FRA VÆR OG VIND TIL BITS AND BYTES

En kvalitativ studie av hvordan aktører i den norske kraftforsyningen forstår og håndterer cyberrisiko som følge av sektorens digitale utvikling.

Foto: Riccardo Annandale, hentet fra Unsplash

Masteroppgave i samfunnssikkerhet

Våren 2020

Universitetet i Stavanger

Maria Halvorsen
Sigrid Haug Selnes

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Samfunnssikkerhet	Vårsemesteret, 2020 Åpen
Forfattere: Maria Halvorsen og Sigrid Haug Selnes	
Fagansvarlig: Ole Andreas Hegland Engen **Veileder:** Ole Andreas Hegland Engen	
Tittel på masteroppgaven: **Fra vær og vind til bits and bytes** - En kvalitativ studie av hvordan aktører i den norske kraftforsyningen forstår og håndterer cyberrisiko som følge av sektorens digitale utvikling. **Engelsk tittel:** **From Rain and Storm to Bits and Bytes** - A qualitative study of how actors in the Norwegian power supply understand and manage cyber risk as a result of digital development.	
Studiepoeng: 30	
Emneord: Samfunnssikkerhet, cybersikkerhet, cyberrisiko, kompleksitet, risikoforståelse, kraftforsyning, digitalisering	Sidetall: 94 + vedlegg/annet: 100 Stavanger, 15. juni 2020

Forord

I det øyeblikket denne oppgaven leveres, feirer vi en fullført masteroppgave i samfunnssikkerhet. Disse to årene har vært lærerike, krevende, travle, morsomme og givende. Vi føler oss godt rustet til å møte arbeidslivet som nyutdannede innenfor et fagfelt hvor vi føler det er bruk for oss.

Det har vært en annerledes tid å skrive masteroppgave i. Universitetet er stengt, og lange arbeidsdager på biblioteket med felles lunsjpause ble brått erstattet med hjemmekontor. Det har tidvis vært utfordrende. Samtidig har det ført til at vi har fått god øvelse i å finne nye løsninger, nye metoder og nye arbeidsformer. Det gikk bra til slutt det også!

Vi vil gjerne takke alle forelesere ved samfunnssikkerhet på UiS, som har gitt oss et solid grunnlag for å kunne skrive denne oppgaven. Takk for all deres kunnskap, engasjement og oppfølging. Vi vil også takke Janne Hagen i Norges vassdrags- og energidirektorat, som har bidratt med gode og relevante innspill i prosjektets innledende fase.

Spesielt vil vi takke Ole Andreas H. Engen, vår veileder gjennom dette prosjektet. Du har loset oss gjennom oppturer og nedturer. Du har vært optimistisk, støttende, tydelig, og alltid kommet med konstruktive råd og god faglig veiledning. Du er raus med tiden din, alltid tilgjengelig, og du har vært en god samarbeidspartner fra start til slutt. Tusen takk Ole Andreas, for at du har delt din erfaring og alt det du kan om hvordan å skrive en god oppgave med oss!

Takk til informantene våre fra den norske kraftsektoren, som velvillig har stilt opp til intervjuer. Takk for at dere har brukt tid på å dele deres kunnskap og innsikt med oss. Dere har vært engasjerte i oppgaven og engasjerte i tematikken. Det har vært inspirerende for oss og gitt oss en bekreftelse på at det vi har jobbet med er relevant for flere enn oss selv.

Til slutt vil vi takke Jonas og Per Christian, for mental og praktisk støtte gjennom våren. Både når alt går på skinner, og når alt går litt trått. Dere er gode å ha. Takk Isak og Levi for at dere har holdt ut med noe varierende pedagogisk innhold i hjemmebarnehagen.

Fra oss til oss: takk for samarbeidet. God lesning!

Stavanger, 15 juni 2020

Maria Halvorsen
Sigrid Haug Selnes

Sammendrag

Som et svar på et økende behov for å forstå og håndtere cyberrisiko som følger med samfunnets digitale utvikling, ønsker denne oppgaven å belyse disse aspektene i en sektor som forvalter en av våre mest kritiske funksjoner; den norske kraftforsyningen. Studiens problemstilling er derfor følgende:

Hvordan forstår og håndterer aktører i den norske kraftforsyningen cyberrisiko som følge av sektorens digitale utvikling?

For å besvare problemstillingen har offentlige dokumenter utgitt på nasjonalt nivå og av sektoren selv blitt analysert. Det er også gjennomført kvalitative intervjuer med åtte aktører tilknyttet den norske kraftforsyningen, som har delt sin erfaring og kunnskap om digitaliseringen i sektoren.

For å besvare problemstillingen har vi benyttet ulike teorier innen sikkerhetsfeltet. Teorien om normale ulykker illustrerer hvilken innvirkning digitaliseringen har hatt på bransjens risikostruktur. Ulike teoretiske perspektiver på risiko og sikkerhet belyser hvordan aktørene forstår risikoen som digitaliseringen introduserer. Teorier om HRO, resiliens og sikkerhetskultur har videre bidratt til å belyse hvordan nye farer og trusler håndteres.

Studien har avdekket at aktørene i den norske kraftforsyningen har en uklar forståelse av begrepet cyberrisko, og at hva de ulike aktørene legger i begrepet, varierer. Sammenstillingen av svar viser likevel at aktørene implisitt har en forståelse for at cyberrisiko som følge av digitaliseringen rommer mange ulike former for farer og trusler, utilsiktede og tilsiktede. Ulikheter i begrepstilnærmingen og variasjoner i oppfatninger om hva som kan forårsake en cyberhendelse indikerer at det kan være behov å skape konsensus i bransjen rundt disse forholdene.

Cyberrisiko håndteres videre gjennom risikovurderinger og preventive mekanismer i organisasjonen, samt samhandling på tvers av selskaper i sektoren. Viktigst blant alle disse er opplæring og bevisstgjøring av øvrige ansatte, og en underliggende forankring i ledelsen som bidrar til å muliggjøre nettopp dette; en felles risikoforståelse i hele virksomheten.

Innholdsfortegnelse

Figurer:

Forkortelser og forklaringer

AMS	Avanserte målesystemer
CISO	Chief information security officer (IKT-sikkerhetsleder)
DDoS	Distributed Denial-of-Service (tjenestenektangrep)
DSB	Direktoratet for samfunnssikkerhet og beredskap
EKOM	Elektronisk kommunikasjon og tilhørende infrastruktur
HRO	High reliability organization (høypålitelige organisasjoner)
HRT	High reliability theory
IKT	Informasjons- og kommunikasjonsteknologi
IT	Informasjonsteknologi (informational technology)
KBO	Kraftforsyningens beredskapsorganisasjon
NAT	Normal accident theory (teorien om normale ulykker)
NSM	Nasjonal sikkerhetsmyndighet
NSR	Næringslivets sikkerhertsråd
NVE	Norges vassdrags- og energidirektorat
OT	Operasjonell teknologi
PST	Politiets sikkerhetstjeneste
SCADA	Supervisory control and data acquisition systems (driftskontrollsystemer)
SoMe	Sosiale medier

1.0 Innledning

Den digitale utviklingen i Norge innebærer at samfunnet og dets funksjoner er i endring (NOU 2018:14, s. 22). Utviklingen gir en rekke gevinster samfunnet som helhet kan nyte godt av, men gevinster er ikke det eneste som følger med teknologisk utvikling. (NOU 2015:13). Utviklingen medfører at verdier flyttes til digitale domener, nye sårbarheter oppstår, og trusselbildet blir dynamisk og utfordrende. I tillegg konstrueres komplekse systemer som er vanskelig å forstå (NOU 2015:13; Nasjonal sikkerhetsmyndighet, 2020).

En av infrastrukturene som preges av digitaliseringen, er den norske kraftforsyningen. Sektoren er svært viktig for samfunnets overordnede funksjonalitet (Direktoratet for samfunnssikkerhet og beredskap, 2016, s. 89). Dersom energiforsyningen faller ut, vil store deler av samfunnet stoppe opp (NSM, 2020, s. 10). Det er derfor avgjørende at sektoren evner å beskytte seg mot både tilsiktede og utilsiktede hendelser som kan føre til forstyrrelser og sammenbrudd i infrastrukturens funksjonsevne. En bransje som er godt vant med håndtering av uønskede hendelser som følge av vær og vind, står nå overfor betydelige endringer i risikobildet som følge av digitaliseringen (Norges vassdrags- og energidirektorat, 2017a). Det er derfor viktig at sikkerhetsarbeidet i sektoren også dekker risikoen som introduseres ved overgangen til digitale løsninger og tjenester.

Den digitale utviklingen påvirker også samfunnssikkerheten i Norge, ved at kritiske funksjoner eksponeres for nye trusler og farer (NOU 2018:14). Vi fant det derfor av stor interesse å betrakte denne utviklingen gjennom en sektor som forvalter en av våre mest kritiske funksjoner, den norske kraftforsyningen. Denne studien er dermed basert på et ønske om å forstå og skape innsikt i sektorens tolkning og håndtering av cyberrisiko.

1.1 Bakgrunn

I løpet av de siste årene har en rekke offentlige dokumenter og utredninger med fokus på risiko tilknyttet den digitale utviklingen blitt publisert. Det nasjonale søkelyset på digital sikkerhet illustrerer at digitaliseringen kan utfordre samfunnssikkerheten i Norge.

Av Lysneutvalget (NOU 2015:13) ble beskyttelse av enkeltmennesker og samfunn i en digitalisert verden satt på den offentlige dagsorden. I tillegg utfordres kritiske infrastrukturer og samfunnsfunksjoner i deres evne til å håndtere økt kompleksitet som følge av digital utvikling. Utredningen ledet til at Norge i 2017 fikk sin første stortingsmelding som utelukkende omhandler digital sikkerhet, "IKT-sikkerhet – et felles ansvar" (Justis- og beredskapsdepartementet, 2017).

Den digitale utviklingens innvirkning på samfunnets sårbarhet utredes på nytt av Sikkerhetsutvalget i 2016, som konkluderte med at digitaliseringen krever dynamiske og tidsriktige verktøy for kunne håndtere trusler i det digitale rom (NOU 2016:19, s. 11). I 2017 følges anbefalingen opp. Utenriksdepartementet presenterer en internasjonal cyberstrategi for Norge, som redegjør for landets strategiske prioriteringer innenfor internasjonal cyberpolitikk (Utenriksdepartementet, 2017). Regjeringen øker også bevillingene i statsbudsjettet med flere titalls millioner kroner til arbeidet med IKT-sikkerhet i både 2018, 2019 og 2020. Pengene øremerkes håndtering av cybertrusler (Finansdepartementet, 2020). I 2018 fremmer IKT-sikkerhetsutvalget behovet for en egen lov som omhandler IKT-sikkerhet på bakgrunn av endringer i samfunnets risikobilde. Utvalget anbefaler også opprettelsen av et eget IKT-sikkerhetssenter (NOU 2018:14).

Ett år senere opprettes Nasjonalt cybersikkerhetssenter i Oslo, med formål om å gi anbefalinger og rådgivning til offentlige myndigheter og næringsliv (NSM, 2019). Det samme året blir Norge medlem av cybersikkerhetssenteret i Tallinn, med mål om å ta del i det internasjonale samarbeidet om digital sikkerhet og bidra til å tilrettelegge for en felles statlig oppførsel i det digitale rom (Forsvarsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet, 2019). Regjeringen lanserer samme år sin egen strategi for digital sikkerhet, den fjerde i rekken, med den hensikt å gjøre samfunnet bedre rustet til å avdekke og håndtere digitale angrep (Departementene, 2019).

Det nasjonale søkelyset på cybersikkerhet og cybertrusler illustreres også gjennom årlige rapporter fra Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM), hvor begge påpeker at trusler i det digitale rom både er svært sannsynlig og potensielt svært alvorlig. Særlig trekkes digital kartlegging og sabotasje av kritisk infrastruktur frem som de mest alvorlige truslene vi står overfor i året som kommer (PST, 2020). Årets risikorapport fra NSM konstaterer at teknologiutviklingen leder til konstruksjon av lange og komplekse digitale verdikjeder på tvers av og innad i ulike samfunnsfunksjoner og infrastrukturer. I tillegg skriver rapporten at en stor del av trusselaktiviteten mot Norge skjer i digitale domener, hvilket gjør det viktig å forstå implikasjonene som følge av digitaliseringen i samfunnet generelt, og innad i ulike sektorer spesielt (NSM, 2020).

1.2 Problemstilling

Denne studien har en analytisk tilnærming, hvor formålet er å skape innsikt i risikoforståelse og risikohåndtering i sammenheng med digital utvikling. Den norske kraftsektoren er objekt for studiet. Problemstillingen er formulert som følger:

Hvordan forstår og håndterer aktører i den norske kraftforsyningen cyberrisiko som følge av sektorens digitale utvikling?

Det er formulert fire forskningsspørsmål som på hver sin måte skal bidra til besvarelsen av problemstillingen. For å forstå helheten i studien, og et viktig aspekt ved problemstillingen, er det hensiktsmessig å forklare hvordan digitalisering har endret bransjens risikostruktur[1]. Dette har ledet til følgende forskningsspørsmål:

1. På hvilken måte endrer digitaliseringsprosesser kraftforsyningens risikostruktur?

[1] Risikostruktur: henviser til hvordan risiko samspiller med et gitt system og måten det er bygget opp. Systemet det er snakk om i denne studien er den norske kraftforsyningen

Det andre forskningsspørsmålet vil belyse hvordan aktørene i kraftforsyningen oppfatter risikoen for cyberhendelser, med bakgrunn i sektorens digitale utvikling. Risikoen som fremstilles i denne oppgaven er cyberrisiko og kan bestå av tilsiktede og utilsiktede hendelser. Oppgavens andre forskningsspørsmål er formulert som følgende:

2. Hvordan forstås risikoen for cyberhendelser av aktører i kraftforsyningen?

Videre kan det antas at risikovurderinger spiller en rolle i den strategiske håndteringen av bransjens risiko, gjennom kartleggingen av aktuelle farer og trusler som krever sikringstiltak. Tredje forskningsspørsmål har derfor som mål å undersøke hvilke analysemetoder som benyttes i risikovurderingsprosessen relatert til sektorens digitale systemer, samt hvilke farer og trusler som vektlegges i vurderingene. Dette har ledet til følgende formulering:

3. Hvilke metoder benyttes i risikovurderingsprosessen, og hvilke farer og trusler vektlegges?

Organisatoriske betingelser kan tilrettelegge for eller svekke håndteringen av cyberrisiko. For å forstå hvilke organisatoriske betingelser som har betydning, og hvilken betydning de har i arbeidet med cybersikkerhet, lyder det siste forskningsspørsmålet som følger:

4. Hvilke organisatoriske betingelser har betydning for aktørenes evne til å håndtere cyberrisiko?

1.3 Avgrensning

Begrepet digitalisering benyttes ofte som en samlebetegnelse for "overgangen fra analoge, mekaniske og papirbaserte løsninger, prosesser og systemer, til elektroniske og digitale løsninger" (Kommunal- og moderniseringsdepartementet, 2014). Digitalisering innebærer dermed både etableringen av nye IT-systemer og oppgradering av utdaterte og gamle løsninger.

Digitalisering er et omfattende begrep, og vi har derfor valgt å avgrense studien til utvalgte digitaliseringsprosesser i den norske kraftforsyningen. De valgte prosessene er utrulling av avanserte måle- og styringssystemer (AMS), integrering av eksisterende systemer og bruk av skybaserte tjenester. Disse digitaliseringsprosessene utdypes i kapittel 2. Avgrensningen har videre

bidratt til å generere informanter med spisskompetanse innenfor fagfeltet (IKT-sikkerhet i en digital epoke). Den samme avgrensningen har lagt føringer for søk etter relevante dokumenter.

Selv om cybersikkerhet i flere tilfeller må forstås av alle i organisasjonen, er forståelsene som fremkommer i oppgaven tuftet på meningsbærere som har inngående kunnskap på fagområdet. Studiens aktører avgrenses derfor til personer som har en sentral rolle i arbeidet med cybersikkerhet og digitalisering i kraftforsyningen.

Tidligere studier har avdekket at risikoreduserende tiltak ofte er todelt, hvor det skilles mellom organisatoriske og teknologiske sikkerhetstiltak. Denne studien vil avgrenses til de organisatoriske tiltakene, da disse har vist seg å være blant de mest effektive for å kunne hanskes med IKT-sikkerhetsutfordringer (Hagen, Albrechtsen & Hovden, 2008; Røyksund, 2011).

Videre er begrepet risiko forstått i lys av cyberdomenet. Dette vil si at risikoen har en relasjon til digitaliseringsprosessene, ved at den berører elementer (fysiske og ikke-fysiske) som er sårbare gjennom bruk av IKT (informasjons- og kommunikasjonsteknologi). Hva som menes med cyber vil også redegjøres for i kapittel 2.

1.4 Faglig relevans

Norge er et av de mest digitaliserte landene i verden, og har dratt nytte av enorme effektiviseringsgevinster som følge av utviklingen (NOU 2018:14). Samtidig kommuniserer nasjonale sikkerhetsmyndigheter som PST og NSM at utviklingen forårsaker store endringer i samfunnets risikobilde ved at nye farer og trusler introduseres. Slike endringer er sektorovergripende, noe som tilsier at digitaliseringen rokker ved samfunnssikkerheten i Norge (NSM, 2020). Det er derfor hensiktsmessig å avdekke hvilke utfordringer som kan oppstå når samfunnets kritiske funksjoner utsettes for nye farer og trusler. For å møte disse utfordringene med tilstrekkelig og relevant kunnskap er det behov for mer forskning innen feltet. Kritiske infrastrukturer og samfunnsfunksjoner ivaretar noen av de viktigste oppgavene relatert til samfunnets sikkerhet (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016). Problemstillingen er dermed relevant for det samfunnssikkerhetsfaglige miljøet. Teori fra fagfeltet vil bidra til å sette

digital utvikling med tilhørende farer og trusler i kraftforsyningen inn i et samfunnssikkerhetsperspektiv.

1.5 Oppgavens struktur

Gjennom første kapittel er leseren gjort kjent med oppgavens tematikk, problemstilling og avgrensning. Videre struktur for oppgaven er som følger:

Kapittel 2 vil sette de kontekstuelle rammene for oppgaven. Her vil sentrale begreper som cyber- og IKT-sikkerhet presenteres for å gi leseren videre innsikt i tematikken som studeres. I dette kapittelet vil leseren også finne en beskrivelse av involverte aktører og lovverk som er gjeldende og relevante for kraftbransjen i en digital epoke. Kapittel 3 presenterer det teoretiske rammeverket som senere vil benyttes i oppgavens analyse, samt andre relevante studier innen fagfeltet. Kapittel 4 redegjør for metodiske valg som er tatt med hensyn til prosjektets fremgangsmåte, gjennomførelse og kvalitet.

Det empiriske datamaterialet og oppgavens analyse presenteres deretter i kapittel 5. Delkapitlene i denne seksjonen representerer hvert enkelt forskningsspørsmål. Det er verdt å merke seg at valgt struktur innebærer en empirisk fremstilling av datamateriale før funn analyseres opp mot oppgavens teoretiske rammeverk. De fire forskningsspørsmålene besvares i hvert sitt delkapittel etter tilhørende analyse. Ved å velge en slik struktur tilrettelegges det for at leseren fortløpende vil kunne finne svarene på de enkelte forskningsspørsmålene, hvilket vi mener vil få frem helheten på en ryddig måte uten unødvendige gjentakelser.

I tillegg gir denne strukturen mulighet til å gjennomføre en grundig analyse av de ulike funnene som senere skal svare på oppgavens problemstilling. Kapittel 6 er studiens avsluttende kapittel. Her vil sentrale funn legges frem og problemstillingen vil besvares i sin helhet. Avslutningsvis vil det legges frem forslag til videre forskning på temaet.

2.0 Digitalisering og den norske kraftforsyningen

Dette kapittelet vil sette de kontekstuelle rammene for oppgaven. Kraftforsyningens digitale utvikling innleder kapittelet, da hensikten med studien er å skape innsikt i forståelsen og håndteringen av cyberrisiko i den norske kraftforsyningen. Utviklingen skisseres gjennom tre ulike digitaliseringsprosesser, som sammen og separat belyser noe av omfanget av digitaliseringen i bransjen.

Digital utvikling medfører som sagt endringer i risikobildet. Risikobegrepet kobles til cyberdomenet for å vise sammenhengen mellom risiko og digitalisering. Kapittelet vil derfor forklare sentrale begreper som benyttes senere i oppgaven, herunder cyber- og IKT-sikkerhet. Deretter følger en presentasjon av aktører som er involvert i sikkerhetsarbeidet i sektoren. Avslutningsvis presenteres den nylig reviderte Kraftberedskapsforskriften, som legger føringer for sektorens håndtering av risiko.

2.1 Digital utvikling i norsk kraftsektor

Digitalisering er et omfattende begrep. I denne studien viser digitalisering til prosesser hvor digital teknologi implementeres, eller hvor digitale løsninger erstatter tidligere analoge prosesser (Det Norske Veritas, 2019, s. 6). I kraftforsyningen, som i samfunnet forøvrig, ser man en massiv investering i digitale løsninger. Denne teknologien viser seg i form av IKT-systemer og digitale verktøy som benyttes aktivt gjennom hele kraftforsyningens verdikjede. Ved gjennomgang av en rekke offentlige dokumenter var det særlig tre prosesser som utpekte seg i diskusjoner om bransjens digitale sårbarhet. De valgte prosessene, som består av utrullingen av AMS, integrering av eksisterende systemer (SCADA og administrative systemer) og bruk av skybaserte tjenester, vil presenteres i påfølgende avsnitt.

2.1.1 Utrulling av avanserte målesystemer

1. januar 2019 ble nettselskapene pålagt å installere en strømmåler med toveiskommunikasjon hos alle sine strømkunder (NVE, 2017a, s. 20). De avanserte måle- og styringssystemene (AMS) foretar målinger i den enkeltes husstand, og har åpnet for at strømforbruket registreres med en oppløsning på en time eller mindre (NVE, 2018a, s. 7). Utrullingen av AMS er en prosess hvor ny

teknologi har blitt implementert i kraftforsyningens styringssystemer. Systemet støttes gjennom automatiserte prosesser, og gjør det i større grad mulig å fange opp feilsituasjoner i strømnettet (NOU, 2015:13, s. 139). Dette gir nettselskapene en mer nøyaktig informasjon knyttet til status og oversikt i distribusjonsnettet, som igjen bidrar til å bedre forsyningssikkerheten. Samtidig forsterker AMS avhengigheten mellom energi- og ekomsektoren, som gjør at IKT-sikkerhet er blitt sentralt for driftssikkerheten i bransjen (NVE, 2017a, s. 20; NOU 2015:13, s. 129).

Behovet for IKT-sikkerhet forsterkes ved at systemet, og teknologien som understøtter systemet, multipliserer antall flater som er utsatt for angrep og funksjonsfeil. Slike flater representeres ved antall husstander og virksomheter som er tilknyttet systemet. Kompleksiteten forsterkes ytterligere ved at dataoverføringen mellom AMS og Elhub til dels støttes av kommersielle systemer og internett (NOU, 2015:13, s. 140).

2.1.2 Integrering av eksisterende systemer

Kraftforsyningens verdikjede støttes i stor grad av IKT-systemer for drift, overvåkning og fjernstyring, også kalt driftskontrollsystemer (SCADA) (NOU 2015:13, s. 41). Dette er svært komplekse systemer, som benytter datanett til signaloverføring, samt stasjonsdatamaskiner og annet utstyr som oversetter digitale signaler til fysisk handling. Systemene rommer i tillegg driftssentralene, hvor operatører kan fjernstyre systemet basert på sanntidsinformasjon (NOU, 2015:13, s. 129). Tidligere var driftskontrollsystemene helt uavhengige av andre IKT-systemer, noe som har endret seg ved at de stadig knyttes tettere opp mot den administrative delen av selskapene (NOU 2015:13). Administrative systemer defineres av NVE (2017a) som ".. alt som ikke er å betrakte som prosesskontrollsystemer" (s. 31). Dette kan være webservere, mailservere, filservere og skrivere, samt laptoper, smarttelefoner og lignende som er koblet til de ulike serverne gjennom lokale nettverk. Systemene forvalter også store mengder verdifull informasjon og kan potensielt fungere som inngangsport til andre kritiske deler av kraftforsyningen, eksempelvis driftskontrollsystemene (NVE, 2017a, s. 132). Integrasjon av slike systemer er en utvikling som omtales i tråd med digitaliseringsbegrepet, og trekkes frem av Lysneutvalget som en bidragsyter til kraftforsyningens økende kompleksitet (NOU 2015:13, s. 129-136).

2.1.3 Bruk av skybaserte tjenester

En annen digitaliseringstrend er bruk av skytjenester. Skytjenester er i hovedsak tjenester for lagring og prosessering av informasjon over internett, gjerne hos en ekstern aktør (NVE, 2015, s. 35). Andre kjennetegn ved skybaserte løsninger er at de er behovsbaserte, fleksible og ressursorienterte, og gjør det mulig å hente ut informasjon fra internett uavhengig av tid og sted (Kommunal- og moderniseringsdepartementet, 2016, s. 7). I kraftforsyningen kan slike tjenester benyttes til å gi virksomheter et godt bilde av slitasje og belastning i nettet, noe som gjør det enklere å drive vedlikehold. Samtidig kan bruken av dem eksponere kraftforsyningen for nye farer og trusler, ved at sårbarheter kan oppstå over hele tjenestespekteret, det vil si hos leverandører, i kommunikasjonskanaler og egen arkitektur (Borgund, 2014, s. 2). Bruk av slike tjenester representerer derfor en teknologiutvikling som i likhet med ovennevnte prosesser påvirker sektorens kompleksitet.

2.2 IKT- og cybersikkerhet

Cybersikkerhet er et begrep som ofte benyttes synonymt med IKT-sikkerhet. Denne oppgaven tar utgangspunkt i begrepene som synonymer på bakgrunn av diffuse skiller som fremkommer av offentlige klassifiseringer.

Figur 1 Klassifisering av begrepene informasjonssikkerhet, IKT-sikkerhet og cybersikkerhet (tilpasset fra NVE, 2017a, s. 15)

Klassifiseringen viser at IKT- og cybersikkerhet begge omhandler sikkerhet relatert til digitale systemer og tilknyttede elementer. Det til dels uklare skillet mellom begrepene kan illustreres gjennom begrepenes overlappende tendenser (se figur *1*). Hvor IKT-sikkerhet relateres til sikring av IT-systemer i form av fysisk programvare og informasjon, vil cybersikkerhet omhandle både beskyttelse av IKT-systemer og eksterne tilkoblede elementer. Cybersikkerhet viser dermed til beskyttelse av fysiske og ikke-fysiske ting som er sårbare gjennom bruk av IKT (NVE, 2017a). I fellesskap kan derfor cyber- og IKT-sikkerhet forstås som beskyttelse av "alt" som er sårbart fordi det er koblet til eller er avhengig av informasjons- og kommunikasjonsteknologi.

Ifølge Norges vassdrags- og energidirektorat vil sårbarheten til sammenkoblede IKT-systemer alltid representeres ved det svakeste ledd. Man kan derfor argumentere for at cybersikkerhet vil avhenge av sikkerheten til de enkelte delsystemene som kobles sammen (som illustrert ved samhandling mellom administrative systemer og driftskontrollsystemet), hele systemer som AMS, samt andre nettbaserte systemer og deres interaksjon med omverdenen (NVE, 2017a, s. 23).

2.3 Farer og trusler ved digitalisering

Det helhetlige bildet av farer og trusler som følge av digitaliseringen i kraftforsyningen er sammensatt. Det inkluderer menneskelige feil, organisatorisk svikt, systemsvikt og målrettede angrep initiert av mennesker (NVE, 2017a, s. 28-29). Mørketallsundersøkelsen utført av Næringslivets sikkerhetsråd i 2016 viser at kun et fåtall av opplevde angrep anmeldes, og at det sjelden rapporteres om betydelig kostnadstap som følge av hendelsene. Dette indikerer at mørketallene er store, og at digital kriminalitet oppleves som en attraktiv metode for å sabotere eller skaffe seg sensitive opplysninger (NSR; 2016, NVE, 2017a, s. 29). Den samme undersøkelsen fra 2018 viser en økning i antall uønskede hendelser knyttet til informasjonssikkerhet. De vanligste hendelsene omfatter virus, phishing (e-post med infisert vedlegg eller lenke), forsøk på hacking, faktisk hacking, DDoS-angrep (hindre at legitime brukere får tilgang til en tjeneste eller informasjon) og bedrageri (NSR, 2018, s. 4). Motivene for slike angrep er mangfoldige, og kan bestå av å demonstrere ferdigheter, påvise sårbarheter, utøve makt og politisk press, eller økonomisk gevinst. Cyberangrep kan være tilfeldige, ved at aktørene sender ut et virus til mange ulike organisasjoner og slår til der de lykkes med å få tilgang, eller de kan være rettet mot spesifikke mottakere (NOU, 2015:13, s. 54).

Ifølge NSM (2019) og PST (2020) fortsetter cybertrusler rettet mot infrastruktur, demokrati og IKT-systemer å øke. De vurderer det som svært sannsynlig at vi vil oppleve målrettede angrep i 2020, og at spionasje fra fremmed etterretning vil øke i omfang. Digitale systemer innenfor kraftsektoren er å anse som spesielt etterretningsutsatt på bakgrunn av sektorens rolle som kritisk infrastruktur (NVE, 2017a, s. 30).

