Norsk kraftforsyning i møte med fremtidens trusselbilde og moderne sårbarhetsflater

Bjørn Henrik Lundqvist

Masteroppgave i Samfunnssikkerhet

Institutt for sikkerhet, økonomi og planlegging

Universitetet i Stavanger

Våren 2023

DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

MASTEROPPGAVE

Studieprogram/spesialisering: Masterprogram i samfunnssikkerhet	*Vår, 2023* Åpen
Forfatter: Bjørn Henrik Lundqvist	
Fagansvarlig ved UiS: Claudia Morsut	
Tittel på oppgaven: Norsk kraftforsyning i møte med fremtidens trusselbilde og moderne sårbarhetsflater Engelsk tittel: Norwegian power supply in the face of future threats and modern vulnerabilities	
Studiepoeng: 30	
Emneord: Digitalt trusselbilde Energipolitikk Energisikkerhet Kraftberedskap Kraftforsyning Sammensatte trusler Sikkerhetspolitikk	Sidetall: 103 + vedlegg/annet: 133 Stavanger, *14.06.23*

Forord

Jeg er stolt over å endelig være i mål med masteroppgaven ved samfunnssikkerhetsprogrammet på UIS. Til tross for et stort faglig engasjement, imøtekommende informanter og en dyktig veileder har arbeidet tidvis vært utfordrende og faglig krevende. Herunder har tilgangen på informasjon og konkretiseringen av oppgavens struktur periodevis budt på utfordringer og stilt store krav til pågangsmot og kreativitet. Likevel har skriveprosessen vært akademisk utviklende og jeg opplever å ha tilegnet meg et betydelig læringsutbytte gjennom forskningsprosjektet. Videre har det vært faglig givende å få muligheten til å engasjere seg i en samfunnaktuell utfordring og en interessesant tematikk.

I møte med oppgavens problemstilling har jeg fokusert på å legge til rette for en bred, innledende litteraturgjennomgang og en helhetlig informasjonsinnhenting. I dette arbeidet vil jeg rette en stor takk til relevante virksomheter og organisasjoner som har bidratt med informanter. Herunder har Norges vassdrags- og Energidirektorat (NVE), Forsvarets forskningsinstitutt (FFI) og Elvia vært svært behjelpelige med å stille informanter til disposisjon. Informantene har i kraft av sin funksjon, faglige kunnskap og erfaringsbaserte innsikt bidratt med verdifull informasjon og utgjort et helt essensielt bidrag til besvarelsen av oppgavens problemstilling. Muligheten til å få diskutere oppgavens tematikk med et tverrfaglig spekter av toneangivende aktører på feltet har samtidig åpnet for ny innsikt og interessante perspektiver. Videre vil jeg rette en stor takk til min veileder ved Universitetet i Stavanger, Claudia Morsut. Hennes faglige innspill og konstruktive tilbakemeldinger har vært retningsgivende for prosjektet og uvurderlige i utformingen av sluttproduktet.

Samlet sett erfarer jeg at kombinasjonen av faglig interesse, en dynamisk sikkerhetspolitisk situasjon og interesserte støttespillere har bidratt til et stort engasjement og rikelig med diskusjoner rundt kraftforsyningen som kritisk samfunnsfunksjon. Alt i alt har skriveprosessen vært svært lærerik på et personlig plan, så vel som på et faglig plan. Jeg håper med dette å levere en oppgave som bidrar til rette søkelyset mot den samfunnsmessige betydningen av en funksjonell og pålitelig kraftforsyning.

God lesning!
Stavanger, 14.06.23

Sammendrag

Kraftforsyningen viser på et overordnet nivå til de systemer og leveranser som er nødvendig for å ivareta samfunnets behov for elektrisk energi. Det norske kraftsystemet er et sammenhengende og komplekst system bestående av ulike elementer som må koordineres og virke i samspill for at systemet som helhet skal fungere tilfredsstillende. Følgelig vil en enkeltstående svikt i en vital part kunne forårsake en kaskade av eskalerende ringvirkninger. Som samfunnsfunksjon utgjør kraftsektoren samtidig en essensiell komponent i opprettholdelsen av en rekke andre grunnleggende samfunnsfunksjoner og infrastrukturer. Skadepotensialet og samfunnsrisikoen ved et bortfall i leveransesikkerheten er dermed enormt og utgjør en vesentlig sikkerhetsutfordring for den norske samfunnssikkerheten. Som en konsekvens av den tiltagende samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen har imidlertid trusselbildet mot kraftforsyningen skjerpet seg i takt med det siste årets geopolitiske uroligheter. Med utgangspunkt i kraftforsyningen som kritisk samfunnsfunksjon har jeg på denne bakgrunn ønsket å belyse hvordan sikkerheten rundt norsk kraftforsyning påvirkes av samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen gjennom en kvalitativ forskningstilnærming.

Til tross for at den digitale utviklingen bidrar til effektivisering og praktiske løsninger på komplekse utfordringer, følger det samtidig et bredt spekter av nye sårbarhetsflater i kjølvannet av den omfattende samfunnsdigitaliseringen. Som en konsekvens av at organisasjoner, teknologi og fysiske enheter koples sammen på måter som tidligere var utenkelige forsterkes det gjensidige avhengighetsforholdet mellom systemer og maskiner. I den forbindelse fremheves den tiltagende bruken av digitale underleverandører, eksponering av sentrale driftssystemer mot det åpne nettet, økt avhengighet til IKT-systemer, tvetydige sikkerhetskrav og knapphet på kompetent personell som sentrale sikkerhetsutfordringer der åpner for en bredere eksponering mot digitale trusselaktører.

Som et resultat av den antatte russiske målsetningen om å sette europeisk energisikkerhet under press og den tiltagende energikrisen Europa står i, har norsk olje- og energisektor samtidig fått en stadig større sikkerhetspolitisk betydning for resten av Europa. I takt med den voksende sikkerhetspolitiske verdien og økt internasjonalisering vil naturligvis også trusselbildet mot kraftforsyningen skjerpes. Sett i lys av den geopolitiske utviklingen fremhever informantene som har bidratt til oppgaven at interstatlig etterretningsvirksomhet,

digitale nettverksoperasjoner og cyberangrep utgjør de største «security-truslene» mot leveransesikkerheten. Herunder løfter flere nasjonale sikkerhetsmyndigheter frem russisk etterretningsvirksomhet som den største enkeltstående trusselaktøren mot norske sikkerhetsinteresser. I den forbindelse forventes det at norske virksomheter vil utsettes for et bredere spekter av sammensatte virkemidler og digitale nettverksoperasjoner som et ledd i den interstatlige etterretningsvirksomheten. Som en konsekvens vil det som tidligere var energipolitikk i større grad smelte sammen med, og underordnes, norsk sikkerhetspolitikk.

Sett i sammenheng med det foreliggende trusselbildet legger dagens moderne og digitale sårbarhetsflater til rette for et bredere handlingsrom og nye angrepsflater for ondsinnede trusselaktører. Samtidig vil næringslivets stadig mer sentrale rolle i arbeidet med nasjonale sikkerhetshensyn og den økonomiske logikken om profittmaksimering i flere tilfeller kunne kollidere med nasjonale sikkerhetshensyn og bidra til å bygge opp under de voksende digitale sårbarhetsflatene. Herunder slår nasjonale sikkerhetsmyndigheter fast at potensielle nettverksoperasjoner i hovedsak forventes å rette seg mot relativt enkle sårbarheter ved systemene som utdatert programvare, svake og gjenbrukte passord eller manglende to-faktorautentisering. Følgelig er det nærliggende å legge til grunn at ulike former for sårbarhetsreduserende tiltak og barrierer i betydelig grad vil kunne bidra til å styrke sikkerhetsnivået rundt kraftforforsyningens sentrale systemer og begrense sårbarhetsflatene.

Samlet sett kan det følgelig konkluderes med at samfunnsdigitaliseringen har bidratt til å forandre rammebetingelsene kraftforsyningen opererer under og på denne måten bygd opp under nye sårbarhetsflater for det helhetlige kraftsystemet. De ekspanderende sårbarhetsflatene har samtidig lagt til rette for et bredere handlingsrom for potensielle trusselaktører. All den tid en vedvarende svikt i kraftforsyningen vil få massive ringvirkninger for storsamfunnet i sin helhet er det nærliggende å legge til grunn at disse sårbarhetsflatene utgjør en vesentlig sikkerhetsutfordring for befolknings grunnleggende behov og den norske samfunnssikkerheten. Sett i sammenheng med systemperspektivet utgjør dette sårbarhetsflater aktuelle sikkerhetsaktører på feltet må dimensjonere for i sikkerhetsstyringen gjennom relevante virkemidler og implementering av sårbarhetsreduserende tiltak. Følgelig anbefaler Norges vassdrag- og energidirektorat (NVE), som overordnet beredskapsmyndighet på området, at potensielle digitaliseringsinsentiver i kraftsektoren følges opp av nødvendige sikkerhetsinvesteringer og egnede sikkerhetstiltak.

Summary

At an overall level, the power supply refers to the systems and deliveries that are necessary to meet society's needs for electrical energy. The Norwegian power system is a connected and complex system consisting of various elements that must be coordinated and work together for the system as a whole to function satisfactorily. Accordingly, a single failure in a vital part can cause a cascade of escalating ripple effects. As a societal function, the power sector also constitutes an essential component in the maintenance of a several other basic societal functions and infrastructures. The potential for damage and societal risk in the event of a loss of supply is therefore enormous and constitutes a significant security challenge for the Norwegian societal security. As a consequence of the increasing societal digitization and security policy developments, the threat picture against the power supply has intensified in line with the geopolitical unrest of the past year. Based on the power supply as a critical societal function, I have wanted to shed light on how the security of the Norwegian power supply is affected by societal digitalization and the security policy development through a qualitative research approach.

Despite the fact that digital development contributes to efficiency and practical solutions to complex challenges, there is also a broad range of new vulnerability surfaces in the wake of the extensive societal digitization. As a consequence of organizations, technology, and physical entities being interconnected in ways that were previously unthinkable, the mutual dependency between systems and machines is reinforced. In this context, the increasing use of digital subcontractors, exposure of central operating systems to the open network, increased dependence on ICT-systems, ambiguous security requirements, and scarcity of competent personnel are highlighted as central security challenges that open up for a broader exposure to digital threat actors.

As a result of the assumed Russian objective to put European energy security under pressure and the growing energy crisis that Europe is facing, the Norwegian oil and energy sector has simultaneously gained an increasingly significant security policy importance for the rest of Europe. In line with the growing security policy value and increasing internationalisation, the threat picture against the power supply will naturally be sharpened. In light of the geopolitical developments, the informants who have contributed to the thesis emphasize that interstate intelligence activities, digital network operations, and cyber-attacks constitute the largest

security threats to the Norwegian power supply security. Furthermore, several national security authorities highlight Russian intelligence activities as the single biggest threat to Norwegian security interests. In this context, Norwegian companies are expected to be exposed to a broader range of composite means and digital network operations as part of the interstate intelligence activity. In this way, what was previously energy policy will merge with, and be subordinate to, Norwegian security policy.

In light of the present threat picture, today's modern and digital vulnerability surfaces provide a wider scope of action and new attack surfaces for malicious threat actors. At the same time, the increasingly central role of the business community in national security considerations and the economic logic of profit maximization in several cases may collide with national security considerations and contribute to building up under the growing digital vulnerability surfaces. Herein, national security authorities assert that potential network operations are expected to primarily target relatively simple vulnerabilities in the systems, such as outdated software, weak and reused passwords, or lack of two-factor authentication. Consequently, it is reasonable to assume that various forms of vulnerability-reducing measures and barriers can significantly contribute to strengthening the security level around the central systems of the power supply.

Overall, it can be concluded that societal digitalization has contributed to changing the framework conditions under which the power supply operates and thereby created new vulnerability surfaces for the integrated power system. The expanding vulnerability surfaces have also provided a wider scope of action for potential threat actors. Given that persistent failure in power supply will have massive ripple effects for society as a whole, it is reasonable to assume that these vulnerability surfaces constitute a significant security challenge for the fundamental needs of the population and the Norwegian societal security. In the context of the system perspective, these vulnerability surfaces constitute relevant security challenges that security actors in the field must dimension for in security management through relevant measures and implementation of vulnerability-reducing measures. Consequently, the Norwegian Directorate of Waterways and Energy (NVE), as the supreme security authority in the area, recommends that potential digitalization incentives are followed up by necessary security investments and suitable security measures.

Innholdsfortegnelse

Figurliste

Tabell-liste

1.0 – INNLEDNING MED HOVEDPROBLEMSTILLING

Gjennom masterprogrammet i samfunnssikkerhet har jeg fattet stadig større interesse for betydningen av en funksjonell og pålitelig kraftforsyning. Kraftforsyningen utgjør en essensiell komponent i opprettholdelsen av en rekke grunnleggende samfunnsfunksjoner og en svikt i leveransesikkerheten vil resultere i massive konsekvenser for det norske samfunnet i sin helhet. Den sikkerhetskritiske avhengigheten er på mange måter total i den forstand at samfunnet vil oppleve en spontan stans innenfor de fleste samfunnssektorer i øyeblikket kraftforsyningen opphører og flere kritiske samfunnsfunksjoner vil umiddelbart eller i løpet av kort tid svikte (NVE, 2008).

På bakgrunn av samfunnsdigitaliseringen, dagens geopolitiske uroligheter og den sikkerhetspolitiske utviklingen har imidlertid trusselbildet mot kraftforsyningen endret seg gjennom de siste årene. Kritiske beredskapssituasjoner som tekniske svikter, naturhendelser og ekstremvær har i takt med utviklingen i konfliktflaten mellom Russland og vesten havnet i skyggen av trusselen for intenderte sabotasjehandlinger, komplekse cyberangrep og hybride virkemidler. På bakgrunn av den tiltagende utviklingen i risikobildet ønsker jeg derfor å undersøke hvordan sikkerheten rundt norsk kraftforsyning og de tilhørende sårbarhetsflatene påvirkes av dagens sikkerhetspolitiske situasjon og fremtidens trusselbilde. Herunder ønsker jeg å kartlegge til hvilken grad sikkerheten rundt norsk kraftsektor påvirkes av samfunnsutviklingen, på hvilken måte sikkerhetsstyringen innrettes etter forventet utvikling i det fremtidige trusselbildet og hvordan samfunnsdigitaliseringen har åpnet for nye sårbarhetsflater rundt den norske kraftforsyningen som en kritisk samfunnsfunksjon.

Det operative ansvaret for norsk kraftforsyningsberedskap er i det daglige delegert fra Olje- og energidepartementet (OED) til Norges vassdrags- og energidirektorat (NVE). NVE jobber for at alle involverte aktører innenfor norsk kraftforsyning skal utvikle en bevisst holdning til beredskapsarbeidet og iverksette nødvendige tiltak for å opprettholde robusthet i egne systemer. Den overordne målsetningen med deres beredskapsforberedende arbeid er å legge til rette for en sikker kraftforsyning uten avbrudd i hverdagen, men også under kriser og ved ekstraordinære hendelser. Samfunnsoppdraget løses i hovedsak gjennom forebyggende og proaktive tiltak. Herunder ivaretar NVE sine myndighetsoppgaver gjennom tilsyn, øvelser og veiledning, samtidig som behovet for skadebegrensning og krisehåndtering også vektlegges i definerte tilfeller (NVE, 2008).

I kjølvannet av kraftforsyningens stadig mer sentrale rolle i opprettholdelsen av kritiske samfunnsfunksjoner og vitale samfunnsinteresser følger naturligvis også en bredere sårbarhetsflate. I tidligere tider har den norske leveransesikkerheten primært vært eksponert for ytre påvirkninger som naturhendelser, ekstremvær, fysiske påkjenninger, konstruksjonsfeil, klimaendringer og tekniske svikter. Som følge av krigen i Ukraina er Europa imidlertid blitt kastet inn i en periode preget av sikkerhetspolitiske spenninger og globale endringer i maktstrukturene. I takt med samfunnsutviklingen og den digitale transformasjonen – der det gjensidige avhengighetsforholdet mellom mennesker, teknologi og komplekse systemer forsterkes – følger samtidig et bredt spekter av nye sårbarhetsflater og trusler for storsamfunnet i sin helhet (NSM, 2023).

De senere årene har man også kunnet observere en bred fremvekst i hybrid virkemiddelbruk – av både militær, politisk, økonomisk, sivil og juridisk karakter – i interstatlig krigføring. Virkemidlene rettes mot sårbarheter innenfor alle samfunnssektorer og demokratiske staters institusjoner. Hovedintensjon ved virkemiddelbruken vil i de fleste tilfeller være å påvirke den offentlige opinionen i et samfunn, skade beslutningstakingen og bearbeide motstanderens moral og motstandsdyktighet. I takt med utviklingen i det hybride trusselbildet fremhever Forsvarets forskningsinstitutt (2018, s. 3-5) at et lavintensivt hybridangrep mot norsk infrastruktur og norske institusjoner utgjør et *mulig* scenario. Risikoen for tilsiktede handlinger som dataangrep, sabotasje og påvirkningsoperasjoner vil naturligvis også aktualiseres i takt med fremtidige endringer i det globale trusselbildet og kraftforsyningen utgjør på flere områder et sårbart og virkningsfullt mål for demokratiske samfunn flest. Med andre ord er det naturlig å legge til grunn at dagens sikkerhetspolitiske situasjon – med økende uroligheter og endringer i trusselbildet – også påvirker sikkerheten og beredskapsløsningene rundt det helhetlige systemet av norsk kraftforsyning gjennom flere ulike dimensjoner (Bredesen & Reichborn-Kjennerud, 2016).

1.1 – Tema og problemstilling

Temaet for masteroppgaven vil følgelig være hvordan sikkerheten rundt norsk kraftforsyning påvirkes av samfunnsdigitaliseringen sett i lys av dagens sikkerhetspolitiske uroligheter og til hvilken grad trusselbildet har endret seg i takt med den sikkerhetspolitiske situasjonen. Herunder vil oppgaven spesielt fokusere på hvordan NVE, som ansvarlig forvalter, oppfatter, vurderer og håndterer den ekstraordinære utviklingen i risikobildet. Videre vil identifiseringen av potensielle sårbarheter i opprettholdelsen av leveransesikkerheten stå sentralt. Oppgaven

tar også sikte på å belyse mer tradisjonelle risikoer mot leveransesikkerheten som naturkatastrofer, tekniske svikter, ekstremvær og tilsvarende hendelser. Både for å etablere et overordnet beredskapsområde for kraftforsyningen som kritisk samfunnsfunksjon, men også for å illustrere hvordan risikobildet har utviklet seg i takt med samfunnsutviklingen og tilspisningen av den sikkerhetspolitiske situasjonen.

Med utgangspunkt i kraftforsyningen som kritisk samfunnsfunksjon har jeg utarbeidet følgende problemstilling for oppgaven:

«Hvordan påvirkes sikkerheten rundt norsk kraftforsyning av samfunnsdigitaliseringen, sett i lys av dagens sikkerhetspolitiske situasjon?»

1.1.1 – Forskningsspørsmål

Problemstillingen inviterer til en kartlegging av samfunnsdigitaliseringens innvirkning på sikkerheten og sårbarhetsflatene rundt norsk kraftforsyning, samtidig som den også legger premissene for en vurdering av relevante sikkerhetspolitiske faktorers betydning for utviklingen i trusselbildet. For å konkretisere oppgavens tema og belyse oppgavens problemstilling vil jeg samtidig ta sikte på å besvare følgende supplerende forskningsspørsmål gjennom masteroppgaven:

- *F1: Hvilke kilder til risiko utgjør trusler mot levereansesikkerheten for norsk kraftforsyning?*
- *F2: Hvilke sentrale sårbarheter foreligger i opprettholdelsen av leveransesikkerheten til norsk kraftforsyning?*
- *F3: Hvordan påvirkes trusselbildet mot og sårbarhetsflatene ved norsk kraftforsyning av samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen?*
- *F4: Hvordan kan identifiserte sårbarheter reduseres?*

1.2 – Avgrensning

All den tid norsk kraftforsyning utgjør et svært komplekst system av ulike produsenter, leverandører, kraftverk og magasiner vil jeg være nødt til å behandle kraftforsyningen på et samlet overordnet nivå og som en felles kritisk samfunnsfunksjon slik kraftforsyningen er definert i DSBs rapport om kritiske samfunnsfunksjoner (DSB, 2016, s. 8-19). Følgelig vil jeg

kun i begrenset grad behandle de ulike enkeltkomponentene og undersystemene som tilsammen utgjør kraftforsyningen, men heller innta en generisk tilnærming til kraftproduksjonen som et helhetlig system. Herunder vil sentrale aktører på feltet som Norges vassdrags- og energidirektorat og Kraftforsyningens beredskapsorganisasjon (KBO) stå i fokus. Kraftforsyningen vil avgrenses mot andre kritiske samfunnsfunksjoner som for eksempel vannforsyningen eller elektroniske kommunikasjonstjenester. Organisatoriske likheter tatt i betraktning er det likevel nærliggende å anta at potensielle funn også vil ha en viss overføringsverdi til andre beslektede samfunnsfunksjoner og samfunnskritiske infrastrukturer.

Sett opp mot fremtidens trusselbilde vil det naturligvis være en umulig oppgave å kartlegge alle fremtidige risikoagenter for norsk kraftproduksjon og leveransesikkerhet. Oppgaven tar heller ikke sikte på å identifisere alle tenkelige hendelser som kan true kraftforsyningen, men vil i større grad behandle trusselbildet og sårbarhetsflatene på et overordnet nivå. Herunder avgrenses oppgaven til å i hovedsak kartlegge hvordan sikkerheten rundt norsk kraftforsyning påvirkes av dagens sikkerhetspolitiske uroligheter sett i lys av de nye sårbarhetsflatene samfunnsdigitaliseringen medfører. Den sikkerhetspolitiske situasjonen vil beskrives på et grunnleggende nivå og begrenses til den økende konfliktflaten mellom vesten på den ene siden og autoritære regimer som Kina og Russland på den andre. Det er primært den økende stormaktsrivaliseringen og Russlands angrep på Ukraina som vil stå i fokus. Herunder vil det trekkes paralleller mellom den drastiske utviklingen i det globale sikkerhetspolitiske landskapet og konsekvensene utviklingen får for Norge og norsk kraftforsyning.

Sikkerheten rundt kraftforsyningen vil behandles på et helhetlig og nasjonalt nivå. Jeg vil ikke gå i dybden på lokale kraftanlegg eller konkrete trusselbilder, men underbygge potensielle funn med relevante enkelteksempler fra virkeligheten. Kombinasjonen av sårbarhetsflatene den sikkerhetspolitiske situasjonen og samfunnsdigitaliseringen medfører vil danne fundamentet for oppgaven. Heller enn å fokusere på enkeltdetaljer vil konturene og de overordnede hovedlinjene stå sentralt. Det er primært utviklingen i trussel- og sårbarhetsbildet, og på hvilken måte sentrale aktører på feltet planlegger å håndtere denne utviklingen, som ønskes kartlagt.

1.3 – Disposisjon

For å besvare oppgavens problemstilling vil jeg innledningsvis definere sentrale begreper på området, redegjøre for oppgavens samfunnsmessige kontekst og motivere problemstillingen. Herunder vil jeg kort beskrive kraftforsyningen som kritisk samfunnsfunksjon, sentrale faktorer og utviklingstrekk ved dagens sikkerhetspolitiske situasjon og med utgangspunkt i nasjonale trusselvurderinger presentere potensielle trusler for den norske kraftforsyningen, sett i lys av det siste årets geopolitiske uroligheter. Deretter vil jeg redegjøre for sentrale utviklingstrekk ved samfunnsdigitaliseringen og samtidig beskrive hvordan den digitale transformasjonen åpner opp for en rekke nye sårbarhetsflater i kjølvannet av det gjensidige avhengighetsforholdet som har oppstått mellom mennesker, maskiner og teknologi.

Etter å ha etablert en overordnet samfunnsmessig kontekst, motivert problemstillingen og gjort rede for sentrale forskningsspørsmål vil jeg presentere oppgavens teoretiske rammeverk. Jeg vil samtidig klarlegge på hvilken måte de teoretiske bidragene gjør seg gjeldende i besvarelsen av oppgavens problemstilling og tilhørende forskningsspørsmål. For å finne frem til et helhetlig teoretisk rammeverk har jeg i all hovedsak tatt utgangspunkt i pensumlitteraturen og ulike modeller introdusert gjennom masterprogrammet. Jeg har valgt ut tre teoretiske hovedtilnærminger som i kombinasjon danner et godt grunnlag for å etablere en helhetlig forståelse for NVEs beredskapsforbedrende arbeid med den norske kraftforsyningen og samtidig kartlegge hvilke mekanismer som – sett i lys av samfunnsdigitaliseringen og dagens sikkerhetspolitiske situasjon – virker inn på leveransesikkerheten og sikkerhetsstyringen av norsk kraftforsyning.

Deretter presenteres oppgavens metodiske forankring. Herunder beskrives fremgangsmåten for informasjonsinnhenting og oppgavens overordnede forskningsstrategi. Jeg vil kort redegjøre for de ulike kildene til informasjonen og begrunne valget av informasjonskilder. Samtidig vil jeg utdype hvordan innsamlet data bearbeides, strukturers og analyseres, hvordan oppgaven ivaretar forskningsetiske regler og hvordan sensitive opplysninger behandles. Avslutningsvis vil potensielle svakheter ved metodikken og mulige feilkilder bemerkes. Herunder vil også relevante muligheter og begrensninger ved metodevalget beskrives og min forutforståelse for oppgavens tematikk anskueliggjøres.

I empiridelen vil jeg presentere det innsamlede datamaterialet og oppsummere resultatene fra de foreliggende empiriske undersøkelsene. Herunder presenteres en oppsummering av

gjennomførte intervjuer og sentrale funn fra dokumentanalysene. Videre vil innsamlet data sees i sammenheng med oppgavens teoretiske rammeverk, samfunnsmessige kontekst og drøftes opp mot problemstillingen under delkapittel 6.0. Resultatenes faktiske innebyrd og potensielle feilkilder diskuteres, før sentrale funn konkretiseres og den faglige diskusjonen sluttelig oppsummeres i konklusjonen. Avslutningsvis presenteres forslag til eventuelle oppfølgingsstudier på bakgrunn av oppgavens funn, konklusjoner og samfunnsmessige kontekst.

1.4 – Begrepsavklaring

Samfunnsrisiko

På et overordnet nivå definerer Aven og Renn (2010) begrepet risiko som usikkerheten om og alvorlighetsgraden av konsekvensene (eller utfallene) av en aktivitet med hensyn til verdier mennesker verdsetter. Samfunnsrisiko defineres på den andre siden som kombinasjonen av sannsynligheten for at en gitt hendelse inntreffer og antallet personer som utsettes for eksponering av faren i en gitt populasjon (Njå, Sommer, Rake & Braut, 2021, s. 217-219). På generelt grunnlag ønsker man i et samfunnssikkerhetsperspektiv at risikoen knyttet til aktiviteter og virksomheter begrenses til et akseptabelt nivå. Hva som representerer et akseptabelt risikonivå vil imidlertid variere fra system til system avhengig av type virksomhet, i hvilken sammenheng virksomheten foregår og hvem som utfører virksomheten og vil fastsettes utefra definerte akseptkriterier (Njå et al., 2021, s. 207-208). På bakgrunn av det moderne samfunnets nye farer introduserte Beck (1992) begrepet «risikosamfunnet» som viser til hvordan majoriteten av nye risikoer oppstår som en konsekvens av vitenskapelige, samfunnsmessige og menneskeskapte endringer, der vitenskap og teknologi spiller en vesentlig rolle som både årsak til risikoene, redskap til å definere risikoene og midler for å begrense risikoene.

Samfunnssikkerhet

I stortingsmelding nr. 10 (Justis- og beredskapsdepartementet, 2017, s. 8-10) *Risiko i et trygt samfunn – Samfunnssikkerhet* defineres samfunnssikkerhet som *«Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare».*

Det presiseres at hendelsene kan være utløst av naturen, et utslag av intenderte handlinger eller forårsaket av teknisk eller menneskelig svikt. Utover konkrete enkelthendelser kan også tilstander i samfunnet true samfunnssikkerheten og utgjøre en fare for samfunnets grunnleggende verdier og funksjoner. På bakgrunn av de vide definisjonene bør samfunnssikkerhet følgelig forståes som konsept heller enn et entydig begrep. I pensumlitteraturen defineres samfunnssikkerhet som *alle tiltak og aktiviteter som bidrar til at samfunnets kritiske funksjoner ivaretas for å sikre borgernes liv, helse og grunnleggende behov.* Samtidig fremheves det at «samfunnets kritiske funksjoner» tar utgangspunkt i dynamiske forståelser i stadig endring og vil variere basert på organisatorisk nivå og samfunnets utvikling (Njå et. al., 2021, s. 14-15).

På overordnet nivå kan samfunnssikkerheten sies å påvirkes av tre grunnleggende faktorer. Herunder:
- Verdiene som skal beskyttes og deres tilhørende sårbarhetsflater.
- Farene og truslene samfunnet står ovenfor.
- Samfunnets evne til å forebygge og håndtere uønskede hendelser (Justis- og beredskapsdepartementet, 2017, s. 9-10).

Sårbarhet

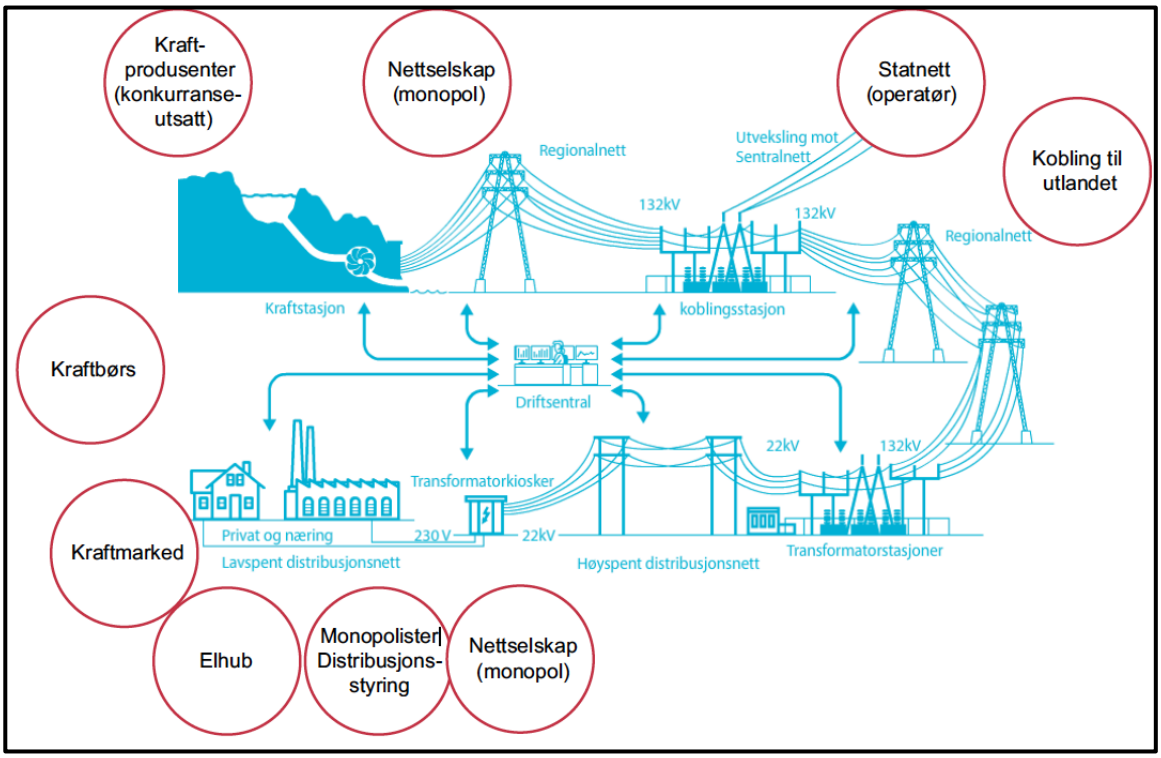
I et samfunnsikkerhetsfaglig perspektiv forståes sårbarhet som sannsynlighetsgraden for at et system eller deler av et system tar skade av å eksponeres for en fare og gir uttrykk for de utfordringer et system vil få med å fungere når det utsettes for en uønsket hendelse eller en ytre påkjenning (Rossignol, Delvenne & Turcanu, 2015, s. 129-131). Et system kan eksempelvis vise til en stat, en virksomhet, en organisasjon eller et enkeltstående datasystem. Sårbarhet må følgelig ses i sammenheng med evnen systemet har til å forsvare seg mot ulike former for trusler og til hvilken grad systemet evner å opprettholde normal drift eller gjenoppta sin opprinnelige virksomhet etter å ha vært utsatt for en ekstraordinær hendelse. Aktuelle trusler inkluderer både intenderte, ondsinnede handlinger og ikke-planlagte, vilkårlige farer. Som begrep er sårbarhet ofte knyttet opp mot mulige tap av samfunnsverdier. Det motsatte av et sårbart system vil som regel omtales som et *resilient* eller et *robust* system. Resiliente systemer beskrives som tilpasningsdyktige til uønskede hendelser og har fokus på gode praksiser og organisatorisk læring heller enn svikt, mangler og uønskede hendelser (Engen, Gould, Kruke, Lindøe, Olsen & Olsen, 2021, s. 99-102).

