsk kraftforsyning

Forsyningssikkerheten i Norge er avhengig av god beredskap for å håndtere IKT-angrep mot strømforsyningen. Det er nettselskapene selv som er ansvarlige for å planlegge og gjennomføre de nødvendige investeringene i sitt nett for å ivareta forsyning av strøm til

forbrukere (NOU 2022: 6). Dette gjelder også IKT-sikkerhetstiltak (Riksrevisjonen, 2021). IKT-sikkerhet kan defineres som «beskyttelsen av informasjons- og kommunikasjons-systemene, samvirket mellom systemene, tjenestene som leveres av systemene, eller informasjon som behandles i systemene» (Riksrevisjonen, 2021, s. 6). Arbeidet med IKT-sikkerhet i kraftforsyningen har som hovedmål å fremme en sikker kraftforsyning, og som delmål å påse at beredskapen i energiforsyningen er god og i tråd med gjeldende krav (Riksrevisjonen, 2021).

Undersøkelser har vist eksisterende svakheter hos flere av nettselskapenes arbeid med IKT-sikkerhet (Riksrevisjonen, 2021). Det stilles mange krav som er funksjonsbaserte, noe som vil si at det er selskapene selv som må vurdere hvilke sikkerhetsløsninger som vil gi tilstrekkelig IKT-sikkerhet. Funksjonsbaserte krav gir større fleksibilitet til å følge den teknologiske utviklingen, samtidig som kravene kan tilpasses selskapers verdier og risiko (Riksrevisjonen, 2021). Denne formen for IKT-sikkerhetsarbeid krever høy kompetanse og kapasitet. Mangel på IKT-sikkerhetskompetanse hos nettselskaper har vist seg å være en stor utfordring for den generelle IKT-sikkerheten i kraftbransjen. Rapporter peker på et behov for å styrke kompetanse rundt egne systemer, for å øke forståelse knyttet til risiko og sårbarheter som oppstår i digitaliseringen av kraftbransjen (Frøystad, Jaatun, Bersmed & Moe, 2018; Riksrevisjonen, 2021; Røyksund & Valdal, 2020; Tøien et al., 2021).

2.3 Rammeverk for kraftforsyningsberedskap

2.3.1 Energiloven og kraftberedskapsforskriften

For å ivareta blant annet forsyningssikkerhet, verdiskapning og effektiv overføring, er det utformet lover og forskrifter i kraftbransjen (Meld. St. 25 (2015-2016)). I denne sammenheng er energiloven (1990) kapittel 9 om beredskap svært relevant. Kapittelet beskriver blant annet kraftforsyningens beredskapsorganisasjon (KBO), beredskapstiltak, og informasjonssikkerhet. KBO består av KBO-enheter, KDS (kraftforsyningens distriktssjefer) og beredskapsmyndigheten, og KSL (kraftforsyningens sentrale ledelse). I forlengelse av energiloven er kraftberedskapsforskriften (2012) utarbeidet og spesielt viktig.

Kraftberedskapsforskriften (2012) skal opprettholde formålet med energiloven gjennom å bygge en robust kraftforsyning. Virkeområdet til forskriften er «forebygging, håndtering og begrensning av virkningene av ekstraordinære situasjoner som kan skade eller hindre

produksjon, omforming, overføring, omsetning og fordeling av elektrisk energi eller fjernvarme» (Kraftberedskapsforskriften, 2012, § 1-2). Forskriften gjelder for virksomheter som blir definert som KBO-enheter. KBO-enheter er større kraftprodusenter, nettselskaper, fjernvarmeselskaper, og større vindkraftverk som har klassifiserte anlegg, jf. kap. 5 i kraftberedskapsforskriften (2012). Andre virksomheter kan i tillegg bli utpekt av NVE som KBO-enhet, hvis de har vesentlig betydning for kraftforsyningen. NVE har det overordnede ansvaret for KBO (Meld. St. 25 (2015-2016)).

Det er mange krav som følger av å være en KBO-enhet. Ett av kravene er blant annet å utpeke en IKT-sikkerhetskoordinator. Hovedoppgaven til en IKT-sikkerhetskoordinator er å ha oversikt over arbeidet med IKT-sikkerhet og være bindeledd til beredskapsmyndigheten i forbindelse med IKT-sikkerhet. Videre er det forskriftsfestet at KBO-enheter, eller andre pålagte virksomheter, skal varsle NVE om ekstraordinære hendelser (Kraftberedskapsforskriften, 2012, § 2-5). Når det oppstår uønskede hendelser er i tillegg KBO-enhetene forpliktet til å informere internt i virksomheten, og eksternt til berørte myndigheter, samfunnskritiske virksomheter, andre relevante KBO-enheter, publikum eller media (Kraftberedskapsforskriften, 2012, § 2-8). En viktig del av prosessen med å bli utsatt for en uønsket hendelse, er å gjennomføre en evaluering i ettertid. Dette er forskriftsfestet i § 2-9 (Kraftberedskapsforskriften, 2012). Gjennomføring av en evaluering bidrar til å forbedre kompetanse, oppdatering av planer og risikovurderinger, og iverksetting av sikkerhetstiltak.

Kraftsensitiv informasjon er taushetsbelagt og defineres som «spesifikk og inngående opplysninger om kraftforsyningen som kan brukes til å skade anlegg, system eller annet eller påvirke funksjoner som har betydning for kraftforsyningen» (Kraftberedskapsforskriften, 2012, § 6-2). Energiloven (1990, § 9-3) skriver at «alle enheter i KBO skal vurdere sikkerheten ved all behandling av informasjon om kraftforsyningen». Det inkluderer å identifisere informasjon som er kraftsensitiv, hvor den befinner seg og hvem som har tilgang (Kraftberedskapsforskriften, 2012, § 6-1). KBO-enhetene må selv vurdere om det er «tjenstlig behov» for å videreformidle den sensitive informasjonen. Hvis kraftsensitiv informasjon blir delt av KBO-enheter med andre virksomheter, kan ikke de formidle informasjonen videre (Kraftberedskapsforskriften, 2012, § 6-1).

2.3.2 NSM sine grunnprinsipper for IKT-sikkerhet

NSM og virksomheter som forvalter kritiske samfunnsfunksjoner eller kritisk infrastruktur, har samarbeidet om å utarbeide fire overordnede grunnprinsipper som en del av det forebyggende arbeidet med IKT-sikkerhet (NSM, 2020). Formålet med prinsippene er å beskytte mot uønsket tilgang, misbruk eller skade i informasjonssystemer. Aktiv opprettholdelse og etterfølgelse av prinsippene bidrar til god beskyttelse mot cybertrusler, men det er ingen garanti for at cyberangrep ikke oppstår (NSM, 2020).

Det første prinsippet er *identifisere og kartlegge*. Først og fremst handler det om å opparbeide en forståelse av virksomheten, som er særlig tilknyttet IKT-systemene, prioriteringer til ledelsen, og styringsstrukturer. Deretter kan sikkerhetstiltak fokuseres mot områder som har betydning for risikostyringen. Dette arbeidet foregår kontinuerlig og utvikles over tid (NSM, 2020). Det andre prinsippet er *beskytte og opprettholde.* For å ivareta en forsvarlig sikring av IKT-systemene, må virksomheter beskytte og opprettholde en sikker tilstand over tid og ved endringer (NSM, 2020). Det utføres ved å etablere tiltak som motstår eller begrenser konsekvensene av et cyberangrep. I praksis kan det for eksempel innebære å konfigurere og tilpasse programvarer til ulike oppgaver i virksomheten (Tøien et al., 2021). Det tredje prinsippet er *oppdage*, og innebærer å oppdage og fjerne sårbarheter og trusler. Det gjøres ved å systematisk kartlegge sårbarheter og overvåke IKT-systemet, samt oppdage avvik fra sikker og ønsket normaltilstand (NSM, 2020). Mangelfull overvåkning og analyser av systemene, kan hjelpe angripere med å skjule handlinger i IKT-systemet til virksomheter (Tøien et al., 2021). Det siste prinsippet er *håndtere og gjenopprette*. Prinsippet handler om effektiv håndtering av uønskede hendelser og gjenoppretting av funksjonaliteten til systemet (NSM, 2020).

2.4 Organisasjoner som tilrettelegger for erfaringsdeling i kraftbransjen

I kraftbransjen finnes det ulike organisasjoner som tilrettelegger for samarbeid og erfaringsdeling mellom nettselskaper. I den sammenheng vil det redegjøres for KraftCERT, Forum for informasjonssikkerhet i kraftforsyningen (FSK), Samfunnsbedriftene, Nettalliansen og Fornybar Norge. KraftCERT er et sektor-responsmiljø for blant annet kraftbransjen som ble opprettet i 2014, og de bistår selskaper med håndtering av hendelser og informasjonsdeling. Selv om KraftCERT er et uavhengig selskap, har de et varslingsansvar til myndighetene ved alvorlige cyberangrep (KraftCERT, u.å.). FSK er et bransjeinitiativ som

ble stiftet i 2010. Bakgrunnen for stiftelsen var en oppfordring fra NVE om mer samarbeid om metoder og løsninger for informasjonssikkerhet, som kan bidra til å oppfylle kravene i kraftberedskapsforskriften. Erfaringsdelingen mellom medlemmene foregår gjennom arbeidsgrupper, workshops, diskusjoner m.m. (FSK, u.å.).

En tredje organisasjon som også tilrettelegger for erfaringsdeling i bransjen er Samfunnsbedriftene Energi. Medlemsbedriftene får bistand med å bygge beredskap for leveringssikkerhet, og får tilgang til kompetansebyggende kurs og programmer for bransjen (Samfunnbedriftene, u.å.). Nettalliansen er den fjerde organisasjonen, og består av små og mellomstore nettselskaper. De ble dannet av åtte små nettselskaper som gikk sammen om felles innkjøp, kompetanse- og ressursdeling, digitalisering og arbeidsprosesser som standardiseres. Nettalliansen bidrar til å bygge en bransjeløsning for IT-behov, hvor samhandling på tvers er sentralt (Nettalliansen, u.å.). Til slutt er Fornybar Norge (u.å.) en interesseorganisasjon for bedrifter i fornybarnæringen som har satt samarbeid rundt IKT-sikkerhet på agendaen. Interesseorganisasjonen avholder kurs og konferanser både digitalt og fysisk. De støtter medlemmene og tilrettelegger for kompetanseheving i bransjen (Fornybar Norge, u.å.). Det eksisterer dermed flere organisasjoner som har samarbeid og erfaringsdeling som en del av sitt virkeområde.

3 Teori

I teorikapittelet er formålet å presentere og utforske teorier som kan bidra til å besvare forskningsspørsmål og problemstilling. Kapittelet innleder med en redegjørelse av komplekse systemer, hvor cyberfysisk system er et relevant bidrag. Videre vil cyberangrep presenteres i lys av trefaktormodellen. Det vil også være hensiktsmessig å behandle begrepet resiliens, og ulike aspekter ved begrepet. Til slutt vil teori tilknyttet erfaringsdeling bli presentert, hvor erfaringsdeling settes i sammenheng med kunnskap og læring.

3.1 Komplekse systemer

Det har blitt nødvendig for samfunnet å utvikle komplekse systemer i møte med blant annet teknologisk utvikling, økende krav til produktivitet og effektivisering. Komplekse systemer er systemer som består av mange deler som samhandler på en uforutsigbar måte. Charles Perrow og Nancy Leveson er to teoretikere som har bidratt til å øke forståelsen av komplekse systemer, og hvordan de kan analyseres og forbedres for å redusere risikoen for ulykker og feil. Normal accident theory (NAT) forklarer innebygde risikoer for ulykker i komplekse og tett koblede systemer, som gjør ulykker «normale» (Perrow, 1999).

Det er oppbyggingen av systemene som forklarer feilene som oppstår, og det tilsier at organisasjonen eller menneskene ikke kunne forhindret ulykken. Perrow (1999) opererer med en dimensjonering fra lineær til kompleks, og fra løst til tett koblede systemer. Systemenes karakteristikker og sammensetninger gjør det umulig å forutse alle scenarioer og feil som potensielt kan oppstå, og uforutsette interaksjoner som kan finne sted. Enheter og deler er nært knyttet i komplekse systemer, selv om de ikke hører sammen. Det skaper interaksjoner som er uforutsette. På den andre siden av skalaen eksisterer det lineære systemer som har større avstand mellom direkte knyttede deler og enheter. Interaksjoner oppstår sjeldent i slike systemer (Perrow, 1999).

Systemulykker kan ikke forebygges, men det finnes styringsløsninger for komplekse systemer som er tett koblet. Desentralisert ledelse styrer best komplekse og løst koblede systemer, mens sentralisert ledelse styrer best lineære og tett koblede systemer. I desentralisert styring er ansvaret for risikohåndtering fordelt mellom aktører, noe som sikrer at en får analysert en uønsket hendelse og minimere konsekvensene av denne. Etter dette må gjenopprettelsestiltak finne sted. Et løst koblet system gjør eksperimentering med ressurser og alternative løsninger

mulig (Perrow, 1999). En sentralisert styring sikrer oversikt og helhetlig forståelse av et system. Gjennom denne formen for styring blir avgjørelser om sikkerhet tatt av en sentral ledelse, noe som bidrar til konsistent styring og allokering av ressurser (Perrow, 1999). Komplekse systemer som er tett koblet bør styres med en kombinasjon av desentralisering og sentralisering. Dette er svært utfordrende i praksis, og ifølge Perrow (1999) nærmest umulig.

Nancy Leveson presenterer en teori om kompleksitet som tar sikte på å forstå og håndtere risiko i komplekse systemer. Systemene som blant annet blir inkludert i samfunnsviktige funksjoner blir omtalt som organisert kompleksitet. Teorien tar utgangspunkt i at komplekse systemer består av ulike elementer som kan samhandle på uforutsigbare måter (Leveson, 2012). Systemene er «for komplekse for fullstendige analyser og for organiserte for statistiske vurderinger» (Leveson, 2012, s. 63, egen oversettelse). For å håndtere den organiserte kompleksiteten, må man ha en systematisk og helhetlig tilnærming som tar hensyn til både tekniske og organisatoriske faktorer. Leveson (2012) understreker også viktigheten av å ha en kontinuerlig læringstilnærming til risikoer i komplekse systemer. Dette innebærer kontinuerlig evaluering og forbedring av systemet, og at man må ha en åpen og transparent tilnærming til risikohåndtering som involverer alle relevante aktører. Samlet sett legger teori om organisert kompleksitet vekt på viktigheten av å ha en helhetlig og systematisk tilnærming til risikohåndtering i komplekse systemer.

Perrow (1999) og Leveson (2012) sitt bidrag har gitt en økt forståelse av komplekse systemer, både når det gjelder analyse og håndtering. Dette er av stor betydning for å øke forståelsen av komplekse systemer og for å utvikle systemer som er mer pålitelige, sikrere og effektive.

3.1.1 Cyberfysiske systemer

Cyberfysiske systemer har vokst frem i lys av den digitale utviklingen, og det moderne samfunnet er avhengig av komplekse og sammenkoblede systemer for å forbedre ytelse og effektivitet (Arghandeh, von Meier, Mehrmanesh & Mili, 2016). Cyberfysiske systemer består av en kombinasjon av digitale og fysiske prosesser som interagerer. Fysiske strukturer blir overvåket, kalkulert og kontrollert gjennom nettverkssystemer (Lee, 2008). Prosesser og komponenter i systemer blir dermed koblet sammen i et omfattende og komplekst nettverk, hvor det er gjensidig avhengighet mellom cyberkomponenter og fysiske komponenter (Ashibani & Mahmoud, 2017). Cyberfysiske systemer kan dermed sies å være komplekse systemer med tette koblinger (Perrow, 1999). Det blir stadig mer utfordrende å karakterisere

hva som ikke er et cyberfysisk system, ettersom det har blitt en integrert del av de fleste systemer (Törngren, Asplund, Bensalem, McDermid, Passerone, Pfeifer, Sangiovanni-Vincentelli & Schätz, 2017).

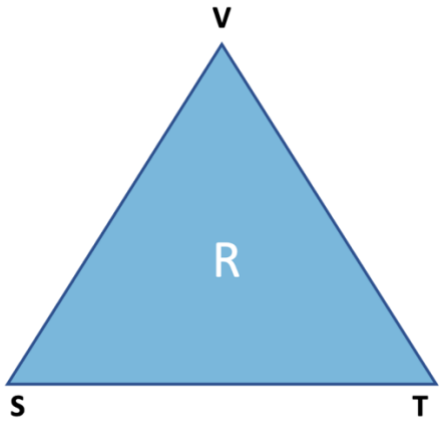
I kraftsystemet har det vært en rask utvikling i sammensmelting av digitale styringssystemer og fysisk infrastruktur. Systemene har stor betydning for kontroll, overvåkning og automatisering i bransjen, som videre har innvirkning på effektiviteten og påliteligheten til strømforsyningen (Arghandeh et al., 2016). Disse systemene kan også bidra til å øke sikkerheten og redusere risikoen for strømbrudd og andre avbrudd. Det er en viktig teknologi som bransjen har stort behov for. På grunn av samfunnsutviklingen vil det i tiden fremover stilles enda større krav til strømforsyningen. Et alternativ for å bygge et mer resilient strømnett er å gjøre det «smartere», noe som innebærer videreutvikling av cyberfysiske systemer (CPS-Summit, 2008; Yaacoub, Salman, Noura, Kaaniche & Malli, 2020). Det kan bidra til ytterligere effektivisering, utnytting av fleksibilitet og nyvinning på området. Samtidig fører det til større sårbarhet og trusler, som for eksempel uautorisert tilgang og cyberangrep (Ashibani & Mahmoud, 2017). Trusselaktører vil kunne utnytte teknologiske fremskritt med innebygde sårbarheter. Ytterligere integrering av cyberfysiske systemer stiller dermed store krav til sikring og sikkerhet i kraftbransjen (Skotnes, 2018).

3.2 Cyberangrep

Et cyberangrep kan defineres som «en ekstern trussel som har som hensikt å skade, forstyrre eller overbelaste et system» (NHO, 2022). Definisjonen tolkes til også å inkludere angrep som ikke har ført til konsekvenser i et selskap, samt forsøk på cyberangrep. Cyberangrep kan kategoriseres som en security-trussel. Security defineres som «den oppfattede eller faktiske evnen til å forberede seg på, tilpasse seg, motstå og komme seg fra farer og kriser forårsaket av menneskers bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking» (Jore, 2019, s. 157, egen oversettelse). Security er et begrep som har ulike dimensjoner og omfatter bredt, men basert på oppgavens kontekst vil security-begrepet bli tilknyttet kritisk infrastruktur. I denne dimensjonen er systemets sårbarhet i fokus, samt et angreps potensial for kaskadeeffekt (Jore, 2019). Slike angrep kan komme i form av cyberangrep. Det mest alvorlige konsekvensene av et vellykket cyberangrep er systemer som slutter å virke (NSM, 2023). Dette gir grunn til å anse cyberangrep som en voksende trussel mot kraftbransjen og beskyttelsen av kritisk norsk infrastruktur.

3.2.1 Cyberangrep i trefaktormodellen

For å beskrive sammenhengen mellom cybertrusler, kraftbransjens sårbarheter og de verdiene de ønsker å beskytte, vil det være nyttig å se til trefaktormodellen. Modellen brukes ofte i vurdering av security-risiko, ettersom vanlige risikovurderinger fordrer at man har et tilstrekkelig datagrunnlag for å beregne sannsynlighet, noe som er vanskelig med tilsiktede cyberangrep (NSM, Politidirektoratet [POD] & Politiets sikkerhetstjeneste [PST], 2015). I figuren utgjør trusler, verdier og sårbarheter viktige knutepunkter for å vurdere risiko.



Figur 2: Trefaktormodellen (NSM, POD & PST, 2015, s. 19)

Det er to viktige faktorer som er bestemmende for hvorvidt en trussel anses som stor; intensjon og kapasitet (NSM, POD & PST, 2015). Trusselaktørene som kraftbransjen står overfor er alt fra enkeltpersoner til nasjonale aktører. Intensjon og evne hos aktørene varierer dermed i stor grad, noe som kan gjøre vurdering av risiko vanskelig. Trusselaktører som har som intensjon å manipulere kritisk infrastruktur behøver ressurser, innsats og ekspertise for å lykkes med et cyberangrep (Geers, 2009). Det finnes flere trusselaktører som innehar slike ressurser, noe som for eksempel har blitt tydeligere gjennom Russland sine angrep mot Ukraina og deres kritiske infrastruktur (Pléta et al., 2020). Tilsiktede og ondsinnede angrep er preget av en ytterligere usikkerhetsdimensjon som følge av at trusselaktørene er rasjonelle og hemmelighetsfulle (NSM, 2023). Ofte vet man ikke hvilken evne og intensjon som ligger i en trusselaktør før angrepet har skjedd.

Videre må trusselaktørenes tilpasningsdyktighet understrekes. Metoder som blir brukt er i stadig endring, ettersom trusselaktørene utvikler nye teknikker og måter i å infiltrere systemer på (NSM, 2023). Ulike security-tiltak kan begrense handlingsrommet til eventuelle angripere slik at de aller fleste angrep blir forhindret, men i noen tilfeller vil security-tiltak føre til at

trusselaktører legger nye planer eller retter oppmerksomheten mot andre mål. I slike tilfeller kan security-tiltak virke mot sin hensikt (Engen, Gould, Kruke, Lindøe, Olsen & Olsen, 2021). Et angrep kan komme uavhengig av iverksetting av nye tiltak, men de kan ramme mer uforutsigbart enn tidligere. Dette beskrives som risikomigrasjon, hvor risikofaktorer migrerer til mer sårbare områder (Grunnan et al., 2008). Risiko for security-angrep forflytter seg på denne måten fra et selskap med velfungerende security-tiltak, til et selskap med svakere security-tiltak i samme bransje (Grunnan et al., 2008).

Det andre punktet i modellen er verdi. Som kritisk infrastruktur representerer kraftbransjen flere verdier som er helt nødvendige for at næringsliv og befolkning i Norge skal kunne fungere optimalt. Dette er verdier som for eksempel kan videreselges, brukes til utpressing, eller omsettes av trusselaktører (NorSIS, 2021). En av de viktigste verdiene kraftbransjen beskytter er strømforsyning. Uten forsyning av strøm er det mange kritiske samfunnsfunksjoner som kan kollapse (NOU 2006: 6). Siden det er nettselskapene som samlet har ansvar for å beskytte strømforsyningen, vil de være naturlige mål for trusselaktører som har som hensikt å skade eller svekke denne verdien.

På bakgrunn av dette er det spesielt viktig at nettselskaper i bransjen sikrer seg mot angrep ved å lokalisere og fjerne sårbarheter i egne systemer. Sårbarheter er det tredje punktet i modellen, og representerer muligheter trusselaktører kan utnytte for å skade de verdiene det er mål om å beskytte. Sårbarhetene kan utnyttes for å få tilgang til de verdiene som kraftbransjen representerer (NSM, 2023). Det vil derfor være viktig for de ulike virksomhetene å identifisere de trusselaktørene en står overfor, hvilke verdier en har som mål å beskytte, samt egne sårbarheter, slik at en har et riktig grunnlag for å kunne vurdere risiko knyttet til cyberangrep.

3.3 Resiliens

Resiliens blir i mange sammenhenger ansett som en måte organisasjoner og bransjer kan imøtekomme en kompleks og usikker verden (Anholt & Boersma, 2018). Resiliens handler i bred forstand om motstandsdyktighet, men det er mange ulike definisjoner på begrepet. Det kan blant annet defineres som «(...) et objekts evne til å gjenvinne sin opprinnelige form eller gjenopprette sin funksjon etter at det har blitt utsatt for en ytre påkjenning» (Kongsvik, Albrechtesen, Antonsen, Herrera, Hovden & Schiefloe, 2018, s. 88). Denne definisjonen har

likhetstrekk med definisjonen av security (Jore, 2019), presentert i delkapittel *3.2 Cyberangrep*. Begge definisjonene omtaler evnen til å gjenopprette eller komme seg fra påkjenninger eller farer. Det blir ofte gitt en generell definisjon på resiliens, men flere forskere deler resiliens i ulike former og nivåer.

3.3.1 Precursor, restoration og recovery resiliens

Pettersen og Schulman (2016) omtaler tre ulike former for resiliens. Den første formen er *precursor* resiliens. Det omhandler evnen til å overvåke og opprettholde forhold, og raskt reagere ved behov for gjenoppretting. Det vil være en måte å håndtere risiko på, samt en proaktiv form for resiliens. Eksempler på dette kan være å ha tiltak på plass for å hindre at et cyberangrep inntreffer, eller å ha beredskapsplaner på plass for å håndtere et angrep. *Restoration* resiliens er den andre formen som innebærer å gjenoppta driften etter midlertidige påkjenninger med raske handlinger. Det kan inkludere å ha resiliente systemer for å hindre eller minimere nedetid, eller en plan for å gjenopprette kritisk infrastruktur etter en hendelse (Pettersen & Schulman, 2016). Den tredje formen er *recovery resiliens*, som består av å sammensette systemene igjen for å etablere en «ny normal». Den nye normalen burde være minst like pålitelig og resilient som tidligere, hvis ikke enda mer forbedret (Pettersen & Schulman, 2016). Dette inkluderer å bruke lærdommen fra hendelsen til å forbedre forebyggende tiltak, eller å øke kapasiteten for å håndtere fremtidige hendelser.

Recovery resiliens kan kobles til det Martin (2019) omtaler som aktiv resiliens, noe som innebærer «å bli stadig tøffere ved å lære av motgang og bli bedre i stand til å håndtere fremtidige påkjenninger» (Martin, 2019, s. 76, egen oversettelse). Læringsaspektet i aktiv resiliens er svært viktig her. I etterkant av hendelser vil det være ideelt for organisasjoner å gjøre mer enn å gjenopprette sin funksjon. Organisasjonene kan i tillegg lære av erfaringene og bygge resiliens. Målet er å utvikle et sterkere forsvar og øke systemets tilpasningsevne (Ruth & Gössling-Reisemann, 2019). Sannsynligheten for at organisasjonen er bedre rustet, vil være høyere (Martin, 2019). De tre ulike formene for resiliens kan brukes for å forklare og poengtere sammenkoblingen mellom resiliens og erfaringsdeling, men i oppgaven vil det særlig være søkelys på læringsaspektet i recovery resiliens og aktiv resiliens. Det er på bakgrunn av problemstillingens formulering om å undersøke erfaringsdeling i etterkant av cyberangrep.