IKT-hendelser består ikke bare av cybertrusler. Farer i form av utilsiktede hendelser kan også få konsekvenser for sikkerheten. Ekstremvær som storm eller flom kan føre til materielle skader og strømbrudd som følge av trær som faller over høyspentledninger, eller vann som fører til fiberbrudd (NOU 2015:13, s. 52). Andre utilsiktede hendelser kan skyldes ulike typer svikt. Menneskelig svikt kan oppstå som konsekvens av manglende sikkerhetskunnskap eller lav brukervennlighet, men også stress, uoppmerksomhet eller hendelser i privatlivet som påvirker enkeltindividers fokus. Organisatorisk svikt kan innebære at systemer ikke er oppdaterte, eller at virksomheter ikke har oversikt over sine egne verdier og dermed ikke oversikt over hva som bør sikres. Systemsvikt omhandler tekniske feil eller svikt i enkeltkomponenter, som videre kan forplante seg til andre deler av systemet (NOU 2015:13, s. 53). Det samlede risikobildet knyttet til digitaliseringen i kraftbransjen er derfor bredt. Det består av mange ulike cyberfarer og cybertrusler, hvilket betyr at virksomheter og aktører er nødt til å ta hensyn til mange ulike faktorer for å kunne møte, redusere og håndtere de risikoene de står overfor.

2.4 Aktører og ansvar i den norske kraftforsyningen

I arbeidet med sikkerhet og beredskap involveres flere aktører i kraftforsyningen. En overordnet oversikt over risiko og sårbarhet, også relatert til IKT- og cybersikkerhet, skal holdes av myndighetsaktører. I kraftforsyningen representeres myndighetene ved Olje- og energidepartementet. Videre involveres tilsynsmyndigheter, nettselskap, kraftprodusenter, og andre aktører som aktivt vurderer eller håndterer problemstillinger tilknyttet bransjens sikkerhet (NOU 2015:13).

Norges vassdrags- og energidirektorat (NVE) fører tilsyn med sikkerheten og beredskapen i sektoren, og kontrollerer etterlevelse av gjeldende lover og forskrifter hos underlagte enheter

(NOU 2015:13, s. 130). Energibransjen består av selskaper med enerett (nettselskaper) og markedsprodusenter (produsenter av energi, kjøpere og selgere av energi, og andre tredjeparter). Avhengig av størrelse og anleggenes kritikalitet for forsyningssikkerheten, er noen av aktørene pålagt å inngå i kraftforsyningens beredskapsorganisasjon (KBO). Enheter som inngår i KBO er pliktet til å rapportere til NVE dersom de står overfor en situasjon som kan true sikkerheten. Alle enhetene har i tillegg et selvstendig ansvar for å sørge for effektiv sikring og implementering av forebyggende tiltak, samt å begrense og håndtere ekstraordinære situasjoner. Enhetene plikter også å sikre anlegg fra skade som følge av naturhendelser, teknisk svikt, sabotasje, terror, eller andre hendelser relatert til IKT og cybersikkerhet (NVE, 2019a). Kraftforsyningens distriktssjefer (KDS) har en viktig rolle i sikkerhets- og beredskapsarbeidet i sektoren. Distriktssjefene er utpekt av NVE, og skal sørge for godt samarbeid mellom de ulike kraftselskapene. De har ansvar for hver sine distrikter, hvor de skal ha oversikt over vesentlige beredskapsutfordringer, og følge opp disse på en hensiktsmessig måte. Det forventes at de opprettholder jevnlig kontakt med de ulike KBO-enhetene når det gjelder status for beredskapsplaner, ROS-analyser, og eventuelt status i en pågående krisesituasjon. De er dermed også en viktig samarbeidspartner for NVE (NVE, 2019a).

KraftCERT spiller også en sentral rolle i arbeidet tilknyttet IKT- og cybersikkerhet i sektoren, og skal bistå medlemmene med håndtering og forebygging av trusler mot selskapenes systemer (KraftCERT, 2015). Likevel ligger hovedansvaret hos de enkelte selskapene. I tråd med ansvarsprinsippet, hvilket betyr at den virksomheten som til daglig har ansvar for et område, også har ansvaret for nødvendige sikkerhets- og beredskapsforberedelser, og for å håndtere ekstraordinære hendelser (NOU 2015:13). Dermed foregår mye av det viktigste grunnlaget for å kunne håndtere hendelser relatert til IKT- og cybersikkerhet, samt øvrig sikkerhets- og beredskapsarbeid hos virksomheten selv (NOU 2015:13, s. 134).

2.5 Kraftberedskapsforskriften

Endringer i sektorens risiko- og sårbarhetsbilde som følge av digitaliseringen har ført til behov for revidering av tidligere lovverk (NVE, 2019b). 1. januar 2019 trådte derfor Kraftberedskapsforskriften i kraft, med nye og tydelige krav til IKT-sikkerhet.

Den reviderte forskriften om sikkerhet og beredskap (Kraftberedskapsforskriften) skal sikre forsvarlige beredskapsmessige hensyn for at kraftforsyningen skal kunne opprettholde sin funksjonalitet under ekstraordinære påkjenninger. Forskriften er fastsatt av Norges vassdrags- og energidirektorat og bestemmelser er underlagt energilovens overordnede formål fastsatt gjennom forskriftens §1-2 (Kraftberedskapsforskriften, 2012).

Forskriften stiller omfattende krav til IKT-sikkerhet, hvilket tydeliggjøres gjennom forskriftens § 6-9 som stiller særskilte krav til sikring og risikovurdering av digitale informasjonssystemer. Den digitale grunnsikringen innebærer at virksomheter plikter å sikre digitale informasjonssystemer slik at konfidensialitet, integritet og tilgjengelighet ivaretas. Grunnsikringen skal etterleve anerkjente standarder og normer, hvilket tilsier at aktørene må jobbe strukturert med å identifisere og dokumentere potensielle sårbarheter, farer og trusler. Dette skal videre legge føringer for arbeidet med sikring og håndtering av avdekte sikkerhetsutfordringer, slik at evnen til gjenopprettelse etter uønsket påkjenning ivaretas. Videre fastsetter lovverket at ansvaret for sikring ligger hos de enkelte virksomhetene (Kraftberedskapsforskriften, 2012).

3.0 Teori

I dette kapittelet vil det teoretiske rammeverket for oppgaven presenteres. Som illustrert i kapittel 2 har den norske kraftsektoren gjennomgått flere digitaliseringsprosesser, hvilket har ført til økt kompleksitet i bransjen. Charles Perrows teori om normale ulykker vil derfor innlede kapittelet og legge det teoretiske grunnlaget for oppgavens første forskningsspørsmål. Ved å anvende Perrows teori er hensikten å belyse hvordan bransjens risikostruktur endres som følge av teknologisk utvikling.

Den samme utviklingen medfører også nye farer og trusler. Oppgavens andre forskningsspørsmål belyses derfor gjennom ulike teoretiske tilnærminger til risiko og sikkerhet (safety og security). Hensikten med dette er å kunne forklare hvordan potensielle hendelser knyttet til bransjens nye risikostruktur oppfattes av aktørene i sektoren.

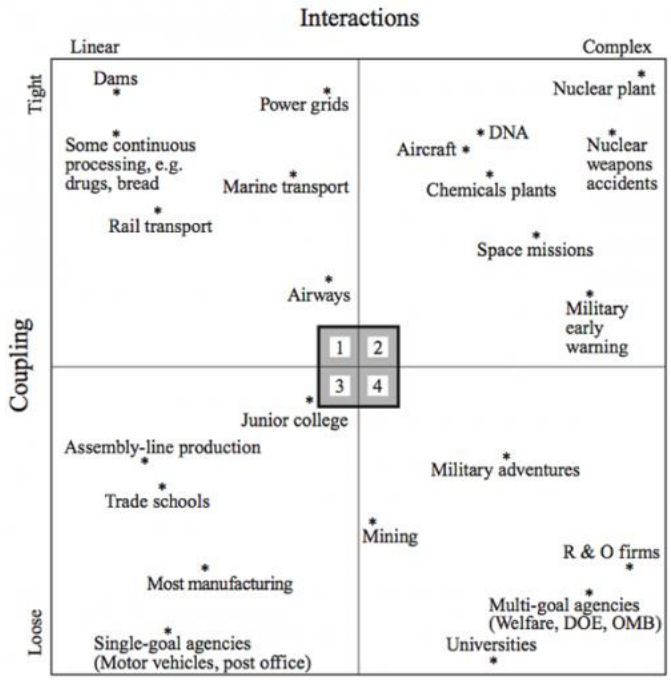
Videre presenteres ulike tilnærminger til risikovurderinger, som antas å spille en rolle i den strategiske håndteringen av risiko. Dette understøtter problemstillingens vektlegging av risikohåndtering, og vil benyttes i besvarelsen av oppgavens tredje forskningsspørsmål. Kapittelet avsluttes med teori om HRO, resiliens og sikkerhetskultur, som alle proklamerer ulike måter å håndtere risiko på. Dette danner grunnlag for å analysere bransjens risikohåndtering fra et organisatorisk ståsted. Valgte teorier er alle veletablerte konsepter og forståelser innen samfunnssikkerhetsfeltet.

3.1 Normal Accident Theory (NAT)

Charles Perrow (1999) mener vår teknologiske utvikling forårsaker høyrisikoteknologier hvor ulykker til dels er uunngåelige og kan betraktes som normale. Den teknologiske utviklingen er særlig relevant for denne studien, og kan betraktes i lys av kraftsektorens pågående digitale utvikling, hvor nye teknologier implementeres og tas i bruk. Ved å studere ulykker relatert til høyrisikoteknologier har Perrow identifisert forhold og karakteristikker som øker risikoen for ulykker. Videre hevder NAT at målet ikke nødvendigvis er å sikre høyteknologiske systemer totalt fra ulykker, men heller å forstå hvordan og hvorfor risikoen for ulykker vokser. I tillegg hevder

teorien at ulykkespotensialet ikke kan reduseres ved hjelp av sikkerhetsmekanismer. Tvert imot vil implementeringen av slike løsninger heller øke systemets kompleksitet og gjøre det enda mer utsatt for ulykker. Selv om vår analyse ikke eksplisitt omhandler ulykker i den norske kraftsektoren, mener vi NAT i stor grad kan overføres til å illustrere hvilke implikasjoner kraftsektorens digitale utvikling har hatt for bransjens risikostruktur. Grunnen til dette er at premissene som illustreres i teorien kan illustrere hvilke følger teknologisk utvikling kan ha for kraftforsyningens systemsammensetning, samt hvordan risiko kan utfolde seg som en følge av slike endringer.

Perrow (1999) skiller i sin teori mellom ulike typer ulykker. En komponentfeil-ulykke viser til uønskede situasjoner forårsaket av svikt i en eller et fåtall komponenter, og fører vanligvis ikke til kritiske situasjoner da de er relativt enkle å hanskes med. Systemulykker er preget av uforventede interaksjoner av svikt i et flertall av komponentene, og er vanskelig å forutse, forstå og håndtere. Disse ulykkene fordrer at systemet er tett koblet, og at graden av kompleksitet i interaksjoner mellom ulike komponenter er høy. I tillegg er det en forutsetning at systemet er preget av avansert teknologi, som alene eller i samspill med mennesker og organisasjon kan forårsake alvorlige ulykker. I tråd med disse premissene skiller Perrow (1999) mellom komplekse og lineære interaksjoner, og tette og løse koblinger. Dersom et system er preget av løse koblinger og lineære interaksjoner hevder NAT at risikoen for alvorlige systemulykker vil være lav, da disse egenskaper gir rom for å håndtere hendelser før de når et alvorlig konsekvenspotensial. Er systemet derimot preget av tette koblinger og komplekse interaksjoner vil sterk tidsavhengighet og lite slakk og buffer føre til at hendelser raskt kan forplante seg videre i systemet, og øke potensialet for å skape alvorlige ulykker (Perrow, 1999).



Figur 2 Interaksjon/koblingskart (Perrow, 1999, s. 97).

I figur *2* er ulike systemer kategorisert etter ovennevnte premisser. Kraftforsyningen kan anses som et relativt høyteknologisk system, og figuren har allerede plassert strømnett (forstått som kraftforsyningen) som et system preget av tette koblinger. Med tanke på at denne kategoriseringen er fra en stund tilbake, kan det argumenteres for at plasseringen ikke lenger er like representativ, særlig om man inkluderer den digitale utviklingen i sektoren. Kraftforsyningen er i dag derfor trolig nærmere figurens høyre ytterpunkt. Den teknologiske utviklingen medfører blant annet at ulike komponenter kobles tettere sammen. Samtidig kan den teknologiske utviklingen føre til at interaksjoner oppstår på nye og uforutsigbare måter, hvilket gjør at en kan se at flere av forutsetningene som ligger til grunn for det Perrow omtaler for systemulykker oppfylles.

3.2 Sårbarhet

Digital utvikling kan i tillegg til å forandre et systems forutsetninger for ulykker, føre til nye og mer avanserte former for sårbarheter. Kraftforsyningen og samfunnet forøvrig, er utsatt for sårbarheter som kan utnyttes av trusselaktører og rammes av uønskede hendelser. I Norsk Standard fra 2012 defineres sårbarhet som en enhets "manglende evne til å motstå en uønsket hendelse eller å opprettholde en stabil tilstand dersom en verdi er utsatt for uønsket påvirkning" (NS 5820:2012, s. 5). Sårbarheter kan utvikle seg over tid, og ligge lenge i et system uten at det legges merke til

(Engen et al., 2016, s. 47). Av Lysneutvalget (NOU 2015:13) påpekes det i sammenheng med sårbarhetsbegrepet at uønsket påvirkning kan bestå av både tilsiktede og utilsiktede handlinger og hendelser, og inkluderer dermed en bred risikoforståelse (s. 31).

3.3 Risiko

Den digitale utviklingen i norsk kraftsektor og samfunnet forøvrig medfører risiko. I denne studien forstås risiko i lys av cyberdomenet, som tidligere nevnt involverer "alt" som er sårbart fordi det er koblet til, eller avhengig av, informasjons- og kommunikasjonsteknologi. Ifølge National Institute of Standards and Technology (2017) viser cyberrisiko til risikoen for finansielt tap, operasjonelle forstyrrelser eller skader forårsaket av svikt i digital teknologi implementert for å støtte informasjon eller operasjonelle funksjoner (NIST, 2017, s. 46).

Risiko trekkes inn i teorikapittelet på bakgrunn av et ønske om å forstå hvilke perspektiver som er fremtredende hos aktørene når de inkluderer cyberkonseptet i risikobegrepet. Risikobegrepet anvendes i analysen for å belyse aktørenes forståelse av risikoen for cyberhendelser med bakgrunn i sektorens digitale utvikling.

Ifølge Aven (2015) kan risiko forstås som kombinasjonen av konsekvenser av en aktivitet og usikkerheten rundt hva disse konsekvensene kan være (s. 42). En slik definisjon viser i stor grad til en situasjon hvor risiko grovt sett forklares gjennom faktorer som sannsynlighet og konsekvens med tilhørende usikkerhet. Omsetter vi dette perspektivet til forståelsen av cyberrisiko, vil cyberrisiko kunne forstås som en prosess hvor informasjons- og kommunikasjonsteknologi, og tilkoblede enheter blir utsatt for uønskede hendelser med konsekvenspotensial, hvor det er usikkerhet tilknyttet både hendelsene og konsekvenspotensialet.

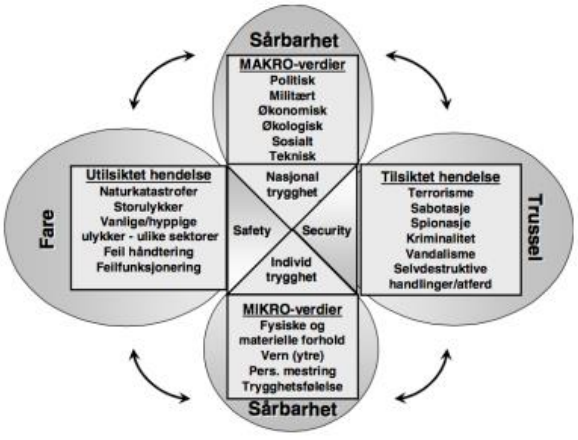
Den teknologiske utviklingen medfører også endringer i kraftforsyningens trusselbilde. En annen tilnærming til risikobegrepet, er derfor å forstå risiko som en kombinasjon av trussel, sårbarhet og verdi, som ofte forbindes med risiko tilknyttet tilsiktede handlinger (Engen et al, 2016). En slik terminologi er blant annet brukt av den internasjonale standarden for risikostyring av informasjonsteknologi, hvor risiko defineres som "potensialet for at en gitt trussel vil utnytte sårbarhetene til et sett av verdier og derigjennom forårsake skade" (ISO 27005:2018, s. 33). Omsatt

i tråd med cyberbegrepet, kan derfor cyberrisiko i et slikt perspektiv knyttes til potensielle trusselaktører og deres kapasitet til å utnytte sårbarheter i digitale systemer, og dermed forårsake skade på gitte verdier.

3.4 Sikkerhet

Sikkerheten som omtales i denne studien er cybersikkerhet, som inkluderer både tekniske, organisatoriske og administrative sikkerhetstiltak. Sikkerhet kan defineres som "den evne et system har til å unngå skader og tap" (Boyesen, Sandve, Olsen, Njå og Aven, 2004, s. 17). Systemene kan bestå av fysiske og sosiale miljøer, som teknologiske systemer og omgivelser, eller menneskelig atferd og beslutninger i organisasjoner. En annen tilnærming til sikkerhet finner vi i Norsk Standard fra 2012 hvor sikkerhet defineres som en "reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare" (NS 5830:2012, s. 4). Sikkerhet kan derfor både forstås som en fysisk tilstand og en sinnstilstand (Stranden, 2019, s. 32).

Hovden (2004) presenterer hvordan begrepet sikkerhet kan brukes om en rekke ulike fenomener, hendelser, situasjoner og tilstander innenfor samtlige arenaer i samfunnet, også kraftforsyningen (s. 40). Omfanget av dette beskrives gjennom figur 3. I figurens horisontale akse ser vi at sikkerhetfeltet dekker alt fra uønskede hendelser som naturkatastrofer, menneskeskapte og teknologirelaterte feilfunksjoner til de overlagte og ondsinnede handlingene som kriminalitet, sabotasje og spionasje (Hovden, 2004, s.40).



Figur 3 Sikkerhet og beredskap - fagfeltes omfang og mangfold (Hovden, 1998, gjengitt i Hovden, 2004).

Cybersikkerhet omfattes også av de samme dimensjonene, og implementering av sikkerhetstiltak vil derfor kunne bestå av respons på alle, eller deler av ovennevnte hendelser. Risiko må derfor forstås gjennom både tilsiktede (security) og utilsiktede (safety) hendelser. Denne situasjonen er også gjeldende for kraftforsyningen, hvor cybersikkerhet kan bety beskyttelse mot både farer og trusler som illustrert gjennom figuren. I tillegg forvalter kraftforsyningen både makro- og mikroverdier, som gjennom digitalisering forflyttes til digitale verdikjeder bestående av både fysiske og ikke-fysiske elementer. Cybersikkerhet kan derfor omsettes til det overordnede kraftsystemet og de delkomponenter som gjør at systemet opprettholder en tilstand med fravær av uønskede hendelser. Dette gjør at delkomponenter, som SCADA, AMS, administrative systemer, skytjenester og andre enheter, som er koblet til eller er avhengig av IKT-løsninger, vil være enheter som individuelt og sammen påvirker et overordnet cybersikkerhetsnivå i bransjen. Tilstanden kan både være reell og oppfattet, eller en kombinasjon av begge. Eksempelvis kan sikkerhetsnivået oppfattes som høyt, men realiteten kan være en helt annen da systemer allerede kan være kompromitterte. Dette kan gjøre at sikkerheten feilberegnes og at det kan oppstå skjulte konfliktsituasjoner mellom reell og oppfattet virkelighet. En slik usikkerhet trekkes frem av Hovden (2004) som hevder at man må arbeide på en måte som gjør at man oppfatter slike misforhold, og at sikkerheten kan korrigeres mot en reell tilstand. Den totale risikoen innebærer derfor at man må vurdere forhold tilknyttet både utilsiktede og tilsiktede uønskede hendelser, som i praksis betyr at man må vurdere sikkerhet både for eksempelvis naturkatastrofer og sabotasje (Hovden, 2004).

3.4.1 Safety og security

Tidligere beskrev vi risiko som et resultat av sannsynlighet og konsekvens med tilhørende usikkerhet, eller som et resultat av trussel, sårbarhet og verdi. Ofte kan en se at sikkerhetsperspektiver sammenfaller med fortolkning av risiko. På engelsk benyttes ofte to ulike ord for å beskrive sikkerhet, hvor “safety” ofte knyttes til risikoen for utilsiktede hendelser, mens “security” henviser til risikoen for tilsiktede handlinger (Engen et al., 2016). De ulike tilnærmingene kan ha betydning for valg av sikkerhetstiltak og utformingen av sikkerhetspolicyer.

Vanligvis refererer vi til security som sikring mot tilsiktede uønskede hendelser, hvor sikkerhetstiltak gjenspeiler identifiserte og potensielle trusler (Stranden, 2019, s. 32; Jore, 2017, s.

2). Sikkerhet gjennom security kan blant annet bestå av beskyttelse mot tap som skyldes tilsiktede menneskelige handlinger. Safety forstås som beskyttelse mot menneskelige og tekniske feil, skade på mennesker og systemer forårsaket av vilkårlige eller uintenderte hendelser, og naturkatastrofer (Jore, 2017, s. 5). Cybersikkerhet vil inkludere elementer både fra safety og security, ettersom forstyrrelser av digitale systemer vil kunne reagere likt uavhengig om forstyrrelsen skyldes en tilsiktet eller utilsiktet handling (Sivertsen, 2007, s. 32; Nilsen, 2019, s. 9). En kan derfor argumentere for at inkluderingen av begge perspektivene vil være viktig for å opprettholde et godt cybersikkerhetsnivå i kraftforsyningen.

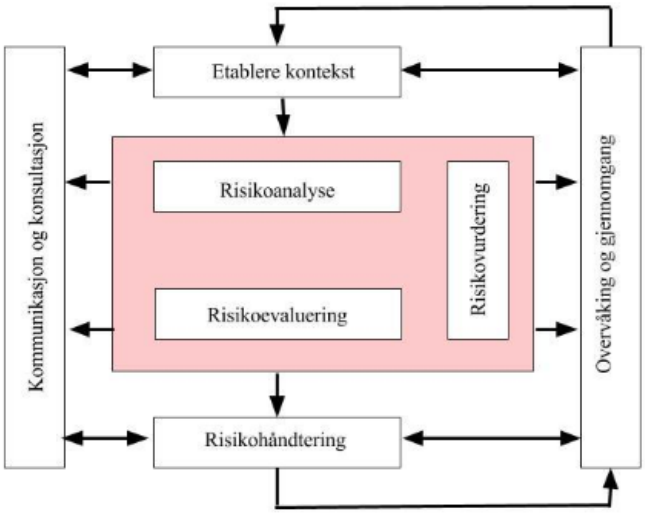
3.5 Risikostyring

En måte å styre risiko på kan forstås gjennom teori om risikostyring. Dette er en viktig oppgave for mange virksomheter, og særlig de som håndterer eller er utsatt for risiko gjennom sine aktiviteter og virkeområder. Risikostyring er også en viktig del av kraftforsyningens oppgaver. Blant annet skisserer Kraftberedskapsforskriftens §2-3 en sentral del av risikostyringsprosessen ved å vektlegge gjennomføringen av risikovurderinger, og at vurderingene må ha mål om å forebygge, håndtere og begrense virkningene av ekstraordinære påkjenninger (Kraftberedskapsforskriften, 2012).

Den helhetlige risikostyringsprosessen viser ifølge Aven til "alle tiltak og aktiviteter som gjøres for å styre risiko" (Aven, 2015, s. 13). Prosessen er todelt, hvor målet på den ene siden er å skape innsikt i risiko, og på den andre siden å påvirke risikoforholdet i ønsket retning. Risikostyringens formål er videre "å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap" (Aven, 2015, s. 14). Digitalisering kan illustrere dette hårfine skillet ved at utviklingen kan tilføre samfunnet verdi gjennom effektiviseringsmuligheter, samtidig som den samme teknologien åpner opp for nye farer, trusler og sårbarheter gjennom økt kompleksitet. I det følgende vil vi gjennomgå det teoretiske utgangspunktet for risikovurderinger, som er en av to hovedprinsipper i risikostyringsprosessen. Risikohåndtering, som er den andre, vil senere presenteres med utgangspunkt i organisasjonsteori knyttet til sikkerhetsdisiplinen.

3.5.1 Risikovurdering

Ifølge Aven (2015) og Rausand (2011) viser risikovurderingsprosessen til totaliteten av analyse og evaluering (Aven, 2015, s. 15), og starter som regel med en risikoanalyse hvor man bruker tilgjengelig informasjon til å identifisere risiko tilknyttet den aktuelle aktiviteten (Rausand, 2011, s. 7). Ofte benyttes en sannsynlighet og konsekvenstilnærming i analysene, som kan bestå av fareidentifikasjon, årsaks- og frekvensanalyse, og konsekvensanalyse. Risikoevalueringen er neste steg av risikovurderingen, og viser til prosessen hvor beslutninger fattes basert på informasjonen som fremkommer i risikoanalysene (Aven, 2015; Rausand, 2011). Figuren under viser gangen i den helhetlige risikostyringsprosessen, og fremhever risikovurderingens plass i den helhetlige styringsprosessen (Aven, 2015).



Figur 4 Risikostyringsprosess (Aven, 2015, s. 15).

NVE ga i 2010 ut en veileder for risiko og sårbarhetsanalyse i kraftbransjen som bygger på tilsvarende prinsipper. Her anbefales blant annet en strukturert grovanalyse i gjennomføringen av ROS-analyser på overordnet nivå. For mer detaljerte nivåer, som ved analyse av delsystemer eller komponenter, anbefales feiltre- og hendelsestreanalyse (NVE, 2010, s. 16). Sentrale deler av analysen består av kartlegging av farer, trusler og uønskede hendelser, hvor resultatene tas videre inn i en vurdering av hendelsenes årsak, sannsynlighet og konsekvens (NVE, 2010).

En prosess som benytter sannsynlighet og konsekvens i beregning av risiko kan også kalles en tofaktormodell, og tar som regel utgangspunkt i tilgjengelig informasjon (Busmundrud, Maal, Kiran & Endregard, 2015). Når det gjelder tilsiktede handlinger, kan et slikt datagrunnlag være vanskelig å fremdrive. Mennesker med onde hensikter kan i større grad kalkulere mønstre og angrepsmetoder med mål om å forårsake mest mulig skade. En risikovurdering basert på en tofaktormodell kan derfor være utilstrekkelig ved aktiviteter og situasjoner som er utsatt for både tilsiktede og utilsiktede handlinger, noe vi tidligere nevnte kan være tilfellet ved forstyrrelser av digitale systemer (Sivertsen, 2007).

3.5.2 Sikringsrisikovurdering

En annen tilnærming til risikovurderinger ser vi i trefaktormodellen. Trefaktormodellen inkluderer en verdivurdering, trusselvurdering og sårbarhetsvurdering, hvor fellesskapet viser til et antatt risikonivå tilknyttet sektoren under analyse (Busmundrud et al., 2015, s. 32). Denne tilnærmingen sammenfaller med hvordan vi tidligere forklarte risiko som et produkt av trussel, sårbarhet og verdi, og omtales som en sikringsrisikovurdering. Metoden benyttes ofte i vurderingen av risiko for tilsiktede hendelser, selv om også farer (utilsiktede hendelser) kan omsettes i sikringsrisikovurderingen (Engen et al., 2016). Tilnærmingen er gjenkjennelig i tilleggsveilederen til den nye Kraftberedskapsforskriften som trådte i kraft i 2019. Selv om veilederen henviser til metoder som sammenfaller med en vurdering av risiko gjennom sannsynlighet og konsekvens, fremmer veilederen at analyser for tilsiktede hendelser kan og bør baseres på andre metoder. For å vurdere risikoen for slike hendelser anbefaler veilederen at analyser bør baseres på en kvalitativ kunnskapsbasert vurdering, og inkludere en kartlegging av verdier, trusler og sårbarheter, samt en subjektiv vurdering av tilhørende usikkerhet (NVE, 2018b, s. 28).

Figur 5 Risikotrekanten - visualisering av total risiko i henhold til trefaktormodellen (Busmundrud et al, 2015, s. 34).

Som digitaliseringen illustrerer, vil påvirkning forårsaket av både tilsiktede og utilsiktede hendelser kunne lede til uønskede konsekvenser, og en kan derfor argumentere for at risikovurderingen i kraftforsyningen må ta høyde for begge former for uønsket påvirkning.

3.6 Sikkerhet i organisasjoner

Som nevnt kan risikostyringsprosessen anses som et todelt forhold, bestående av risikovurdering og risikohåndtering. Risikohåndteringen innebærer de strategier som benyttes for å redusere, overføre eller stå støtt i å møte risikoen man har avdekket i risikovurderingene (Aven, 2015, s. 15). Strategiene for håndtering har sammenheng med hvordan man fokuserer på sikkerhet i organisasjoner. I denne seksjonen vil vi derfor belyse hvordan cyberrisiko som følge av digitalisering kan håndteres gjennom ulike organisatoriske strukturer og mekanismer.