2.0 – KONTEKST

2.1 – Norsk kraftforsyning

Kraftforsyningen viser på et overordnet nivå til de systemer og leveranser som er nødvendig for å ivareta samfunnets behov for elektrisk energi til blant annet husholdninger, oppvarming, transport, produksjon og fjernvarme. I DSBs (2016, s. 86-90) rapport om kritiske samfunnsfunksjoner defineres kraftforsyningen som en essensiell funksjon for samfunnets funksjonalitet. Blant annet fremheves det at en rekke kritiske samfunnsoppgaver og samfunnsfunksjoner er helt avhengige av et velfungerende el-system med en pålitelig energiforsyning for å opprettholde normal drift. Spesielt for Norge er at elektrisiteten utgjør en betydelig høyrere andel av den totale energibruken enn i de fleste andre sammenlignbare land. Den sikkerhetskritiske avhengigheten gjør følgelig at det må stilles særdeles strenge krav til sikkerhetsstyringen av norsk kraftforsyning og leveransesikkerheten for norsk elektrisitet (DSB, 2016, s. 87-90).

Det norske kraftsystemet er et sammenhengende og komplekst system bestående av ulike elementer som må koordineres og virke i samspill for at systemet som helhet skal fungere tilfredsstillende. Kraftproduksjonen av elektrisk energi utgjøres i all hovedsak – til 98,5% – av vannkraftverk. Videre transporteres energien fra produsentene til forbrukerne gjennom ulike forsyningsanlegg. Herunder har kraftforsyningsnettet i Norge tre ulike nivåer: sentralnettet, regionalnettene og distribusjonsnettene. Sentralnettet binder sammen produksjonen og forbrukerne i ulike landsdeler, gir aktørene adgang til en markedsplass og sørger for sentrale utvekslingspunkt i alle regioner. Regionalnettet utgjør bindeleddet mellom sentralnettet og distribusjonsnettene i de ulike regionene, mens distribusjonsnettene viser til de lokale strømnettene som til slutt distribuerer elektrisk energi til sluttbrukerne. Driftssentralene har ansvaret med fjernovervåking og fjernstyring av kraftforsyningen og har en sentral oppgave i den tekniske driften av kraftnettet. Samtidig vil også andre driftsoppgaver som planlegging, tilstandskontroll, feilretting og daglig ledelse kobles til driftssentralene i det enkelte nettselskap. Samlet sett er kraftsystemet dimensjonert for å kunne overføre tilstrekkelig med elektrisk energi til forbrukerne i timene av året hvor forbruket er høyest. Den totale energietterspørselen i samfunnet dekkes i hovedsak av Norges egen elektrisitetsproduksjon, men i økende grad også gjennom import fra europeiske naboland (NOU 2015:13, s. 129-132). Figuren under er hentet fra NOU av 2015:13 om digital sårbarhet (s. 130) og presenter en forenklet fremstilling av det norske kraftsystemet.



Figur 1: *Forenklet modell av det norske kraftsystemet (NOU 2015:13, s. 130)*

På overordnet nivå er det Olje- og energidepartementet (OED) som har ansvaret for å påse at forvaltningen av kraftforsyningen utføres etter de retningslinjene regjeringen gir. Videre har OED også eieransvaret for statsforetaket Statnett som drifter det riksdekkende sentralnettet. Ansvaret for å forvalte de innenlandske energiressursene er imidlertid delegert til Norges vassdrags- og energidirektorat som er nasjonal reguleringsmyndighet for elektrisitetssektoren. Herunder har NVE det overordnede ansvaret for forsyningssikkerheten i kraftsystemet, og for å samordne beredskapsplanleggingen på området. Under krig og ved beredskapssituasjoner er det følgelig NVE som er definert direktorat til å lede landets kraftforsyning (Olje- og energidepartementet, 2021).

For dette formål er Kraftforsyningens beredskapsorganisasjon (KBO) etablert. KBO ledes av NVE og viser til samarbeidsstrukturen for samordning og ledelse av kraftsystemet. Herunder består KBO-strukturen av alle virksomheter som eier eller driver anlegg (KBO-enheter) med vesentlig betydning for driften av den norske kraftforsyningen. Alle virksomheter som faller inn under KBOs ansvarsområde innehar etter kraftberedskapsforskriften følgelig en selvstendig plikt til å sørge for effektiv sikring og beredskap ved egne anlegg og til å iverksette tiltak for å forebygge, begrense og håndtere virkningene ved ekstraordinære

situasjoner. Herunder utgjør evnen til å opprettholde konfidensialitet, integritet og tilgjengelighet grunnleggende faktorer for kraftforsyningssikkerheten. Direktoratet for samfunnssikkerhet og beredskap (DSB) har på sin side ansvaret for elsikkerhetsregelverket og utgjør dermed også en viktig aktør for innretningen av forsyningssystemet, tilsyn med regelverket og gjennomføringen av risiko- og sårbarhetsanalyser på området (Kraftberedskapsforskriften, 2012, §2-1; NVE, 2013).

2.2 – Sikkerhetspolitiske- og geopolitiske faktorer

24. februar 2022 invaderte Russland nabolandet Ukraina. Siden har konflikten ført til verdensomspennende ringvirkninger på globalt nivå og forandret den sikkerhetspolitiske situasjonen i Europa for uoverskuelig fremtid. I Norge har de geopolitiske urolighetene bidratt til å skjerpe trusselbildet mot samfunnskritisk infrastruktur og nasjonale og internasjonale sikkerhetsinteresser. Som følger har regjerningen ved flere tilfeller siden krigens frembrudd styrket forsvarets beredskap og økt tilstedeværelsen rundt samfunnskritiske objekter og infrastrukturer. Sett under ett beskrives den sikkerhetspolitiske situasjonen som den mest alvorlige på flere tiår og de økte spenningene gjør Norge mer eksponert for påvirkningsoperasjoner, trusler og utenlandsk etterretningsvirksomhet (Statsministerens kontor, 2022).

Forsvarets etterretningstjeneste (2022, s. 8) fremhever i sin årlige trusselvurdering for 2022 at stormaktsrivaliseringen vil prege den sikkerhetspolitiske utviklingen i årene fremover og føre til sterkere og tiltagende polarisering. Her vil mindre stater, som Norge, i stadig større grad avkreves å ta stilling i internasjonale konfliktspørsmål og utsettes for press fra autoritære stormakter som Russland og Kina. Videre vil sammensatte trusler og ulike former for hybride virkemidler som cyberangrep, sabotasje og statlig etterretningsvirksomhet aktualiseres og dominere fremtidens trusselbilde mot Norge og norsk infrastruktur.

Sett opp mot norsk kraftforsyning som kritisk samfunnsfunksjon er det nærliggende å anta at trusselbildet mot leveransesikkerheten vil skjerpes i takt med at energikrisen i Europa tiltar. Energikrisen viser til destabiliseringen av energimarkedene og den utfordrende energisituasjonen som har oppstått i Europa i kjølvannet av Russlands angrepskrig mot Ukraina. Sanksjoner, rettslige implikasjoner og en polarisert geopolitisk debatt har ført til store kutt i importen av russisk gass. Sett i sammenheng med avviklingen av alternative energikilder som kull og kjernekraft har Europa havnet i et energiunderskudd (NOU 2023:3,

s. 33-35). Parallelt med stormaktsrivaliseringen og utviklingen i det sikkerhetspolitiske klimaet beskriver etterretningstjenesten (2023, s. 28-32) at det følgelig er naturlig å anta at trusselbildet mot norske kraftinstallasjoner har tiltatt som et ledd i autoritære regimers hybride krigføring. Særlig siden Norge – i samarbeid med en rekke andre NATO- og EU-land – har tatt aktivt stilling i konflikten gjennom økonomiske bidrag og våpenstøtte til Ukraina og internasjonale fordømmelser av Russlands angrepskrig. Dette har ført til et eskalerende ordskifte, omfattende sanksjoner og sammenbrudd i diplomatiet mellom Russland og de fleste vestlige demokratier (Etterretningstjenesten, 2023, s. 5-6 & s. 28-32).

Som følger truer Russland for første gang på flere tiår med bruk av millitærmakt, atomvåpen og storkrig. Samtidig har man det siste året sett flere eksempler på ekstraordinære hendelser som mistenkes å være russiske sabotasjeaksjoner mot europeiske gass- og energiinstallasjoner. Samlet sett beskriver forsvarets etterretningstjeneste at hendelsene har bidratt til å skjerpe trusselbildet og samtidig ført til at en rekke europeiske land har hevet beredskapen rundt kritiske infrastrukturer og samfunnsfunksjoner. Med andre ord står den norske energiinfrastrukturen ovenfor et endret trusselbilde med potensiale til å utfordre drifts- og forsyningssikkerheten i kraftsystemet. Følgelig har det som tidligere var norsk energipolitikk i større grad smeltet sammen med, og underordnet seg norsk sikkerhetspolitikk (NOU 2023:3, s. 33-35).

2.3 – Samfunnsdigitalisering

På et grunnleggende nivå oppfattes digitaliseringen ofte som et fremtidsrettet og fruktbart samfunnsfenomen som mange aktører ønsker eierskap til. Kort oppsummert innebærer den digitale transformasjonen at analog informasjon gjøres digitalt tilgjengelig og at krevende manuelle arbeidsprosesser, oppgaver, vurderinger og beslutninger automatiseres (Engen et al, 2021, s. 240-246). På denne måtes forsterkes det gjensidige avhengighetsforholdet mellom mennesker og maskiner. Gjennom en samfunnsmessig tilpasning kan følgelig organisasjoner, mennesker og teknologi koples sammen på måter som tidligere var utenkelige og umulige. Digitaliseringen av viktige samfunnsinstitusjoner og kritiske infrastrukturer bidrar på denne måten til praktiske løsninger på komplekse utfordringer, automatisering av manuelle arbeidsoppgaver og en enklere hverdag for folk flest (Unruh og Kiron, 2017). I kjølvannet av samfunnsdigitaliseringen følger imidlertid en bredere sårbarhetsflate som potensielt vil kunne utnyttes av målrettede aktører med ondsinnede intensjoner. Den digitale utviklingen åpner med andre ord for en bredere eksponering mot digitale trusler som cyberangrep, nettsvindel

og uautorisert tilgang til kritiske systemer. Følgelig vil den digitale omstillingen i årene fremover også stilles større krav til en kunnskapsbasert risikohåndtering og en preventiv tilnærming i møte med fremtidens digitale trusselbilde (Engen et al, 2021, s. 242-247).

3.0 – TEORETISK RAMMEVERK

For å finne frem til et helhetlig teoretisk rammeverk som bidrar til å belyse oppgavens forskningsspørsmål har jeg i all hovedsak tatt utgangspunkt i pensumlitteraturen og ulike teoretiske modeller introdusert gjennom masterprogrammet. Herunder har jeg valgt ut tre hovedtilnærminger som satt sammen danner et godt grunnlag for å etablere en forståelse for NVEs sikkerhetsstyring av norsk kraftforsyning og samtidig til å analysere hvilke mekanismer som, sett i lys av samfunnsdigitaliseringen og dagens sikkerhetspolitiske situasjon, vil virke inn på og potensielt true opprettholdelsen av leveransesikkerheten. Hovedtilnærmingene vil suppleres av andre relevante bidrag og teoretiske konsepter fra pensumlitteraturen.

Jeg vil innledningsvis redegjøre for sikkerhet som konsept og beskrive den teoretiske skillelinjen mellom «safety»- og «security»- risikoer. Videre vil jeg med utgangspunkt i DSBs (2016) KIKS-rapport redegjøre kort for samfunnets kritiske funksjoner og infrastrukturer, samt trekke paralleller til kraftforsyningen som kritisk samfunnsfunksjon. Deretter presenteres modell for sikkerhetsstyring av systemer introdusert gjennom Njå et al. (2021, s. 64-65) i pensumlitteraturen. Herunder vil jeg beskrive sentrale tilnærminger på feltet som NAT- og HRO- systemteoriene, redegjøre for grunnleggende aspekter innenfor sikkerhetsstyring og sikkerhetsarbeid og løfte frem betydningen av en god sikkerhetskultur. Videre vil jeg presentere trefaktor-modellen som et hensiktsmessig analyseverktøy for security-trusler og James Reasons (1997) modell om barrierer i dybdeforsvaret av et system. Sluttelig vil jeg redegjøre for potensielle fallgruver og dilemmaer ved samfunnsdigitaliseringen, den tiltagende avhengigheten til digitale verdikjeder og økende integrasjonen av cyber-fysiske systemer.

3.1 – Sikkerhet som konsept

Sikkerhet utgjør et flerdimensjonalt og omdiskutert konsept som har utviklet seg gjennom tidene. På historisk grunnlag har sikkerhet referert til individets trygghetsfølelse og blitt forstått som fraværet av farer. I takt med samfunnsutviklingen har forståelsen imidlertid

utviklet seg til å i større grad omfavne beskyttelsen av storsamfunnet i sin helhet og overlevelsen til nasjonalstaten. Innenfor samfunnssikkerhet som vitenskapsfelt trekkes det som regel en teoretisk skillelinje mellom tradisjonelle safety-risikoer på den ene siden og tilsiktede security-risikoer på den andre. Der safety-risikoer i hovedsak refererer til utilsiktede og ikke-planlagte hendelser som industriulykker, naturkatastrofer og tekniske svikter, viser security-risikoer til målrettede og ondsinnede handlinger som for eksempel cyberangrep, sabotasje og terrorisme. Illustrativt kan skillet visualiseres langs et kontinuum av sikkerhetstruende hendelser, der safety- og security-risikoer representerer hvert sitt ytterpunkt. Hendelsene vil kunne plasseres langs kontinuumet basert på graden av ondsinnet intensjon bak handlingen og vil sprike fra uhell og ulykker på den ene siden til intendere og målrettede tilslag på den andre (Jore, 2019a, s. 156-167).

Jore (2019a, s. 156-158) beskriver «security» som *«...den opplevde eller faktiske evnen til å forberede seg på, tilpasse seg til, motstå og hente seg inn fra farer og kriser forårsaket av menneskers bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking*». All den tid security-risikoer består av målrettede og intenderte handlinger utført av dynamiske trusselaktører vil de, utefra et organisatorisk perspektiv, som regel være mer krevende å identifisere, forutse og forebygge enn mer tradisjonelle safety-risikoer. Herunder vil trusselaktørene som planlegger å begå handlingene kunne vurdere både konsekvensene ved handlingen og sannsynligheten for å oppnå ønsket effekt. Der safety-risikoer ofte kan kvantifiseres og estimeres, vil analyser av security-risikoer preges av usikkerhet, og i større grad stille krav til kvalitative analyseverktøy og faglig ekspertise på bakgrunn av truslenes dynamiske natur og underliggende karakteristikker (Engen et. al, 2021, s. 101; Jore, 2019b, s. 4043-4047).

Innenfor security-feltet opereres det i hovedsak med et konstruktivistisk risikoperspektiv, hvor security-risikoer forståes som et sosialt konstruert begrep der samfunnsviktige systemer eksponeres for tilsiktede handlinger og ondsinnede trusler. All den tid et intendert tilslag forutsetter en rasjonell motpart, som vil justere seg etter potensielle barrierer og iverksatte mottiltak, bør security-trusler følgelig vurderes gjennom andre analyseverktøy enn mer beregnelige safety-risikoer. Samlet sett utgjør security-trusler i større grad en dynamisk risiko med et tilnærmet ubegrenset antall potensielle angrepsscenarioer. Følgelig kan det bli svært utfordrende å kartlegge alle tenkelige sårbarhetsflater og sikre verdiene man ønsker å beskytte fra identifiserte trusselaktører (Jore, 2015, s. 4-6). Utilstrekkelig eller manglende beskyttelse

vil imidlertid medføre sårbarheter som eksponerer verdiene samfunnet ønsker å beskytte. Den samlede risikoen mot en definert verdi kan dermed sees som et uttrykk for forholdet mellom trusselen mot verdien og verdiens sårbarhet mot den konkrete trusselen. Trusselens styrke vil som regel vurderes utefra trusselaktørenes intensjon og kapasitet til å gjennomføre intensjonen. Ulike former for sikringstiltak, som fysiske barrierer eller overvåkning, vil derimot kunne bidra til å begrense trusselaktørens handlingsrom og i mange tilfeller forhindre eller forebygge at handlingene gjennomføres (Engen et. al, 2021, s. 101-103).

3.1.1 – Risikobaserte reguleringsregimer og resiliens

Gjennom historien har security-trusler primært blitt håndtert gjennom preskriptiv lovgivning og statlige reguleringer, og ikke utgjort sikkerhetsutfordringer den enkelte virksomhet har regulert på selvstendig grunnlag. I takt med den teknologiske utviklingen har imidlertid den voksende mengden detaljkrav ført til at regelbaserte tilnærminger ble uhåndterbare og i større grad erstattet av funksjonelle og risikobaserte reguleringsstrategier (Heyerdal, 2022a, s. 6-10). Risikobaserte reguleringsregimer har til å hensikt å kartlegge potensielle risikoer før de manifesterer seg i form av en sikkerhetstruende handling og kjennetegnes av risikokarakteriseringer og målorientering. Når en mulig risiko er identifisert, kan forebyggende tiltak implementeres. Følgelig skal forutgående risikoanalyser danne fundamentet for utviklingen av sikkerhetstiltak med utgangspunkt i funksjonelle målsetninger til sikkerhetsnivået og identifiserte risikoer, heller enn lovfestede detaljkrav (Heyerdal, 2022a, s. 7-11; Jore, 2015, s. 3-7).

En risikobasert tilnærming legger til rette for at den enkelte virksomhet kan utvikle fleksible sikkerhetsløsninger på bakgrunn av intern kunnskap om egne verdier, ressurser og sårbarheter, men stiller samtidig krav til forutgående risiko- og sårbarhetsvurderinger. I en praktisk risikohåndteringskontekst må virksomhetene dermed inneha den nødvendige faglige kompetansen for å skille mellom hvilke risikoer som kan aksepteres og hvilke som bør håndteres. For å kunne håndtere og forebygge aktuelle risikoer må risikokildene først identifiseres. Risikovurderingsprosessen tar utgangspunkt i en systematisk gjennomgang av potensielle risikoelementer og handler om å kartlegge relevante farekilder, samt analysere mulige skadevirkninger og sannsynligheten for at risikoene realiseres. Risikoidentifiseringen og risikoanalysen danner videre fundamentet for risikoevalueringen, hvor det sonderes rundt forebyggende og risikodempende tiltak (Renn, 2008, s. 68-70). Som sikkerhetsutfordring vil security-trusler imidlertid ikke kunne håndteres utelukkende gjennom mer treffsikre modeller,

nye data eller økt kunnskap, all den tid utfordringene som regel er forbundet med tverrsektorielle ansvarsområder, stor usikkerhet og lave sannsynlighetsestimater. Sett fra et helhetlig samfunnsperspektiv vil en balansert håndtering av security-trusler med andre ord inkludere både forbyggende tiltak med hensikt å forhindre, avverge og beskytte, men også resiliente virkemidler med hensikt å håndtere kriser, begrense konsekvenser og tilpasse systemene til nye rammebetingelser (Anholt & Boersma, 2018, s. 2-5).

Justis- og beredskapsdepartementet (2017, s. 30-32) definerer resiliens som samfunnets evne til å tåle og håndtere store hendelser, gjenopprette kritiske funksjoner og om nødvendig tilpasse seg til endrede forutsetninger. En resiliensbasert strategi åpner altså opp for at sikkerhetstruende hendelser vil forekomme, og fokuserer i større grad på å videreutvikle samfunnets proaktive respons- og tilpasningsevne. Følgelig kan resiliens forståes som kontinuerlige sykluser av fornyelse, vekst, omstrukturering og akkumulering i takt med at nye trusler oppstår og forhold forandres. Herunder skal utviklingen av organisatorisk resiliens bidra til at samfunnet etablerer løsninger for å absorbere sjokket fra uønskede hendelser, raskt gjenoppretter normaltilstand og samtidig tilpasser seg til endrede rammebetingelser (Anholt & Boersma, 2018, s. 2-3; Martin, 2019, s. 74-90).

3.2 – Kritisk infrastruktur og kritiske samfunnsfunksjoner

3.2.1 – Kritiske samfunnsfunksjoner

Samfunnskritiske funksjoner viser til de funksjonene som ivaretar befolkningens trygghetsfølelse og dekker samfunnets grunnleggende behov. Etter DSBs kriterier defineres samfunnsfunksjoner som kritiske dersom en svikt eller et bortfall i løpet av kort tid vil kunne resultere i følbare konsekvenser for befolkningen eller alvorlige ringvirkninger for samfunnet i sin helhet (DSB, 2016, s. 26-27). For å legge til rette for et fokusert og målrettet samfunnssikkerhetsarbeid har DBS i sin rapport fra 2016 – *Samfunnets kritiske funksjoner* utledet hvilke funksjoner som er kritiske for samfunnssikkerheten. KIKS (kritisk infrastruktur og kritiske samfunnsfunksjoner)-rapporten utgjør et overordnet styringsdokument for kategoriseringen av samfunnskritiske funksjoner og beskriver hvilken funksjonsevne det er nødvendig for samfunnet å opprettholde til enhver tid. Herunder er de ulike samfunnsfunksjonene brutt ned i følgende tre hovedkategorier på bakgrunn av hvordan et eventuelt bortfall vil virke inn på befolkningens grunnleggende behov:

- *Befolkningens sikkerhet* – Viser til de funksjoner som har en direkte betydning for samfunnets evne til å ivareta befolkningens grunnleggende sikkerhet, demokratiske rettigheter og vern mot fysisk skade (DSB, 2016, s. 28).

- *Styringsevne og suverenitet* – Viser til de funksjonene som utgjør elementære rammebetingelser for at øvrige samfunnsfunksjoner skal kunne ivaretas. Herunder evnen til å møte ekstraordinære situasjoner, sikre kontinuitet i styringsaktiviteter og opprettholdelse av styringsmessig og territoriell integritet (DSB, 2016, s. 28).

- *Samfunnets funksjonalitet* – Viser til de funksjoner som først og fremst har en indirekte betydning for samfunnets evne til å opprettholde befolkningens sikkerhet og grunnleggende trygghetsfølelse. Typisk vil dette være ulike typer av forsyningssystemer og infrastrukturbaserte tjenester hvor en svikt i funksjonsevnen vil kunne forårsake uro og bekymring i befolkningen (DSB, 2016, s. 28).

De tre hovedkategoriene er i KIKS-rapporten delt inn i fjorten kritiske samfunnsfunksjoner. Utefra de fjorten konkretiserte samfunnsfunksjonene er det videre utledet 40 underliggende «kapabiliteter» med tilhørende definert funksjonsevne som beskriver hvilke tjenester og leveranser som må opprettholdes til enhver tid for at samfunnets samlede behov skal ivaretas. I rapporten defineres en samfunnsfunksjon som kritisk dersom en svikt i den respektive samfunnsfunksjonen vil true *befolkningens trygghet* eller *samfunnets grunnleggende behov* i løpet av en periode på syv døgn. Tidsavgrensningen baserer seg på hvor lenge samfunnet kan fungere uten den respektive samfunnsfunksjonen før det går på bekostning av befolkningens elementære behov og trygghetsfølelse. Videre forutsettes det at landets beredskapsressurser blir utfordret og at uønskede hendelser inntreffer i løpet av den samme syvdagers-perioden. DSB begrunner tidsavgrensningen med at behovet for akutt beredskap og kontinuitetsplaner trolig vil være mindre i tilfeller hvor det tar mer enn syv dager før bortfallet får konsekvenser for befolkningens grunnleggende behov. I disse tilfellene vil samfunnet inneha et større handlingsrom og bedre tid til å etablere redundante løsningsalternativer (DSB, 2016, s. 26-29).

3.2.2 – Kritisk infrastruktur

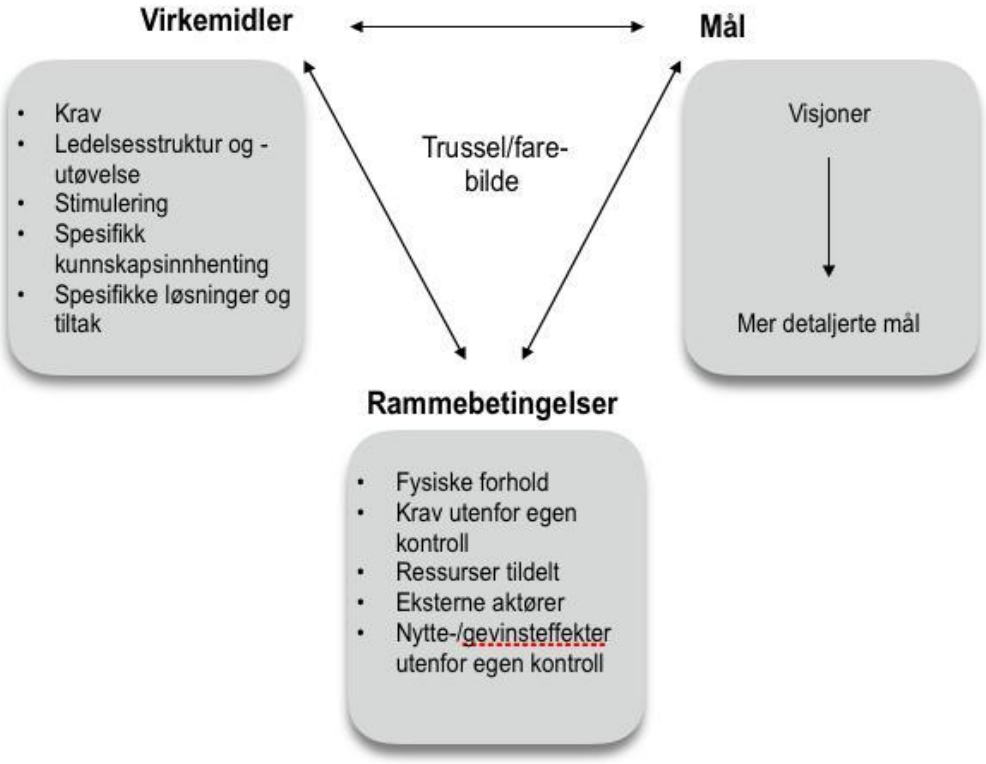
Kritiske infrastrukturer viser på sin side til de systemer og faste anlegg som er essensielle for at et samfunn skal fungere, og som ved en vedvarende svikt vil medføre at samfunnet ikke

lenger vil kunne opprettholde de leveranser av varer og tjenester som befolkningen behøver. Infrastrukturene har med andre ord en direkte nytteverdi for samfunnet og skal legge til rette for at de samfunnskritiske funksjonene opprettholder normal drift. Felles for de kritiske infrastrukturene er at en alvorlig svikt som regel vil ha en sektorovergripende karakter og raskt føre til massive forstyrrelser i samfunnet. Infrastrukturene innehar følgelig et bredt sårbarhetspotensial (NOU 2006:6, s. 31-34 & s. 139-140). Hvorvidt en infrastruktur anses som samfunnskritisk eller ikke vil blant annet bero på alternative løsninger ved en svikt, til hvilken grad infrastrukturen er tett koblet og de ulike samfunnsfunksjonenes sikkerhetskritiske avhengigheter til den aktuelle infrastrukturen (Njå et. al., 2021, s. 116-120).

Til forskjell fra systembegrepet viser infrastrukturer til det funksjonelle grunnlaget for en eller flere samfunnstjenester. Der et system i all hovedsak vil levere funksjonalitet og tjenester til innehaveren av systemet for egen anvendelse, vil en infrastruktur som regel inneha et bredt spekter av brukere fra husholdninger og enkeltindivider på den ene siden, til større private og offentlige virksomheter på den andre. En infrastruktur utgjør med andre ord et ledd i en kompleks verdikjede og viser til de sosiale strukturer, fysiske anlegg og tekniske systemer som er essensielle for å ivareta og opprettholde samfunnets kritiske funksjoner (Njå. et. al., 2021, s. 139-141; NOU 2006:6).

3.3 – Modell for sikkerhetsstyring

I *Samfunnssikkerhet: Analyse, styring og evaluering* introduserer Njå et. al (2021, s. 64-88) «systemperspektivet». Systemperspektivet viser til en grunnleggende modell for styring og studier av samfunnssikkerhetsfaglige systemer og er satt sammen av hovedelementene virkemidler, visjoner/mål og rammebetingelser. De tre hovedelementene utgjør til sammen selve «systemet» og vil virke gjensidig inn på hverandre. Herunder legger modellstrukturen til grunn at ethvert system har et eller flere formål med sin virksomhet. For å nå de definerte målsetningene vil systemeierne benytte seg av relevante virkemidler og iverksette formålstjenlige tiltak. Både målsetningene og virkemidlene utformes imidlertid på bakgrunn av rammebetingelsene systemet opererer under. Videre forutsetter modellen at det alltid vil eksistere en forestilling om usikkerheter, farer og trusler internt i systemet som vil virke inn på forståelsen av de tre øvrige hovedelementene. Modellen er følgelig anvendelig i komplekse systemer med tidvis konflikterende mål hvor rammebetingelsene kan bidra til å komplisere sikkerhetsarbeidet ytterligere (Njå et. al, 2021, s. 64-76).



Figur 2*: Modell for sikkerhetsstyring (Njå et. al., 2021, s. 67)*

For å kartlegge hvordan sikkerhetsarbeidet rundt norsk kraftforsyning påvirkes av samfunnsdigitaliseringen vil det være å hensiktsmessig å anvende seg av systemperspektivet for å bryte kraftsystemet ned i ulike hovedelementer. På denne måten får man vurdert norsk kraftforsyning som et helhetlig system. Ved å identifisere de overordnede målsetningene for sikkerhetsarbeidet vil relevante suksesskriterier kunne defineres og presise sikkerhetsmål etableres. Videre vil man kunne kartlegge og beskrive rammebetingelsene kraftforsyningen opererer under. Rammebetingelsene vil videre virke inn på utformingen av potensielle sikkerhetstiltak og kan eksempelvis bestå av geopolitiske faktorer eller lovfestede sikkerhetskrav utenfor NVEs kontroll. For å identifisere tiltak som kan bidra til å redusere kartlagte sårbarhetsflater ved norsk kraftforsyningen som system må det imidlertid spesifiseres noen krav til involverte virksomheters sikkerhetsstyring. Kravene bør baseres på rammebetingelsene systemet opererer under og de definerte sikkerhetsmålsetningene for kraftforsyningen som kritisk samfunnsfunksjon. Sluttelig vil man kunne utvikle funksjons- og ytelseskrav til systemet basert på de ulike systemelementene og det samlede trusselbildet (Njå et. al, 2021, s. 64-76).

3.3.1 – Sikkerhetsstyring

Sikkerhetsstyringen av et definert system eller en virksomhet viser til alle de tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med etablerte målsetninger. Følgelig utgjør sikkerhetsstyring en kontinuerlig aktivitet som foregår i alt av prosjekterings- og planleggingsarbeid. Med utgangspunkt i modellen for sikkerhetsstyring vil de sentrale trinnene i en sikkerhetsstyringsprosess være å kartlegge aktuelle rammebetingelser, utvikle relevante sikkerhetsmål og finne frem til løsninger, tiltak og virkemidler tilpasset rammebetingelsene som best mulig fremmer de etablerte sikkerhetsmålsetningene. Rammebetingelsene vil naturligvis variere fra system til system, men kan typisk bestå av sosiale føringer, miljøbetingelser, lokale og internasjonale forhold, lovverk og andre forutsetninger som analyseobjektet har begrenset eller ingen innflytelse over (Njå et al., 2021, s. 121-124).

Det overordnede formålet med alt samfunnssikkerhetsarbeid vil være å sikre at samfunnets kritiske funksjoner ivaretas for å sikre borgernes liv, helse og grunnleggende behov.
Med utgangspunkt i et systems visjoner og rammebetingelser vil man kunne utforme funksjonelle krav til sikkerheten som videre danner grunnlaget for å utvikle relevante løsningsforslag og virkemidler (Njå et.al., 2021, s. 63-68). Sett under ett vil det primære formålet med hele sikkerhetsstyringsprosessen være å etablere metoder og prinsipper for hensiktsmessig styring av risiko, sikkerhet og beredskap, samt begrense faren for tap, ulykker og sikkerhetstruende hendelser (Njå et al., 2021, s. 119-124).

Fra et teoretisk perspektiv kan sikkerhetsstyringsprosessen brytes ned i seks ulike faser. Innledningsvis gjennomføres en situasjonsanalyse hvor analyseobjektet og potensielle problemstillinger beskrives grundig. Basert på premisset om hva som er sikkert nok utformes videre interne målsetninger og sikkerhetskrav. Med utgangspunkt i de definerte sikkerhetsmålene videreutvikles løsningsforslag som kan bidra til å oppnå og tilfredsstille de fastsatte målsetningene. Deretter må de ulike løsningsforslagene analyseres. Basert på analysen besluttes implementeringen av de best egnede virkemidlene og løsningsforslagene. Avslutningsvis evalueres den valgte løsningen på bakgrunn av forhåndsdefinerte sikkerhetskriterier (Njå et al., 2021, s. 119-126).