3.3.2 Situert, strukturell og systemisk resiliens

Resiliens kan videre omtales på ulike nivåer; situert, strukturell og systemisk. Ifølge Macrae (2019) beskriver situert, strukturell og systemisk resiliens ulike øyeblikk med resiliens. Situert resiliens foregår på mikronivå ved eller i nærheten av den operative frontlinjen. Det innebærer forstyrrende hendelser som oppdages og håndteres raskt. Strukturell resiliens er aktivitet på mesonivå, og refererer til organisatoriske prosesser med å omorganisere og forbedre sosiotekniske ressurser, samt etablerte praksiser. Det koordineres av flere organisatoriske enheter som overvåker aktiviteter i frontlinjen. Aktivitetene på strukturelt nivå blir aktivt gjennomgått, og blir blant annet sett i lys av tidligere erfaringer. Dette er aktiviteter som kan foregå fra uker til år (Macrae, 2019). Måten det arbeides på for å håndtere risiko på det strukturelle nivået kan relateres til det Perrow (1999) kaller desentralisert styring, ettersom denne formen for styring tillater fordeling av ansvar på flere aktører.

For å håndtere forstyrrelse i de eksisterende ordningene vil det ikke alltid være nok å gjøre strukturelle endringer. Dermed kan det være nødvendig med systemiske endringer i måten ting er organisert på for å håndtere forstyrrelsene mer effektivt (Macrae & Wiig, 2019). Dette finner sted på det systemiske nivået av resiliens, og foregår på makronivå (Macrae, 2019). Systemisk resiliens handler om å grunnleggende endre og forbedre måten å designe, produsere, bruke og dele de sosiotekniske ressursene som er avgjørende for sikkerhet. For å skape systemisk resiliens, må det være en oppfatning av at forstyrrelser kan skape en systemisk krise. Dette betyr at de nåværende ordningene som gir systemet de nødvendige ressursene for å fungere og kontrolleres effektivt, feiler (Macrae & Wiig, 2019). Derfor blir det nødvendig å gjøre store endringer for å få systemet til å fungere på en bedre måte. Det kan for eksempel innebære store endringer i grunnleggende forutsetninger, regler eller teknologiske systemer som er sentrale i aktiviteter i bransjen. Arbeidet kan utspille seg over måneder og år, involvere mange mennesker, og gå på tvers av en hel bransje (Macrae, 2019). Det systemiske nivået kan relateres til det Perrow (1999) kalles sentralisert styring, ettersom sentralisert styring ønsker å sikre oversikt og en helhetlig forståelse av et system gjennom en konsistent sentral ledelse. Søkelyset på en overordnet forståelse av et system samstemmer dermed med systemisk resiliens.

Resiliensnivåene interagerer og må ses i sammenheng. Implikasjoner på lavere nivå kan ha betydning for resiliens på et høyere nivå, og omvendt (Macrae, 2019). Det foregår en vertikal samordning mellom nivåene, og bransjer har behov for personell på ulike nivåer som evner å

knytte nivåene sammen. Macrae (2019) vektlegger i tillegg utfordringen med å se sammenhengen mellom aktiviteter på ulike nivåer, og at det gjenstår mye arbeid rundt å forklare hvordan nivåene blir påvirket av ulike aktiviteter. Å utvikle mer resiliente systemer krever evnen til å konseptuelt analysere og praktisk integrere de ulike resiliensnivåene. Resiliensnivåene vil i oppgaven brukes for å beskrive hvordan resiliens bygges både på selskapsnivå (strukturell resiliens) og på bransjenivå (systemisk resiliens).

3.3.3 Cyberresiliens

Resiliens blir i stadig større grad koblet til håndtering av kompleksitet, spesielt teknologisk kompleksitet, og kan av den grunn kobles til Perrow (1999) og Leveson (2012) sine bidrag om komplekse systemer. Ved å benytte resiliens som en strategi for kompleksitetshåndtering, vil det gjøre fremtidige security-utfordringer overkommelig for organisasjoner og bransjer (Engen et al., 2021; Ruth & Gössling-Reisemann, 2019). Det vil ikke lenger være aktuelt å eliminere risikoer, men heller «tilpasse seg, håndtere og komme seg etter endrede forhold og ulike trusler» (Jore, 2019, s. 165). I den forbindelse blir begrepet cyberresiliens ofte benyttet.

Cyberresiliens har vokst frem som et viktig begrep innenfor cybersikkerhet, og forskere har aktivt begynt å bruke begrepet. Cyberresiliens har fått en sentral posisjon i måten organisasjoner kan forbedre sin evne til å forebygge og gjenopprette sin virksomhet etter cyberangrep. Begrepet er noe omdiskutert, og det eksisterer dermed ulike definisjoner. Cyberresiliens blir i denne oppgaven basert på definisjonen som omtaler «evnen til kontinuerlig å levere det tiltenkte resultatet til tross for uønskede cyberhendelser» (Björck et al., 2015, s. 312, egen oversettelse). Definisjonen viser til evnen nettselskaper har til å opprettholde norsk strømforsyning, selv om noen mekanismer har sviktet under eller etter et cyberangrep. Björck et al. (2015) trekker videre frem læring etter cyberangrep som et viktig element for å bygge cyberresiliens. Ved å ha søkelys på å lære av fortidens cyberangrep og konsekvenser, tilpasse seg nåtiden trusselaktører og utvikle motstandsdyktighet i fremtiden, kan nettselskaper i kraftbransjen øke cyberresiliens.

Myndigheter og virksomheter har i økende grad tillit til cyberfysiske systemer som en integrert del av kritiske samfunnsfunksjoner og infrastruktur (Linkov, Eisenberg, Plourde, Seager, Allen & Kott, 2013). Av den grunn har cyberresiliens blitt en nøkkelegenskap for kritisk infrastruktur, som til enhver tid blir utsatt for cybertrusler. Det involverer de fleste aktører i samfunnet, og tverrseksjonelt samarbeid mellom aktører blir omtalt som essensielt

for å oppnå effektiv cyberresiliens (Dupont, 2019). Samarbeid og tillit blir viktige faktorer for å styrke arbeidet, og bidra til en helhetlig tilnærming (Hausken, 2020). Teori om komplekse systemer legger også vekt på viktigheten av å ha en helhetlig og systematisk tilnærming til risikohåndtering i komplekse systemer (Leveson, 2012; Perrow, 1999), og cyberresiliens kan derfor ses i sammenheng med risikohåndtering i komplekse systemer.

I motsetning til risikostyring av cybersikkerhet hvor det er ønskelig å minimere risikoer, vil cyberresiliens fokusere på et høyt ytelsesnivå uavhengig av farer og risikoer man står overfor. Det vil være behov for å utarbeide kapasiteter og ressurser som evner å tilpasse seg situasjoner, samt er pålitelige (Dupont, 2019). Videre vil det kreve kontinuerlig evaluering og forbedring av cyberresiliens, da truslene og teknologien stadig utvikler seg (Hausken, 2020). I oppgaven vil teori om resiliens og cyberresiliens knyttes sammen ved å omtale de ulike resiliensnivåene i et cyberperspektiv; situert cyberresiliens, strukturell cyberresiliens og systemisk cyberresilens. I et cyberperspektiv representerer de ulike nivåene hvordan ansatte, nettselskaper og kraftbransjen håndterer cybertrusler og -angrep. De strukturelle og systemiske nivåene vil være mest relevant, ettersom oppgaven søkelys er på nettselskaper og kraftbransjen som helhet.

3.4 Erfaringsdeling

Gjennom tidligere forskning har det blitt klart at informasjonsutveksling og kommunikasjon kan redusere det ukjente, og gi aktører i kritisk infrastruktur bedre grunnlag for å arbeide med cybertrusler (Aakre, 2020; Bodsberg et al., 2018; Gjesvik, 2019; Hausken 2007; Rak, 2002). En måte å utveksle informasjon er basert på erfaringer fra en opplevd hendelse.

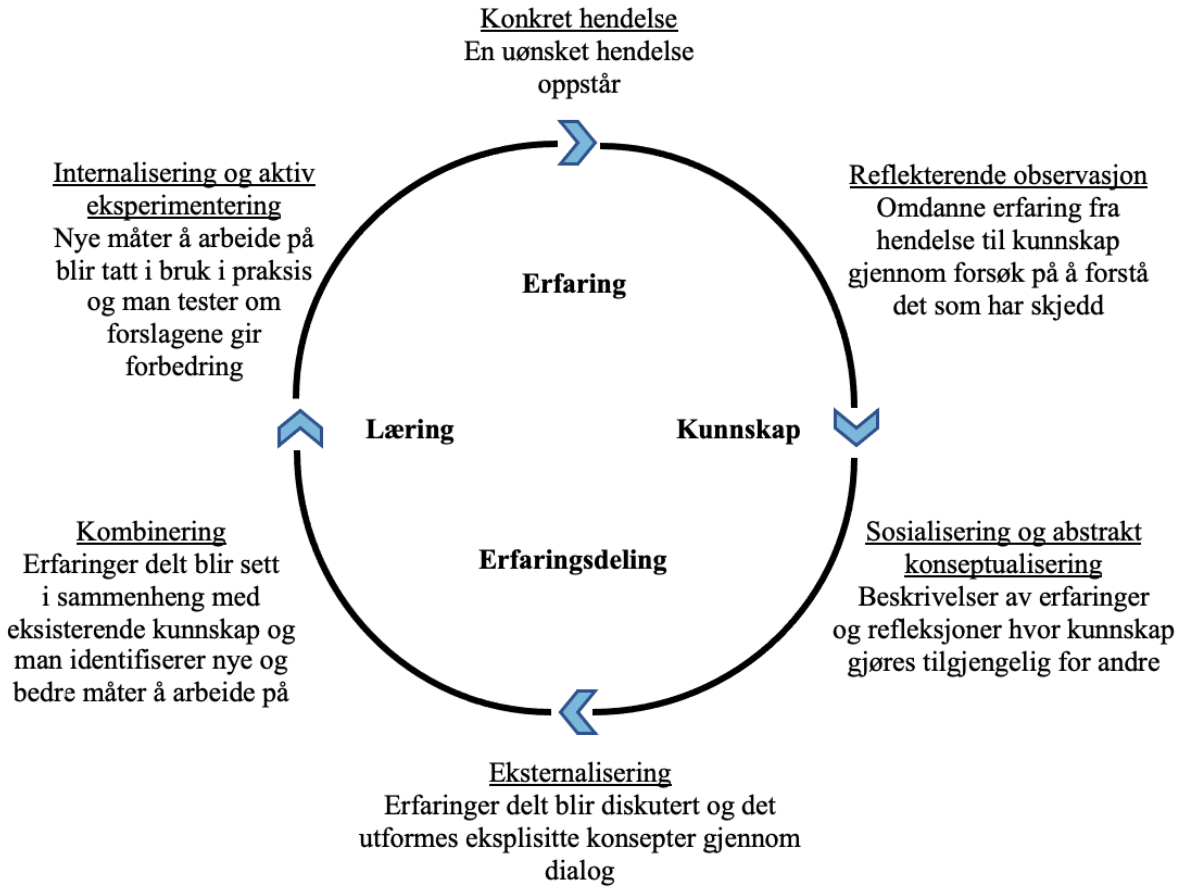
3.4.1 Kunnskap, erfaringsdeling og læring

Kolb (2015) definerer læring som en prosess som omdanner erfaringer til kunnskap. Denne prosessen begynner med konkrete erfaringer som en opplever gjennom en hendelse. Deretter reflekteres det over hendelsen som er erfart gjennom reflekterende observasjon. Målet er å forstå det som har skjedd og å forklare eventuelle uoverensstemmelser mellom det som faktisk skjedde og tidligere forståelser (Kolb, 2015). Å sette ord på dette, enten for seg selv eller kommunisert til andre, kalles abstrakt konseptualisering. I tillegg til en beskrivelse av erfaringer og refleksjoner, vil aktører på dette stadiet også utforme ideer og forslag til hva som kan gjøres bedre. Når disse forslagene prøves i praksis brukes aktiv eksperimentering for

å teste om endringsforslagene gir forbedring eller ikke (Kolb, 2015). Dette vil igjen gi nye erfaringer og muligheter til ytterligere læring ved at læringssirkelen begynner på nytt.

Et annet teoretisk bidrag som omhandler læring, er Nonaka og Takeuchi (1995) sine faser for kunnskapsutvikling. Læring presenterer her som en prosess hvor kunnskap utvikles. De deler utviklingen av kunnskap inn i fire faser: sosialisering, eksternalisering, kombinering og internalisering. Fasene kan ses som komplementære til Kolb (2015) sin læringssirkel for læring av erfaringer. I sosialiseringsfasen formidles erfaringsbasert kunnskap blant individer med ulik bakgrunn, perspektiver og motivasjoner. Dette kan være utfordrende, men gjennom å dele følelser og tanker rundt erfaringene, bygges det tillit mellom individene (Nonaka & Takeuchi, 1995). For å klare det må det bygges et «felt» hvor individene kan interagere med hverandre gjennom dialoger ansikt-til-ansikt. Typisk vil disse feltene være selvorganisert, hvor medlemmer fra ulike områder jobber sammen for å nå et felles mål (Nonaka & Takeuchi, 1995). I eksternaliseringsfasen blir erfaringer delt diskutert, og det utformes eksplisitte konsepter gjennom dialog. I kombineringsfasen vurderes nye kunnskap, konsept eller informasjon som verdt å investere i eller ikke. Det er også viktig at det gjøres en vurdering om investeringen bidrar til samfunnet som helhet (Nonaka & Takeuchi, 1995). I kombineringsfasen blir aksepterte konsepter videre konvertert til noe håndfast eller konkret. I denne fasen blir ny kunnskap sett i sammenheng med eksisterende kunnskap, slik at en arbeidet på en ny eller forbedret måte (Nonaka & Takeuchi, 1995). Den siste fasen, internaliseringsfasen, tar i bruk den nye måten å arbeide på i praksis, og gir grunnlag for videre kunnskapsbygging.

Læringssirkelen til Kolb (2015), og Nonaka og Takeuchi (1995) sine faser for utvikling av kunnskap, er sammenstilt i figuren nedenfor. Figuren viser sammenhengen mellom erfaringsdeling, kunnskap og læring.



Figur 3: Sammenhengen mellom kunnskap, erfaringsdeling og læring, basert på Kolb (2015) sin læringssirkel, og Nonaka og Takeuchi (1995) sine faser for utvikling av kunnskap

En konkret hendelse vil i oppgavens kontekst være et tilsiktet cyberangrep utført av ondsinnede trusselaktører. Angrepet vil treffe et nettselskap, og læringssirkelen starter ved at selskapet omgjør erfaringer fra angrepet til kunnskap gjennom reflekterende observasjon. Dette inkluderer for eksempel kunnskap om trusselaktører og metoder, sårbarheter i egne systemer, måter å håndtere angrep på, samt hvordan en bør gjenopprette systemer. Når kunnskapen gjøres tilgjengelig for andre skjer det en sosialisering eller abstrakt konseptualisering av kunnskap. Dette steget beskriver første fase av erfaringsdeling, hvor erfaringer og tilhørende kunnskap blir delt mellom nettselskaper.

Eksternalisering representerer den andre fasen av erfaringsdeling. Erfaringer i etterkant av deling blir diskutert mellom selskapene, og det utformes eksplisitte konsepter. Dette kan i oppgavens kontekst være ideer om trusler, eller sårbarheter i egne systemer som må settes søkelys på. Konseptene bygges videre i kombineringsfasen, hvor nettselskaper ser ny kunnskap i sammenheng med eksisterende kunnskap om truslene og sårbarhetene. Det gjøres

deretter en vurdering om nye IKT-sikkerhetstiltak er nødvendig å implementere i eget selskap eller ikke. Dette kan inkludere en analyse av egne styrker og svakheter, hvor ny kunnskap vurderes om den bidrar til økt IKT-sikkerhet eller ikke. Hvis konklusjonen av disse vurderingene er positiv, vil internalisering og aktiv eksperimentering kunne finne sted. Det er de siste fasene i figuren.

Figuren kan kobles til teori om komplekse systemer, hvor en kontinuerlig læringstilnærming til risikoer blir trukket frem som viktig for å håndtere kompleksiteten i et system (Leveson, 2012). For å oppnå det må man blant annet ha en åpen og transparent tilnærming som involverer alle relevante aktører, og det samsvarer med hvordan erfaringsdeling er plassert i figuren. Figuren kan videre ses i lys av teori om strukturell resiliens (Macrae, 2019). På det strukturelle nivået opplever selskaper cyberangrep, og reflekterer rundt hendelsen i ettertid. Nivået innebærer også å iverksette nødvendige tiltak, basert på erfaringsdeling. På denne måten henger læring og resiliens nøye sammen, og det understrekes også i teori om aktiv resiliens (Martin, 2019), i definisjonen av cyberresiliens (Björck et al., 2015), og i Hausken (2020) sine punkter om forskning på cyberresiliens.

3.4.2 Erfaringsdeling i praksisfellesskap

I modellen fremkommer sosiale arenaer for erfaringsdeling som viktig for læring. Slike instanser har de sosiale relasjonene mellom mennesker i fokus. Målet er å ha sosiale prosesser som skaper og opprettholder en passende kontekst for læring (Gherardi, Nicoloni & Odella, 1998). Læring handler dermed om å observere hva andre gjør, og å ha dialog og interaksjoner med mennesker som har mer kunnskap om et tema enn deg selv. Denne formen for læring tar plass i sosiale fellesskap (Lave & Wenger, 1991). I denne sammenheng kan en omtale praksisfellesskap. Det vil si gruppe mennesker som deler bekymringer, problemer og entusiasme for et tema, og sammen utvikler kunnskap og ekspertise på områder gjennom kontinuerlig dialog med hverandre (Wenger, McDermott & Snyder, 2002). Praksisfelleskap kan ses i relasjon til det Nonaka og Takeuchi (1995) beskriver som felt hvor individer kan interagere med hverandre gjennom dialoger ansikt-til-ansikt.

3.4.2.1 Delt forståelse, gjensidig utbytte og tillit i et praksisfellesskap

I tidligere forskning ble delt forståelse, gjensidig utbytte og tillit introdusert som viktige insentiv for samarbeid mellom ulike aktører (Gjesvik, 2019). Delt forståelse handler om å

forstå samfunnssikkerhet utover de umiddelbare interessene til et selskap (Gjesvik, 2019). Strømforsyning ble under *3.2 Cyberangrep* presentert som en av de viktigste verdiene som kraftbransjen representerer. En delt forståelse av risiko som truer systemer man er en del av, vil videre akselerere samarbeid (Atkins & Lawson, 2021). En mangel på forståelse av hvordan felles trusler gjør aktører gjensidig avhengig av hverandre vil derimot svekke forekomsten av deling (Hausken, 2007; Rak, 2002). Delt forståelse kan derfor ses i sammenheng med trefaktormodellen som gjør en vurdering av risiko knyttet til trusler, verdier og sårbarheter (NSM, POD & PST, 2015).

Delt forståelse kan videre skape gjensidig utbytte og tillit mellom organisasjoner (Gjesvik, 2019). Gjensidig utbytte baserer seg på en organisasjons evne til å dele verdifulle råd og erfaringer. Delt informasjon må i tillegg gi merverdi som oppleves som relevant og handlingsdyktig. Informasjon som er handlingsdyktig, kan beskrives som at deltakere får bruk for delt erfaring og kunnskap i sitt praktiske arbeid. Det er viktig for evalueringen av erfaringsbasert læring (Njå, Sommer, Rake & Braut, 2020). Tillit er «en tilstand der man aksepterer sårbarhet basert på positive forventninger til intensjonen til en annen» (Rousseau, Sitkins, Burt & Camerer, 1998, s. 395). Tillit handler både om tillit mellom organisasjoner, men også mellom individer (Gjesvik, 2019). Mellom organisasjoner er det snakk om tillit til intensjoner på et samfunnsnivå. Dette kan for eksempel være intensjoner om hvorfor en deler erfaringer eller hvordan en behandler delte erfaringer. Tillit mellom individer omhandler hvorvidt menneskene i de ulike institusjonene kjenner og stoler på hverandre. Denne formen for tillit kan kobles til sosialiseringsfasen. Der bygges tillit mellom individer gjennom deling av følelser og tanker rundt delte erfaringer (Nonaka & Takeuchi, 1995).

Det vil være viktig å forstå hvorvidt nettselskapene opplever delt forståelse, gjensidig utbytte og tillit gjennom dagens praksis for erfaringsdeling. En vurdering av dette må gjøres på bakgrunn av en kartlegging av nettselskapenes opplevelse av praksisfellesskapene de er en del av (Engen et al., 2021). I den sammenheng vil det være viktig å se på hvordan erfaringsdeling og kunnskapsutvikling forekommer i de ulike læringsarenaene, samt undersøke hvilke læringsarenaer aktører synes er viktige for å oppnå målet om å utvikle ny kunnskap gjennom erfaringsdeling.

4 Forskningsmetode

Følgende kapittel vil redegjøre for den metodiske fremgangsmåten som ble anvendt for å besvare oppgavens problemstilling. Det vil redegjøres for valg som er tatt, samt fremlegges en vurdering av forskningens styrker og svakheter.

4.1 Forskningsdesign og forskningsprosess

Tilnærmingen til analysen er abduktiv, og det betyr at målet for studien er å forstå en del av samfunnet basert på sosiale aktørers meninger og motiver i konteksten av deres hverdagslige aktiviteter (Blaikie & Priest, 2019). Denne oppgaven baserer seg på Danermark, Ekström og Karlsson (2019) sin forståelse av abduktiv tilnærming som en strategi hvor en starter med et teoretisk rammeverk, for deretter å gjøre empiriske observasjoner. Basert på observasjonene gjør en tolkninger i tråd med de foreliggende teoriene. Det har imidlertid blitt vekslet mellom empiri og teori gjennom prosessen, for å sikre at analysen er tilpasset ny kunnskap. Ved å la forskningsprosessen være flytende i natur kan en være mer utforskende i veien mot riktig tolkning av et fenomen. Det råder en antakelse om at det nødvendigvis ikke finnes en enkelt sannhet, men forskningsdesign og -prosess har som mål å finne koblinger som gjør det mulig å forklare og belyse oppgavens problemstilling og forskningsspørsmål.

Tabellen under viser en gjennomgang av forskningsprosessen. Den illustrerer hvordan prosessen har vært flytende, og hvordan justeringer av elementer har skjedd underveis.

Når	**Aktivitet**	**Formål**	**Resultat**
Januar	Lage fremdriftsplan. Utforme problemstilling og forskningsspørsmål. Struktur og metodevalg. Begynne på teori- og metodekapittel. Artikkelsøk i forbindelse med tidligere forskning og teori gjennom søk i Google Scholar- og Oria-portalen. Kartlegging av informanter.	Ha en plan for arbeidet. Begynte på flere kapitler i oppgaven for å komme i gang med skrivingen og skape en oversikt. Nyttig å få oversikt over oppgaven før intervjuprosessen startet. Anså det som viktig å kartlegge informanter på et tidlig tidspunkt. Da fikk vi et inntrykk av hvilke personer det var aktuelt å kontakte.	Formulerte problemstilling og forskningsspørsmål for å ha et utgangspunkt for oppgaveskriving. Flere kapitler ble påbegynt. Laget en liste med aktuelle informanter.

Februar	Arbeid med innledning, bakgrunn, kontekst, teori og metode. Kontakte informanter. Utforming av informasjonsskriv og intervjuguide. Gjennomføring av intervju.	Fortsatte på de påbegynte kapitlene og begynte på nye for å få et helhetlig inntrykk av hvordan oppgaven skulle se ut. Kontaktet informantene tidlig fordi vi antok det ville være varierende responderingstid. Utformet informasjonsskriv og intervjuguide for å sikre god kvalitet under intervjuene.	Førsteutkast på innledning, bakgrunn og metode ble klart. Kontaktet og avtalte tidspunkt med informanter fra midten av februar.
Mars	Arbeid med innledning, bakgrunn, kontekst, teori og metode. Gjennomføring av intervju. Databehandling og datareduksjon av intervjuene. Arbeid med dokumentanalyse.	Jobbet videre med flere kapitler etter hvert som intervjuer ble gjennomført. Fikk en mer inngående forståelse av hva som burde inkluderes. Leste oss opp på dokumentanalyse for å supplere øvrig datainnsamling. Fant relevante dokumenter og analyserte disse.	Det siste intervjuet i den første runden ble gjennomført 20. mars. Gjennomførte en dokumentanalyse.
April	Påbegynnelse av analyse og drøfting. Ferdigstilling av teorikapittelet. Oppfølgingsspørsmål til informantene. Arbeid med dokumentanalyse. Spissing av problemstilling og forskningsspørsmål. Kontakt av flere informanter.	Ferdigstilte teorikapittelet etter påbegynt analyse- og drøftingskapittel for å spisse teorien mot funnene. Sendte oppfølgingsspørsmål til informantene på områder vi ønsket større metning. Ønsket flere informanter til oppgaven for å sikre metning etter å ha justert problemstillingen.	Sendte oppfølgingsspørsmål til informanter i uke 12, og fikk svar fortløpende. Kontaktet flere informanter som resulterte i tre nye planlagte intervjuer.
Mai	Utformet ny intervjuguide, og gjennomførte en ny runde med intervjuer i starten av mai. Databehandling og datareduksjon av de siste intervjuene. Hovedfokus på analyse og drøfting.	Ønsket å sikre metning i oppgaven basert på ny problemstilling. Prioriterte mye tid til oppbygning og innholdet i analyse- og drøftingskapittelet.	Tre intervjuer ble gjennomført og basert på disse ble det vurdert at metning var god. Et førsteutkast av hele oppgaven var klart i midten av mai.

	Jobbet parallelt med ferdigstillelse av de andre kapitlene.		
Juni	Ferdigstillelse av oppgaven.	Klargjøre dokumentet for innlevering.	Innlevering av oppgaven 15. juni.

Tabell 1: Forskningsprosessen

4.2 Kvalitativ metode

For å besvare oppgavens problemstilling på best måte er det i hovedsak valgt å bruke primærdata (Blaikie & Priest, 2019). Valget om å samle inn primærdata er tatt på bakgrunn av at det ikke eksisterer forskning som ser spesifikt på erfaringsdeling mellom nettselskaper etter cyberangrep i kraftbransjen. Gjennom metoder for innsamling av primærdata vil det foreligge en nærhet til data som samles inn, samtidig som en deltar i innsamlingen. På denne måten vil en være i stand til å vurdere om innsamling er av god kvalitet, og om dataene er passende for prosjektet (Blaikie & Priest, 2019). For å samle inn primærdata ble det benyttet kvalitativ metode. Kvalitativ forskningsmetode søker å generere data om hvordan mennesker forstår og opplever aspekter ved ulike fenomener (Clark, Forster & Bryman, 2019). Samtidig blir det ofte benyttet i forskning på temaer som ikke lett lar seg direkte måle eller observere. Det kan argumenteres for at problemstillingen for oppgaven ikke enkelt besvares gjennom kvantitative observasjoner. Dermed vil kvalitativ metode være hensiktsmessig for prosjektets datainnsamling. Formålet med den kvalitative innsamlingen vil hovedsakelig være å få refleksjoner rundt og forståelse for erfaringsdeling.