3.6.1 Høypålitelige organisasjoner (high reliability organizations)

I kapittel 2 nevnte vi at digitaliseringen påvirker kraftforsyningens kompleksitet. Det kan tyde på at sektoren står overfor en rekke utfordringer tilknyttet sikkerhetsstyring og risikohåndtering som følge av slike endringer. Teorien om HRT (high reliability theory) proklamerer at komplekse og risikofylte miljøer kan håndteres ved å organisere seg etter betingelser som fremmer sterk ytelseskraft (Weick, Sutcliffe & Obstfeld, 1999, s. 33). Organisasjoner som fremmer slike krav til ytelse er i teorien omtalt som HROer (high reliability organizations), som på tross av sin komplekse og utsatte natur er i stand til å operere feilfritt under dynamiske og krevende forhold. HROer kjennetegnes ved deres tydelige og veldefinerte mål, driften er preget av avansert teknologi, og det er høy grad av avhengighet mellom ulike funksjoner i organisasjonene (La Porte, 1996).

Rosness et al. (2010) nevner særlig tre egenskaper som utpeker seg i organisasjoner med høy grad av pålitelighet. Blant disse finner vi organisatorisk redundans, evne til spontan omstilling og mindfulness (årvåkenhet). Organisatorisk redundans defineres gjennom en strukturell og en kulturell dimensjon. Den strukturelle dimensjonen viser til hvordan arbeidsoppgaver og ansvarsforhold er fordelt i organisasjonen, og består av fokus på gjensidig observasjon, overlappende kompetanse, ansvar og arbeidsoppgaver. Den kulturelle dimensjonen består av informasjonsdeling, intern villighet til å motta beskjeder, og evnen til å omstille seg nye beslutninger og prosedyrer (s. 58). Spontan omstilling viser til evnen til å raskt kunne endre organisasjonens hierarkiske strukturer, som kan bety å gå fra sentralisert til desentralisert beslutningstaking. Dette kan være særlig viktig ved cyberhendelser da angrep raskt kan forplante seg i organisasjoners digitale systemer. Den siste sentrale egenskapen er mindfulness, som viser til en føre-var tankegang. Det handler med andre ord om å tilrettelegge for å fokusere på oppdagelsen av mulige feil og forvente det uforutsette, noe som kan forstås som evne til å være årvåken overfor fremtidige hendelser (Rosness et al., 2010; Weick, Sutcliffe & Obstfeld, 1999).

3.6.2 Sikkerhetskultur

Sikkerhetskultur omhandler hvordan sikkerhet prioriteres i organisasjoner.

Kraftforsyningen består av mange aktører, både store og små, interne og eksterne. Med digitalisering kan en se at sektoren må forholde seg til nye farer, trusler og sårbarheter som gjør at sikkerhet tilknyttet teknologisk utvikling må prioriteres på alle nivå. Reason (2016) viser til hvordan sikkerhetskultur bør inkludere alle involverte aktører og øke fokus på sikkerhet gjennom samhandling i organisasjoner. Sikkerhetskultur innebærer at alle i organisasjonen og tilhørende aktører har delte verdier, tro, oppfatning og normer om hva som er viktig (Reason, 2016, s. 192). Dette er spesielt viktig i forbindelse med cybersikkerhet, da det er sentralt at alle som interagerer med systemene har en felles forståelse for farene og truslene som kan utfordre sikkerheten. "Organisasjoner som har en positiv sikkerhetskultur er kjennetegnet ved en kommunikasjon bygget på gjensidig tillit, felles oppfatning om betydningen av sikkerhet, og med tiltro til at organisasjoners sikkerhetsmål fungerer effektivt" (s. 194). Et annet sentralt begrep i denne sammenheng er *informert kultur*, som innebærer at virksomheter må ha tilrettelagte strukturer for

rapportering, fremme rettferdighet, være fleksible og lære av hverandre og tidligere hendelser (Reason, 2016).

3.6.3 Resiliens

Resiliens beskrives som organisasjoners evne til å lære og til å ha en proaktiv tilnærming som fokuserer på evnen til tilpasning ved utfordrende og skiftende forhold (Hollnagel, 2017s. 402). Med andre ord vil en resilient virksomhet evne å opprettholde en viss funksjonalitet ved kritiske sikkerhetshendelser, samt gjenopprette sin virksomhet ved forstyrrelsens slutt (t'Hart & Sundelius, 2013). Betingelser som fremmer resiliens integreres til stadighet i virksomheter, og konseptet er også overført til cyberdomenet. Cyberresiliens består av organisasjonsstrategier hvor man søker å bygge motstandsdyktige og fleksible løsninger for å håndtere farer og trusler over digitale flater (Dickson & Goodwin, 2019).

Resiliente virksomheter kan også kjennetegnes gjennom deres proaktive og reaktive strategier, og den pågående læringsspiralen som hele tiden sikter mot å forbedre evnen til risikohåndtering. Nøkkelprinsipper i denne sammenheng er evnen til aktsomhet, overvåkning av prosesser, kontinuerlig læring og evnen til respons. Prinsippene må gjenkjennes på alle nivåene i en organisasjon, fra individnivå til bedriftsnivå, og særlig på ledelsesnivå (Hollnagel, 2017, s. 402). Resiliens viser dermed til en tankegang hvor en ikke kan akseptere at kriser kun håndteres når de oppstår, men må forebygges gjennom tilrettelegging.

Digitalisering er en pågående prosess, hvor nye løsninger integreres i systemers operasjonelle miljø. Denne dynamiske utviklingen kan tilsi at responsmekanismer må evne å takle fleksible og uforutsette hendelser, og man kan dermed argumentere for at strategier tilknyttet resiliens vil være gode motsvar til utfordringene som følger av den digitale utviklingen.

3.7 Andre relevante studier

Andre relevante studier innen feltet (kraftforsyningen og cybersikkerhet) viser at det kan se ut til å være korrelasjon mellom opplevde hendelser og hvordan man tolker risiko (Røyksund, 2011). Som en del av et større forskningsprosjekt, har Skotnes (2015) undersøkt en rekke andre problemstillinger knyttet til IKT-sikkerhet (safety og security) i norske nettselskaper. Artikkelen

fra 2015 gir innsikt i faktorer som påvirker ledere og ansattes risikopersepsjon. Resultatet fra undersøkelsen viste at risiko knyttet til angrep på, eller funksjonsfeil ved systemene var ansett som lav av representanter fra norske nettselskap. Faktorer som påvirket dette var erfaring med angrep og farer, kompleksiteten i IKT-systemene og manglende kommunikasjon mellom subkulturer. Det trekkes også frem at tilliten til systemene og tilbyderne av systemene er høy, og at aktører kan ta for gitt at sikkerheten tilknyttet disse systemene er ivaretatt av tredjeparten (Skotnes, 2015).

Eirik Albrechtsen (2008) har i forbindelse med sin doktorgradsavhandling gjennomført en rekke studier tilknyttet informasjonssikkerhet. Disse er ikke direkte knyttet til kraftforsyningen, men resultatene gir likevel innsikt i hvordan organisasjoner generelt håndterer risiko og informasjonssikkerhet. Blant relevante funn finner vi at en økning av arbeidsoppgaver knyttet til informasjonssikkerhet skaper interessekonflikt mellom sikkerhet og effektivitet i arbeidshverdagen. Studiene viser også at det er et gap mellom sikkerhetsledere og øvrige ansattes risikoforståelse. Gapet viser et behov for å skape en felles forståelse for sikkerhetsarbeidet som foregår i den skarpe enden, og på denne måten involvere alle ansatte, og ikke bare de som har sikkerhet som sin eneste arbeidsoppgave (Albrechtsen, 2008). Albrechtsen og Hovden (2007) påpeker at det parallelt med den teknologiske revolusjonen er et behov for tilsvarende IKT-sikkerhet, integritet og konfidensialitet på alle områder i dagens samfunn. Tidligere har IKT-sikkerhet hatt hovedfokus på tekniske sårbarheter og feil, og menneskelige feilhandlinger har vært ansett som tilsiktede og ondsinnede. Utilsiktede handlinger har tidligere fått lite fokus (Albrechtsen & Hovden, 2007). I forbindelse med et annet forskningsprosjekt har Hagen, Albrechtsen & Hovden (2008) undersøkt effektiviteten til ulike informasjonssikkerhetstiltak. Gjennom studiet kom det frem at organisasjoner i stor grad benyttet teknisk-administrative sikkerhetstiltak i form av sikkerhetspolicyer, prosedyrer og metoder, og i liten grad bevisstgjørende tiltak. Likevel var det paradoksalt nok de bevisstgjørende tiltakene som var ansett som mest effektive (Hagen, et al., 2008).

I dag har den digitale utviklingen kommet mye lenger, og blitt viet mye oppmerksomhet i de senere årene. Det kan være interessant å se om funnene til Røyksund fortsatt er gjeldende når det kommer til korrelasjonen mellom opplevde hendelser og tolkning av risiko. Vi er også nysgjerrige på om IKT-sikkerheten i kraftbransjen i dag tilsvarer nivået på digitaliseringen, og hvilke farer og trusler som nå har størst fokus hos aktørene.

4.0 Metode

I dette kapittelet gjør vi rede for oppgavens metodiske valg. Et kvalitativt forskningsprosjekt må følge visse krav for å kunne oppnå den nødvendige strengheten som kreves for å sikre kvaliteten i prosjektet. Dette innebærer blant annet en beskrivelse av de metodiske valgene, og av hvordan datamaterialet er hentet inn og analysert. I tillegg er det viktig å være bevisst på metodens styrker og svakheter (Sovacool, Axsen & Sorell, 2018, s. 26-27).

I det følgende vil leseren finne en oversikt over studiens forskningsdesign, strategi, og forskningsprosess. Vi vil også gjøre rede for og begrunne de metodiske valgene som er gjort i henhold til datainnsamling, dataanalyse, kvalitetskriterier og forskningsetikk. Kapittelet avsluttes med en seksjon som reflekterer over styrker og svakheter ved valgte metoder.

4.1 Forskningsdesign

Forskningsdesignet viser til den helhetlige forskningsprosessen, og inkluderer valg tilknyttet den aktuelle tematikken samt hvordan man ønsker å gå frem ved undersøkelse av studiens problemstilling. Studien har et eksplorerende design, hvor hensikten er å utforske mulige sammenhenger (Hellevik, 2002, s. 36). I dette tilfellet ønsker vi å skape innsikt i hvordan sentrale aktører forstår og håndterer cyberrisiko i lys av kraftforsyningens digitale utvikling.

For å oppnå dette har vi valgt å vektlegge sosiale aktørers forståelse av verden, hvilket sammenfaller med hva Blaikie og Priest omtaler som den abduktive forskningsstrategien (Blaikie & Priest, 2019, s. 99). Ved en abduktiv tilnærming er målet å se etter mulige sammenhenger og slutninger mellom ulike fenomener. Den abduktive forskningen har ikke som mål å generalisere, men heller å skape ny innsikt i allerede etablerte fenomener. Ved å benytte denne strategien kan vi i tråd med studiens formål skape bevissthet rundt mulige sammenhenger heller enn gitte sannheter. Den abduktive strategien tilrettelegger også for å forstå et fenomen i lys av nye kontekster og rammer. Dette gjøres ved å plassere fenomenet (digital utvikling i norsk kraftsektor) inn i et samfunnssikkerhetsperspektiv (Danermark, Ekstöm, Jacobsen & Karlsson, 2002, s. 90-91).

I tråd med studiens hensikt og den abduktive strategien, har vi vurdert en kvalitativ fremgangsmåte som best egnet. Den kvalitative forskningsmetoden innebærer en beskrivelse av virkeligheten gjennom et relativt begrenset utvalg, hvor formålet er å gå i dybden heller enn i bredden (Ringdal, 2013). Basert på dokumentanalyser og intervjuer med informanter vil vi gjennom en kvalitativ datainnsamling bedre kunne illustrere og forklare hvordan teknologisk utvikling i kraftbransjen påvirker forståelsen og arbeidet med cybersikkerhet.

4.2 Forskningsprosess

Forskningsprosessen ble igangsatt i januar 2020. Etter utarbeidelse av prosjektskisse påbegynte vi arbeidet med å innhente relevant bakgrunnsinformasjon. Problemstilling og forskningsspørsmål ble utarbeidet tidlig, selv om disse har vært revidert gjentatte ganger gjennom forskningsprosessen. I løpet av de første ukene ble utkast til kapitlene om bakgrunn, kontekst, faglig relevans og tidligere forskning skrevet. Potensielle informanter ble kartlagt og deretter kontaktet, og en mal for intervjuguider ble utformet. Disse ble senere justert og tilpasset informantene. Intervjuene ble gjennomført i mars og april måned. Transkribering av intervjuer og dokumentanalyser ble gjennomført parallelt. Etter innhenting av relevant empiri ble resten av oppgaven skrevet. Forskningsprosjektet ble ferdigstilt den 15. juni 2020.

4.3 Datainnsamling

Datamaterialet i denne studien er todelt, og består av dokumentanalyse og kvalitative intervjuer. Dokumentene er analysert både i forkant, parallelt med, og i etterkant av intervjuene. I tillegg til å være et hjelpemiddel i arbeidets innledende fase, har utvalgte dokumenter bidratt til oppgavens empiriske datamateriale. Selv om dokumenter har vært viktige i oppgavens empiriske fremstilling, hviler hovedvekten av empirien på kvalitative intervjuer. Intervjuer har vært hensiktsmessig i den forstand at det er aktørene i de ulike selskapene som må håndtere utfordringene tilknyttet cybersikkerhet i det daglige. I praksis har data bestått av et mindre utvalg informanter, rapporter, veiledere og offentlige dokumenter.

Det har vært vår oppgave som forskere å kommunisere informantenes opplevelser og meninger, selv når ulikheter i forståelse og meninger tyder på at oppfatninger ikke kan tolkes som objektivt

korrekte. En kombinasjon av dokumentanalyse og informantintervjuer har vært fordelaktig, ved at primærdata og sekundærdata har kunnet utfylle hverandre.

4.3.1 Utvalg

Utvalget i oppgaven er strategisk valgt, med bakgrunn i hvilken kunnskap som var nødvendig å innhente og hvor denne kunnskapen var lokalisert. Ettersom utvalget vil påvirke studiens kvalitet var kravet til informantene at de måtte ha kunnskap og innsideinformasjon om deres fagfelt som kunne kobles opp mot cybersikkerhet, IKT, digitalisering og sikkerhet. På denne måten sikres det at utvalget er representativt for å kunne besvare problemstillingen.

Totalt ble det gjennomført åtte dybdeintervjuer. Utvalget kan betraktes som lite sammenlignet med kraftsektorens størrelse. Likevel er utvalgets kvalitet sikret gjennom variasjon i informantenes sammensetning, slik at ulike aktører i sektoren er inkludert. Begrensningen er også gjort på bakgrunn av dybdeintervjuenes varighet. Et stort og omfattende datamateriale kan være utfordrende å håndtere når det kommer til å trekke ut relevant informasjon.

Ved 7 av 8 tilfeller var utvalget definert etter hva Blaikie og Priest (2019) omtaler som selektive og forhåndsbestemte strategier, som sikrer at utvalget er representativt for studiens formål. Den siste informanten ble innhentet etter snøballmetoden, ettersom informant 7 henviste til ytterligere en aktør som viste seg hensiktsmessig å inkludere. Utvalget består totalt av 6 informanter fra konsern, kraftprodusenter og nettselskap og 2 informanter som involveres i selskapene gjennom tilsyn og håndtering av sikkerhetshendelser på overordnet nivå (tilsynsmyndighet og leverandør). Felles for utvalget er at informantene arbeider tett med, og er engasjert i sikkerhet, IKT og digitalisering ved de respektive selskapene og organisasjonene. Utvalget anses videre som relevant og tilstrekkelig basert på informantenes variasjon når det kommer til rollebeskrivelse internt, og selskapenes variasjon eksternt. Utvalget kan dermed forventes å gi et tilstrekkelig bilde av hvordan aktørene forstår og håndterer cyberrisiko.

Informantene i utvalget ble rekruttert gjennom direkte kontakt med selskapene. Da kontaktinformasjon til ansatte i kraftbransjen i noen tilfeller kan betraktes som kraftsensitivt, var vi nødt til å henvende forespørsel om intervju gjennom selskapenes postmail.

4.3.2 Intervjuer

Intervjuene ble gjennomført i mars og april 2020. I forkant av hvert intervju ble det utformet en intervjuguide. En del av spørsmålene er stilt alle informantene. På den måten kunne vi se etter fellestrekk og trender. I tillegg ble deler av hver intervjuguide tilpasset den enkelte informant, da disse har ulik kunnskap og ulikt grunnlag for å kunne gi informasjon knyttet til forskningsspørsmålene. Intervjuguiden ble sendt til informanten i forkant av intervjuet.

Alle intervjuer ble gjennomført via digitale løsninger som Teams eller Zoom. Bakgrunnen for dette var myndighetspålagte restriksjoner knyttet til reisevirksomhet, fysiske møter og bruk av kontorlokaler utenfor hjemmet som følge av Covid-19. Da fysiske møter ikke var mulig, var videokonferanse den nest beste løsningen, og fungerte godt. Videokonferanse gir fortsatt mulighet for å danne et helhetlig inntrykk av informanten og informasjonen som blir gitt, gjennom bruk av kroppsspråk, ansiktsuttrykk og tonefall, selv om dette vil reduseres noe sammenlignet med fysiske møter. Vi opplevde også at informantene var fornøyde med denne løsningen, og at samtalen foregikk på en naturlig og avslappet måte.

Ved første intervju opplevde vi at intervjuguiden var mer spesifikk og strukturert enn hensiktsmessig, og reduserte samtaleflyten og informantenes mulighet til å reflektere. Dette vil utdypes videre i kapittel 4.7 om metodiske styrker og svakheter. Opplevelsen ledet til en grundig gjennomgang av intervjuguiden i forkant av neste intervju, hvor noen av spørsmålene ble åpnet og andre kuttet. Etter redigeringen opplevde vi en betydelig endring i samtaleflyt og informantenes egne refleksjoner rundt spørsmålenes tematikk. Det førte også til en mer semi-strukturert intervjusituasjon, hvor muligheten til å stille oppfølgingsspørsmål ble større. Overgangen til en semi-strukturert intervjuform førte også til at intervjuene ble lenger (45-90 minutter). Vi opplevde dette som positivt og fordelaktig for både informanten og oss, da det for vår del ledet til en større mengde nyttig informasjon, og for informantenes del ved at vedkommende fikk snakket ferdig om temaer som engasjerte dem.

4.3.3 Dokumenter

Dokumentanalysen har inkludert nasjonale dokumenter og rapporter. De fleste dokumentene er utgitt av NVE, og omhandler digitalisering og IKT sikkerhet i bransjen. Totalt har 9 dokumenter dannet grunnlag for den empiriske dokumentanalysen.

For å systematisere data og få oversikt over rapportenes innholdsverdi, har vi benyttet søkeord tilknyttet studiets problemstilling. Blant flere er søkeord som "risiko", "digitalisering", "cybersikkerhet", "IKT-sikkerhet", "AMS", "SCADA", "administrative systemer", "skytjenester", "farer" og "trusler" benyttet. En slik strategi har også bidratt til å systematisere og trekke ut relevant data for å besvare studiens forskningsspørsmål. Oversikt over dokumentene som er inkludert i dokumentanalysen finnes i vedlegg 1.

4.4 Dataanalyse

Gjennom analysen av datamaterialet har vi hatt fokus på å hente ut relevant og viktig informasjon. Intervjuene resulterte i 82 sider med transkribert tekst. Vi gjorde oss godt kjent med innholdet i teksten gjennom transkriberingsprosessen. Dette har vi gjort ved hjelp av en grundig gjennomgang, hvor vi har samlet og kategorisert informasjonen under de enkelte spørsmålene i intervjuguiden. Deretter har vi knyttet de ulike kategoriene opp mot hvert av de fire forskningsspørsmålene i oppgaven. På denne måten har både fellestrekk og forskjeller mellom informantene blitt synlige.

Dokumentanalysen er gjennomført på samme måte, ved at vi har markert og kopiert relevante poenger, og plassert de i tilhørende forskningsspørsmål på lik linje som de transkriberte intervjuene. Å kategorisere datamaterialet på denne måten har vist seg å være svært nyttig, da det ga en veldig god oversikt før datamaterialet ble skrevet ut i sin helhet.

4.5 Kvalitetskriterier

I både kvantitative og kvalitative studier benyttes kriterier for å vurdere studiets kvalitet, og ofte benyttes validitet (intern og ekstern) og reliabilitet i denne sammenheng (Lincoln & Guba, 1985). I denne studien har vi derimot valgt kriteriene pålitelighet (reliabilitet), gyldighet, bekreftbarhet og overførbarhet på bakgrunn av studiens kvalitative tilnærming.

4.5.1 Pålitelighet

Reliabilitet viser til forskningens pålitelighet, som betyr at en studie med tilsvarende måleinstrumenter vil gi et tilsvarende resultat (Yin, 2018). I denne studien har vi valgt å vektlegge kravene til anonymitet tyngre enn kravene til etterprøvbarhet. Derimot er transparens etterstrebet ved at intervjuguiden er vedlagt og at dokumenter er offentlig tilgjengelige. En annen relevant problemstilling tilknyttet etterprøvbarhet, er at det er rimelig å anta at kraftsektoren vil stå overfor betydelige endringer når det kommer til bransjens pågående digitalisering og utviklingens innvirkning på sikkerheten i bransjen. Dette kan forårsake at aktører endrer forståelse for studiens fenomen ved at kunnskapen utvikler seg. Påliteligheten er derfor etterstrebet ved å fremme konsistente funn hos involverte aktører, og deretter skape en reell sammenheng mellom empiriske funn, analyser og resultater (Tjora, 2012). Dette er sikret gjennom veiledning av fageksperter og informantenes godkjenning av datamateriale der dette har vært etterspurt.

4.5.2 Gyldighet

Studiens gyldighet handler om hvorvidt datamateriale har en klar sammenheng og besvarer oppgavens problemstilling og forskningsspørsmål (Tjora, 2012). Vi opplevde at problemstilling og forskningsspørsmål ved flere anledninger krevde justeringer ettersom vi tilegnet oss mer kunnskap. Selv om ordlyd og oppbygging ved flere anledninger har blitt endret, har substansen i spørsmålene bestått. Denne substansen har også blitt brukt til utforming av intervjuguider som har vist seg å være dekkende for besvarelse av problemstilling og forskningsspørsmål.

Gyldigheten kan også sikres gjennom datasikring (Yin, 2018). Alle informantene ble gitt retten til å godkjenne tekst basert på sine sitater og utsagn, hvor en av informantene ønsket å benytte seg av dette tilbudet. Ved en slik avtale er informantene gitt retten til å sikre at datamaterialet er korrekt presentert. En kan argumentere for at studiens gyldighet ville økt dersom alle informantene tok i bruk retten til å godkjenne datamaterialet. Vi har likevel vært oppmerksom på våre egne antakelser og subjektivitet, og har etterstrebet en nøytral og objektiv presentasjon av informantenes uttalelser.

4.5.3 Bekreftbarhet

Studiens bekreftbarhet sikres gjennom at forskeren er kritisk til egne tolkninger, og bevisst på at ens egen forutinntatthet kan ha påvirket resultatene (Lincoln & Guba, 1985). Vi hadde i forkant av

datainnsamlingen gjort oss noen tanker om hva vi kunne komme til å finne. Likevel er bekreftbarheten forsøkt sikret gjennom å la informantene fortelle sine egne oppfatninger omkring oppgavens tematikk. At mange har lignende svar, styrker oppfatningen om at funnene er konsistente. Samtidig har vi vært bevisste på å også inkludere funn som skiller seg ut, og som kan balansere resultatene. På denne måten sikrer vi at vi ikke kun leter etter ønsket resultat, men inkluderer alle relevante funn.

4.5.4 Overførbarhet

Overførbarhet handler innen kvalitativ forskning om muligheten for å kunne fastslå om funnene er anvendbare i andre sammenhenger og kontekster. Målet er å tilrettelegge for at leseren skal få nok informasjon til å forstå datamaterialet, og selv kunne avgjøre i hvilken grad resultatene kan være overførbare (Lincoln & Guba, 1985). Om funnene i dette forskningsprosjektet kan overføres til andre sektorer er vanskelig å si med sikkerhet. Det er likevel nærliggende å tro at alle bransjer som i en eller annen form går gjennom en digital utvikling vil kunne gjenkjenne og dra nytte av funnene som fremkommer av forskningen.

4.6 Etiske vurderinger

I ethvert forskningsprosjekt er det behov for å gjøre etiske vurderinger både i forkant av og underveis i et prosjekt (Blaikie & Priest, 2019). I dette tilfellet har de etiske vurderingene i størst grad omhandlet informantenes rett til beskyttelse av sin identitet, sine meninger, holdninger og utsagn. Brudd på personvernreglene kan, i tillegg til at det krenker individet, få følger for den aktuelle virksomhetens sikkerhet. I tråd med de nye reglene for personvern meldte vi prosjektet til Norsk senter for forskningsdata (NSD) i januar 2020, hvor vi beskrev hvilke metoder vi skulle ta i bruk, og hvordan data skulle oppbevares og benyttes. Prosjektet ble kort tid etter godkjent, og vi har vært bevisste på å handle i tråd med NSDs retningslinjer gjennom hele perioden. Når det kommer til forskningsetikk i kvalitative intervjuer har vi vurdert fire etiske problemstillinger i tråd med hva Qu & Dumay (2011) hevder er viktige kriterier for etisk forskning. Kriteriene samsvarer godt med kravene fra NSD, og har hjulpet oss med å være bevisst på etiske avveininger gjennom forskningsprosessen.

Intervjuobjektet skal delta frivillig. Vedkommende skal være informert om hvordan dataene blir brukt, hvilken rolle vi har som forskere i det aktuelle prosjektet, og hvilken risiko deltakelse kan føre med seg (Qu & Dumay, 2011, s. 252). Dette er ivaretatt ved å sende ut samtykkeerklæring som beskriver studiens tema, formål og hensikt. Erklæringen inneholder også informasjon om deltakerens rettigheter. Videre har vi vurdert risikoen ved deltakelse i dette studiet som lav, så lenge personvernet er godt ivaretatt. Alle informantene har bekreftet frivillig deltakelse i studien gjennom samtykkeerklæringen.

Forskeren må vurdere om det foreligger maktrelasjoner eller andre relasjoner som kan påvirke resultatet, og ta hensyn til dette i samhandlingen med informanten (Qu & Dumay, 2011). Vi har vurdert relasjonen mellom informantene og oss som forskere som tilnærmet nøytral, selv om informantene kan sies å sitte på makt i form av kunnskap vi ikke besitter. I tillegg er det viktig å være bevisst på at forholdet og dialogen man utvikler i løpet av intervjuet kan bidra til at nøytraliteten svekkes. Dette søkte vi å unngå ved å la informantene snakke fritt, uten å lede samtalen i en bestemt retning.

Forskeren må vurdere hvor mye informasjon som skal deles med informanten i forkant av et intervju. Det må være nok til å bygge tillit, men ikke så mye at svarene påvirkes (Qu & Dumay, 2011, s. 253). Dette har vi løst ved å fortelle informantene om oppgavens tema og problemstilling, og sendt intervjuguiden på forhånd slik at de er blitt gitt muligheten til å forberede seg. Samtidig har vi unngått å fortelle hvilke resultater vi forventer, eller hvilke antakelser vi har gjort på forhånd.

Personvern bør være ukrenkelig, og innsamlet data bør være anonymisert (Qu & Dumay, 2011, s. 254). Konfidensialitet i denne oppgaven har veid tungt. Noe av grunnen til dette er at personlig informasjon kan benyttes til målrettede angrep. Ettersom kraftforsyningen er en kritisk samfunnsfunksjon, har det vært viktig å verne om aktørenes identitet. Informantene i utvalget er identifisert gjennom nøkkelord, som eksempelvis “NI1” og “NI2”, hvor “NI” viser til “nøkkelinformant” og tallkarakteren viser til hvilken informant det dreier seg om. Intervjuene er transkribert samme dag, og opptakene deretter slettet.

4.7 Metodiske styrker og svakheter

Ved valg av forskningsmetode bør en vurdere potensielle implikasjoner av metodens innvirkning på studiens formål og hensikt. Den abduktive forskningsstrategien utfordrer muligheten til å generalisere, og kan dermed anses som en metodisk begrensning generelt (Blaikie & Priest, 2019). I tråd med oppgavens hensikt, å forstå mulige sammenhenger og slutninger mellom sosiale fenomener, har derimot den abduktive tilnærmingen tilrettelagt for studiens formål. Derfor anser vi abduksjon som en metodisk styrke heller enn en svakhet i dette forskningsprosjektet.

Anonymisering utfordrer muligheten til å etterprøve resultatene, og kan dermed anses som en svakhet. Likevel mener vi dette valget har styrket kvaliteten på datamaterialet. Ved å forsikre informantene om at de ikke ville gjenkjennes i fremstillingen, diskuterte de åpent sine synspunkter rundt positive eller negative trender i bransjen. Anonymisering kan videre rettferdiggjøres ved at kvalitative undersøkelser i flere tilfeller uansett er vanskelig å gjenskape, blant annet ved at personlige interaksjoner er preget av alle parter som deltar (Blaikie og Priest, 2019).

En mulig begrensning ved metoden er at utvalget er relativt lite gitt kraftforsyningens størrelse, noe som kan føre til at funnene vi har etablert baseres på mindretallets sannhet. Dette kunne vært forhindret gjennom metodetriangulering ved å inkludere kvantitative tilnærminger. Eksempelvis kunne vi ha sendt ut en spørreundersøkelse i etterkant av intervjuene for å se om informantenes meninger var gjeldende for en større del av bransjen. For å kompensere for slike svakheter er dokumenter utgitt av sektoren benyttet for å belyse gjentakende trender som er gjeldende for hele sektoren.