3.3.2 – Høypålitelige organisasjoner (HRO)

Innenfor sikkerhetsstyringen av virksomheter og systemer har teorien om høypålitelige organisasjoner (High reliability organizations-teorien) stått sentralt. Teorien tar utgangspunkt i at uønskede hendelser i høyteknologiske systemer kan forebygges gjennom god planlegging og har en optimistisk tilnærming til sikkerhetsstyringen som konsept. For å kunne defineres som en høypålitelig organisasjon stiller systemteorien imidlertid krav til visse organisatoriske betingelser, herunder en integrert pålitelighetskultur, høy ytelse, bred teknologisk kompetanse, fleksible lederstrukturer under kriser og kontinuerlig driftskontroll. Til tross for ulike upålitelige enkeltkomponenter legger HRO-teorien til grunn at virksomheter kan utvikle pålitelige systemer gjennom et organisasjonsdesign som vektlegger sterk organisasjonskultur, fokus på kontinuerlig læring og desentralisert ledelse. Samtidig forutsetter HRO-teoriene at pålitelighet og sikkerhet gis høyeste prioritet og at upålitelige enkeltkomponenter beskyttes gjennom overlapp, redundans og barrierer (Roe & Schoulman, 2008, s. 53-56).

Den fleksible tilpasningsevnen skal legge til rette for at organisasjonene opprettholder et nødvendig sikkerhetsnivå også ved uforutsette hendelser, og ikke viker fra sine grunnleggende sikkerhetsprinsipper (Njå et al., 2021, s. 113-117). Gjennom en kultur som identifiserer latente sårbarheter og åpner for organisatorisk læring skal en høypålitelig organisasjon bruke erfaringer og nestenulykker til å gjenkjenne hva som i fremtiden kan føre til skadelige «kjernehendelser». Evnen til å utvikle gjeldende rutiner og tilpasse seg uforutsette hendelser skal samtidig bidra til å bygge en organisatorisk resiliens i møte med sikkerhetstruende hendelser. En resiliensbasert tilnærming skal videre bidra til å proaktivt forebygge «kjernehendelser» og bygge opp under en robust tilpasningsevne i møte med endrede rammevilkår (Engen et al., 2021, s. 170-173; Roe & Schulman, 2008, s. 53-59).

3.3.3 – Normal Accident-teorien (NAT)

Som en motpol til teorien om høypålitelige organisasjoner presenterte den amerikanske sosiologen Charles Perrow (1999, s. 3-5) teorien om «normale ulykker». Perrows systemteorier legger til grunn at antallet høyrisikoutfordringer øker i takt med at systemer utvikles og blir mer komplekse. Herunder underbygger Perrow systemteoriene ved å anføre at enkelte systemer er såpass utsatt for fare at sikkerhetstruende hendelser og ulykker ikke bare er uunngåelig, men også bør ansees som normalt til tross for en veldrevet sikkerhetsstyring. Teorien om normale ulykker kan dermed sies å representere en pessimistisk motsetning til

HRO-teorien og tar utgangspunkt i et deterministisk perspektiv på sikkerhetsstyring som konsept (Perrow, 1999, s. 3-8).

I henhold til Perrows (1999) systemteori karakteriseres et system som komplekst dersom interaksjonene i systemet foregår i ukjente eller uventede sekvenser, som enten er ikke-synlige eller krevende å forstå. Kompleksiteten i systemet vil ofte gjøre det utfordrende å forstå og forutse hvordan et system vil yte under ulike forhold. I tråd med systemteorien bør systemene dermed forståes som helhet, heller enn å brytes ned og reduseres til enkeltkomponenter. Et komplekst system kan likevel betraktes som et hierarki av ulike organisatoriske nivåer, der hvert nivå vil være mer komplekst enn nivået under. Herunder deler Perrow komplekse systemer inn i følgende fire nivåer: system, subsystem, enhet og del. I den fysiske verden – eksempelvis i et produksjonssystem – viser de ulike nivåene vanligvis til ulike former for fysiske deler. Nivåene kan imidlertid også inneha en overføringsverdi til digitale systemer (Perrow, 1999, s. 76-79).

Sikkerhetstruende hendelser som skyldes en kombinasjon av uforutsette og sammensatte feil vil defineres som systemulykker. Kompleksiteten i systemene vil følgelig gjøre uønskede hendelser og de tilhørende ringvirkningene langt mer utfordrende å predikere og forhindre. Samtidig vektlegger Perrow at risikoen for høyrisikoutfordringer øker i tett koblede systemer med komplekse interaksjoner. Tett koblede systemer beskrives som uoversiktlige i sin natur kjennetegnet av stor tidsavhengighet, ufravikelige sekvenser, prosesser som vanskelig eller i begrenset grad kan stoppes og liten mulighet til improvisering. Videre vil en feil raskt kunne forplante seg og det vil være vanskelig å identifisere aktuelle feilkilder innad i systemet. Begrepet «normale ulykker» henviser i den forbindelse til den uunngåelige restrisikoen som eksisterer i virksomheter som opererer med komplekse systemer (Perrow, 1999, s. 70-80).

Sluttelig understreker Perrow at de fleste virksomheter i hovedsak vil være avhengig av produksjon og profitt for ikke å gå konkurs. Kostbare sikkerhetstiltak vil i mange tilfeller utgjøre en betydelig utgift som ikke nødvendigvis harmonerer med private organisasjoners målsetning om profittmaksimering. Dermed vil produksjonen i mange tilfeller prioriteres over sikkerheten, og sikkerhet vil med andre ord være langt fra det eneste fokusområdet for ledelsen i en bedrift eller en samfunnsvirksomhet. På generelt grunnlag anførte Perrow at majoriteten av operatørene ved et system eller i en virksomhet derfor vil være dårligere trent i sikkerhetsprosedyrer enn rendyrkede produksjonsprosesser (Perrow, 1999, s. 2-6).

3.3.4 – Sikkerhetskultur og sikkerhetsarbeid

Begrepet sikkerhetskultur er rettet mot organisasjoners evne til å styre egen sikkerhet. Forenklet beskrives ofte en virksomhets sikkerhetskultur som «måten vi gjør ting på her» og viser til summen av de ansattes motivasjon, kunnskap, atferd og holdninger, som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd (Burke and Litwin, 1992, s. 523-530). Herunder refererer en kultur til noe som skapes og deles innad i en gruppe av individer. Ifølge Besnard et al. (2018, s. 27-29) karakteriseres en god sikkerhetskultur av en virksomhets evne til å identifisere utfordringer som oppstår i grensesnittet mellom ulike avdelinger og evnen å samhandle på tvers av fagområder. Spesielt gjør dette seg gjeldende ved utformingen av sikkerhetsbarrierer, tilbakemeldinger om operasjonelle erfaringer, analyse og håndtering av informasjon og utvikling av oppfølgingstiltak i etterkant av hendelser og «nestenulykker». Herunder kjennetegnes en god sikkerhetskultur av effektiv koordinering, kommunikasjon, kunnskapsdeling og samhandling mellom ulike sikkerhetsavdelinger og en helhetlig organisatorisk forståelse for virksomhetens sikkerhetsarbeid.

Det systematiske arbeidet med sikkerhet og beredskap i en virksomhet omfatter blant annet:
- Forebygging og tiltak for å redusere muligheten for sikkerhetstruende hendelser
- Beredskap og tiltak som skal styrke muligheten til å håndtere sikkerhetstruende hendelser
- Beredskapsplaner med tiltakskort
- Krisehåndtering og bruk av planlagte verktøy når sikkerhetstruende hendelser inntreffer
- Evnen til gjenoppretting av normalsituasjonen.
- Rollebeskrivelser og samvirke
- Læring, evaluering og gjennomgang av uønskede og sikkerhetstruende hendelser (Besnard, Boissières, Daniellou, & Villena, 2018, s. 27-40).

3.4 – Funksjons- og ytelseskrav

Sett fra et samfunnssikkerhetsperspektiv ønsker man i utgangspunktet at risikoer knyttet til virksomheter og aktiviteter begrenses til *akseptabelt* nivå. Hva som utgjør et *akseptabelt* risikonivå vil imidlertid variere fra system til system avhengig av type virksomhet, formålet med virksomheten, i hvilken sammenheng virksomheten foregår og hvem som utfører virksomheten (Njå et al., 2021, s. 207-210). Basert på fastsatte akseptkriterier vil en virksomhet videre kunne utvikles funksjons- og ytelseskrav til systemene som analyseres. Ved vurderingen av ulike løsningsalternativer og behovet for sikkerhetstiltak vil funksjons- og ytelseskravene utgjøre et egnet referansegrunnlag. Samtidig bør også andre parametere

som effekt, kostnad og nytteverdi naturligvis inkluderes i vurderingen. Kostnad-nytte-vurderingen benyttes for å synliggjøre mulige effekter ved en aktivitet eller et tiltak og må sees i sammenheng med tiltakets kostander og sideeffekter. Herunder kan aktuelle vurderingsmomenter i helhetsvurderingen blant annet være trygghet, økonomisk kostnadsnivå, risikoprofil eller mediefokus (Njå et al., 2021, s. 211-215).

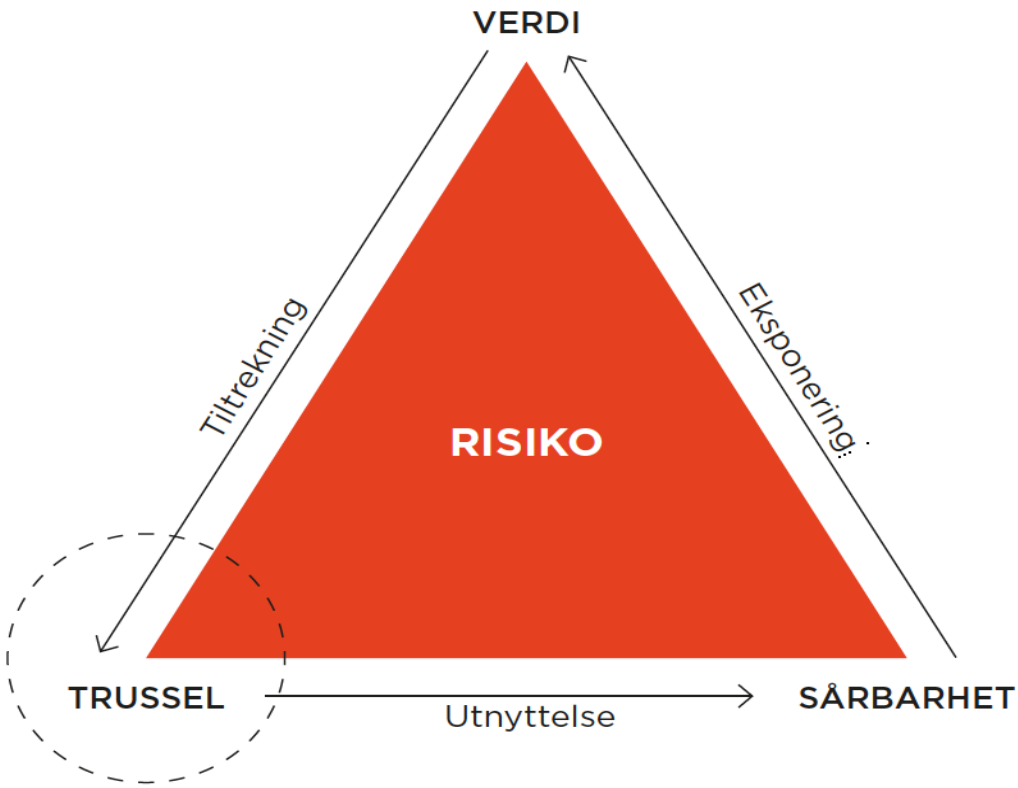
I pensumlitteraturen viser funksjons- og ytelseskrav til definerte krav for beredskapsressursene som skal respondere på potensielle sikkerhetstruende hendelser. Med utgangspunkt i utførte beredskapsanalyser og de overordne målsetningene for beredskapen vil man kunne utvikle funksjonskrav til håndteringen av definerte beredskapssituasjoner som må innfris for å oppnå en tilfredsstillende beredskap på et område. En ytelse viser videre til en konkretisering av innsatsen som skal til for å innfri et fastsatt funksjonskrav. Ytelseskravene utgjør følgelig de nødvendige prestasjonskravene beredskapsressursene som skal respondere på hendelsene må forholde seg til for å kunne håndtere hendelsene på et akseptabelt nivå (Eriksen, Rake & Sommer, 2018, s. 3-8; Njå et al., 2021, s. 211-215).

3.5 – VTS-modellen

All den tid et cyberangrep, en sabotasjeaksjon eller en sikkerhetspolitisk krise vil forutsette en kalkulerende og rasjonell motpart, vil man i større grad stå ovenfor karakteristiske security-risikoer i møte med sikkerhetsutfordringene som følger i kjølvannet av dagens sikkerhetspolitiske spenninger. Heller enn å forholde seg til en klassisk kvantitativ risikomodell hvor det vurderes farer det ikke kan knyttes forsett til, vil man i møte med security-risikoer i større utstrekning ta utgangpunkt i en kvalitativ trefaktor-modell. Her vurderes og analyseres størrelsene sårbarhet, verdi og trussel heller enn fremtid, hendelser og konsekvenser. Handlingene som vurderes kan i prinsippet strekke seg over et vidtrekkende kontinuum fra mindre hærverk på den ene siden til komplekse cyberangrep og omfattende sabotasjeaksjoner på den andre (Engen et. al., 2021, s. 102-103).

Det totale risikobildet illustreres gjerne ved VTS-modellen basert på veiledere fra Politiets sikkerhetstjeneste, Norsk Standard 5832 og Nasjonal sikkerhetsmyndighet. Her viser trusselbegrepet til de relevante farekategoriene og baseres på den eller de aktuelle trusselaktørenes intensjon, kapasitet og tilstedeværelse. Verdibegrepet innebefatter det aktuelle systemet som skal beskyttes, mens sårbarhetsbegrepet viser til den evnen systemet har til å forsvare seg mot ulike former for trusler og til hvilken grad systemet vil kunne

utsettes for en ekstraordinær situasjon og fremdeles opprettholde normal drift. Samlet sett utgjør de tre dimensjonene hvert sitt punkt i en risikotrekant og det totale risikobildet synliggjøres gjerne ved risikotrekantens samlede areal. Satt sammen skal de tre størrelsene bidra til en samlet vurdering av risikoen og illustrere sammenhengen mellom sannsynlighet og konsekvenser. Videre vil de ulike størrelsene virke gjensidig inn på hverandre og må dermed sees i sammenheng. Ved å fjerne eller begrense en av størrelsene, for eksempel ved å inkapasitere sentrale trusselaktører, vil den samlede risikoen reduseres tilsvarende. Det overordne formålet med sikkerhetsarbeidet vil naturligvis være å redusere arealet på risikotrekanten mest mulig. Dersom trusselen elimineres vil også den samlede risikoen opphøre (Heyerdahl, 2022b, s. 252-261; Standard Norge, 2014). Figuren under viser risikotrekanten slik den blir presentert i Politiet sikkerhetstjenestes (PST) nasjonale trusselvurdering.



Figur 3: *Viser risikotrekanten slik den er presentert i PSTs nasjonale trusselvurdering for 2023 (PST, 2023, s. 3)*

Sett i sammenheng med oppgavens tema og problemstilling vil VTS-modellen kunne benyttes for å analysere potensielle sårbarheter ved norsk kraftforsyning på bakgrunn av

samfunnsdigitaliseringen og dagens sikkerhetspolitiske uroligheter. All den tid den geopolitiske konteksten åpner opp for et bredere trusselbilde, vil man kunne legge til grunn at norsk kraftforsyningen kommer til å stå ovenfor et mer komplekst trusselbilde i møte med endringene i den sikkerhetspolitiske situasjonen. Herunder er det nærliggende å forutsette at samfunnet i større grad må belage seg på å stilles ovenfor rasjonelle og målrettede aktører i takt med økt etterretningsvirksomhet og den voksende internasjonale konfliktflaten. Følgelig bør også sikkerhetsstyringen basere seg på andre prinsipper enn stilt ovenfor mer tradisjonelle safety-risikoer som naturhendelser, ekstremvær og menneskelig svikt. Særlig siden en rasjonell og dynamisk trusselaktør vil kunne tilpasse seg iverksatte sikkerhetstiltak og handle deretter. Evnen til planlegging og målrettede angrep gjør følgelig risikohåndteringen og sikkerhetsstyringen til en langt mer utfordrende oppgave. Risikobildet vil samtidig være retningsgivende for hvilke sikringstiltak som bør vurderes og implementeres (Engen et al., 2021, s. 101-103).

3.6 – Barrierer og sikkerhetstiltak - The Swiss cheese model of defences

Kraftforsyningens overordnede målsetning er å ivareta samfunnets behov for elektrisk energi. Som ansvarlig forvalter skal NVE arbeide for en robust kraftforsyning med stabile kraftleveranser, også ved kriser og under ekstraordinære situasjoner. Målsetningene sikres i tråd med klassisk samfunnssikkerhetsarbeid gjennom sikkerhetstiltak og barrierer av både konsekvens- og sannsynlighetsreduserende karakter (DSB, 2016, s. 86-89). James Reason (1997) introduserte på slutten av 90-tallet en modell for å illustrere forekomsten av latente sårbarheter i et dybdeforsvar. Formålet med modellen er å synliggjøre de sikkerhetstiltak og barrierer som står mellom verdiene virksomheten ønsker å beskytte og de identifiserte truslene. Med barrierer henviser Reason til de mekanismer, hindringer og sikkerhetstiltak som skal bidra til å beskytte verdiene fra både menneskeskapte trusler og naturlige farer.

Herunder presiserer Reason (1997, s. 6-8) at alle barrierer er utformet for å ivareta en eller flere av følgende sju funksjoner:

- *Utvikle bevissthet og skape forståelse rundt potensielle risikoer og lokale farer*
- *Skape sikkerhetsbarrierer mellom verdiene man ønsker å beskytte og potensielle trusler*
- *Veilede om sikker bruk og håndtering*
- *Advare og alarmere når fare er overhengende*
- *Gjenopprette normal og sikker tilstand ved ekstraordinære situasjoner*
- *Begrense konsekvensene ved eventuelle trusler som unnslipper barrierene*

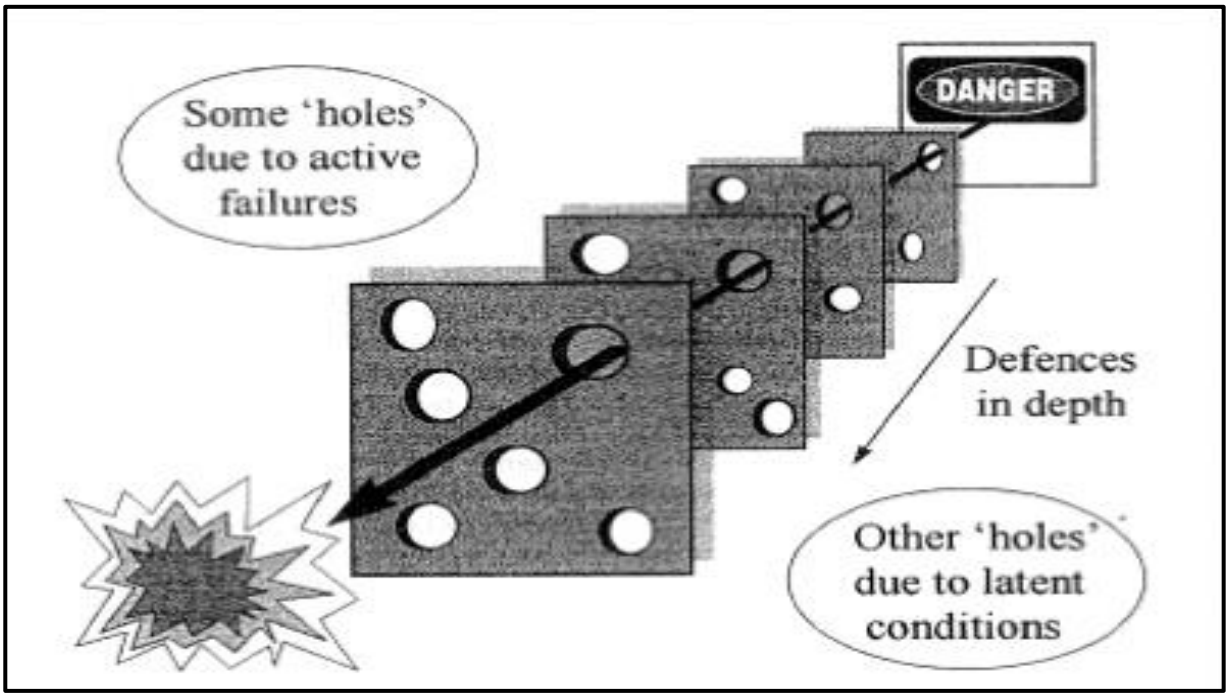
- Fungere som rednings- eller rømningsmidler

Reason tydeliggjør at det er mangfoldet av de ulike barrierene som i dybden danner sikkerhetssystemer som skal forebygge kriser, beskytte mot sikkerhetstruende hendelser og immunisere systemene mot menneskelige enkeltfeil. De ulike barrierene kan videre kategoriseres inn i to former for underkategorier, henholdsvis «harde» og «myke» barrierer. En myk barriere refererer til en kombinasjon av mennesker og lovgivning, herunder regler og prosedyrer, administrative kontroller, opplæring, regulatorisk overvåking, sertifisering, øvelser, tilsyn, kritiske frontlinjeoperatører og lisensiering. «Harde» barrierer viser på den andre siden til tekniske enheter som fysiske barrierer, ikke-destruktive tester, nøkler, automatiserte sikkerhetsfunksjoner, forbedret systemdesign, personlig verneutstyr og alarmer og varslere (Reason, 1997, s. 6-10).

I en ideell verden påpeker Reason at samtlige barrierer vil fungere feilfritt. I virkeligheten vil hvert sikkerhetstiltak imidlertid inneha en rekke underliggende feil og latente sårbarheter. I *The Swiss cheese model of defences* refererer Reason til de latente svakhetene som «sikkerhetshull». Modellen illustrertes ved at hver barriere representeres gjennom en plate. Platene står oppstilt etter hverandre og utgjør samlet sett «dybdeforsvaret». Ideelt vil alle barrierer og sikkerhetstiltak fungere adekvat, slik at ingen trusler kan penetrere seg gjennom det samlede «dybdeforsvaret». I realiteten innehar barrierene imidlertid flere sikkerhetshull og Reason beskriver følgelig platene som «sveitsiske osteskiver» stilt etter hverandre. Platene innehar dynamiske hull som vil forsvinne, oppstå, bevege seg, vokse eller krympe alt etter hvordan ulike lokale forhold håndteres. En organisatorisk ulykke forutsetter en kombinasjon av sikkerhetshull i de ulike barrierene. I Reasons modell illustreres dette ved at sikkerhetshullene korresponderer og danner en tunnel frem til verdiene virksomheten ønsker å beskytte. Kombinasjonen av aktive og latente feil kan dermed forårsake en delvis eller total penetrasjon av systemets dybdeforsvar (Reason, 1997, s. 5-13).

Sikkerhetstruende hendelser og ekstraordinære situasjoner vil som regel utløses av aktive feil begått av frontlinjeoperatører i den «skarpe enden» av virksomheten. Når det er sagt strekker den moderne forståelsen av komplekse ulykkeskjeder seg lenger enn menneskelige feil begått av enkeltindivider. I høyteknologiske systemer foreligger det bred konsensus om at forklaringsmodellene også må ta høyde for underliggende sårbarheter og latente forhold. I den forbindelse viser latente forhold til feil og svakheter som får utvikle seg i dybdeforsvarets

ulike lag av barrierer over tid. Eksempelvis gjennom manglende tilsyn, upresis opplæring, vedlikeholdsmangel eller utilstrekkelig utstyr. De latente svakhetene vil kunne eksistere uoppdaget i systemet i flere år, før de i kombinasjon med lokale forhold og aktive feil vil trenge gjennom et systems ulike barrierer. Latente svakheter vil samtidig øke sannsynligheten for menneskelige feil gjennom en forsterkning av lokale faktorer som fremmer brudd på optimal praksis (Reason, 1997, s. 8-12).



Figur 4: *Viser «The Swiss cheese model of defences» slik modellen er illustrert i «Managing the risks of organizational accidents» (Reason, 1997, s. 12)*

Sett i sammenheng med norsk kraftforsyning vil sårbarheter oppstå der underliggende feil og latente svakheter får utvikle seg ubemerket i dybdeforsvaret av barrierer og sikkerhetstiltak. På denne måten legges forholdene til rette for en uønsket hendelse eller en svikt i leveransesikkerheten. All den tid ulykker i høyteknologiske organisasjoner ofte vil kunne spores langt tilbake i systemet og som regel skyldes flere svikter i mangfoldet av sikkerhetstiltak blir personorienterte forklaringsmodeller i de fleste tilfeller utilstrekkelige. Den menneskelige tilstanden kan ikke endres, men de lokale forholdene vil på andre siden kunne påvirkes gjennom en bredere forståelse av organisatoriske ulykkers og sikkerhetstruende hendelsers grunnleggende natur (Reason, 1997, s. 11-15).

3.7 – Digitalisering, digitale verdikjeder og cyber-fysiske systemer

Cyber-fysiske systemer defineres som nettverk av samvirkende elementer med fysisk input og output i stedet for frittstående enheter og viser til de systemer som kombinerer fysiske- og digitale datakomponenter. Systemene er som regel tett koblede og blir stadig mer nærværende i dagens digitale samfunn. Wolf og Serpanos (2018, s. 3-11) understreker at cyber-fysiske systemer i dag er godt integrert og oppfattes som en essensiell forutsetning for opprettholdelsen av en rekke vitale samfunnsfunksjoner som industrien, den elektroniske kommunikasjonen, helsevesenet og kraftforsyningen. Herunder bidrar cyber-fysiske systemer til at ulike enheter integrerer cyber-fysiske løsninger for å øke den miljømessige og økonomiske effektiviteten. Sett i sammenheng med samtidsfenomenet Internet of Things (IoT), som refererer til hvordan fysiske enheter kobles opp mot det virtuelle og kommuniserer gjennom skyplattformer og sensornettverk, viser cyber-fysiske systemer i sin mest trivielle form til relativt enkle forbrukerenheter som droner, varmeovner og støvsugere. På den andre siden av spekteret løftes større infrastrukturer og «smarte byer» frem som tett koplede og svært komplekse cyber-fysiske systemer. Gjennom integrerte teknologiske løsninger legger enhetene til rette for at digitale systemer og datakomponenter gir fysiske utslag uten at menneskelig involvering er nødvendig (US. Department of Homeland Security, 2015, s. 6-9). Herunder fremhever NVE (2021) viktigheten av cyber-fysiske systemer og integrerte IKT-løsninger for styringen av kraftforsyningen og den generelle driftskontrollen i sin rapport om IKT-sikkerhetstilstanden i kraftforsyningen.

På den andre siden påpeker både Nasjonal sikkerhetsmyndighet (NSM), som er nasjonalt fagorgan for forebyggende sikkerhet, og DSB i sine rapporter *Risiko 2023 – Økt uforutsigbarhet krever høyere beredskap* og *Risikostyring i digitale verdikjeder* (2020) at det åpnes for en langt bredere sårbarhetsflate i kjølvannet av den digitale samfunnsutviklingen. I takt med at cyber-fysiske systemer stadig integreres i en rekke ulike samfunnsfunksjoner viskes skillet mellom den fysiske og digitale verden ut og ringvirkningene av sikkerhetstruende hendelser vil samtidig øke i omfang og kompleksitet. Både for den enkelte virksomhet, men også for tilhørende virksomheter knyttet sammen i et nettverk av verdikjeder. Herunder fremhever US. Department of Homeland Security (2015, s. 2) at de cyber-fysiske systemene vil havne i skjæringspunktet mellom ondsinnede security-risikoer og mer tradisjonelle safety-risikoer. Crossover-effektene og de komplekse gjensidige avhengighetene kan på denne måten introdusere nye og uventede sårbarhetsflater.

Til forskjell fra tidligere vil dermed fysiske og digitale trusler i større grad virke inn på hverandres domener. For eksempel ved at målrettede cyberangrep som slår ut de digitale driftssystemene, samtidig vil kunne slå ut den fysiske elforsyningen og på denne måten forårsake fysiske funksjonsfeil. Motsatt vil også en naturulykke som slår ut den fysiske kraftforsyningen, samtidig kunne føre til en svikt i de digitale tjenestene som drifter strømfordelingen. Den nye risikoen som oppstår ved utvikling og bruk av cyber-fysiske systemer ligger dermed i skjæringspunktet mellom domenene safety- og security- risikoer. Den gjensidige påvirkningen åpner videre for ringvirkninger det kan være svært krevende å se rekkevidden av, både for den enkelte virksomhet, men også for storsamfunnet i sin helhet (Wolf & Serpanos, 2018, s. 3-11).

3.7.1 – Silotenking og risikopersepsjon

I samfunnssikkerhetsarbeidet er safety- og security-risikoer to områder som tradisjonelt sett har blitt behandlet separat. Segregeringen medfører dermed en risiko for at de ulike fagområdene utvikler en form for silotenking som går på bekostning av effektiv kommunikasjon og helhetlig samhandling. Faren er at den enkelte enhet blir for fokusert på egne målsetninger uten å ta hensyn til systemet som helhet og at de ulike fagområdene mister et overordnet perspektiv på sikkerhetsstyringen av virksomheten. Digitalisering og økt cyber-fysisk konvergens krever dermed at organisasjonene ser forbi tradisjonelle skillelinjer mellom ulike avdelinger og ulike risikostyringstradisjoner. Det kulturelle, utdannings- og erfaringsmessige skillet mellom ulike enheter kan på denne måten komplisere evnen til effektiv samhandling og føre til en form for silotenking der den enkelte enhet kun jobber etter egne sektorielle målsetninger. Dersom de enkelte avdelingene i en organisasjon blir for opptatt av egne oppgaver, slik at det går på bekostning av organisasjonen som helhet, kan det resultere i en suboptimaliserende effekt (Gould og Bieder, 2020, s. 2-7).

Tradisjonelt sett har fysiske farer imidlertid skapt større frykt i befolkningen enn rendyrkede digitale risikoer. Dette henger sammen med klassiske faktorer innenfor risikopersepsjon og skyldes at folk flest vurderer farer utefra om risikoen er kjent eller ukjent og til hvilken grad trusselen assosieres med frykt. I motsetning til brutale terroranslag med fremtredende og håndgripelige konsekvenser oppfattes ofte konsekvensene ved digitale tilslag som tvetydige og uklare. Som et resultat av manglende kunnskap og forståelse vies derfor de digitale trusselagentene ofte mindre oppmerksomhet enn mer håndfaste, fysiske farer i samfunnssikkerhetsarbeidet. Et redusert fokus kan videre føre til et lavere engasjement rundt

de digitale risikoene og følgelig et svekket digitalt sikkerhetsarbeid (Njå. et. al, 2021, s. 44-46).

3.7.2 – Verdikjeder

En klassisk verdikjede beskriver verdiskapningen i en bedrift fra strategisk nivå og følger flyten av kunder, varer, og andre aktiviteter gjennom hele den verdiskapende prosessen. I dagens internasjonaliserte samfunn er det vanlig at de fleste bedrifter har utviklet avhengigheter til ulike typer av leverandører og underleverandører. Særegent for digitale verdikjeder, som har blitt stadig mer utbredt i takt med den teknologiske utviklingen, er at en svikt et sted i verdikjeden har en tendens til å spre seg momentant og tidvis på uforutsigbare måter. I hovedsak skyldes dette at tjenestene som inngår i de digitale verdikjedene ofte er av sektorovergripende karakter og er underlagt ulikeartede regelverk og tilsynsregimer. For utviklere på toppen er det dermed svært utfordrende å etablere oversikt over hvilke sårbarheter tjenestene er eksponert for på et dypere nivå i verdikjeden (DSB, 2020, s. 11-16).

Sårbarheten ved et system vil blant annet bero på graden av avhengighet mellom de ulike leddene i verdikjedene systemet bygger på. Komplekse systemer preget av tette koblinger med mange involverte aktører og et fragmentert systemansvar vil gjøre det vanskeligere å identifisere og håndtere potensielle kilder til feil. Som følge av de digitale verdikjedenes kompleksitet og den momentane propageringen av feil vil verdikjedene dermed kunne utfordre og komplisere virksomhetenes sikkerhetsstyring. Videre vil forsyningskjedenes transnasjonale karakter innebære at ulike deler av kjeden ofte er underlagt ulike staters jurisdiksjoner og tilsynsvirksomhet. Følgelig vil norske myndigheter kun i begrenset grad ha oversikt og kontroll over sikkerhetshullene ved de ulike leverandørkjedene (DSB, 2020, s. 11-12).