4.2.1 Semistrukturerte dybdeintervjuer

Primærkilden for den kvalitative datainnsamlingen er semistrukturerte dybdeintervjuer. Semistrukturerte intervjuer gir mulighet for å gjennomføre intervjuet etter noen overordnede spørsmål eller temaer, men samtidig ha fleksibilitet til å endre rekkefølge eller stille oppfølgingsspørsmål underveis i intervjuet (Johannessen, Tufte & Christoffersen, 2021). Spørsmålene ble forsøkt formulert på en slik måte at en fikk utfyllende og åpne svar fra informantene, og gjennom oppfølgingsspørsmålene var målet å få mer detaljerte svar. Blant annet i form av eksempler. Ved å strukturere intervjuene på denne måten, var det også mulig å inkorporere flere spørsmål underveis i intervjuprosessen basert på hvilke temaer som ble tatt opp av informantene. Informantene får på denne måten større frihet til å uttrykke sine opplevelser og meninger slik de ønsker, samtidig som det er mulig å innhente fyldige og

detaljerte beskrivelser som datagrunnlag for analysen. Dette sikret god bredde i datagrunnlaget.

4.2.2 Utvalg av informanter

Utvalget av informanter er svært betydningsfullt for besvarelsen av oppgavens problemstilling (Johannessen et al., 2021). Oppgavens problemstilling og dens forskningsspørsmål søker å belyse tanker og meninger ulike aktører i kraftbransjen har i forbindelse med erfaringsdelingens bidrag til økt cyberresiliens for å sikre strømforsyning. Det empiriske grunnlaget for oppgaven baserte seg på samarbeidsorganisasjoner som er involvert i erfaringsdeling mellom nettselskaper, og store nettselskaper. Relevante informanter i samarbeidsorganisasjonene og nettselskapene var personer med kunnskap og kompetanse om erfaringsdeling mellom selskaper. Det var hensiktsmessig å intervjue informanter i samarbeidsorganisasjonene for å få et overblikk på erfaringsdeling på bransjenivå. I tillegg bidrar flere samarbeidsorganisasjoner med tilrettelegging og aktiv erfaringsdeling for nettselskapene. Informantene i nettselskapene er den andre parten som er direkte involvert i erfaringsdeling, og de bidro med kunnskap både på bransjenivå og organisasjonsnivå. Kombinasjonen av informanter på bransje- og organisasjonsnivå ga en utfyllende og helhetlig tilnærming til problemstillingen.

For å komme i kontakt med informanter ble det i hovedsak benyttet et tilgjengelighetsutvalg. Det er en strategisk utvelgelse av tilgjengelige deltakere som representerer egenskaper som er relevant for oppgaven (Thagaard, 2018). Det ble utformet en liste over store nettselskapene i Norge, samt en liste over relevante samarbeidsorganisasjoner i bransjen som vi oppfattet kunne ha nyttige refleksjoner til oppgavens problemstilling. Vi startet med å kontakte samarbeidsorganisasjonene per e-post. Det ble ansett som hensiktsmessig å intervjue først informanter i samarbeidsorganisasjonene, fordi det ville gi et innblikk i erfaringsdeling fra et overordnet nivå. I e-posten til de potensielle informanter ble det kort redegjort for formålet med oppgaven, og på hvilken måte de kunne bidra i prosjektet. I tillegg ble det utformet et informasjonsskriv med flere detaljer om prosjektet og rettighetene til informantene.

Etter å ha gjennomført tre intervjuer med samarbeidsorganisasjoner, begynte vi å ta kontakt med nettselskaper. Da hadde vi en mer inngående forståelse for hva nettselskapene burde bli spurt om. Samtidig hadde samarbeidsorganisasjonene god kjennskap til nettselskapene, og hvilke personer det ville være relevant å kontakte videre. Dermed ble også snøballmetoden

benyttet for å komme i kontakt med informanter, som innebærer bruk av det sosiale nettverket til utvalget (Loseke, 2017). Til sammen ble fjorten informanter intervjuet, hvor henholdsvis fem informanter representerte samarbeidsorganisasjoner (O) og åtte informanter representerte nettselskaper (N). Det siste intervjuet ble gjennomført med en informant fra et selskap som hadde kjennskap til å dele erfaringer underveis og i etterkant av et cyberangrep (E). I tabellen under blir informantene presentert med stillingstittelen de oppga på intervjutidspunktet.

Informant 1O	Leder i samarbeidsorganisasjon
Informant 2O	Leder for IT-sikkerhet og beredskap
Informant 3O	Rådgiver for digitalisering og IKT-sikkerhet
Informant 4O	Seksjonssjef
Informant 5O	Leder i samarbeidsorganisasjon
Informant 6N	Leder for informasjonssikkerhet
Informant 7N	IKT-sikkerhetskoordinator
Informant 8N	Seksjonssjef og IKT-sikkerhetskoordinator
Informant 9N	IKT-sikkerhetskoordinator
Informant 10N	IKT-sikkerhetskoordinator
Informant 11N	CISO (chief information security officer)
Informant 12N	IKT-sikkerhetsansvarlig
Informant 13N	IKT-sikkerhetskoordinator
Informant 14E	CISO (chief information security officer), eksternt selskap

Tabell 2: Oversikt over informanter

4.2.3 Gjennomføring av intervju

Samarbeidsorganisasjonene og nettselskapene hadde lokasjoner spredt i Norge, noe som resulterte i digitale intervjuer over Teams. Det gjorde at vi fikk tilgang til et langt større utvalg av informanter enn om vi hadde begrenset oss til fysiske intervjuer. Selv om intervjuene ble gjennomført digitalt var det viktig for oss at informantene følte seg komfortabel og forberedt på hva vi skulle snakke om. Vi begynte derfor hvert intervju med en introduksjonsrunde, kort gjengivelse av de viktigste punktene fra informasjonsskrivet, og ga informantene mulighet for å stille spørsmål om intervjuet og prosjektet. Å skape fortrolighet med informantene innledningsvis bidrar positivt for gjennomføringen av dybdeintervju. Det skaper en relasjon og bygger tillit (Halvorsen, 2008).

Alle intervjuene ble gjennomført med én informant per intervju, og estimert varighet ble satt fra 45 minutter til 1 time. Intervjuene endte med å vare fra 40 minutter til litt over en time. Den estimerte lengden på intervjuene ble satt for å sikre at informantene fikk svare så utdypende som mulig på spørsmålene i intervjuguiden. Tidsrammen inkluderte i tillegg et tidsrom på slutten hvor det var mulighet for å stille andre spørsmål enn de som stod i intervjuguiden, og hvor informantene kunne redegjøre for andre poeng de anså som relevant. For å dokumentere det som ble sagt i intervjuene, ble det gjort lydopptak med informantenes samtykke (Johannessen et al., 2021). En sentral fordel med lydopptak var å sikre dokumentering av viktig informasjon som informanten uttrykte ved besvarelse av spørsmål. I tillegg fører lydopptak til at intervjuerne kan fokusere på svarene til informanten, og stille gode oppfølgingsspørsmål, i stedet for å være opptatt med å notere svarene (Johannesen et al., 2021). Transkribering av intervjuene ble gjort fortløpende etter gjennomføring.

Intervjuene ble utført i to ulike runder. I den første runden ble elleve informanter intervjuet. I tre av de siste intervjuene i den første runden ble noen mindre poeng belyst. Disse ønsket vi å få en dypere forståelse av, ettersom det trolig ville gi oss et bedre analysegrunnlag. På grunn av dette valgte vi å sende e-post med oppfølgingsspørsmål til de informantene som hadde blitt intervjuet tidligere i den første runden. Gjennom både intervjuer og oppfølgingsspørsmål bekreftet informantene i stor grad hverandres utsagn, noe som førte til god metning av dataene. Til tross for det, ble det vurdert hensiktsmessig å gjennomføre en ny runde med noen flere intervjuer. Det ble gjort fordi problemstillingen og forskningsspørsmålene ble noe justert underveis i prosessen, selv om hovedfokuset var konsekvent. Ny runde med intervjuer sikret mulighet til god besvarelse av nyeste problemstilling og forskningsspørsmål. To ytterligere intervjuer med nettselskaper ble derfor gjennomført, samt et intervju med et eksternt selskap. Basert på en vurdering etter de siste tre intervjuene ble gjennomført, ble det bestemt at de fjorten intervjuer ga god metning for å svare på oppgavens justerte problemstilling.

4.2.4 Dokumentanalyse

Det ble valgt å gjennomføre en forskningsbasert dokumentanalyse, som bestod av tidligere gjennomførte og offentliggjorte undersøkelser og statistikk. Dokumentanalyse har blitt brukt som sekundærdata i oppgaven for å støtte opp under funn i innsamling av primærdata. Dokumentene kan belyse relevant informasjon og sammenhenger som underbygger informantenes utsagn. Det ble lagt ulike kriterier til grunn for utvelgelse av hva som var

relevante dokumenter. Aktuelle dokumenter ble nøye gjennomgått for å sikre oppfyllelse av kriteriene som var satt for utvelgelse av dokumentene. Ett av kriteriene var at dokumentene måtte inneholde informasjon om erfaringsdeling, samarbeid eller læring, eller gi informativ kunnskap om cyberangrep direkte rettet mot kraftbransjen. De utvalgte dokumentene er listet opp i tabellen.

1	Nasjonal sikkerhetsmyndighet (2023) *Risiko 2023: Økt uforutsigbarhet krever høyere beredskap*
2	Norges vassdrags- og energidirektorat Tøien et al. (2021) *IKT-sikkerhetstilstanden i kraftforsyningen 2021*
3	Meld. St. 38. (2016-2017) *IKT-sikkerhet: Et felles ansvar*
4	Næringslivets sikkerhetsråd (NSR) (2022) *Mørketallsundersøkelsen 2022*
5	Riksrevisjonen (2021) *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen*

Tabell 3: Liste over dokumenter

NSM (2023) utgir årlig en trussel- og risikovurdering som beskriver trusselaktører og sårbarheter hos virksomheter, samt risikoen dette medfører. *Risiko 2023: Økt uforutsigbarhet krever høyere beredskap* er relevant fordi den skriver om norsk kritisk infrastruktur, cyberangrep, IKT-sikkerhet, resiliens og samarbeid på tvers av virksomheter. NSM vektlegger blant annet hvordan dagens risikobilde krever mer samarbeid og felles motstandskraft.

NVE sin eksterne rapport om *IKT-sikkerhetstilstanden i kraftforsyningen 2021* bygger på data fra spørreundersøkelser, samt diskusjoner med en referansegruppe bestående av virksomheter, myndighetene, interesseorganisasjoner og leverandører i bransjen (Tøien et al., 2021). Rapporten besvarer hvordan bransjen vurderer IKT-sikkerheten i kraftforsyningen, og i hvilken grad cyberangrep har hatt konsekvenser for funksjonaliteten til driftskontrollsystem

og forsyningssikkerhet. Dokumentet kan bidra til å underbygge eventuelle behov for økt samarbeid og resiliensbygging presentert av informantene i oppgaven.

IKT-sikkerhet - Et felles ansvar (Meld. St. 38 (2016-2017)) presenterer strategier og tiltak for styrke IKT-sikkerheten i Norge. Stortingsmeldingen er relevant å inkludere i dokumentanalysen fordi den skisserer eksplisitt forebygging, avdekking og håndtering av digitale angrep i IKT-infrastruktur, samt et kapittel om energiforsyning. To sentrale punkter som fremkommer er tilrettelegging for god informasjonsdeling, og stimulere til større og mer ressurssterke fagmiljøer innen IKT-sikkerhet.

Mørketallsundersøkelsen (NSR, 2022) legger fram statistikk og data som gjenspeiler dagens organisering av IT-drift, hvilke hendelser som har hendt samt negative konsekvenser, hvilke årsaker som har ført til sikkerhetsbrudd, konsekvenser og håndtering av hendelser, samt forslag til tiltak for å håndtere risikoene. Populasjonen for rapporten er norske virksomheter i privat og offentlig sektor med 5 eller flere ansatte. Det er gjennomført 2500 intervju i undersøkelsen. Rapporten har bidratt til økt forståelse av hvilke trusler og trender som gjelder i norsk næringsliv.

Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen (Riksrevisjonen, 2021) har søkelys på IKT-sikkerhet i kraftbransjen, og gir en beskrivelse av tilstanden i dag. Grunnlaget for rapporten er en rekke dokumentanalyser, intervjuer og saksgjennomganger. I tillegg er det sammenstilt og analysert statistikk, og utvalget har deltatt som observatør på ulike IKT-tilsyn gjort av NVE. Rapporten beskriver dagens praksis for rapportering av cyberangrep i kraftbransjen og utfordringer knyttet til dette. Utfordringer presentert har blitt videre undersøkt gjennom oppgavens intervjuer.

4.2.5 Dataanalyse

Dataanalyse er en viktig del av forskningsprosessen hvor bearbeidelse av innhentet datamateriale finner sted (Clark et al., 2019). Denne prosessen foregikk fortløpende for både intervjuene og dokumentene. Datamaterialet som ble innhentet først var intervjuene, og disse ble transkribert rett etter gjennomføring. Det ble ansett som viktig for å ha intervjuene friskt i minne. Muntlig språk er noe utfordrende å transkribere, men transkribering rett etter gjennomføring kan bidra til å sikre kvaliteten på overgangen fra lydfil til tekst. Etter bearbeiding av data var neste steg å kode intervjuene.

4.2.5.1 Koding

Den innledende fasen av kodingsprosessen innebar å få en generell oversikt over innholdet i intervjuene og dokumentene. De transkriberte intervjuene ble skrevet ut, og lest i papirformat. Det ble gjort for å få et helhetsinntrykk og en sammenfatning av hva som var gjennomgående temaer i intervjuene. Dokumentene ble også skrevet ut og lest før kodingen begynte. Dette var for å sikre god forståelse av innholdet. Koding kan organiseres på ulike måter, og det ble gjort en vurdering på hva som skulle bli benyttet før prosessen begynte. Et alternativ var å bruke NVivo, som er et anerkjent analyseverktøy. Vi hadde lite kjennskap til denne måten å analysere data på, og anså det som tidsbesparende å heller lage et eget system Excel. Denne måten å analysere data på hadde vi kjennskap til fra tidligere. Både intervjuene og dokumentene ble kodet på samme måte.

Vi tok utgangspunkt i stegvis-deduktiv induktiv metode (SDI-metode) for å kode datamaterialet (Tjora, 2021). Abduktiv tilnærming ligger et sted mellom induktiv og deduktiv tilnærming ettersom en kombinerer empirisk data med teoretisk resonnement (Blaikie & Priest, 2019). Ved bruk av SDI-metoden hadde vi mulighet til å navigere mellom empiri og teori. SDI-metoden benytter empirinær koding, også kalt in-vivo-koding (Clark et al., 2019). En kode er «et utsnitt av teksten – oftest en setning eller et avsnitt – som klassifiserer informasjonen» (Johannessen et al., 2021, s. 172). Ved empirinær koding foregår kodingen nedenfra, noe som betyr at kodene blir utformet direkte fra datamaterialet. En slik strategi for koding gjør det mulig «å redusere påvirkningen av forventinger og teorier som enhver forsker mer eller mindre eksplisitt vil trekke inn i analysen» (Tjora, 2021, s. 218). Det var noe varierende hvor mange empirinære koder hvert intervju og dokument inneholdt, men det estimeres at antallet lå mellom førti og seksti koder. Det er gunstig for det empiriske innholdet at kodingen ble gjennomført detaljert, for å inkludere alle viktige utsagn og ivareta det spesifikke materialet (Tjora, 2021).

I kodingens neste fase ble de empirinære kodene tematisk gruppert i såkalte kodegrupper. Kodegruppene var inndelt etter fem temaer som ble ansett som viktig for å svare på oppgavens problemstilling. Eksempler på overordnede temaer var dagens praksis, utfordringer, og resiliens. Prosessen resulterte i fire kodegrupper på første tema, fem kodegrupper på andre tema, to kodegrupper på tredje tema, to kodegrupper på fjerde tema og en kodegruppe på siste tema. I tillegg hadde vi en kodegruppe som het diverse. Den

kodegruppen ble brukt for innhold i intervjuene og dokumentene som ble ansett relevant, men som ikke passet inn i de øvrige kodene.

Kodingen foregikk i første omgang i hvert enkelt transkriberte intervju og dokument. Vi vekslet mellom koding av avsnitt og hele setninger, for å ivareta sammenhengen til utsagn og innhold. Deretter ble kodingen ført inn og sammenstilt i et Excel-dokument. Intervjuene og dokumentene fikk hvert sitt Excel-ark, som gjorde det mer oversiktlig. Det var likevel enkelt å navigere mellom arkene og sammenfatte innhold. Samme struktur ble brukt i begge Excel-arkene. Det endte med femten kodegrupper som vi organiserte innhold rundt, og de ble systematisk listet opp. Farger ble benyttet som virkemiddel i Excel-dokumentet for å tydeliggjøre kodene. I tillegg ble utsagnene fra samarbeidsorganisasjoner og nettselskaper skilt ved bruk av farger. Dette var med bakgrunn i at formålet og resultatet av intervjuene var noe ulik, og det ble dermed vurdert som viktig å skille utvalget i analyseprosessen. Vi kodet halvparten av intervjuene og dokumentene hver, og for å sikre samsvar og kvalitet ble hverandres kodinger gjennomgått av den andre.

Etter intervjuene og dokumentene var ferdig kodet, ble hver kodegruppe gjennomgått systematisk. Funn fra intervjuene og dokumentene ble sett i sammenheng. Det skapte en helhetlig dataanalyse, samt bidro til å se hvilke hovedpoeng fra kodegruppene som var gjennomgående og kunne underbygges med metodetriangulering. Metodetriangulering utdypes i neste delkapittel.

4.3 Validitet og reliabilitet

I dette delkapittelet blir begrepene validitet og reliabilitet benyttet for å redegjøre for kvaliteten i oppgaven. Validitet og reliabilitet er kvalitetskriterier i forskning, som bidrar til å belyse gyldigheten og påliteligheten til den metodiske fremgangsmåten (Clark et al., 2019). Å vurdere validitet og reliabilitet er en kontinuerlig prosess gjennom hele forskningsprosessen, fra design til datainnsamling og analyse. Høy grad av validitet og reliabilitet i forskningen bidrar til å øke tilliten til forskningsresultatene, og gir forskere muligheten til å bygge videre på disse resultatene i fremtidig forskning.

4.3.1 Validitet

I forskningslitteraturen anvendes begrepet validitet for å beskrive graden av gyldighet i en studie. Vanligvis skilles det mellom to former for validitet; intern og ekstern. Intern validitet refererer til i hvilken grad forskerens metoder og funn gjenspeiler formålet med studien og representerer virkeligheten (Johannessen et al., 2021). For å styrke den interne validiteten i denne studien ble det benyttet metodetriangulering. Metodetriangulering vil si at vi har brukt ulike metoder for å samle inn data. Det har gitt en mer helhetlig og nyansert forståelse av undersøkelser gjort i forbindelse med problemstillingen (Clark et al., 2019). Metodetrianguleringen inkluderte både intervjuer med nøkkelpersoner i samarbeidsorganisasjoner og nettselskap, samt en dokumentanalyse.

Totalt ble det gjennomført fjorten intervjuer med informanter som var direkte involvert og hadde god kunnskap om erfaringsdeling i bransjen. Intervjuguider ble utformet og benyttet konsistent for nettselskapene og samarbeidsorganisasjonene. For å underbygge funnene fra intervjuene, ble dokumentanalysen nøye utført og kodet på samme måte som intervjuene. Det ble inkludert fem dokumenter fra anerkjente aktører i relasjon til kraftbransjen og/eller IKT-sikkerhet i analysen. For å ytterligere styrke den interne validiteten kunne det eksempelvis blitt inkludert en spørreundersøkelse i metodetrianguleringen. Denne kunne inkludert små og mellomstore selskaper som intervjuobjekter, for å sikre bredde i form av ulike perspektiver. Til tross for det ble store nettselskaper vurdert til å ha høyest grad av innsikt i erfaringsdeling i kraftbransjen, og informanter til oppgaven ble utvalgt basert på dette.

Ekstern validitet handler om overførbarhet fra studien til andre områder (Johannessen et al., 2021). Oppgaven undersøker spesifikt erfaringsdeling mellom nettselskap etter cyberangrep. Nettselskaper er i en særstilling i den forstand at de er monopolister og ikke konkurrerer på samme måte som selskaper i andre bransjer. Det er ikke et mål for studien at funn skal være overførbare til andre områder. Abduktiv strategi skiller seg på denne måten fra induktiv strategi i dens søkelys på tolkning fremfor generalisering (Blaikie & Priest, 2019). Samtidig foregår deling av erfaringer også i andre bransjer. Beskrivelser, begreper, tolkninger og forklaringer som fremkommer av funnene i oppgaven, kan være nyttig på andre områder enn det som undersøkes her (Johannessen et al., 2021).

4.3.2 Reliabilitet

Reliabilitet handler om påliteligheten til undersøkelsesdataen (Johannessen et al., 2021). Det styrker reliabiliteten med en grundig beskrivelse og gjennomgang av den metodiske fremgangsmåten, noe som er gjort gjennom metodekapittelet. Undersøkelsen kan på denne måten bli etterprøvbar og pålitelig ved å være transparent.

Det er flere faktorer som både svekker og styrker reliabiliteten til intervjuene. For det første består datainnsamlingen av fjorten informanter, hvor fem informanter er fra sentrale samarbeidsorganisasjonene som har inngående kunnskap eller direkte kjennskap til erfaringsdeling i kraftbransjen. De resterende informantene har tilhørighet til store nettselskaper. Det styrker reliabiliteten å basere datagrunnlaget på relativt mange aktører som er tett knyttet til erfaringsdelingen i kraftbransjen, og å få refleksjoner fra begge parter. For det andre ble det benyttet lydopptak av intervjuene som dokumenterte hva informantene svarte på de ulike spørsmålene, og det er en styrke for reliabiliteten. Det sikrer kvaliteten på informasjonen som fremkommer, sitatbruk i oppgaven, og reduserer i tillegg evnen til egen fortolkning av notatene i etterkant av intervjuene.

En tredje styrke for reliabiliteten er utsendelse av informasjonsskriv i forkant av alle intervjuene (se vedlegg 1). Da hadde informantene likt utgangspunkt og beskrivelse av oppgavens formål og hensikt. En fjerde faktor som bidrar til å øke reliabiliteten er begge sin deltakelse i alle intervjuene som sikret en ensartet gjennomføring. Informantene hadde på denne måten det samme utgangspunktet til å fremme sine meninger og oppfatninger. Noe som kan ha påvirket relabiliteten i oppgaven var beslutningen om å rullere på hvem som hadde ansvar for å stille spørsmålene fra intervjuguiden. Begrunnelsen for valget om å rullere var at intervjuene i første runde ble gjennomført relativt intensivt, og ved noen anledninger foregikk det flere intervjuer på samme dag. Da fikk vi avlastet hverandre, og hovedoppgaven med å lede intervjuet ble fordelt. I tillegg er det ikke mulig å gjennomføre kvalitative intervjuer på helt lik måte, noe som kan svekke reliabiliteten i oppgaven. Selv om intervjuene forholder seg til en intervjuguide, har det vært ulike oppfølgingsspørsmål underveis i intervjuene. Informantene snakket derfor mer om noen temaer enn andre. Informantene var videre fra både nettselskaper og samarbeidsorganisasjoner, som resulterte i to intervjuguider med noe ulikt innhold.

Det er flere faktorer som også styrker og svekker reliabiliteten til dokumentanalysen. Dokumentene som ble valgt ut til analyse er skrevet av blant annet NSM, NVE og NSR. Dette er anerkjente aktører som er troverdig og pålitelig i sin mangeårige utgivelsesrekke av rapporter og artikler. Dette bidrar til å styrke reliabiliteten i dokumentanalysen. Ved koding og analyse av dokumentene kan det alltid være mulighet for at forskerens personlige bias eller forståelse har påvirkningen på studien. Dette vil svekke reliabiliteten. For å motvirke dette, ble alle dokumentene gjennomgått av oss begge. Det bidrar til å sikre kvalitet på utførelse og pålitelighet.

4.4 Etiske betraktninger

Gjennom forskningsprosessen er det viktig å ivareta etiske forskningsprinsipper. Før gjennomføring av intervjuer ble prosjektet derfor meldt inn til NSD for godkjenning. Dette ble gjort fordi vi ønsket å bruke lydopptak under intervjuene. Prosjektet er godkjent i henhold til NSD sine retningslinjer (se vedlegg 2). Det er videre flere forskningsprinsipper som er viktig å ta hensyn til i forbindelse med bruk av informanter som datainnsamling. Det er blant annet informantenes rett til å bestemme over egen deltakelse (Johannessen et al., 2021). Alle informantene fikk tilsendt et informasjonsskriv i forkant av intervjuene som inneholdt beskrivelser av deres rettigheter og en samtykkeerklæring. Selv om informasjonsskrivet ble sendt ut i forkant, ble det ansett som viktig å gjengi de mest sentrale punktene innledningsvis i intervjuene. Det sikret at alle informantene fikk med seg innholdet i informasjonsskrivet. Ti informanter valgte å underskrive samtykkeerklæringen i informasjonsskrivet, mens fire av informantene valgte å gi muntlig samtykke av praktiske hensyn.

Et annet etisk forskningsprinsipp er at forskningen ikke skal skade eller ha negative konsekvenser for informanter eller virksomhet (Johannessen et al., 2021). Én måte å ivareta dette forskningsprinsippet, er å sikre anonymitet til informantene i hele forskningsprosessen. Lydopptakene ble gjort i Nettskjema-Diktafon-appen utarbeidet av Universitetet i Oslo. Deretter ble lydopptakene lagret i Nettskjema, som umiddelbart krypterte opptakene på en egen dataserver. Informantene fikk hver sin kode, og oversikt over kodene ble lagret eksternt fra de transkriberte intervjuene. I tillegg var det bevisst å ikke stille spørsmål som innhentet kraftsensitiv informasjon. Det kunne potensielt fått negative konsekvenser for informanten og selskapet informanten tilhørte, men de formulerte spørsmålene la opp til generelle refleksjoner og meninger fra informantene.

5 Empiri og analyse

Det følgende kapittelet presenterer de viktigste funnene fra vår datainnsamling og analyse. Kapittelet er strukturert etter seks hovedtemaer; status for IKT-sikkerhet i kraftbransjen, status for erfaringsdeling mellom nettselskaper, resiliens i nettselskaper, identifiserte insentiver for erfaringsdeling mellom nettselskaper, dagen praksis for erfaringsdeling i samarbeidsorganisasjoner, og utfordringer tilknyttet erfaringsdeling. Temaene er valgt på bakgrunn av deres bidrag til å besvare oppgavens problemstilling.