Som tidligere nevnt opplevde vi at intervjuguiden ved første intervju tidvis bar preg av førende og lukkede spørsmål, som igjen førte til at informantene drøftet lite rundt spørsmålene. Dette kan ha fått implikasjoner for oppgaven ved at viktig informasjon gikk tapt. Opplevelsen førte imidlertid til en streng gjennomgang og modifikasjon av intervjuguiden, og ga verdifull erfaring før de resterende intervjuene. At intervjuene ble gjennomført via videokonferanse førte til noen tilfeller av kommunikasjonsforstyrrelser ved at vi enten snakket i munnen på hverandre, eller ble stille i påvente av svar fra andre. Ved fysisk møte ville dette kunne vært unngått ved at en ofte signaliserer med kroppsspråket at man er i ferd med å si noe. Slike observasjoner reduseres når

kommunikasjonen foregår elektronisk. Vi vurderer likevel at disse forstyrrelsene ikke har påvirket resultatene nevneverdig, da både vi og informantene fortløpende korrigerte oss selv. Med tanke på situasjonen rundt coronapandemien kan det videre tenkes at fysisk oppmøte ville svekket samtalen ytterligere ved at både vi og intervjuobjekt ville følt på risikoen for smitte.

5.0 Empiri og analyse

Dette kapittelet presenterer empiriske resultater og analyse. Som vi argumenterte for i kapittel 1.5 har vi valgt en struktur som presenterer resultater og analyse i samme kapittel. Det er relativt omfattende tematikker som presenteres, og vi har vurdert det slik at kapitlene trenger en ryddig fremstilling ved å holde empiri og analyse separat innad de ulike delkapitlene.

Som nevnt innledningsvis er det formulert fire forskningsspørsmål for å kunne besvare problemstillingen: "hvordan forstår og håndterer aktører i den norske kraftforsyningen cyberrisiko som følge av sektorens digitale utvikling?". De ulike kapitlene er inndelt etter de 4 forskningsspørsmålene. Kapittel 5.1 vil innlede denne seksjonen, og illustrere hvordan teknologisk utvikling, gjennom nevnte digitaliseringsprosesser, endrer bransjens risikostruktur. Dette etablerer kontekst for øvrige forskningsspørsmål og gir en overgang til 5.2 som omhandler hvordan aktørene oppfatter slike endringer gjennom risikoen for cyberhendelser. Kapittel 5.3 viser deretter overgangen til problemstillingens vektlegging av håndtering, og presenterer empiri og analyse av funn tilhørende oppgavens tredje forskningsspørsmål, som omhandler risikovurderingsprosessen. Håndtering belyses ytterligere i 5.4 fra et organisatorisk perspektiv, hvor vi undersøker hvilke organisatoriske betingelser som tilrettelegger for (eller svekker) aktørenes evne til å håndtere cyberrisiko. I kapittel 5.5 sammenfattes de ulike analysene og delkonklusjonene.

5.1 På hvilken måte endrer digitaliseringsprosesser kraftforsyningens risikostruktur?

I dette kapittelet setter vi søkelys på problemstillingens vektleggelse av bransjens digitale utvikling, og danner bakteppet for øvrige forskningsspørsmål. Bransjens økte innslag av IKT, sammen med potensielle sårbarheter, trusler og farer, vil derfor presenteres i følgende delkapittel. Dette vil danne grunnlaget for å illustrere hvilke endringer som har skjedd med henblikk til bransjens risikostruktur.

5.1.1 Digital utvikling i norsk kraftsektor

Digital sårbarhet - sikkert samfunn

I 2015 presenterte Lysneutvalget en omfattende vurdering av digital sårbarhet knyttet til teknologisk utvikling, og fremmer flere utfordringer som knyttes til digitaliseringen i kraftbransjen. Utviklingen fører til at sektoren i stadig større grad benytter IKT til å understøtte sentrale funksjoner. En annen bekymring er at den digitale utviklingen fører til at stadig flere IKT-løsninger integreres i og mellom systemer, hvilket bidrar til en betydelig økning i bransjens kompleksitet (NOU 2015:13). Slike sammensmeltninger med IKT fører til situasjoner hvor bransjen blir mer eksponert for cybertrusler og utilsiktede feil. Digitalisering fører også til at det konstrueres lange digitale verdikjeder med komplekse samhandlingsmønstre og avhengighetsforhold. Dette kan videre føre til situasjoner hvor sårbarheter kan oppstå i alle ledd, og forplante seg videre i verdikjeden (NOU 2015:13, s. 136).

Videre er avhengighet til eksterne systemer og infrastruktur trukket frem som en fare: "En gradvis effektivisering over tid, der personell blir erstattet med informasjons- og kommunikasjonssystemer, forsterker avhengigheten av telekommunikasjon" (NOU 2015:13, s. 141). Selv om det vektlegges at kraftbransjen i stor grad skal kunne drifte kraftsystemet uten hjelp av annen infrastruktur stiller utvalget seg kritisk til dette, og mener at teknologiskiftet i kraftbransjen vil øke sektorens avhengighet til annen infrastruktur, i hovedsak EKOM (NOU 2015:13).

Utvalget fremmer også problemstillinger knyttet til driftskontrollsystemene (SCADA) som tidligere var helt separert fra den digitale omverdenen. Systemene kobles nå i større grad opp mot administrative deler av virksomhetene. Dette kan by på et mangfold av utfordringer, hvor en av dem er at driftskontrollsystemet ikke har vært utviklet med tanke på sikkerhet. Videre nevner utvalget at bruk av sikkerhetstiltak som antivirusprogrammer og overvåkningssystemer for å sikre slike systemer mot uautorisert tilgang kan være problematisk. Dette er særlig knyttet til de eldre systemene fordi "risikoen er stor for at disse systemene forstyrrer, forsinker eller stopper lovlig og nødvendig datatrafikk" (NOU 2015:13, s. 137). I tillegg kan slike tekniske sikkerhetstiltak by på

utfordringer i seg selv dersom de implementeres i integrerte systemer som tidligere har vært konfigurert separat, for ulike formål (NOU 2015:13, s. 137).

Norges vassdrags- og energidirektorat

Fra 2014 til dags dato ser man en økning i antall rapporter publisert av Norges vassdrags- og energidirektorat med fokus på digitalisering og IKT-sikkerhet i kraftbransjen. I 2014 fokuseres det på bruk av skytjenester, hvor Borgund (2014) på oppdrag fra NVE har vurdert sikkerhetsmessige utfordringer tilknyttet tredjepartsinvolvering. Utfordringene består av et sammensatt bilde, men oppsummert er det liknende risiko som ved tradisjonell outsourcing, som kan svekke virksomhetenes evne til å få innsyn i sikkerhetstiltak, og hvem som har tilgang til systemene (Borgund, 2014, s. 5).

Året etter utgir NVE en rapport om den samme tematikken. Selv om store globale skyleverandører er profesjonelle i ivaretakelsen av sikkerhet, kan tjenestene gi utfordringer i form av mangel på kontroll og innsyn. I tillegg løftes problematikken rundt mulig konsentrasjonsrisiko[2] frem, som refererer til situasjoner hvor en samler tjenester, systemer og andre løsninger hos en enkelt leverandør, eller på et geografisk avgrenset område (NVE, 2015, s. 57).

Digitale sårbarheter forbundet med AMS-systemet trekkes også frem. AMS omtales i rapporten som et komplekst sammensatt system bestående av maskinvare, programvare og fastvare med mange tusen endepunkter hvor hendelser kan oppstå. Systemene vil ha et stort potensial for latente feil[3], i tillegg til at det vil kunne finnes ubeskyttede inngangsporter som kan utnyttes (NVE, 2015, s. 25). Også i forbindelse med AMS trekkes potensiell konsentrasjonsrisiko frem, hvilket kan bli tilfelle dersom bransjen i Norge ender opp med et fåtall større leverandører. Konsentrasjonsrisiko kan føre til at både utilsiktede feil og målrettede handlinger kan påvirke forsyningssikkerheten dersom målerne faller ut (NVE, 2015, s. 58-59). En annen problematikk som trekkes frem er systemers generelle tekniske sammensetning som følge av digitaliseringen. Systemer kan bli

[2] Konsentrasjonsrisiko: brukes til å beskrive en situasjon hvor en spesiell type produkter eller tjenester øker risikoen i sektoren grunnet opphoping av avhengigheter (NVE, 2015, s. 41)
[3] Latente feil og feil vil alltid finnes i systemer, og en viktig faktor i ulykkesforebygging er å identifisere disse, så de ikke blir liggende lenge i systemet og føre til uønskede hendelser på et senere tidspunkt. Latente feil kan bestå av utilsiktede feilhandlinger gjort av mennesker, dårlig design eller mangel på prosedyrer (Reason, 2016)

vanskeligere å forstå, og det vil i større grad kunne oppstå uforventede interaksjoner som følge av tilsiktet eller utilsiktet påvirkning (NVE, 2015, s. 48-51).

Videre nevnes kontroll og oversikt over systemene, samt forvaltning av informasjon og data i forbindelse med økningen av antall leverandører og underleverandører. Utviklingen vil kunne skape utfordringer når det kommer til oversiktligheten til hele digitale verdikjeder (NVE, 2015, s. 6). Selv om rapporten illustrerer flere utfordringer tilknyttet digitaliseringen i sektoren, viser den også til at flere selskaper og aktører mener det kan bli vanskelig å stå på utsiden av utviklingen uten å bli hengende etter (NVE, 2015, s. 35).

I 2016 utgir NVE en rapport om IKT-systemers rolle og betydning for strukturen i kraftbransjen. Store endringer som følge av teknologisk utvikling forventes å påvirke bransjen. Sårbarheter tilknyttet AMS-systemet trekkes nok en gang frem, og er i rapporten knyttet til kraftforsyningens økende avhengighet til IKT (s. 10). Videre skrives det at enkeltleverandører av SCADA har store markedsandeler i Norge, som kan lede til at feil hos en leverandør kan forplante seg og påvirke øvrige selskaper i kraftsektoren. Digitalisering i tjenesteutvikling også kan forårsake risiko i systemer, ved at integrasjon av ulike del- og støttesystemer fører til at man konstruerer systemer med komplekse samhandlingsmønstre. Slike utviklingstrender vil kunne føre til tekniske avhengigheter mellom ulike delsystemer, og kan være utslagsgivende for bransjens kompleksitet (NVE, 2016).

Påfølgende år blir tre nye rapporter utgitt. En kartlegger informasjonssikkerhetstilstanden i kraftforsyningen (NVE, 2017b). Den andre omhandler metoder for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem (NVE, 2017c), og den tredje tar for seg regulering av IKT-sikkerhet (NVE, 2017a). De tre rapportene hevder at digitaliseringen i kraftsektoren endrer bransjens risikobilde, og at det er forventet å skje tilsvarende endringer i IKT-trusselbildet. Også utilsiktede feil påpekes i forbindelse med digitaliseringen i sektoren, ved at feil i programvare, maskinvare og konfigurasjon kan forstyrre driften dersom det forplanter seg i det digitale systemet (NVE, 2017b, s. 1).

I tillegg fremmer rapporten om regulering av IKT-sikkerhet at sikkerheten i selskapenes digitale systemer ikke er bedre enn det svakeste leddet i verdikjeden (NVE, 2017a, s. 12).

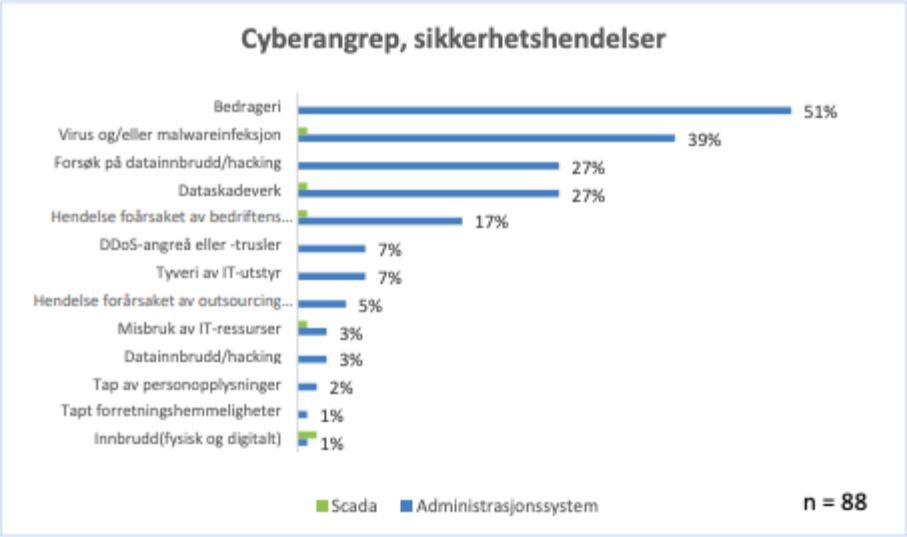
> Når IKT-systemer som driftskontrollsystemer, administrasjonssystemer og andre nettbaserte systemer kobles sammen, vil det svakeste leddet i kjeden kunne være en inngangsport til tilknyttede systemer. I tillegg vil svakheter og feil i systemkonfigurasjonen og programvare kunne medføre systemsvikt, eller gjøre systemene åpne for angrep fra opportunistiske angripere (NVE, 2017a, s. 23).

I år er det utgitt enda en konsulentrapport på vegne av kraftsektoren, som kartlegger bruken av tingenes internett i energiforsyningen (NVE, 2020). Også her trekkes digitaliseringen frem som utslagsgivende på bransjens utsatthet for trusler og andre uønskede hendelser. Likevel hevdes det, som i øvrige rapporter, at digitaliseringen er noe som vil prege både nåtid og fremtid, og at veien til smarte nett og smarte kraftsystem vil skje gjennom videre digitalisering, teknologiutvikling og innføringen av automatiserte prosesser (NVE, 2020, s. 5).

Cybertrusler

Gjennom flere år har NSM rapportert om en jevn økning i målrettede datainnbrudd mot offentlig og privat sektor. Funn fremlagt i Mørketallsundersøkelsen fra 2018 viser en økning i målrettede angrep som utspiller seg i cyberdomenet, hvor phishing er den vanligste (NSR, 2018, s. 42). Dette stemmer godt overens med trusler rettet mot kraftbransjen spesifikt, da det fremkommer i en rapport utgitt av NVE at spearphishing (målrettet phishing) var en gjentakende angrepsmetode (NVE, 2015, s. 18).

Funnene i NVEs rapport fra 2017 indikerer at angrep rettet mot administrasjonssystemer forekommer ved flest tilfeller, men sektoren har også rapportert om noen få hendelser rettet mot SCADA-systemer. Figuren under er hentet fra rapporten og viser angrepsmetoder rettet mot de ulike systemene (NVE, 2017b).



Figur 6 Cyberangrep, sikkerhetshendelser (NVE, 2017b, s. 16).

I tillegg til overnevnte systemer, anslås også skytjenester å være et attraktivt mål for internettbasert etterretning ettersom de forvalter og lagrer viktig informasjon (NVE, 2015, s. 18).

5.1.2 Digital utvikling - fra aktørenes perspektiv

Utviklingens forløp

Ved spørsmål om hvordan informantene selv opplever den digitale utviklingen i sektoren, forteller de at noen prosesser har foregått over lenger tid, mens andre har utviklet seg raskt. "En løpende utvikling som har foregått i flere år" sier informant 3, som videre hevder at utviklingen går tilbake til da man begynte å fjernstyre anleggene for flere tiår siden. Likevel understreker han at det som har skjedd i senere år er en helt annen form for digitalisering (NI3). Informant 5 hevder bransjen har grovt sett hengt etter når det kommer til digitalisering, men dette etterslepet er nå i ferd med å jevnes ut. Utviklingen frem til nå har vært preget av både tilbakeholdenhet og et ønske om å henge med i svingene, og informanten forteller at det kan være vanskelig å finne riktig balanse mellom "brems" og "kjør" når det gjelder hvilke trender og løsninger de takker ja til. På en side ønsker de å være oppdaterte og fremoverlente, mens de på den andre siden har sett seg nødt til å si nei og holde tilbake noe av utviklingen da forslag fra leverandørene ikke alltid var like gode og modne (NI5).

Informant 2 hevder at digitaliseringen mest sannsynlig vil fortsette å skyte fart i årene som kommer, da innføringen av nye løsninger trolig vil kreve at andre prosesser må digitaliseres for å

sikre kompatibilitet. Slike forhold mener han kan skape positive synergieffekter, som fører til at de digitale innslagene i sektoren øker selv uten at dette er intensjonen (NI2).

Utviklingens konsekvenser

Flere av informantene forteller om hvilken avhengighet de føler til digitale systemer. Informant 5 og 8 mener den digitale utviklingen kan føre til situasjoner hvor en glemmer tiden før de digitale løsningene kom på banen. Kunnskap om systemene slik de var før kan gå tapt når generasjonen som kjente nettet før digitaliseringen pensjonerer seg (NI5). Informant 8 hevder at selskapene vil trenge en helhetlig kompetanse i og med at systemene i flere tilfeller kan bestå av gammel og ny teknologi (NI8).

> En blir så avhengig av de digitale løsningene at det liksom ikke er noen vei tilbake, og dermed så blir en jo enda mer avhengig av at de fungerer, og det er nok også det jeg ser på som den største sårbarheten (NI2).

En annen faktor som påvirker sektorens avhengighet fremmes av informant 8, som opplever at selskapene er svært avhengige av relevant kompetanse, og vektlegger leverandøravhengighet når det kommer til spesialiserte systemer som AMS:

> Hvis vi finner ut at vi ikke kan bruke leverandør A lenger, så vil vi i det øyeblikket vi sier opp avtalen vår miste all kompetanse på dette området. Vi har jo strengt tatt ingen kompetanse på dette området, og alt må da bygges opp på nytt kompetansemessig og kunnskapsmessig. Det kan være en relativt dyr prosess. I tillegg er jo en av ulempene ved spesialiserte systemer at det kun er en håndfull leverdører i Norge av AMS-drift. Vi kan jo ikke gå til hvem som helst og si at vi vil at de skal drifte AMS-systemet for de aner ikke hva det er for noe (NI8).

Informant 7 mener at avhengighet til leverandører må sees i forbindelse med kompetanse og ressurser til å drifte IT-systemer selv, kontra å sette det ut. "Det er ikke tvil om at selskaper som er veldig små vil ha vansker med å drømme opp kompetanse til å drifte tjenester på en forsvarlig måte" (NI7). Den samme informanten hevder at de har sett en stadig økende trend med kompromittering av leverandører, som uten grep ville føre til en situasjon som "spinner helt ut av kontroll" (NI7). Videre forteller hun at risikoen tilknyttet avhengighet til leverandører ville gi seg til kjenne etter nåværende krise (Covid-19), særlig når det gjelder outsourcing av tjenester til land med andre styreformer:

> Det er jo en del problemstillinger nå som er ganske interessante. Du har jo de som outsourcer til for eksempel India hvor de nå jager folk hjem med pisk på grunn av Covid-19, og hvor igjen ingen indiske arbeidere får lov til å jobbe mot datasentre hjemmefra. Så hvordan bemanningen i India er vet jeg ikke, men jeg tipper den er ganske dårlig (NI7).

Utviklingen fører ofte til at leverandørene benytter flere underleverandører som videre fører til lange digitale verdikjeder og komplekse avhengighetsforhold mellom involverte parter:

> I forbindelse med disse leverandørene, så har vi jo sånne verdikjedeangrep som vi kaller det, der en ser at man hacker leverandører istedenfor det ekte målet, også går det via leverandører og mot hovedmålet. Der er det mer risiko (NI2).

Informant 6 mener avhengighetsforhold til leverandører kan være problematisk, og utfordrer evnen til å holde full oversikt. Særlig illustrerer han dette ved økt bruk av skytjenester, og at de har informasjon lagret i ulike skyer på mange forskjellige steder. "Hvordan er egentlig forvaltningen av det når vi ikke ser? Vi har jo ikke peiling" (NI6). Utfordringer knyttet til uoversiktlighet gjør det ekstra viktig at en stiller seg kritisk til å legge verdifull informasjonen til skyen, og hos leverandører man ikke har full kontroll over. Dette fører til at arbeid med å gjenvinne kontroll og innsikt i informasjonsflyt blir tydelige fokusområder for å sikre at en ikke mister oversikten. Han mener bransjen fortsatt ligger et stykke bakpå når det kommer til å ha full kontroll på leverandører og hvor informasjon flyter (NI6).

Risiko som følge av digital eksponering

Informant 4 forteller hvordan den digitale utviklingen har ført til situasjoner hvor en eksponerer seg på helt andre måter enn tidligere. "Altså når ting før var manuelt så var det jo lettere å holde en høy grad av sikkerhet. Men jo mer du digitaliser jo mer eksponerer du deg i verden" (NI4). Også informant 7 skisserer dette: "i en analog verden, som denne bransjen kommer fra, så måtte man være onsight for å koble ting, mens nå fungerer ting via fjerntilkobling" (NI7). Informant 1 illustrerer endringene i bransjens risikobilde med utrullingen av AMS:

> Når du tidligere hadde de analoge målerne, så var de ikke tilknyttet internett, og dermed heller ikke eksponert for skadevare og programvare som andre har utviklet. Det er de jo nå med de digitale målerne på en helt annen måte (NI1).

Tilsvarende argumentasjon presenteres av informant 5 som mener at digitalisering, og mer utbredt kobling til internett i sektoren gjør at en eksponerer seg for utenforstående (og interne) farer og trusler:

> Det kan være sårbarheter som vi kanskje kjenner godt til, men ikke har brydd oss om å patche så mye fordi de har vært på isolerte systemer. Nå kobler man systemer til internett, og da vil plutselig en angriper kunne utnytte sårbarhetene. Så det kan gå fra å være en lav sårbarhet til å bli veldig kritisk når de kan utnytte de. Det er jo mange sårbarheter som følger med digitaliseringen, og vi mennesker er kanskje en av de største sårbarhetene også, siden vi klikker på ting og åpner vedlegg (NI5).

Informant 8 hevder risikoen går fra "10 til 1000" når man tar i bruk nye digitale løsninger eller integrerer eksisterende system opp mot hverandre. Eksempelvis anså informanten at AMS kunne være en trussel for SCADA-systemet, i og med at AMS har "en relativt direkte tilkobling" til SCADA. Dette kan føre til situasjoner hvor risiko tilhørende AMS også er gjeldende for SCADA, og omvendt. For å eliminere all risiko anså informanten at det eneste alternativet var å koble AMS-systemet helt vekk (NI8).

Videre nevner et flertall av informantene at digitaliseringen leder til et økt behov for generell sikkerhet. Informant 2 og 4 forteller at sikkerhetsløsninger er viktig ved innføring av digitale systemer som AMS, og at det er sentralt at disse er "up to date" (NI4). Videre nevner informant 5 at den digitale utviklingen har ledet til behov for nye sikkerhetstiltak, med tanke på at risikoen har tatt nye former og truslene kan spenne bredt. "Nå er det jo helt andre trusler man kanskje står overfor, og det er nesten blitt viktigere å tenke på hvordan man beskytter digitale systemer fremfor å vurdere hvor tykk dør man har på diverse stasjoner" (NI5). Det økte behovet for sikkerhet gjenspeiles også i hvordan risikobildet påvirkes av at kompleksiteten øker. "Kompleksitet er jo alltid sikkerhetens verste fiende" (NI1).

5.1.3 Analyse av funn

Empirien viser at digitaliseringsprosessene som har preget kraftbransjen i de senere årene har endret sektorens risikostruktur på flere måter. For det første illustrerer funn i dokumentene at norsk kraftsektor har blitt mer avhengig av teknologi og digitale systemer, hvilket implisitt betyr at sektoren har økt sin avhengighet til cyberdomenet. Cyberdomenet er sammensatt i seg selv, og

består av et mangfold av systemer, komponenter og aktører, hvilket resulterer i sammensatte interaksjoner og prosesser innad i og på tvers av kraftsektoren. Kraftsektoren er allerede preget av tette koblinger som følge av den kritiske balansegangen mellom strømproduksjon og forbruk, og kan allerede nå betraktes som et relativt høyteknologisk system, i tråd med Charles Perrows (1999) teori om normale ulykker. Den digitale utviklingen i sektoren berører både koblingene og interaksjonene i systemet. Utviklingen indikerer derfor at kraftforsyningen er blitt enda mer kompleks, hvilket gjør at sektoren i større grad oppfyller kriteriene Perrow fremmer for å kunne betraktes som høyteknologisk. Prinsippene som fremlegges i NAT kan videre omsettes i praksis for å illustrere hvilke endringer den digitale utviklingen har hatt for bransjens risikostruktur.

Tette koblinger og komplekse interaksjoner

Som Perrow (1999) skriver vil et systems kompleksitet kjennetegnes av egenskapene til koblingene og interaksjonene i systemet. Ettersom kraftbransjen kan betraktes som et høyteknologisk system vil endringer i systemets koblinger og interaksjoner trolig tilsi at systemet vil være mer utsatt for systemulykker. Selv om målet ikke er å anslå hvorvidt bransjen vil være utsatt for større systemulykker, vil likevel prinsippene i teorien kunne si noe om hvordan risiko forflytter seg i et system dersom en introduserer faktorer som påvirker hvordan systemet er koblet. Som empirien viser introduserer digitaliseringsprosesser flere slike faktorer.

Den første faktoren som tydelig kommer fram i empirien er den generelle avhengigheten digitaliseringen skaper. Det er videre verdt å merke seg at avhengighet er omtalt i ulike settinger, hvilket gjør det til en allsidig faktor som påvirker bransjens sammensetning på flere måter, og dermed også hvordan risiko forplanter seg i systemet. Som dokumentanalysen også viser er det mye som tyder på at utviklingen i sektoren og samfunnet forøvrig går mot konseptet "smart", hvilket indikerer at digitaliseringen i sektoren har og vil fortsette å utvikle seg relativt raskt. Faktoren forsterkes videre gjennom en av informantenes uttalelser om positive synergieffekter, hvilket betyr at dersom man implementerer en digital løsning, vil det trolig være behov for å digitalisere ytterligere for å gjøre systemene kompatible. En kan derfor anta at det digitale innslaget i sektoren vil vokse eksponentielt, hvilket tilsier at avhengigheten til slike løsninger vil vokse tilsvarende. Dette støttes ytterligere gjennom funn fra dokumentanalysen hvor bransjens økende avhengighet til IKT er trukket frem flere ganger de siste årene.

I tillegg til den generelle avhengigheten til digitale løsninger, viser empirien at implementering av digitale løsninger ofte skaper avhengighetsforhold til eksterne aktører der drift av slike tjenester er satt ut til tredjeparter. Dette problematiseres av dokumenter og informanter. Dersom man ser slike faktorer i lys av Perrows teori er det mye som tyder på at avhengighet, både til selve tjenestene og eksterne aktører, vil kunne gjøre systemene mer komplekse. Kompleksiteten øker når digitale systemer øker innslaget av teknologi, og når verdikjeden utvides ved at man legger til ekstra ledd, eksempelvis leverandører. Dette kan bidra til at risiko kan forplante seg både i de nye systemene, og hos eksterne aktører som er inkludert i verdikjeden. Med andre ord skaper avhengighet lange og komplekse interaksjonskjeder som resulterer i en utvidelse av antall flater hvor utilsiktede og tilsiktede hendelser kan oppstå. Dette illustreres også gjennom både dokumenter og informantenes uttalelser, hvor det trekkes frem at leverandører ofte benyttes som inngangsport for tilsiktede hendelser. Betraktet i lys av NAT vil en derfor kunne si at den digitale utviklingen i kraftsektoren fører til uklare linjer mellom hva en kan betrakte som en del av selve systemet, og hva som er eksterne aktører og systemer. Det er derfor mye som tyder på at en må inkludere eksterne aktører og systemer som en del av selve kraftsektoren som helhet. I tillegg belyser empirien at situasjoner hvor en er nødt til å inkludere tredjeparter vil kunne lede til at en mister kontroll og innsyn, hvilket kan tyde på at systemet blir uforutsigbart. Perrow mener dette er en forsterkende faktor i forbindelse med ulykker (Perrow, 1999).

Empirien viser videre at digitale løsninger i flere tilfeller betraktes som systemer bestående av komponenter med sterke tekniske avhengigheter, som indikerer at koblinger i slike systemer er tette. Perrow (1999) hevder at systemer som kjennetegnes av slike prinsipper vil kunne ha sterk tidsavhengighet, hvilket indikerer at det er lite slakk dersom komponenter feiler. Tette koblinger bidrar ifølge Perrow til å øke ulykkespotensialet ved at hendelser raskt kan forplante seg i uforventede frekvenser videre innover i systemet. Med tanke på at kraftbransjen til stadighet kobler systemer sammen, og tar i bruk nye løsninger vil derfor sårbarheter ved et system kunne sies å være gjeldende for tilkoblede enheter. Dette gjør at en kan betrakte cyberhendelser, dersom de skulle skje, som "normale ulykker".

Normale ulykker

Som nevnt er ikke målet med dette forskningsspørsmålet å tolke hvorvidt bransjen vil møte alvorlige ulykker som følge av digitaliseringen. Derimot kan strukturelle endringer innad i sektoren, sammen med nye farer og trusler som følger av digitaliseringen vise til hvorvidt systemets kompleksitet kan utnyttes, hvilket vil kunne gi oss tydelige eksempler på hvordan risikostrukturen har endret seg.