Til tross for flere alternative underleverandører og en forestilling om redundans, har det i flere tilfeller vist seg at visse leverandører har en tendens til befinne seg i bunnen av en rekke ulike forsyningskjeder. Følgelig vil et bortfall i den underliggende tjenesten kunne få uforutsigbare og potensielt massive ringvirkninger for verdikjeden i sin helhet. I dagens internasjonaliserte og høyteknologiske samfunn er det i utgangspunktet ingen land, virksomheter eller samfunnssektorer som kan styre eller kontrollere sin digitale sårbarhet på egenhånd. I takt med at systemene blir stadig mer komplekse og verdikjedene uoversiktlige blir det dermed vanskeligere for beslutningstakere å ivareta en helhetlig oversikt over leveransekjedenes

sårbarheter. Til en viss grad vil alle systemer dermed «arve» digitale sårbarheter fra andre sektorer og deres «underleverandører» til tross god sikkerhetsstyring i eget system (DSB, 2020, s. 11-16).

3.8 – Oppsummering av teori

Sett i lys av oppgavens kontekst er det nærliggende å legge til grunn at de nye truslene som oppstår i skjæringsfeltet mellom samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen vil inneha en malisiøs og målrettet karakter. I tråd med tradisjonelt samfunnssikkerhetsarbeid vil det følgelig være hensiktsmessig å trekke en teoretisk skillelinje mellom safety- og security-risikoer mot norsk kraftsektor. Slik vil man i større grad evne å etablere en forståelse for truslenes dynamiske natur og underliggende karakteristikker. Samtidig vil en grovkategorisering bidra til å forenkle det videre analysearbeidet og danne bakteppet for oppgavens overordnede risikoperspektiv (Jore, 2019a).

For å kartlegge hvordan sikkerheten rundt kraftforsyningen påvirkes av samfunnsdigitaliseringen vil det videre være hensiktsmessig å trekke paralleller mellom kraftforsyningen og DSBs (2016) kriterier for kritiske samfunnsfunksjoner. På denne måten vil man etablere et rammeverk for å belyse ringvirkningene ved en potensiell svikt i leveransesikkerheten, de sikkerhetskritiske avhengighetene mellom ulike samfunnsfunksjoner og samtidig understreke betydningen av en funksjonell og pålitelig kraftforsyning. Videre vil systemperspektivet (Njå et. al., 2021) bestående av visjoner, sikkerhetstiltak og rammebetingelser tjene som et hensiktsmessig analyseverktøy for å bryte kraftsystemet ned i ulike hovedelementer. Blant annet for å belyse hvordan den digitale utviklingen vil påvirke ulike sider ved sikkerhetsstyringsprosessen og etablere en helhetlig forståelse for sårbarhetsflatene som følger i kjølvannet av endrede rammebetingelser. Samtidig vil man kunne trekke inn relevante aspekter fra sentrale systemteorier som NAT- og HRO-teoriene for å underbygge hvilke mekanismer som – sett i lys av samfunnsdigitaliseringen og dagens sikkerhetspolitiske situasjon – vil virke inn på og potensielt true opprettholdelsen av leveransesikkerheten.

All den tid sikkerhetsutfordringene som følger i kjølvannet av dagens geopolitiske uroligheter i hovedsak forutsetter en kalkulerende og rasjonell motpart vil man i større grad ta utgangpunkt i en kvalitativ trefaktor-modell ved den samlede risikovurderingen. Her analyseres og vurderes størrelsene sårbarhet, verdi og trussel heller enn fremtid, hendelser og

konsekvenser (Engen et. al., 2021, s. 102-103). Sett i sammenheng med oppgavens tematikk vil VTS-modellen kunne benyttes for å analysere hvordan potensielle sårbarhetsflater, verdier og utviklingen i trusselbildet virker gjensidig inn på hverandre og hvordan sikkerheten rundt norsk kraftsektor påvirkes av samfunnsutviklingen. Videre vil Reasons (1997) «sveitserostmodell» bidra til å skape en forståelse for hvordan samfunnsdigitaliseringen har åpnet for nye sårbarhetsflater og synliggjøre hvordan sårbarheter vil kunne oppstå der latente svakheter får utvikle seg ubemerket i kraftsektorens eksisterende barrierer og sikkerhetstiltak.

Sluttelig har jeg valgt å trekke inn sentrale utviklingstrekk ved samfunnsdigitaliseringen for å bidra til å tydeliggjøre og eksemplifisere hvilke mekanismer og tendenser som følger i kjølvannet av den digitale utviklingen. Herunder fremheves relevante dimensjoner og dilemmaer som avhengigheten til digitale verdikjer, integrasjonen av cyber-fysiske systemer og potensielle fallgruver ved klassisk risikopersepsjon. Disse dimensjonene vil tjene som egnede konsepter for å illustrere hvordan samfunnsdigitaliseringen kan bidra til å skape nye sårbarhetsflater for kritiske samfunnsfunksjoner. Samlet sett skal det teoretiske rammeverket og de presenterte modellene tjene som egnede analyseverktøy og bidra til å belyse hvordan samfunnsdigitaliseringens og aktuelle sikkerhetspolitiske faktorer virker inn på sikkerheten rundt norsk kraftforsyning.

4.0 – METODE OG FORSKNINGSSTRATEGI

For å besvare problemstillingen og tilhørende forskningsspørsmål etter akademisk kvalifiserte standarder stilles det strenge krav til oppgavens forskningsstrategi og metodiske forankring. Metodebruken handler om hvordan en finner frem til relevant informasjon og hvordan innhentet data struktureres, brytes ned og anvendes i oppgaven. For å sikre notoritet og danne et grunnlag for kontroll og vurdering av resultatene for potensielle lesere er det essensielt at en redegjør for oppgavens metodiske tilnærming (Jacobsen, 2016).

Informasjonsinnhentingen til oppgaven har basert seg på et bredt spekter av faglitteratur, fellesutgivelser og offentlige publikasjoner som berører oppgavens tematikk. Herunder har samfunnsvitenskapelig forskning, utredninger, offentlige rapporter og vitenskapelige artikler dannet rammene for den innledende litteraturgjennomgangen. Sentrale aktører som NVE, Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets Forskningsinstitutt utmerker seg med flere og mer dyptgripende bidrag på feltet og har dermed utgjort en større del av

litteraturunderlaget. Deler av prosjektet vil følgelig forankres i studier av allerede eksisterende forskning og empirisk dokumentasjon. Aktuelle publikasjoner er valgt ut for å fange opp helheten og ikke beskrive et for snevert segment av kraftsektoren. For å finne frem til definisjoner og redegjørelser rundt aktuelle begreper og fenomener som benyttes i oppgaven har jeg i stor grad tatt utgangspunkt i pensumlitteraturen for masterprogrammet i samfunnssikkerhet. Herunder vil Njå, Sommer, Rake & Braut (2021) utgjøre et faglig rammeverk for relevante modeller og prinsipper innenfor samfunnssikkerhetsfaget. Blant annet vil sentrale konsepter som fortolkninger av sårbarhet og risiko, analysemetoder og modellen for sikkerhetsstyring baseres på begrepsavklaringene og definisjonene til Njå et al. (2021).

Majoriteten av besvarelsen vil likevel baseres på innsamlede data. Ved å benytte primærdata vil jeg som forsker selv delta aktivt i informasjonsinnhentingen og følgelig utvikle et nært forhold til innsamlet informasjon. Den overordnede målsetningen med datainnsamlingen har vært å utvikle innsikt og forståelse rundt norsk kraftforsyning og den tilhørende leveransesikkerheten innenfor rammen av samfunnsdigitaliseringen og dagens sikkerhetspolitiske situasjon. Basert på det innsamlede datagrunnlaget vil jeg gjennom oppgaven forsøke å belyse aktuelle sårbarheter ved kraftsystemet og samtidig kartlegge hvordan digitaliseringen og ulike sikkerhetspolitiske faktorer virker inn på sikkerheten rundt kraftforsyning som kritisk samfunnsfunksjon. Informasjonsbehov knyttet til oppgavens øvrige forskningsspørsmål har også stått sentralt ved informasjonsinnsamlingen. Innsamlet empiri og primærdata vil suppleres med teoretiske bidrag fra samfunnsvitenskapelig forskning og offentlige publikasjoner på feltet (Jacobsen, 2016).

4.1 – Metodisk tilnærming

Innenfor metodefaget skilles det ofte mellom kvalitativ og kvantitativ metode. Kvantitativ metode benyttes primært ved innsamlingen av større mengder informasjon og vil gi målbare data som videre kan struktureres kvantitativt ved hjelp av tabeller og grafer. Ved en kvalitativ fremgangsmåte ønsker man derimot å undersøke et tema eller et samfunnsfenomen i dybden og går derfor systematisk frem for å samle inn fyldige data som ofte beskrives og struktureres tekstuelt. Slik søker man å gjøre forståelig for andre den mening, erfaring eller hensikt en hendelse eller et fenomen har for de involverte (Dalland, 2017, s. 50-60; Grønmo, 2023).

I besvarelsen av denne masteroppgaven har jeg tatt utgangspunkt i en kvalitativ metodikk all den tid jeg gjennom prosjektet har ønsket å utvikle en dybdeforståelse rundt kraftforsyningens sårbarhetsflater og sikkerhetsstyringen av kraftforsyningen som kritisk samfunnsfunksjon. Ved en kvalitativ tilnærming har jeg samtidig fått muligheten til å innhente relevant dybdeinformasjon om subjektive vurderinger, hendelser og tiltak som til sammen bidrar til å belyse oppgavens overordnede problemstilling og tilhørende forskningsspørsmål på en oversiktlig måte. Videre har den kvalitative tilnærmingen åpnet opp for at datainnsamlingen kan konsentreres inn mot tematikken som er relevant for oppgaven. Herunder har de gjennomførte intervjuene og dokumentanalysen i hovedsak rettet seg mot sentrale aspekter ved sikkerhetsstyringen av kraftsektoren og den fremtidige utviklingen i trusselbildet, aktuelle sårbarhetsflater sett i lys av samfunnsdigitaliseringen og potensielle sårbarhets- og risikoreduserende tiltak.

4.2 – Vitenskapelig dokumentanalyse

En vitenskapelig dokumentanalyse viser til en kvalitativ innholdsanalyse av relevante publikasjoner med formål om å innhente relevant informasjon som skal analyseres for å kartlegge mulige sammenhenger og mekanismer (Grønmo, 2015, s. 50-60). For å etablere en innledende oversikt på feltet har jeg analysert relevante dokumenter og offentlige publikasjoner som omhandler kraftforsyningen som kritisk samfunnsfunksjon og tilhørende sårbarhetsflater. De skriftlige arkivaliene dokumentanalysen er basert på utgjorde utgangspunktet for datainnsamlingen. Gjennom analysen har jeg kun benyttet meg av offentlige publikasjoner utarbeidet av statlige myndigheter underlagt lovpålagte retningslinjer for utgivelse av informativt virke. Samtlige dokumenter vurderes følgelig som pålitelige og autentiske.

Samlet sett har det vært en omfattende prosess å skaffe oversikt og bryte ned litteraturen på området for å finne frem til de mest relevante publikasjonene. I forkant av dokumentanalysen har jeg derfor avgrenset tema og konsentrert gjennomgangen inn mot sårbarheter og dilemmaer ved sikkerheten og sikkerhetsstyringen av kraftforsyningen som kritisk samfunnsfunksjon. For å sikre et bredt datagrunnlag har jeg blant annet tatt utgangspunkt i to sentrale NOUer om samfunnssikkerhet, relevante trusselvurderinger fra statlige sikkerhetsmyndigheter og et utvalg av fagrapporter og forskningspublikasjoner på feltet. En helhetlig oversikt over arkivaliene benyttet under dokumentanalysen fremkommer av delkapittel 5.1.1. Utover å benytte meg av primærkilden har jeg også søkt å identifisere og

benytte meg av publikasjonenes sekundærkilder for å redusere muligheten for feiltolkning og danne en bredere forståelse av meningsinnholdet. Datagrunnlaget fra dokumentanalysen har bidratt til å konkretisere problemområdene jeg gjennom oppgaven ønsket å se nærmere på og gitt verdifulle opplysninger om sikkerhetsstyringen av norsk kraftforsyning som helhetlig system.

4.3 – Intervjuer og intervjuguide

For å supplere dokumentanalysen og finne frem til relevante primærdata har jeg gjennomført fire intervjuer med aktuelle informanter. Herunder relevante nøkkelpersoner ved Norges vassdrags- og energidirektorat, Forsvarets forskningsinstitutt, den digitale sikkerhetssektoren og enheter som faller inn under Kraftforsyningens beredskapsorganisasjon. Gjennom intervjuene har jeg søkt å finne frem til relevant informasjon for å utvikle en dypere forståelse rundt leveransesikkerheten for norsk kraftforsyning og det respektive trusselbildet. Intervjuene tok utgangspunkt i en utfyllende intervjuguide utviklet i forkant av intervjuene. Jeg utarbeidet en intervjuguide designet for informantene tilknyttet kraftsektoren og en egen intervjuguide tilpasset informantene fra FFI og den digitale sikkerhetssektoren.. Intervjuguidene baserte seg på oppgavens problemstilling, forskningsspørsmål og det foreliggende teoretiske rammeverket. Videre definerte jeg prioriterte informasjonsbehov og utformet hovedspørsmålene jeg søkte besvart gjennom intervjuet. Intervjuguidene har følgelig dannet grunnlaget for de planlagte intervjuene og består av ulike hovedspørsmål kategorisert etter tema, med underliggende delspørsmål.

All den tid jeg blant annet har gjennomført intervjuer av informanter med førstehåndserfaringer fra sikkerheten rundt kraftsystemet og utfyllende kunnskaper om den sikkerhetspolitiske situasjonen har jeg gjennom prosjektet benyttet meg av semistrukturerte intervjuer. Semistrukturerte intervjuer innebærer at hovedspørsmålene er utviklet i forkant av intervjuet og definert i en intervjuguide, men at intervjuer selv står fritt til å supplere med utfyllende og sonderende oppfølgingsspørsmål for å innhente relevant overskuddsinformasjon (Qu & Dumay, 2011). De utformede intervjuguidene tar følgelig utgangspunkt i åpne spørsmål hvor svaralternativene ikke nødvendigvis er gitt i forkant og intervjuguiden har med andre ord ikke blitt fulgt mekanisk gjennom intervjuene. Det enkelte intervju ble videre tilpasset intervjuobjektet utefra praksis, erfaring og kunnskapsfelt.

Intervjuene har foregått muntlig og enten blitt gjennomført digitalt over egnet videoløsning eller ved fysisk oppmøte. Som intervjuer har jeg lagt til rette for at informantene i størst mulig grad har fått føre ordet. For å bygge opp under dataens validitet har jeg samtidig vært bevisst på egen innflytelse på informantens svar og forsøkt å påvirke informantens budskap minimalt. På denne måten opplever jeg å ha lagt til rette for at informantene har fått muligheten til å bidra med relevant og upåvirket overskuddsinformasjon ut over det feeorventede (Qu & Dumay, 2011; Dalen, 2011). Innsamlet primærdata har blitt bearbeidet og strukturert og sett i sammenheng med relevante funn fra dokumentanalysen under den avsluttende drøftingen. De empiriske funnene fra intervjuene er oppsummert under delkapittel 5.2.

4.4 – Valg av informanter

For å innhente pålitelig og relevant informasjon ønsket jeg å komme i kontakt med informanter med utfyllende kunnskaper om kraftforsyningen som system, kjennskap til det foreliggende trusselbildet og generelt bred innsikt i oppgavens tematikk for øvrig. Av hensyn til oppgavens begrensede tidsrammer var jeg derfor nødt til å foreta et strategisk utvalg av potensielle kandidater. Jeg etablerte tidlig kontakt med Norges vassdrags- og energidirektorat og Elvia som nettselskap tilknyttet Kraftforsyningens beredskapsorganisasjonen. Basert på kunnskapsnivå, faglig funksjon og erfaringsbasert innsikt vurderte jeg deres informanter til å inneha et solid faglig grunnlag for å svare ut definerte informasjonsbehov og bidra med relevant informasjon om norsk kraftsektor. For å belyse den sikkerhetspolitiske situasjonen og sivilsamfunnets sikkerhetsutfordringer ønsket jeg samtidig å gjennomføre et intervju med en informant fra FFI. Som forsvarssektorens egen forskningsinstitusjon representerer FFI et fremtredende forskningsinstitutt med militær og politisk innsikt og et solid faglig fundament for å beskrive sivilsamfunnets sikkerhetsutfordringer (FFI, 2023a). Sluttelig gjennomførte jeg også et intervju med en informant med bred erfaring fra den digitale sikkerhetssektoren. Intervjuobjektet ønsket imidlertid ikke å presenteres eller identifiseres med virksomheten vedkommende jobber i.

Samtlige informanter ble innledningsvis gjort kjent med prosjektet og informert om hvorfor deres kunnskap og erfaringer ble vurdert som essensielle for å belyse oppgavens forskningsspørsmål. Videre ble informantene gjort kjent med at sensitive opplysninger anonymiseres, at de har mulighet til å la være å svare på enkeltspørsmål og at de har anledning til å trekke seg fra prosjektet etter eget ønske uten videre negative konsekvenser. Intervjuene ble tatt opp på lyd ved hjelp av båndopptaker for å fange helheten i informantens

resonnementer og sikre notariatet ved datainnsamlingen. Videre ble svarene protokolert stikkordsvis i en intervjuprotokoll og oppsummert i et sammendrag av intervjuet. De ferdigstilte resyméene ble avslutningsvis sendt til informantene for godkjenning, rettelser og eventuelle tilføyelser.

4.5 – Forskningsstrategi

Innsamlet empiri og funnene fra dokumentanalysen vil sees i sammenheng med oppgavens teoretiske rammeverk under den avsluttende drøftingen. Jeg har følgelig valgt å ta utgangspunkt i en abduktiv forskningsstrategi. Det vitenskapsteoretiske begrepet «abduksjon» ble introdusert av filosofen Charles Sanders Peirce. Kort oppsummert handler abduksjon om hvordan nye ideer og hypoteser oppstår og hvordan vi velger blant dem. En abduktiv forskningsstrategi tillater oss med andre ord å rekontekstualisere samfunnsfenomener, slik at fenomenet kan forståes på en ny måte ved å fortolkes utefra et definert teoretisk rammeverk. Følgelig kan man etablere ny mening ved et allerede kjent fenomen gjennom å avdekke nye sammenhenger og forbindelser (Persson, 2019). En abduktiv tilnærming vil ikke nødvendigvis produsere en logisk konklusjon, men heller generere flere mulige fortolkninger. Til forskjell fra deduksjon som – gitt sanne premisser – vil etablere enn strengt logisk slutning, vil abduksjon beskrive hvordan noe sannsynligvis kan være. I motsetning til induksjon utledes heller ingen generalisering utefra de foretatte observasjonene. Observasjonene sees i stedet i sammenheng med et teoretisk rammeverk for å etablere en plausibel forklaring eller fortolkning på et fenomen eller en hypotese (Danermark, Ekström & Karlsson, 2019, s. 80-90).

Blaikie og Priest (2019) hevdet på sin side at det teoretiske rammeverket utgjør resultatet av en studie heller enn studiets utgangspunkt. Med andre ord baseres den samfunnsvitenskapelige forskningen på at man i en sosial verden kun observerer en sosial konstruksjon av virkeligheten. Konstruksjonen er etablert av de sosiale aktørene og representerer aktørenes forståelser, meninger og kunnskaper. På denne måten skiller Blaikie og Priests perspektiv seg fra Danermark ved at de inntar et ulikt utgangspunkt for sin abduktive forskningsstrategi. Når det er sagt deler partene oppfatning om at abduksjon kan brukes som en ´forskningsstrategi for å skape ny innsikt og fortolke sosiale fenomener (Blaikie & Priest, 2019, s. 114-119).

I denne masteroppgaven vil jeg ta utgangspunkt i det teoretiske rammeverk presentert i delkapittel 3.0. Videre gjøres observasjoner og dataanalyser som sees i sammenheng med det foreliggende rammeverket. Kombinasjon av teori og empiri vil til slutt resultere i en faglig diskusjon og en fortolkning hvor det trekkes paralleller mellom innsamlede data og presentert teori for å etablere en plausibel fortolkning på oppgavens problemstilling. All den tid en abduktiv tilnærming tillater forskeren å rekontekstualisere fenomener utefra et definert teoretisk rammeverk kan det etableres ny mening ved et allerede kjent fenomen gjennom å plassere potensielle funn i en bredere kontekst og avdekke nye relasjoner, mønstre og forbindelser. Heller enn å utvikle allmenngyldige slutninger vil oppgaven med andre ord produsere mer eller mindre sannsynlig fortolkninger basert på foreliggende teori og innsamlet empiri (Danermark et al., 2019, s. 80-90; Blaikie & Priest, 2019, s. 114-119).

4.6 – Begrensninger og avgrensninger ved metodevalg

En kvalitativ fremgangsmåte og en abduktiv forskningsstrategi medfører imidlertid flere potensielle fallgruver for validiteten ved forskningsprosjektet det er viktig at en som forsker er oppmerksom på. Herunder vill resultatene fra en kvalitativ studie kunne kontamineres av forskerens forforståelse, antagelser og subjektivitet. I oppgavebesvarelsen vil fortolkningen av innsamlet data til en viss grad baseres på intervjuobjektets direkte uttalelser, men uttalelsene vil også kunne videreutvikles i dialog med forskeren. Fordi intervjuobjektet kan svare slik intervjueren «ønsker» foreligger det en risiko for at intervjuobjektet «pynter på» sannheten og det kan være utfordrende å innhente selvstendige svar. Videre vil potensielle funn kunne sees i lys av forskerens forutforståelse og på denne måten feiltolkes utefra forskerens tidligere erfaringer (Dalen, 2011, s. 30-36).

Spesielt for oppgavens tematikk er den store mengden sikkerhetsgradert informasjon på området. Sensitive data har utgjort en utfordring i flere av de gjennomførte intervjuene og det har vært enkelte spørsmål visse informanter ikke har hatt anledning til å gå nærmere inn på av hensyn til konfidensialiteten. En informant har også vært nødt til å trekke seg fra prosjektet. Alle intervjuobjektene ble i forkant av intervjuene gjort kjent med at de selv avgjorde hvilke spørsmål de ønsket å besvare og at det på ingen måte ville forventes å få tilgang til taushetsbelagt informasjon. Utfordringen har imidlertid vært av begrenset karakter all den tid det er de overordnede hovedlinjene som har stått sentralt gjennom intervjuene, og spesifikke enkeltdetaljer har blitt tillagt mindre vekt. Det er i hovedsak tekniske detaljer ved systemene,

definerte sårbarhetsflater og konkretiserte prosedyrer unntatt offentligheten som informantene ikke har kunnet uttale seg detaljert om.

Til tross for metodikkens svakheter og potensielle begrensninger er jeg likevel av den oppfatning at en kvalitativ tilnærming åpner for et rikt tilfang av overskuddsinformasjon i form av kunnskap, meninger, erfaringer og tidligere opplevelser og følgelig utgjør den best egnede fremgangsmåten for datainnsamling til oppgaven. Det begrensede omfanget av kvantitative data og generaliserbare slutninger utgjør imidlertid en mulig svakhet for allmenngjøringen av oppgavens funn og resultater.

4.6.1 – Validitet

I en samfunnsvitenskapelig kontekst handler validitet om hvorvidt en forskningsmetode er egnet til å undersøke det man gjennom forskningsprosjektet faktisk ønsker å undersøke og kan beskrives som en indikator på funnenes relevans og gyldighet. Herunder skiller man ofte mellom intern og ekstern validitet. Intern validitet er uttrykk for funnenes gyldighet og handler om målemetodene faktisk måler hva de tiltenkt å måle og om informasjonsinnhentingen er relevant for å besvare problemstillingen. Funnenes gyldighet må sees i sammenheng med utvalget og fenomenet som studeres (Kvale, Brinkmann, Anderssen & Rygge, 2015, s. 276-280). For å styrke studiens interne validitet har jeg gjennom de foretatte intervjuene vært bevisst på følge opp med utdypende og sonderende oppfølgingsspørsmål for å forebygge misforståelser. Videre fikk informantene mulighet til å komme med rettelser og tilføyelser til intervjuet i etterkant. Slik fikk man oppklart potensielle uklarheter og på denne måten styrket oppgavens interne validitet. Ved å supplere intervjuene med dokumentanalyser av aktuelle publikasjoner fikk jeg samtidig utfordret fortolkningene av datamaterialet fra intervjuene og styrket dataens gyldighet ved å benytte meg av et bredere kildegrunnlag. All den tid flere av intervjuobjekter innehar sentrale funksjoner ved samfunnsvirksomheter innenfor energi- og forsvarssektoren kan det samtidig argumenteres for at deres perspektiver har vært relevante og av stor betydning for å belyse oppgavens tematikk.

Ekstern validitet handler på sin side om hvorvidt resultatene fra en studie kan generaliseres og også vil være gyldige under andre forhold og betingelser (Johannessen et al., 2010, s. 230-232). All den tid jeg har tatt utgangspunkt i en abduktiv forskningsstrategi kan det være utfordrende å generalisere resultatene fra forskningsprosjektet. I motsetning til en deduktiv

slutning, hvor funnene kan generaliseres fra det allmenne til enkelttilfeller, vil en abduktiv forskningsstrategi heller produsere en mer eller mindre sannsynlig fortolkning basert på teori og empiri. Den overordnede målsetningen ved studien vil følgelig være å forstå og skape ny mening ved å fortolke innsamlede data gjennom et eksisterende teoretisk rammeverk, heller enn å utvikle generaliserbare slutninger (Yin, 2017, s. 78-80).

4.6.2 – Reliabilitet

Reliabilitet viser til studiens stabilitet og konsistens. En reliabel målemetode vil gi samme resultatet hvis den gjentas flere ganger på samme måleobjekt. I dette forskningsprosjektet vil resultatenes reliabilitet imidlertid kunne påvirkes ved at informantene endrer oppfatning over tid eller uttrykker seg på en annen måte ved et senere intervju. Det er dermed ikke gitt at andre som benytter seg av samme metodikk og fremgangsmåte vil lande på de samme konklusjonene på et senere tidspunkt. De studerte organisasjonene vil for eksempel kunne endre struktur eller funksjon og på denne måten påvirke studiens reliabilitet. Den menneskelige og samfunnsmessige dynamikken utgjør på denne måten en utfordring ved samfunnsvitenskapelig forskning generelt og ved en abduktiv tilnærming spesielt. At en metode innehar høy reliabilitet innebærer imidlertid ingen garanti for at metoden faktisk måler egenskapene eller konstruksjonen metoden er designet for å måle. En studie kan altså være reliabel uten at den nødvendigvis er valid. Potensielle feilkilder som kan gå utover studiens validitet og reliabilitet kan blant annet være kortsiktig variasjon hos informantene, situasjonelle faktorer ved intervjusituasjonen, påvirkning fra intervjuer, feil ved avgivelsen av svar, feil ved kodingen eller registeringen av svar eller feil ved analysen og fortolkningen av innsamlede data (Yin, 2017, s. 78-83; Blaikie & Priest, 2019, s. 120-126).

4.7 – Forskningsprosess

Hvorvidt resultatene og funnene fra forskningsprosjektet vil vurderes som gyldige og autentiske vil blant annet påvirkes av valgene som er foretatt gjennom forskningsprosessen. I tabellen under presenteres en kronologisk oversikt over forskningsaktivitetene som er gjennomført under arbeidet med masteroppgaven. Herunder er tabellen utformet med utgangspunkt i kategoriene «når», «hva» og «hvorfor» for å beskrive valgene som ligger bak de ulike forskningsaktivitetene. Tabellen tar sikte på å beskrive valgene som er foretatt på et overordnet nivå og vil ikke gå i dybden på de enkelte forskningsaktivitetene.

***Tabell 1**: Forskningsprosess*

Når	Hva	Hvorfor
November 2022	Utforming av prosjektskisse og definering av tema for masteroppgaven.	Jeg tok på et tidlig stadium tak i utviklingen av oppgavens tematikk. Herunder startet jeg tankeprosessen med å finne frem til en egnet og forskningsmessig interessant problemstilling.
Desember 2022	Ferdigstillelse av prosjektskisse og innsending av søknad om masteroppgave i samarbeidsportalen. I den forbindelse utarbeidet jeg en foreløpig problemstilling med tilhørende forskningsspørsmål.	Etter grundige tankeprosesser og innledende litteraturgjennomganger fant jeg frem til oppgavens tematikk og definerte en foreløpig problemstilling.
Januar 2023	Med utgangspunkt i problemstillingen og oppgavens tematikk fant jeg frem til egnede teoretiske bidrag i pensumlitteraturen. Videre kartla jeg relevante publikasjoner og forskningsrapporter for den vitenskapelige dokumentanalysen. Jeg etablerte samtidig en oversikt over aktuelle intervjuobjekter.	Da jeg hadde funnet frem til et relevant teoretisk rammeverk tok jeg fatt på oppgavens teorikapittel. Ved å etablere en oversikt over aktuell teori, sentrale publikasjoner på feltet og relevante intervjuobjekter utviklet jeg en dypere forståelse for oppgavens tematikk. Slik var det også enklere å finne frem til relevante intervjuobjekter og aktuelle publikasjoner for dokumentanalysen.

Når	Hva	Hvorfor
Februar 2023	Basert på oppgavens problemstilling, forskningsspørsmål og det foreliggende teoretiske rammeverket utviklet jeg to dekkende intervjuguider. Herunder utformet jeg også informasjonsskriv om oppgaven og nødvendige samtykkeerklæringer. Videre etablerte jeg kontakt med relevante samarbeidspartnere og tidfestet tidspunkt for intervjuene. Forskningsprosjektet ble også meldt inn til SIKT (kunnskapssektorens tjenesteleverandør) gjennom standardiserte meldeskjemaer.	For å kunne kontakte aktuelle intervjuobjekter var det sentralt å tidlig ferdigstille arbeidet med intervjuguidene og informasjonsskrivet. Det var essensielt å få meldt inn forskningsprosjektet til SIKT på et tidlig stadium for å få godkjenningen til å gjennomføre intervjuene i god tid. Videre var arbeidet med intervjuguidene retningsgivende for den videre oppgavebesvarelsen.
Mars 2023	På bakgrunn av innledende litteraturgjennomganger fant jeg frem til relevante arkivalier for dokumentanalysen. Dokumentene ble brutt ned og analysert med henblikk på å innhente relevante data for å besvare oppgavens problemstilling. Intervjuguidene ble revidert på bakgrunn av sentrale funn og informasjonsbehov fra dokumentanalysen.	For å etablere en dybdeforståelse for oppgavens tematikk ønsket jeg å gjennomføre dokumentanalysen i forkant av intervjuene. På denne måten opplevde jeg å utvikle en bredere innsikt i relevante sammenhenger og faglige konsepter før jeg gjennomførte de kvalitative intervjuene.
April 2023	I april ferdigstilte jeg dokumentanalysen og mottok godkjenning fra SIKT til å behandle personopplysninger. I den forbindelse gjennomførte jeg de første kvalitative intervjuene. Totalt	Intervjuene ble gjennomført for å samle inn primærdata og supplere dokumentanalysen. Gjennom intervjuene søkte

Når	Hva	Hvorfor
	gjennomførte jeg fire intervjuer i løpet av forskningsprosjektet.	jeg å finne frem til relevant informasjon og besvare definerte informasjonsbehov. I etterkant av intervjuene satt jeg også igjen med verdifull overskuddsinformasjon som bidro til å belyse nye aspekter ved problemstillingen.
Mai 2023	Det siste intervjuet ble gjennomført i slutten av mai. Etter å ha gjennomført dokumentanalysen og relevante intervjuer ble innsamlet data analysert og strukturert. Aktuelle funn ble deretter sett i sammenheng med oppgavens teoretiske rammeverk og drøftet opp mot oppgavens overordnede problemstilling.	Innsamlet empiri ble i tråd med en abduktiv forskningsstrategi sett i sammenheng med relevante teoretiske bidrag for å bygge fundamentet for en faglig diskusjon og relevante fortolkninger på oppgavens problemstilling og forskningsspørsmål.
Juni 2023	Avslutningsvis ble sentrale funn konkretisert og den faglige diskusjonen oppsummert. Basert på oppgavens funn, konklusjoner og samfunnsmessige kontekst ble det videre utviklet forslag til relevante oppfølgingsstudier. Sluttelig ble nødvendige justeringer, tilføyelser og referansegjennomganger ferdigstilt på bakgrunn av den avsluttende veiledningen.	Oppgaven ble revidert og justert for å fremheve og klarlegge den røde tråden i oppgavebesvarelsen. Samtidig ble dokumentet strukturert for å gjøres mest mulig leservennlig. Oppgaven ble levert i henhold til fristen 15. juni 2023.