5.1 Status for IKT-sikkerhet i kraftbransjen

Samlet viser funnene at kraftbransjen historisk sett har vært en bransje som har ligget bakpå når det gjelder IKT-sikkerhet, og som typisk har hatt søkelys på HMS og fysisk sikring. Samtlige informanter pekte på økende oppmerksomhet på IKT-sikkerhet i bransjen. De nevnte at digitale trusler hadde eksistert i lang tid, men det hadde ikke alltid vært høyt på dagsordenen. Den økende oppmerksomheten hadde skjedd i løpet av de siste årene, både fra myndighetenes side, men også hos KBO-enhetene og det øvrige konsernet som disse er organisert under.

> *Alle i kraftbransjen har skjønt at sikkerhet er viktig. Alle har puttet inn ressurser og gjort noe der (...)* (Rådgiver for digitalisering og IKT-sikkerhet).

Seks av informantene nevnte at grunnene til den økte oppmerksomheten blant annet var innføring av ny teknologi, bruk av skytjenester, utenlandske leverandører, tilkobling av systemer til internett, og sikkerhetssituasjonen som følge av krigen i Ukraina og tilhørende cyberhendelser. Bruk av ny teknologi og utenlandske leverandører er utviklingstrekk som gjør kraftbransjen til et mer komplekst system, i henhold til Perrow (1999) og Leveson (2012) sine teoretiske bidrag. Funn fra dokumentanalysen tydeliggjorde at kraftbransjen var i utvikling og opplevde et høyt angrepstrykk, og det var forventet å vedvare i tiden fremover (Tøien et al., 2021). Dagens sikkerhetssituasjon i Europa viste at norske selskaper måtte være forberedt på et bredt spekter av sammensatte trusler, samt holde seg oppdatert på utviklingen av den digitale sårbarhetsflaten (NSM, 2023). Særlig to informanter, samt dokumentet fra NSM (2023), poengterte at kraftbransjen er et attraktivt mål hvis en trusselaktør ønsker å gjøre stor samfunnsmessig skade.

Mange av informantene fortalte at nettselskapene stod overfor de samme trusselaktørene. En av informantene beskrev tre ulike trusselaktører som kraftbransjen stod overfor. Den første var opportunister som masseutsender phishing- eller utpressingsmail i håp om å finne en sårbarhet. De stod for ca. 80% av phishing-mailene i en av informantenes nettselskap. Den andre var personer med en økonomisk, men ikke-politisk agenda. De forsøkte å komme seg inn, kryptere, hente ut data, og utpresse. I den forbindelse var det snakk om store beløp. Den tredje var såkalte Advanced Persistent Threat (ATPer) med politiske motiver, vanligvis nasjonalstater eller statsautoriserte grupper. Aktører som har som mål å manipulere kritisk infrastruktur behøver ressurser og ekspertise (Geers, 2009). ATPer var kjent for informantene som aktørene med svært høy kapasitet og kompetanse, og hvis de ønsket å angripe norske selskaper, var det svært få som trodde de kunne motstå angrepet. Bransjen stod dermed overfor ulike trusselaktører, hvor noen hadde potensial til å gi større konsekvenser enn andre.

Dokumentene fra NVE (Tøien et al., 2021), Riksrevisjonen (2021) og Meld. St. 38 (2016-2017) understrekte at det ble gjort mye godt arbeid med IKT-sikkerhet i kraftbransjen, men at det fortsatt var visse svakheter hos noen selskaper. To av informantene fortalte at mange angrep var basert på utnyttelse av åpne sårbarheter som kunne vært forhindret med noen enkle tiltak, slik som å ha kontroll på brukere og tilganger, begrense antall administratorrettigheter, holde seg oppdatert på trusselbildet, og å følge NSM sine grunnprinsipper. En redegjørelse av NSM sine grunnprinsipper finnes i delkapittel *2.3.2 NSM sine grunnprinsipper for IKT-sikkerhet*. Seksjonssjef og IKT-sikkerhetskoordinator sa følgende om sårbarheter i IKT-systemene:

> *Hvis man jobber med grunnsikringen hele tiden, så er veldig mye gjort* (Seksjonssjef og IKT-sikkerhetskoordinator).

Det ble samtidig poengtert at en av grunnene til at det fortsatt eksisterte svakheter ved grunnsikringen av IKT-sikkerhet i noen selskaper, kunne være den raske teknologiske utviklingen som skjedde i bransjen. Teknologiutviklingen innebar blant annet at den fysiske OT-biten frem til nå hadde være helt isolert fra internett. Det skjedde en utvikling hvor innsamlet data fra sensorer ble koblet til internett for å styre strømnettet. Dette er i samsvar med Lee (2008) sin beskrivelse av cyberfysiske systemer. Informantene var opptatt av at nye teknologiske løsninger skulle sikres godt, slik at man unngikk at trusselaktører enkelt kunne utnytte nye inngangsporter til strømnettet. Dette støttes i dokumentet fra NVE (Tøien et al.,

2021), hvor det ble påpekt at ved nye digitaliseringsinitiativer var det viktig at selskaper styrte risiko ved å investere i IKT-sikkerhetstiltak, prosedyrer og beredskap.

5.2 Status for erfaringsdeling mellom nettselskaper

En informant fortalte om erfaringsdeling som en etablert praksis i kraftbransjen, og en del av samarbeidet mellom nettselskaper. På et overordnet nivå anerkjente samtlige informanter erfaringsdeling som en arena hvor nettselskaper kunne hente inspirasjon og lære av hverandre, samt opprettholde kontakt seg imellom. Det hadde vært en utvikling rundt deling av erfaringer og åpenhet i bransjen, og det ble opplevd som mer akseptert de senere årene.

> *Vi ser hele tiden at de som er åpne og deler om hendelser som regel kommer veldig godt ut av det* (CISO).

Bakgrunnen for denne utviklingen var, ifølge flere av informantene, en kombinasjon av ulike faktorer. Blant annet den sikkerhetspolitiske situasjonen i Europa, opplevd nyttighet ved å dele og økt fokus blant aktører i kraftbransjen. Samtidig var det noen utsagn fra informantene som tilsa et forbedringspotensial for erfaringsdeling. For eksempel var det en av informantene som sjeldent opplevde erfaringsdeling i etterkant av cyberangrep. En annen sa det generelt var svært lite erfaringsdeling i kraftbransjen. Samlet sett er informantene både positive og negative til hvordan erfaringsdelingen skjer i kraftbransjen i dag, men hovedinntrykket er at de fleste informantene var fornøyde.

Det var videre to eksempler på åpenhet og erfaringsdeling i forbindelse med cyberangrep som gikk igjen blant informantene. Det var Hydro- og Volue-hendelsen. Fire av informantene fortalte at dette var cyberangrep som har blitt hyppig brukt som eksempler på arrangementer i etterkant av angrepene.

> *Volue-hendelsen har vist at [cyberangrep] er et tema som kan tas opp og som vi kan diskutere problemstillinger rundt. Det har gjort det lettere å se for seg hva man bør tenke på ved en eventuell hendelse. Vi bruker det nødvendigvis ikke bevisst eller systematisk, men (...) ting som har skjedd før vil alltid være med oss når vi prøver å se for oss potensielle angrep. Man bruker det i praksis som læring* (Leder for informasjonssikkerhet).

Den siterte informanten fortalte at i tillegg til å hente inspirasjon og ta lærdom fra Volue-hendelsen, hadde Hydro-hendelsen blitt ansett som et vendepunkt for IKT-sikkerhet i mange nettselskaper. Ifølge informanten var årsaken stor medieoppmerksomhet, som videre førte til økt bevissthet rundt IKT-sikkerhet blant ansatte og ledelsen i nettselskapene. Hendelsene viser hvordan erfaringsdeling og åpenhet kan foregå i praksis. Informantene sa derfor at hendelsene kunne gjøre det lettere for dem å se for seg hva de burde tenke på ved et eventuelt cyberangrep.

5.3 Resiliens i nettselskaper

Resiliens er et begrep som har blitt benyttet i varierende grad av samarbeidsorganisasjonene og nettselskapene. For to av informantene var resiliens et fremmedord, men da informantene fikk presentert en definisjon av begrepet, sa de at det var måten de jobbet på i praksis. I de resterende nettselskapene var resiliens et begrep som ble benyttet. En av lederne i samarbeidsorganisasjonene hadde et bredt kontaktnettverk i bransjen, og opplevde begrepet resiliens som mer og mer innarbeidet.

Noe av bakgrunnen for et større søkelys på resiliens, var samarbeidsorganisasjonene og nettselskapene sin brede enighet om at det ikke var oppnåelig å beskytte seg fullstendig mot alle cyberangrep. Teoretiske bidrag omtaler også resiliens som en måte selskaper og bransjer kan imøtekomme en kompleks og usikker verden (Anholt & Boersma, 2018). I den forbindelse har også teori rundt begrepet resiliens blitt utvidet til cyberresiliens, hvor fokuset er spesifikt knyttet til å forebygge og gjenopprette etter cyberangrep (Björck et al., 2015). Tre av informanten sa at hvis trusselaktører ønsket å ramme strømforsyningen, ville de finne en måte å utføre et angrep. Siden det ikke ville være oppnåelig å beskytte seg fullstendig mot cyberangrep, poengterte syv av informantene at de måtte forberede seg på å forebygge og eventuelt håndtere et angrep.

> *En av de beste måtene å forberede seg, er å tenke at det faktisk kan skje. Det er hvert fall det vi jobber aktivt med. Ikke bare å forhindre at de lykkes, men også være forberedt på å håndtere det hvis de faktisk lykkes* (Leder for informasjonssikkerhet).

Informantens sitat er gjenkjennbart i det Pettersen og Schulman (2016) skriver om resiliens i teorikapittelet, som innebærer å opparbeide en evne til å overvåke, oppdage, håndtere og

gjenopprette. For å bygge et motstandsdyktig nettselskap la informantene vekt på flere sentrale elementer. For eksempel å ha på plass systemer som oppdager inntrengere, sikkerhetsovervåking, backup-rutiner, beredskapsøvelser, hendelseshåndteringsteam, og gjenopprettingsplaner. Dette er punkter som er sentrale i alle de tre formene for resiliens; precursor, restoration og recovery (Pettersen & Schulman, 2016). I tillegg nevnte fire informanter kulturbygging i selskap som helt essensielt for å oppnå større grad av resiliens. Selv om kultur i selskaper vil være en naturlig del av alle formene for resiliens, er det særlig viktig å ha søkelys på i recovery resiliens (Pettersen & Schulman, 2016). Dette er også i samsvar med Martin (2019) sin omtalelse av aktiv resiliens, hvor et viktig steg er å lære av sine erfaringer.

Et annet punkt som var viktig for å bygge motstandsdyktighet, som lederen for en samarbeidsorganisasjon fortalte om, var at det i mange tilfeller ikke var gunstig å fortsette å bygge for at systemene skulle bli sikrere og sikrere. Tiltakene ville ikke nødvendigvis ha den tiltenkte effekten, hvis dette ble praktisert.

> *Det er også veldig problematisk å gjenoppbygge en tjeneste fordi man bør egentlig bygge den på nytt. Hvis man tar hensyn til de opprinnelige årsakene til at det skjedde, årsakene til at det utviklet seg, og årsakene til at det ikke ble detektert, når bygger opp igjen, så har det hvert fall blitt litt bedre* (Leder i samarbeidsorganisasjon).

Ifølge sitatet vil det dermed være aktuelt å ta hensyn til alle aspektene i hendelsesforløpet og vurdere resiliente tiltak deretter. Her vil det være relevant å vise til Kolb (2015), Nonaka og Takeuchi (1995), som berører temaene kunnskap, læring, og kombinering av ny og eksisterende kunnskap.

5.4 Identifiserte insentiver for erfaringsdeling mellom nettselskaper

Gjennom oppgavens funn er det identifisert flere faktorer til at nettselskaper velger å dele erfaringer med hverandre. Disse kan kategoriseres under Gjesvik (2019) sine tre insentiver for å dele informasjon beskrevet i teorikapittelet; gjensidig utbytte, tillit og delt forståelse.

5.4.1 Gjensidig utbytte av erfaringsdeling

Mye av erfaringsdelingen i kraftbransjen skjer i regi av ulike samarbeidsorganisasjoner. I dokumentanalysen ble det avdekket at organisasjoner i bransjen var opptatt av å sikre at medlemmene opplevde merverdi gjennom sine medlemskap (Riksrevisjonen, 2021). Ifølge informantene fra organisasjonene fikk de gode tilbakemeldinger på at erfaringsdeling ga utbytte for medlemmene. Syv av åtte nettselskaper sa også at de opplevde utbytte av erfaringsdelingen som skjedde i kraftbransjen i dag. Det viste i stor grad samsvar mellom organisasjonene og nettselskapenes oppfattelse av utbytte gjennom erfaringsdeling.

> *Det er nesten uten unntak at vi har utbytte av erfaringsdeling* (IKT-sikkerhetskoordinator).

> *Jeg føler veldig at vi har nytte av erfaringsdeling. Det må jeg poengtere veldig høyt. Vi har definitivt utbytte av det* (Seksjonssjef og IKT-sikkerhetskoordinator).

Flere av informantene fra selskapene mente de ble mer bevisst på trusler og løsninger knyttet til IKT-sikkerhet, oppdaget felles problemstillinger, og klarte å forankre informasjon og erfaringer i arbeidet med IKT-sikkerhet i eget selskap gjennom erfaringsdeling. Basert på intervjuene er det derfor identifisert tre bidrag for opplevelsen av gjensidig utbytte blant nettselskapene; bevisstgjøring, felles problemstillinger og forankring i eget selskap.

5.4.1.1 Bevisstgjøring gjennom erfaringsdeling

Fem av informantene beskrev bevisstgjøring som et virkemiddel for å belyse ukjente faktorer i forbindelse med trusselbildet og sårbarheter i felles leverandører eller systemer. Poenget samsvarer med tidligere forskning hvor informasjonsutveksling og kommunikasjon presenteres som faktorer som kan redusere det ukjente og gi bedre grunnlag for aktører å arbeide med cybertrusler (Aakre, 2020). Bevisstgjøring skjedde, ifølge informantene, både gjennom samarbeidsorganisasjoners utsendelser av informasjon til medlemmer, og gjennom arrangementer hvor medlemmene møttes og delte erfaringer. Generelt bidro dette til større bevissthet rundt IKT-sikkerhetsproblemer og -løsninger hos informantene fra nettselskapene. To av informantene følte at de ble mer bevisst gjennom informasjon tilsendt fra samarbeidsorganisasjonene de var medlem av, fordi de ikke hadde mulighet eller ikke ønsket å delta på arrangementer i regi av samarbeidsorganisasjonene. Informantene som deltok på

arrangementer opplevde større bevissthet gjennom medlemmenes egne foredrag om erfaringer, enn gjennom informasjon tilsendt på e-post.

> *Hvis du hører fra andre som har hatt et angrep kan det være interessant å snakke med det selskapet direkte, og ha noen oppfølgingsspørsmål og dialog rundt det* (IKT-sikkerhetskoordinator).

> *Når det har vært hendelser, så er det veldig interessant å høre det de andre sier. Det føler jeg vi får mye ut av* (IKT-sikkerhetskoordinator).

> *Jeg tror i høyeste grad at den informasjonen vi ga ut etter angrepet mot oss, hadde verdi for andre virksomheter* (CISO, eksternt selskap).

Utsagnene gir indikasjoner på at nettselskapene ønsket å lære av hverandre, og de syntes det var spennende å høre hverandres erfaringer og tanker i etterkant av cyberangrep. Leder fra en samarbeidsorganisasjon uttalte videre at erfaringsdeling blant medlemmene var av stor betydning for å øke bevissthet, da sårbarheter og risikoer kunne bli belyst og diskutert i fellesskap. Dette understøttes også av dokumentet fra NVE (Tøien et al., 2021), som skrev at å holde oversikt og administrere sårbarheter ga mulighet til å oppdage og rette mulige svakheter i systemet.

> *Det at medlemmer deler det de opplever er nok med på å bevisstgjøre andre medlemmer som kanskje ikke enda har opplevd de store tingene. På forrige konferanse var det et medlem som fortalte om en konkret hendelse de hadde hatt i sitt driftskontrollsystem. Jeg tenker at den informasjonen var veldig viktig for de andre medlemmene for det viser hvor sårbart ting er, og hvor viktig det er å beskytte og ha kontroll på risikoene som de alle står overfor* (Leder i samarbeidsorganisasjon).

Slike utsagn underbygger at selskapene opplevde at direkte kommunikasjon mellom medlemmene førte til større bevissthet enn informasjon som ble sendt ut av samarbeidsorganisasjoner. Dette samsvarer med tidligere forskning, hvor innflytelsestiltak gjort av myndigheter var av mindre betydning enn de investeringene som aktører i bransjen gjorde selv (Atkins & Lawson, 2021). Sitatene belyser også et annet viktig poeng om gjensidig nytte, nemlig at nettselskapene sto overfor felles problemstillinger.

5.4.1.2 Felles problemstillinger blant nettselskaper

Ti av informantene ga uttrykk for at en av de primære grunnene for at nettselskaper delte erfaringer seg imellom var på grunn av felles problemstillinger de stod overfor. Dette omfattet både bruk av mange av lignende systemene, leverandørene og metodene, samt at de stod overfor de samme trusselaktørene.

> *Vi har de samme systemene, de samme leverandørene og mye av de samme type løsningene. Når veldig mye er likt er det greit for andre å vite om man har sett noen trusler mot disse, eller finner svakheter* (IKT-sikkerhetskoordinator).

Dokumentene fra NVE (Tøien et al., 2021) og Riksrevisjonen (2021) støtter opp under dette ved å beskrive nettselskapene som brukere av samme leverandører og systemer. Ifølge en av informantene fra nettselskapene var det derfor meget nyttig for andre selskaper om man selv har sett trusler eller svakheter i felles leverandører eller systemer, og delte denne informasjonen. På denne måten kunne andre selskaper oppdage eller avdekke svakheter eller trusler, og potensielt forhindre angrep mot seg selv. Blant informantene fra nettselskapene ble informasjon om indikatorer trukket frem som svært nyttig i møte med felles problemstillinger.

> *Når vi får indikatorer eller tekniske detaljer slik at vi kan søke opp IP-adresser, så synes vi det er veldig nyttig for å beskytte oss. Da kan vi søke i våre systemer etter lignende aktivitet, så vi prøver veldig ofte å få tak i indikatorer. Det er noe av det viktigste man kan dele* (Seksjonssjef og IKT-sikkerhetskoordinator).

> *Indikatorvarslene er veldig bra. Da får vi liste over applikasjoner som blir brukt, IP-adresser, URLer. Det er veldig fint å putte de inn i sine egne system og få flagget, hvis noe skulle oppføre seg underlig. Det har skjedd mer enn en gang at det har slått ut på indikatorene hos oss, så det viser at det er nytte i det* (IKT-sikkerhetsansvarlig).

Ved å få informasjon om ulike indikatorer i etterkant av et angrep kunne selskaper bruke informasjonen til å «scanne» sitt eget system, og potensielt oppdage spor eller tegn på innbrudd. En av informantene sa at dette var relevant på grunn av hvordan trusselaktører opererte mot aktører i kraftbransjen, da visse angrepsgrupper kunne infiltrere systemene og vente i opptil et år før de gjennomførte et angrep på et passende tidspunkt. I den forbindelse

kan det være nyttig å se til begrepet precursor resiliens, som involverer evnen til å overvåke og opprettholde forholdene for å forebygge hendelser (Pettersen & Schulman, 2016).

> *Hvis du klarer å oppdage disse gruppene før de klarert utnytte posisjonen sin, vil erfaringsdeling ha en svært positiv effekt på IKT-sikkerheten i kraftbransjen* (CISO).

Flere av informantene trakk også fram at selskapene hadde ulike ressurser når det kom til IKT-sikkerhet. Noen var derfor helt avhengig av å få informasjon fra andre, da de ikke hadde kapasitet til å overvåke egne systemer. Dette førte til betydelig variasjon i evnen til å oppdage angrep blant nettselskapene. Hvis et selskap ikke var i stand til å oppdage trusler mot sine egne systemer, visste de heller ikke om potensielle inntrengere «lå inne og ventet». I slike situasjoner ville indikatorer fra andre være «gull verdt». Felles problemstillinger knyttet til systemer og trusselaktører virket derfor som at bidrar til en følelse av gjensidig utbytte av erfaringsdeling blant nettselskapene.

5.4.1.3 Forankring i eget nettselskap

For at informasjon om felles utfordringer skulle føre til utbytte var det viktig at nettselskapet klarte å forankre informasjonen i eget arbeid, ifølge en av informantene fra samarbeidsorganisasjonene. Flere av informantene fra organisasjonene sa videre at de opplevde at deres medlemmer klarte å bruke informasjon og erfaringer som ble delt.

> *Vi har fått veldig god respons fra flere medlemmer hvor de har redegjort for hvordan de benytter informasjonen de har fått fra oss inn i sitt arbeid. Det synes jeg er veldig flott å høre* (Leder i samarbeidsorganisasjon).

Sitatet ble også støttet av fem av nettselskapene. De beskrev situasjoner hvor de hadde lest eller hørt noe gjennom samarbeidsorganisasjoner de var medlem i, og deretter implementert sikkerhetstiltak i eget selskap. Å forankre det man har lært kan ses i sammenheng med internaliseringsfasen og aktiv eksperimentering, presentert i teorikapittelet (Kolb, 2015; Nonake & Takeuchi, 1995). Her brukes forslag til forbedring i praksis, noe som i stor grad sammenfaller med det nettselskapene gjør når de forankrer erfaringer delt i eget arbeid.

> *Det er ofte litt småting man hører folk har løst på en litt annen måte, som man kan ta med seg hjem igjen og implementere hos seg selv* (IKT-sikkerhetskoordinator).

> *Det som er fint med å dele erfaringer er at du ofte får refleksjoner, diskusjoner og dialog tilbake. Det hjelper ofte med å ta forbedringer med tilbake i egen organisasjon. Jeg ser på det som et godt bidrag til forbedringsarbeidet. Hvordan du kan forbedre arbeidsprosesser, prosedyrer, håndteringen av ting osv. Du samler egentlig ideer når du har en dialog med andre, kan du si litt enkelt* (CISO, eksternt selskap).

Slike utsagn viser at nettselskapene erkjente verdien av å dele erfaringer med hverandre. Det kunne både hjelpe andre til å implementere nye IKT-sikkerhetstiltak, samtidig som det inviterte andre til å videreutvikle tiltak med selskapet som delte. Basert på det informantene sa, virket det også som det hadde blitt enklere å implementere IKT-sikkerhetstiltak internt i eget selskap over tid. Dette skyldtes en økende forståelse for cyberangrep og de potensielle konsekvensene av slike hendelser sammenlignet med tidligere. Et av nettselskapene sa at ledere og økonomiansvarlige i deres selskap var mer åpen for innspill om sikkerhetstiltak som IKT-avdelingen mente de burde implementere. Til tross for det, var det også flere informanter som synes det var vanskelig å få ledelsen i eget selskap til å forstå kritikaliteten og derav investere i IKT-sikkerhetstiltak.

> *Jeg synes det har blitt lettere de siste årene. Folk som sitter med pengesekken forstår gjerne konsekvensene av et cyberangrep bedre etter krigen i Ukraina* (IKT-sikkerhetsansvarlig).

> *Jeg kan med sikkerhet si at ledelsen ikke er bevisst på slike forhold. Det er min avdeling som har fokus på dette og prioriterer det* (IKT-sikkerhetskoordinator).

Utsagnene indikerer at nettselskapene hadde varierende synspunkter på involvering og forståelse i ledelsen angående IKT-sikkerhet. En av informantene sa at hvorvidt ledelsen i et selskap hadde kunnskap og forståelse rundt IKT-sikkerhet, hadde en innvirkning på hvilken grad det var mulig til å bruke det man hadde lært av andre nettselskaper inn i eget selskap. Det er i den forbindelse relevant å referere til kombineringsfasen til Nonaka og Taceuchi (1995). I kombineringsfasen blir ny kunnskap integrert med eksisterende kunnskap, og det vurderes om det er nødvendig å forbedre arbeidsmetodene. Utsagnene antyder en god forståelse og involvering av ledelse i IKT-sikkerhet kan bidra til at nye IKT-sikkerhetstiltak blir tatt i bruk, noe som kan styrke gjensidig utbytte av erfaringsdeling.

5.4.2 Tillit mellom nettselskaper

Datamaterialet viser at tillit var svært viktig for at nettselskaper skulle dele erfaringer med hverandre. Alle nettselskapene uttalte at kjennskap til hverandre, tidligere møter og samtaler om relevante temaer gjorde det enklere å dele nye erfaringer. Tillit var, ifølge en av samarbeidsorganisasjonene, viktig for å skape en lavere terskel for å kunne snakke «jovialt» om hva man hadde sett i eget selskap. Dette åpnet opp for at andre selskaper også bidro med sine observasjoner, og så begynte det å «rulle». Slik ble det generelt lettere å dele og spørre om råd. Informantenes oppfatning av tillit stemmer overens med funnene fra tidligere forskning, der tillit gjennom personlige nettverk ble identifisert som svært viktig for lettere deling av informasjon (Bodsberg et al., 2018).

> *Du er nesten nødt til å ha tillit. Hvis ikke vil mye av samarbeidet falle i grus* (IKT-sikkerhetskoordinator).

> *Jo bedre du kjenner en part, jo større sannsynlighet er det for at du har tillit nok til å dele* (Leder i samarbeidsorganisasjon).

Informantene ga generelt inntrykk av at de delte sine erfaringer med personer de stolte på, hadde bekjentskap med, og som de visste stod overfor samme problemstilling. Tillit var, ifølge en av informantene, helt nødvendig for at nettselskapene skulle dele erfaringer med hverandre. Informantenes refleksjoner rundt bekjentskaper og etablering av relasjoner, samsvarer med det som blir omtalt som tillit mellom individer (Gjesvik, 2019). Disse faktorer kan betraktes som mellommenneskelige, og ble fremhevet som å kreve en høy grad av åpenhet. Et dokument hevdet også at åpenhet dannet grunnlaget for læring og bidro til at virksomheter i bransjen var i bedre stand til å forebygge, avdekke og håndtere hendelser (Meld. St. 38 (2016-2017)). Utsagn fra en av informantene støttet opp om dette ved å si at de delte informasjon fordi de ønsket å lære mer og forbedre seg. Informanten nevnte det var av personlig initiativ, og ikke pålagt gjennom arbeidsgiver. Basert på funnene om tillit, kan det virke som om informantene delte en oppfatning av tillit og åpenhet som viktige faktorer for læring gjennom erfaringsdeling.

En av informantene fra samarbeidsorganisasjonene sa at en faktor som påvirket grad av tillit, var de regulatoriske retningslinjene som nettselskapene måtte forholde seg til. Først og fremst var nettselskapene klassifisert som monopolister, og flere av informantene sa at det gjorde at

de kunne snakke mer åpent med hverandre. De var ikke redde for å avsløre bedriftshemmeligheter, og hadde derfor en lav terskel for å dele erfaringer. For det andre var samtlige av informantenes nettselskap KBO-enheter. Gjennom KBO-ordningen var det enda enklere å dele informasjon, da KBO-enheter kan dele kraftsensitiv informasjon med andre virksomheter (Kraftberedskapsforskriften, 2012, § 6-1).