Empirien viser at det har skjedd flere endringer i bransjens risikobilde som følge av digitaliseringen i sektoren og i samfunnet forøvrig. Funn fra dokumentanalysen viser blant annet at det er skjedd en økning i cybertrusler mot offentlig og privat sektor, også i kraftsektoren. Basert på den digitale utviklingen i kraftforsyningen omsatt i NAT kan man betrakte følgende scenario:

En mindre kriminell gruppe har funnet ut at kraftforsyningen er et godt alternativ for et målrettet angrep ettersom sektoren er verdifull for samfunnets øvrige funksjonalitet. De går inn med en intensjon om økonomisk gevinst, og anslår at et gitt selskap vil betale seg ut dersom angrepet er vellykket. På forhånd har de vurdert at den komplekse systemsammensetningen kan utnyttes gjennom å innrette angrepet mot selskapets administrative systemer. I gjennomføringen av angrepet benytter de seg av spearphishing, hvor de tilpasser e-posten med det infiserte vedlegget slik at det ser ut til å komme fra en betrodd leverandør.

Utilsiktede feil kan også ha stort skadepotensial dersom de initieres. Som scenariet over belyser vil en del av suksessfaktoren forutsette at det er en menneskelig faktor som har initiert selve ulykken ved å trykke på det infiserte vedlegget, selv om intensjonen er utilsiktet. Som NAT også påpeker, er det ikke kun teknologien som utelukkende er skyld i ulykker, men også menneskene som operer i det. Dermed kan en stille spørsmål om hvorvidt den menneskelige faktoren i samspill med kraftsektorens digitale utvikling også er medvirkende til at ulykkespotensialet i sektoren vokser, hvilket støttes av empirien. Dette kan i stor grad se ut til å være en forsterkende faktor ved integrasjon av systemer, og særlig til den administrative delen som består av mange endepunkter. Utilsiktede hendelser som skjer i grenseland mellom teknologi og menneske, vil derfor videre også kunne anses som en normal ulykke i lys av NAT (Perrow, 1999).

Sårbarhet

Sårbarheter som følge av sektorens digitale utvikling er et tema stort sett gjennom alle dokumenter og av informantene. I kapittel 3 definerte vi sårbarhet som et systems "manglende evne til å motstå en uønsket hendelse eller å opprettholde en stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (NS 5830:2012, s. 5). Som nevnt benyttes stadig mer IKT til å understøtte kraftbransjens funksjoner, hvilket indikerer at verdier også forflyttes over i digitale domener. Ergo foreligger det et gjensidig påvirkningsforhold ved at digitaliseringen forflytter sektorens verdier, hvilket igjen gjør de utsatt for utnyttelse gjennom nettopp hva vi har diskutert over - kraftforsyningens stadig tettere koblinger og komplekse interaksjoner. Et annet interessant dilemma som trekkes frem i empirien er det faktum at et systems sårbarhet ofte vil kjennetegnes at dets svakeste komponent. Analysen har illustrert at slike svakheter kan finnes mangfoldige plasser. Det kan dreie seg om svakheter innad i egne systemer, hos leverandører og hos mennesker, gitt at de betraktes som en del av et større hele, hvilket de gjør ved at de inngår i verdikjeden og støtter sektorens samfunnsansvar. Det er likevel ikke gitt at aktørene er bevisst på denne helheten, og at de ikke anser leverandører eller andre tredjeparter som en del av sitt system. Dette kan bidra til at latente feil blir liggende i systemet og på den måten gjøre det mer sårbart.

Oppsummert kan vi argumentere for at digitaliseringsprosessene kraftforsyningen har gjennomgått gjør at sektoren kan betraktes som et høyteknologisk system, som gjennom teknologisk utvikling presses mot høyre ytterpunkt i Perrows (1999) interaksjons- og koblingskart.

5.1.4 Delkonklusjon

Som svar på forskningsspørsmål 1 viser empirien og analysen i dette delkapittelet at bransjens risikostruktur har endret seg på flere måter som følge av digitalisering. Dette viser seg ved at faren for svikt og forstyrrelser har vokst, hvilket betyr at kraftbransjens cyberrisiko har økt og inngår i alle spektre som trekkes frem i analysen. Digitaliseringsprosessene, og bransjens generelle digitale utvikling, har ledet til at det introduseres flere farer og trusler, og at slike risikoforhold til tider kan være vanskelige å skille fra hverandre. Videre medfører den digitale utviklingen at det opprettes flere sårbarheter som kan utnyttes og utfordres av farene og truslene som introduseres av utviklingen. Likevel er kanskje de viktigste endringene i bransjens risikostruktur belyst gjennom konseptualiseringen av Perrows teori om normale ulykker. Når man omsetter kraftsektoren i

teorien illustreres de strukturelle endringene digitaliseringen har ledet til, ved at det konstrueres tettere koblinger og komplekse interaksjoner. Det er slike strukturelle endringer som gir farer og trusler et bredt spekter av innfallsvinkler, og gjør at cyberhendelser kan forplante seg over større deler av sektorens funksjoner og systemer. Dette viser at strukturelle endringer i bransjen, sammen med en vekst i farer og trusler viser til en ny risikostruktur, hvor uønskede hendelser kan forplante seg bredt.

5.2 Hvordan forstås risikoen for cyberhendelser av aktører i kraftforsyningen?

For å kunne besvare oppgavens problemstilling om hvordan aktørene forstår og håndterer cyberrisiko som følge av utviklingen skissert i studiens første forskningsspørsmål, vil vi undersøke hvordan de forholder seg til risikoen for cyberhendelser. Dette gjøres gjennom en kartlegging av hvordan aktørene tolker begrepet cyberrisiko. Videre vil konsekvenspotensialet ved uønsket påvirkning på sektorens digitale systemer avklare hvilke deler av driften de opplever som spesielt utsatt for denne typen risiko, og dermed også avklare hvilke farer og trusler de anser som mest fremtredende.

5.2.1 Tolkning av terminologi

Alle informantene ble spurt om hva de legger i begrepet cyberrisiko. Ifølge informant 2 handler det om bevisste skadelige handlinger rettet mot kraftsektoren, i hovedsak gjennom internett, og "ikke noe mer mystisk enn det" (NI2). Informant 3 mener cyberrisiko handler om sannsynlighet for, og konsekvenser av, målrettede dataangrep mot kritiske anlegg i sektoren (NI3).

Også informant 4 tolker begrepet til å omfatte målrettede angrep, og hevder at cyberrisiko må forstås som risikoen for at andre uvedkommende skal kunne ta over selskapets funksjonalitet eller arbeidssystemer slik at de mister kontroll. Han kobler særlig begrepet opp mot scenarier hvor selskapet kan settes i økonomiske gisselsituasjoner, eller situasjoner hvor trusselaktører kan koble ut anlegget og skape kjedereaksjoner som vil kunne sette liv og helse i fare (NI4).

Informant 5 mener cyberrisiko er risikoen som følger med sektorens digitalisering. Hun mener utviklingen har åpnet opp for helt nye angrepsflater som kan utnyttes av trusselaktører. Hun forklarer dette ved å henvise til driftskontrollsystemet, hvor kjente sårbarheter tidligere ikke var ansett som et problem, nettopp fordi det var isolert fra omverdenen. Når systemer kobles sammen og man får mer kommunikasjon mellom det administrative systemet og driftskontrollsystemet, skifter risikoen fra det fysiske landskapet til cyberdomet (NI5).

Ifølge informant 7 unngås begreper som cyberrisiko og IKT-risiko, nettopp fordi det er så stor forskjell i hva folk legger i begrepet.

> Vi prøver å unngå både IKT, IT og cyber fordi det er en del som har fikse ideer om at da gjelder det ikke meg. Si at hvis vi bruker IKT-sikkerhet, da gjelder det ikke kontrollsystemer. Cyber, nei jeg jobber bare med administrative systemer. Jeg kaller det ofte for digital sikkerhet, og det beskriver jo også litt hva jeg mener med risikoen (NI7).

Ifølge informant 6 og 8 er cyberrisiko et begrep under utvikling, hvor innholdsverdien påvirkes av den pågående digitaliseringen. Begrepets innhold blir enormt mye større jo mer digitalisering en bedriver, og kan betraktes "som et tog som ikke kan stoppes" (NI8). Derfor det viktigste en kan gjøre er å erkjenne at risikoen finnes, heller enn å avgrense betydningen gjennom fastsatte definisjoner. Han uttaler at så lenge noe er tilkoblet så er det en risiko ved det, men risikoen er vanskelig å definere ettersom en ofte ikke kjenner risikoen på forhånd. "Det er kanskje det som er problemet, at en ikke vet hva risikoen er før den faktisk blir avdekket" (NI8).

5.2.2 Farer og trusler

Ved spørsmål om hvilke farer og trusler aktørene mener bransjen står overfor som følge av digitalisering, forteller informant 1 at bransjen påvirkes av de samme truslene og farene som kommuniseres gjennom nasjonale rapporter. Informanten henviser til PSTs trusselrapporter, Mørketallsundersøkelsene og funn fremlagt av Lysneutvalget.

Ifølge informant 2 kan truslene rettet mot bransjen bestå av fremmede statsmakter med strategiske og politiske motiver. De planlegger ikke nødvendigvis å gjennomføre målrettede angrep per i dag, men søker innpass i digitale systemer som kan utnyttes ved senere anledninger. Dette illustrerer

han med eksempler fra andre land hvor trusselaktører har forsøkt å infiltrere driftskontrollsystemer og administrative systemer. Særlig mente han at innpass i administrative systemer var en vanlig angrepsvinkel, som var høyst relevant også for den norske kraftbransjen i en digital epoke hvor systemer kobles sammen (NI2). Det samme mener informant 5, og sier at det har vært en vekst i opportunistiske aktører som sender ut phishing e-post til en bred mottakerliste i et forsøk på å "få napp hvor som helst" (NI5). Særlig har de sett en stor økning i slike hendelser under den pågående corona-pandemien. "Angriperne utnytter jo denne coronastituasjonen voldsomt, så vi ser at det stoppes utrolig mye phishing e-mail og malware. Det har gått opp enormt" (NI5).

Kriminelle grupper med økonomiske incentiver er en annen med trussel som følger med digitaliseringen. Det kan føre til hendelser hvor selskaper kan settes i en gisselsituasjoner (NI2). Selv om informant 2 vektlegger tilsiktede hendelser i besvarelsen, mener han at slike trusler ikke må overskygge hvilke farer bransjen ved flest tilfeller står overfor, som er farer som følge av været. "At det blåser ned master og diverse er jo den største ubevisste hendelsen vil jeg si" (NI2).

Informant 3 forteller at han oppfatter det som rart å knytte cyber opp mot utilsiktede hendelser som rammer fysiske elementer, men forteller videre at farer og trusler handler om to forhold, hvor det ene er at ting ikke virker, og det andre er at ting virker feil (NI3). Slike forhold kan forårsakes av både feilhandlinger og målrettede angrep, og en må derfor være bevisst på begge former for risiko når man tenker sikkerhet. Feilhandlinger knyttet til digitale systemer nevnes også av informant 4, som mener at slike hendelser også må forstås som potensielle farer.

> Det er jo en risiko for at vi kan gjøre feil, som gjør at vi skaper et problem for oss selv. Så vi må hele tiden være bevisst på handlingene våre, og hvilke endringer vi gjør. Også må vi gjøre vurderinger av slike endringer sånn at vi er helt sikre på at vi har den nødvendige sikkerheten som systemet krever (NI4).

Informant 5 viser også til at farer kan komme av at en bruker systemene feil. Dette mener hun må kompenseres med sikkerhet i form av opplæring av brukere og begrensninger tilknyttet hvem som faktisk kan gjøre koblinger i systemet. En liten feil kan bli alvorlig selv om den er gjort i beste hensikt (NI5).

En stor frykt i kraftbransjen er ifølge informant 6 at uvedkommende får tilgang til kritiske systemer gjennom klienter, eksempelvis PCer, som benyttes av administrativt personell. Dette er en risiko som kan forsterkes dersom selskapet er organisert med et konsern som distribuerer fellestjenester som IT, økonomi og anskaffelser til flere selskaper. Ved slike tilfeller er selskapene avhengige av at sikkerheten ivaretas og overvåkes av morselskapet. Informanten forteller at dette kan lede til situasjoner hvor sikkerhetsarbeidet kan falle mellom stoler.

> En av de største fryktene i kraftverdenen er at noen skal kunne komme inn på en økonomiarbeider sin PC og klare å påvirke strømnettet. Dette er jo skiller du ønsker å ha tett, sant, men når alt skjer nå med fjerntilkobling fra jobb-PCer hjemmefra så er det en del interessante ting som kan oppstå, og det er utrolig farlig når ting kan falle mellom stoler. I noen tilfeller kan jo noen i produksjonsselskapet tenke at morselskapet har sikret klienten og at det sånn sett ikke kan oppstå feil, mens morselskapet igjen kan tenke at produksjonsselskapet har håndtert sikkerheten selv (NI6).

Den samme informanten mener farer og trusler representerer en "fin miks" i kraftsektoren, og at begge kategorier må ha prioritet. Spesielt mener han den utilsiktede delen som kommer med digitaliseringen er meget interessant da nye digitale løsninger representerer en omveltning som få av de som har jobbet i kraftbransjen lenge er særlig kjent med. "Man har jo gjerne en IT-avdeling på 40 stykker hvor ingen har vokst opp med skykonfigurasjon, så den utilsiktede risikoen for databrudd er jo ganske høy fremover" (NI6).

Farer som følge av feilkonfigurasjon, og andre utilsiktede hendelser, kan igjen akselerere truslene. Informanten forklarer dette som at farer og trusler i flere tilfeller vil påvirkes og forsterkes av hverandre (NI6). Informant 7 mener også at skillet mellom farer og trusler kan være hårfint, og at det ved flere tilfeller handler om et definisjonsspørsmål.

> Eksempelvis kan man si at hvis noen har mottatt en phishing e-post og klikker, og ting blir kjørt og infisert, så er det jo en utilsiktet handling fra den ansattes side, men igjen, det er jo noen som har ønsket at dette skal skje så da er det jo også en tilsiktet hendelse (NI7).

Informant 6 mener det kan være utfordrende å få kontroll på potensielle trusler mot bransjen, ettersom de kan involvere et mangfold av aktører. Selv mente han at selskapet trolig allerede var implementert i krigsplaner hos enkelte nasjoner, med tanke på kraftforsyningens rolle som kritisk infrastruktur (NI6). Informant 8 forteller at det er stor sannsynlighet for at fremmede statsmakter

sitter på informasjon og tilgang til det norske kraftnettet som de kan benytte ved krigssituasjoner. Han mener likevel ikke dette er en overhengende trussel, fordi den politiske situasjonen i Norge og vår relasjon til andre land er relativt stabil. Endrer derimot det politiske klimaet seg, frykter han konsekvensene:

> Havner vi i en konfliktsituasjon med Russland, Kina eller USA ville jeg vært mer bekymret. Veldig bekymret. Risikoen blir jo da så stor at forsvar for et enkelt kraftselskap er fånyttes (...) En angriper vil ha store kapasiteter. Jeg er EN mann, det er måte på hvor mye jeg kan gjøre når det kommer til forsvar. Så det er risikoanalysen min, vi har ikke sjans om "shit hits the fan" (NI8).

Informant 7 forteller at man har sett en økt bevissthet i kriminelle grupper om at kraftbransjen også kan angripes. Slike aktører er ute etter økonomisk gevinst, og forsøker å kryptere systemer for å kunne hente ut løsepenger. I tillegg henviser hun til trusler som følge av det politiske klimaet. "Når vi ser russiske krigsskip i Nordsjøen, må vi kunne regne med at det lurker noen på internett også" (NI7).

5.2.3 Konsekvenspotensial ved uønsket påvirkning

Alle informantene ble spurt om hvilke konsekvenser de anså som potensielle og reelle dersom deres digitale systemer ble utsatt for uønsket påvirkning. Informant 5 forteller at hun vurderer at den største konsekvensen som nettleverandør vil være å få et brudd i strømforsyningen, slik at de ikke kan levere det de er ansvarlige for, nemlig strøm hjem til kundene sine.

Flere av informantene mener at konsekvensene av et cyberangrep på driftskontrollsystemet kan være omfattende, og at det i verste fall kan få konsekvenser for helse, miljø og sikkerhet. Økt fjerntilkobling har også ført til at det vil ta tid å gjenvinne kontroll om slike hendelser inntreffer. Informant 2 forteller at man ved et tjenestenektangrep kan risikere å ikke få koblet inn eller ut, eller gjort omkoblinger i energiforsyningen. Man kan også se for seg å miste kontrollen, eller at andre overtar kontrollen. Det er mulig å bemanne anlegget manuelt, men det tar tid og krever utholdenhet av mannskapet som gjør det (NI2). I ytterste konsekvens kan det ta måneder å bygge opp igjen kraftnettet etter skade på driftskontrollsystemene.

> Har du litt finesse så kan du kanskje klare å steppe opp spenningen inn og ut av trafo, som gjør at du ødelegger utstyret rundt omkring. Hvis du ødelegger større trafostasjoner, så er ikke det akkurat

> hyllevare. Da kan det gå i alle fall uker og kanskje måneder før en får bygget opp igjen kraftnettet. I tillegg kan det gå direkte utover liv og helse hvis en saboterer maskinene som operatørene ser på, hvis de ser at okei spenningen i den trafostasjonen er av, men så er det folk inni der og jobber, og spenningen er på, så kan det gå liv tapt (NI8).

Nødnettet har en levetid på 48 timer. Etter to døgn vil man kunne begynne å se samfunnsmessige konsekvenser av strømbruddet, utover at det blir kaldt og mørkt i husene til folk. Strømbruddet kan føre til at blålysetatene har ikke kommunikasjonsveier lenger. I tillegg vil mobiltelefonnett og dabnett slutte å fungere. Konsekvensene kan være enorme (NI8). Selv om det er enighet blant informantene om at slike hendelser er svært alvorlige, er ikke alle samstemte rundt ideen om at det er en reell fare for en hendelse av slik karakter. Informant 5 argumenterer for at det som foregår i et SCADA-nettverk er relativt konstant. Det samme påpekes av informant 7 som hevder at dersom en ikke gjør endringer vil systemene bare "surre og gå" (NI7). Det er de samme systemene som snakker med hverandre, hvilket betyr at det i teorien ikke skal skje så mye uforutsett. Unntaket er om det dukker opp nye enheter, og om enheter som tidligere ikke har hatt kontakt med hverandre plutselig begynner å snakke sammen, eller snakke opp mot internett. Fordelen med at systemene er koblet sammen er at synligheten i nettet er mye større enn tidligere. Det har ført til at systemet kan kontrolleres på en bedre måte enn før, ved at det sendes varsler umiddelbart om det dukker opp noe unormalt (NI5).

Informant 6 forteller at en avansert aktør kan skru av strømmen om de ønsker det, og om de bruker nok ressurser. Dette er noe han selvsagt håper "de ikke gidder, siden det er så dyrt" (NI6). I tillegg til brudd i funksjonalitet, nevner informanten konsekvenser i form av økonomisk tap, og konsekvenser for deres eksistens som selskap.

> Hvis du har et omfattende løsepengeangrep som går mot backupene våre først, og så alt vi har av data, så vet vi ikke hvem noen av kundene våre er. Da eksisterer vi ikke lenger. Da er det bare å selge kraftverkene, for da er det ikke noe firma lenger (NI6).

Når informantene snakker om konsekvenser av uønskede hendelser rettet mot AMS, forteller flere om konsekvenser som først og fremst er alvorlige for virksomhetens drift, som økonomiske konsekvenser internt, eller for kraftmarkedet som helhet. "AMS er jo et veldig viktig system for

oss. Det er jo det som er faktureringsgrunnlaget vårt. Hvis måleverdiene ikke blir sendt til Elhub, og vi ikke har det selv, så vil vi miste faktureringsgrunnlaget" (NI2).

Utrullingen av avanserte målesystemer har vært gjenstand for diskusjon og debatt når det kommer til personvern. Målerne gir svært nøyaktig data om kundene. Det vil kunne være mulig å hente ut personopplysninger og opplysninger om rutiner, vaner og oppholdstid i hjemmet på bakgrunn av strømforbruket. Dette er opplysninger som kan misbrukes, og som skaper bekymring for bransjens konfidensialitet og integritet. I tillegg står de i fare for å oppleve et massivt omdømmetap dersom opplysningene skulle bli lekket og misbrukt (NI2). Likevel er ytterste konsekvens av uønsket påvirkning på AMS at det får konsekvenser for liv og helse, eksempelvis for mennesker som har medisinsk utstyr hjemme som de er avhengige av strøm for å bruke (NI3).

To av informantene snakker om konsekvenser som kan oppstå som følge av påvirkning på integrerte systemer, og henviser til Hydro-hendelsen og konsekvensene av denne. De forteller at hackerne fikk tilgang til industrikonsernets integrerte systemer etter at en ansatt åpnet en infisert e-post. Hendelsen førte til store tilgjengelighetsproblemer og økonomiske tap, og er et godt eksempel på konsekvenser som kan oppstå dersom angripere får innpass i administrative systemer (NI5; NI7). I tillegg kan handelssystemet Nordpool bli berørt, og gi utslag på børsen for krafthandelen (NI7).

Videre hevdes det at administrative systemer ikke er kritisk for selve driften av kraftselskapene og forsyningssikkerheten, men at driften likevel kan forstyrres ved uønsket påvirkning. Forstyrrelser på de administrative systemene vanskeliggjør den daglige kontakten med Statnett, hvor strømproduksjonen for neste dag reguleres. Konsekvensen av kommunikasjonsstopp mellom disse kan være at det produseres feil mengde strøm. Dette kan føre til ubalanse i nettet, som videre kan få fysiske konsekvenser (NI7).

Alle informantene vi har snakket med bruker skytjenester i sin virksomhet. Det kan eksempelvis være Teams, Skype, mail, eller Workplace, som brukes for kommunikasjon internt. Her utpekes samhandlingsproblemer som den største utfordringen ved svikt, da en er nødt til å ringe eller besøke hverandre på kontoret for å kommunisere. Dette er lite effektivt (NI2). Utilgjengelighet til

informasjonssystemer, kan også påvirke evnen til å innhente informasjon daglig, og til å fakturere kunder. Det er ikke den mest alvorlige konsekvensen i det store bildet, men vil kunne forstyrre driften (NI5). Informant 2 er enig i at konsekvensene av svikt i skytjenestene på kort sikt ikke er så store, men at de vil kunne bli det dersom tjenestene er utilgjengelige over tid. Han peker spesielt på situasjoner hvor man er ekstra avhengig av denne type tjenester, som i disse tider (Covid-19) hvor stort sett hele bransjen har hjemmekontor, og hvor all kommunikasjon foregår via skytjenester (NI2). Informant 8 er skeptisk til utviklingstrenden hvor stadig flere systemer legges i skytjenester:

> Det er jo snakk om SCADA i skyen. Jeg er jo kjempeskeptisk til spesielt sånn type SCADA i skyen, for det vil være ekstremt attraktive mål for uvedkommende. Plutselig har du ikke bare ett kraftselskap, men du har kanskje ti eller hundre kraftselskap sine styringssystemer på en plass. Det er en fantastisk mulighet til å få gjort mye skade eller få mye informasjon. Sentralisering av sånne systemer liker jeg i utgangspunktet ikke tanken på, og jeg har helt ærlig ikke tatt kjempestilling til det heller. For meg er det utopi at vi skal havne på en sånn plass (NI8).

5.2.4 Analyse av funn

Empiriske funn viser at det er variasjoner i hvordan aktørene oppfatter og forstår risikoen for cyberhendelser. Variasjonen er tilstede både når aktørene tolker begrepet cyberrisiko, og når de reflekterer rundt hvilke farer og trusler de mener bransjen står overfor som følge av sektorens digitale utvikling. Aktørenes oppfatning av cyberhendelser kan derfor ses i sammenheng med hvordan de tillegger begrepet mening, hvordan de mener bransjen kan rammes, og hvilke farer og trusler de mener er risikobefengt.

Ulik risikoforståelse

I kapittel 3 forklares begrepet cyberrisiko som "risikoen for finansielt tap, operasjonelle forstyrrelser eller skader forårsaket av svikt i digital teknologi implementert for å støtte informasjon eller operasjonelle funksjoner" (NIST, 2017). I intervjuene ble alle informantene spurt om å forklare begrepet cyberrisiko ut fra deres egen forståelse. Tilnærmet alle informantene tolker begrepet ulikt, men et flertall forstår begrepet i tråd med risiko for tilsiktede hendelser. Derimot knytter alle informantene begrepet opp mot sektorens digitale utvikling, hvilket tyder på at alle forståelsene inkluderer visse aspekter av definisjonen på cyberrisiko fremlagt av NIST (2017). En

kan derfor argumentere for at samtlige informanter forstår det som at digitaliseringen i sektoren medfører cyberrisiko, men at det er variasjoner i den teoretiske tilnærmingen til begrepet og hva den faktiske risikoen kan innebære.

I kapittel 3 redegjøres det for øvrige tilnærminger til risikobegrepet. Det fremkommer her at risiko kan forstås som en kombinasjon av sannsynlighet og konsekvens med tilhørende usikkerhet (Aven, 2015), og som et sammensatt konsept bestående av parameterne trussel, sårbarhet og verdi (Engen et al, 2016; ISO 27005: 2018). Avens risikoforståelse ser vi tydelig hos informant 3, som eksplisitt nevner sannsynlighet og konsekvens for tilsiktede hendelser. Risiko forstått gjennom parameterne trussel, sårbarhet og verdi nevnes derimot implisitt av informant 4, og delvis av informant 5, hvor særlig førstnevnte omsetter begrepet i scenariotekning og knytter dermed risikoen til tenkte potensielle tilsiktede cyberhendelser.

Ettersom aktørene ikke har en felles forståelse av begrepet cyberrisiko, kan det som informant 7 påpeker være grunn til å vurdere hvorvidt det er hensiktsmessig å benytte seg av definisjoner som tolkes såpass subjektivt og forskjellig.

Safety og security

Aktørene oppfatter farer og trusler som følge av bransjens digitalisering som sammensatt av et bredt spekter av potensielle hendelser. Det er videre interessant at tilnærmet alle aktørene forteller at slike hendelser kan være et resultat av både målrettede og utilsiktede forhold, selv om begrepet cyberrisiko tolkes i retning tilsiktede hendelser av flertallet. Blant annet møtte vi motstand hos informant 3, når vi på oppfordring fra vedkommende forklarte at cyberhendelser også kan være utilsiktede. Noe av dette kan forklares med at terminologien tillegges ulikt innhold, og det kan virke som at informantene kobler konseptet "cyber" til trusler. Dette utfordrer på et vis sammenhengen mellom risiko- og sikkerhetsforståelsen hos aktørene, ved at risikoen kobles til tilsiktede hendelser, mens utfordringer når det gjelder sikkerhet består av både farer og trusler.

Et annet funn er at informantene forbinder cyberhendelser til menneskene som opererer i systemene, trusler som kan forstyrre systemene, eller teknologien i seg selv, hvilket tyder på at aktørene forstår at digitaliseringen i sektoren åpner opp for et mangfold av endepunkter hvor

hendelser kan initieres, hvilket samsvarer godt med funn i delkapittel 5.1. Det kan derfor argumenteres for aktørene implisitt forstår cyberrisiko som både risikoen for tilsiktede og utilsiktede hendelser ved at de inkluderer både "safety" og "security" når de omtaler cyberhendelser, selv om terminologien i større grad kobles til "security". Dette kan ses i sammenheng med hvordan Hovden (2004) nevner at sikkerhet kan utfordres av et mangfold potensielle hendelser og at slike hendelser derfor må forstås i lys av flere sikkerhetsdimensjoner.

Det kan være vanskelig å avgrense potensielle hendelser til å være enten en fare eller trussel, hvilket informant 7 trekker frem ved å si at en trusselhendelse kan være utilsiktet generert. Dette tyder på at det er diffuse skiller mellom farer og trusler når det kommer til digitalisering, men at det i bunn og grunn er relevant å hanskes med begge. Dette kan ses i sammenheng med Sivertsens (2007) uttalelser om at forstyrrelser på digitale systemer vil kunne reagere likt uavhengig om en hendelse er tilsiktet eller utilsiktet, hvilket informantene også ser ut til å være oppmerksomme på gjennom sine uttalelser.

Selv om diskusjonen viser at det er overensstemmelse blant informantene om at cyberhendelser kan være et resultat av både tilsiktede og utilsiktede hendelser, er det store variasjoner i hvordan de forteller om slike hendelser. Grunnen kan være at det har vært få cyberhendelser hittil i den norske kraftsektoren som har generert alvorlige konsekvenser. Tidligere forskning har også vist at risiko tilknyttet angrep og funksjonsfeil på digitale systemer har vært ansett som lav av aktører i norsk kraftsektor (Røyksund, 2011; Skotnes, 2015). Funn i denne studien indikerer derimot at selv om det forekommer få hendelser, oppfatter flere av aktørene risikoen som tilstede, hvilket viser at det har skjedd en utvikling i risikoforståelsen.