4.8 – Ivaretakelse av forskningsetiske regler

Et sentralt aspekt ved all forskning er å legge til rette for at forskningsetiske normer blir ivaretatt. Etiske overveielser handler om mer enn bare formelt nedfelte retningslinjer og blir av Dalland (2017, s. 167-169) beskrevet som vurderinger ved forskningen sett opp samfunnets verdier og normer. Herunder vektlegges ivaretakelsen av menneskene som deltar i forskningsprosjektet, opprettholdelsen av personvern og respekt for enkeltpersonenes velferd og integritet (Johannessen, Christoffersen og Tufte, 2010). I arbeidet med denne masteroppgaven har jeg tatt utgangspunkt i Den nasjonale forskningsetiske komité for samfunnsvitenskap og humaniora sine retningslinjer for å sikre ivaretakelse av grunnleggende forskningsetiske prinsipper.

For å ivareta informantenes rett til selvbestemmelse har deltakelse i prosjektet basert seg på den enkelte informants eget informerte samtykke. Informantene har samtidig blitt orientert om at de gjennom hele forskningsperioden kan trekke seg fra prosjektet uten videre begrunnelse. For å ivareta personvernet ble samtlige informanter som har bidratt i prosjektet anonymisert. I tråd med bestemmelsene som følger av personopplysningsloven har forskningsprosjektet blitt meldt inn til Norsk senter for forskningsdata (NSD, 2022) all den tid intervjuene har blitt tatt opp på lyd og enkelte personopplysninger har blitt protokolert. Hvilken virksomhet intervjuobjektene tilhører og hvilken faglig funksjon de innehar vil imidlertid fremkomme av oppgavebesvarelsen i den grad det anses som relevant for evalueringen og vurderingen av oppgavens funn. NSD har blitt opplyst om forskningsprosjektet gjennom standardiserte meldeskjemaer hvor det redegjøres for forskningsprosjektets formål, metodiske fremgangsmåte og på hvilken måte innsamlet data vil lagres. Samtlige informanter som har bidratt med informasjon til oppgavebesvarelsen har i forkant av intervjuet blitt orientert om forskningsprosjektet gjennom klargjørende informasjonsskriv og fylt ut og signert standardiserte samtykkeerklæringer. Samtlige informasjonsskriv, samtykkeskjemaer og benyttede intervjuguider ligger vedlagt under oppgavens vedlegg (Johannessen et al., 2010).

4.9 – Bearbeidelse av data

For den store majoriteten av datainnsamlingsmetoder stilles det krav til en etterfølgende manipulering og raffinering av innsamlede data for å omsette informasjonen til en form som kan analyseres (Blaikie, N. & Priest, 2019, s. 227-236). Herunder må dataene samles inn, reduseres og analyseres. I henhold til Blaikie og Priest (2019) er det umulig å separere disse

prosessene, da de vil blandes med hverandre i en syklisk prosess. Analysen av kvalitative data handler med andre ord om å samle inn informasjonen, beskrive materialet, systematisere og kategorisere dataene for å etablere oversikt over området og sluttelig se dataene i en større sammenheng og fortolke informasjonen for å finne frem til en plausibel forklaring (Blaikie, N. & Priest, 2019, s. 230-240).

For å forenkle den videre bearbeidingen av informasjon og etablere en helhetlig oversikt over innhentet empiri vil innsamlet primærdata brytes ned og struktureres under delkapittel 5.0. Herunder vil funnene fra dokumentanalysen struktureres og presenteres i en samlet og tematisk oppsummering, mens informantenes bidrag vil kategoriseres utefra tema og informantens faglige funksjon. I tråd med en abduktiv forskningsstrategi vil innsamlet data deretter sees i sammenheng med og fortolkes i lys av det foreliggende teoretiske rammeverket. Slik søker jeg å identifisere mønstre og fellesnevnere i det empiriske datagrunnlaget. Det teoretiske rammeverket beskrevet i delkapittel 3.0 har følgelig vært retningsgivende for både utformingen av intervjuguider og den påfølgende analysen av empiriske data. Ved å trekke paralleller mellom teori og empiri søker jeg videre å etablere ny innsikt i hvordan sikkerheten rundt norsk kraftforsyning påvirkes av samfunnsdigitaliseringen, innenfor rammene av dagens sikkerhetspolitiske situasjon.

4.10 – Forutforståelse

Før jeg tar fatt på oppgavens hoveddel vil jeg gjennom å redegjøre for min forutforståelse avklare hvilken subjektiv forståelse av temaet jeg bringer med meg inn i skriveprosessen. Forutforståelsen beskrives som den forståelsen en bringer med seg inn til materialet som skal fortolkes og baseres på summen av tidligere erfaringer og tilegnet kunnskap (Thurén, 2009, s. 65-70). Ved å redegjøre for min forutforståelse vil både jeg som forsker og potensielle lesere gjøres oppmerksom på hvilken påvirkning forkunnskapene mine kan ha for de slutningene og resonnementene som presenteres videre i oppgaven.

Min forutforståelse bygger dels på kunnskaper tilegnet gjennom masterprogrammet i samfunnssikkerhet, dels på aktuelle arbeidserfaringer, dels på beskrivelser fra toneangivende aktører på feltet og dels på inntrykk formet av det rådende nyhetsbildet, relevant faglitteratur og den generelle samfunnsoppfatningen. Basert på disse ulike kildene til informasjon er mitt inntrykk, før jeg tar fatt på studien, at kraftforsyningen utgjør en helt essensiell samfunnsfunksjon for opprettholdelsen av en rekke andre kritiske samfunnsfunksjoner og

infrastrukturer. Skadepotensialet og samfunnsrisikoen som følger i kjølvannet er følgelig enormt og utgjør en vesentlig større sikkerhetsutfordring enn hva den allmenne oppfatningen i samfunnet tilkjennegir. I takt med samfunnsdigitaliseringen er mitt inntrykk at sårbarhetsflatene har ekspandert og at de digitale avhengighetene har åpnet for nye sikkerhetsutfordringer. Sett i sammenheng med det sikkerhetspolitiske landskapet og utviklingen i trusselbildet er det nærliggende å legge til grunn at de voksende sårbarhetsflatene i større grad vil kunne utnyttes av ondsinnede aktører i tiden fremover. Herunder underbygger dagsaktuelle hendelser som den antatte sabotasjen mot de undersjøiske Nord Stream- gassrørledningene (NRK, 2022) eller det store mangfoldet av cyberangrep mot europeiske samfunnsinstitusjoner de siste årene trusselaktørenes kapasitet og intensjon på området.

Sett opp mot oppgavens tematikk er det med andre ord naturlig å legge til grunn at samfunnsdigitaliseringen på den ene siden bidrar til effektivisering, men på ande siden åpner for nye sårbarheter som vil kunne medføre en direkte konsekvens for sikkerheten rundt norsk kraftforsyning. Videre er det nærliggende å anta at trusselbildet har forandret seg drastisk i lys av det siste årets sikkerhetspolitiske uroligheter og at dette har hatt stor innvirkning på sikkerhetsstyringen av kraftforsyningen som system. Samlet sett er mitt inntrykk at trusselbildet og sårbarhetsflatene har endret seg i takt samfunnsutviklingen og tilspisningen av den sikkerhetspolitiske situasjonen. Jeg legger dermed til grunn at denne utviklingen har fått en direkte innvirkning på det beredskapsforberedende arbeidet til sentrale aktører på feltet og NVEs tilnærming til sikkerhetsstyringen av kraftsektoren som helhet.

5.0 – EMPIRI

I følgende delkapittel presenteres en oppsummering av innhentet materiale fra intervjuer og gjennomførte dokumentanalyser. For å etablere en oversikt på feltet og danne fundamentet for den videre datainnsamlingen ble det innledningsvis gjennomført en utfyllende dokumentanalyse av aktuelle fagrapporter og publikasjoner på området. Herunder har jeg tatt utgangspunkt i relevante utgivelser og NOUer som omhandler samfunnsdigitaliseringen, kraftforsyningen som kritisk samfunnsfunksjon og det tilhørende trusselbildet. På bakgrunn av funnene fra dokumentanalysen, oppgavens problemstilling og det presenterte teoretiske rammeverket ble det videre utformet to ulike intervjuguider som danner grunnlaget for de supplerende intervjuene.

Intervjuene er tematisk strukturert. Første del av intervjuene for informantene tilknyttet kraftsektoren omhandler kraftforsyningen som kritisk samfunnsfunksjon og det generelle trusselbildet mot kraftforsyningen som system. Andre del av intervjuene gikk, i tråd med problemstillingen, nærmere inn på potensielle sårbarheter og observerte endringer i trusselbildet sett i lys av samfunnsdigitaliseringen og dagens sikkerhetspolitiske situasjon. Intervjuene med informantene tilknyttet FFI og den digitale sikkerhetssektoren tok i større grad sikte på å belyse den sikkerhetspolitiske utviklingen og sivilsamfunnets sikkerhetsutfordringer på et overordnet nivå. Etter å ha gjennomført dokumentanalysen og planlagte intervjuer ble innsamlet data analysert og strukturert. Aktuelle funn fra intervjuene og dokumentanalysene er konkretisert og oppsummert i de påfølgende delkapitlene. I delkapittel 6.0 sees relevante funn i sammenheng med oppgavens teoretiske rammeverk og drøftes opp mot oppgavens overordnede problemstilling og tilhørende forskningsspørsmål.

5.1 – Funn fra dokumentanalyser

5.1.1 – Arkivalier benyttet i dokumentanalysen

For å etablere en innledende oversikt har jeg i den videre datainnsamlingen tatt utgangspunkt i og analysert relevante rapporter, publikasjoner og NOUer som omhandler kraftforsyningen som kritisk samfunnsfunksjon. Jeg har i hovedsak basert dokumentanalysen på publikasjoner utarbeidet av offentlige myndigheter, sikkerhetspolitiske fagforum og ekspertorganer med ansvar for drift, opprettholdelse og sikkerhetsstyring av kraftforsyningen som system. Som følge av det brede omfanget av fagrapporter og publikasjoner på feltet har jeg i forkant av dokumentanalysen avgrenset tema og konsentrert analysen inn mot sårbarheter i driften av kraftforsyningen som samfunnsfunksjon, sett i lys av samfunnsdigitaliseringen og utviklingen i det sikkerhetspolitiske landskapet. For å sikre et bredt datagrunnlag har jeg tatt utgangspunkt i publikasjoner fra flere forskjellige utgivere, herunder NOUer som omhandler samfunnssikkerhet og digital sårbarhet, sikkerhetspolitiske trusselvurderinger fra aktuelle fagforum som Etterretningstjenesten, PST og NSM, samt eksternrapporter, forskningspublikasjoner og offentlige utgivelser fra relevante aktører på feltet.

De ulike dokumentene er valgt ut på bakgrunn av deres fokus på ulike aspekter ved oppgavens tematikk. Samlet sett har de ulike dokumentene bidratt med relevante data egnet til å belyse oppgavens problemstilling og til å konkretisere problemområdene jeg ønsket å se nærmere på gjennom prosjektet. Herunder har dokumentanalysen tilført verdifulle

opplysninger om kraftforsyningen som kritisk samfunnsfunksjon, sentrale trekk ved dagens sikkerhetssituasjon, digitale sårbarhetsflater og aktuelle sårbarhetsreduserende tiltak. Tabellen under viser en fremstilling av dokumentene og kildematerialet jeg har benyttet som grunnlag for dokumentanalysen:

***Tabell 2**: Arkivalier benyttet i dokumentanalysen*

Aktør/ Etat	**Tittel**	**Format**
Direktorat for samfunnssikkerhet og beredskap	*Samfunnets kritiske funksjoner (2016)*	Rapport
Forsvarets etterretningstjeneste	*Fokus (2023)*	Rapport
Forsvarets forskningsinstitutt	*En sårbar kraftforsyning - Sluttrapport etter BAS3 (2001)*	Rapport
Nasjonal sikkerhetsmyndighet	*Risiko 2023 - Økt uforutsigbarhet krever økt beredskap (2023)*	Rapport
Norges vassdrags- og energidirektorat	*IKT-sikkerhetstilstanden i kraftforsyningen (2021)*	Rapport
Norges vassdrags- og energidirektorat	*Risikostyring av IKT-sikkerhet i leverandørkjeder (2022)*	Rapport
Norges vassdrags- og energidirektorat	*Veiledning til forskrift om sikkerhet og beredskap i kraftforsyningen - Kraftberedskapsforskriften (2012)*	Veileder
Politiet sikkerhetstjeneste	*Nasjonal trusselvurdering (2023)*	Rapport
Justis- og politidepartementet	NOU 2006:6: *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner (2006)*	NOU
Justis- og beredskapsdepartementet	NOU 2015:13: *Digital sårbarhet – sikkert samfunn (2015)*	NOU

I de påfølgende delkapitlene presenteres relevante funn gjort gjennom dokumentanalysene. Gjennomgangen vil naturligvis ikke være uttømmende, men tar for seg de mest aktuelle momentene sett opp mot oppgavens overordnede problemstilling, forskningsspørsmål og avgrensninger. Innsamlet informasjon er bearbeidet, redusert og analysert og i det videre

strukturert under tematiske overskrifter. De ulike deloverskriftene vil romme bearbeidet data og relevante funn fra flere av de analyserte dokumentene.

5.1.2 – Kraftforsyningen som kritisk samfunnsfunksjon og tilknyttet lovverk

På overordnet nivå omfatter kraftforsyningen de systemer og leveranser som er nødvendig for å ivareta samfunnets behov for elektrisk energi. Som det fremkommer av DSBs rapport (2016, s. 9-10) kategoriseres kraftforsyningen som en kritisk samfunnsfunksjon utefra DSBs definerte kriterier. Med andre ord legger DSB til grunn at en svikt i kraftleveransen i løpet av kort tid vil true befolkningens trygghet og samfunnets grunnleggende behov og i samme periode utfordre landets beredskapsressurser. Herunder fremheves det i NOU (2006:6, s. 80-81) om samfunnets kritiske funksjoner og infrastrukturer at kraftforsyningen utgjør en essensiell komponent i opprettholdelsen av befolknings elementære behov og samfunnets grunnleggende funksjonalitet. På bakgrunn av kraftforsyningens samfunnskritiske rolle ble det allerede i 1991 etablert sikkerhetsbestemmelser i form av energiloven med det formål å sikre kraftforsyningens leveransesikkerhet. Sikkerhetsbestemmelsene omhandlet tiltak som skulle sikre anlegg av betydning for landets kraftforsyning mot sabotasje og for å hindre uvedkommende i å skaffe seg informasjon om og adgang til kraftforsyningsanlegg i den hensikt å ødelegge eller forstyrre virksomheten. Herunder innebefatter kraftforsyningen som samfunnsfunksjon en rekke særegne objekter som kraftstasjoner, damanlegg og ledningsnett der vil være sårbare for sabotasje og skadeverk. I nyere tid er disse sikkerhetsbestemmelsene i større grad blitt erstattet og utfylt av en egen forskrift om sikkerhet og beredskap i kraftsektoren (Kraftberedskapsforskriften, 2012; NOU 2006:6, s. 80-90).

Av formålsbestemmelsen i kraftberedskapsforskriften (2012, §1) fremkommer det at forskriften skal sikre at kraftforsyningen opprettholdes og at normal leveranse gjenopprettes på en effektiv og sikker måte i og etter ekstraordinære situasjoner for å redusere de samfunnsmessige konsekvensene. Forskriften gjelder for de virksomheter som defineres som KBO-enheter etter forskriftens §2-1 og viser til alle aktører som eier eller driver anlegg av vesentlig betydning for kraftsektoren. Disse virksomhetene plikter etter forskriften å sørge for effektiv sikring og beredskap og til å forebygge, håndtere og begrense skadevirkningene ved ekstraordinære situasjoner. Herunder skal virksomhetene gjennomføre risikovurderinger, varsle ved ekstraordinære forhold, gjennomføre øvelser slik at personellet utvikler kompetanse til å håndtere kritiske hendelser, ivareta effektive informasjonsplaner og en effektiv informasjonsberedskap og sluttelig rapportere ved mistanke om sikkerhetstruende

atferd, sikkerhetstruende hendelser, forsøk på inntrenging, avbrudd i el-distribusjonen eller ved forsøk på sabotasje og hærverk (Kraftberedskapsforskriften, 2012; NVE, 2012, s. 13-18 & s. 24-26).

Samlet sett fremheves det i NOU av 2006:6 (s. 99-100) at kraftforsyningen spiller en avgjørende rolle i opprettholdelsen av en rekke vitale tjenester i samfunnet. Følgelig vil et bortfall av leveransesikkerheten og et avbrudd i elektrisitetsdistribusjonen kunne utløse en kaskadeeffekt av eskalerende feil i tilknyttede infrastrukturer og samfunnsfunksjoner. Videre vil informasjons- og ledelsesapparatet som trer i kraft ved kriser og katastrofer og responderende beredskapsressurser få store utfordringer med samhandlingen dersom bortfallet av kraftforsyningen samtidig fører til forstyrrelser i den elektroniske kommunikasjonen. På denne bakgrunn understrekes behovet for redundante løsninger og en kontinuerlig identifikasjon av mulige sårbarhetsflater og risikofaktorer i kraftsektoren. Samtidig vises det videre til Forsvarets forskningsinstitutt (FFI) sine BAS-prosjekter for sårbarhetsanalyser av kraftforsyningen som kritisk samfunnsfunksjon og for effektivitetsanalyser av sårbarhetsreduserende tiltak (NOU 2006:6, s. 99-101 & 170).

5.1.3 – Foreliggende trusselbilde og kilder til risiko

I PSTs nasjonale trusselvurdering for 2023 løftes statlig etterretningsvirksomhet frem som en sentral faktor i det nasjonale trusselbildet samfunnet står ovenfor i det inneværende året. I denne sammenheng poengteres det at krigen mellom Russland og Ukraina har endret de mellomstatlige relasjonene mellom Russland og vesten på fundamentalt vis. De sikkerhetspolitiske spenningene bidrar videre til å aktualisere trusselen fra utenlandsk etterretningstjeneste og den russiske etterretningen fremheves som den største enkeltstående trusselaktøren mot norske sikkerhetsinteresser i 2023. Samtidig understrekes det at etterretningstrusselen fra andre autoritære regimer holder seg mer eller mindre uendret sammenlignet med tidligere år. Herunder løftes kilderekruttering, digitale nettverksoperasjoner og fordekt anskaffelsesvirksomhet frem som metoder norske virksomheter vil utsettes for i løpet av det kommende året (PST, 2023, s. 1-5).

Konkrete sabotasjeaksjoner mot norsk territorium vurderes imidlertid som *lite sannsynlig* sett opp mot PST standardiserte sannsynlighetsangivelser. Dette innebærer at PST vurderer at det er *liten grunn* (mellom 10-40 % sannsynlighet) til å forvente russisk sabotasje mot Norge i det inneværende året. PST tar i sin trusselvurdering imidlertid et forbehold om at

sabotasjehandlinger mot strategiske mål i Norge kan bli et mer aktuelt scenario dersom Russlands vilje til å eskalere konflikten med NATO og Vesten tiltar. I et slikt tilfelle fremheves spesielt petroleumssektoren, men også infrastrukturen tilknyttet kraftsektoren som særlig utsatte mål. En potensiell sabotasjehandling vil etter PSTs vurdering kunne gjennomføres fysisk så vel som digitalt, men mest sannsynlig på en måte som gjør det krevende å tilskrive handlingen til aktøren som står bak (PST, 2023, s. 17-21).

Nasjonal sikkerhetsmyndighet (NSM) vektlegger også den sikkerhetspolitiske utviklingen i sin vurdering av risikobildet for 2023. Herunder fremheves sammensatte virkemidler og cyberangrep som sentrale trusler mot de eksponerte sårbarhetsflatene til samfunnskritiske virksomheter og institusjoner. Sett under ett beskriver NSM dagens sikkerhetspolitiske situasjon som langt mer uforutsigbar enn tidligere år. Spesielt løftes sabotasje, høy kartleggingsvirksomhet mot kritisk infrastruktur og digitale trusler frem som presserende risikoområder for det norske samfunnet. Videre presiserer NSM at den digitale sårbarhetsflaten stadig ekspanderes i takt med at norske virksomheter i økende grad baserer seg på underleverandører og verdikjeder som ofte er langt dårligere sikret enn selve virksomhetene. Sett i sammenheng med svakere økonomiske tider frykter NSM samtidig at sikkerhetsinvesteringer vil nedprioriteres til fordel for produksjonen i flere private sektorer. Her vil utviklingen av sikkerhetstiltak i mange tilfeller utgjøre en betydelig utgift som ikke nødvendigvis harmonerer med næringslivets målsetning om profittmaksimering eller bedriftenes «kjernevirksomhet». I den forbindelse kan det være fristende for bedriftene å senke sikkerhetsnivået for å heller kunne allokere ressursene til andre produksjonsmessige formål. Sett hen til næringslivets stadig mer sentrale rolle i arbeidet med nasjonale sikkerhetshensyn vil sikkerhetsutfordringer for den enkelte organisasjon imidlertid raskt kunne forplante seg og få ringvirkninger for samfunnets samlede motstandsdyktighet. Følgelig kan svakere driftsøkonomi og nedprioriteringen av sikkerhetstiltak potensielt kollidere med nasjonale sikkerhetshensyn (NSM, 2023, s. 7-15).

Alt i alt beskriver NSM at summen av komplekse sårbarhetsflater og utviklingen i trusselbildet utgjør en risiko for koordinerte og tverrsektorielle tilslag mot strategiske mål og sikkerhetsinteresser. Særlig vil stormaktsrivaliseringen, Kinas voksende politiske ambisjoner og Russlands angrepskrig i Ukraina bygge opp under konfliktflaten mellom vestlige demokratier på den ene siden og autoritære regimer på den andre. I kjølvannet av denne konfliktflaten legger NSM til grunn at risikoen for at grunnleggende samfunnsfunksjoner og

tilhørende leverandørkjeder utsettes for hybride og sammensatte virkemidler, som et ledd i interstatlig interessestrid, vil øke. Samtidig vil også de voksende cybersårbarhetene utgjøre en kilde til risiko for alvorlige digitale hendelser i henhold til NSMs risiko- og sårbarhetsvurdering (NSM, 2023, s. 7-20).

5.1.4 – Kartlagte sårbarhetsflater i kraftsektoren

Forsvarets forskningsinstitutt har gjennom BAS (beskyttelse av samfunnet) -prosjektene hatt en målsetning om å utvikle kunnskap for sivile og militære myndigheters arbeid innenfor samfunnssikkerhet og sivil-militært samarbeid siden den første BAS-rapporten ble publisert i 1994. Herunder skal BAS-prosjektene bidra til et gjennomarbeidet konsept for beskyttelse av samfunnets kritiske funksjoner og infrastrukturer (FFI, 2023b). I BAS3-prosjektet ble aktuelle sårbarheter ved kraftforsyningen kartlagt. Til tross for at prosjektet strekker seg langt tilbake i tid utgjør sluttrapporten et referansedokument ved flere av de andre utgivelsene dokumentanalysen baserer seg på. BAS-prosjektene har videre innehatt en fremtidsrettet tidshorisont og funnene fra analysen av sluttrapporten harmonerer med funnene fra flere av de øvrige fagrapportene i oppgaven. Følgelig vurderes flere av de identifiserte sårbarhetsflatene konkretisert i BAS-prosjektets sluttrapport fremdeles som dagsaktuelle og som et hensiktsmessig bidrag til å belyse oppgavens problemstilling, til tross for rapportens opprinnelige utgivelsestidspunkt (FFI, 2001; NOU 2006:6, s. 170).

I sluttrapporten av 2001 (FFI, 2001, s. 7) løftes fysiske påkjenninger og digitale angrep mot informasjonssystemer frem som kritiske sårbarhetsflater for kraftforsyningen som system. Herunder påpeker rapporten at totalsummen av en økende IKT-avhengighet, internasjonalisering, et tiltagende effektiviseringsjag og knapphet på kompetent personell formentlig vil bidra til å bygge opp under disse sårbarhetsflatene også i fremtiden. For å sikre en stabil kraftforsyning foreslår FFI derfor at kraftforsyningen sikres ved tiltak som reduserer de mest utpregede sårbarhetsflatene mot målrettede anslag. Blant annet gjennom en helhetlig sikring av IKT-systemer, satsing på personell og kompetanseutvikling og fysisk sikring av kritiske objekter og driftssentraler. Til tross for at tiltakene vil utgjøre et viktig løft av grunnleggende svakheter ved sikkerheten rundt kraftforsyningen konkluderer rapporten likevel med at kraftforsyningen som en kritisk samfunnsfunksjon fremdeles vil være sårbar for «*større målrettede aksjoner utført av ressurssterke motstandere*» (FFI, 2001, s. 7). Følgelig anbefales det på lengre sikt at kraftforsyningen sikres utover det anbefalte nivået,

gjennom markedsmessige grep som sikrer nyinvesteringer og fokus på relevante sikrings-og beredskapstiltak (FFI, 2001, s. 7-8).

Selve kraftproduksjonen som delsystem fremheves imidlertid som lite sårbart all den tid kraftsektoren består av et stort antall kraftstasjoner fordelt over hele landet. Kraftsystemet er i stor grad redundant, og betydningen av det enkelte anlegget vil variere med temperaturer, årstid, nedbør, revisjoner og tidspunkt på døgnet. Avhengigheten til det enkelte anlegg er i hovedsak av begrenset betydning og flere av anleggene er dimensjonert slik at det normalt må en krigstrussel til for å ødelegge deres produksjonskapasitet. Videre er hovednettet godt dimensjonert mot ekstreme værbelastninger og fysiske påkjenner gjennom alternative og redundante leveransetraséer (FFI, 2001, s. 12-15). Forbindelsene og transformatorstasjonene er imidlertid mindre robuste og en ondsinnet aktør vil med relativt enkle midler kunne angripe disse. Gjennom å ta ut et fåtall transformatorstasjoner vil vedkommende aktør kunne ramme kraftforsyningen til en stor befolkningsgruppe over lang tid. Herunder understreker FFI i BAS-rapporten at den fysiske sikringen rundt kraftforsyningens kritiske objekter ofte er mangelfull ovenfor både enkle sabotasjeaksjoner og moderne våpenvirkninger. På denne måten vil en ondsinnet trusselaktør potensielt kunne ta ut el-distribusjonen til befolkningstette områder med relativt enkle midler. Samtidig bidrar effektiviseringsprosessene til at vedlikehold utsettes og levetiden for enkeltkomponenter tøyes, slik at infrastrukturen eldes og potensielt slites ut og leveransesikkerhet svekkes. Utviklingen fører også til at infrastrukturen konsentreres, eksempelvis ved at flere kraftlinjer etableres langs samme trasé, fordi dette er mer økonomisk og mindre miljømessig kontroversielt. På denne måten åpner effektiviserinsjaget en ny sårbarhetsflate ved at enkeltpåkjenninger kan ramme større deler av kraftsektoren samtidig (FFI, 2001, s. 14-16; NOU 2006:6, s. 80-82)

Videre påpeker FFI at sårbarhetsflatene i drift- og styringssystemene har ekspandert i takt med implementeringen av moderne informasjons- og kommunikasjonsteknologi. Der det tidligere var ansatte som overvåket og betjente installasjonene på større kraftforsyningsanlegg fjernstyres nå de samme anleggene fra et fåtall driftssentraler gjennom kompliserte IT-systemer og et velfungerende samband. De teknologiske løsningene bidrar til økt effektivitet, men samtidig til sårbare løsninger knyttet til driften av anleggene. Kraftselskapenes IKT-systemer er i økende grad basert på standardiserte systemer med til dels kjente sikkerhetshull, som kobles sammen med forretningssystemene for å oppnå effektive markedsmekanismer. Følgelig oppstår det en sikkerhetskritisk avhengighet til systemene og den offentlige

telekommunikasjonens pålitelighet. Parallelt med operasjonaliseringen av moderne IKT-løsninger, vil behovet for personell og nyrekruttering naturligvis reduseres. Slik vil digitaliseringen bidra til en selvforsterkende avhengighet til IKT-systemene i takt med at kompetanse og tilgang på kompetent personell går tapt (FFI, 2001, s. 17-20; NOU 2015:13, s. 140-144)

I NOU av 2015 (s. 135-136) om digital sårbarhet løftes de digitale sårbarhetsflatene ved kraftforsyningen frem som de mest eksponerte. I mangel på norsk statistikk trekkes det paralleller til USA hvor det fremkommer av ICS-CERTs (the industrial control systems cyber emergency response team) statistikker at hele 87% av de kartlagte sårbarhetsflatene i driftskontrollsystemene i USA kunne utnyttes gjennom fjernaksess, mens det bare var de resterende 13% som stilte krav til lokale tilganger. Videre ble 65% av de identifiserte sårbarhetsflatene ved amerikansk kraftsektor klassifisert som høyprioritetssårbarheter. Som følge av den digitale utviklingen og den stadig tettere sammenkoblingen av nettverk og systemer har de totale systemene blitt mer komplekse. Det kan følgelig være utfordrende å etablere en helhetlig oversikt over hvordan samhandlingen mellom de ulike systemene fungerer, parallelt med at risikoen for menneskelig svikt og tekniske feil øker. Driftssystemenes eksponering mot internett gjennom fjernaksesstilganger vil samtidig åpne muligheten for uautorisert inntrenging fra ondsinnede datakyndige aktører og kriminelle grupperinger (NOU 2015:13, s. 55-57).

Sluttelig fremhever FFI at den økende internasjonaliseringen og samkjøringen av kraftmarkedene bidrar til styrket forsyningssikkerheten. På den andre siden vil sårbarheten i samarbeidslandene samtidig kunne påvirke den norske kraftforsyningen. På denne måten vil eksempelvis et alvorlig strømutfall i Sverige, også kunne få konsekvenser for stabiliteten ved den norske leveransesikkerheten. Den økte gjensidige avhengigheten til utlandet og underleverandører tilsier dermed et økt behov for beredskapsmessig samarbeid med samhandlende naboland. Samtidig påpeker FFI risikoen for at et internasjonalt beredskapsmessig samarbeid raskt kan bli en «sovepute» som går på bekostning av den nasjonale sikkerheten rundt egen kraftforsyning (FFI, 2001, s. 8)

Samlet sett konkluderer FFI i sluttrapporten fra BAS-prosjektet og Justis- og Beredskapsdepartementet i NOU om digital sårbarhet med at den norske kraftforsyningen er dimensjonert til å tåle naturhendelser og er gjennomgående robust mot fysiske påkjenninger

som følge av en desentralisert produksjonsstruktur og et forsterket forsyningsnett inn mot befolkningssentrene. På den andre siden ligger infrastrukturen lett tilgengelig til i terrenget og er følgelig vanskelig å overvåke og sikre mot målrettede tilslag eller rekognoseringsvirksomhet fra ondsinnede trusselaktører. I takt med den økende avhengigheten til IKT-baserte prosesstyringssystemer, integrasjonen i det europeiske kraftmarkedet, økt kommunikasjonsavhengighet og knapphet på spesialkompetanse vil samtidig den totale sårbarhetsflaten for kraftforsyningen som helthetlig system ekspandere parallelt med samfunnsdigitaliseringen. Herunder fremheves de digitale sårbarhetsflatene som de mest utsatte for målrettede og intenderte tilslag fra fiendtlige trusselaktører (FFI, 2001; NOU 2015:13, s. 129-145).

5.1.5 – Konsekvenser ved bortfall

All den tid tilgang på elektrisitet har utviklet seg til en nødvendig forutsetning for bortimot enhver samfunnsaktivitet påpeker FFI i BAS3-rapporten at en svikt i kraftforsyningen vil få vidtrekkende konsekvenser for samfunnet i sin helhet. Den generelle samfunnsmessige velstandsøkningen og den tiltagende veksten i behovet for informasjons- og kommunikasjonsteknologi har ført til et betydelig høyere energiforbruk. Som tidligere nevnt vil de gjensidige avhengighetene ulike samfunnssektorer i mellom raskt resultere i eskalerende ringvirkninger ved et bortfall av en kritisk samfunnsfunksjon. Herunder vil de sikkerhetskritiske avhengighetene flere offentlige funksjoner har utviklet til kraftforsyningen forsterke de negative konsekvensene ved en potensiell svikt. Avhengig av årstid vil også evnen til elektrisk oppvarming raskt opphøre ved et vedvarende bortfall i leveransesikkerheten. Ved lave utetemperaturer og krevende værforhold kan altså krisesituasjoner med fare for liv og helse oppstå relativt akutt dersom tilgangen på elektrisk energi og fjernvarme forsvinner i større områder over flere døgn (FFI, 2001, s. 8-12).

For å illustrere avhengigheten av uforstyrret tilgang på elektrisk kraft viser FFI til utvalgte erfaringer fra langvarige kraftutfall på slutten av 1990-tallet. Blant annet løftes is-stormen i Quebéc i 1998, orkanene i Frankrike i 1999 og NATOs angrep mot kraftforsyningen i Serbia i 1999 frem som eksempler på hendelser hvor millioner av mennesker har mistet tilgangen på elektrisitet over et tidsrom av en viss varighet. Ved samtlige av de ovennevnte kraftutfallene har man kunnet observert at det normale samfunnslivet raskt gikk i stå, blant annet som en konsekvens at økonomien stanset opp og at folk ikke kom seg på jobb. Følgelig fikk kraftbruddene eskalerende ringvirkninger som etter kort tid også gikk ut over tilknyttede

samfunnsfunksjoner og infrastrukturer. På denne bakgrunn oppsto det raskt utfordringer med grunnleggende samfunnsmessige behov som oppvarming, tilberedning av mat og ivaretakelse av hygiene, samtidig som det oppsto store forstyrrelser i tilgangen på arbeidskraft og evnen til beredskapsrespons. Alt i alt resulterte kraftbruddene i enorme kostnader på samfunnsøkonomisk nivå og førte til stor uro i befolkningen (FFI, 2001, s. 10-12).