> *Der har jo NVE gjort det enkelt for oss, fordi at de har sagt at såkalte KBO-enheter har lov til å dele informasjon seg imellom, selv om det er klassifisert som kraftsensitivt. Alle KBO-enheter er underlagt det samme lovverket. Så da slipper vi å forholde oss til det. Altså å passe veldig på hva vi sier vi ikke sier, og det er definitivt bidragsytende for at vi kan dele erfaringer med hverandre på den måten vi gjør* (IKT-sikkerhetskoordinator).

En av informantene beskrev KBO-ordningen som et insentiv for å dele erfaringer i seg selv. Ifølge informanten trengte ikke nettselskapene å være så forsiktige med hva de delte med hverandre på grunn av denne ordningen. Basert på fremlagte utsagn, virker KBO-ordningen og monopolvirksomheten å være bidrag til økt tillit mellom nettselskapene, siden de var klar over at den informasjon de delte ikke kunne bli videreformidlet.

5.4.3 Delt forståelse av trusler, verdier og sårbarheter

I møte med den digitale utviklingen i samfunnet ble det identifisert i dokumentanalysen et behov for å se «hele bildet» for å sikre felles verdier (Tøien et al., 2021). Videre ble betydningen av felles motstandskraft i et komplekst risikobilde fremhevet (NSM, 2023). Flere av informantenes utsagn støttet funnene i dokumentanalysen, og beskrev sitt eget selskap som en del av noe større.

> *Jeg tror at erfaringsdeling kan hjelpe bransjen som helhet, men jeg tror at man må få alle til å skjønne at man er en del av det. Å se seg selv i et større bilde er utrolig viktig* (CISO).

> *For å beskytte norsk kritisk infrastruktur som helhet er det helt avgjørende at vi er motstandsdyktige alle sammen* (Seksjonssjef og IKT-sikkerhetskoordinator).

> *Det er viktigere i dag å dele mer på tvers, og egentlig ha et økosystem for deling. Trusselaktørene bruker alle muligheter til å få tak i informasjon, så (...) selskapene må bli mye flinkere til å stå sammen som én enhet. Da gjelder det å dele informasjon. Da tror jeg vi på en måte sitter på mye større ressurser enn angriperne* (CISO, eksternt selskap).

De fleste av informantene delte den samme forståelsen av at felles motstandskraft var viktig for beskyttelsen av verdiene som kraftbransjen representerer. Oppgavens funn samsvarer med funn presentert i tidligere forskning, hvor bevissthet rundt hvilke kritiske verdier som krever beskyttelse ble presentert som viktig for god IKT-sikkerhet (Bodsberg et al., 2018). Tidligere forskning har også påpekt at trusler som truer et system som helhet, kan akselerere samarbeidet mellom aktører (Atkins & Lawson, 2021). Informantenes utsagn i lys av dette, kan tyde på at felles trusselaktører på lignende vis har skapt større rom for erfaringsdeling mellom nettselskapene. Flesteparten av informantene i oppgaven uttrykte videre at det var «gladelig deling» mellom dem. Gladelig deling kan sammenlignes med det Rak (2002) kalte todelt deling, hvor selskaper både deler med andre og føler at andre deler med dem.

> *Vi har ikke noe problem med å dele, for både vi og de vi deler med kommer styrket ut av erfaringsdeling. Den største motivasjonen for å dele med andre er at vi kan styrke andre basert på våre erfaringer* (IKT-sikkerhetskoordinator).

Flere av informantene ga dermed uttrykk for at erfaringsdeling var en viktig arena for å oppnå delt forståelse av verdier, trusler og sårbarheter i kraftbransjen. Kjennskap til sårbarheter var, ifølge Rak (2002), helt nødvendig for at todelt deling kunne finne sted. Informantenes utsagn understøttes av funn gjort i dokumentanalysen, der kjennskap til trusler og verdier ble trukket fram som viktig for god IKT-sikkerhet (NSM, 2023).

> *Vi må kjenne dem og de som truer oss og våre verdier. Vi må vite hvordan de påvirker oss, hvilke verktøy de bruker* (NSM, 2023).

Trusler og verdier er sammen med sårbarheter de tre punktene som utgjør trefaktormodellen, presentert i teorikapittelet (NSM, POD & PST, 2015). Gjennom oppgavens funn kan det virke som at mange av informantene i nettselskapene innehadde en delt forståelse av trusler, verdier og sårbarheter knyttet til kraftbransjen.

5.5 Dagens praksis for erfaringsdeling i samarbeidsorganisasjoner

I dette kapittelet presenteres informantenes gjenfortellinger rundt organisering av samarbeidsorganisasjoner, hva som fungerer bra i samarbeidsorganisasjonene, den uformelle kontakten som oppstod mellom nettselskaper, ulik erfaringsdeling blant nettselskaper og hvilke erfaringer som ble delt mellom nettselskaper.

5.5.1 Organisering av samarbeidsorganisasjoner

Erfaringsdeling foregikk hovedsakelig gjennom ulike samarbeidsorganisasjoner. Samarbeidsorganisasjonene kan betegnes som praksisfellesskap, hvor en gruppe mennesker deler bekymringer, problemer og entusiasme for et tema, og sammen utvikler kunnskap på områder gjennom dialog med hverandre (Wenger et al., 1991). Måten erfaringsdeling foregikk gjennom samarbeidsorganisasjonene kan ses i sammenheng med læringssirkelen basert på Kolb (2015), og Nonaka og Takeuchi (1995). I sirkelen starter læringsprosessen med en konkret hendelse, og videre blir erfaringer fra hendelsen delt med andre på en sosial arena, eller et såkalt praksisfellesskap (Wenger et al., 1991).

Informantene nevnte følgende samarbeidsorganisasjoner; KraftCERT, Nettalliansen, Forum for informasjonssikkerhet i kraftforsyningen (FSK), og i noen grad Fornybar Norge. Disse ble redegjort for i *2.4 Samarbeidsorganisasjoner i kraftbransjen*. NVE ble også nevnt som en aktør som hadde bidratt og oppfordret til erfaringsdeling. Alle informantene i oppgaven sa at de var medlem av KraftCERT og/eller FSK, mens ingen av dem var medlem av Nettalliansen. Nettalliansen var forbeholdt små og mellomstore nettselskap, og ingen av nettselskapene passet inn i denne beskrivelsen. Videre var det noe varierende om informantene nevnte Fornybar Norge eller ikke, samt hvordan denne samarbeidsorganisasjonen ble omtalt i forbindelse med erfaringsdeling og sikkerhetsområdet. Av noen informanter ble det omtalt som en organisasjon som ikke tilbyr eller har fagkompetanse innen sikkerhet, mens andre påpekte at Fornybar Norge har fått sikkerhet på agendaen den siste tiden og at de var medlem der.

Organiseringen av samarbeidsorganisasjonene ble opplevd av de fleste informantene fra nettselskapene som velfungerende. Ifølge informantene fra nettselskapene fungerte samarbeidsorganisasjonene som naturlige samlingspunkter og dialogpunkter rundt IKT-sikkerhet. Samarbeidsorganisasjonene hadde litt ulike kapasiteter og tilnærminger, og det

gjorde at de utfylte hverandre gjorde godt. En informant anså det som en fordel at samarbeidsorganisasjonene hadde litt ulik tilnærming og fokus, fordi bransjen bestod av personer som hadde ulike interessefelt og preferanser på hva de er opptatt av i sin stilling. Da hadde informantene ulike arenaer å velge mellom, og kunne prioritere selv hvilke man ønsket å delta på.

KraftCERT ble beskrevet som en medlemsorganisasjon som arrangerer møter og webinarer, sendte ut informasjon via e-post, og hadde opprettet en chatplattform. I tillegg nevnte informantene at de hadde et sektoransvar, som blant annet innebar å dele informasjon og erfaringer med både medlemmer og ikke-medlemmer. Det ble forklart som en del av avtalen KraftCERT hadde med myndighetene. Dokumentanalysen påpekte at posisjonen til KraftCERT gjorde de til et viktig bindeledd mellom aktører i kraftbransjen (Tøien et al., 2021). De fleste informantene var overordnet fornøyde med hvordan KraftCERT fungerte. KraftCERT ble beskrevet som relativt flinke til å varsle om pågående angrep, sårbarheter eller indikatorer. Fem av informanter mente det var viktig at KraftCERT «var på banen», samt at de holdt nettselskapene kontinuerlig oppdatert på relevant informasjon. KraftCERT ble også trukket frem som en verdifull sparringspartner, hvis det oppstod spørsmål blant selskapene om diverse problemstillinger. Dette samsvarer med dokumentanalysen som viste at KraftCERT har bidratt til at NVE har fått bedre oversikt over trusselbildet, som følge av at de blant annet overvåket utviklinger i sårbar teknologi som virksomheter i kraftforsyningen brukte, og delte dette videre (Tøien et al., 2021).

FSK var den andre samarbeidsorganisasjonen oftest trukket fram av informantene. De arrangerte to årlige konferanser hvor erfaringsdeling fant sted. Medlemmene kunne møtes for å snakke om hva som har skjedd, hvilke fokusområder de hadde, og hva de skulle jobbe med fremover. Informantene vektla at den ene dagen var lukket for alle utenom medlemmene, mens den andre dagen var åpen for også andre aktører. Fire av informantene påpekte at det ble lagt opp til åpenhet blant medlemmene, ved at det var et lukket forum. En av informantene presiserte at store deler av første dagen gikk til at medlemmene presenterte, og diskusjoner. Informantene presenterte dette som en av de viktigste faktorene for den vellykkede erfaringsdelingen som foregikk på arrangementene. De fleste informantene mente FSK sitt mandat og formål ble oppfylt på en god måte, og var svært fornøyd med dagens praksis. Det ble ansett som særlig interessant og verdifullt å høre på andre selskaper presentere om hvordan de for eksempel hadde håndtert hendelser. Utover å avholde konferanser, mente

informantene at FSK var en viktig bidragsyter i tilretteleggelsen og opprettholdelsen av en uformell kontakt mellom medlemmene.

5.5.2 Uformell kontakt mellom nettselskaper

Samlet viser funnene at samarbeidsorganisasjonene fungerte som fasilitator for både formell og uformell kontakt blant deres medlemmer. Ved å delta på arrangementer i regi av samarbeidsorganisasjonene, fortalte informantene fra nettselskapene at de utviklet relasjoner på tvers av selskaper. Syv av åtte nettselskaper sa de hadde kontaktet eller hadde blitt kontaktet av andre nettselskaper om IKT-sikkerhet i en uformell setting. Flere nevnte det var svært nyttig å ha uformelle kontakter for å høre andre sine erfaringer med hvordan de håndterte typiske felles problemstillinger. Dette var relasjoner som de kunne bruke til uformell kontakt utenom arrangementene, og ble ansett som en attraktiv mulighet å snakke med personer som hadde samme eller liknende rolle. Informanten fra det eksterne selskapet underbygget informantene fra nettselskapene sine refleksjoner rundt uformell deling.

> *En ting vi gjør er å passe på og bygge nettverk med personer som har samme rolle. Jeg snakker jevnlig med de som er CISO i [navn på selskaper], og vi passer på å ha korte veier til hverandre og ha jevnlige møter for å dele erfaringer. Når du gjør det, så har du etablerte kanaler for å dele når det er noe som dukker opp eller hvis du får noen spørsmål. Det er en form for uformell kommunikasjon* (CISO, eksternt selskap).

Den uformelle kontakten utenom arrangementene var basert på personlig initiativ, og opplevelsen av utbyttet de ila aktiviteten. Initiativ og utbytte var varierende, men den generelle oppfatningen hos nettselskapene var at uformell deling var viktig for å kunne lære av hverandre, gjennom å stille spørsmål til kjente kollegaer i bransjen ved behov.

> *Jeg kjenner folk her og der, og de prater jeg med og vi deler litt informasjon. Hvis de har funnet noe, så sier de ifra til meg. Hvis jeg har funnet noe, så sier jeg ifra til dem* (Seksjonssjef og IKT-sikkerhetskoordinator).

Uformell deling kan dermed foregå på selskapene sine premisser. Terskelen for denne type erfaringsdelingsdeling ble omtalt som svært lav. I flere tilfeller fortalte informantene at de heller tok kontakt med andre nettselskaper på en uformell måte, enn å stille spørsmål i for eksempel KraftCERT sitt chatforum.

5.5.3 Ulik erfaringsdeling blant nettselskaper

Det var en overordnet enighet blant elleve av informantene om at alle nettselskaper var flinke til å dele erfaringer med hverandre. Selv om kun noen få av informantene hadde opplevd cyberangrep av større betydning eller konsekvens mot deres nettselskap, uttalte flertallet at de fortsatt delte relevante erfaringer knyttet til det de beskrev som forsøk på cyberangrep eller angrep av mindre betydning

I intervjuene kom det fram at noen nettselskaper naturligvis opplevde flere cyberangrep enn andre, og selskapets størrelse spilte en rolle i denne sammenhengen. Ifølge noen av informantene var de små nettselskapene ofte det svakeste leddet på grunn av begrenset kapasitet eller kunnskap om IKT-sikkerhet, og dermed var de mer sårbare for cyberangrep. En annen informant påpekte samtidig at mindre nettselskaper ennå ikke hadde blitt rammet av større cyberangrep. I forlengelse av dette ble det fremhevet at store nettselskaper var mer attraktive for trusselaktører som ønsket å ramme strømforsyningen. Av den grunn ble det forklart at det var mulig at de større nettselskapene hadde mer informasjon og flere erfaringer å dele om cyberangrep. Samtidig var det en generell opplevelse av at alle var relativt transparente med hverandre om hendelsene og problemstillinger selskapene stod overfor.

> *Jeg har vært tydelig på at hvis vi får en hendelse er det ikke noe vits i å grave det ned og ikke fortelle om det. Det kommer bare til å møte oss igjen senere, så vi må prøve å eie det. Eie kommunikasjonen og historien selv* (CISO).

Dette samsvarte med flere av de andre informantene sine tankeganger. Et annet poeng som tydeliggjorde hvem som ønsket å dele erfaringer, var om ansatte fra selskaper valgte å delta på arrangementer i regi av samarbeidsorganisasjonene. En informant sa at dette fortalte indirekte om selskapene hadde et ønske om åpenhet og erfaringsdeling.

Uavhengig av hvem som delte, viser samlede funn at det mest optimale var å fortelle om hele hendelsesforløpet. Det inkluderte først informasjon om trusselaktørene. Tre av informantene mente det var nyttig å vite hva som gjorde at de lykkes med angrepet, hvem man trodde stod bak, og mulige motiv for angrepet. Ifølge dokumentanalysen hadde trusselaktører en evne til å tilpasse seg og rask utvikle nye angrepsmetoder (NSM, 2023), men det var fortsatt interessant for flere av informantene i få kunnskap om metoder de tidligere hadde brukt. I tillegg var det

nyttig for flere informanter å vite hvordan angrepet ble oppdaget, hva som skjedde underveis, konsekvensene, og hvordan ble det håndtert.

5.6 Utfordringer tilknyttet erfaringsdeling etter cyberangrep

Det har blitt trukket frem flere utfordringer blant informantene knyttet til erfaringsdeling etter cyberangrep. Først vil det fremlegges funn av utfordringer i samarbeidsorganisasjonene, før generelle utfordringer for bransjen presenteres.

5.6.1 Utfordringer i samarbeidsorganisasjoner

Selv om de fleste informantene var relativt fornøyde med hvordan erfaringsdeling i samarbeidsorganisasjonene fungerte, ble det nevnt flere utfordringer knyttet til dagens arenaer for erfaringsdeling i bransjen. Flere av informanter fra nettselskapene mente for eksempel at bransjen måtte passe på at det ikke ble for mange samarbeidsorganisasjoner. Det var enighet de hadde et ønske om å samarbeide og dele erfaringer, men at det kunne bli for mange arenaer å samarbeide på.

> *FSK er et veldig godt fora. Og så har man Fornybar Norge som prøver å gjøre noe av det samme, så blir det smør på flesk. Det blir litt for likt FSK sitt form, og da tror jeg at medlemmene i stor grad føler; «Ah, må vi gjøre det samme der også?». Det blir litt for mye av det samme* (IKT-sikkerhetskoordinator).

Hvis det ble opprettet enda flere samarbeidsorganisasjoner, sa den siterte informanten at de måtte velge hvilke arrangementer de skulle delta på. Ifølge en av de andre informantene fra nettselskapene burde nye behov og problemstillinger derfor tilpasses og videreutvikles i de eksisterende samarbeidsorganisasjonene. Videre sa informanten at det optimale var at alle deltok på det samme, og det ville ivareta samarbeid og erfaringsdeling på best mulig måte. Dette støttes av en tredje informant fra nettselskapene som mente man kunne miste litt fokus i samarbeidsorganisasjonene man allerede var en del av, hvis det hele tiden ble skapt nye arenaer for deling. Det kan i den forbindelse vises til teori om komplekse systemer. Flere samarbeidsorganisasjoner kunne blitt beskrevet som å øke kompleksitet i kraftbransjen (Perrow, 1999).

En annen utfordring trukket frem ved flere samarbeidsorganisasjoner, var selve volumet av informasjon. Flere av informantene fra nettselskapene sa de ikke fant frem til den

informasjonen de trengte, fordi det rett og slett var «information overload». Dette ble beskrevet som et av de største utfordringene bransjen stod overfor. For mye informasjon kunne være overveldende, selv for selskaper med godt utviklede sikkerhetsteam. Funn i oppgaven peker på de samme problemstillingene som ble presentert i tidligere forskning, hvor selve volumet av informasjon ble sett som en utfordring for utbytte man hadde av informasjonsdeling (Gjesvik, 2019). Det ble videre forklart at denne informasjonen kunne være overlappende. Dette ble spesielt trukket frem som en utfordring for de større selskapene, da de ofte var klar over mye som ble tatt opp på arrangementene.

Det ble også trukket fram utfordringer direkte tilknyttet KraftCERT. Ifølge to informanter hadde KraftCERT et forbedringspotensial når det gjaldt å dele relevant informasjon og erfaringer. De skulle ønske de fikk tilsendt mer informasjon som i mye større grad var relevant for dem. I tillegg nevnte informantene at det var behov for at KraftCERT var mer detaljerte i deres deling for at det skulle være nyttig for dem. Ofte hadde de ikke nok informasjon om detaljene i et angrep til å få best mulig utbytte av erfaringsdelingen i ettertid av hendelsen. Informasjon delt gjennom samarbeidsorganisasjoner ble dermed både beskrevet som å være for overveldende, og for lite detaljert, noen som tilsier en noe ulik mening blant informantene. Informasjonen som gikk gjennom KraftCERT ble videre anonymisert før den ble sendt ut til andre i bransjen. Basert på dette beskrev en av informantene fra nettselskapene KraftCERT som en «propp» for informasjonsdeling. Ulempen med denne praksisen var ifølge informanten at selskapene ikke fikk anledning til å stille oppfølgingsspørsmål direkte til selskapet som hadde blitt utsatt for et angrep. Det ble ansett som en tungvint løsning. En av informantene fra samarbeidsorganisasjonene påstod derimot at selskapene ikke var interessert i å vite hvem som hadde blitt truffet av et angrep, men bare hva de hadde blitt truffet av. Det tilsier en noe ulik vurdering rundt betydningen av å vite hvem som har opplevd hendelsen blant informantene.

5.6.2 Mangel på cyberangrep av betydning

En av de største utfordringene for erfaringsdeling etter cyberangrep i bransjen var at det ikke hadde skjedd mange alvorlige cyberangrep mot nettselskapene, og heller ingen som hadde ført til avbrudd i kraftforsyningen. Dette funnet understøttes av lignende funn fra flere av dokumentene (NSR, 2022; Tøien et al., 2021). En av samarbeidsorganisasjonene sa deres medlemmer var forberedt på større angrep, men at det lot vente på seg. Flere av informantene fra nettselskapene forventet også mer aktivitet i cyberdomenet i deres retning, etter krigen i

Ukraina brøt ut, og var enige om at trusselen fra statlige aktører var større de senere årene enn hva det var før. Alt tatt i betraktning hadde de ikke sett en økning fra denne typen trusselaktører, slik de muligens hadde forventet.

> *Den største utfordringen vil jeg si er mangel på cyberangrep. På grunn av dette er det ikke mange nevneverdige hendelser å utveksle erfaringer om* (IKT-sikkerhetskoordinator).

Selskapene ble utsatt for «vanlige» angrep, men det var svært få som hadde konkrete eksempler på angrep som hadde hatt en konsekvens, eller som har vært av nevneverdig omfang. «Vanlige angrep» ble brukt om phishing-mail og opportunistiske trusselaktører som skannet systemer i håp om å finne sårbarheter. Samtlige av informantene fra nettselskapene sa at de ble utsatt for denne typen angrep «hele tiden», noen opptil flere millioner ganger om dagen. Det meste ble stoppet av brannmurer og andre tekniske forsvarsmekanismer, og informantene fra nettselskapene var stort sett enig i at slike former for angrep ikke var verdt å rapportere videre.

> *Mange sier «vi har flere millioner angrep om dagen», men det har du fordi du er på internett, noen vil alltid prøve på ett eller annet. Det er jo et stykke vekk fra å få alvorlig hendelser* (CISO).

> *Hadde vi blitt utsatt for noe, så hadde vi nok delt informasjonen, men det er vanskelig å si på forhånd. Det er heller ikke et område i forbereder oss på. Vi forbereder oss ikke på deling av informasjon etter et cyberangrep. Hjernen vår klarer ikke helt å forholde seg til et hypotetisk angrep. Vi vil jo helst at det ikke skal skje. Det blir en kognitiv dissonans inn i bildet. I en hektisk hverdag er det ikke prioritert å lage en prosedyre for erfaringsdeling ved cyberangrep.* (Leder for informasjonssikkerhet).

Noen informanter sa at de håpet at de ville dele informasjon tidlig, og at det kunne hjelpe andre nettselskaper. Fem av de andre informantene fortalte at mangelen på nevneverdige cyberangrep gjorde det vanskelig å si noe om hvordan de hadde reagert om de ble utsatt for et angrep som hadde ført til konsekvenser, og hvordan man ville delt informasjonen videre med andre. Mangelen på store angrep gjorde det derfor utfordrende for nettselskapene å si om erfaringsdeling skjedde på en optimal måte i bransjen.

5.6.3 Menneskelige utfordringer

Menneskelige faktorer som skam og redsel ble trukket fram som viktig for hvor mye selskapene valgte å dele etter en hendelse. Cyberangrep var et område som opplevdes av informantene som litt «touchy», noe som betydde at det var et tema som mange synes det var vanskelig å snakke om. Flere av informantene var enige om at det kunne sitte langt inne for selskapene å dele etter cyberangrep, og at det eksisterte en tendens for å holde igjen detaljer og skjule informasjon. En fra samarbeidsorganisasjonene strakk seg så langt som å omtale det å dele erfaringer etter cyberangrep som tabu. Informanten forklarte hvordan det hadde vært flere hendelser blant medlemmene i organisasjonen, men svært få av disse hadde blitt delt videre til de andre medlemmene.

> *Jeg tror de som ikke deler, som oftest, ikke gjør det fordi de enten er redd for å fremstå som dumme, eller fordi de er redd for å bli sårbare ved å dele* (Leder i samarbeidsorganisasjon).

Funnene i oppgaven underbygger dermed det Aakre (2020) tidligere fant om at erfaringsdeling etter cyberangrep krevde en villighet til å dele og utgi seg på en måte som ikke alltid oppfattes som ønskelig. Basert på oppgavens funn er skam og redsel identifisert som to viktige faktorer som spilte inn i nettselskapers avgjørelse om å dele erfaringer eller ikke.

5.6.3.1 Skam tilknyttet svakheter i egen IKT-sikkerhet

Flere av informantene beskrev det å bli rammet et cyberangrep som skambelagt. Det ble ofte forbundet med at man hadde svakheter i egen sikkerhet. Selv om nettselskapene var monopolister, og ikke konkurrenter, ønsket de å unngå og sette egen integritet og omdømme i fare. Informantene uttrykte at dette gjaldt spesielt i situasjoner hvor de var usikre på om det var deres egne feil som førte til et angrep. I slike instanser var det ikke lett for informantene å fortelle om en hendelse.

> *Erfaringsdeling kan av og til sitte litt langt inne, spesielt hvis en selv føler at en blir tatt på sengen, gjorde noe galt, ikke var oppmerksom nok, eller gjorde feil i*

> *håndteringen. Det er alltid en eller annen grunn til å begynne å stille spørsmål ved seg selv* (IKT-sikkerhetskoordinator).

En av informantene fra samarbeidsorganisasjonene mente grunnen til at selskaper delte åpent, var hvis de ble «tatt med buksen nede». Dette viser at informanter fra både nettselskaper og samarbeidsorganisasjoner hadde samme inntrykk av skamfølelsen rundt å bli angrepet, og begge parter mente det skulle mye til før et selskap delte åpent om sine erfaringer. Spesielt hvis det involverte å synliggjøre egne svakheter.

5.6.3.2 Redsel for utnyttelse av delte erfaringer

Det fremstod som svært viktig for selskapene å dekke egne sikkerhetshull og ha kontroll på en hendelse før erfaringer ble delt videre til andre selskaper. En av informantene fra samarbeidsorganisasjonene forklarte at før et gitt tidspunkt kunne en faktisk ikke dele noe, i frykt for at inngangen fortsatt stod åpen for inntrengere. Funn i dokumentanalysen underbygger dette. Åpen deling av informasjon ble trukket frem som ønskelig, men ble beskrevet som vanskelig siden deling også burde skje på en så sikker måte som mulig (NSM, 2023). Oppgavens funn samsvarer dermed med utfordringer for informasjonsdeling funnet i tidligere forskning, hvor aktører ble beskrevet som redde for hvordan informasjon delt med andre kunne brukes av trusselaktører (Aakre, 2020).

> *Når man går ut med informasjon blant nettselskaper, så må man nesten anta at den blir offentlig. Angripere kan dermed dra nytte av informasjonen som kommer ut. Når du går ut med informasjon om det du vet, så går du også ut med informasjon om det du ikke vet om hendelsen. Det er nok også en årsak til at det er litt tilbakehold* (IKT-sikkerhetskoordinator).

Som nevnt i *5.4.2 Tillit mellom nettselskapene*, legger kraftberedskapsforskriften og KBO-ordningen til rette for deling av kraftsensitiv informasjon mellom selskaper. Imidlertid forklarte fem av informantene fra nettselskapene at deling av kraftsensitiv informasjon ofte ble holdt igjen til de hadde en viss oversikt over cyberangrepet. Flere av informantene ga utrykk for at regelverket ikke stoppet informasjon fra å lekke ut til allmennheten. Når det skjedde, kunne den også være tilgjengelig for trusselaktører. Flere av informantene sa at det i perioden under og etter et angrep måtte gjøres en vurdering av hvilke informasjon som kunne gjøre større skade og hva som var trygt å dele. Ifølge Kraftberedskapsforskriften (2012, § 6-1)

må det på dette tidspunktet gjøres en avveining på hva det er «tjenstlig behov» for å dele med andre selskaper. Tre av informantene opplevde denne avveiningen som noe vanskelig.