I kapittel 3 definerte vi sikkerhet som en "reell eller oppfattet tilstand som innebærer fravær av uønskede hendelser, frykt eller fare" (NS 5830:12, s. 4). Hvorvidt aktørene oppfatter trusler og farer som reelle kontra potensielle er også preget av nyanseringer. Det kan derfor tenkes at aktørene per nå oppfatter risikoen for cyberhendelser som en sinnstilstand, hvilket kan forklares med at det er variasjoner i oppfatninger tilknyttet hva risikoen kan være. Realiteten rundt digitaliseringens innvirkning på bransjens risikostruktur har vært under diskusjon i delkapittel 5.1. Som Hovden (2004) presiserer er det viktig at man har forståelse for mulige konfliktsituasjoner mellom oppfattet

og reell virkelighet. Det er derfor sentralt at aktører som jobber med sikkerhet er oppmerksom på at det kan foreligge et slikt misforhold.

Et annet interessant aspekt fremkommer av informantenes uttalelser om konsekvenser av uønsket påvirkning. Som ved cyberrisiko, forteller de også her tilnærmet utelukket om konsekvenser initiert av tilsiktede hendelser. Hvorfor slike hendelser forbindes med større konsekvenser er uvisst, men på et vis kan det tyde på at de oppfatter at slike hendelser er beheftet med større usikkerhet og mindre grad av kontroll enn utilsiktede hendelser.

5.2.5 Delkonklusjon

Analysen viser at det ikke er enkelt å gi et entydig svar på hvordan aktørene forstår risikoen for cyberhendelser. Risikoen forstås ulikt blant aktørene, og begrepet cyberrisiko tillegges ulikt innhold. Det vi derimot kan slå fast, er at det er en felles oppfatning om at digitaliseringen i sektoren medfører både farer og trusler. Dette kan derfor indikere at aktørene forstår konseptet cyberrisiko som sammensatt at begge former for risikoforhold, selv om den terminologiske tilnærmingen er ulik. Dersom man sammenfatter svarene til samtlige informanter er det grunn til å anta at aktørene oppfatter at risikoen de står overfor som følge av digitaliseringen er mangfoldig, dynamisk og vanskelig å definere. Likevel er det paradoksalt nok de tilsiktede handlingene som trekkes frem når aktørene snakker om konsekvenspotensial. Det er derfor belegg for å anta at aktørene i den norske kraftforsyningen ser på cyberhendelser i form av trusler, og ikke farer, som mest risikobefengt.

5.3 Hvilke metoder benyttes i risikovurderingsprosessen, og hvilke farer og trusler vektlegges?

I besvarelsen av det tredje forskningsspørsmålet vil det empiriske grunnlaget skissere overgangen til aspektet ved problemstillingen som omhandler risikohåndtering. Dette gjøres gjennom å kartlegge hvilke metoder og tilnærminger som benyttes i risikovurderingsprosessen, og hvilke farer og trusler som vektlegges. Kartleggingen benyttes videre til å avdekke hvilke forutsetninger som legges til grunn for aktørenes arbeid med cybersikkerhet, og til å se om det kan underbygge antakelsen om at risikovurderinger kan påvirke den videre håndteringen av bransjens cyberrisiko.

5.3.1 Tilnærminger til risikovurderinger

Ved spørsmål om hvilke metoder som benyttes for risikovurderinger relatert til digitaliseringsprosesser og systemendringer, forteller flere av informantene at de vurderer risiko som et resultat av sannsynlighet og konsekvens. NVEs veileder i risiko- og sårbarhetsanalyser for kraftforsyningen brukes ofte som utgangspunkt (NI1; NI5; NI6). Tre av informantene har tilpasset metoden etter inspirasjon fra eksterne samarbeidspartnere, som også tilrettelegger for å vurdere risiko ut fra sannsynlighet og konsekvens (NI2; NI3; NI4).

Ved ett tilfelle var ikke NVEs veileder kjent for intervjuobjektet. Vedkommende forteller at selskapet forholder seg til kraftberedskapsforskriftens kapittel 6 og 7 når de gjennomfører risikovurderinger av digitale systemer. Selve metoden består av en standard ROS-analyse hvor man identifiserer risikomomenter tilknyttet de ulike systemene, før man foretar en vurdering av sannsynlighet og konsekvens. Dette inkluderer en vurdering av hvilke sikkerhetsutfordringer systemet kan medføre, hvilke typer informasjon som ligger der, og hvilke systemer det er knyttet opp mot (NI8).

Risikovurderingsprosessen starter med en identifisering av uønskede hendelser som benyttes videre i en grovanalyse før hendelsene plasseres inn i ulike kategorier (NI5). Informant 6 understreker at det kreative forarbeidet hvor man fremprovoserer gode scenarier er spesielt viktig, særlig i forbindelse med IKT og bransjens pågående digitalisering. Risikovurderingene i bransjen er preget av lange tider med fokus på flom trær og linjer, og trenger at noen tør å lage scenarioer som kobles til en "høy og skummel verdi. Da er du egentlig i mål". Sannsynlighet og konsekvens anses av informanten som noe man "slenger på til slutt" (NI6).

Selv om informantene som har bidratt til denne studien vurderer risiko ut fra sannsynlighet og konsekvens, påpekte flere at de hadde sett tilfeller hos andre selskaper hvor de hadde benyttet seg av en trefaktortilnærming. Dette henger sammen med størrelse og ressurser ifølge informant 1, som antar at de små selskapene har nok med å forholde seg til kjent og kjær praksis. Samtidig tenkes det at endringer hos de store vil lede til påfølgende endringer hos de små "når de store begynner med dette, så vil de små komme etter" (NI1).

5.3.2 Behov for å tenke nytt

Problematikken rundt utdaterte og utilstrekkelige metoder påpekes av flere av informantene. Blant annet mener informant 5 at veilederen fra 2010 er utdatert i forhold til digitaliseringens hastighet, og svekker evnen til å risikovurdere digitale informasjonssystemer. Informant 6 mener at metodene som benyttes i selskapet ikke er tilstrekkelig i en tid hvor bransjens risikobilde er i drastisk endring. Likevel mener han at det først og fremst er viktig "å få de mest relevante risikoene på bordet i det hele tatt" og at de derfor per nå har "mer enn nok med sannsynlighet og konsekvens" (NI6). Behovet for å implementere nye relevante risikoscenarier understrekes ved at statistisk relevante hendelser som eksempelvis værforhold har vært prioritert, i motsetning cyberhendelser. Ved gjennomgang av tidligere analyser hadde han også kommet over risikovurderinger hvor cyberrisiko var kraftig nedprioritert (NI6).

Cyberhendelser, spesielt tilsiktede, krever nye former for risikovurderinger. Vurderingen må fokusere mindre på sannsynlighet, "ellers blir risikoen så liten. Selv om det ikke har skjedd før i Norge, så må vi være forberedt på at det endrer seg fort og plutselig kan skje" (NI2). Behovet for å tenke annerledes i gjennomføringene av risikovurderingene påpekes også av informant 5. Hun begrunner behovet med at sannsynligheten for at uønskede cyberhendelser inntreffer, øker som følge av digitaliseringen, og da må konsekvens- og sannsynlighetsvurderinger følge etter. Hun forteller at det nå jobbes med å tilpasse rammeverket slik at cyberrisiko ikke blir nedprioritert (NI5).

Et annet nevneverdig poeng er ifølge informant 6 at lovkrav til hva som skal risikovurderes har kommet sent gitt digitaliseringens hastighet. Selv om han mener at man ikke skal lene seg på lovkrav, men være proaktiv selv, er det mange som forholder seg til slike retningslinjer. Er ikke retningslinjene på plass, kan det oppstå situasjoner hvor aktører glemmer å tenke nytt i arbeidet med cybersikkerhet (NI6).

> Det lovverket vi har er jo også jækla treigt. Det var jo ett år siden det det begynte å gjelde at administrative systemer skulle risikovurderes. Ett år siden. Det er jo helt sprøtt. Ikke at det er noen unnskyldning, vi skulle vært der av oss selv (NI6).

5.3.3 Vektlegging av farer og trusler

Ifølge informant 1 har digitaliseringsprosesser i og utenfor sektoren generelt vært preget av lite fokus på sikkerhet, men dette bildet er nå i ferd med å endre seg. Samtidig mener informant 2 og 5 at det kan være utfordrende å endre fokus i en bransje hvor hendelsene er tydelig overrepresentert ved farer og utilsiktede forhold. Det poengteres videre at de har et stort forbedringspotensiale når det kommer til å implementere cyberrisiko i vurderingene på lik linje med tradisjonelle hendelser som vær og vind.

> Vi forsøker jo å få med hele bildet, men det overskygger jo veldig det med ubevisste handlinger. Hvis du setter opp et pai-diagram så er det liksom 99 % av hendelsene som skyldes været, så det er klart det får mye fokus. Men vi prøver jo også å holde fokuset oppe på det som gjelder bevisste handlinger. Selv om det ikke har skjedd før, så vil konsekvensene være store hvis det skjer (NI2).

Informant 6 sier at de vektlegger trusler og farer likt, men at disse ikke utelukkende omhandler farer og trusler tilknyttet digitalisering. Det kan de heller ikke gjøre, ettersom bransjen fortsatt er utsatt for påkjenninger gjennom værforhold som ikke direkte kan kobles til digitaliseringen. Samtidig mener han at risikoen som presenteres per nå ikke er representativ for bransjens digitale utvikling, og en av hans store agendaer er å få informasjonssikkerhetsscenarier inn i alle pågående risikovurderingsprosesser på alle nivåer (NI6). Uten implementering av relevante scenarier mener han hele prosessen vil være nytteløs, og at det er ved slike tilfeller man "går på en smell". For å få til denne endringen må risikoen kobles til sentrale verdier (NI6).

5.3.4 Fra risikovurdering til praktisk sikkerhetsarbeid

Informantene forteller at funn fra risikovurderingene setter rammene for hvordan aktørene skal håndtere risikoen i praksis. Ifølge informant 2 gjøres dette ved å etablere nye barrierer, eller ved at man reduserer risikoen til et akseptabelt nivå. Det er viktig at risikovurderingene følges opp. Selskapet til informant 2 har tidligere fått kritikk for mangler på dette området:

> Vi har fått litt kritikk på dette området. Da fikk vi blant annet tilbakemelding på at vi ikke var tydelige nok på å sette eierskap og frister på det som ble definert som uakseptabel risiko. Så det har vi veldig fokus på nå, at all uakseptabel risiko blir tildelt en eier, eller en ansvarlig og en tidsfrist, slik at det ikke er noe som bare blir beskrevet også blir det ikke gjort noe med (NI2).

Informant 6 deler samme oppfatning, og sier at de også har opplevd utfordrende situasjoner hvor ingen egentlig tar ansvar for den uakseptable risikoen:

> Vi kjenner veldig på dette med litt sånn pulverisering av ansvar. Både internt og eksternt. Internt mellom miljøene våre. Vi har liksom IT, vi har OT, vi har forskjellige gjenger og vi har fibergjengen i midten liksom. Der kommer ting til å falle mellom stoler, og det å snakke sammen der sier vi hele tiden er viktig, men så faller man tilbake i hverdagen hvor alle skal oppnå sine mål (NI6).

Informant 5 fremhever viktigheten av å mitigere risikoen gjennom etablerte strukturer. Det viktigste er å ikke stå igjen med uakseptabel risiko ved de digitale systemene. Risikoen må reduseres før man i det hele tatt implementerer løsningen (NI5). Det er likevel ikke i alle tilfeller det settes inn risikoreduserende tiltak, og flere av informantene mener at det ikke alltid er hensiktsmessig at enhver risiko skal reduseres til et minimum:

> Det handler om å redusere risikoen, altså summen av sannsynlighet og konsekvens til et akseptabelt nivå, og så lavt som fornuftig. Det betyr ikke at en skal reduserer ethvert funn ned til et minimum uavhengig av alle andre faktorer. En risiko du mener du kan leve med skal ikke nødvendigvis reduseres hvis det koster veldig masse (NI3).

5.3.5 Analyse av funn

Det er flere likheter hos informantene når det kommer til hvordan de gjennomfører risikovurderingsprosessen. Sammenstillingen av svar viser også at det er NVEs veileder fra 2010 som benyttes som referanse hos et flertall av informantene. Hvor dette ikke er tilfelle benyttes liknende fremgangsmåter. ROS-analyser består derfor hos de aller fleste av informantene av kvalitative analyser som fastsetter risiko ut fra parameterne sannsynlighet og konsekvens.

Statistisk relevante hendelser

Gjennom forskningen har det dukket opp flere forklaringer på hvorfor metoder i tråd med ovennevnte prinsipper fortsatt er utbredt i sektoren. Som Aven (2015) og Rausand (2011) skriver, starter ofte en risikoanalyse med at man benytter tilgjengelig informasjon til å identifisere relevante farer og trusler. Som et stort flertall av informantene forteller, er det statistisk relevante hendelser i form av vær og vind som står for majoriteten av hendelsene i bransjen, og det er derfor disse hendelsene som utgjør det største erfaringsgrunnlaget. Informantenes uttalelser tyder på at det kan

være utfordrende å inkludere cyberhendelser på lik linje med statistisk relevante hendelser, nettopp fordi det er så lite erfaring og tilgjengelig informasjon tilknyttet slike hendelser i Norge.

At dette kan være problematisk fremheves av samtlige informanter, og særlig uttalelsene til informant 6, 5 og 2 understøtter at det er utfordringer tilknyttet erfaringsgrunnlaget analysene baseres på. Argumentasjonen til informant 2 sine uttalelser om at alvorlige cyberhendelser i Norge er få, spesielt rettet mot kraftsektoren, kan bidra til å forklare dette. Det er derfor mye som tyder på at erfaringsgrunnlaget og informasjon for å etablere kontekst for vurderingen, bør hentes fra andre steder enn Norge, og fra andre sektorer enn kraft.

Diskusjonen over belyser et tydelig paradoks. Metodikk i tråd med Aven (2015), Rausand (2011), og NVE (2010), bidrar til at risiko og risikoaksept vurderes basert på sannsynlighet og konsekvens. Mangel på erfaring og statistikk tilknyttet cyberhendelser i norsk kraftsektor kan gjøre at slike hendelser står i fare for å bli nedprioritert, ved at de tildeles lav sannsynlighet eller utelates i kartleggingen av potensielle farer og trusler.

Utfordringer

I forlengelsen av diskusjonen over kan det tenkes at overnevnte metodikk vanskeliggjør risikostyring av cyber. Som teorien trekker frem er risikostyring en viktig oppgave for virksomheter som er utsatt for risiko gjennom sine aktiviteter (Aven, 2015). Som illustrert i kapittel 5.1 introduserer digitaliseringen i bransjen nye risikoforhold, hvilket indikerer at en sentral oppgave for sektoren er å styre risikoen slik at det ikke oppstår uønskede situasjoner. Baseres analysen kun på erfaringer og statistisk relevante hendelser, kan det utfordre muligheten til å skaffe innsikt i disse nye risikoforholdene, hvilket potensielt kan vanskeliggjøre videre praktisk håndtering.

Med utgangspunkt i diskusjonen er det rimelig å anta at de metodiske tilnærmingene som per nå er utbredt i sektoren vil undergrave aktørenes mulighet til å vurdere risikoen tilknyttet cyberhendelser på lik linje med andre hendelser. Dette fordi sannsynlighetsvurderingen vil kunne proklamere at risikoen er lav. Argumentasjonen støttes også av empirien, hvor informantene kommuniserer at vurderingen av cyberrisiko utfordres av de metodiske tilnærmingene som per nå

er utbredt. Som trukket frem i teorien setter ROS-analysen videre rammer for risikoevalueringen. Risikoevalueringen viser ifølge Aven (2015) og Rausand (2011) til prosessen hvor beslutninger fattes basert på resultatene til risikoanalysene. Det kan derfor tenkes at ROS-analysen vil kunne påvirke videre beslutninger dersom cyberhendelser tildeles lav sannsynlighet. Det kan derfor argumenteres for at dersom man nedprioriterer cyberhendelser i vurderingene vil de sannsynligvis også bli nedprioritert i det praktiske sikkerhetsarbeidet.

Resultatene av diskusjonen tilsier at det kan være et behov for å bruke en annen metode i styringen av cyber. Den foreløpige tilleggsveilederen til Kraftberedskapsforskriften (NVE, 2018b) som presenteres i teorien støtter opp under samme antakelse, og fremmer at spesielt tilsiktede hendelser bør inkludere en kartlegging av verdier, trusler og sårbarheter, hvilket implisitt viser til trefaktortilnærming (Busmundrud et al, 2015). Av informantene vi intervjuet var det per nå ingen som benytter slike tilnærminger, men det fantes tilfeller i sektoren forøvrig hvor disse tilnærmingene var tatt i bruk. Med utgangspunkt i informant 1 sine uttalelser om at bransjen lærer av hverandre vil en kunne anta at aktørene vil tilegne seg nye metoder om de viser seg å være hensiktsmessige.

Det er likevel interessant at forskriften anbefaler andre metodiske tilnærminger i vurderingen av tilsiktede hendelser når kapittel 5.2 avdekket at flere av informantene mener hendelser som i utgangspunktet er tilsiktet kan være utilsiktet initiert. Dette viser indirekte at slike risikoforhold til dels er avhengig av hverandre for å kunne forårsake kritiske konsekvenser. I tillegg poengteres tilsiktede feil som en reell fare. Eksempelvis belyser kapittel 5.1 og 5.2 at det være mennesker uten tilsiktede motiver som ofte utløser farepotensialet. En kan derfor argumentere for at risikovurderingene må ta høyde for både farer og trusler, og at det kan være problematisk å skille de i en praktisk vurdering. Som det fremkommer i teorien kan farer også omsettes i en sikringsrisikovurdering, hvilket gjør den anvendbar til vurdering av begge former for hendelser (Engen et al, 2016).

Et annet interessant aspekt finner vi i uttalelser fra informant 6 om at lovgivning har kommet sent gitt digitaliseringens hastighet. Ettersom et stort flertall forholder seg til veilederen fra 2010 kan det tyde på at aktørene vil følge retningslinjer og anbefalinger fra myndigheter, hvilket gjør at det

kan tenkes av metodiske tilnærminger vil endres i takt med anbefalte retningslinjer og erfaringsutveksling.

5.3.6 Delkonklusjon

Oppsummert kan vi slå fast at aktørene i denne studien benytter seg av analysemetoder hvor risiko vurderes ut fra parameterne sannsynlighet og konsekvens i risikovurderingsprosessen. I tillegg er det relativt tydelig at de farer og trusler som vektlegges fortsatt er dominert av forhold uten direkte kobling til sektorens digitale utvikling. Det er statisk relevante hendelser som vær- og vindforhold som utpeker seg. Selv om forskningsspørsmålet virker ukomplisert, har det gjennom forskningen likevel dukket opp en rekke problemstillinger tilknyttet risikovurderingsprosessen, særlig med henblikk til vurderingen og inkluderingen av cyberrisiko. De tilnærmingene som per nå er utbredt i sektoren kan føre til at slike risikoforhold blir nedprioritert, ved at sannsynligheten anses som lav. Likevel viser analysen i 5.1 at konsekvenspotensialet kan være omfattende i et komplekst og tett koblet system. Sammen med uttalelser om at det ofte er funn fra analysene som setter rammer for videre håndtering, er det rimelig å anta at metoder som tilrettelegger for å nedprioritere cyberhendelser (gjennom sannsynlighetsvurdering) vil kunne påvirke risikostyringen av cyberrisiko i negativ retning. I tillegg viser funn at informantene mener det ikke er nødvendig at enhver risiko mitigeres dersom sannsynlighet eller konsekvens vurderes som lav. Dette kan potensielt medføre at aktørene velger å leve med cyberrisiko som følger av digitaliseringen, heller enn å redusere den.

5.4 Hvilke organisatoriske betingelser har betydning for aktørenes evne til å håndtere cyberrisiko?

For å besvare det siste forskningsspørsmålet vil vi først presentere betingelsene informantene mener fremmer et godt sikkerhetsarbeid. Vi antar at de organisatoriske betingelsene vil kunne legge føringer for hvordan cyberrisiko håndteres innad i organisasjonen og i bransjen som helhet. Derfor presenteres også ulike utfordringer som ifølge informantene kan virke hemmende for sikkerhetsarbeidet. Eksempler på opplevde hendelser avklarer hvordan slike mekanismer fremstår ved praktisk håndtering av hendelser, og danner sammen med øvrige betingelser grunnlag for å analysere funnene i tråd med teorier om sikkerhet i organisasjoner.

5.4.1 Organisatoriske betingelser som fremmer godt sikkerhetsarbeid

Forankring i ledelsen

På spørsmål om hva som anses som viktige betingelser for et godt cybersikkerhetsarbeid svarer informant 8 at det aller viktigste er forankring i ledelsen. At ledelsen er tydelig på viktigheten, mener han er veldig viktig for vellykket IKT-sikkerhetsarbeid (NI8). Det samme poenget trekkes frem av informant 5, som forteller at ledelsen i selskapet er veldig interessert i sikkerhet, inkludert cybersikkerhet. Informanten, som er IKT-sikkerhetsrådgiver, er jevnlig inne i ledergruppen i løpet av året, hvor hun presenterer trusler og farer selskapet står overfor. Videre hevder hun at forankring i ledelsen trolig også vil påvirke kunnskapsnivået til øvrige ansatte:

> Kunnskapsnivået er nok ikke så veldig stort all over, men jeg tenker vi har en ledelse som er veldig interessert i det, og sikkerhet er et ledelsesansvar. Uten forankring i ledelsen så kommer man ingen vei (NI5).

Oppfatningene til informant 5 og 8 deles av øvrige informanter. De forteller at sikkerhet er noe som angår alle, og ikke bare noe IT-avdelingen skal sitte alene med på et eget rom. Hvis ledelsen er med på laget, og greier å kommunisere dette videre nedover i organisasjonen, har man kommet langt på vei (NI4;NI7).

Informant 8 skisserer hvordan forankring i ledelsen sikrer at arbeidet med cybersikkerhet får et vedvarende fokus. I deres organisasjon var IKT-sikkerhet ett av fem prioriteringsområder de neste tre årene. Han mener også at ved å ha ledelsen med på laget, sikres det at stillingen han selv besitter, og IT-avdelingen generelt, ikke blir sett ned på av andre i firmaet. Akkurat denne situasjonen hadde han opplevd tidligere i et annet selskap. "Hvis IT blir uglesett av ledelsen så blir de uglesett av alle i firmaet. Jeg har jobbet i et selskap hvor det har vært sånn, og det er ikke så veldig artig" (NI8). Han forteller videre:

> Litt av grunnen til at de andre i selskapet ikke anser meg som en paranoid type tror jeg faktisk skyldes at fokuset på IKT-sikkerhet kommer fra ledelsen. Ledelsen har veldig fokus på det, og er veldig bevisste på det. I alle allmøter er det et eget punkt om akkurat IKT-sikkerhetsarbeid i organisasjonen, og dette kommer fra administrerende direktør (NI8).

Ved tilfeller hvor ledelsen ikke har forståelse for risikoen som følger med digitaliseringen blir det opp til den enkelte avdeling, eller de som sitter med ansvaret for systemene å kommunisere

sikkerhetsbehovet. Da blir personlige egenskaper en viktig faktor for å kunne formidle sentrale problemstillinger tydelig (NI6). Det kan derimot være utfordrende nok å håndtere risikoen, uten å hele tiden måtte overbevise ledelsen og andre ansatte om at det er viktig. "Du må jo nesten være en SoMe Gud, hvor du kommuniserer behovet, og legger ut noe hver dag parallelt med at du håndterer disse risikoene" (NI6). At ledelsen lytter til fagfolk, og at de opplever at de blir hørt, er dermed svært viktig. Ikke minst er det viktig at en får de ressursene som trengs for å iverksette tiltakene. "Slik er det med alt beredskapsarbeid og sikkerhetsarbeid" (NI3).

Informant 6 mener veien videre bør lede til situasjoner hvor IKT-sikkerhetsansvarlig (CISO) sitter ved bordet på lik linje med resten av ledelsen. "Det tøffeste er når CISO-rollen er med i konsernledelsen, da er det skikkelig action" (NI6). I deres tilfelle forteller han at CISO-rollen sitter under digitaliseringsdirektøren, men at den pågående digitaliseringen i kraftsektoren kan tilsi at situasjonen bør endres.

> Tenk når CISO sitter ved bordet parallelt med de andre i konsernledelsen og snakker om muligheter og risiko. Det er jo noen organisasjoner som har kommet seg dit og der kommer kanskje vi også etterhvert. For det er jo klart at nå når digitaliseringen tar fart og du snakker om enkeltrisikoer med sånn 700 millioner konsekvenser, så må du liksom dele informasjon om det (NI6).

Tydelige organisatoriske strukturer og ansvarsområder

Flere av informantene peker på viktigheten av tydelige roller, og at alle vet hvilket ansvar de har. "Det høres gjerne opplagt ut, men det er ikke like opplagt rundt omkring" (NI2). Informant 4 forteller at tydelig definerte roller vil legge til rette for at det ikke skal være noen tvil om hvordan en skal handle dersom en får et problem med sikkerheten:

> Det er viktig med tydelige roller hvis det skjer et eller annet, og det må være tydelig hvem som skal gjøre hva og egentlig hvordan du håndterer det hvis du skulle få en eller annen utfordring med sikkerheten (...) og i forbindelse med dette kjører jo konsernet hele veien sikkerhetskampanjer på hvordan du håndterer forskjellige uønskede hendelser (NI4).

Videre er korte og tydelige rapporteringsveier en sentral faktor, som i praksis betyr at man ikke må gjennom mange nivåer hvis det har hendt noe alvorlig (NI2). Dette trekkes også frem av informant 8:

> I og med at organisasjonen er så liten så vet jeg hvem jeg skal kontakte i ulike situasjoner. Og på samme vis, hvis andre oppdager IKT-relaterte ting så vil de ta kontakt med enten sjefen min eller meg direkte, uansett tid på døgnet egentlig (NI8).

Erfaringsutveksling og kommunikasjon

Delingskultur trekkes også frem som en viktig faktor. At erfaringer deles med andre innad i organisasjonen er viktig for å skape en felles forståelse for de risikoene en står overfor, og øker villigheten blant de ansatte til å bidra med det de kan. Informant 8 forteller at han deler alt han har av relevant informasjon med alle ansatte i selskapet, og mener dette bidrar positivt til brukeropplæring. Dette er viktig ettersom alle ansatte på hver sin måte kan være en styrke eller svakhet i selskapets helhetlige cybersikkerhet (NI8).

Den samme informanten forteller at de har etablerte rutiner innad i organisasjonen for varsling av uønskede sikkerhetshendelser. Blant annet har de en SMS-varslingstjeneste de tar i bruk ved hendelser av både mindre og større omfang. Slike SMS-tjenester er noe en finner i alle kraftselskap, da de er ment for ekstern bruk. Likevel kan tjenesten også benyttes internt, noe de selv hadde gjort ved en tidligere hendelse (NI8).

Ifølge informant 6 er det også viktig å få de ulike sikkerhetsmiljøene innad i konsernet og på tvers av selskaper til å kommunisere godt. Selv sitter han som IKT-sikkerhetsleder i et konsern med flere underlagte KBO-enheter. Å sikre at sikkerhetsnivået er jevnt over godt hos de underlagte selskapene er derfor viktig, i og med at en endring i systemet et sted, potensielt kan påvirke øvrige selskaper og funksjoner. Han forteller at kulturen og interessen for samhandling er der, men det er likevel faktorer som påvirker hvorvidt man faktisk har mulighet til å følge opp slike strukturer jevnlig (NI6).

> Interessen er der, du har IT og OT som liker det her, men det går mer på at alle føler seg nedjammet i hverdagen. Så det å huske å dele, og sette en kultur hvor det deles, det tar tid, og man må tenke veldig lurt. Det er velvilje om å sparre, men plutselig har det gått to uker før man har snakket sammen igjen og da vet man ikke hva de andre holder på med (NI6).

Videre forteller informanten at han deltar i et sikkerhetsråd, hvor alle IKT-sikkerhetskoordinatorene fra de underlagte KBOene sitter. I sikkerhetsrådet deles sikkerhetshendelser og annen relevant informasjon, noe som fremmer en slags delingskultur på tvers av de underlagte selskapene og konsernet. Ellers er det litt opp til den enkelte som opplever hendelser eller andre problemer å løfte det opp til relevante fora og personer (NI6).

Informant 2 forteller at selskapet har ulike kommunikasjonslinjer hvor de formidler uønskede hendelser innad i virksomheten. Avvikssystemet er ment for hendelser av mindre omfang, og tilrettelegger for at ansatte fortløpende kan registrere avvik. Er hendelsen alvorlig er det lagt til rette for å rapportere til mailadresser eller å opprette telefonisk kontakt, slik at beredskapsorganisasjonen får beskjed og kan planlegge for videre håndtering. De samme arenaene for rapportering og kommunikasjon fremmes også av informant 3, 4 og 5. Derimot forteller informant 3 at det ikke alltid er ønskelig å kommunisere alle hendelser ut i organisasjonen med en gang. Dette er særlig relevant for cyberhendelser, da det kan være en mulighet for at den kan være initiert innenifra. Dersom det er mistanke om dette, mener informanten at det kan være behov for å skaffe seg oversikt først, og sette inn tiltak i det skjulte (NI3).

Ifølge informant 5 samarbeider de godt i selskapet, både innad i de ulike avdelingene og på tvers av funksjoner. Hun opplever kollegaer som samarbeidsvillige, med unntak av enkelte som ikke alltid forstår det nye risikobildet:

> Det er veldig god kommunikasjon mellom avdelingene, og vi er ikke et så stort selskap, vi er rett over 200 ansatte totalt, og vi sitter i samme bygg så det er jo veldig kort vei til folk. Folk er også veldig samarbeidsvillige, men den største utfordringen er at mange av dem tilhører den eldre garden som har litt problemer med å skjønne risikoen. Så hvis man har avdekket noen sårbarheter eller noe man gjerne vil gjøre så er det ikke alltid de er så samarbeidsvillige på den fronten (NI5).