Samlet sett konkluderer FFI med at Norges avhengighet til uforstyrret tilgang på elektrisk kraft vil tilta i årene som kommer, som følge av den digitale utviklingen og den generelle velstandsøkningen. På denne bakgrunn vil selv et kortvarig bortfall i leveransesikkerheten resultere i store samfunnsøkonomiske kostnader og ved lengre avbrudd vil det samtidig oppstå fare for liv og helse og befolkningens allmenne helsetilstand. Til tross for at erfaringene fra tidligere fredstidsutfall viser at kraftbruddene kan håndteres tilfredsstillende dersom man klarer å kraftsamle tilstrekkelig med kompetente ressurser i utsatte områder, beskriver FFI at dette sannsynligvis ikke vil være mulig i kriselignende scenarioer. Særlig hvis påkjenningene mot kraftforsyningen inntreffer over utstrakte geografiske områder og det ikke finnes tilgang på større internasjonale ressurser. I takt med at samfunnsvirksomhetene stopper opp som følge av kraftbruddets ringvirkninger vil også evnen til krisehåndtering og transport av beredskapsressurser reduseres kraftig (FFI, 2001, s. 8-14; NOU 2006:6, s. 99-101).

5.1.6 – Digitaliseringen av kraftforsyningen og digitale verdikjeder

De siste tiårene har digitaliseringen ført til gjennomgripende samfunnsmessige endringer og forandret måten ulike sektorer styrer prosesser på, slik at komplekse infrastrukturer eller operasjoner i dag kan styres fra noen få sentrale driftssentraler (NOU 2015:13, s. 15). I takt med samfunnsutviklingen har kraftforsyningen blitt digitalisert gjennom økt bruk av digital teknologi og skytjenester levert av transnasjonale leverandører som har åpnet for nye muligheter og effektivisering i kraftsektoren. Ny teknologi, skytjenseter, ulikeartede systemer og utenlandske leverandører bygger imidlertid også opp under nye sårbarhetsflater. NVE beskriver at digitaliseringsrisikoen spesielt knytter seg til følgende tre forhold:

- Vitale funksjoner og tjenester består av komplekse systemer som samfunnet utvikler en økende sikkerhetskritisk avhengighet til.

- Stadig flere angrep utføres av ressurssterke aktører gjennom et bredt spekter av ulike angrepsmetoder.

- Det har oppstått store sikkerhetskritiske avhengigheter mellom de ulike virksomhetene som drifter kritiske samfunnsfunksjoner og kritiske infrastrukturer (NVE, 2022, s. 8-10).

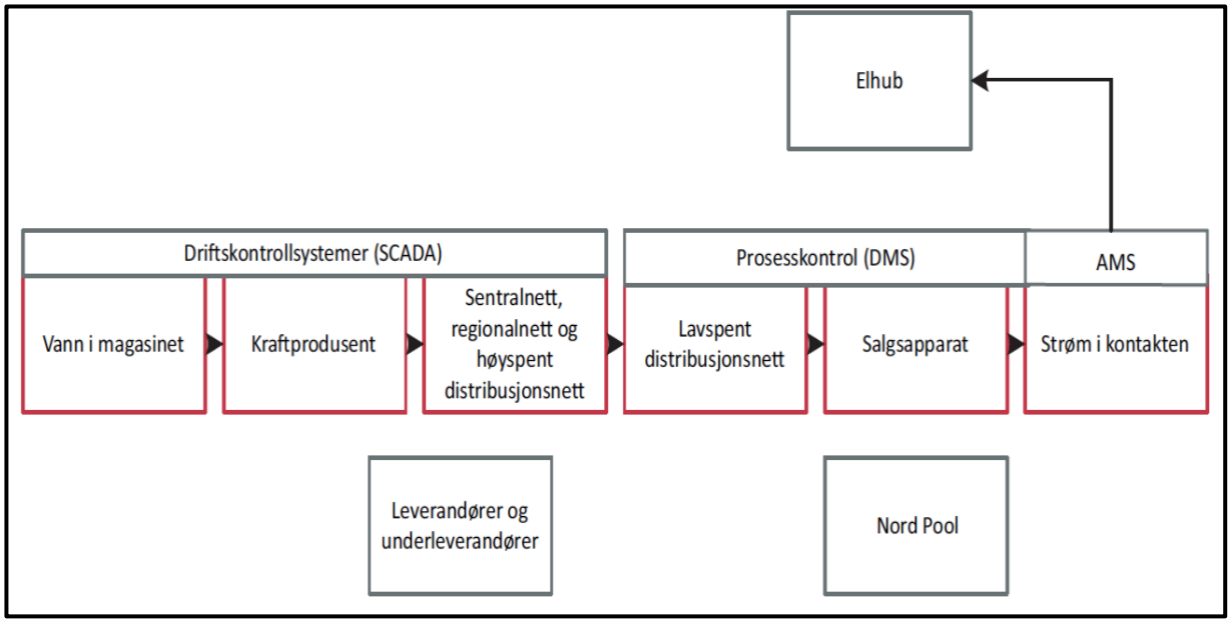
All den tid kraftforsyningen representer et «just in time-system» hvor en endring i strømforbruket må etterfølges av en umiddelbar og tilsvarende endring i produksjonen for at systemet skal være i balanse, stilles det store krav til kraftforsyningens drifts- og styringssystemer. Driftssentralnettet består av datamaskiner og utstyr lokalisert i driftssentralen. De fleste nettselskaper har et eget driftskontrollsystem med en form for redundant reserveløsning. Som følge av det økende behovet for tilgjengelighet og integrert utveksling av data mellom prosesstyringsnett, administrative nett og fortetningsnett kobles disse ofte sammen for å gi brukerne tilstrekkelig funksjonalitet. Siden de administrative nettene som regel er i forbindelse med ulike eksterne aktører åpnes dermed muligheten for fjernaksess og ekstern tilgang fra internett mot de sentrale styringssystemene i driftssentralene. Med andre ord oppstår også risikoen for at ondsinnede datakyndige kan trenge inn i og misbruke driftssystemene. Datainnbrudd og manipulering med fjernstyrte komponenter vil naturligvis kunne forårsake enorm skade og utgjør etter FFI og Justis- og beredskapsdepartementets syn den største enkeltstående sårbarheten ved kraftforsyningen som system. Utover at prosesstyringssystemet åpnes for angrep utenfra stiller handelssystemet for kjøp og salg av kraft videre krav til informasjon om tilstanden i kraftsystemene for å kunne operere i markedene. Informasjonsutvekslingen bidrar på denne måten til et økende press om at sensitiv driftsinformasjon gjøres offentlig tilgjengelig for eksterne aktører (FFI, 2001, s. 14-16; NOU 2015:13, s. 136-140).

Som en konsekvens av at IKT-sikkerhet ikke sto i fokus da driftskontrollsystemene opprinnelig ble utviklet har de moderne kravene til sikring ført til et omfattende og kostbart etterarbeid for å sikre systemene mot uautorisert tilgang. Samtidig har de strenge kravene til systemenes tilgjengelighet komplisert sikringsarbeidet, all den tid tunge systemoppdateringer og sikkerhetsmekanismer også medfører en risiko for nedetid og stans av lovlig datatrafikk. Som følge av den økte kompleksiteten og de strenge kravene til forsyningssikkerheten har flere av virksomhetene innenfor kraftsektoren derfor basert seg på og gjort seg avhengig av

eksterne leverandører og digitale supporttjenester fra utlandet. Blant annet for bistand til vedlikehold og feilretting via fjernaksess. Fjernaksesstjenestene kan imidlertid utfordre kraftberedskapsforskriftens krav til beskyttelse av sensitive data og kontroll med egen informasjon, og samtidig eksponere kraftforsyning for en ny sårbarhetsflate i form av underleverandørens egne sårbarheter og sikkerhetshull. Behovet for fjernaksess vil videre eksponere driftssystemene for internettilgang og i større grad åpne muligheten for uautorisert inntrenging og digital sabotasje fra ondsinnede aktører (NOU 2015:13, s. 138-140; NVE, 2021, s. 14-15)

Som følge av det siste tiårets omfattende digitalisering og globalisering spenner kraftforsyningens digitale leverandørkjeder i dag over et bredt spekter av virksomheter, landegrenser og kontinenter. I sin eksternrapport refererer NVE (2022) til en forskningsrapport av Ponemon Institute (2019) – et amerikansk forskningsinstitutt på cybersikkerhet – som konkluderer med at leverandørkjedene var inngangsporten til systemene for angriper ved over 63% av de registrerte dataangrepene i USA. Videre beskrives målrettede tilslag mot underleverandører, partnere og kunder som en observerbart voksende trend innenfor cyberdomenet generelt og kraftsektoren spesielt. På denne måten har digitale verdikjeder, med komplekse samhandlingsmønstre og sammensatte avhengighetsforhold, ført til en bredere angrepsflate mot kraftsektoren generelt (NVE, 2022,s. 12-14; Ponemon Institute, 2019).

Som et resultat av verdikjedenes kompleksitet vil potensielle svakheter i kjeden samtidig være krevende å kartlegge og identifisere. I takt med økningen av tjenesteutsetting og den tiltagende veksten av digitale underleverandører vil altså sikkerhetsstyringen av kraftforsyningen som system bli stadig mer utfordrende. Som følge av at kraftforsyningen absorberer og integrerer underleverandørenes sårbarheter som sine egne ekspanderes også den totale sårbarhetsflaten for kraftsektoren i sin helhet (NVE, 2022, s. 23-25). Figuren under viser en forenklet fremstilling av verdikjeden i norsk kraftforsyning, fra produksjon i vannmagasinene til strøm hos sluttbrukeren. Modellen er hentet fra NOU om digital sårbarhet (2015:13, s. 137).



Figur 5*: Figuren viser en forenklet fremstilling av verdikjeden i norsk kraftforsyning fra kraftproduksjonen i produksjonsanleggene til strøm i stikkontakten hos sluttbrukeren (NOU 2015:13, s. 137).*

Samlet sett beskriver NVEs rapport (2022) flere utfordringer ved sikkerhets- og risikostyringen av IKT-sikkerheten i kraftsektoren. Informantene som har bidratt med informasjon til NVEs rapport fremhever blant annet mangel på menneskelige ressurser, begrenset med tid til risikostyringsarbeid og oppfølging av risikoreduserende tiltak, mangel på standardiserte prosedyrer for risikostyring av IKT-sikkerhet og uklare krav og sikkerhetsmål til underleverandører som aktuelle utfordringer ved sikkerhetsstyringen av IKT-sikkerheten. Som følge av det store mangfoldet av virksomheter som opererer i kraftforsyningen beskriver flere av informantene samtidig at det kan være problematisk å legge til rette for at ulike virksomheter og avdelinger omforenes om en felles situasjonsforståelse av risikobildet. Videre kan det være en utfordring å få virksomhetene til å ta tilstrekkelig eierskap til den eksisterende risikoen (NVE, 2022, s. 18-26).

Avslutningsvis slår rapporten fast at risikostyringen av IKT-sikkerheten i kraftsektoren vil bli stadig viktigere i takt med at samfunnsdigitaliseringen bidrar til at virksomhetene i et hyppigere omfang vil stilles ovenfor nye digitale trusler. På denne bakgrunn problematiserer rapporten at risiko- og sikkerhetsstyringen av IKT-sikkerheten i kraftsektoren bygger på et svakt empirisk og teoretisk grunnlag og at det foreligger for lite kunnskap om beste praksis på området i form av veiledere eller spesifikke anbefalinger som virksomhetene kan benytte seg

av. På denne bakgrunn foreslår rapporten et bredt spekter av risiko- og sårbarhetsreduserende tiltak som kan bidra til å redusere de digitale sårbarhetsflatene og trygge leveransesikkerheten (NVE, 2022, s. 23-26).

5.1.7 – Sikkerhetspolitiske faktorer og fremtidens trusselbilde

Sett i lys av oppgavens kontekst og dagens globale sikkerhetspolitiske bilde har jeg gjennom dokumentanalysen også tatt utgangspunkt i og analysert relevante trusselvurderinger og offentlige rapporter fra relevante statlige sikkerhetsmyndigheter. Herunder ligger PST sin nasjonale trusselvurdering, NSM sin risikovurdering og Etterretningstjenestens årlige trusselvurdering «Fokus» til grunn for kartleggingen av relevante sikkerhetspolitiske faktorers innvirkning på trusselbildet mot den norske kraftforsyningen. Som det fremkommer av oppgavens avgrensning vil den sikkerhetspolitiske situasjonen kun beskrives på et grunnleggende nivå og i all hovedsak begrenses til den voksende konfliktflaten mellom vesten på den ene siden og autoritære regimer som Kina og Russland på den andre. Herunder vil den økende stormaktsrivaliseringen og Russlands angrep på Ukraina stå i fokus. Felles for de tre ovennevnte trusselvurderingene er at de alle vektlegger uforutsigbarheten ved den foreliggende sikkerhetspolitiske situasjonen.

I den forbindelse fremhever Etterretningstjenesten (2023) at krigen i Ukraina har rokket ved ideen om at tettere økonomisk samhandling reduserer faren for interstatlig konflikt og samtidig har blottlagt aktuelle internasjonale avhengigheter i forsyningskjedene. Ved å strupe gasstilførselen til Europa har Russland forsøkt å så splid i Vesten og svekke vestlig støtte til Ukraina. De økonomiske konsekvensene av krigen har truffet hele Europa og de geopolitiske urolighetene som følger i kjølvannet vil naturligvis påvirke sikkerhetsarbeidet langs flere dimensjoner (Etterretningstjenesten, 2023, s. 5). I tiden fremover legger trusselvurderingene til grunn at en videre tilspisning av situasjonen må forventes. På denne bakgrunn er PSTs vurdering at Russland per dags dato har mer å vinne – og mindre å tape – på å drive ulovlig etterretningsvirksomhet i Norge. Aktiviteten kan illustreres ved det økende antallet pågripelser av personer mistenkt for etterretningsvirksomhet i Norge og andre europeiske naboland det siste året. Samtidig slår PST fast at etterretningsvirksomhet fra andre autoritære regimer som Kina, Iran og Nord-Korea også må forventes. Som et resultat av Norges strategiske beliggenhet, konkurransedyktige teknologi, rike tilgang på naturressurser, Nato-medlemskap og tette samarbeid med USA fremheves Russland likevel som den største

trusselen mot norske sikkerhetsinteresser i det inneværende året (Etterretningstjenesten, 2023, s. 28-30; PST, 2023, s. 7-21)

Gjennom 2022 beskriver PST at forholdet mellom Norge og Russland har blitt vesentlig forverret og at diplomatiske bånd har blitt svekket. De økonomiske sanksjonene har gått på bekostning av handelsrelasjoner, økonomisk samarbeid og transnasjonale investeringer og ført til at norske og russiske myndigheter nå møtes på langt færre bi- og multilaterale arenaer enn tidligere. Følgelig har Russlands tilgang på informasjon om norske forhold blitt vanskeliggjort og som en konsekvens må russiske myndigheter i langt større grad benytte seg av etterretningstjenester for å få dekket sine informasjonsbehov. Slik har det digitale rom blitt viktigere for russisk virkemiddelbruk og Russisk militærdoktrine legger til grunn at nettverksoperasjoner inngår i både strategiske informasjonskampanjer og militære operasjoner. Samtidig vil russisk etterretningstjenestene kunne akseptere en høyere risiko for sin virksomhet all den tid russiske myndigheter har mindre å tape på å bli avslørt som et resultat av den tilspissede relasjonen landene i mellom (Etterretningstjenesten, 2023, s. 28-30; PST, 2023, s. 7-21).

Sett opp mot kraftforsyningen som samfunnsfunksjon fremhever PST at den norske energiforsyningen til Europa har fått en økt sikkerhetspolitisk betydning i etterkant av Russlands angrepskrig mot Ukraina. Herunder har man gjennom det foregående året kunnet observere flere konkrete eksempler på et Russland som ønsker å sette europeisk energisikkerhet under press. På denne bakgrunn forventer PST og etterretningstjenesten at Russland i det inneværende året vil forsøke å innhente informasjon om de fleste forhold ved norsk politikkutforming og gass-, olje- og kraftsektor. Videre vil også informasjon knyttet til norsk krisehåndtering og hvordan Norge vil håndtere en potensiell krisesituasjon med Russland stå sentralt. Eksempelvis ved å teste norsk respons gjennom mindre tilslag og nettverksoperasjoner (Etterretningstjenesten, 2023, s. 30-32; PST, 2023, s. 7-12). Sett under ett forventer PST at fremmede stater vil benytte seg av et bredt spekter av metoder og sammensatte virkemidler i sin etterretningsvirksomhet, som blant annet:

- Kilderekruttering
- Nettverksoperasjoner som tjenestenektangrep eller digital spionasje
- Verdikjedeangrep
- Påvirkningsoperasjoner

- Overvåkning og trusler
- Digital og fysisk sabotasje
- Fordekt anskaffelsesvirksomhet og ulovlig kunnskapsoverføring (PST, 2023, s. 12-15).

I det digitale domenet løfter PST frem Russland og Kina som de største trusselaktørene på bakgrunn av landenes digitale kapasitet og potensielle sikkerhetspolitiske interesser på området. Det forventes at begge landene vil forsøke å ramme norske sikkerhetsinteresser og strategiske mål gjennom 2023. Samtidig har man de senere årene også observert flere eksempler på kriminelle grupperinger som drives av samme intensjoner som statlige aktører eller tilfeller hvor kriminelle hackergrupper samarbeider med statlige etterretningsvirksomheter. I all hovedsak vil disse nettverksoperasjonene innledes ved at trusselaktørene kartlegger en virksomhets digitale sårbarheter. Identifiserte sårbarheter vil videre utnyttes for å skaffe tilgang til en virksomhets digitalt lagrede verdier og konfidensielle informasjon. I hovedsak vil disse nettverksoperasjonene rette seg mot enkeltpersoner og trusselaktørene vil sannsynligvis utnytte relativt enkle sårbarheter ved systemet som utdatert programvare, svake og gjenbrukte passord eller manglende to-faktorautentisering (PST, 2023, s. 12-17).

Sett opp mot oppgavens tematikk og problemstilling vil det i hovedsak være Russland og til dels Kina som peker seg ut som de største interstatlige trusselaktørene mot Norge og norske sikkerhetsinteresser. Til tross for at den konkrete sabotasjerisikoen vurderes som relativt liten bemerkes det av samtlige statlige trusselvurderinger at en ytterligere tilspisning av den sikkerhetspolitiske situasjonen er å forvente. Som følge av Norges Nato-medlemskap, tette politiske samarbeid med USA og energipolitiske betydning er det nærliggende å anta at russisk etterretningsvirksomhet vil tilta i det inneværende året. Herunder vil norsk olje- og kraftsektor være spesielt utsatt som en konsekvens av den økte sikkerhetspolitiske betydningen norsk energiforsyning har fått for Europa. Samtidig forventer de ulike fagforumene at forekomsten av digitale tilslag, verdikjedeangrep og nettverksoperasjoner mot norske virksomheter og demokratiske institusjoner vil tilta i årene fremover (Etterretningstjenesten, 2023, s. 28-35; PST, 2023, s. 12-18).

5.1.8 – Sikkerhetsstyringen av kraftforsyningen

Sikkerhetsstyringen av kraftforsyningen som system tar utgangpunkt i Kraftberedskapsforskriften (2012) og har som overordnet formål å sikre stabile leveranser etter samfunnets behov for elektrisk kraft. Herunder skal involverte virksomheter også legge til rette for at normal forsyning gjenopprettes på en sikker måte under og etter ekstraordinære situasjoner. Som ansvarlig fagdirektorat er det NVE som har det overordnede operative ansvaret for norsk kraftforsyningsberedskap og leveransesikkerhet. På denne bakgrunn har NVE utarbeidet en veileder til kraftberedskapsforskriften (NVE, 2012).

Kraftberedskapsforskriften lovfester at alle KBO-enheter innehar et selvstendig ansvar for å legge til rette for effektiv sikring og beredskap ved egne anlegg, og sørge for tilhørende sikkerhetstiltak for å forebygge, håndtere og begrense virkningene ved ekstraordinære situasjoner. Herunder understrekes det at virksomhetene plikter å sikre egne anlegg og systemer som er eller kan bli av vesentlig betydning for virksomhetens ledelse, drift eller gjenoppretting ved uønskede hendelser og handlinger. I den forbindelse er det virksomhetenes ansvar å tilpasse sikringstiltakene etter systemets oppbygning, funksjon og type. Videre spesifiseres det at utformede sikringstiltak skal ta særlig hensyn til ekstraordinære forhold som brann og eksplosjoner, alvorlig teknisk svikt, uvær og annet naturgitt skade, samt innbrudd, sabotasje og tilsvarende kriminelle handlinger. Anleggene og systemene skal holde funksjonsdyktige og så langt det lar seg gjøre virke etter sin hensikt også under ekstraordinære omstendigheter. De ulike anleggene kategoriseres etter forskriften videre inn i tre ulike klasser utefra sin sikkerhetskritiske betydning for kraftforsyningen som helhet. Desto høyere klasse, desto høyre krav stiller forskriften til implementerte sikringstiltak (NVE, 2012, s. 1-20; Kraftberedskapsforskriften, 2012, §5-1 & 5-2).

Sett i sammenheng med samfunnsdigitaliseringen stiller kraftberedskapsforskriften i kapittel 6 og 7 konkretisere krav til inkluderte virksomheters driftskontrollsystemer og informasjonssikkerhet. Herunder konkretiseres det at alle virksomheter som har eller behandler kraftsensitiv informasjon skal etablere, opprettholde og videreutvikle systemer og rutiner for effektiv beskyttelse, tilgangskontroll og avskjerming av kraftsensitiv informasjon. Blant annet ved å påse at bestemmelsene om informasjonssikkerhet og taushetsplikt for kraftsensitiv informasjon ivaretas ved anskaffelser, at anbudsinnbydelser begrenses når det er nødvendig for å hindre at sikkerhetsgradert informasjon havner på avveie og ved å

gjennomføre personkontroller før ansettelse. Videre skal virksomhetene etablere en grunnsikring for digitale informasjonssystemer, blant annet ved å:

- *Identifisere og dokumentere sentrale verdier, tjenester, systemer, og leveranser.*
- *Risikovurdere systemendringer*.
- *Sikre digitale informasjonssystemer for å motstå eller begrense skade fra uønskede hendelser.*
- *Overvåke digitale informasjonssystemer slik at uønskede hendelser oppdages og registreres.*
- *Varsle uønskede hendelser i digitale informasjonssystemer til aktuell beredskapsmyndighet på området.*
- *Håndtere og gjenopprette uønskede hendelser i digitale informasjonssystemer og gjenopprette normaltilstand.*
- *Utsetting av tjenester for å sikre at sikkerhetsnivået opprettholdes eller forbedres*.
- *Gjennomføre jevnlige sikkerhetsrevisjoner av iverksatte sikringstiltak for sine digitale informasjonssystemer* (Kraftberedskapsforskriften, 2012, §6-3 & 6-9; NVE, 2012).

Samtidig lovfester kraftberedskapsforskriften (2012, §7-1) KBO-virksomhetenes plikt til å legge til rette for at driftskontrollsystemene til enhver tid virker etter hensikt og beskyttes mot alle typer uønskede hendelser. Driftskontrollsystemet innebefatter blant annet driftssentraler, nettverk, utstyr, sambandsanlegg, datarom, samt øvrige anlegg, rom, systemer og komponenter som ivaretar driftskontrollfunksjonene. Omhandlede virksomheter skal blant håndtere og kontrollere sårbarheter i programvare, feilkilder, sikkerhetsbrudd og andre hendelser som kan utgjøre en risiko for driftskontrollsystemet. På overordnet nivå skal virksomhetene også føre kontroll med brukertilgangen og utstyret i driftskontrollrommet, vurdere behovet for systemredundans, kartlegge muligheten for ekstern tilkobling til driftskontrollsystemet og etablere en beredskap for fortsatt drift av anlegg ved en potensiell svikt. Sluttelig spesifiseres en rekke ulike detaljerte sikkerhetskrav til driftskontrollsystemene basert på det enkelte anleggets sikkerhetsklassifisering og sikkerhetskritiske betydning (Kraftberedskapsforskriften, 2012, §7-4 & 7-10).

Sett opp mot NVEs rapport om IKT-sikkerhetstilstanden i Kraftforsyningen (2021) påpekes det at sannsynligheten for vellykkede cyberangrep øker betraktelig dersom virksomhetene

ikke har sikret IKT-systemene godt nok. I den forbindelse peker NVE på betydningen av en god sikkerhetskultur innad i virksomheten og en utpreget sikkerhetsbevissthet i det forbyggende sikkerhetsarbeidet. Videre fremheves viktigheten av å utvikle en helhetlig sikkerhetsstrategi, et robust styringssystem og legge til rette for en god sikkerhetskultur i ledelsen av informasjonssikkerheten. Herunder fremkommer det av rapporten at 80% av beredskapslederne innenfor kraftsektoren svarer bekreftende på at deres virksomhet innehar en IKT-sikkerhetsstrategi. Imidlertid svarer kun 59% av IKT-sikkerhetskoordinatorene at virksomhetene innehar et dedikert styringssystem for informasjonssikkerheten (NVE, 2021, s. 16-21).

Utefra NVEs forståelse viser et styringssystem til prosedyrer og retningslinjer for systematisk styring av informasjonssikkerheten og bygger på de tre grunnpilarene mennesker, teknologi og prosesser. Samlet sett skal styringssystemet minimere risiko ved å aktivt redusere sannsynligheten for sikkerhetsbrudd, begrense virkningen ved uønskede hendelser og sikre forretningskontinuitet. Ved å ha rutiner og personell for å identifisere og håndtere potensielle sårbarheter bidrar virksomheten til å kartlegge, analysere og løse feil og forebygge mulige cyberangrep. Sentrale suksesskriterier i det praktiske sikkerhetsarbeidet vil etter NVEs syn være fokus på kontinuerlig forbedring, oppdaterte risikovurderinger og oversikt over potensielle sårbarheter (NVE, 2021, s. 19-21).

Til tross for et økende fokus på IKT-sikkerhet viser NVEs undersøkelser likevel at det eksisterer en rekke latente svakheter og sårbarheter ved flere av virksomhetenes digitale sikkerhetssystemer. Herunder påpeker NVE flere tilfeller av manglende etterlevelse av kraftberedskapsforskriftens krav til sikring av digitale systemer. I den forbindelse fremheves den eskalerende digitaliseringen som en kompliserende faktor i sikkerhetsarbeidet. Med flere enheter koplet til datanettverkene øker samtidig eksponeringen mot aktuelle digitale trusler og ondsinnede aktører. Videre slår rapporten fast at forsøk på cyberangrep og uautorisert tilgang mot norske KBO-enheter foregår mer eller mindre kontinuerlig. På denne bakgrunn anbefaler NVE at virksomheter i kraftforsyningen som tar en høyere risiko i forbindelse med digitaliseringsinitiativer, samtidig må styre risikoen ved å investere i nødvendige IKT-sikkerhetstiltak, prosedyrer og tilstrekkelig beredskap (NVE, 2021, s. 35-36).

5.1.9 – Relevante tiltak og reduksjon av identifiserte sårbarheter

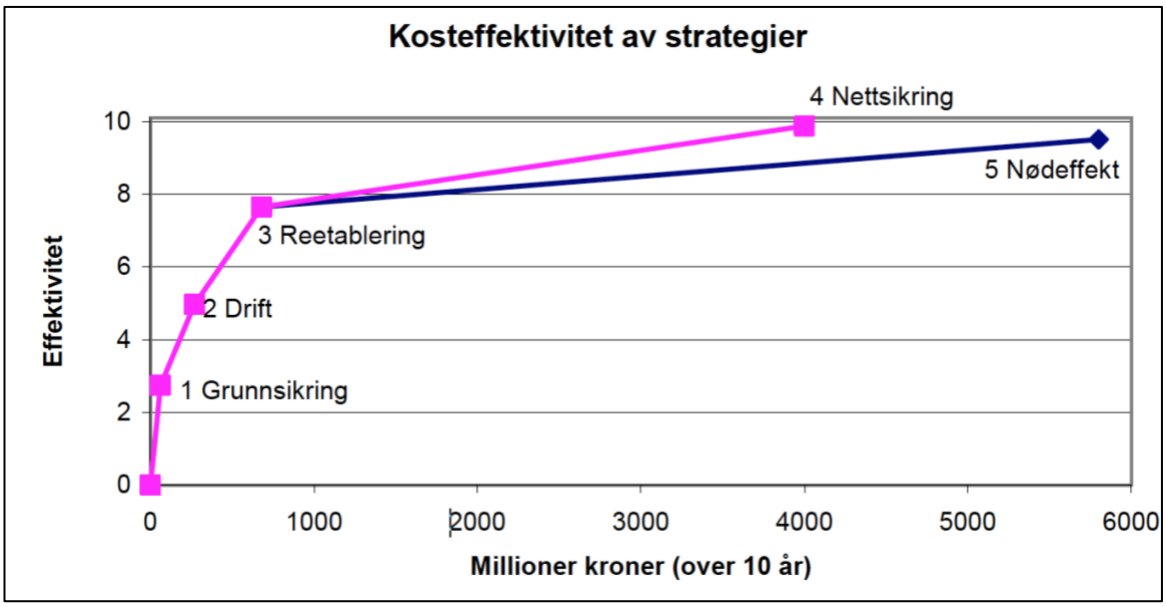
For å redusere identifiserte sårbarhetsflater foreslås det i de analyserte dokumentene en rekke ulike sårbarhetsreduserende tiltak og strategier. Herunder konkretiserer samtlige utgivelser behovet for fastsatte sikkerhetskrav, styrket tilsyn og standardiserte veiledninger innenfor IKT-sikkerhet. I den anledning påpeker Justis- og beredskapsdepartement i NOU (2015:13, s. 143) om digital sårbarhet at den tiltagende digitaliseringen vil stille strengere krav til spissede og kunnskapsbaserte tilsyn innenfor IKT-sektoren. I takt med at det legges opp til stadig tettere koblinger mellom driftskontrollsystemer, administrative systemer og forretningssystemer eksponeres driftskontrollsystemene, som tidligere beskrevet, i større grad for det åpne nettet. De administrative og forretningsmessige gevinstene ved integrasjonen av systemene er imidlertid for store til at utvalget foreslår å jobbe mot denne utviklingen. Isteden foreslår utvalget at utfordringene bør møtes med gode og gjennomgripende tiltak knyttet til teknisk arkitektur, transaksjonskontroller og faglig veiledning. Som følge av den observerte økningen i tjenesteutsetting og mangfoldet av digitale underleverandører foreslår utvalget samtidig at NVE, i fellesskap med interesseorganisasjoner og bransjen i sin helhet, utarbeider utfyllende veiledere på «beste praksis» og standardiserte sikkerhetskrav til tjenesteutsettingen og relevante underleverandører (NOU 2015:13, s. 142-144).

All den tid flere av KBO-enhetene er relativt små med få ansatte vil det imidlertid være en utfordring å etablere og opprettholde kompetente fagmiljøer på IKT-sikkerhet innen den enkelte virksomhet. På denne bakgrunn foreslår utvalget at NVE i samarbeid med relevante interesseorganisasjoner stimulerer til å etablere mer ressurssterke fagmiljøer innen IKT-sikkerhet og samtidig tar initiativ til å bygge opp et operativt fagmiljø med fokus på IKT-hendelseshåndtering. Herunder fremhever utvalget at NVE og de ulike bransjeorganisasjonene bør bidra til å organisere kurs og øvelser rundt IKT-sikkerhet – eksempelvis innenfor prosesstyring, systemintegrasjon og feilretting – slik at bransjen tilegner seg den kompetansen som behøves for å drifte systemene også i fremtiden (NOU 2015:13, s. 142-146).

Som følge av kraftsektorens kritiske funksjon foreslår utvalget samtidig at sektoren etablerer et kompetent fagmiljø for hendelseshåndtering som kan koordinere hendelser internt i sektoren og tjene som kontaktpunkt ut mot andre sektorer. Slik ønsker utvalget å legge til rette for rask informasjonsutveksling om erfarte hendelser, aktuelle trusler og mulige avbøtende tiltak. Avslutningsvis anbefaler utvalget at det gjennomføres brede risiko- og

sårbarhetsanalyser i forkant av alle teknologiskifter, bruksendringer og ved system- og organisasjonsendringer i kraftsektoren for å kontinuerlig identifisere nye sårbarheter og risikoer fortløpende (NOU 2015:13, s. 142-146).