Dette understøttes av funn gjort i dokumentanalysen, hvor det ble forklart at deling av informasjon måtte praktiseres på en slik måte at bestemmelser knyttet til kraftsensitiv informasjon ble ivaretatt, og fordelene ved å dele måtte vurderes opp mot mulige negative konsekvenser (Meld. St. 38 (2016-2017)). Selskaper avventet også med å dele fordi de ønsket å løse problemet internt før de delte informasjon videre (Riksrevisjonen, 2021). Det ville, ifølge en informant, aldri kunne lages en mal for hva man burde dele når, ettersom hvert angrep var ulikt det forrige. Det måtte derfor alltid skje en vurdering av hva som kunne deles når et nytt angrep oppstod. På grunn av dette tok det ofte lang tid før andre nettselskaper fikk tilgang til informasjon som kunne vært viktig for å sikre egne systemer.

> *Vi bekrefter at «det er en hendelse», men man vil ikke gå ut med mer enn det. Det som er utfordrende med sånne hendelser er at vi ofte trenger litt tid for å skjønne hva som har skjedd, så må vi får undersøkt litt nærmere internt og så kan du begynne å dele. Så dette kommer ganske langt etterpå* (CISO).

> *De andre selskapene som er KBO-er, har en selvstendig plikt til å holde taushet om den informasjon som tilhører oss og som de eventuelt skulle fått tilgang til. Det er ikke som å dele informasjon med hvem som helst. Det er nok større rom for det, men vi er veldig forsiktig med å dele intern informasjon* (Leder for informasjonssikkerhet).

En informant fra organisasjonene sa man skulle dele under hele hendelsesforløpet, men hva man delte var avhengig av hva som var et fornuftig tidspunkt. Målet var å dele så mye som mulig, og å dele fortløpende under en hendelse, men det var utfordrende å bestemme seg for hva en burde dele når. Dette underbygget en informant ved å si at man ikke kunne dele for mye informasjon, men heller ikke så lite at det ikke hadde noe verdi. Hvis informasjonen som ble delt var for generell, kunne det være vanskelig å få utbytte av informasjonen. Gjennom dokumentanalysen ble det likevel tydelig at rask informasjonsdeling var nødvendig for å opprettholde god IKT-sikkerhet (NSM, 2023: NSR, 2022).

> *Det er nyttig å dele, og å dele tidlig* (Rådgiver for digitalisering og informasjonssikkerhet i samarbeidsorganisasjon).

Å få informasjon til rett tid var avgjørende for at selskapene skulle kunne forebygge, avdekke og håndtere digitale hendelser, og for at de skulle ha et riktig situasjonsbilde (Meld. St. 38 (2016-2017)). Tidlig deteksjon kunne i beste fall redusere eller fjerne konsekvensene av et angrep (NSR, 2022). Sitatet viser at informantene trakk fram tidlige deling som svært nyttig.

5.6.4 Gratispassasjerer i erfaringsdeling

I tidligere forskning ble gratispassasjerer presentert som et viktig begrep knyttet til informasjonsdeling i kritisk infrastruktur (Hausken, 2007). Relateres dette til funn i dataene, var noen av informantene sin motivasjon for å delta i forum for erfaringsdeling bygget på et ønske om å styrke eget selskap, ikke å bidra til å styrke andre. På grunn av dette kunne flere av informantene fra nettselskapene klassifiseres som «gratispassasjerer».

> *Man blir jo litt egoistisk. Man knytter bånd til andre for å dra nytte av det, og ikke for å være en hjelper som støtter andre* (Leder for informasjonssikkerhet).

> *Man redder seg selv, før man redder andre* (Leder for IT-sikkerhet og beredskap i samarbeidsorganisasjon).

Selv om nettselskapene var monopolvirksomheter og ikke stod i direkte konkurranse med hverandre, brukte de flere av de samme leverandørene og systemene. Ifølge en informant fra en samarbeidsorganisasjon hadde et av deres medlemmer uttalt at hvis de fant en sårbarhet hos en leverandør, var det ikke helt rett frem for de å dele den kunnskapen som de hadde investert penger i. Da ville andre få denne informasjonen gratis. Informanten trodde ikke at dette var en gjennomgående utfordring med erfaringsdeling, men fortalte at dette var en problemstilling personen hadde hørt som var knyttet til det å dele. Informanten beskrev det som at en først redder seg selv, før en redder andre.

5.6.5 Erfaringsdeling som et overskuddsprosjekt

Flere av informantene i oppgaven beskrev erfaringsdeling som et overskuddsprosjekt. En av informantene sa at å være mer utadrettet og samarbeide for å lære, forsvant i en hektisk hverdag. Personen sa det muligens hang sammen med det at sikkerhet generelt hadde en tendens til å bli nedprioritert, «helt til det brant».

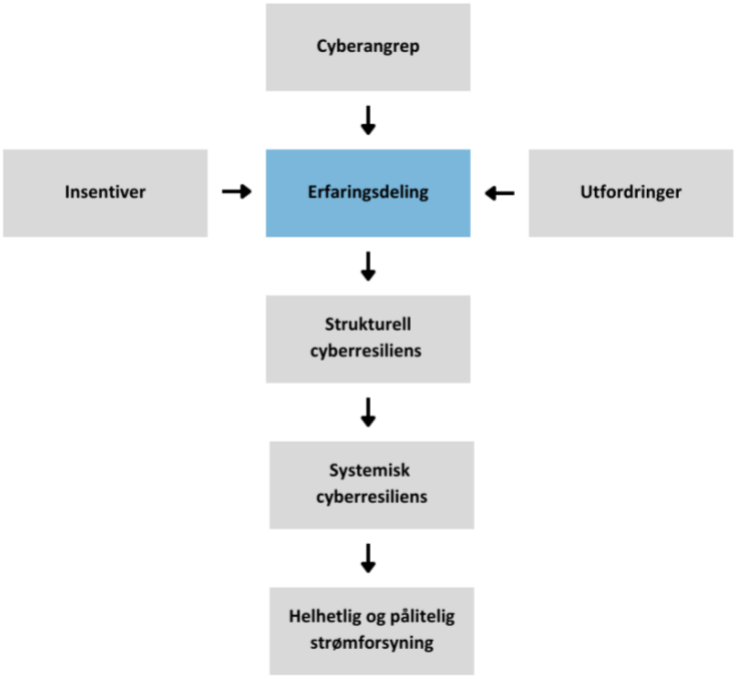
> *Mange har et ønske om å dele mer og samarbeide mer på tvers, og lære mer. Når det kommer til stykket, blir tiden knapp og man skyver på ting. Ofte ender det opp med lite eller ingenting. Det er ofte mange gode intensjoner som ikke blir til noe* (IKT-sikkerhetskoordinator).
>
> *Det blir igjen et overskuddsprosjekt som man gjør i tillegg til å drifte eget selskap* (Leder for informasjonssikkerhet).

Disse utsagnene ble støttet opp av flere andre informanter som forklarte at det var ressurser og tiden man hadde som i størst grad begrenset erfaringsdeling. Mange av informantene fra selskapene pratet mye sammen på felles fagdager i regi av samarbeidsorganisasjonene og ønsket å fortsette dette i etterkant, men hadde travle hverdager som hindret videre kommunikasjon. Ressurser i selskapene varierte også i stor grad, og de selskapene som hadde færrest ressurser knyttet til IKT-sikkerhet ble «slukt» av det daglige arbeidet når de var tilbake på arbeidsplassen. Dette ble også nevnt i forbindelse med felles chatplattformer i samarbeidsorganisasjonene. En informant forklarte at i en travel hverdag var det få som gikk inn for å se om det var noen spørsmål fra andre en kunne besvare, eller se om noen trenger hjelp. Det satt ofte litt lenger inne når man hadde mye å gjøre.

6 Drøfting

Oppgavens funn viser at det har blitt større oppmerksomhet på IKT-sikkerhet i kraftbransjen, som respons på økende cyberangrep i de senere årene. Informantene var enige om at det ikke var mulig å beskytte seg mot alle cyberangrep, og resiliens som både begrep og

arbeidsmetode har derfor blitt mer anerkjent. Åpenhet blant aktørene har også vært i utvikling, og det oppleves i dag som mer akseptert å dele erfaringer. Erfaringsdeling har derav blitt en etablert praksis. Samarbeidsorganisasjoner, også omtalt som praksisfelleskap (Wenger et al. 2002), tilrettelegger for erfaringsdeling, og knytter personer og selskaper i bransjen tettere sammen. Informanter trakk frem tre hovedinsentiver for å dele erfaringer etter et cyberangrep. I tillegg knyttet informanter en rekke utfordringer til erfaringsdeling, både knyttet til praksisfelleskapene og på et generelt grunnlag. I dette kapittelet vil presenterte funn drøftes for å svare på oppgavens problemstilling: *Hvordan kan erfaringsdeling mellom nettselskaper etter cyberangrep bidra til økt cyberresiliens for å sikre norsk strømforsyning?*



Figur 4: Sammenheng mellom oppgavens temaer, med utgangspunkt i resiliensnivåene til Macrae (2019)

Det vil være nyttig å se tilbake til figuren som ble presentert i *1.3.1 Sammenheng mellom oppgavens temaer*. I lys av teorikapittelet er det utviklet en ny versjon av figur 1. Cyberresiliens er en videreutvikling av resiliensbegrepet, og blir i den forbindelse sammenkoblet med til Macrae (2019) i drøftingen. Resiliens på selskapsnivå er byttet ut med strukturell cyberresiliens, og resiliens på bransjenivå er byttet ut med systemisk cyberresiliens. I dette kapittelet vil det tas utgangspunkt i de nye begrepene introdusert i figur 4.

6.1 F1: Hvilke insentiver og utfordringer knytter nettselskaper til erfaringsdeling etter cyberangrep, og hvordan påvirker disse faktorene erfaringsdeling mellom nettselskaper?

I tidligere forskning ble gjensidig utbytte, tillit og delt forståelse trukket frem som de viktigste insentivene for at aktører skulle dele informasjon med hverandre (Atkins & Lawson, 2020; Bodsberg et al., 2018; Gjesvik, 2019). Vi fant de samme insentivene hos informantene i oppgaven, men også tre underinsentiv til gjensidig utbytte; bevisstgjøring, felles utfordringer og forankring. I tillegg ble det identifisert flere utfordringer til hvert insentiv. Utfordringene sammenfaller i noen grad med utfordringer presentert i tidligere forskning, men det er videre identifisert ytterligere utfordringer for erfaringsdeling blant nettselselskapene. For å besvare oppgavens problemstilling, vil det først være nødvendig å diskutere hvordan insentivene påvirker erfaringsdeling mellom nettselskapene i lys av utfordringene. Ved å gjøre dette kan vi forklare hvordan insentivene og utfordringene påvirker erfaringsdelingen mellom nettselskapene, som presentert i figuren ovenfor.

6.1.1 Gjensidig utbytte og tilknyttede utfordringer

Basert på oppgavens funn kan det virke som at felles problemstillinger var den faktoren som bidro mest til nettselskapenes opplevelse av gjensidig utbytte av erfaringsdeling. Dette skyldtes at informantene opplevde delte erfaringer om felles problemstillinger som mest relevant og handlingsdyktig for eget selskap. Siden nettselskapene stod overfor mange av de samme problemstillingene, i form av felles leverandører, systemer og trusselaktører, hadde de innsikt i hva andre nettselskaper ville hatt utbytte av å vite etter et cyberangrep. Dette samsvarer med funn fra Gjesvik (2019), som fant at informasjonen som deles blant aktører i kritisk infrastruktur må gi merverdi om informasjonsdeling skulle oppleves som noe som ga gjensidig utbytte.

Gjennom bevisstgjøring ble selskapene opplyst om hvilke felles utfordringer de stod overfor, og kunne på denne måten lære av hverandre. Direkte kommunikasjon ble trukket frem som et effektivt virkemiddel for å skape bevisstgjøring. Informantene synes det var spennende å lære av hverandres erfaringer, og bevisstgjøring og læring henger således nøye sammen. Måten nettselskapene lærte av hverandre gjennom praksisfelleskap kan kobles til sosialiseringsfasen og abstrakt konseptualisering i læringssirkelen (Kolb, 2015; Nonaka & Takeuchi, 1995). Dette steget kan sammenlignes med hvordan nettselskaper holder foredrag for hverandre i

regi av praksisfelleskap de er medlem i. Eksternaliseringsfasen kan brukes om diskusjoner og uformell kontakt i etterkant av nettselskapers foredrag om erfaringer. Både sosialisering, abstrakt konseptualisering og eksternalisering beskriver øyeblikk med direkte kommunikasjon mellom nettselskaper hvor bevisstgjøring oppstår.

For at bevisstgjøring om felles utfordringer skal gi gjensidig utbytte, er det videre sentralt at nettselskaper evner å forankre erfaringer i sitt eget selskap. Å forankre lærdom gjennom erfaringsdeling skjer i kombineringsfasen, og internaliseringsfasen og aktiv eksperimentering (Kolb, 2015; Nonake & Takeuchi, 1995). I disse stegene tas delte erfaringer med tilbake til eget selskap, og det vurderes om det er behov for å implementere nye tiltak basert på den nye kunnskapen. De tre virkemidlene for gjensidig utbytte henger således nøye sammen, ettersom bevisstgjøring knyttet til felles utfordringer kan føre til forankring i eget selskap.

Likevel viser funnene flere utfordringer som svekket følelsen nettselskapene hadde av gjensidig utbytte. Delte erfaringer og informasjon ble både beskrevet som å være noe overveldende og lite detaljert. Det eksisterte dermed ulike meninger blant informantene rundt delte erfaringer gjennom praksisfelleskap. Begge forståelsene kan argumenteres som svekkende for opplevelsen av utbytte. Det var også delte meninger om antallet samarbeidsarenaer i bransjen. På den ene siden mente flere informanter at de ville fått mer relevant informasjon hvis bransjen ble delt opp etter for eksempel størrelse eller interesseområde. På den andre siden mente andre informanter at alle nettselskapene burde være samlet for å ivareta et helhetlig samarbeid. Noen av informantene fryktet at flere samarbeidsarenaer kunne bety større splittelse blant nettselskapene. Det ideelle var at alle deltok på de samme arrangementene. Det er vanskelig å fastslå hvilken løsning som ville ført til mer deling mellom nettselskapene, men basert på funnene ser det ut som at dagens praksis generelt sett bidrar til deling mellom nettselskapene. Det er på bakgrunn av at ingen informanter uttrykte at ulik størrelse, interesseområde eller organisering av bransjen hindret dem i å dele erfaringer med hverandre.

For å oppleve gjensidig utbytte av erfaringsdeling etter cyberangrep er det imidlertid nødvendig med cyberangrep å dele erfaringer om. Mangelen på angrep gjorde det vanskelig for informantene å si noe om hvordan de hadde reagert og hvordan de ville delt erfaringer etter cyberangrep av betydning, slik informantene beskrev det. Det kan derimot argumenteres for at det er mulig å deles verdifulle erfaringer etter forsøk på cyberangrep eller cyberangrep

av mindre betydning. Det kan gjelde indikatorer, angrepsmetoder, trusselaktører, sårbarheter og barrierer. På denne måten kan erfaringsdeling etter cyberangrep føre til gjensidig utbytte, selv om cyberangrep ikke har vært suksessfullt. Drøftingen av insentivene og utfordringer tyder på at det eksisterer en praksis rundt erfaringsdeling som gir gjensidig utbytte blant nettselskapene.

6.1.2 Tillit og tilknyttede utfordringer

Tillit er et andre insentivet som ble sett som bidragsytende for erfaringsdeling. Gjesvik (2019) skiller mellom to ulike typer tillit; tillit mellom individer og tillit mellom selskaper. Bodsberg et al. (2018) fremhever også tillit gjennom personlige nettverk som et viktig punkt for å kunne dele informasjon. Ifølge informantene var tillit helt nødvendig for at de skulle føle åpenhet og dermed være villige til å dele erfaringer. Å forme bekjentskap og knytte kontakter i bransjen ble presentert som sentralt. Dette tyder på en sterk vektlegging av individuell tillit mellom informantene. Samtidig kan det tenkes at tillit mellom individer er basert på en gjensidig tillit mellom nettselskapene de er ansatt i. Personer som jobber med IKT-sikkerhet i et nettselskap stoler som oftest på individer fra andre nettselskaper, basert på en generell tillit til at andre nettselskaper har de samme intensjonene som sitt eget selskap. Dette kan for eksempel være å bedre IKT-sikkerhet.

Tillit til praksisfelleskap virket å være godt etablert blant nettselskapene. For eksempel anonymiserer KraftCERT informasjon de mottar før de deler den videre. Dette betyr at nettselskapene kunne være trygge på at det ikke ville bli offentlig kjent hvem som hadde opplevd et cyberangrep. Gjennom KraftCERT sin ordning ville det heller ikke bli kjent hvis det hadde oppstått menneskelige feil, om selskapene hadde åpne sårbarheter, eller om de håndterte angrepet på en dårlig måte. Dette kan ha vært et insentiv for nettselskapene til å dele erfaringer med KraftCERT. På samme måte kan det samme prinsippet gjelde for erfaringsdeling mellom medlemmene i FSK. FSK var lukket for alle utenforstående deler av konferansen, og det kan ha bidratt til at selskaper lettere delte erfaringer. Flere informanter støttet denne påstanden, og ordningen skapte tillit til organisasjonen og en tilsynelatende mer åpen arena for deling.

Samtidig var redsel for hvordan informasjon om et angrep kunne bli brukt mot et selskap en av utfordringene informantene knyttet til erfaringsdeling. Flere av nettselskapene hadde en tendens til å være tilbakeholdne med å dele kraftsensitiv informasjon, til tross for at

regelverket la til rette for at de kunne dele denne med andre KBO-enheter. De mente regelverket ikke stoppet informasjon fra å lekke ut til allmennheten. En av bekymringene var at slik informasjonen ville bli tilgjengelig for trusselaktører. På denne måten kan det argumenteres for at redsel henger sammen med tillit. Mangelen på tillit til at delt informasjon ville forbli konfidensiell blant de man delte med, skapte en følelse av redsel. Våre funn samsvarer dermed med funnene til Aakre (2020), som fant at aktører er redde for hvordan informasjon delt med andre kan brukes av trusselaktører.

Skam var en annen menneskelig utfordring for tillit, og representerte den usikkerheten et selskap hadde til egen skyld i et cyberangrep. Som nevnt opplevde flere av informantene at tillit økte gjennom at KraftCERT anonymiserte selskapene i deres deling etter et angrep. Likevel indikerer dette at virksomhetene ikke ønsket at andre skulle få kjennskap til at de hadde blitt utsatt for angrep, og eventuelt om de var ansvarlige for at angrepet fant sted på grunn av sårbarheter eller feil i deres egne systemer. Informantene var enige om at det var vanskelig for et selskap å dele åpent om sine erfaringer etter et angrep, spesielt hvis de kjente på skam knyttet til egen sikkerhet eller håndtering. Funnene viser videre at definisjonen på tillit, presentert i teorikapittelet, er krevende å oppnå, da den tar utgangspunkt i at aktører aksepterer sårbarheter basert på positive forventninger til andres intensjoner (Rousseau et al., 1998).

Skam og redsel i forbindelse med erfaringsdeling ble videre sett som hinder for at erfaringer kunne deles raskt i etterkant av et cyberangrep. Rask deling av informasjon blir omtalt som essensielt om trusler skal oppdages og håndteres (NSM, 2023: NSR, 2022, Rak, 2002). Å dele informasjon tidlig kan være fordelaktig fordi det gir andre selskaper muligheten til å dra nytte av den delte informasjonen. Samtidig kan det øke sårbarheten i det enkelte selskapets egne systemer. Ved å utsette delingen av informasjon kan et selskap sikre sine egne systemer mot nye angrep. Imidlertid kan dette samtidig føre til at alvorlige sårbarheter som påvirker flere selskaper i bransjen ikke blir belyst i tide. Alle nettselskaper står overfor en utfordring når det gjelder å vurdere avveiningen mellom økt cyberresiliens og økt sårbarhet. Dette dilemmaet kan være noe selskapene er bevisste om eller det kan være noe de håndterer uten å være fullstendig klar over det. For at nettselskaper skal kunne dele sine erfaringer med hverandre, er tillit til at informasjonen ikke spres og at de ikke blir dømt for feilene de har begått i forbindelse med et angrep, helt essensielt. Basert på en helhetlig vurdering av tillit og tilknyttede utfordringer, kan det argumenteres for en tilstrekkelig tillit mellom nettselskaper

og individer for deling av erfaringer. Det er også mulighet for forsterket tillit om det settes søkelys på utfordringene tilknyttet tillit mellom nettselskapene.

6.1.3 Delt forståelse og tilknyttede utfordringer

Det er ønskelig med forståelse blant nettselskaper på tre ulike områder; trusler, sårbarheter og verdier. De tre faktorene utgjør trefaktormodellen (NSM, POD & PST, 2015). Hvis nettselskapene oppnår en delt forståelse av faktorene, gir det mulighet til å se risikobildet i kraftbransjen som en helhet. Dette kan fungere som et insentiv for å dele erfaringer med hverandre.

Informantene i oppgaven delte en forståelse av felles trusselaktører og deres kapasitet og ressurser. Tidligere forskning viser at selskaper er mer åpne for samarbeid og informasjonsdeling med hverandre hvis de har en opplevelse av trusler som truer et felles system de var en del av (Atkins & Lawson, 2021). Gjennom en delt forståelse av felles trusler kan det tenkes at nettselskapene ble mer åpne for å dele erfaringer med hverandre. Det kan skyldes en følelse av gjensidig utbytte blant selskapene, hvor indikatorer på trusselaktører og metoder ble trukket frem som spesielt nyttig å dele erfaringer om.

Selskaper må videre forstå sårbarheter i egne systemer for at deling skal finne sted (Rak, 2002). Flere av informantene uttrykte at det var gladelig deling mellom nettselskapene. Det kan derfor argumenteres for at delt forståelse blant selskapene førte til todelt deling, som er essensielt om deling skal ha ønsket effekt (Rak, 2002). I denne konteksten er ønsket effekt at nettselskapene bidrar til å beskytte strømforsyningen. Målet er å være proaktiv, og håndtere sårbarhetene før en angriper utnytter disse (Tøien et al., 2021).

Basert på funnene i oppgaven, virker det som at det var enighet blant flere av informantene at de betraktet sitt nettselskap som en del av et større system, og at dette systemet måtte beskyttes som en helhet. Det kan derfor være mulig å hevde at informantene hadde en delt forståelse av kraftbransjen som kritisk infrastruktur. Ettersom strømforsyning i kraftbransjen kan sees som en viktig verdi (NOU, 2006:6), burde erfaringsdeling i praksisfelleskap bygge på et ønske om å beskytte forsyningen av strøm mot eksterne trusselaktører. Nettselskapene hadde i forbindelse med dette en opplevelse av å stå overfor de samme trusselaktørene. De hadde søkelys på å identifisere sårbarheter i sine egne systemer, og en helhetlig forståelse av

kraftbransjen som kritisk infrastruktur. Dette underbygger ideen om at de innehadde en delt forståelse av hvilke trusler, sårbarheter og verdier som kraftbransjen står overfor.

Imidlertid viste funnene at det også eksisterte utfordringer ved delt forståelse av trusler, sårbarheter og verdier blant nettselskapene. Noen informanter så på egen deltakelse i erfaringsdeling som egoistisk, og etablerte kontakter for egen nytte, ikke for å hjelpe andre. Motivasjonen for å delta i praksisfelleskap var dermed å styrke eget nettselskap. Av den grunn kan det argumenteres for at delt forståelse ikke eksisterte hos alle informantene, og at noen av dem kunne klassifiseres som gratispassasjerer (Hausken, 2007). Dette kan ses i sammenheng med det faktum at erfaringsdeling ble beskrevet som et overskuddsprosjekt av flere informanter.

På den ene siden kan det stilles spørsmål ved om erfaringsdeling som et overskuddsprosjekt stammer fra en mangel på delt forståelse blant nettselskaper. Mangel på forståelse for hvordan erfaringsdeling kan bidra til både forbedret IKT-sikkerhet i eget selskap og beskyttelse av strømforsyningen kan føre til at erfaringsdeling blir nedprioritert i en travel hverdag. Uten å forstå de konkrete fordelene og betydningen av slik deling, kan det være vanskelig å se den langsiktige verdien av å investere tid og ressurser i denne aktiviteten. På den andre siden har IKT-sikkerhet tidligere vært et område med generelt mindre fokus i kraftbransjen, og nedprioritering av erfaringsdeling for å økt IKT-sikkerhet kan derfor være en konsekvens av dette. Erfaringsdeling etter cyberangrep er primært avhengig av et bredt fokus på IKT-sikkerhet i bransjen. Funnene viser samtidig at IKT-sikkerhet har blitt et sentralt fokusområde i løpet av de siste årene. Dette kan indikere at nettselskapene har utviklet en delt forståelse av deres ansvar i håndteringen av trusler, sårbarheter og verdier i kraftbransjen. Dette er et positivt tegn som tyder på økt bevissthet og engasjement blant nettselskapene. Dette kan med tiden føre til at erfaringsdeling ikke lenger oppleves som et overskuddsprosjekt i bransjen. På bakgrunn av diskusjonspunktene vurderes delt forståelse som det svakeste insentivet for erfaringsdeling mellom nettselskaper.

6.2 F2: Hvordan bidrar erfaringsdeling etter cyberangrep til å øke cyberresiliens i nettselskaper, og er cyberresiliens på selskapsnivå overførbart til cyberresiliens på bransjenivå?

Basert på drøftingen av de presenterte insentivene og utfordringene, vil det være mulig å diskutere hvordan erfaringsdeling etter cyberangrep kan bidra til å bygge strukturell cyberresiliens og hvorvidt det har overførbarhet til systemisk cyberresiliens. Figur 4 tydeliggjør hvilken posisjon erfaringsdeling har relatert til cyberresiliens, og hvordan det blir påvirket av insentiver og utfordringer. Overordnet viser funnene at kraftbransjen har innsett viktigheten av IKT-sikkerhet, samt en god modningsprosess i bransjen på relativt kort tid. Samtidig er det fortsatt et forbedringspotensial blant selskaper. Dette skaper en arena for videreutvikling av cyberresiliens i bransjen.