Den gode kommunikasjonen mener informanten er særlig viktig når det handler om å sikre komplekse systemer, som eksempelvis driftskontrollsystemet:

> Når det gjelder driftskontrollsystemet, så er det ikke bare bare å gjøre oppdateringer på enkelte deler av systemet. Det er jo satt sammen av veldig kritiske komponenter, og en oppdatering av en slik komponent kan jo kanskje i seg selv føre til at systemet feiler, og at vi plutselig ikke klarer å levere strøm fordi vi har gjort den oppdateringen. Så det er jo en avveining vi må gjøre og prate med de ulike avdelingene hvor vi snakker for sikkerheten, og de må snakke for deres avdeling og

> hvor kritisk den komponenten er, og kanskje man faktisk i noen tilfeller ikke oppdaterer nettopp fordi det kan være mer kritisk å oppdatere (NI5).

Erfaringsdeling trekkes også frem som en faktor som fremmer bransjens overordnede forståelse og kunnskap tilknyttet cybersikkerhet. Felles for alle informantene er at de har forbindelse til KraftCERT, som bistår kraftselskapene i å detektere og motvirke digitale angrep. Informantene opplever at samarbeidet gjør dem bedre rustet til å holde oversikt over de digitale systemene og over hva som kan true sikkerheten. I tillegg er det stort fokus på sikkerhet og erfaringsutveksling på tvers av selskaper, selv om selskapene også konkurrerer med hverandre:

> Selv om kraftselskapene er konkurrenter til hverandre så er det en ekstrem åpenhet og delingskultur, og det er utrolig behagelig. Jeg snakker med kraftselskap rundt i hele landet og får vite at de har blitt utsatt for sånn og sånn, den og den har prøvd seg, og det er erfaring som vi tar med oss videre i vårt arbeid for å sikre våre systemer bittelitt bedre enn vi gjorde i går (NI8).

Opplæring og forståelse

Informant 2 forteller at de tester ansatte jevnlig ved å sende ut falske phishing e-poster for å fremme bevissthet internt i selskapet. Konseptet går ut på at dersom de ansatte klikker på den falske meldingen, blir de bedt om å ta et e-læringskurs i anti-phishing. Resultatet fra kampanjene er varierende, og har ofte sammenheng med kvaliteten på phishing-mailen. Det vil alltid være noen som klikker uansett, slik at bevissthet blant de ansatte ikke er nok i seg selv. Det vil også være viktig å ha på plass øvrige tiltak slik at man hindrer at ekte forsøk blir vellykkede. Videre forteller han at han mener kunnskapsnivået tilknyttet cybersikkerhet i selskapet generelt er høyt, men at bevisstheten er høyest blant toppledelsen og hos dem som jobber med cybersikkerhet på daglig basis. Selv om de ansatte har et godt nivå av kunnskap, kan det alltid kan bli bedre (NI2).

Tiltak for å øke kunnskapsnivået i selskapet til informant 5, består blant annet av små kampanjer, videosnutter og quiz. Videre hevder hun at kunnskapsnivået tilknyttet cybersikkerhet i selskapet er moderat, og forklarer det med at det ikke er mange som jobber direkte med sikkerhet. Likevel mener hun at digitaliseringen i bransjen, og den stadige økningen i eksponeringsflater, bidrar til folk er mer bevisst og villige til å lære, særlig når både fagekspertise og ledelse er tydelige på sikkerhetsbehovet. Cyberrisiko er noe de snakker om hver dag, og særlig nå etter utrullingen av

AMS. Hun forteller at slike digitale omveltninger leder til at flere ser behovet for å tenke sikkerhet i alle ledd.

Brukeropplæring fremmes også som en svært viktig faktor for god cybersikkerhet av informant 8: "En kan sikre nettverkene sine og PCene sine så mye som en overhodet kan, men det hjelper jo ikke hvis brukerne gir fra seg brukernavn og passord eller klikker på infiserte vedlegg" (NI8). Det handler derfor om å sikre bevissthet rundt mulige farer og trusler som kan ramme en, og hvilken rolle man har i den overordnede sikkerheten. Videre berømmer informanten sine kolleger, både når det kommer til bevissthet, men også for at de viser nysgjerrighet, er forsiktige og påpasselige.

5.4.2 Organisatoriske utfordringer

Modenhet og kompetanse

Flere av informantene mener bransjen er umoden når det gjelder å håndtere risikoen på et tilstrekkelig nivå når den digitale utviklingen pågår kontinuerlig, og nye former for risikoer oppstår i takt med utviklingens hastighet. "Vi ser en risiko nå for at hele sikkerheten i softwareutviklingsprosessen er for dårlig, og at prosessen for å komme til et nivå hvor sikkerheten tilsvarer utviklingen vil være langvarig" (NI6). Det samme påpekes av informant 4, som mener det er utfordrende å skape et forhold hvor sikkerheten alltid holdt tritt med digitaliseringen (NI4). Det kan også være tilfeller hvor ansatte i bedriften ikke erkjenner eller forstår risikoen som digitaliseringen medfører. Dette gjelder særlig personer som har jobbet lenge i bransjen og som kjenner den fra en annen tid. Utfordringene ved utviklingen ligger ofte i at en må foreta endringer vekk fra kjent og kjær praksis (NI5).

> Det er mange som ønsker å ta i bruk nye løsninger, som de mener vil hjelpe dem i arbeidet, men så forstår de ikke da helt den store og hele konsekvensen av å koble ting på nett, og skytjenester og sånne ting. De har som sagt jobbet her i veldig mange år, og er ikke vant med å tenke i bits og bytes. Så der er det en jobb å gjøre (NI5).

Den samme mangelen på forståelse tilknyttet hvilken risiko og sårbarhet som innføres ved å ta i bruk digitale løsninger påpekes også av informant 1, som videre nevner at slike utfordringer må bekjempes ved riktig opplæring og kompetanse. Informant 6 mener kraftbransjen fortsatt er umoden i forhold til andre bransjer:

> Mitt inntrykk er at kraftbransjen er litt umoden på det formelle når det gjelder informasjonssikkerhet. Det er ikke lenge siden min rolle ble opprettet, det er to år siden, og det er veldig kort å jobbe strukturert med dette, det er helt sykt. Det offentlige har liksom blitt mast på med dette her i 8 år allerede av riksrevisjonen. Så jeg tror mange henger litt etter på det formelle (NI6).

Videre mener han slike utfordringer forsterkes dersom en mangler ressurser, hvilket han mener er tilfellet i flere selskaper, særlig de små. Løsningen på problemet vil være å få litt mer manpower med riktig kompetanse (NI6).

Fravær av hendelser

Fraværet av hendelser kan gjøre det utfordrende å forstå behovet for å opprettholde et kontinuerlig høyt sikkerhetsnivå. Det kan føre til at man "senker guarden" og står i fare for å ignorere hendelser som kan ha stort skadepotensial (NI2). Informant 2 sikter til arbeidet med ROS-analyser, hvor man kan høre uttalelser som: "Dette skjer jo ikke her, og det har heller aldri skjedd" (NI2).

"I Norge kan det være lett å dovne litt hen, kanskje. Når det ikke skjer så mye. Men vi skal jo være veldig glad for at det er sånn også, da" (NI2). Informant 7 mener at "siden det aldri har skjedd noe stort, er det kanskje noen som er fristet til å tenke at man sloss mot vindmøller, at det bare er en tenkt fiende" (NI7). Slike utfordringer kan igjen forsterke andre utfordringer, særlig med å få økonomiske ressurser til sikkerhetsarbeidet (NI7).

Informant 2 forteller at han har deltatt i et prosjekt sammen med et israelsk og et rumensk energiselskap, hvor de klassifiserte landene etter anslått risiko for cyberhendelser. Norge hadde her blitt vurdert som lavt, Romania som middels og Israel som høyt, og han hevder en kunne se en tydelig korrelasjon mellom anslått risiko og fokus på cybersikkerhet (NI2).

> I høyrisikoland er fokuset på sikkerhet enormt. Når jeg så hvilke trusler og farer de var utsatt for kontinuerlig, daglig, så var det enormt fokus på dette. Det var aldri snakk om budsjettkutt, de hadde jo nærmest ubegrenset med midler for å motvirke både fysiske og elektroniske angrep, så der var det jo lett å få oppmerksomhet og holde fokuset oppe" (NI2).

Når mennesker bryter barrierene

Informant 8 mener det også finnes utfordringer i gapet mellom sikkerhet og brukervennlighet, som han demonstrativt viser med hendene tilhører to ulike verdener. Slike gap kan lede til situasjoner hvor mennesker prøver å omgå barrierene, fordi systemet blir komplisert å bruke dersom man implementerer flere lag med sikkerhet (NI8).

> Hvis man er for strikt og for streng og gjør ting for vanskelig, vil folk begynne å gå rundt barrierene. It beats the purpose. Okei, jeg har sperret for sånne og sånne nettsider, okei flott det, da bruker de mobiltelefonen og spinner opp nettverksdeling der, også kobler de seg opp og går på de gitte sidene via mobilen. Også kobler de PCen tilbake til nettverket etterpå når de er ferdig (NI8).

Løsningen, og også utfordringen, er å finne den hårfine balansen mellom brukervennlighet og sikkerhet. Jo flere nettsider en åpner for at de ansatte kan bruke i arbeidstiden, jo større risiko utsetter man organisasjonen for. Likevel vurderer han risikoen som større dersom ansatte begynner å bruke skygge-IT, og gå bakveien. "Det er viktig å få folk til å forstå hvorfor jeg velger å sperre enkelte ting, og når de forstår det så tror jeg heller ikke at de vil bruke det" (NI8).

5.4.3 Opplevde hendelser

Alle informantene har opplevd cyberhendelser i sin organisasjon, av større eller mindre omfang. Flere peker på phishing-mail som den mest vanlige hendelsen, hvor falske e-poster blir sendt ut til ansatte i håp om at de skal klikke på en lenke og dermed gi hackere muligheten til å trenge inn i systemet. Informant 2 forteller om en slik hendelse:

> Vi har hatt et forsøk på såkalt direktørsvindel via phishing, hvor e-posten så ut til å komme fra vår direktør med beskjed om at det skulle betales et beløp og at det hastet. Det var nokså målrettet ettersom den var laget med vår logo og alt (NI2).

Det samme var tilfelle hos informant 8 som også hadde opplevd en hendelse hvor angripere hadde fått tak i e-post adresser fra personer internt i selskapet:

> Jeg var i Oslo, stod på tredemølla en tidlig morgen på vei til seminar, og da får jeg en e-post av en kollega av meg som jeg vet er sykemeldt, med beskjed om jeg kan åpne vedlegget. Jeg husker jeg skjønte veldig fort at dette var phishing, og at her er det noen som har fått tak vedkommendes e-postadresse og forsøker seg internt i selskapet (NI8).

Han forteller videre at de også har opplevd at en ansatt i selskapet har blitt utsatt for et såkalt brute-force angrep, som betyr at inntrengere forsøker å logge seg inn på en ekte brukerkonto ved hjelp av tilfeldige passord. Slike hendelser vil raskt kunne oppdages, da det fører til en automatisk sperring av brukerkontoen etter tre mislykkede påloggingsforsøk. Etter samtaler med andre kraftselskap fant informanten ut at flere var forsøkt rammet, hvilket fikk han til å tenke at angrepet helt klart var rettet spesifikt mot kraftbransjen (NI8).

Selv om fraværet av alvorlige uønskede hendelser kan oppstå som følge av gode rutiner, brannmurer, barrierer og godt sikkerhetsarbeid, kan det også være at de rett og slett ikke har oppdaget brudd i sikkerheten enda, hvilket flere av informantene mener er tenkelig. "Sannsynligvis har jo alle et eller annet "shait" på innsiden av brannmuren" (NI7). Det har også vært tilfeller hvor selskapene har vært berørt av sårbarheter som har blitt offentliggjort, noe som øker sannsynligheten for målrettede angrep. I dette tilfellet hadde den samme sårbarheten vært gjeldende på tvers av industrien, hvor den også hadde blitt utnyttet aktivt (NI2;NI7).

Håndtering av hendelser

Informantene forteller at under pågående hendelser jobbes det kontinuerlig med å få oversikt over hva som har skjedd og hvilke akutte tiltak som må settes inn. Arbeidet pågår frem til problemet er under kontroll. I de fleste tilfeller er hendelsene av tilsynelatende lav alvorlighetsgrad, og tiltakene består av å melde fra til kvalitetssystemet, sjefen, andre ansvarlige eller helpdesken i virksomheten (NI5). Informant 6 forteller at målet i deres virksomhet er at alle ansatte skal ha et klart sted hvor de skal kunne melde fra om hendelser, og at alle har kjennskap til disse strukturene i organisasjonen. Videre forteller han at hendelseshåndtering er en prosess man ønsker å heve nivået på hele tiden. Greier man å opprette tydelige kommunikasjonslinjer og ansvar, vil man være godt på vei (NI6).

Ifølge informant 5 ligger mye av evnen til å håndtere hendelser i de preventive metodene. Hennes selskap har derfor tatt i bruk en rekke overvåkningsverktøy for å bedre oversiktligheten i de digitale systemene. "Vi får varsler med en gang det dukker opp nye enheter med rar kommunikasjon, så vi håper sånn sett at dersom det skulle skje noe så vil vi oppdage det i en tidlig fase" (NI5). Likevel understreker hun at en ikke kun kan lene seg på teknologi, det handler også i stor grad om å ha

tydelige planer på hvordan man skal håndtere hendelser dersom de utvikler seg. For IKT-sikkerhetshendelser var planverket fortsatt under utvikling.

> Vi har jo hatt beredskapsplaner, det har vi jo hatt i alle år, men de baserer seg mer på de fysiske hendelsene. Hva som skjer om vi har uvær eller sånne ting, så vi jobber med å implementere IKT-sikkerhetshendelser der, og ulike innsatsplaner for ulike scenarier (NI5).

Øvrige informanter vektlegger at evnen til å håndtere angrep eller annen uønsket påvirkning handler om å agere raskt. Samtidig er det viktig at grundige planer og godt beredskapsarbeid danner grunnlaget for god ad-hoc håndtering.

I forbindelse med et phishing-angrep forteller informant 8 at "det bare var å avbryte den økta på tredemølla, sette en kjapp krisestab og håndtere det der og da" (NI8). Sammen med driftsleverandører klarte de å sperre alle kontoer og skaffe oversikt over alt som var gått ut av kollegaens e-post konto. 3500 infiserte e-poster hadde havnet både hos kunder og leverandører. Dette gjorde at han opprettet kontakt med KraftCERT, hvor de i fellesskap laget en plan for videre håndtering. Den raske håndteringen, sammen med hjelp fra både driftsleverandører og KraftCERT, gjorde at man "fikk reddet dagen i løpet av et par timer" (NI8).

> Det er veldig kjekt hos oss, folk snur seg fort rundt og er villige til å bistå. Ved behov så hanker vi også inn eksterne, eksempelvis kraftCERT. De er jo eksemplariske, det er ingen problem å ringe klokka 19 en fredag og si at hei, noe er galt, jeg trenger noen til å analysere noen minnedumper som jeg har gjort. Og det gjør de. De tar ikke betalt for det engang. Det er morsomt (NI8).

Fører opplevde hendelser til endring i praksis?

En undersøkelse utført av NVE viser at 40% av virksomhetene som opplevde det man kategoriserer som alvorlig hendelse, ikke hadde gjort noen endringer i organisasjonen som følge av hendelsen. I løpet av tidsperioden undersøkelsen pågikk hadde 21% endret rutiner, og bare 18% hadde investert i programmer til bruk for opplæring av de ansatte (NVE, 2017b, s. 27). Vi har undersøkt om disse manglene gjør seg gjeldende også hos våre informanter. Det er likevel ikke fullstendig sammenlignbart, da alle informantene opplyser at hendelsene de har opplevd har vært av mindre alvorlig grad, med unntak av en, hvor etterforskning ble igangsatt. Likevel hevder alle som er spurt at opplevde hendelser fører til endring i praksis, og understreker viktigheten av å ta

hensyn til tidligere erfaringer når en legger veien videre. En av dem etterlyser imidlertid hyppigere rapportering, da han opplever at det finnes lite empiri på hva som faktisk endres (NI1). De andre informantene opplever at deres virksomhet er gode til å endre rutiner etter uønskede hendelser, og trekker frem flere eksempler, som å innføre to-faktor autentisering umiddelbart etter at oppdager et sikkerhetshull. "Vi må tilpasse barrierene etter trusselnivået" (NI2).

Flere av de uønskede hendelsene er en del av hverdagen i kraftforsyningen. Phishing-mail og observert aktivitet i nettet som stoppes av brannmuren før de greier å penetrere systemet, er to eksempler som trekkes frem. Slike hendelser ses ikke på som alvorlige nok til å endre praksis, så lenge de grunnleggende sikkerhetstiltakene og barrierene er på plass. "Vi endrer praksis så lenge det er uønsket nok. Jo mer uønsket det er, jo mer endringer fører det til" (NI6). Flere har også trukket fram endringer som følge av Covid-19, hvor alle nå sitter på hjemmekontor. Kriser åpner for nye sårbarheter i virksomhetene, og nye muligheter for individer eller grupper med onde hensikter. Flere av informantene har opplevd økt aktivitet på nettet i denne perioden, samt en økning i antall svindelforsøk. Dagens situasjon fører også til at ansatte ikke lenger kan "stikke innom" kontoret til IKT-sikkerhetsansvarlig for råd eller deling av informasjon, som det har vært lav terskel for å gjøre tidligere (NI8).

5.4.4 Analyse av funn

Funn relatert til studiens fjerde forskningsspørsmål indikerer at spesielt forankring i ledelsen, tydelige ansvarsområder, erfaringsutveksling, samt opplæring og bevisstgjøring av øvrige ansatte, er organisatoriske betingelser som øker aktørenes evne til å håndtere sektorens cyberrisiko. Sammenstillingen av informantenes svar viser at dette er forutsetninger som trekkes frem av flertallet, hvilket underbygger en antakelse om at betingelsene er gjeldende hos mange av virksomhetene i bransjen.

Felles målsettinger i arbeidet med cybersikkerhet

Som det fremkommer av delkapittel 5.1 introduserer digitaliseringen stadig nye farer og trusler over digitale flater, og utfordrer sektoren på nye måter. Ifølge La Porte (1996) er det viktig at organisasjoner som arbeider under dynamiske og krevende forhold har veldefinerte mål. Tidligere i studien kommer det implisitt frem at hovedmålet til aktørene er å levere strøm trygt hjem til sine

kunder. Delmålene for å komme dit, spesielt i tilknytning til cybersikkerhet, er derimot ikke like entydige. Dette viser seg gjennom variasjoner i ansattes forståelse og kunnskap, og ved at ulike seksjoner innad i de respektive virksomhetene har sine egne oppgaver som krever fokus, og sine egne mål som skal nås.

Som Rosness et al. (2010) hevder, vil pålitelige virksomheter (HRO) kjennetegnes av flere egenskaper, blant annet villigheten til å ta imot og omstille seg etter nye beslutninger. Empirien viser at informantene opplever at forståelsen tilknyttet cybersikkerhet hos øvrige ansatte enten er god, moderat eller varierende. Mangler i risikoforståelsen kan forklares ved at de som har jobbet lenge i bransjen kjenner den fra en annen tid, hvor cyberrisiko ikke har vært et like omfattende problem. Erkjenner ikke ansatte risikoen som følger med utviklingen i bransjen, viser empirien at det kan det være utfordrende å skifte fokus. Dette kan forklare hvorfor informantene underbygger viktigheten av forankring i ledelsen, og at ledelsens sikkerhetsfokus må kommuniseres til alle ansatte for at de skal kunne håndtere cyberrisiko effektivt. Samtlige informanter som har stilt til denne studien forteller at ledelsen i deres respektive virksomheter viser interesse og er delaktig i arbeidet med cybersikkerhet og at dette har hatt en positiv innvirkning på de ansattes felles risikoforståelse.

En felles risikoforståelse vil antakeligvis også forsterke de ansattes evne og villighet til å omstille seg i takt med endringer i risiko- og trusselbildet. Ergo kan man si at etablering av en felles risikoforståelse er en form for håndteringsmekanisme. Videre vil trolig mekanismen gjøre virksomhetene bedre rustet til å operere under dynamiske og krevende forhold, ved at det konstrueres felles målsettinger og virkelighetsoppfatninger innad i virksomhetene (Rosness et al., 2010; La Porte, 1996). Dette kan særlig vise seg viktig ut fra det faktum at informantene påpeker at det kan oppstå utfordringer vedrørende ulike målsettinger på tvers av ulike avdelinger. Er slike betingelser på plass vil det derfor kunne argumenteres for at aktørenes evne til å håndtere cyberrisiko styrkes. Funn i denne studien støttes videre opp av tidligere forskning, hvilket viser at behovet for å skape en felles risikoforståelse blant ansatte og sikkerhetspersonell fortsatt er viktig for å kunne hanskes med utfordringer som følge av teknologisk utvikling (Albrechtsen, 2008).

Mennesker som barriere – viktigheten av opplæring

I forlengelsen av diskusjonen over, fremmer informantene brukeropplæring som en viktig betingelse for evnen til å arbeide strukturert med cybersikkerhet. Dette uttrykkes i forbindelse med at ansatte må inneha forståelse for hvordan de selv kan utgjøre et sikkerhetsproblem, som særlig kan sees i forbindelse med antall phishing e-poster som mottas internt i virksomhetene. Det kommuniseres også at det kan være utfordrende å finne et balansert forhold mellom sikkerhet og brukervennlighet. Dette synliggjøres gjennom informant 8 sine uttalelser rundt dilemmaet mellom sikkerhet og brukervennlighet, hvor mennesker kan gå fra å være en barriere til å bli en sikkerhetsbrist. Empirien antyder videre at slike interessekonflikter bekjempes gjennom fokus på samhandling og opplæring, hvilket samsvarer med betingelser Reason (2016) mener vil tilrettelegge for en god sikkerhetskultur.

Ettersom alle ansatte kan fungere som en barriere eller en sikkerhetsbrist for uønskede cyberhendelser, kan vi si at cybersikkerhet er noe alle i virksomheten er ansvarlige for. At informantenes virksomheter tilrettelegger for opplæring og samhandling gjennom kurs, kampanjer og andre virkemidler vil derfor kunne heve ansvarsforståelsen, og inkorporere cybersikkerhet i øvrige ansattes arbeidsoppgaver. Slike mekanismer fremmer hva Rosness et al., (2010) omtaler som organisatorisk redundans gjennom strukturelle dimensjoner, som viser til måter å hanskes med dynamiske utfordringer i risikofylte miljøer. Samtidig er ovennevnte tiltak eksempler på hvordan aktørene og virksomhetene de tilhører håndterer cyberrisiko som følger av digital utvikling. Det kunne videre vært interessant å få innsyn i hva som inngikk i slike opplæringsseksjoner, samt hvordan øvrige ansattes læring påvirkes av slike tiltak. Selv om dette ikke har vært inkludert i studien, viser tidligere forskning at bevisstgjørende tiltak er blant de mest effektive i arbeidet med IKT-sikkerhet (Hagen, Albrechtsen & Hovden, 2008).

Empirien viser at det er tilrettelagt for rapportering i flertallet av virksomhetene som har bidratt til denne studien. Dette kan bestå av rapportering til KraftCERT, eller til aktuelle personer internt i selskapet. Slike strukturer hevder Hollnagel (2017) vil bedre evnen for å kunne håndtere hendelser på en proaktiv måte ved at man tilrettelegger for oppdagelsen av mulige feil før hendelsen får tid til å eskalere. På samme måte kan betingelsen ses i et HRO-perspektiv, da teorien hevder at slike mekanismer vil tilrettelegge for pålitelig drift under dynamiske og komplekse forhold. I denne

sammenhengen er det viktig at ansatte oppfatter strukturene som tillitsvekkende, hvilket underbygger viktigheten av tidligere nevnte betingelser om forankring i ledelsen og forståelse for cyberrisiko som følger av digitaliseringen. I tråd med delkapittel 5.1 vil selv den minste feil kunne forplante seg videre og forårsake alvorlige konsekvenser. Derfor kan en argumentere for at virksomhetenes tilrettelegging og belønning av rapportering vil være med å forsterke de ansattes villighet til å si ifra om feil og mangler. I tråd med Reason (2016) vil slike mekanismer tilrettelegge for en informert kultur. Vi argumenterer derfor for at ovennevnte forutsetninger vil gjøre aktørene bedre rustet til å håndtere de mangfoldige utfordringene som følger av den digitale utviklingen i sektoren.

Samarbeid og kommunikasjon

Det finnes flere arenaer for samhandling i norsk kraftsektor, blant annet ulike sikkerhetsråd, formelle og uformelle kommunikasjonskanaler internt i selskaper og forbindelser til KraftCERT, som aktørene ser ut til å benytte aktivt. Selskapene i kraftsektoren ser også ut til å samarbeide heller enn å konkurrere for å kunne hanskes med utfordringer som følge av digitaliseringen. Ovennevnte arenaer for kommunikasjon og erfaringsutveksling tyder derfor på at det foreligger forutsetninger for å kunne lære av hverandre. Som Hollnagel (2017) proklamerer vil evnen til kontinuerlig læring være en viktig forutsetning for resiliens, hvilket underbygger at samarbeid og kommunikasjon på tvers av sektoren er en viktig betingelse for at aktørene skal være rustet til å håndtere cyberrisiko.

Fravær av hendelser er en utfordring i arbeidet med cybersikkerhet. Dermed kan arenaene for erfaringsutveksling vise seg å være spesielt viktig for håndteringen av cyberrisiko. Det poengteres også av flere informanter at delingskulturen i sektoren er god, og at all den informasjonen som kan deles, blir delt. Dette er viktig for å kunne veie opp for fraværet av hendelser hos de enkelte, og gir muligheten til å lære av hendelser andre har opplevd. Gjennom samhandling vil derfor utfordringer tilknyttet fravær av hendelser kunne minimeres. Dette kan videre tilrettelegge for håndtering basert på en proaktiv tilnærming ved å hente erfaringer fra andre selskaper i bransjen, og i samfunnet forøvrig.

Organisatoriske betingelser ved uønskede hendelser

At opplevde hendelser fører til endring i praksis, dersom det viser seg å være nødvendig, er viktig for å kunne være proaktiv i møte med den neste hendelsen (Hollnagel, 2017). I henhold til NVEs undersøkelse i 2017, er det et betydelig antall av virksomhetene som ikke implementerer tiltak i etterkant av hendelser, hvilket svekker evnen til å være proaktiv i fremtiden. Informantene i denne studien hevder derimot at nesten alle hendelser fører til endring i praksis, og understreker viktigheten av å implementere tiltak i etterkant av hendelser. Om dette er en tenkt eller reell endring vites derimot ikke med sikkerhet uten videre innsyn.

I tillegg til endring i praksis, viser empirien at det blant aktørene er tydelige eksempler på at de innehar evnen til reaktiv og å hurtig omstilling. Eksempelet fra informant 8, som hoppet av tredemølla og handlet umiddelbart er blant disse, og viser evne til å ta raske og desentraliserte beslutninger under dynamiske forhold. Det samme eksempelet illustrerer videre hvorfor tydelige arbeidsoppgaver og ansvarsområder er viktig. I situasjoner som krever raske beslutninger kan slike mekanismer være sentrale for evnen til rask omstilling (Rosness et al., 2010). Det er vanskelig å tyde om samtlige aktører har den samme evnen til å omstille seg raskt på stående fot. Likevel viser empirien på at det finnes liknende betingelser hos øvrige aktører, hvilket indikerer at forutsetningene er tilsvarende.

Mangel på innsatsplaner for potensielle cyberhendelser trekkes frem av en av informantene. Selv om det hevdes at dette er under utvikling vil fravær av planverk kunne hemme evnen til å opprettholde funksjonaliteten til virksomheten dersom en cyberhendelse mot formodning skulle inntruffet. Å oppnå modenhet på IKT-sikkerhetssiden vil derfor fortsette å prege sektorens utvikling i årene som kommer, særlig i forbindelse med å stabilisere et skiftende risikobilde som følge av implementering av stadig flere digitale systemer og løsninger. Å arbeide strukturert på dette området vil derfor være et viktig arbeid i årene som kommer. Gjennom modningsprosesser vil aktørenes evne til å håndtere farer og trusler over digitale flater trolig øke, hvilket Dickson & Goodwin (2019) hevder er viktige betingelser for cyberresiliens

5.4.5 Delkonklusjon

Som vist i analysen er det flere betingelser som tilrettelegger for aktørenes evne til å håndtere cyberrisiko. Som svar på forskningsspørsmål 4 indikerer funn at de aller viktigste er; forankring i ledelsen, tydelige ansvarsområder og rapporteringsveier, erfaringsutveksling og kommunikasjon, samt betingelser som fremmer opplæring og forståelse. Videre er det tydelig at noen av betingelsene har gjensidig påvirkningskraft, hvilket spesielt kommer til syne gjennom forholdet mellom forankring i ledelsen og risikoforståelse. Dersom ledelsen er fraværende i arbeidet med cybersikkerhet er det mye som tyder på at risikohåndteringen vanskeliggjøres ved at det kan oppstå interessekonflikter mellom hva som anses som viktig av øvrige ansatte i organisasjonen. I en bransje som befinner seg i en epoke med flere endringer, som er vant med andre risikoforhold enn de som utspiller seg over digitale flater, er nettopp den felles risikoforståelsen sentral. For å kunne evne å håndtere slike endringer, er det derfor viktig at alle ansatte er "med på laget", slik at de bistår som en barriere heller enn en fare. Forankring i ledelsen bidrar også til at det genereres økonomiske ressurser, som er avgjørende for å drive en sikkerhetsavdeling med tilstrekkelig personell og kunnskap som er nødvendig for å møte sikkerhetsbehovet. Videre bidrar erfaringsutveksling og kommunikasjon på tvers og internt i bransjen til at aktørenes læringsevne ikke forsinkes av fravær av hendelser i egen organisasjon, hvilket øker forutsetningen for å være resiliente i møte med påkjenninger. Opplevde hendelser illustrerer videre hvilken betydning tydelige ansvarsområder og rapporteringsveier har i møte med cyberhendelser. Funnene indikerer videre at nevnte organisatoriske betingelser er avgjørende for å kunne hanskes med forhold som kan ha stort konsekvenspotensial.