I BAS3-prosjektet har FFI (2001, s. 20-23) på sin side utarbeidet fem strategier – satt sammen av ulike tekniske og organisatoriske tiltak – for redusert sårbarhet i kraftsektoren. Strategiene bygger på hverandre og er utviklet med tanke på forholdet mellom effektivitet og kostand der effektiviteten av strategiene er vurdert opp mot en krisesituasjon med flere samtidige tilslag mot kraftforsyningenes sårbare punkter. Figuren under viser den kartlagte kosteffektiviteten ved de ulike strategiene, beregnet utefra datidens kostnads- og inflasjonsnivåer.



Figur 6: *Kostnad og effektivitet ved de foreslåtte strategiene (Hentet fra: FFI, 2001, s. 22).*

- **Strategi 1:** «Grunnsikring» – Innrettet mot sikring av IT-systemer og driftsfunksjonene. Blant annet gjennom overvåkning av viktige driftssentraler, samøvelser mellom relevante aktører i bransjen og ved å etablere et kompetansesenter for informasjonssikkerhet som skal bistå bransjen ved spørsmål knyttet til informasjonssystemenes sårbarhet og informasjonssikkerhet generelt.

- **Strategi 2**: «Drift» – Fokuserer i større grad på fysiske trusler og trusler mot kraftforsyningens datasystemer. Herunder satser strategien på styrket opplæring og kompetanseheving til beredskapspersonell, samt økt fokus på feiloppretting og reetablering etter ekstraordinære hendelser.

- **Strategi 3**: «Reetablering» – Tar sikte på å forebygge fysiske anslag mot kritiske objekter og styrke evnen til reetablering etter fysisk skade gjennom anskaffelse av mer reparasjonsmateriell som beredskapsmaster og transformatorer. Videre åpner strategien for å etablere en kritisk driftssentral i et sikret fjellanlegg og samtidig bidra til styrket satsing på opplæring av beredskapspersonell.

- **Strategi 4**: «Nettsikring» – Skal forebygge anslag mot kritiske objekter gjennom flere driftssentraler i fjellanlegg, innkjøp av flere reserveretransformatorer og økt redundans i nettet og leveransetraséne.

- **Strategi 5**: «Nødeffekt» – Utgjør en alternativ tilnærming til strategi 4, men tar i større grad sikte på å erstatte nettforsterkningene i strategi 4 med store produksjonsanlegg for bruk i beredskapssituasjoner. Strategien blir følgelig svært kostbar sammenlignet med øvrige foreslåtte strategier.

Sett i sammenheng med utviklingen mot økt sårbarhet og det kommersielle kraftmarkedets ensidige fokus på effektivisering og økonomisk utbytte foreslår FFI at myndighetene som et absolutt minimum sikrer kraftforsyningen i henhold til strategi 3. Samtidig anbefales en oppdatering av regelverket for beredskap mot moderne trusler og på lengre sikt at kraftforsyningen styrkes ytterligere for å sikre leveransesikkerheten inn mot befolkningstette områder. Spesielt gjør dette seg gjeldende for produksjons- og nettkapasiteten (FFI, 2001, s. 23-24).

NVEs rapport om IKT-sikkerhet (2022, s. 17-27) fremhever på sin side viktigheten av et helhetlig styringssystem som bidrar til å etablere en oversikt og kontroll over aktuelle trusler, sårbarheter og risikoer innenfor kraftsektoren. I denne sammenheng blir risikostyringen beskrevet som et kontinuerlig arbeid og som en del av de daglige aktivitetene i virksomhetene. Herunder understreker informantene som har bidratt til studien at sentrale elementer ved risikostyringsprosessen vil være å etablere krav til risikostyringen og kontrollere etterlevelse av kravene gjennom tilsyn. Samtidig påpekes det at all risiko naturligvis ikke kan elimineres og at det følgelig blir viktig å finne frem til en risiko som kan aksepteres. For å fremme god risikostyring oppfordrer informantene til stimulering mot god sikkerhetskultur, bevisstgjøring av ansatte på relevante IKT-trusler og utarbeidelse av et digitalt rammeverk med tilhørende sjekklister, prosedyrer og rutiner.

Med utgangspunkt i risikostyringshjulet og informantenes uttalelser presenterer NVE-rapporten videre et bredt spekter av foreslåtte tiltak for god praksis basert på de ulike fasene i risikostyringsprosessen. Under «risikoidentifiseringsfasen» foreslåes det blant annet at kraftsektoren etablerer en overordnet oversikt over leverandører på feltet og samtidig en ordning for loggføring og godkjenning av leverandører, eksempelvis gjennom krav til sertifisering. Videre anbefaler informantene at beredskapsarbeidet prioriteres høyt i de ulike virksomhetene og at det innhentes oppdaterte trussel- og sårbarhetsvurderinger fra relevante fagforum som KraftCERT (kraftsektorens cyberresponsmiljø), NSM og PST. Under «risikoanalysefasen» foreslås det å etablere konkrete sikkerhetsmål for virksomhetene og underleverandørene, at sikkerhetsmålene evalueres jevnlig og at det benyttes anerkjente metoder – som eksempelvis norsk standard – i analysearbeidet (NVE, 2022, s. 13-18).

I «beredskapsarbeidet» foreslår informantene en implementering av innsatsplaner for de vanligste hendelsene med tilhørende sjekklister og prosedyrer som oppdateres i takt med risikovurderingene. Videre anbefales en overordnet etablering av nødvendige prosedyrer og strukturer for sikkerhetsstyring opp mot definerte sikkerhetsmål. For å kontrollere at etablerte sikkerhetsmål blir ivaretatt ved anskaffelser, organisasjonsendringer og i anbudsprosessen foreslås det utstrakt tilsynsvirksomhet på området. Sluttelig løftes verdien av øvelser og påfølgende evaluering frem som en kritisk faktor i sikkerhetsarbeidet. Herunder foreslår informantene at det etableres interne prosesser for kunnskapsdeling og innhenting av oppdatert informasjon fra evalueringer, overvåkningssystemer, erfaringsmøter og i etterkant av øvelser og ekstraordinære hendelser (NVE, 2022, s. 24-26).

5.2 – Funn fra intervjuer

For å supplere dokumentanalysen og innhente relevante primærdata ønsket jeg også gjennomføre kvalitative intervjuer av toneangivende aktører og nøkkelpersoner på feltet. Totalt ble det gjennomført fire ulike intervjuer. Fellesnevneren for intervjuobjektene er en faglig nærhet til oppgavens tematikk og problemstilling, i kraft av sin funksjon i en samfunnsmessig relevant virksomhet. Et av intervjuobjektene har en tilknytning til NVE og jobber i sitt daglige virke med sikkerhet og beredskap rundt den norske kraftforsyningen. Intervjuobjektet fra NVE har gjennom sitt bidrag medvirket til å etablere en helhetlig oversikt over sikkerhetsstyringen av kraftforsyningen og trusselbildet på overordnet nivå. Videre har informanten i kraft av sitt virke utviklet en inngående kjennskap til integrasjonen av cyber-fysiske systemer i kraftproduksjonen og de potensielle sårbarhetene og risikoelementene som

følger i kjølvannet av samfunnsdigitaliseringen. Den andre informanten fyller en sikkerhetsfunksjon ved nettselskapet Elvia og har gjennom sin stilling en nær tilknytning til Kraftforsyningens beredskapsorganisasjon, og for øvrig bred erfaring med beredskapsarbeid i kraftsektoren. Den tredje informanten jobber ved Forsvarets forskningsinstitutt og er valgt ut på bakgrunn av sin kunnskap om den sikkerhetspolitiske konteksten og de geopolitiske urolighetenes innflytelse på norske sikkerhetsinteresser. Mens den siste informanten er tilknyttet den digitale sikkerhetssektoren og er valgt ut på bakgrunn av sin kunnskap om det digitale risikobildet mot norske virksomheter og samfunnsfunksjoner. Ved å gjennomføre intervjuer av informanter med en variert og tverrfaglig bakgrunn har jeg søkt å belyse sikkerhetsarbeidet og faktorer som virker inn på sikkerheten rundt kraftforsyningen fra ulike perspektiver og i en større sammenheng. Funnene fra intervjuene er oppsummert under og strukturert utefra virksomhetene informantene har en tilknytning til.

5.2.1 – Informant fra NVE

Informanten fra NVE jobber med sikkerhetsstyringen av kraftforsyningen og har en funksjonell tilknytning til NVEs som sikkerhetsrådgiver. Intervjuobjektet tydeliggjorde i forkant av intervjuet at han svarte på vegne av NVE som helhet og i tråd med deres visjoner og sikkerhetsmålsetninger. Intervjuet tok utgangspunkt i den utformede intervjueguiden, samtidig som den semistrukturerte intervjuformen la til rette for at intervjuobjektet fikk bidra med overskuddsinformasjon utover de forhåndsdefinerte spørsmålene. Første del av intervjuet omhandlet kraftforsyningen som system, men andre del av intervjuet gikk nærmere inn på samfunnsdigitaliseringens og relevante sikkerhetspolitiske faktorers innvirkning på sikkerheten rundt kraftsystemet.

Innledningsvis redegjorde informanten for den organisatoriske strukturen og påpekte at NVE utgjør den øverste beredskapsmyndigheten for kraftforsyningen, som leder av Kraftforsyningens beredskapsorganisasjon. Følgelig innehar NVE det overordnede ansvaret for forsyningssikkerheten i kraftsystemet og for å samordne beredskapsplanleggingen på området. KBO-strukturen viser til de virksomheter som er av vesentlig betydning for kraftforsyningen og består av cirka 170 ulike selskaper. Felles for KBO-enhetene er at de plikter å rette seg etter kraftberedskapsforskriftens lovfestede krav til helhetlig sikring og beredskap. Enkelte av kravene er av detaljert karakter, men i all hovedsak baserer forskriften seg på funksjonelle krav som gir relativt vide fullmakter til den enkelte KBO-enhet. NVEs hovedoppgaver i det beredskapsforbedrende arbeidet er med andre ord å føre tilsyn med at

KBO-enhetene innfrir de definerte sikkerhetskravene og veilede virksomhetene om hvordan de skal forholde seg til kraftberedskapsforskriftens bestemmelser.

Som kritisk samfunnsfunksjon presiserer informanten at kraftforsyning står i en særstilling. I dagens moderne samfunn utgjør elektrisitet en helt vital forutsetning for opprettholdelsen av normal samfunnsdrift og et bortfall i leveransesikkerheten vil i løpet av kort tid føre til en spontan stans innenfor de fleste samfunnssektorer. I den forbindelse er kraftforsyningen aktualisert som kritisk samfunnsfunksjon i en rekke sikkerhetsfaglige rammeverk, herunder DSBs rapport om *samfunnets kritiske funksjoner*, men også i NSMs rapport om *Grunnleggende nasjonal funksjoner* og som en av sju kritiske funksjoner i NATOs *baseline requirements.* Med andre ord beskriver informanten at kraftforsyningen naturligvis fyller en avgjørende funksjon for den norske samfunnssikkerheten.

Av hensyn til konfidensialiteten kunne ikke informanten peke ut definerte og konkretisere sårbarhetsområder for kraftforsyningen som system, men beskriver at kraftsektoren fra et teoretisk perspektiv naturligvis står ovenfor et bredt risikobilde. Først og fremst vil den fysiske infrastrukturen alltid være eksponert for naturhendelser, ekstremvær og klimatiske utfordringer. All den tid forsyningsnettet strekker seg over deler av landet med periodevis vanvittige værforhold vil man følgelig måtte ta høyde for enkelte bortfall i kraftleveransene som følge av klimatiske påkjenninger. I takt med klimaendringene frykter informanten samtidig at man i årene fremover vil oppleve mer ekstremvær og en økning i miljømessige sikkerhetsutfordringer. Denne typen hendelser har imidlertid nettoperatørene vist at de i all hovedsak evner å håndtere og rette opp i løpet av kort tid.

Sett opp mot mer målrettede og ondsinnede trusselaktører fremhever informanten at det norske trusselbildet ikke kan sidestilles med Ukraina og andre land i krig. Fra et historisk perspektiv har fokuset på security-trusler imidlertid økt i takt med samfunnsutviklingen. Eksempelvis ble KBO-strukturen etablert i etterkant av andre verdenskrig for å sikre tilstrekkelig fokus på sikkerhet og beredskap rundt kraftsektoren. Videre opplevde man et ekstraordinært trusselbilde under den kalde krigen der faren for storkrig og atomhendelser var overhengende og høyst reel. Sett i retrospekt var kraftforsyningen og det norske forsvaret i større grad dimensjonert for krig og tilpasset alvorlige sikkerhetstruende handlinger under den kalde krigen enn hva det er i dag. I takt med samfunnsdigitaliseringen og den økende avhengigheten til internettbaserte tjenester har systemene samtidig blitt mer komplekse og

mindre oversiktlige. Til tross for at automatiseringen fremheves som et utviklingsideal og har bidratt til effektivisering, vil den digitale utviklingen naturligvis også føre med seg en rekke nye sårbarhetsflater. Selv om økt kompleksitet ikke nødvendigvis er ensbetydende med økt risiko bidrar de komplekse interaksjonene til at kraftforsyningen som helhet er mindre oversiktlig og gjør det vanskeligere å identifisere potensielle feilkilder ved en svikt. Samtidig vil alle systemer som digitaliseres og kobles mot internett i teorien kunne hackes. Til tross for at Norge rent empirisk aldri har vært utsatt for et større cyberangrep, på linje med for eksempel cyberangrepene mot Ukraina i 2014, kan man ikke utelukke at det finnes statlige aktører med kapasitet til å utføre avanserte tilslag mot den digitale infrastrukturen og det norske kraftsystemet. Selv om Kraftberedskapsforskriften i utgangspunktet stiller krav til en robust og motstandsdyktig IKT-sikkerhet har man av tidligere hendelser observert interstatlige aktører som har demonstrert en evne til å gjennomføre sofistikerte cyberangrep mot kritisk infrastruktur og kritiske samfunnsfunksjoner.

Sett i sammenheng med utviklingen i trusselbildet fremhever informanten at risikobildet er vesentlig endret og at man på overordnet nivå er mest bekymret for større statlige aktører med evne til å ramme bredt. Med utgangspunkt i PST, Etterretningstjenesten og NSMs trusselvurderinger har man samtidig blitt bevisst på en forhøyet etterretningstrussel fra Russland mot Norge generelt og kritisk infrastruktur spesielt. Herunder har man blitt oppmerksom på at mindre tilslag kan være en del av et større bilde for å teste kraftforsyningens beredskap. Uten at man har sett en konkret økning i antallet tilslag er NVE likevel bevisst på den endrede sikkerhetspolitiske situasjonen. Som en av Europas fremtredende gass- og kraftleverandører understreker informanten at det finnes et mulig motiv for å ramme norsk energisektor.

Som en konsekvens av den digitale utviklingen har man også observert en vedvarende økning i bruken av digitale underleverandører og tjenesteutsetting av IKT-driften i kraftsektoren. Til tross for at tjenesteutsettingen i seg selv har sine gode grunner, utfordres imidlertid flere av kraftberedskapsforksriftens lovfestede krav til sikkerhet og beredskap. Herunder ser man av tidligere hendelser at det ofte er underleverandørene og de digitale verdikjedene som er blitt kompromittert. Samtidig er risikoen at de ulike KBO-enhetene mister elementær nøkkelkompetanse i takt med at stadig flere oppgaver baseres på underliggende tjenesteleverandører. Til tross for at virksomhetene i utgangspunktet er lovpålagt å beholde tilstrekkelig kompetanse til å kunne drifte systemene manuelt, påpeker informanten at det er

rimelig å anta at denne kompetansen svekkes som et resultat av at flere og flere prosesser automatiseres. Videre kan det problematiseres at de ulike leverandørene og underleverandørene ikke utgjør KBO-enheter, og følgelig ikke er underlagt kraftberedskapsforskriftens krav og retningslinjer. Det blir dermed vanskeligere for NVE å føre kontroll med sikkerhetslandskapet når stadig flere aktører integreres i den digitale verdikjeden. NVE vil heller ikke inneha samme mandat til å gjennomføre tilsyn og veiledning med underleverandørene.

I møte med et dynamisk trusselbilde er kraftforsyningens viktigste grunnsikring at virksomhetene følger opp og ivaretar sikkerhetskravene som følger av kraftberedskapsforskriften. Samtidig utgjør NVE en samarbeidsorganisasjon som driver med konkret veiledning, motivasjon og lederskap, og spiller på lag med KBO-virksomhetene gjennom en helhetlig tilnærming til sikkerhetsstyringen. Herunder skal NVE holde seg oppdatert på den internasjonale situasjonen og aktuelle risiko- og trusselvurderinger. På bakgrunn av dagens geopolitiske uroligheter har beredskap havnet høyere på agendaen hos både NVE og underliggende KBO-enheter de siste årene. Som følge av den teknologiske utviklingen baseres sikkerhetsstyringen i stadig større grad på funksjonelle krav som gir den enkelte KBO-enhet et bredere handlingsrom. I takt med den akselererende digitaliseringen blir det samtidig stadig mer utfordrende å holde tritt med utviklingen, og konsekvensen er følgelig at NVE tidvis driver tilsyn med systemer og ny teknologi de innehar begrenset erfaring med fra tidligere. Når det er sagt fører integrasjonen av cyber-fysiske systemer samtidig med seg en rekke fantastiske muligheter kraftsystemene er avhengig av for å henge med i utviklingen. På den andre siden problematiserer informanten at utviklingen går så raskt at man ikke nødvendigvis ser rekkevidden av konsekvensene, og de potensielle fallgruvene ved den omfattende samfunnsdigitaliseringen.

Sett opp mot den sikkerhetspolitiske situasjonen fremhever informanten at økte geopolitiske spenninger naturligvis også vil ha en innvirkning på trusselbildet mot norsk kraftforsyning. Herunder har krigen i Ukraina bidratt til en skjerpet trussel fra utenlandsk etterretningsvirksomhet, og en økt usikkerhet på politisk nivå. På denne bakgrunn frykter informanten en utvikling mot en mer multipolar verden med mindre frihandel og økt stormaktsrivalisering. I dagens samfunn er spesialkompetansen såpass spredd at de vestlige samfunnene er helt avhengig av global verdenshandel for at ulike samfunnsfunksjonene skal gå rundt. Samtidig påpeker informanten at man vet for lite om hvordan et mer desperat

Russland, som ønsker å svekke vestlig samhold og som tar større risikoer i etterretningsvirksomheten, vil forholde seg til Norge. Som følge av den europeiske energikrisen har flere land blitt nødt til å se seg om etter nye løsninger, fordi det europeiske kraftsystemet i mange år har vært helt avhengig av russisk gassimport. Parallelt med at strømprisene øker, vil også tilliten til myndighetene i mange land svekkes. Russland fører på denne måten en energikrig med Europa, der europeiske land svekker egen energisikkerhet som en del av en solidaritetsstrategi for å svekke Russland økonomisk. I takt med trangere økonomiske tider og økt inflasjon er det samtidig rimelig å anta at økte produksjonskostnader kan gå utover de ulike virksomhetens økonomiske handlingsrom, og at nødvendige sikkerhetsinvesteringer i visse tilfeller nedprioriteres av kostnadsbesparende hensyn.

For å møte utviklingen i trusselbildet har NVE økt frekvensen på kommunikasjonen med KBO-enhetene, tilpasset tilsynsvirksomheten, stimulert til god sikkerhetskultur og oppfordret til økt årvåkenhet. Videre bidrar den skjerpede situasjonen til å aktualisere flere av kravene i kraftberedskapsforskriften. Herunder fremhever informanten betydningen av utfyllende risikovurderinger, oversikt over potensielle sårbarheter i systemene og en risikoinformert styring. I den forbindelse bør virksomhetene etablere en oversikt over verdiene som ønskes beskyttet, potensielle sårbarhetsflater og aktuelle sikkerhetstiltak. Risikoanalysene skal på denne måten tjene som grunnlag for god risikostyring, og ligger til grunn for en risikobasert tilnærming til både digitale og fysiske trusler mot kraftforsyningen. For øvrig viser informanten til NVEs fagrapporter på området for en grundigere analyse av fremtidens digitale trusler og sårbarhetsflater.

5.2.2 – Informant fra Elvia

Informanten fra Elvia jobber til daglig med kraftberedskap, fyller en sikkerhetsfunksjon ved nettselskapet og skal gjennom sitt virke bidra til å sikre operativ drift av regional- og distribusjonsnettene til Elvia. Som Norges største nettselskap målt i kunder og nettområde, utgjør Elvia en sentral KBO-enhet med en sikkerhetskritisk betydning for leveransesikkerheten i samfunnet. Herunder har Elvia ansvaret for å sikre en stabil kraftforsyning til mer enn 900 000 kunder, og over to millioner mennesker i Innlandet, Oslo og Viken hver dag gjennom hele året. Som en del av KBO-strukturen er Elvia samtidig underlagt kraftberedskapsforskriftens bestemmelser, og er dermed lovpålagt å ivareta nødvendige sikkerhetskrav og implementere forskriftsmessige sikringstiltak.

Innledningsvis redegjorde informanten for den organisatoriske strukturen og tydeliggjorde at Elvia organisatorisk ligger under NVE, som er øverste beredskapsmyndighet og fagdirektorat for kraftforsyningen. NVE forvalter sitt mandat gjennom å utvikle regler, forskrifter og instrukser for de underliggende KBO-enhetene og føre tilsyn med etterlevelse av kravene. Ved krisesituasjoner er det videre NVE som setter kriseledelse i samråd med kraftforsyningens ulike distriktssjefer. Samlet sett er Norge delt inn i tretten ulike kraftdistrikter, der hvert distrikt har en distriktssjef. På fylkesnivå inngår flere av nettselskapene også i fylkesberedskapsrådet (FBR), hvor den samfunnsmessige beredskapen koordineres og organiseres i samspill med andre samfunnskritiske aktører.

På overordnet nivå er det Statnett som er ansvarlig for å forvalte og drifte det riksdekkende sentralnettet. Nettselskapene, ut over Statnett, har på sin side ansvaret for å forvalte og drifte de regionale og lokale distribusjonsnettene. I grensepunktet mellom sentralnettet og de regionale distribusjonsnettene ligger transformatorstasjonene. Transformatorstasjonene omformerer spenningen på strømnettet fra et nivå til et annet, og er kritiske for transmisjonen av strøm fra sentralnettet til distribusjonsnettene. En svikt i en transformatorstasjon kan med andre ord få større ringvirkninger for leveransesikkerhet i et definert område og utgjør en potensiell sårbarhetsflate for det samlede kraftsystemet. For øvrig er den lokale kraftforsyningen til en viss grad sårbar for naturhendelser, ekstremvær og fysiske enkeltpåkjenninger. Eksempelvis ved at trefall eller krevende værforhold kan skape utfordringer for kraftleveransene innenfor avgrensede geografiske områder. Nettselskapene har imidlertid bygd inn en viss grad av redundans i leveransekjedene og informanten fremhever at det stort sett alltid vil være mulig å rute om forsyningen gjennom en alternativ forsyningsvei, dersom en leveransetrasé i det regionale distribusjonsnettet skulle svikte. Videre er nettselskapene dimensjonert med reservedeler og kritiske kraftkomponenter og har – basert på underliggende risikovurderinger – bygd inn redundans i nettanleggene for å raskt kunne gjenopprette kraftforsyningen ved lokale bortfall.

Sett opp mot den sikkerhetspolitiske situasjonen har de foreliggende trusselvurderingene ikke indikert at kraftanleggene er særlig utsatt for terrorisme eller fysisk sabotasje per dags dato. På den andre siden løftes imidlertid kartlegging og rekognoseringsvirksomhet rundt sentrale anlegg frem som en aktuell sikkerhetsutfordring. Som følger har flere nettselskap derfor iverksatt en rekke ulike tiltak for å redusere den utenlandske etterretningsrisikoen. Som KBO-enhet er Elvia eksempelvis underlagt et strengt regelverk for sikring av kraftsensitiv

informasjon, samtidig som det også gjennomføres bakgrunnssjekker av alle som ansettes i nettselskapet for å redusere innsiderisikoen. Videre beskriver informanten at kraftforsyningen står ovenfor et sammensatt IKT-risikobilde med høy aktivitet. I den forbindelse fremheves viktigheten av at nettselskapene sikrer et høyt sikkerhetsnivå rundt driftskontrollsystemene og ivaretar de digitale sårbarhetsflatene

Sett opp mot samfunnsdigitaliseringen beskriver informanten at det naturligvis vil følge en bredere sårbarhetsflate i kjølvannet av den digitale utviklingen. Kraftforsyningen opererer imidlertid med to forskjellige typer systemer. Herunder skal driftskontrollsystemene ivareta den daglige driften av selve kraftforsyningen, mens de administrative systemene skal ivareta den digitale samhandlingen med kunder og andre samarbeidspartnere. Som en konsekvens av at driftskontrollsystemene er mest kritiske for den daglige driften stilles det naturligvis strengere krav til overvåkning og beskyttelse av driftssystemene. En svikt her vil raskt kunne få ringvirkninger og skape utfordringer for forsyningssikkerheten. Som følge av økende digitalisering og automatisering har den teknologiske utviklingen utløst et økt behov for sensorer og overvåkningsmekanismer tilknyttet anleggene, og et bredere fokus på integrerte sikkerhetsløsninger og datasikkerhet på individnivå. Sett opp mot de administrative systemene har det samtidig oppstått et større behov for tilgang til og utveksling av data med samarbeidspartnere og tredjeparter. Den økende digitale informasjonsutvekslingen kan på sin side utfordre kraftberedskapsforskriftens krav til effektiv beskyttelse av kraftsensitiv informasjon.

Som en konsekvens av den omfattende samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen legger informanten til grunn at det vil bli et økt fokus på personsikkerhet, personkontroll ved rekruttering og ansvarliggjøring ved bruk av konsulenter og underleverandører i tiden fremover. I takt med kraftforsyningens økende avhengighet til underliggende leverandørkjeder har behovet for eksterne supporttjenester samtidig vokst seg større. Videre kan bruken av underleverdører raskt utvikle seg til et risikoelement dersom kraftforsyningen i for stor grad gjør seg avhengig av en enkeltstående leverandørkjede. På denne måten vil en svikt eller potensielle sikkerhetshull hos de underliggende leverandørkjedene indirekte kunne skape ringvirkninger for Elvias operasjonelle drift. Samtidig vil det raskt oppstå sikkerhetsutfordringer dersom en av underleverandørene blir kompromittert eller tilgangen på supporttjenester forsvinner. Leverandørkjedene vil heller ikke være underlagt kraftberedskapsforskriftens lovfestede sikkerhetskrav, og nettselskapene

må derfor være påpasselige med å videreføre de samme kravene gjennom sine bestillinger og anskaffelser, og følge opp at kravene etterleves gjennom revisjoner og tilsynsvirksomhet.

All den tid kraftforsyningen utgjør en kritisk samfunnsfunksjon vil en vedvarende svikt i driftssystemene eller et bortfall av kraftleveransene kunne få store ringvirkninger på samfunnsnivå. For å identifisere og avdekke potensielle sårbarhetsflater ved leveransesystemet jobber Elvia med sikkerhetsstyringen gjennom øvelser, tester, gjennomganger og revisjoner. Videre ivaretas sikkerhetsmålsetningene i stor grad gjennom oppfølging av kraftberedskapsforskriften og energilovens sikkerhetskrav, implementasjon av nødvendige sikringstiltak og oppfølging av relevante trusselvurderinger. Som nettselskap er Elvia også medlem av KraftCERT som er kraftsektorens cyberresponsmiljø og har ansvaret for å overvåke norske energiselskapers IT-systemer og håndtere uønskede IT-sikkerhetshendelser.

5.2.3 – Informant fra FFI

For å belyse den sikkerhetspolitiske situasjonen og de geopolitiske urolighetens konsekvenser for den norske samfunnssikkerheten ønsket jeg også å gjennomføre et intervju med en informant tilknyttet FFI. Som forsvarssektorens egen forskningsinstitusjon utgjør FFI et faglig anerkjent forskningsinstitutt med militær og politisk innsikt, og et solid faglig fundament for å beskrive sivilsamfunnets sikkerhetsutfordringer. Følgelig tok intervjuet i større grad sikte på å belyse den sikkerhetspolitiske utviklingens konsekvenser for samfunnssikkerheten på et overordnet nivå og baserte seg på intervjuguiden i vedlegg 4. Informanten jobber som seniorforsker ved FFI og har fra tidligere bred erfaring med energi- og teknologiutvikling knyttet til totalforsvaret av storsamfunnet. Første del av intervjuet omhandlet utviklingen i trusselbildet mot norske sikkerhetsinteresser, del to gikk nærmere inn på utviklingen i trusselbildet mot og sårbarhetsflatene ved norsk kraftforsyning, mens del tre sluttelig fokuserte på hvordan identifiserte sårbarhetsflater kan reduseres.

Innledningsvis beskrev informanten, med henvisning til nasjonale trusselvurderinger fra Etterretningstjenesten, NSM og PST, at trusselbildet mot norske sikkerhetsinteresser naturligvis har endret seg fundamentalt i kjølvannet av Russlands krig mot Ukraina. Den pågående energikrisen i Europa, i kombinasjon med en omfattende samfunnsdigitalisering, har samtidig skapt betydelig usikkerhet rundt fremtidens sikkerhetsutfordringer og stor uforutsigbarhet knyttet til den sikkerhetspolitiske situasjonen. Usikkerheten utgjør på flere

måter en sikkerhetsutfordring i seg selv, og som en konsekvens av den raske samfunnsutviklingen har man ikke fullstendig oversikt over alle potensielle sikkerhetshull ved de kritiske systemene samfunnet baserer seg på. Dette skaper et mulighetsrom for aktuelle trusselaktører, og gjør det svært krevende å forutse hvordan ulike stater og grupperinger vil agere i fremtidige scenarioer. Sett opp mot den norske samfunnssikkerheten foreligger det relativt bred enighet blant sentrale nasjonale sikkerhetsforum om at det er Kina og Russland som markerer seg som de største interstatlige trusselaktørene gjennom ulike former for etterretningsvirksomhet. Samtidig har den sikkerhetspolitiske utviklingen reist en rekke nye problemstillinger uten definerte fasitsvar. Eksempelvis foreligger det stor usikkerhet knyttet til hvordan et større digitalt tilslag vil tolkes i lys av NATOs artikkel 5 om gjensidig bistand og forsvarsplikt.

Som kritisk samfunnsfunksjon utgjør kraftforsyningen en kompleks sårbarhetsflate med potensiale for store ringvirkninger og massive konsekvenser på samfunnsnivå. Til tross for en i utgangspunktet robust forsyningssikkerhet ved normalsituasjoner, vet man mindre om hvordan kraftforsyningen vil ivaretas under en krisesituasjon. Videre vil den tiltagende internasjonaliseringen og integreringen mot utenlandske kraftmarkeder bidra til at norsk kraftforsyning i større grad påvirkes av sikkerhetspolitiske forhold utenfor Norges egne grenser. For eksempel ved at sikkerhetstruende hendelser i naboland vil kunne få en større innvirkning på den norske forsyningssikkerheten, eksempelvis gjennom det nordiske kraftsamarbeidet. Informanten spår videre at de internasjonale avhengighetene vil vokse i tiden fremover, i takt med nye og oppdaterte avtaler om klimamål og økt elektrifisering.

Stadig tettere koblinger mellom kritiske samfunnsfunksjoner og infrastrukturer gjør det samtidig krevende å se rekkevidden av ringvirkningene ved en svikt i kraftforsyningen. Informanten fremhever følgelig at det blir enda viktigere å sikre latente sikkerhetshull i kraftforsyningens systemer. På den andre siden legger informanten til grunn at potensielle trusselaktører også er bevisste på det norske samfunnets sikkerhetskritiske avhengigheter, og formentlig har utviklet god innsikt i aktuelle sårbarhetsflater ved den norske samfunnssikkerheten. I nyere tid har man eksempelvis observert en bred fremvekst av hybride trusler der sammensatte virkemidler benyttes koordinert mot konkrete sårbarheter for å fremme trusselaktørens strategiske og politiske mål. Herunder kan aktuelle målsetninger ved et angrep mot den norske kraftforsyningen eksempelvis være å lamme den norske økonomien,

teste beredskapen, skape uro i befolkningen, kartlegge sentrale nettanlegg, skade infrastrukturen eller å redusere forsvarsevnen.

Sett i sammenheng med samfunnsdigitaliseringen beskriver informanten at den digitale utviklingen naturligvis vil bidra til effektivisering og forretningsmessige gevinster i hverdagen, men potensielt også kan komplisere beredskapsarbeidet og krisehåndteringen, eksempelvis ved å utfordre kraftrasjoneringen. I tråd med eksisterende kriseplaner vil kraftforsyningen, ved større tilfeller av strømunderskudd, rasjoneres til et begrenset område av gangen og deretter flyttes fra område til område. Som følge av den omfattende digitaliseringen har samfunnet imidlertid gjort seg avhengig av kontinuerlig strømtilførsel på et bredt spekter av arenaer og det vil ikke lenger være like enkelt å isolere kraftforsyningen til et enkelt område av gangen. Herunder vil for eksempel «smarte hjem», ulike former for elektroniske kommunikasjonstjenester og tilgangen til internett stille krav til en vedvarende kraftforsyning. Til tross for at visse kritiske samfunnsfunksjoner har tilgang på nødaggregater, vil de færreste virksomheter klare seg særlig mye lenger enn tre døgn uten en ekstern strømtilførsel. Over tid vil en svikt i leveransesikkerheten med andre ord få store ringvirkninger, utfordre responsevnen for responderende beredskapspersonell og raskt gå utover funksjonsevnen til øvrige kritiske samfunnsfunksjoner. På denne måten bidrar samfunnsdigitaliseringen til at spekteret mellom normalsituasjonen og krisesituasjoner øker.