6.2.1 Strukturell cyberresiliens ved forankring av delte erfaringer

Funnene peker, først og fremst, på at erfaringsdeling kan bidra til å bygge strukturell cyberresiliens i nettselskaper. Basert på funnene er gjensidig utbytte et sterkt hovedinsentiv som ser ut til å være relativt godt etablert blant nettselskapene. Gjensidig utbytte innebærer blant annet at erfaringene som deles med andre nettselskaper blir omgjort til kunnskap, som deretter må forankres i selskapene (Kolb, 2015). Å forankre kunnskap basert på erfaringsdeling, kan dermed argumenteres for å være en stor bidragsyter til å bygge strukturell cyberresiliens. Forankring vil si å ta lærdom av et cyberangrep, omgjøre erfaringer til kunnskap, integrere kunnskapen med allerede eksisterende kunnskap, og eventuelt tilpasse eller iverksette cyberresiliente tiltak.

Forankring kan spesielt relateres til de to siste stegene i læringssirkelen, nemlig kombinering, og internalisering og aktiv eksperimentering (Kolb, 2015; Nonake & Takeuchi, 1995). Stegene innebærer både å se delte erfaringer i sammenheng med eksisterende kunnskap i selskapet, og å ta i bruk nye måter å arbeide på. Kombinering er i overensstemmelse med en informants utsagn om at det ikke nødvendigvis vil være gunstig å fortsette og bygge strukturell cyberresiliens for å bli sikrere og sikrere. Når nye erfaringer forankres i selskapet, må de heller ses i sammenheng med eksisterende kunnskap. Dette må gjøres for at iverksettelse av nye tiltak skal ha sin tiltenkte effekt. Hvis en ikke gjør dette kan de undergrave utbyttet nettselskapet har av erfaringsdeling, samt mulighet for bygging av strukturell cyberresiliens. Hvis nettselskaper derimot følger læringssirkelen (Kolb, 2015;

Nonake & Takeuchi, 1995), kan det ha stor betydning for selskapets evne til å forankre erfaringer for økt strukturell cyberresiliens.

Det er mulig å hevde det eksisterer et dilemma som utfordrer læringsaspektet i etterkant av cyberangrep. Det handler om hvorvidt det er oppnåelig å ta lærdom av cyberangrep som kontinuerlig foregår mot selskaper (NSM, 2023). Som en konsekvens av kontinuerlige cyberangrep, kan det være begrenset med tid og kapasitet til å dele og lære av erfaringer etter hvert enkelt angrep. Aktiv resiliens (Martin, 2019) og recovery resiliens (Pettersen & Schulman, 2016) er teoretiske bidrag på peker på læring etter hendelser som en essensiell faktor for å øke strukturell cyberresiliens. Denne formen for bygging av cyberresiliens gjennom læring av erfaringer, er også illustrert i læringssirkelen (Kolb, 2015; Nonaka & Takeuchi, 1995). Kontinuerlige cyberangrep kan begrense aktørene til å komme bare til det andre eller tredje steget i læringssirkelen, som involverer forståelse av hendelsen og deling av beskrivelser og refleksjoner med andre. Når et nytt cyberangrepet inntreffer, starter læringssirkelen på nytt, og nye erfaringer blir omdannet til kunnskap for å forsøke og forstå det nyoppståtte som har skjedd. Dette kan indikere at aktører og selskaper ofte befinner seg i de to til tre første stegene av sirkelen, og videre ikke får mulighet til å fullføre prosessen med erfaringsdeling og forankring i eget selskap. Det kan ha negativ betydning for erfaringsdeling mellom nettselskaper i etterkant av et cyberangrep, samt deres muligheter til å bygge strukturell cyberresiliens som følge av erfaringsdeling.

Samtidig viser flere funn at dette ikke nødvendigvis er en aktuell problemstilling for erfaringsdeling og læring blant nettselskapene i dag. Funnene viser at det har skjedd få cyberangrep av nevneverdig betydning mot nettselskapene. Et begrenset antall cyberangrep gir få muligheter til å dele og lære av erfaringer. I den forbindelse nevnte mange av informantene at cyberangrepet på Hydro i 2019 har vært gjentagende på konferanser og fagdager i kraftbransjen. Det kan skyldes en kombinasjon av deres vellykkede deling av informasjon underveis og deling av erfaringer i ettertid, og at det er et aktuelt cyberangrep å eksemplifisere med i kraftbransjen. Samlet tyder disse funnene på at nettselskap og samarbeidsorganisasjonene i dag kan fullføre læringssirkelen etter et cyberangrep. Som et resultat av å fullføre sirkelen, kan nettselskapene oppleve å få større utbytte av erfaringsdeling. Dette vil videre ha positiv betydning for bygging av strukturell cyberresiliens.

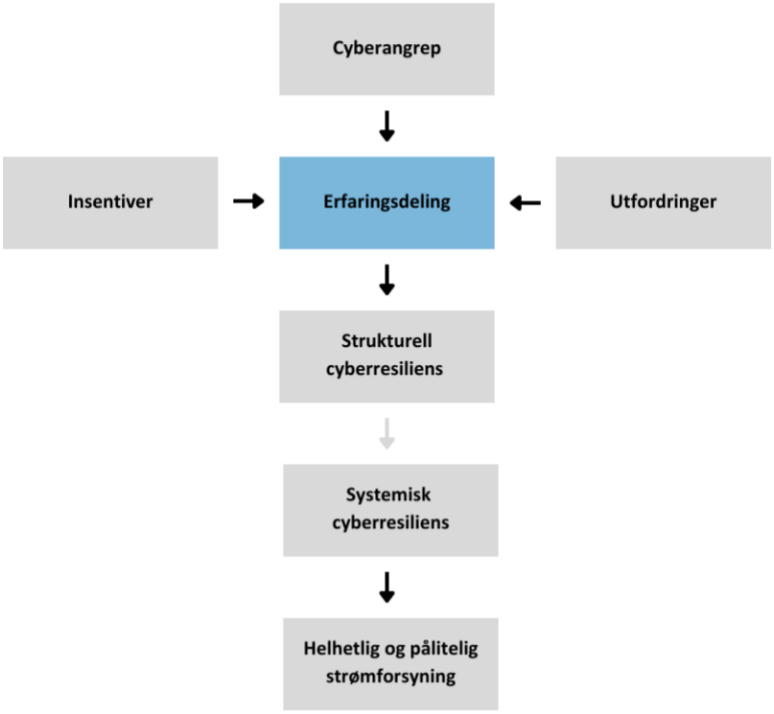
6.2.2 Strukturell cyberresiliens gjennom delt forståelse

Delt forståelse virker å ha betydning på hvordan nettselskaper kan bruke erfaringsdeling til å bygge strukturell cyberresiliens. Det er spesielt ett poeng som påvirker denne betydningen; informantenes varierende kjennskap til begrepet resiliens. For noen informanter var resiliens et ukjent begrep. Det vil være rimelig å argumentere for at det er grunnleggende å ha en delt forståelse av begrepet resiliens, for å kunne dra nytte av erfaringsdeling og øke cyberresiliens. En delt forståelse av begrepet kan legge et grunnlag for og styrke betydning av erfaringsdeling som element for å øke cyberresiliens i nettselskaper. Et av hovedargumentene som tilsier at cyberresiliens bør bli et mer innarbeidet begrep, er manglende ledelsesinvolvering i IKT-sikkerhetsarbeidet. Noen informanter ga uttrykk for at det var vanskelig å få ledelsen til å opparbeide en tilstrekkelig forståelse og kunnskap rundt IKT-sikkerhet, samt IKT-sikkerhetstiltak som burde iverksettes for å øke cyberresiliens. Hvis det er varierende eller manglende forståelse på ulike selskapsnivåer om hva cyberresiliens er og hvordan det kan oppnås, vil det gå på bekostning av både erfaringsdeling som bidragende praksis, og selskapets evne til å opparbeide strukturell cyberresiliens. Dette kan tolkes som en manglende delt forståelse av resiliens i IKT-sikkerhetsarbeidet, som er i strid med Leveson (2012) sin tilnærming om at selskaper må ha en helhetlig tilnærming til trusler og risikoer i komplekse systemer.

Samtidig opplevde flesteparten av informantene at resiliens var et innarbeidet begrep i deres nettselskap. Når begrepet ble forklart for de som opplevde resiliens som et fremmedord, påpekte de videre at det beskrev måten de arbeidet på i praksis. Hvis selskaper benytter felles terminologi og oppnår en delt forståelse av cyberresiliens, kan IKT-sikkerhetsarbeidet overordnet bli mer helhetlig og lettere å kommunisere på tvers av nivåer og avdelinger i selskapet. Det vil være i tråd med både Leveson (2012) som vektlegger en helhetlig tilnærming til trusler og risikoer, og første grunnprinsipp fra NSM (2020) som innebærer å ha en forståelse av selskapet som en helhet for å iverksette IKT-sikkerhetstiltak. Ledelsen blir i den sammenheng påpekt som sentrale. En felles forståelse av begrepet kan gjøre det enklere for informanter å forankre og iverksette nødvendige IKT-sikkerhetstiltak, som blir godkjent av ledelsen. Disse funnene tyder på at samtlige av nettselskapene i oppgaven har opparbeidet en form for strukturell cyberresiliens gjennom erfaringsdeling. Hvilken evne de har til å gjennomføre denne prosessen, kan ha betydning for overførbarheten til systemisk cyberresiliens.

6.2.3 Overførbarhet fra strukturell cyberresiliens til systemisk cyberresiliens

Overførbarheten mellom strukturell cyberresiliens og systemisk cyberresiliens kan diskuteres i lys av desentralisert og sentralisert styring (Macrae, 2019; Perrow, 1999). Basert på de ulike teoretiske bidragene, har det blitt utformet en ny versjon av figur 4. Figuren illustrer hvordan overførbarheten fra strukturell cyberresiliens i nettselskaper til systemisk cyberresiliens i kraftbransjen kan problematiseres.



Figur 5: Problematisering av overførbarheten fra strukturell cyberresiliens til systemisk cyberresiliens

Strukturell cyberresiliens kan relateres til desentralisering, og systemisk cyberresiliens til sentralisering. Kjernen i strukturell cyberresiliens og desentralisert styring sammenfaller ved at begge setter søkelys på ansvarsfordeling blant flere aktører for å håndtere risiko. I strukturell resiliens er aktiv gjennomgåelse av aktiviteter koordinert av flere enheter for å skape prosesser for omorganisering og vurdering av ressurser (Macrae, 2019). I desentralisert styring vektlegges fordeling mellom aktører, ettersom det sikrer en analyse av den uønskede hendelse og minimert konsekvensene, før en vurderer ulike alternative løsninger (Perrow, 1999). Begge teoriene har derav søkelys på kontinuerlig vurdering av risikohåndtering som er fordelt på ulike aktører. Strukturell cyberresiliens gjennom desentralisert styring kan beskrive hvordan nettselskaper i kraftbransjen overvåker sine IKT-systemene for cyberangrep, og analyserer eventuelle angrep og konsekvenser av disse. I ettertid av et angrep vil selskapene

implementere nye og bedre tiltak. Som tidligere forklart, gjør forankring av erfaringsdeling mellom nettselskapene dette mulig.

Det er videre nærliggende å se systemisk cyberresiliens i sammenheng med sentralisert styring (Perrow, 1999) Systemisk cyberresiliens og sentralisert styring samsvarer i deres søkelys på å ha en overordnet forståelse av et system. Beslutninger blir i sentralisert styring tatt av en konsistent sentral ledelse som har bestemmende kraft over endringer, allokering av ressurser og sikkerhetstiltak (Perrow, 1999). I systemisk cyberresiliens kan det være nødvendig med systemiske endringer, for eksempel i regelverk eller teknologi, for at systemet skal motstå og håndtere forstyrrelser på en bedre måte (Macrae, 2019). Således samsvarer sentralisert styring og systemisk resiliens i deres ønske om å forbedre et system ved å ha en helhetlig oversikt.

Forskjellen mellom sentralisert styring og systemisk resiliens ligger i hvem som har ansvaret for endringer. I sentralisert styring er det et ønske om at slike endringer skal gjøres av en sentral ledergruppe, mens i systemisk cyberresiliens kan avgjørelsene involvere mange aktører på ulike nivåer, og på tvers av en hel bransje. Det kan eksempelvis skje gjennom den nære tilknytningen mellom KBO-enhetene og NVE for å sikre IKT-sikkerhet i bransjen. På et lavere nivå finnes KBO-enhetene som er lovpålagt å gjøre endringer og justere tiltak og ressurser tilknyttet egen IKT-sikkerhet (Kraftberedskapsforskriften, 2012). På et overordnet nivå finnes NVE og systemansvarlig (Statnett), og de kan sammen betraktes som en sentral ledergruppe i kraftbransjen, kjent som kraftforsyningens sentrale ledelse (KSL) (Kraftberedskapsforskriften, 2012, § 2-1). Styring gjennom KSL kan dermed samsvare med sentralisert styring (Perrow, 1999). På grunn av at NVE har det overordnede ansvaret for KBO-enhetene, og det i tillegg foregår et tett samarbeid mellom NVE og KBO-enhetene om å sikre strømforsyning, kan vi finne tegn til systemisk cyberresiliens gjennom sentralisert styring i bransjen.

Perrow (1999) hevder styring av komplekse systemer ikke er mulig, fordi det krever både desentralisert og sentralisert styring. Gjennom kraftbransjens samhandling av cyberfysiske systemer oppstår det tette koblinger i et komplekst system. Ifølge Perrow (1999) vil det derfor ikke være mulig å styre kraftbransjen som system. Ettersom nivåene i resiliens har blitt sett i sammenheng med de to ulike formene for styring i komplekse systemer, kan det resonneres frem til at Perrow hadde vært lite optimistisk til en overførbarhet mellom strukturell

cyberresiliens til systemisk cyberresiliens. Det er også lite trolig at han hadde vært positiv til at de to nivåene kan eksistere på samme tid. Perrow ville argumentert for at samhandlingen mellom nivåene bidrar til flere tette koblinger som tilfører enda mer kompleksitet i et system. Som følge av at helhetlig og pålitelig strømforsyning krever systemisk cyberresiliens, vil liten overførbarhet fra strukturell cyberresiliens kunne true kraftbransjens evne til å opprettholde en pålitelig strømforsyning til det norske samfunnet.

Resiliensteori innehar derimot et optimistisk syn på at systemisk cyberresiliens ikke bare er mulig, men at det kan eksistere samtidig som strukturell cyberresiliens. Overførbarheten fra strukturell til systemisk cyberresiliens støttes av Macrae (2019), som sier at resiliensnivåene interagerer og må ses i sammenheng med hverandre. For at to eller flere nivåer skal interagere, vil det være naturlig at de eksisterer på samme tid. Implikasjoner på strukturelt nivå kan dermed ha betydning for resiliens på systemisk nivå. For at dette skal skje, kreves det personell på ulike nivåer som evner å knytte nivåene sammen (Macrae, 2019). Ettersom informantenes nettselskaper er inkludert i KBO-ordningen, er det krav til at de skal ha IKT-sikkerhetskoordinatorer. IKT-sikkerhetskoordinatorer skal ha oversikt over arbeidet med IKT-sikkerhet i sitt selskap, samt være et bindeledd mellom nettselskapet og NVE (Kraftberedskapsforskriften, 2012). IKT-sikkerhetskoordinatorene i nettselskapene kan betraktes som personer som knyttet det strukturelle og systemiske nivået sammen. De styrer både IKT-sikkerhet gjennom desentralisert styring i eget nettselskap, og samtidig er en del av en konsistent sentral ledelse på bransjenivå gjennom sitt samarbeid med NVE. Det vil argumenteres for at det er overførbarhet fra strukturell cyberresiliens til systemisk cyberresiliens, basert på resiliensteoriens optimistiske syn. Det vil likevel kreve noe mer enn strukturell resiliens for å oppnå et nivå av systemisk resiliens.

6.2.4 Systemisk resiliens krever delt forståelse

Basert på poengene presentert fra de ulike teoretiske perspektivene, er det tydelig at overførbarheten fra strukturell cyberresiliens til systemisk cyberresiliens kan være noe utfordrende. Teori knyttet til komplekse systemer ser svært problematisk på dette, og selv optimistisk resiliensteori peker på at systemisk resiliens krever noe mer enn hva som kan overføres fra strukturell resiliens. Macrae og Wiig (2019) mener systemisk resiliens krever en oppfattelse blant aktører om at trusler kan skape en systemisk krise. En delt forståelse av kraftbransjens trusler, sårbarheter og verdier kan argumenteres for å gi en oppfattelse av at trusler mot bransjen kan skape en systemisk krise, for eksempel bortfall av strømforsyning.

Delt forståelse ble likevel identifisert som det svakeste av de tre hovedinsentivene for erfaringsdeling. Det er derfor avgjørende at alle nettselskap er klar over at de har like stor betydning for systemisk cyberresiliens, uavhengig av størrelse. Det er fordi risiko har en tendens til å migrere til det svakeste leddet, som er der systemet er mest sårbart (NSM, 2023). Når risikoen samler seg i det svakeste leddet, kan det utgjøre en potensiell trussel for hele systemet (Grunnan et al., 2008). Å utgjøre det svakeste leddet kan skyldes begrensninger i ressurser, manglende oppmerksomhet eller prioritering av IKT-sikkerhet, eller bare en naturlig sårbarhet i en bestemt del av systemet. Noen av informantene mente det var de mindre nettselskapene som ofte var det svakeste leddet. Det var på grunn av at de ikke hadde like mye kapasitet eller kunnskap til å sette søkelys på IKT-sikkerhet. En informant nyanserte denne påstanden ved å si at et større cyberangrep fortsatt ikke har rammet mindre nettselskap. Mer utdypende sa en annen informant at de store nettselskapene ofte var mer attraktive for trusselaktører, nettopp fordi de hadde flere kunder og opererte innenfor et større geografisk område. Det gjorde at trusselaktørene kunne gjøre større skade ved et vellykket angrep. Uavhengig om de større eller de mindre nettselskapene blir ansett som de mest utsatte leddene i kraftbransjen, er det essensielt å identifisere og styrke de svake leddene for å redusere risiko og oppnå systemisk cyberresiliens. Det er i disse tilfellene erfaringsdeling kan være en bidragsytende faktor. Å dele erfaringer og informasjon om for eksempel IKT-sikkerhetstiltak som er iverksatt, kan gjennom erfaringsdeling redusere sårbarheter i et system.

Det er et faktum at det eksisterte et skille mellom hvordan informantene reflekterte rundt viktigheten av å dele erfaringer, og hvordan de praktiserte erfaringsdeling. Flesteparten av informantene sa de hadde en delt forståelse av å være en del av en større helhet, som gjorde at de måtte bidra i erfaringsdeling. En informant sa eksplisitt at det var helt avgjørende å være resilient for å beskytte den kritiske infrastrukturen som en helhet. Nettselskapenes samlede hovedoppgave er å kontinuerlig sikre en pålitelig forsyning av strøm (Meld. St. 38 (2016-2017)). Det understreker at nettselskaper har ansvar for mer enn kun strukturell cyberresiliens i eget selskap. Imidlertid er det utsagn, fra spesielt tre av informantene fra nettselskapene, som tilsier at delt forståelse ikke gjenspeiles i praksis. Som tidligere forklart er noen av nettselskapene blitt beskrevet som gratispassasjerer i erfaringsdeling (Hausken, 2007). Det kan være et resultat av at nettselskapene er monopolister, og fordi erfaringsdeling for mange blir ansett som et overskuddsprosjekt i bransjen. Det er motsigende å ha en forståelse av å være en del av noe større, men samtidig være en gratispassasjer i erfaringsdeling.

Det kan derfor tolkes slik at noen informanter i teorien var klar over at de hadde en like viktig rolle for den samlede strømforsyningen som andre nettselskaper, men at de i praksis ikke etterfulgte denne tankegangen. Denne diversiteten mellom informantenes refleksjoner og praksis vil ha negative implikasjoner på hvorvidt systemisk cyberresiliens er oppnåelig i kraftbransjen.

Samlet vurderes strukturell cyberresiliens til å ha en viss overførbarhet til systemisk cyberresiliens. Systemisk cyberresiliens anses likevel å kreve en delt forståelse av trusler, sårbarheter og verdier blant nettselskaper, i både teori og praksis. For å etterstrebe systemisk cyberresiliens burde insentivet delt forståelse derfor styrkes. Å bygge resiliens gjennom delt forståelse kan beskrives som en kontinuerlig prosess hvor aktører må utvikle seg for å møte fremtidens trusler (Hausken, 2020). På bakgrunn av dette vil arbeidet mot systemisk cyberresiliens kreve vedvarende oppmerksomhet og prioritering fra samtlige aktører i kraftbransjen.

7 Konklusjon

Målet med denne oppgaven har vært å belyse og drøfte erfaringsdeling mellom nettselskaper etter cyberangrep, med utgangspunkt i intervjuer med sentrale informanter i kraftbransjen og en dokumentanalyse. Vi ønsket å utforske hvordan erfaringsdeling foregår kraftbransjen i dag og om det kan bidra til økt cyberresiliens i lys av den vedvarende trusselen cyberangrep utgjør mot norsk strømforsyning. Følgende problemstilling ble derfor utformet: *Hvordan kan erfaringsdeling mellom nettselskaper etter cyberangrep bidra til økt cyberresiliens for å sikre norsk strømforsyning?*

Insentivene og utfordringene har utpekt seg som styrende for om erfaringsdeling oppleves som ønskelig og gjennomførbart mellom nettselskaper. Basert på oppgavens funn kan det konstateres at nettselskapene opplever gjensidig utbytte av erfaringsdeling. Tilliten mellom nettselskapene er relativ god, selv om menneskelige utfordringer som skam og redsel eksisterer. Videre viser funnene at nettselskapene til en viss grad har en delt forståelse av trusler, sårbarheter og verdier i kraftbransjen, men det er også svakheter tilknyttet insentivet. Basert på en samlet vurdering av de tre identifiserte hovedinsentivene virker erfaringsdeling å være godt etablert mellom nettselskapene, til tross for tilknyttede utfordringer.

Forankring av erfaringer har vist seg som vesentlig for å øke strukturell cyberresiliens i nettselskaper. Nettselskaper har mulighet til å fullføre læringsprosessen hvor det deles erfaringer som blir forankret i eget selskap. Strukturell cyberresiliens i nettselskaper har til en viss grad overførbarhet til systemisk cyberresiliens i kraftbransjen, ettersom nettselskapene er en del av en større helhet. For å oppnå systemisk cyberresiliens kreves overførbarhet fra strukturell cyberresiliens, men også en delt forståelse av felles trusler, sårbarheter og verdier. Konklusjonen er at erfaringsdeling bidrar til å oppnå systemisk cyberresiliens, og at systemisk cyberresiliens kan sikre en helhetlig og pålitelig strømforsyning i kraftbransjen. Det vil derfor hevdes at nettselskaper og praksisfelleskap bør legge et solid grunnlag for erfaringsdeling i dag, da dette vil være til deres fordel i møte med fremtidig utvikling av trusselbildet i smarte strømnett.

7.1 Forslag til videre forskning

Videre forskning av oppgavens temaer, basert på mellomstore og små nettselskaper, kan gi innsikt i hvordan mindre nettselskaper opplever erfaringsdeling. Det kan også gi indikasjoner på hvor stor betydning erfaringsdeling har for deres strukturelle resiliens. Aktuelle forskningsmetoder er foreslått til å være spørreundersøkelse og intervjuer. En spørreundersøkelse vil sikre bred oversikt over hvem som deltar i erfaringsdeling, og nettselskapenes generelle praksis rundt erfaringsdeling. Gjennomføring av dybdeintervjuer vil gi bedre innsikt i insentiver og utfordringer knyttet til erfaringsdeling og reiliensbygging, som kan ses i lys av denne oppgavens funn. I forbindelse med utvidelse av søkelyset til mellomstore og små nettselskaper, er det også andre aktører i kraftbransjen inkluderes i videre forskning. Det kan for eksempel være kraftprodusenter eller leverandører. Det vil være interessant å undersøke hvorvidt slike aktører blir utsatt for cyberangrep, om de deler erfaringer med hverandre, og dets betydning for hvordan resiliens på selskaps- og bransjenivå kan føre til helhetlig sikring av kraftbransjen. Forskningsmetodene burde være i likhet med de som brukes i undersøkelser av mellomstore og små nettselskaper.

For det andre kan det være hensiktsmessig å undersøke kultur for erfaringsdeling, og i den forbindelse hvordan erfaringsdeling kan optimaliseres for å bidra til økt resiliens. En kartleggelse av dette kan gi forståelse av hvordan åpenhet i intern kultur potensielt skaper grunnlag for hvordan et nettselskap deler informasjon og erfaringer eksternt. En casestudie kan gi dybdekunnskap om kulturen rundt deling ved hjelp av intervjuer, dokumenter og observasjoner i et selskap. Kultur er ofte et komplekst område å undersøke, og en casestudie vil dermed være nyttig i den sammenheng. I forskningen kan det være aktuelt å se til Reason (1997) sine fire komponenter for informerende kultur, Westrums (2005) tre typer organisasjonskultur, og teori tilknyttet HRO-perspektivet (LaPorte & Consolini, 1991; Weick & Sutcliffe, 2007).

Et siste forslag til videre forskning knyttes til systemisk cyberresiliens. I oppgaven blir delt forståelse trukket fram som viktig for å etablere cyberresiliens på bransjenivå. Det vil derfor være nyttig å undersøke på hvilken måte delt forståelse knyttet til kraftbransjens trusler, sårbarheter og verdier fremkommer blant nettselskapene, samt hvilke tiltak som kan iverksettes for økt delt forståelse på det systemiske nivået. Det systemiske nivået i kraftbransjen inkluderer NVE og til dels KBO-enhetene. Kvalitative spørreundersøkelser kan brukes for å undersøke delt forståelse blant KBO-enhetene. Deltakende observasjon burde tas

i bruk for å undersøke hvordan NVE utarbeider sine informasjonsskriv til aktører i kraftbransjen, hvor trusler og sårbarheter blir presentert. Basert på undersøkelsene vil der være mulig å utarbeide forslag til hvordan økt forståelse blant nettselskapene kan økes for å sikre systemisk cyberresiliens i kraftbransjen. I gjennomførelse av forskningen kan det være nyttig å se til Jasanoff (1988) sin beskrivelse av risikopersepsjon, og Njå et al. (2020) sin modell for sikkerhetsstyring.

Referanseliste

Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma - Tidsskrift for økonomi og ledelse, 0220*, 18-26.

Anholt, R. & Boersma, F. K. (2018). From security to resilience: New vistas for international responses to protracted crises. *Resilience, 2*, 25-32.

Aoyama, T., Naruoka, H., Koshijima, I. & Watanabe, K. (2015). How Management Goes Wrong? – The Human Factor Lessons Learned from a Cyber Incident Handling Exercise *Procedia Manufacturing, 3,* 1082-1087. https://doi.org/10.1016/j.promfg.2015.07.178

Arghandeh, R., Von Meier, A., Mehrmanesh, L. & Mili, L. (2016). On the definition of cyber-physical resilience in power systems. *Renewable and Sustainable Energy Reviews, 58*, 1060-1069. https://doi.org/10.1016/j.rser.2015.12.193

Ashibani, Y. & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security, 68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

Atkins, S. & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity, 7*(1), 1-11. https://doi.org/10.1093/cybsec/tyab024

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience – fundamentals for a definition. I A. Rocha, A. M. Correia, S. Costanzo & L. P. Reis (Red.), *New Contributions in Information Systems and Technologies: Volume 1* (s. 311-316). Springer International Publishing.