5.5 Sammenfatning

I denne studien har vi etterstrebet å skape sammenhenger mellom metode, empiriske funn og analyse for å styrke studiens pålitelighet. I denne oppsummeringen samler vi trådene før vi avslutningsvis konkluderer og svarer på oppgavens problemstilling.

I undersøkelsen av hvordan aktører i den norske kraftforsyningen forstår og håndterer cyberrisiko som følge av sektorens digitale utvikling har 8 informanter blitt intervjuet. Informantene har fått spørsmål som anses som relevante for å belyse flere aspekter ved studiens problemstilling. Studien

har ved bruk av den abduktive forskningsstrategien søkt å finne mulige sammenhenger mellom gitte fenomener. I dette tilfellet er fenomenene kraftforsyningens digitale utvikling, og forståelse og håndtering av cyberrisiko som digitaliseringen fører med seg. Studien har avdekket at slike sammenhenger finnes, blant annet ved at digitalisering gjør bransjens systemer mer komplekse, som videre har hatt innvirkning på bransjens cyberrisiko. Dette viser at det er et behov at forståelsen og håndteringen følger den samme utviklingen. Gitt kraftforsyningens størrelse, og omfanget av involverte aktører, er utvalget for lite til å kunne generalisere funnene til en hel bransje. Samtidig er cyberrisiko som følge av digital utvikling noe som angår alle i bransjen, og som kan illustreres ved utrullingen av avanserte strømmålere (AMS) som har vært pålagt samtlige nettselskaper. Dokumentanalysen indikerer også at IKT-baserte løsninger er noe som benyttes i stadig større omfang i sektoren, hvilket viser at utviklingen, og tilhørende utfordringer, sannsynligvis kan være relevant for flere aktører i kraftbransjen.

Studiens analyse baseres på empiriske funn sett i lys av valgt teoretisk rammeverk. De valgte teoriene har vist seg hensiktsmessig ved at de har bidratt til å skape forståelse for fenomenene gjennom etablerte konsepter innenfor samfunnssikkerhetsfeltet. Gjennom studiens delkapitler tilknyttet de ulike forskningsspørsmålene kan vi kort oppsummere følgende hovedfunn:

Digitaliseringsprosessene har endret kraftforsyningens risikostruktur ved å gjøre systemene mer komplekse, og dermed mer utsatt for sårbarheter og cyberrisiko. Perrows teori om normale ulykker har lagt grunnlaget for å skape en forståelse for disse sammenhengene, og belyser hvordan digital utvikling har endret bransjens risikostruktur ved innføringen av avanserte målesystemer, bruk av skybaserte tjenester og integrering av eksisterende systemer.

Begrepet cyberrisiko forstås av flertallet som risikoen for tilsiktede hendelser rettet mot kraftsektoren. Informantene har også vist en bredere forståelse av konseptet ved å forklare at cyberhendelser kan være et resultat av både farer og trusler.

Innledningsvis fremhevet studien risikovurderingsprosessen som en arena hvor aktørene håndterer cyberrisiko. Dette bekreftes av teorien da risikovurderingen inngår i den helhetlige risikostyringsprosessen (Aven, 2015). Studien har avdekket at aktørene benytter ROS-analyser,

hvor risiko vurderes basert på sannsynlighet og konsekvens. Selv om farer og trusler vektlegges likt, indikerer funn at det i stor grad er farer og trusler som ikke direkte kobles til bransjens digitale utvikling som får fokus. Cyberrisiko kan derfor stå i fare for å bli nedprioritert på bakgrunn av to forhold; enten ved at det mangler informasjon tilknyttet slike hendelser i kraftverdenen i Norge eller ved at sannsynlighetsverdien er lav. Det er heller ikke usannsynlig at disse to faktorene henger sammen.

Rammer for praktisk håndtering av cyberrisiko som avdekkes i risikovurderingene settes av organisatoriske betingelser som forankring i ledelsen, klare ansvarsforhold og rapporteringsveier, opplæring og læring av tidligere hendelser. Funn viser også at evnen til risikohåndtering vil svekkes dersom ikke enkelte av disse betingelsene er på plass. Teoriene om HRO, sikkerhetskultur og resiliens bekrefter slike sammenhenger, og har bidratt til å belyse hvilken betydning de ulike organisatoriske betingelsene har for hvordan man evner å håndtere utfordrende situasjoner og fenomener.

Valg av informanter, metode og teori, har vist seg i stor grad å være hensiktsmessig for å svare på studiens forskningsspørsmål og problemstilling. Selv om ikke alle aspekter ved teoriene og alle nyanser av empiri får plass i studiens avsluttende kapittel, vurderer vi at helheten har bidratt til plausible svar, som videre presenteres i studiens hovedkonklusjon.

6.0 Konklusjon

Formålet med denne studien har vært å belyse hvordan aktører i norsk kraftsektor forstår og håndterer cyberrisiko som følge av bransjens digitale utvikling. Dette kapittelet tar for seg slutten på denne forskningsprosessen, og skal besvare oppgavens problemstilling:

Hvordan forstår og håndterer aktører i den norske kraftforsyningen cyberrisiko som følge av sektorens digitale utvikling?

For å besvare problemstillingen har sektorens digitale utvikling blitt presentert og diskutert gjennom fire utledende forskningsspørsmål. Resultatene viser at cyberrisiko har fått en mer sentral plass i bransjens risikobilde. Videre har digitaliseringsprosessene etter vår oppfatning bidratt til at risikostrukturen er endret gjennom implementering av og oppdatering til digitale løsninger. Dette kan få konsekvenser ved at det kontinuerlig introduseres nye farer og trusler som alene eller i fellesskap kan forårsake kritiske ringvirkninger i en sektor som stadig blir mer kompleks. Samlet sett er dette medvirkende til å skape sektorens cyberrisiko.

Aktørene i kraftforsyningen har ingen felles teoretisk forståelse eller definisjon av begrepet cyberrisiko. En av informantene unngår å bruke begrepet, nettopp fordi det kan forstås ulikt og føre til begrensninger i det helhetlige arbeidet med cybersikkerhet, som følge av at mange kan tenke at dette er noe som ikke gjelder dem. En annen mener det viktigste er å erkjenne at risikoen finnes, heller enn å definere den. Sammenstillingen av svar viser også at et flertall ser cyberrisiko som risikoen for tilsiktede hendelser, og koblet dermed begrepet til "security". Videre viser undersøkelsen av hvilke farer og trusler aktørene mener bransjen står overfor som følge av digitaliseringen, at de her også legger til utilsiktede handlinger, altså "safety" eller farer.

Vi kan derfor konkludere med rimelig stor grad av sikkerhet at aktørene samlet sett forstår cyberrisiko som sammensatt av både farer og trusler. Ulikheter i begrepstilnærmingen og variasjoner i oppfatninger om hva som kan forårsake en cyberhendelse indikerer at det kan være behov for å skape konsensus i bransjen rundt disse forholdene.

Videre har vi undersøkt hvordan aktørene håndterer cyberrisiko. Aktørene er gjennom lovkrav pålagt å håndtere og redusere farer og trusler som kan sette forsyningssikkerheten i fare. Det problematiseres at slike lovkrav frem til nå ikke har fulgt det samme tempoet som den digitale utviklingen. Dette antyder at det kan være behov for en proaktiv tilnærming til håndteringen av cyberrisiko og at en ikke kun må lene seg på lovkrav.

Et flertall av informantene benytter seg av risiko- og sårbarhetsanalyser hvor risiko vurderes basert på resultatet av sannsynlighet og konsekvens. Resultatet benyttes videre til å vurdere hvilke tiltak eller barrierer som skal settes inn for å redusere og håndtere farer og trusler som avdekkes. Utfordringen med å bruke denne metoden for risikovurdering er at analysene prioriterer risikoforhold som gjennom analysen viser seg å være sannsynlig, hvilket fører til at cyberrisiko kan bli nedprioritert i risikostyringens innledende fase. Dette vil kunne påvirke evnen til risikohåndtering i negativ retning. Dersom dette skjer, er det desto viktigere å håndtere cyberrisiko gjennom andre mekanismer og prosesser.

Vi har tidligere skrevet at utilsiktede hendelser skjer i grenseland mellom teknologi og menneske, og at alle ansatte kan fungere som en barriere eller sikkerhetsbrist. Det er derfor viktig å inkludere alle ansatte i risikohåndteringen, noe det også er tydelig enighet om blant aktørene. Å styrke øvrige ansattes risikoforståelse er derfor en svært viktig faktor. Studien har belyst hvordan tydelige ansvarsområder, rapportering, bevisstgjøring og opplæring av ansatte er avgjørende for aktørenes håndtering av cyberrisiko. Det er også lagt til rette for samhandling på tvers av virksomhetene i bransjen, noe som særlig kan være viktig med tanke på at fravær av hendelser i den norske kraftforsyningen trekkes frem som en utfordring. Erfaringsdeling bidrar til at de ulike virksomhetene kan lære av hverandre, slik at de står bedre rustet til å håndtere en faktisk cyberhendelse dersom den skulle inntreffe. Det viser seg derfor at aktørene bruker overnevnte forutsetninger som arena til å håndtere cyberrisiko som følge av sektorens digitalisering.

Det er videre synliggjort gjennom analysen hvordan støtte og forankring i ledelse har stor innvirkning på effekten til de ovennevnte mekanismene. Vi kan dermed konkludere med at aktørene i den norske kraftforsyningen håndterer cyberrisiko som følge av sektorens digitale utvikling gjennom ovennevnte organisatorisk betingelser, og ved å inkorporere egen forståelse av

cyberrisiko inn i virksomhetene gjennom opplæring og bevisstgjøring av de ansatte. I hvilken grad man lykkes med dette vil imidlertid være avhengig av støtte og forankring i ledelsen.

6.1 Videre forskning

I undersøkelsen av studiens problemstilling har det dukket opp flere elementer som hadde vært interessante å belyse ytterligere. For det første viser funn at risikovurderingsprosessene fortsatt bærer preg av analysemetoder som anslår risiko ut fra sannsynlighet og konsekvens, og at dette kan ha negativ innvirkning på risikostyringen av cyber. Det kunne derfor vært hensiktsmessig å undersøke hvordan denne prosessen, og de metoder som benyttes, påvirker aktørenes arbeid med cybersikkerhet. For det andre er det mye som tyder på at det har skjedd en utvikling i risikoforståelsen tilknyttet både utilsiktede og tilsiktede cyberhendelser fra tidligere studier. Hva som har påvirket denne utviklingen kunne derfor vist seg interessant å belyse i sammenheng med at det har skjedd en betydelig vekst i digitale løsninger. Det anbefales også en undersøkelse av kraftforsyningens modenhet til å håndtere cyberhendelser. Som studien viser er det skjedd betydelige endringer i bransjens risikostruktur. Hvordan risikostyringen er egnet til å møte disse endringene kan derfor være en viktig studie i årene som kommer.

Litteraturliste

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees.* (Doktoravhandling). Trondheim: Norges teknisk-naturvitenskapelige universitet.

Albrechtsen, E. & Hovden, J. (2007). Industrial safety management and information security management: risk characteristics and management approaches. (u.s).

Aven, T. (2015). *Risikostyring. Grunnleggende prinsipper og ideer* (2.utg). Oslo: Universitetsforlaget.

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

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

Beredskapsforskriften. (2018). Forskrift om endring i forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (FOR-2018-11-01-1641). Hentet fra https://lovdata.no/dokument/LTI/forskrift/2018-11-01-1641

Borgund, L. (2014, 12 april). Skytjenester i energiforsyningen, En forstudie, Deloitte.

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (FFI rapport 00923/2015). Hentet fra https://www.ffi.no/no/Rapporter/15-00923.pdf

Danermark, B., Ekström, M., Jakobsen, L. &J. C. Karlsson. (2002). *Explaining Society: Critical Realism in the Social Sciences.* London: Routledge.

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

Det Norske Veritas. (2019). *Digitalization and the future of energy: beyond the hype - how to create value by combining digital technology, people and business strategy.* Hentet fra: https://www.dnvgl.com/power-renewables/themes/digitalization/index.html

Direktoratet for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner.* Hentet fra https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Dickson, F. & Goodwin, P. (2019). *Five Key Technologies for Enabling a Cyber-Resilience Framework.* Hentet fra https://www.ibm.com/downloads/cas/YBDGKDXO

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

Finansdepartementet. (2020). Statsbudsjettet. (Prop. 1 S (2019-2020)) Hentet fra: https://www.regjeringen.no/contentassets/e5b05593a20a49a8865ef3538c7e2f1e/no/pdfs/prp201920200001guldddpdfs.pdf

Forskningsrådet. (2019, 22. august). Cybersikkerhet i det norske kraftnettet. Hentet fra https://www.forskningsradet.no/contentassets/fde911cb10ff493b8eeb83bd17311601/forskningsradet-workshop-22082019--cybersikkerhet-i-energisektoren-rev.2.0.pdf

Forsvarsdepartementet, Justis- og beredskapsdepartementet, Utenriksdepartementet. (2019, 13. juni). Styrker internasjonalt samarbeid mot digitale trusler. Hentet fra https://www.regjeringen.no/no/aktuelt/styrker-internasjonalt-samarbeid-mot-digitale-trusler/id2654348/

Hagen, J.M., Albrechtsen, E. & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397.

´t Hart, P. & Sundelius, B. (2013). Crisis Management revisited: A new agenda for research, training and capacity building within Europe. *Cooperation and Conflict*, *48*(3), 444-461.

Hellevik, O. (2002). *Forskningsmetode i sosiologi og statsvitenskap* (7. utg.). Oslo: Universitetsforlaget.

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

Hovden, J. (2004). Sikkerhet i forskning og praksis: Et utfordrende mangfold med Sikkerhetsdagene som arena. I Lydersen, S (Red.), *Fra flis i fingeren til ragnarok* (s. 31-50). Trondheim: Tapir Akademisk Forlag.

International Organization for Standardization (ISO) and International Electrotechnical Comisson (IEC). (2018). 27005. *Information technology, security techniques, information security risk management.*

Jore, S.H. (2017). The Conceptual Scientific Demarcation of Security in Contrast to Safety. Published online: Springer

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

https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

KraftCERT. (2015). Hentet fra: https://www.kraftcert.no

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

Kommunal - og moderniseringsdepartementet. (2014, 6. desember). Digitalisering i offentlig sektor. Hentet fra https://www.regjeringen.no/no/tema/statlig-forvaltning/ikt-politikk/digitaliseringen-i-offentlig-sektor/id2340245/

Kommunal- og moderniseringsdepartementet. (2016). *Nasjonal strategi for bruk av skytjenester*. Hentet fra https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/nasjonal_strategi_for_bruk_av_skytenester.pdf

La Porte, T. (1996). High Reliability Organizations: Unlikely, Demanding and At Risk. *Journal of Contingencies and Crisis Management,* 4(2), 60-71.

Lincoln, Y. S., & Guba. (1985). *Naturalistic iniquiry*. Newbury Park: Sage publications.

Nasjonal sikkerhetsmyndighet (NSM). (2019). *Risiko 2019.* Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

Nasjonal sikkerhetsmyndighet (NSM). (2020). *Risiko 2020*. Hentet fra https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm-risiko-2020.pdf

National Institute of Standards and Technology (NIST). (2017). *Cybersecurity Framework Manufacturing Profile.* Hentet fra https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf

Nilsen, T. (2019). Cybersikkerhet i nettselskap. (Masteravhandling). Stavanger: Universitetet i Stavanger.

Norges vassdrags- og energidirektorat (NVE). (2010). Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen. (2-2010). Hentet fra: http://publikasjoner.nve.no/veileder/2010/veileder2010_02.pdf

Norges vassdrags- og energidirektorat (NVE). (2015). *Teknologiskifte i energiforsyningen.* (118-2015). Hentet fra http://publikasjoner.nve.no/rapport/2015/rapport2015_118.pdf

Norges vassdrags- og energidirektorat (NVE). (2016). *IKT-systemers rolle og betydning for strukturen i kraftbransjen.* (32-2016). Hentet fra http://publikasjoner.nve.no/rapport/2016/rapport2016_32.pdf

Norges vassdrags- og energidirektorat (NVE). (2017a). *Regulering av IKT- sikkerhet.* (26-2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_26.pdf

Norges vassdrags- og energidirektorat (NVE). (2017b). *Informasjonssikkerhetstilstanden i energiforsyningen.* (90-2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

Norges vassdrags- og energidirektorat (NVE). (2017c). *Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem.* (14-2017). Hentet fra http://publikasjoner.nve.no/rapport/2017/rapport2017_14.pdf

Norges vassdrags- og energidirektorat (NVE). (2018a). *Risiko- og sårbarhetsanalyse for økt integrasjon av AMS-DMS-SCADA* (15-2018). Hentet fra http://publikasjoner.nve.no/eksternrapport/2018/eksternrapport2018_15.pdf

Norges vassdrags- og energidirektorat (NVE). (2018b). *Foreløpig tilleggsveileder til Kraftberedskapsforskriften.* Hentet fra: https://www.nve.no/media/7598/forel%C3%B8pig-tilleggsveileder-kraftberedskapsforskriften.pdf

Norges vassdrags- og energidirektorat (NVE). (2019a, 6. mai). Kraftforsyningens beredskapsorganisasjon (KBO). Hentet fra: https://www.nve.no/damsikkerhet-og-kraftforsyningsberedskap/kraftforsyningsberedskap/organisering-av-kraftforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/

Norges vassdrags- og energidirektorat (NVE). (2019b, 22. januar). Kraftberedskapsforskriften har trådt i kraft. Hentet fra: https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/kraftberedskapsforskriften-har-tradt-i-kraft/

Norges vassdrags- og energidirektorat (NVE). (2020). *Kartlegging av bruk av tingenes internett (IoT/ IIoT) i norsk kraftforsyning.* (2-2020). Hentet fra: http://publikasjoner.nve.no/eksternrapport/2020/eksternrapport2020_02.pdf

NOU 2015: 13. (2015). *Digital sårbarhet - sikkert samfunn.* Hentet fra https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2016: 19. (2016). *Samhandling for sikkerhet.* Hentet fra https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

NOU 2018: 14. (2018). *IKT-sikkerhet i alle ledd - Organisering og regulering av nasjonal IKT-sikkerhet.* Hentet fra https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/?ch=2

Næringslivets sikkerhetsråd (NSR). (2016). *Mørketallsundersøkelsen 2016*. Hentet fra https://www.nsr-org.no/getfile.php/137423-1474384915/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf

Næringslivets sikkerhetsråd (NSR). (2018). *Mørketallsundersøkelsen 2018.* Hentet fra https://www.nsr-org.no/getfile.php/1311303-1537281687/Bilder/Mørketallsundersøkelsen/Mørketallsundersøkelsen%202018%20low.pdf

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

Politiets sikkerhetstjeneste (PST). (2020, 4. februar). *Nasjonal trusselvurdering 2020*. Hentet fra https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Qu, S. Q., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management, 8(3), s. 238-264. https://doi.org/10.1108/11766091111162070*

Rausand, M. (2011). *Risk Assessment.* Wiley: New Jersey.

Ringdal, K. (2013). *Enhet og mangfold: samfunnsvitenskapelig forskning og kvantitativ metode*. Bergen, Fagbokforlaget.

Reason, J. (2016). *Managing the Risks of Organizational Accidents.* New York: Routlegde

Rosness, R., Grøtan, T.O., Guttormsen, G., Herrera, I.A., Steiro, T., Størseth, F., Tinmannsvik, R.K., & Wærø, I. (2010) *Organisational Accidents and Resilient Organisations: Five Perspectives. Revision 2.* Trondheim: SINTEF

Røyksund, M. (2011). *Informasjonssikkerhet i kraftforsyningen.* (Masteravhandling). Stavanger: Universitetet i Stavanger.

Sivertsen, T. K. (2007). *Risikoanalyse av samfunnskritiske ikt-systemer-Teknologiske Erfaringer* (FFI RAPPORT 2007/00910). Hentet fra

http://rapporter.ffi.no/rapporter/2007/00910.pdf

Skotnes, R. Ø. (2015). *Risk perception regarding the safety and security of ICT systems in electric power supply network companies*. *1*(19), article 4.

Standard Norge, NS 5830. (2012). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – terminologi.

Standard Norge, NS 5832. (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.

Stranden, R. (2019). *Sikring*. Gyldendal: Oslo.

Sovacool, B.K., Axsen, J., Sorrell, S. (2018). Promoting novelty, rigor, and style in energy social science: *Towards codes of practice for appropriate methods and research design. Energy Research & Social Science*(45), 12-42.

Tjora, A. (2012). *Kvalitative forskningsmetoder i praksis.* Oslo: Gyldendal.

Utenriksdepartementet. (2017, 27. september). Internasjonal cyberstrategi for Norge. Hentet fra: https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategi_web.pdf

Weick, K.E, Sutcliffe, K.M & Obstfeld, D. (1999). Organizing for High Reliability: Processes of Collective Mindfulness. *Research in Organizational Behaviour*(1), 81-123.

Yin, R. K. (2018). *Case Study Research. Design and Methods*. Thousand Oaks: Sage.

.

Vedlegg 1: Oversikt over dokumenter til dokumentanalyse

Utgivelsesår	**Utgiver**	**Tittel**
2014	Deloitte	Skytjenester i energiforsyningen - en forstudie
2015	Justis- og beredskapsdepartementet	Digital sårbarhet - sikkert samfunn
2015	NVE	Teknologiskifte i energiforsyningen
2016	NVE	IKT-systemers rolle og betydning for strukturen i kraftforsyningen
2017	NVE	Informasjonssikkerhetstilstanden i energiforsyningen
2017	NVE	Metodikk for informasjonsinnhenting etter IKT-sikkerhetshendelser i driftskontrollsystem
2017	NVE	Regulering av IKT-sikkerhet
2020	NVE	Kartlegging av bruk av tingenes internett (IoT/ IIoT) i norsk kraftforsyning
2018	Næringslivets sikkerhetsråd (NSR)	Mørketallsundersøkelsen 2018

Vedlegg 2: Intervjuguide

Introduksjonsrunde
En liten presentasjonsrunde om oss selv og oppgaven, samt formålet med denne.

Introduksjonsspørsmål
1. Hvilken bakgrunn har du?

2. Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder du har?

3. Kan du fortelle litt om hvilken rolle virksomheten har i kraftforsyningen, da nærmere;
- Overordnet
- Tilknyttet arbeid med IKT og cybersikkerhet

Digitalisering og risiko
Kraftforsyningen har vært utsatt for flere teknologiske utviklinger. I denne oppgaven har vi eksempelvis sett til utrullering av AMS, tilkobling av SCADA til tilgrensende systemer, bruk av skybaserte tjenester og administrative systemer. Den teknologiske utviklingen tatt i betraktning;

4. Hva vil du legge i begrepet cyberrisiko?

5. Det uttrykkes av flere utvalg og nasjonale sikkerhetsmyndigheter (NSM, PST, Lysneutvalget) at risiko tilknyttet digitalisering kan være et resultat av både tilsiktede og utilsiktede hendelser. Med bakgrunn i dette;
- Hvilke farer og trusler mener du kraftforsyningen står ovenfor?
- Relatert til trusler og potensielle trusselaktører, hva mener du er deres intensjon og motivasjon?

6. Hvordan mener du digitalisering påvirker bransjens risikobilde?
- Kan du tenke på noen konkrete endringer i risikobilde etter implementering av og/eller oppdatering til digitale løsninger?

7. Hvilke konsekvenser kan oppstå dersom dere utsettes for uønskede hendelser? Eksempelvis forstyrrelser, sabotasje, kompromittering og svikt relatert til;
- Administrative system
- SCADA/driftskontrollsystemene
- AMS
- Skybaserte tjenester

8. I lys av tidligere diskuterte farer og trusler, kan du si noe om potensielle sårbarheter ved digitalisering?

Risikovurdering
9. Ifølge kraftberedskapsforskriften skal risikovurderinger gjennomgås årlig og oppdateres ved behov. Videre vises det av § 6-9 at virksomheter skal gjennomføre risikovurdering ved systemendringer av digitale informasjonssystemer
- Hvordan jobber dere med dette?
- Hvilke metoder benytter dere for risikovurdering ved systemendringer?
- Hvordan benyttes resultatene fra vurderingen?

10. Benyttes NVE's veileder for risiko og sårbarhetsanalyser (2010)?
- Åpner veilederen opp for å analysere risikoen for både tilsiktede og utilsiktede hendelser?

11. Kraftberedskapsforskriften fremmer også krav til sikring av digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser
- Har dere opplevd slike uønskede hendelser?
- Kan du si noe om hendelsenes karakter, er de tilsiktede/utilsiktede?
- Påvirker erfarte hendelser oppdatering og gjennomgang av risikovurderinger? Eventuelt hvordan?

12. Påvirker digitaliseringsprosesser gjennomføring/oppdatering av risikovurderinger? Eventuelt hvordan?

Risikohåndtering
13. Med bakgrunn i hva dere avdekker i risikovurderingene, hvordan følges potensielle farer og trusler opp i det praktiske sikkerhetsarbeidet?

14. Ifølge Kraftberedskapsforskriften § 6-9 skal virksomheter sikre digitale informasjonssystemer med tanke på ivaretakelse av konfidensialitet, integritet og tilgjengelighet.
- Hvordan arbeider dere i henhold til dette lovverket?
- Hvordan oppfatter dere andre aktører i kraftforsyningen arbeider med sikring av digitale informasjonssystemer?

15. Om dere har opplevd uønskede hendelser relatert til digitale informasjonssystemer, hvordan ble situasjonen håndtert?
- Hvordan forebygges liknende eller relaterte situasjoner?
- Hvordan formidles potensielle uønskede hendelser innad i virksomheten?
- Fører uønskede hendelser til endring i praksis?

16. Finnes det arenaer for erfaringsutveksling etter uønskede hendelser?
- Innad virksomheten
- På tvers mellom virksomheter i kraftforsyningen

17. Kan du si noe om kunnskapsnivået tilknyttet cybersikkerhet i virksomheten?

18. Opplever dere noen utfordringer tilknyttet arbeid med cybersikkerhet i virksomheten? Eventuelt hvilke?

19. Hva anser du som viktige organisatoriske betingelser for god cybersikkerhet?

20. Har digitaliseringen av kraftbransjen hatt betydning for det praktiske sikkerhetsarbeidet?
- På hvilken måte?

Er det noen spørsmål eller tema du forventet ville bli tatt opp under i intervjuet, som er utelatt?

Vedlegg 3: Oversikt over informanter

Informant	**Funksjon og erfaring**
Informant 1	Mer enn 30 år erfaring innen kraftbransjen i ulike funksjoner
Informant 2	Mer enn 20 års erfaring innen IKT-sikkerhet i kraftbransjen, IKT-sikkerhetskoordinator
Informant 3	Mer enn 15 års erfaring innen kraftbransjen i ulike funksjoner, beredskapskoordinator
Informant 4	Flere tiårs erfaring innen kraftselskap, AMS-ansvarlig
Informant 5	Mer enn 5 års erfaring innen cybersikkerhet, IKT-sikkerhetsrådgiver
Informant 6	Jobber som IKT-sikkerhetsleder i kraftkonsern
Informant 7	Lang erfaring fra ulike sikkerhetsmiljøer. Jobber med digital sikkerhet i kraftbransjen
Informant 8	Jobber som IKT-sikkerhetsleder i kraftselskap

Vedlegg 4: NSD sin vurdering

Prosjekttittel
Cybersikkerhet i kraftbransjen

Referansenummer
463747

Registrert
31.01.2020 av Sigrid Haug Selnes - sh.selnes@stud.uis.no

Behandlingsansvarlig institusjon
Universitetet i Stavanger / Det teknisk- naturvitenskapelige fakultet / Institutt for sikkerheit, økonomi og planlegging

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)
Ole Andreas Engen, ole.a.engen@uis.no, tlf: 92467852

Type prosjekt
Studentprosjekt, masterstudium

Kontaktinformasjon, student
Sigrid Haug Selnes, sigrid_hs@hotmail.com, tlf: 99531534

Prosjektperiode
01.01.2020 - 15.06.2020

Status
11.02.2020 - Vurdert

Vurdering (1)

11.02.2020 - Vurdert
Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet 11.02.2020 med vedlegg, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 15.06.2020.

LOVLIG GRUNNLAG

Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER

NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om: - lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen - formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke viderebehandles til nye uforenlige formål - dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet - lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet.

DE REGISTRERTES RETTIGHETER

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20). NSD vurderer at informasjonen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13. Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER

NSD 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). For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET

NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet. Lykke til med prosjektet! Tlf. Personverntjenester: 55 58 21 17 (tast 1)