Blaikie, N. & Priest, J. (2019). *Designing social research: the logic of anticipation* (3. utg.). Polity Press.

Bodsberg, L., Hale, B., Dahl, Ø., Grøtan, T. O., Jaatun, M. G., Moe. M. & Onshun, T. (2018). *Kunnskapsprosjekt IKT-sikkerhet; Industrielle kontroll- og sikkerhetssystemer i petroleumsvirksomheten* (2018:00572). SINTEF. https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/kunnskapsprosjekt-ikt-sikkerhet-sluttrapport-med-underskrift.pdf

Brown, C., Seville, E. & Vargo, J. (2017). Measuring the organizational resilience of critical infrastructure providers: A New Zealand case study. *International Journal of Critical Infrastructure Protection, 18*, 37–49. https://doi.org/10.1016/j.ijcip.2017.05.002

Bruvoll, J., Brattekås, K. & Nystuen, K. O. (2020). Funksjonsbasert risikovurdering. I H. Bergsjø, R. Windvik & L. Øverlier (Red.), *Digital sikkerhet – En innføring* (s. 185-201). Universitetsforlaget.

Cantelmi, R., Di Gravio, G., & Patriarca, R. (2021). Reviewing qualitative research approaches in the context of critical infrastructure resilience. *Environment Systems & Decisions, 41*(3), 341–376. https://doi.org/10.1007/s10669-020-09795-8

Clark, T., Foster, L. & Bryman, A. (2019). *How to do your Social Research Project or Dissertation*. Oxford University Press.

CPS-Summit (2008). *Report: Cyber-Physical Systems Summit*. https://iccps2012.cse.wustl.edu/_doc/CPS_Summit_Report.pdf

Danermark, B., Ekström, M. & Karlsson, J. C. (2019). *Explaining Society*: *Critical Realism in the Social Sciences* (2. utg.). Routledge.

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner – Hvilken funksjonsevne må samfunnet opprettholde til enhver tid*. Versjon 1.0. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity, 5*(1), 1-17. https://doi.org/10.1093/cybsec/tyz013

Energiloven. (1990). *Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.* (LOV-1990-06-29-50). Lovdata. https://lovdata.no/dokument/NL/lov/1990-06-29-50

Engen, O. A. H., Gould, K. A. P., Kruke, B. I., Lindøe, P. H., Olsen, K. H. & Olsen, O. E. (2021). *Perspektiver på samfunnssikkerhet* (2. utg.). Cappelen Damm Akademisk.

Fornybar Norge. (u.å.). *Fornybarakademiet - kunnskap for en fornybar fremtid*. https://www.fornybarnorge.no/kurs-og-konferanser2/

Forum for informasjonssikkerhet i kraftforsyningen. (u.å.). *Om*. https://fsk-forum.no/om/

Frøystad, C., Jaatun, M. G., Bernsmed, K. & Moe, M. (2018). *Risiko- og sårbarhetsanalyse for økt integrasjon mellom AMS, DMS og SCADA* (Nr. 15/2018). Norges vassdrags- og energidirektorat. http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf?fbclid=IwAR32I2lhxK-wCjsXcFNA86mY3kJla6dphpxXtG6Go0oxS9YY8DtVayBJZLo

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal, 18*(1), 1–7. https://doi.org/10.1080/19393550802676097

Gherardi, S., Nocolini, D. & Odella, F. (1998). Towards a Social Understanding of How People Learn in Organizations: The Notion of Situated Curriculum. *Management Learning*, *29*(3), 273-297. https://doi.org/10.1177/1350507698293002

Gjesvik, L. (2019). *Comparing Cyber Security. Critical Infrastructure protection in Norway, the UK and Finland*. NUPI Report 5/2019. Norwegian Institute of International Affairs. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2598280/NUPI_Report_5_2019_Gjesvik.pdf?sequence=1&isAllowed=y

Grunnan, T., Bjørnskau, T. & Kolbenstvedt, M. (2008). *Sikkerhet på tvers i samferdselssektoren* (TØI rapport 954/2008). Transportøkonomisk institutt.

Halvorsen, K. (2008). *Å forske på samfunnet: En innføring i samfunnsvitenskapelig metode* (5. utg.). Cappelen Akademiske Forlag.

Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, *26*(6), 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/j.iot.2020.100204

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

Jasanoff, S. (1988). The political science of risk perception. *Reliability Engeneering & System Safety*, *59*(1), 91-99. https://doi.org/10.1016/S0951-8320(97)00129-4

Johannessen, A., Tufte, P.A. & Christoffersen, L. (2021). *Introduksjon til samfunnsvitenskapelig metode* (6. utg.). Abstrakt forlag.

Jore, S. H. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Kolb, D. A. (2015). *Experiential learning: experience as the source of learning and development* (2. utg.). Pearson Education.

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

Kraftberedskapsforskriften. (2012). *Forskrift om sikkerhet og beredskap i kraftforsyningen* (FOR-2012-12-07-1157). Lovdata. https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

KraftCERT. (u.å.). *Om KraftCERT*. https://www.kraftcert.no/no/#om

LaPorte, T. R. & Consolini, P. M. (1991). Working in practice put not in theory. Theoretical challenges of "high-reliability organisations". Journal of Public Administration Research and Theory. J-PART 1 (1): 19-48. https://doi.org/10.1093/oxfordjournals.jpart.a037070

Lave, J. & Wenger, E. (1991). *Situated Learning: Legitimate peripherial participation.* Cambridge University Press.

Lee, E. A. (2008). Cyber Physical Systems: Design Challenges. *2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC),* 363–369. https://doi.org/10.1109/ISORC.2008.25

Leveson, N. G. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press. https://doi.org/10.7551/mitpress/8179.001.0001

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J. & Kott, A. (2012). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33,* 471–476. https://doi.org/10.1007/s10669-013-9485-y

Loseke, D. R. (2017). *Methodological thinking: Basic Principles of Social Research Design* (2. utg.). SAGE Publications.

Macrae, C. (2019). Moments of Resilience: Time, Space, and the Organisation of Safety in Complex Sociotechnical Systems. I S. Wiig & B. Fahlbruch (Red.), *Exploring Resilience: A Scientific Journey from Practice to Theory* (s. 15-21). Springer Open.

Macrae, C. & Wiig, S. (2019). Resilience: From Practice to Theory and Back Again. I S. Wiig & B. Fahlbruch (Red.), *Exploring Resilience: A Scientific Journey from Practice to Theory* (s. 121-128). Springer Open.

Martin, P. (2019). *The rules of security: staying safe in a risky world*. Oxford University Press.

Meld. St. 14 (2011-2012). *Vi bygger Norge – om utbygging av strømnett*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/19472ee2fcc54a0eaae169972fd61c98/no/pdfs/stm201120120014000dddpdfs.pdf

Meld. St. 25 (2015-2016). *Kraft til endring: Energipolitikken mot 2030*. Olje- og energidepartementet. https://www.regjeringen.no/contentassets/31249efa2ca6425cab08130b35ebb997/no/pdfs/stm201520160025000dddpdfs.pdf

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

Nasjonal sikkerhetsmyndighet, Politidirektoratet & Politiets sikkerhetstjeneste. (2015). *Terrorsikring. En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger*. https://www.politiet.no/globalassets/03-rad-og-forebygging/beredskap/terrorsikring_en_veileder

Nasjonal sikkerhetsmyndighet. (2017). *Rammeverk for handtering av IKT-sikkerhetshendelser*. https://nsm.no/getfile.php/133853-1593022504/NSM/Filer/Dokumenter/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

Nasjonal sikkerhetsmyndighet. (2020). *NSMs grunnprinsipper for IKT-sikkerhet*. Versjon 2.0. https://nsm.no/getfile.php/133735-1592917067/NSM/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

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

Nettalliansen. (u.å.) *Om Nettalliansen*. https://nettalliansen.no/om-nettalliansen

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

Nonake, I. & Takeuchi, H. (1995). *The knowledge-creating company: how Japanese companies create the dynamics of innovation.* Oxford University Press.

Norges vassdrags- og energidirektorat (2022). *Årsrapport for NVE 2021*. https://publikasjoner.nve.no/rapport/2022/rapport2022_17.pdf

Norges vassdrags- og energidirektorat (2023). *Nett.* https://www.nve.no/energi/energisystem/nett/

NorSIS. (2021). *Trusler og trender 2021*. https://norsis.no/content/uploads/2022/05/NorSIS_Trusler_Trender_2021_Digital.pdf

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

NOU 2012: 9. (2012). *Energiutredningen – verdiskaping, forsyningssikkerhet og miljø*. Olje- og energidepartementet.

NOU 2022: 6. (2022). *Nett i tide – om utvikling av strømnettet.* Olje- og energidepartementet.

Næringslivets Hovedorganisasjon (2019). *Åpenhet har hindret nye cyberangrep*. https://www.nho.no/tema/offentlig-sektor-og-naeringslivet/artikler/apenhet-har-hindret-nye-cyberangrep/?fbclid=IwAR3oOQ9yj5kzWKmWe9-62TzC0B4KRPE2GstsiURljJ3M0bfQTQIDjopAH5U

Næringslivets sikkerhetsråd (2022). *Mørketallsundersøkelsen 2022*. https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen

Olje- og energidepartementet (2022). *Strømforsyning og strømnettet.* Regjeringen. https://www.regjeringen.no/no/tema/energi/strom/stromforsyning-og-stromnettet/id2353792/

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

Pettersen, K. A. & Schulman, P. R. (2019). Drift, adaptation, resilience, and reliability: Toward an empirical clarification. *Safety Science*, *117*, 460–468. https://doi.org/10.1016/j.ssci.2016.03.004

Pléta, T., Tvaronavičienė, M., Casa, S. D. & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. *Insight into Regional Development, 2*(3), 703-715. https://doi.org/10.9770/IRD.2020.2.3(7)

Rak, A. (2002). Information Sharing in the Cyber Age: a Key to Critical Infrastructure Protection. *Information Security Technical Report, 7*(2), 50-56. https://doi.org/10.1016/S1363-4127(02)02006-X

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

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet I kraftforsyningen*. Dokument 3:7 (2020-2021). https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

Rinaldi, S. M., Peerenboom, J. P. og Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11-25. https://doi.org/10.1109/37.969131

Rousseau, D., Sitkin, S., Burt, R. & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *The Academy of Management Review*, *23*(3), 393–404. https://doi.org/10.5465/AMR.1998.926617

Ruth, M. & Goessling-Reisemann, S. (2019). *Handbook on Resilience of Socio-Technical Systems*. Edward Elgar Pub.

Røyksund, M. & Valdal, A. K. (2020). Kartlegging av bruk av tingenes internett (IoT/ IIoT) i norsk kraftforsyning (Nr. 2/2020). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf

Salvi, A., Spagnoletti, P. & Noori, N. S. (2022). Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem. *Computers & Security*, *112*, 102507. https://doi.org/10.1016/j.cose.2021.102507

Samfunnsbedriftene. (u.å.). *Kompetansebyggende kurs og programmer for energibransjen*. https://www.samfunnsbedriftene.no/bransjer/energi/kompetanseutvikling/

Shutterstock (2022). *Arkiv Vektor ID: 1548552875*. https://www.shutterstock.com/nb/image-vector/high-voltage-power-line-electric-transmission-1548552875

SINTEF (u.å.). SmartGrids. https://www.sintef.no/fagomrader/smartgrids/

Skotnes, R. (2018). Regulering og standardisering av IKT-sikkerhet i kraftsektoren – holdninger, fordeler og ulemper. I P. H. Lindøe & G. S. Braut (Red.), *Regulering og standardisering — Perspektiver og praksis*. Universitetsforlaget.

Spilde, D., Hodge, L. E., Magnussen, I. H., Hole, J., Buvik, M. & Horne, H. (2019). *Strømforbruk mot 2040: Analyse av strømforbruk i Fastlands-Norge, Norden og utvalgte EU-land.* Norges vassdrags- og energidirektorat. http://publikasjoner.nve.no/rapport/2019/rapport2019_22.pdf

Statnett. (2018). *Slik fungerer kraftsystemet*. https://www.statnett.no/om-statnett/bli-bedre-kjent-med-statnett/slik-fungerer-kraftsystemet/

Sørgard, L., Reiten, E. & Bjella, K. (2014). *Et bedre organisert strømnett*. Olje- og energidepartementet. https://www.regjeringen.no/globalassets/upload/oed/pdf_filer_2/rapport_et_bedre_organisert_stroemnett.pdf

Thagaard, T. (2018). *Systematikk og innlevelse: en innføring i kvalitative metoder* (5.utg.). Fagbokforlaget.

Tjora, A. H. (2021). *Kvalitative forskningsmetoder i praksis* (4. utg.). Gyldendal.

Tøien, F. K., Fagermyr, J., Treider, G. & Remvang, H. (2021). *IKT-sikkerhetstilstanden i kraftforsyningen 2021* (Nr. 19/2021). Norges vassdrags- og energidirektorat. https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

Törngren, M., Asplund, F., Bensalem, S., McDermid, J., Passerone, R., Pfeifer, H., Sangiovanni-Vincentelli, A., & Schätz, B. (2017). Characterization, Analysis, and Recommendations for Exploiting the Opportunities of Cyber-Physical Systems. I H. Song, D. B. Rawat, S. Jeschke, & C. Brecher (Red.), *Cyber-Physical Systems: Foundations, Principles and Applications* (s. 3–14). Academic Press. https://doi.org/10.1016/B978-0-12-803801-7.00001-8

Weick, K. & Sutcliffe, K. M. (2007). *Managing the unexpected. Assuring high performance in an age of complexity.* Jossey-Bass.

Wenger, E., McDermott, R. A. & Snyder, W. M. (2002). *Cultivating Communities of Practice: A Guide to Managing Knowledge.* Harvard Business Review Press.

Westrum, R. (2005). A Typology of Organizational Cultures. *Quality and Safety in Health Care*, *13*(2), 22-27. https://doi.org/10.1136/qhc.13.suppl_2.ii22

Yaacoub, J. P. A, Salman, O., Noura, H. N., Kaaniche, N., Chehab, A. & Malli, M. (2020). Cyber-physical systems security: Limitations, issues, and future trends. *Microprocessors and Microsystems, 77,* 103201–103201. https://doi.org/10.1016/j.micpro.2020.103201

VEDLEGG 1 – Informasjonsskriv

Vil du delta i forskningsprosjektet «erfaringsdeling i kraftbransjen»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt for en masteroppgave i samfunnssikkerhet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette er et prosjekt i forbindelse med vår masteroppgave i samfunnssikkerhet ved Universitetet i Stavanger.

Forsyning av elektrisk kraft til samfunnet blir betegnet som en kritisk samfunnsfunksjon. Samtidig opplever kraftbransjen en ekspansjon i digitalisering. Det gjør at bransjen står overfor nye sårbarheter og en ny måte å forholde seg til digitale problemstillinger som ofte er komplekse og tvetydelige. Gjennom denne utviklingen har det oppstått cyberfysiske systemer. Ettersom truslene mot de cyberfysiske systemene vokser i omfang og konsekvens har flere virksomheter gått sammen om å dele kompetanse og erfaringer, for å være bedre rustet mot angrep. Likevel er det virksomheter som ikke er en del av dette samarbeidet. I den forbindelse ønsker vi å undersøke hvilken betydning erfaringsdeling på tvers av virksomheter kan ha for cyberresiliens i kraftbransjen.

Gjennom intervjuer med nettselskaper og organisasjoner i bransjen håper vi å få innsikt i hva aktørene selv tenker om dagens samarbeid gjennom erfaringsdeling, hva som er utfordringene og hva de ønsker at fremtidens erfaringsdeling skal føre med seg.

Forskningsprosjektets problemstilling er:
På hvilken måte kan erfaringsdeling mellom nettselskaper etter cyberhendelser bidra til økt cyberresilens i forsyningssikkerheten i kraftbransjen?

For å besvare problemstillingen er det utarbeidet tre forskningsspørsmål:
1: Hvordan arbeider nettselskaper med erfaringsdeling etter cyberhendelser i dag?
2: Hvilke utfordringer knytter aktører i kraftbransjen til erfaringsdeling etter cyberhendelser?
3: Hvordan vurderer aktørene erfaringsdeling som strategi for cyberresiliens i fremtiden?

Den endelige problemstillingen og forskningsspørsmålene spikres som oftest mot slutten av prosjektet.

Datainnsamlingen til prosjektet vil ikke bli benyttet til andre formål enn til masteroppgaven.

Hvem er ansvarlig for forskningsprosjektet?
Universitetet i Stavanger ved Kenneth Arne Pettersen Gould er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
På bakgrunn av problemstillingen ønsker vi å komme i kontakt med personer som jobber i mellomstore og store nettselskaper, samt organisasjoner som har innsikt i ulike muligheter og problemstillinger knyttet til erfaringsdeling i kraftbransjen.

Du får spørsmål om å delta fordi vi anser deg og din rolle som en relevant og hensiktsmessig kilde for forskningsprosjektets formål.

Et passende utvalg for en masteroppgave er ca. 10-15 personer. Det vil dermed være en del nettselskaper og organisasjoner som vil få forespørsel om å stille til intervju.

Hva innebærer det for deg å delta?
Hvis du velger å delta i prosjektet, innebærer det å stille til et semistrukturert intervju. Varigheten på intervjuet er antatt å være omtrent 45-60 minutter.

Det vil bli gjort lydopptak av intervjuet. Det er kun for å opprettholde god kvalitet på prosjektet, og all data fra intervjuet som anvendes i oppgaven vil bli sendt til deg for godkjenning. Lydopptakene blir gjort gjennom en app som heter *Nettskjema-Diktafon*. Videre blir lydopptakene oppbevart i *Nettskjema*, som er en sikker løsning for innsamling av data gjennom lydopptak. Dette krever innlogging for å få tilgang. Løsningen er utviklet av Universitetet i Oslo.

Det er verdt å påpeke at det er den faglige tematikken som står i fokus, ikke virksomheten eller informantene som deltar. Informantene som rekrutteres til dette forskningsprosjektet vil kun svare som representanter på vegne av ansvarsområdet i virksomheten.

Det er frivillig å delta

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

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.
Det vil kun være de to masterstudentene i prosjektet som har tilgang til de personlige datafilene.

Vi vil gjøre følgende for å sikre at ingen andre personer får tilgang til de personlige dataene:

- Vi vil erstatte ditt navn og din kontaktinformasjon med en kode.
- Listen over navn, kontaktinformasjon og relevante koder vil lagres atskilt fra de øvrige innsamlede dataene.
- Dataene vil bli lagret på en egen data-server.

Deltakere vil bli anonymisert i prosjektoppgaven.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Prosjektet skal etter planen avsluttes 15. juni 2023. Ved avslutning av prosjektet skal alle digitale opptak og personopplysninger bli slettet.

De anonymiserte opplysningene som fremkommer i intervjuet, vil være allment tilgjengelig på ubestemt tid da masteroppgaven publiseres offentlig på internett (UiS Brage).

Dine rettigheter

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

- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet)
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

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

Hvor kan du finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Emma Amundsen, masterstudent: em.amundsen@stud.uis.no
- Ida-Kristin Johnsen, masterstudent: ida.johnsen@stud.uis.no
- Universitetet i Stavanger ved Kenneth Arne Pettersen Gould: kenneth.a.pettersen@uis.no
- Vårt personvernombud kan nåes på e-post: personvernombud@uis.no

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

- NSD – Norsk senter for forskningsdata AS, på e-post (personverntjenester@nsd.no) eller tlf. 55582117.

Med vennlig hilsen

Kenneth Arne Pettersen Gould	Emma Amundsen og Ida-Kristin Johnsen
Veileder for masteroppgaven	Masterstudenter/forfattere

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "erfaringsdeling i kraftbransjen", og har fått anledning til å stille spørsmål. Jeg samtykker til:

□ å delta i et intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. 15. juni 2023.

(Prosjektdeltakers signatur, dato)

VEDLEGG 2 – Godkjenning av NSD

Kommentar

OM VURDERINGEN

Sikt har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

DELE PROSJEKTET MED PROSJEKTANSVARLIG

Du må dele prosjektet med prosjektansvarlig. Velg "Del prosjekt" øverst i meldeskjemaet. Hvis prosjektansvarlig ikke godtar invitasjonen innen én uke, må du sende en ny invitasjon.

FØLG DIN INSTITUSJONS RETNINGSLINJER

Vi har vurdert at du har lovlig grunnlag til å behandle personopplysningene, men husk at det er institusjonen du er ansatt/student ved som avgjør hvilke databehandlere du kan bruke og hvordan du må lagre og sikre data i ditt prosjekt. Husk å bruke leverandører som din institusjon har avtale med (f.eks. ved skylagring, nettspørreskjema, videosamtale el.)

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

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Se våre nettsider om hvilke endringer du må melde: https://sikt.no/melde-endringar-i-meldeskjema

OPPFØLGING AV PROSJEKTET

Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

VEDLEGG 3 – Intervjuguide for samarbeidsorganisasjoner

Denne intervjuguiden ble tilpasset de ulike samarbeidsorganisasjonene.

Presentasjon av oss, masteroppgaven, og hovedpunkter fra informasjonsskrivet.

Innledende spørsmål

Kan du fortelle kort om deg selv og dine viktigste arbeidsoppgaver?
Hva er overordnet status for IKT-sikkerhet i kraftbransjen i dag?
Hva er bakgrunnen for at samarbeidsorganisasjonen ble opprettet?
Hvorfor ser dere et behov for erfaringsdeling mellom nettselskaper?

Tema 1: Dagens praksis

Opplever nettselskapene å bli utsatt for større cyberangrep?

- Hvilke typer angrep forekommer mest hos selskapene?
- Hva er de mest alvorlige konsekvensene som kan ramme selskaper?

Hvordan foregår erfaringsdeling mellom nettselskaper i praksis i samarbeidsorganisasjonen?
Hvilke typer erfaringer er det vanlig å dele etter et cyberangrep?
Hvordan arbeider nettselskapene videre med informasjonen de mottar?
Hva er inntrykket deres av nettselskapenes utbytte av erfaringsdeling etter cyberhendelser?
Hvilke faktorer mener dere er viktig for å sikre godt utbytte av erfaringsdeling mellom nettselskaper?
Hva er samarbeidsorganisasjonen sin rolle i forhold til andre samarbeidsorganisasjoner i bransjen?

Tema 2: Utfordringer med erfaringsdeling

Hvilke utfordringer opplever dere knyttet til erfaringsdeling mellom nettselskaper?
Hvilke typer cyberangrep opplever du det er vanskeligere for nettselskaper å dele erfaringer rundt?

- Hva tenker du kan være grunner til at visse typer erfaringer ikke blir delt med andre medlemmer?

Hvor raskt etter en hendelse er det oppnåelig at et selskap klarer å dele erfaringer med andre nettselskaper?
Hvilke faktorer mener du at kan svekke erfaringsdeling mellom nettselskaper?

Tema 3: Resiliens

Tenker du det er oppnåelig for selskaper å beskytte seg fullstendig mot cyberangrep?

- Hvis nei: Hva er alternativet?

Er resiliens et begrep du har kjennskap til, og som blir brukt i deres organisasjon?

Hvordan vil du beskrive et motstandsdyktig nettselskap?

Hvordan tenker du erfaringsdeling kan påvirke motstandsdyktighet?

Tema 4: Tiden fremover

Har dere oppnådd det dere ønsket med samarbeidsorganisasjonen?

Hva er målet videre for samarbeidsorganisasjonen når det gjelder erfaringsdeling mellom nettselskaper?

Hva tenker du ville vært den mest ideelle løsningen for bransjen når det gjelder erfaringsdeling mellom nettselskaper?

Avsluttende spørsmål

Er det noe du vil presisere eller legge til?

Opplyser informanten om at han/hun kan kontakte oss på e-post i etterkant, hvis det spørsmål eller ytterligere innspill.

Takke informanten for intervjuet.

VEDLEGG 4 – Intervjuguide for nettselskaper

Denne intervjuguiden ble tilpasset de ulike nettselskapene.

Presentasjon av oss, masteroppgaven og hovedpunkter fra informasjonsskriv.

Innledende spørsmål

Kan du fortelle kort om deg selv og dine viktigste arbeidsoppgaver?

Hva er overordnet status er for IKT-sikkerhet i kraftbransjen i dag?

Hva er dine overordnede tanker om erfaringsdeling i kraftbransjen?

Tema 1: Dagens praksis

Opplever dere å bli utsatt for større cyberangrep?

- Hvilke typer angrep forekommer mest?
- Hva er de mest alvorlige konsekvensene for dere?

Er dere medlem i en eller flere organisasjoner som tilrettelegger for erfaringsdeling?

- Hvis ja: Hvilke?

Hvordan foregår deling av erfaringer mellom dere og andre nettselskaper i praksis i samarbeidsorganisasjonen(e)?

- Har dere delt erfaringer fra angrep med andre nettselskap?
- Hvilke erfaringer er det mest interessant for dere om andre deler?

Hvilket utbytte har dere av erfaringsdeling etter cyberangrep?

Hvilke faktorer anser du som viktig for at dere skal dere erfaringer med andre?

Hva er deres største motivasjon for å dele erfaringer med andre nettselskaper?

Hvordan arbeider dere videre med informasjon dere mottar fra organisasjonen(e) og deres medlemmer?

Tema 2: Utfordringer med erfaringsdeling

Hvilke utfordringer opplever dere knyttet til erfaringsdeling mellom nettselskaper?

Opplever du forskjeller i hva ulike selskaper velger å dele erfaringer om?

- Hvis ja: Hvilke?

Hvor raskt etter et angrep er det oppnåelig at dere kan dele erfaringer med andre nettselskaper?

Hvilke faktorer mener du at kan svekke erfaringsdeling mellom dere og andre nettselskaper?

Tema 3: Resiliens

Tenker du at det er oppnåelig å beskytte seg fullstendig mot cyberangrep?

- Hvis nei: Hva er alternativet?

Er resiliens et begrep du har kjennskap til, og som blir brukt i deres selskap?

Hvordan vil du beskrive et motstandsdyktig nettselskap?

Hvordan tenker du erfaringsdeling kan påvirke motstandsdyktighet?

Tema 4: Tiden fremover

Hvordan ser du for deg at erfaringsdeling vil foregå i kraftbransjen fremover?

Hva tenker du ville vært den mest ideelle løsningen for erfaringsdeling mellom nettselskaper?

Avsluttende spørsmål

Er det noe du vil presisere eller legge til?

Opplyser informanten om at han/hun kan kontakte oss på e-post i etterkant, hvis det spørsmål eller ytterligere innspill.

Takke informanter for intervjuet.