I takt med internasjonaliseringen og den digitale omstillingen vil samfunnet samtidig utvikle kritiske avhengigheter til den globale verdenshandelen og underleverandører av materialer og komponenter vi ikke produserer selv. Til tross for at teknologien i dag er svært utbredt, er det kun et fåtall land som faktisk produserer de nødvendige komponentene som kreves i en digital hverdag. Herunder er det eksempelvis lang leveringstid på visse kritiske komponenter som behøves i transformatorstasjoner. Leveringstiden kan bli ytterligere forlenget som følge av krigen i Ukraina og den etterfølgende gjenoppbygging av kritisk infrastruktur. Videre er det heller ikke gitt at alle underleverandørene vil være villig til å forsyne oss med materialene vi behøver ved en potensiell internasjonal konfliktsituasjon. Det kan for eksempel tenkes at kritiske leverandører, gjennom flere ledd, har en tilknytning til statlige aktører Norge og vesten havner i konflikt med. Forsyningslinjene vil samtidig være sårbare for krig, konflikt og sikkerhetspolitiske uroligheter og de underliggende verdikjedene vil på denne måten utgjøre en potensiell sårbarhetsflate for den helhetlige samfunnssikkerheten.

For å redusere og begrense aktuelle sårbarhetsflater i kraftforsyningen løfter informanten frem behovet for samarbeid og kommunikasjon. Dersom de ulike virksomhetene jobber etter sektorprinsippet og ikke utveksler informasjon om løsningsforslag og sikkerhetstiltak, kan man i verste fall risikere at løsningene motvirker hverandre og skape utfordringer for den overordnede sikkerhetsstyringen. I takt med nye klimamål og økende internasjonalisering er man også avhengig av felles løsninger på tvers av landegrenser. For å finne frem til aktuelle løsningsforslag er man nødt til å etablere en oversikt over de ulike sammenkoblingene og sikkerhetskritiske avhengighetene samfunnsfunksjonene har utviklet til hverandre. For å håndtere sårbarhetene stilles det videre krav til en helhetlig sikkerhetsstrategi, bred samhandling og et tilstrekkelig sikkerhetsfokus. På den andre siden er risikoen, i takt med økende privatisering av samfunnsfunksjonene, at det kortsiktige økonomiske bildet prioriteres fremfor langsiktige sikkerhetsløsninger. På denne måten utgjør profittmaksimering og kostnadsbesparende løsninger et sikkerhetskritisk dilemma for samfunnssikkerheten og de ulike samfunnsfunksjonene.

5.2.4 – Informant tilknyttet den digitale sikkerhetssektoren

For å belyse dagens digitale risikobilde mot norske samfunnsfunksjoner på et overordnet nivå ønsket jeg å supplere dokumentanalysen og gjennomføre et kvalitativt intervju av en informant med tilknytning til den digitale sikkerhetssektoren. Intervjuet baserte seg på den samme intervjuguiden som lå til grunn ved intervjuet av informanten fra FFI, men tok i større grad form av et ustrukturert intervju der informanten vektla de digitale aspektene vedkommende innehar bred innsikt i og i mindre grad uttalte seg om de geopolitiske faktorene og den sikkerhetspolitiske situasjonen. Intervjuet tok først og fremst sikte på å kartlegge utviklingen i det digitale trusselbildet og beskrive risikobildet mot norsk kraftforsyning, sett i lys av den omfattende samfunnsdigitaliseringen. Fra tidligere har informanten lang erfaring med digitalt sikkerhetsarbeid i privat sektor og generelt en bred innsikt i utvalgte deler av oppgavens tematikk. Informanten ønsket imidlertid ikke å presenteres eller identifiseres med virksomheten vedkommende jobber i. Videre presiserte informanten at han i utgangspunktet kun ønsket å besvare spørsmål av mer generell karakter og ikke ville ha anledning til å bevege seg inn på mer sensitive temaer. Basert på erfaring og utdanningsnivå vurderes informanten likevel å inneha et solid faglig grunnlag for å svare ut definerte informasjonsbehov.

Sett opp mot utviklingen i trusselbildet mot norske sikkerhetsinteresser beskriver informanten at Norge i tiden fremover vil stå ovenfor et mer uforutsigbart sikkerhetspolitisk bilde enn man

har gjort på mange år. I takt med en skjerpet sikkerhetspolitisk situasjon vil norske sikkerhetsinteresser naturligvis utfordres og det må forventes at utenlandske trusselaktører vil benytte seg av en rekke virkemidler for å fremme sine interesser på Norges bekostning. Samtidig vil den teknologiske utviklingen og hurtige samfunnsdigitaliseringen bidra til at samfunnets sårbarheter blir mer komplekse, at virksomhetene i større grad blir nødt til å basere seg på underleverandører og uoversiktlige verdikjeder og at angrepsflaten for potensielle trusselaktører utvides. Som en konsekvens risikerer man at gapet mellom aktuelle trusler og det nødvendige digitale sikkerhetsnivået i samfunnet øker.

I takt med at samfunnet og kritiske samfunnsfunksjoner i stadig større grad baserer seg på underleverandører og digitale verdikjeder vil aktuelle sikkerhetshull hos underleverandørene med andre ord integreres som en del av den respektive samfunnsfunksjons sårbarhetsflater. Når det er sagt beskriver informanten at de samfunnsmessige og samfunnsøkonomiske gevinstene ved tjenesteutsetting, automatiseringen, digitalisering og sammenkoblingen av systemer er for store til at noen virksomhet er tjent med å jobbe mot utviklingen, til tross for at den raske utviklingen naturligvis åpner for en langt bredere eksponering mot digitale trusler. Fra et overordnet perspektiv ser man imidlertid at den store majoriteten av sikkerhetstruende cyberhendelser og dataangrep mot norske virksomheter baserer seg på menneskelig feil og sviktende sikkerhetsrutiner, som utnyttes av ondsinnede aktører. Følgelig vil relativt enkle sikkerhetstiltak, den enkelte ansattes sikkerhetsbevissthet og stimulering mot en god sikkerhetskultur i mange tilfeller kunne gi en betydelig sikkerhetsgevinst for virksomheten i sin helhet. Videre foreligger det en risiko for at de digitale truslene og sårbarhetsflatene i flere tilfeller oversees og nedprioriteres i det forebyggende sikkerhetsarbeidet, som en konsekvens av manglende forståelse og kompetanse på området og økonomisk kostbare sikkerhetssystemer. Informanten illustrerer problemstillingen med at det ofte er lettere å se rekkevidden av konsekvensene og ringvirkningene av fysiske trusler og farer enn rendyrkede digitale sikkerhetstruende hendelser. Aktuelle sikkerhetstiltak bør med andre ord baseres på underliggende risikoanalyser, heller enn unøyaktige risikoforestillinger.

Når det er sagt beskriver informanten at ringvirkningene fra digitale angrep, i en verden hvor cyber-fysiske systemer blir stadig mer integrert, er svært uoversiktlige og i mange tilfeller kan bli enorme. Uten at informanten har direkte erfaring med kraftforsyningen som samfunnsfunksjon beskriver vedkommende at kraftforsyningen, som alle andre samfunnsfunksjoner og moderne virksomheter, formentlig har utviklet en rekke

sikkerhetskritiske avhengigheter til sine digitale driftssystemer. Med andre ord vil et omfattende cyberangrep i stor grad kunne påvirke og forstyrre kraftforsyningens systemdrift og daglige funksjon. Samtidig har man, i takt med at stadig flere systemer integreres mot det åpne nettet, observert en vedvarende økning i det voksende spekteret av mulige digitale angrepsmetoder og kompetente digitale trusselaktører. Sett i lys av den sikkerhetspolitiske utviklingen frykter man på generelt nivå at norske virksomheter og kritiske samfunnsfunksjoner utsettes for omfattende anslag med potensiale for massive skadevirkninger på samfunnsnivå. Herunder vises det til flere av de avanserte og sofistikerte cyberangrepene russisk etterretningstjeneste og underliggende grupperinger har utført mot Ukraina i løpet av de siste årene, hvor enkelte av angrepne også har bidratt til å slå ut deler av kraftsystemet.

For å redusere og begrense de digitale sårabarhetsflatene som følger i kjølvannet av den omfattende digitaliseringen og forbygge skadevirkningene ved potensielle anslag fremhever informanten betydningen av den tekniske arkitekturen, robuste datanettverk, tilstrekkelig med digitale sikkerhetstiltak og behovet for kompetent IKT-personell med evne til å tolke trusselbildet og monitorere systemdriften. Samtidig understrekes viktigheten av en helhetlig digital sikkerhetsstrategi, effektiv informasjonsflyt og en oversikt over potensielle sikkerhetshull og underleverandører. Til tross for en observert økning i omfanget av komplekse cyberangrep, legger informanten til grunn at driftssystemene i mange tilfeller vil være godt sikret mot digitale angrep, men at systemoperatørene eller den enkelte ansatt som regel vil være enklere å «manipulere». Således vil relativt simple angrepsmetoder eller latente sårbarheter som utdatert programvare og svake passord i mange tilfeller ligge til grunn for cyberangrep med potensielt store konsekvenser for den enkelte virksomhet. Det må derfor stilles krav til at virksomhetene sikrer tilstrekkelig opplæring, digital kompetanseheving, nødvendig utstyr og at det føres jevnlig tilsyn med definerte sikkerhetskrav og aktuelle sikkerhetstiltak.

På den andre siden understreker informanten at flere sikkerhetstiltak i mange tilfeller også kan føre til økt kompleksitet og utfordre brukervennligheten ved systemene. Redusert brukervennlighet kan på generelt grunnlag komplisere systemdriften for operatørene og gå utover driftseffektiviteten. Videre er en naturlig konsekvens av redusert brukervennlighet at operatørene finner egne snarveier som igjen åpner opp for nye risikoer og sårbarheter. Samlet sett er det altså vesentlig at en finner frem til en balansegang mellom akseptert risiko,

nødvendige sikkerhetstiltak og brukervennlige systemer. Flere sofistikerte sikkerhetstiltak vil samtidig medføre en stor økonomisk kostand og det bør følgelig gjennomføres kostnad-nytte analyser for å finne frem til hvilke risikoer som kan aksepteres og hvilke som i større grad bør håndteres, på bakgrunn av trusselbildet og aktuelle kilder til risiko.

6.0 – DRØFTELSE

I tråd med en abduktiv forskningsstrategi vil det innsamlede datamaterialet og funnene fra de foreliggende empiriske undersøkelsene sees i sammenheng med oppgavens teoretiske rammeverk, samfunnsmessige kontekst og drøftes opp mot den overordnede problemstillingen. Den faglige diskusjonen vil videre ta utgangspunkt i en kombinasjon av teori og empiri hvor det trekkes paralleller mellom innsamlede data og presentert teori for å belyse oppgavens forskningsspørsmål. Herunder vil jeg innledningsvis beskrive kraftforsyningen som kritisk samfunnsfunksjon og drøfte hvorvidt kraftsektorens visjoner og endrede rammebetingelser påvirker sikkerheten rundt kraftforsyningen. Videre vil jeg beskrive kraftforsyningen som et komplekst system og trekke paralleller til sentrale teoretiske bidrag på feltet. Med utgangspunkt i kraftforsyningens kompleksitet og endrede rammebetingelser vil jeg deretter drøfte hvordan et skjerpet trusselbilde, tiltagende digitalisering og nye rammebetingelser bidrar til å forsterke og skape nye sårbarhetflater for kraftforsyningen som system. Sluttelig vil jeg diskutere hvordan identifiserte sårbarheter kan reduseres gjennom ulike former sikkerhetstiltak, barrierer og prosedyrer. Sett i lys av oppgavens problemstilling ønsker jeg gjennom den faglige diskusjonen å belyse hvordan sikkerheten rundt kraftforsyningen påvirkes av samfunnsdigitaliseringen innenfor rammene av den sikkerhetspolitiske situasjonen og hvilke ringvirkninger utviklingen kan få på samfunnsnivå.

6.1 – Kraftforsyningen som samfunnsfunksjon – rammebetingelser og visjoner

Til grunn for kategoriseringen av kritiske samfunnsfunksjoner ligger premisset om at et bortfall i løpet syv døgn eller mindre vil true befolkningens grunnleggende behov og samtidig utfordre landets beredskapsressurser i løpet av samme periode (DSB, 2016, s. 7-20). Som en kritisk samfunnsfunksjon ligger kraftforsyningen til grunn for at flere av landets øvrige samfunnsfunksjoner skal kunne opprettholde sin funksjonsevne i det daglige. Videre er samfunnet helt avhengig av en trygg og stabil kraftforsyning for å dekke et bredt spekter av

befolkningens essensielle behov som varme, produksjon, transport og kommunikasjonsmuligheter. En omfattende svikt eller et lengre bortfall vil dermed få umiddelbare konsekvenser og i løpet av kort tid føre til store forstyrrelser i samfunnet. Herunder utgjør kraftforsyningen og leveransesikkerheten en helt essensiell forutsetning for blant annet opprettholdelsen av stabile helsetjenester, elektronisk kommunikasjon, nødvendig IKT-sikkerhet og befolknings behov for øvrig. Med andre ord representerer kraftforsyningen en integrert, sikkerhetskritisk forutsetning for flere av landets øvrige kritiske samfunnsfunksjoner og infrastrukturer. Et bortfall i leveransesikkerheten vil dermed kunne få massive ringvirkninger for storsamfunnet i sin helhet og som følge av kraftsektorens samfunnskritiske funksjon stilles det naturligvis respektive strenge krav til sikkerhetsstyringen av kraftforsyningen som system (DSB, 2016, s. 9-15).

I lys av oppgavens kontekst gir informanten fra Norges vassdrags- og energidirektorat tydelig uttrykk for at den digitale infrastrukturen rundt kraftsystemet har ekspandert betraktelig i takt med den økende samfunnsdigitaliseringen. Til tross for at den digitale omstillingen på den ene siden fremheves som et utviklingsideal, er informantene som har bidratt til oppgaven omforente om at kompleksiteten i systemene og angrepsflaten for potensielle trusler vil utvides. Blant annet som en konsekvens av den brede eksponeringen mot det åpne nettet og den økte integrasjonen av cyber-fysiske systemer. En større angrepsflate vil være vanskeligere å sikre og samtidig medføre en utvidet sårbarhetsflate for kraftforsyningen som kritisk samfunnsfunksjon. Samtidig er informantene samstemte om at den sikkerhetspolitiske situasjonen og de geopolitiske urolighetene som følger i kjølvannet av Russlands angrepskrig mot Ukraina, vil utgjøre en vesentlig faktor med betydelig innvirkning på sikkerhetsstyringen av kraftforsyningen som samfunnsfunksjon. Herunder presiseres det at dagens sikkerhetspolitiske spenninger har medført en drastisk tilspisning i trusselbildet mot norske samfunnsfunksjoner og infrastrukturer generelt, samtidig som den europeiske energikrisen har bidratt til å skjerpe trusselbildet mot norsk kraft- og energisektor spesielt.

Sett i sammenheng med modell for sikkerhetsstyring presentert tidligere i oppgaven kan kraftforsyningen som system deles opp i de tre grunnleggende elementene *rammebetingelser, visjon og tiltak* (Njå et. al, 2021, s. 67). Den uttalte hovedvisjonen ved kraftforsyningen som system er som nevnt å ivareta samfunnets behov for elektrisk energi. Herunder stilles det lovfestede funksjonskrav til kraftforsyningens ytelse og det forventes kontinuerlig tilgjengelighet, stabil drift og effektiv sikring mot sikkerhetstruende hendelser

(Kraftberedskapsforskriften, 2012). Som ansvarlig fagdirektorat for norsk kraftforsyningsberedskap er det NVE som innehar det overordnede operative ansvaret for å forvalte den norske forsyningssikkerheten og sikre at kraftsektoren drives i tråd med retningsgivende visjoner. Videre skal NVE legge til rette for at kraftforsyningen opprettholder og gjenoppretter normal drift under og i etterkant av ekstraordinære hendelser. Når det er sagt åpner kraftberedskapsforskriften (2012) opp for at den enkelte KBO-enhet i betydelig grad kan utvikle sikkerhetssystemer og tiltak basert på identifiserte risikoer og funksjonelle målsetninger, heller enn detaljstyrte lovkrav (NOU 2015:13, s. 110-111).

Som system må Kraftforsyningen imidlertid tilpasses til og harmonere med rammebetingelsene systemet er undergitt. I intervjuene beskriver enkelte av informantene at utenforliggende forhold som miljøbetingelser, topografiske forhold og klimaendringer utgjør rammebetingelser som under ulike omstendigheter kan virke negativt inn på driftssikkerheten, eksempelvis gjennom fysiske påkjenninger som naturhendelser, ekstremvær og tekniske svikter. På den andre siden utgjør mindre håndfaste forhold som geopolitiske faktorer, endringer i trusselbildet og digital utvikling et annet sett med rammebetingelser NVE er nødt til å forholde seg til og dimensjonere for i det beredskapsforbedrende arbeidet. På bakgrunn av definerte visjoner og identifiserte rammebetingelser skal NVE, som ansvarlig forvalter, opprettholde og videreutvikle et akseptabelt sikkerhetsnivå i overensstemmelse med de etablerte sikkerhetsmålene, gjennom ulike former for tilsynsvirksomhet, sikringstiltak og barrierer. Sikkerhetstiltakene skal blant annet bidra til å bygge opp under og videreutvikle sikkerhetsmålsetningene for kraftsektoren innenfor rammene av ovennevnte rammebetingelser og tar form av både teknisk, juridisk og organisatorisk karakter.

Når det er sagt slår flere av informantene og Forsvarets Forskningsinstitutt – gjennom BAS3-prosjektet om aktuelle sårbarheter ved kraftforsyningen – mer eller mindre fast at kraftsektoren i stor grad er svært redundant mot fysiske påkjenninger. Herunder vises det til at kraftproduksjonsanleggene er dimensjonert slik at det normalt må en krigstrussel til for å ødelegge deres produksjonskapasitet, samtidig som leveransesikkerheten er beskyttet mot ekstreme værbelastninger og fysiske påkjenner gjennom alternative og redundante leveransetraséer inn mot befolkningstette områder (FFI, 2001, s. 14-15). Med andre ord kan det legges til grunn at kraftsystemet i all hovedsak er lite sårbart stilt ovenfor tradisjonelle safety-risikoer som ekstremvær, naturkatastrofer og ulykker. Stilt ovenfor tilsiktede anslag utført av dynamiske trusselaktører, målrettet mot systemets svakheter vil kraftforsyning

imidlertid inneha en vesentlig større sårbarhetsflate. Til tross for at den omfattende samfunnsdigitaliseringen i all hovedsak har bidratt til å effektivisere den daglige driften og åpnet for praktiske løsninger, påpeker enkelte av informantene at den digitale utviklingen samtidig har medført et stort sårbarhetspotensial. All den tid kraftforsyningen utgjør et «just in time»-system med tidsavhengige prosesser vil et målrettet tilslag på denne måten kunne forårsake en kaskade av eskalerende feil som vil kunne spre seg momentant på uforutsette måter. Som en konsekvens av de gjensidige avhengighetene ulike samfunnssektorer i mellom, vil en omfattende svikt i kraftsektoren samtidig kunne forårsake alvorlige ringvirkninger for tilknyttede samfunnsfunksjoner, infrastrukturer og samfunnsviktige systemer generelt (DSB, 2016, s. 86-89; FFI, 2001, s. 14-16).

Til tross for nye sårbarhetsflater og økende eksponering mot det åpne nettet påpeker Justis- og beredskapsdepartementet likevel i sin NOU (2015:13, s. 142-144) om digital sårbarhet at de administrative og forretningsmessige gevinstene ved integrasjonen av de ulike systemene er for store til at utvalget foreslår å jobbe mot utviklingen. Anbefalingen samsvarer med informantenes uttalelser om de positive driftseffektene ved automatisering av manuelle arbeidsoppgaver og økt integrasjon av cyber-fysiske systemer. NVE (2022, s. 8-10) fremhever imidlertid at digitaliseringsrisikoen som følger i kjølvannet av den digitale utviklingen og endrede digitale rammebetingelser spesielt knytter seg til tre ulike forhold. Herunder vises det til den økende sikkerhetskritiske avhengigheten samfunnet har utviklet til komplekse systemer, det voksende spekteret av nye angrepsmetoder og ressurssterke trusselaktører og de store sikkerhetskritiske avhengighetene som har oppstått mellom de ulike virksomhetene som drifter kritiske samfunnsfunksjoner og kritiske infrastrukturer. Sett i lys av dagens tilspissede trusselbilde kan samfunnsdigitaliseringen dermed sies å ha bidratt til å åpne opp for et nytt spekter av effektive angrepsmetoder med potensiale for massive og uforutsigbare skadevirkninger på samfunnsnivå. Samtidig påpeker informanten fra FFI at samfunnets voksende avhengighet til kontinuerlig strømtilførsel videre kan komplisere beredskapsarbeidet under krisesituasjoner, og raskt gå utover funksjonsevnen til respondere beredskapspersonell ved en svikt.

6.2 – Kraftforsyningen som komplekst system

Som kritisk samfunnsfunksjon utgjør kraftforsyningen i sin helhet et komplekst system av ulike komponenter og enheter med tidsavhengige prosesser og begrenset mulighet til improvisering når systemet først er i drift. I likhet med andre tett koblede systemer eksisterer

det naturligvis en rekke latente sårbarheter i- og omkring kraftforsyningen som leveransesystem. Potensielle sårbarheter vil kunne ligge til grunn for uønskede hendelser og kan på denne måte virke inn på kraftforsyningens sikkerhetsstyring og evne til opprettholdelse av sikker drift. Sett fra Perrows deterministiske perspektiv vil digitaliseringen – utover å effektivisere kraftforsyningen og samfunnsfunksjonene for øvrig – samtidig føre med seg en rekke nye sårbarhetsflater som vanskelig kan forebygges fullstendig. Herunder vil Perrows (1999) teori om «normale ulykker» kunne bidra til å underbygge aktuelle utfordringer i den digitale sikkerhetsstyringen. All den tid kraftforsyningen i stor grad baserer seg på cyber-fysiske systemer, som eksempelvis industrielle kontrollsystemer, vil det helhetlige kraftsystemet følgelig inneha en rekke tette koplinger og komplekse interaksjoner. Når kraftforsyningen først er i drift stilles det krav til at systemet virker i en sekvensiell struktur i et gitt mønster for å oppnå ønsket resultat. Sett fra et overordnet perspektiv kan de ulike samfunnsfunksjonene videre sies å utgjøre et komplekst «system av systemer» og feil et sted i kjeden vil dermed inneha et stort eskaleringspotensial og raskt kunne forplante seg til øvrige tilknyttede samfunnskjoner og infrastrukturer (NOU 2015:13).

I denne komplekse strukturen tar NAT-teoriene utgangspunkt i at uønskede hendelser ikke bare er uunngåelig, men også må anses som «normalt». Implementeringen av ytterligere sikkerhetstiltak og barrierer vil etter Perrows syn samtidig kunne forsterke systemets kompleksitet og i enda større grad bidra til å gjøre systemet opakt for operatørene. Momentene samsvarer med uttalelsene fra informanten tilknyttet den digitale sikkerhetssektoren, som vektlegger at flere sikkerhetstiltak i mange tilfeller vil føre til økt kompleksitet og utfordre brukervennligheten. En redusert brukervennlighet vil videre kunne gå på bekostning av driftseffektiviteten og bidra til at systemoperatørene finner snarveier som igjen åpner opp for nye risikoer. Til tross for at Perrows NAT-teorier i utgangspunktet henviser til større industriulykker er det nærliggende å legge til grunn at systemteoriene også vil ha overføringsverdi i møte med dynamiske trusselaktører og utpregede security-trusler. Blant annet ved at kraftforsyningens kompleksitet og tette koblinger naturligvis vil kunne bidra til å forsterke ringvirkningene ved et potensielt målrettet tilslag, og samtidig problematisere arbeidet med å identifisere aktuelle feilkilder og sårbarhetsflater innad i systemet. Herunder vil kraftforsyningens komplekse interaksjoner med andre systemer og kritiske samfunnsfunksjoner bidra til å komplisere sikkerhetsstyringen ytterligere og på denne måten utfordre samfunnssikkerheten (Perrow, 1999, s. 70-80).

Forsøk på uautorisert inntrenging, nettverksoperasjoner, verdikjedeangrep eller digital sabotasje utgjør alle eksempler på opptakten til mulige «kjernehendelser» NVE og aktuelle KBO-enheter aktivt må jobbe mot å forebygge i sin sikkerhetsstyring av kraftsystemet. Som følge av kraftforsyningens tette koblinger og sikkerhetskritiske funksjon vil et vellykket anslag kunne få enorme konsekvenser på samfunnsnivå. Som en motpol til NAT-teoriene poengterte imidlertid Roe & Schoulman (2008, s. 53-55) gjennom sine HRO-teorier at høypålitelige organisasjoner kan distansere seg fra uønskede hendelser gjennom fleksibel sikkerhetsstyring, aktiv bruk av redundans og forebyggende tiltak. I motsetning til teorien om normale ulykker har teorien om høypålitelige organisasjoner en optimistisk tilnærming til sikkerhetsstyringen. På overordnet nivå viser HRO-teorien til grunnleggende prinsipper høypålitelige organisasjoner bør integrere i sikkerhetsstyringen for å forebygge og forhindre uønskede hendelser i høyteknologiske systemer. Herunder fremheves organisatoriske betingelser som en integrert pålitelighetskultur, høy ytelse, bred teknologisk kompetanse, fleksible lederstrukturer og sterk sikkerhetskultur. Samtidig forutsetter HRO-teoriene at sikkerhet gis høyeste prioritet og at upålitelige enkeltkomponenter beskyttes gjennom overlapp og redundans (Roe & Schoulman, 2008, s. 52-57).

For kraftforsyningen som system fremhever informantene fra både NVE og Elvia at de har integrert et mangfold av redundante løsninger i dimensjoneringen av leveransesikkerheten og lagt til rette for en tilpasningsdyktig sikkerhetsstrategi i møte med samfunnsdigitaliseringens nye trusler. Herunder vises det til forebyggende tiltak og barrierer som hyppig og tilpasset tilsynsvirksomhet, utvikling av funksjonelle krav til sikkerhet og beredskap, motivasjon og lederskap gjennom helhetlig sikkerhetsstyring, konkret veiledning, grunnsikring for digitale informasjonssystemer, løpende kommunikasjon med KBO-enhetene, stimulering til god sikkerhetskultur og utfyllende trussel- og sårbarhetsvurderinger. Nevnte tiltak harmonerer i stor grad med Kraftberedskapsforskriftens lovfestede krav til sikringstiltak og high relability-teoriens grunnleggende sikkerhetsprinsipper.

6.3 – Utvikling i sårbarhetsflater og trusselbilde

Sett opp mot dagens geopolitiske uroligheter og den sikkerhetspolitiske utviklingen, med tiltagende stormaktsrivalisering og færre diplomatiske arenaer, understreker både PST (2023) og Etterretningstjenesten (2023) at det norske samfunnet i økende grad vil utsettes for ulovlig etterretningsvirksomhet fra autoritære regimer. I den forbindelse pekes Russland ut som den største enkeltstående trusselaktøren mot norske sikkerhetsinteresser i det inneværende året.

Blant annet som en konsekvens av den antatte russiske målsetningen om å sette europeisk energisikkerhet under press. Som følge av norsk energiforsynings voksende sikkerhetspolitiske betydning for Europa påpeker PST (2023) samtidig at aktuelle objekter innenfor norsk kraftsektor utmerker seg som særlig eksponerte mål. Til tross for at den konkrete, fysiske sabotasjerisikoen vurderes som relativt liten bemerkes det at en ytterligere tilspisning av den sikkerhetspolitiske situasjonen er å forvente og at sabotasjehandlinger mot strategiske mål i Norge kan bli et aktuelt scenario dersom Russlands vilje til å eskalere konflikten med NATO og vesten tiltar. I den anledning løftes det digitale domenet frem som en spesielt eksponert angrepsflate for russiske nettverksoperasjoner og digital etterretningsvirksomhet (Etterretningstjenesten, 2023, s. 11-17; PST, 2023, s. 7-23).

I møte med utenlandsk etterretningsvirksomhet og sikkerhetsutfordringene som følger i kjølvannet av dagens geopolitiske uroligheter vil kraftforsyningen i økende grad stå ovenfor målrettede og dynamiske trusselaktører heller enn vilkårlige og ikke-intenderte farer. Fremfor å basere seg på kvantitative risikomodeller vil man i analysen av security-risikoer i større grad ta utgangpunkt i kvalitative trefaktor-modeller. Her vil det det totale risikobildet kunne illustreres ved «risikotrekantens» samlede areal som utgjør skjæringspunktet mellom dimensjonene verdi, trussel og sårbarhet (Heyerdahl, 2022b, s. 254-261). Sett i lys av oppdaterte trusselvurderinger fra relevante statlige sikkerhetsmyndigheter løftes russisk press på norske sikkerhetsinteresser og utenlandsk etterretningsvirksomhet frem som de mest presserende truslene mot det norske storsamfunnet. I tråd med oppgavens kontekst vil systemet og verdiene NVE søker å beskytte gjennom sin sikkerhetsstyring naturligvis være kraftsektoren generelt, og sentrale anlegg og vitale komponenter spesielt. Sluttelig viser sårbarhetsbegrepet i modellen til den forsvarsevnen kraftforsyningen vil være i stand til å møte de identifiserte truslene med og til hvilken grad kraftforsyningen vil kunne utsettes for ekstraordinære hendelser og fremdeles opprettholde normale kraftleveranser (Etterretningstjenesten, 2023; PST, 2023).

Herunder påpeker FFI (2001) gjennom BAS3-prosjektet at den økende avhengigheten til IKT-baserte prosesstyringssystemer, integrasjonen i det europeiske kraftmarkedet, økt kommunikasjons- og sambandsavhengighet og knapphet på spesialkompetanse vil bidra til å ekspandere den totale sårbarhetsflaten for kraftforsyningen som helthetlig system. Videre fremheves de voksende digitale sårbarhetsflatene som de mest eksponerte på bakgrunn av den tiltagende implementeringen av moderne informasjons- og kommunikasjonsteknologi,

driftssystemenes eksponering mot internett og den økende avhengigheten til eksterne underleverandører og utenlandske supporttjenester. Som en konsekvens av at kraftsektoren i stadig større grad baserer seg på tjenesteutsetting og innfløkte verdikjeder i den digitale sikkerhetsstyringen vil kraftforsyningen samtidig arve og absorbere latente svakheter og sikkerhetshull fra underliggende tjenesteleverandører. Spesielt for de digitale verdikjedene er at en svikt har en tendens til å spre seg momentant og tidvis på uforutsigbare måter. Med andre ord vil et bortfall i den underliggende tjenesten potensielt kunne utløse massive ringvirkninger for den digitale verdikjeden i sin helhet og på denne måten også gå utover kraftforsyningens drifts- og datasystemer. All den tid driftssentralene står i kraftforsyningens sentrum vil en vedvarende svikt i driftssystemene raskt kunne påvirke og gå på bekostning av kraftsektorens samlede evne til kraftleveranser (FFI, 2001, s. 18-20; NSM, 2023, s. 7-25; NVE, 2021, s. 33-34).

I NVEs (2022) studie om risikostyring av IKT-sikkerhet i leverandørkjeder tydeliggjøres flere av de dagsaktuelle sikkerhetsutfordringene ved den økende bruken av eksterne leverandører og digital tjenesteutsetting. Herunder beskriver flere av informantene som har bidratt til studien at svakhetene i verdikjedene er krevende å kartlegge og identifisere som et resultat av verdikjedenes voksende kompleksitet. Videre gjør det store mangfoldet av virksomheter som opererer i kraftforsyningen det krevende å legge til rette for at de ulike virksomhetene omforenes om en felles situasjonsforståelse av risikobildet og tar tilstrekkelig eierskap til den eksisterende risikoen. Den økende bruken av fjernaksesstjenester eksponerer samtidig driftssystemene for uautorisert inntrenging og utfordrer kraftberedskapsforskriftens krav til beskyttelse av sensitive data og kontroll med egen informasjon. For å illustrere utfordringen refererer NVE i sin eksternrapport til en forskningsrapport av Ponemon Institute (2019) som konkluderer med at leverandørkjedene var inngangsporten til systemene for angriper ved mer enn 63% av de registrerte dataangrepene i USA. Denne skildringen harmonerer med NSM og PSTs trusselvurderinger som vektlegger at ondsinnede nettverksoperasjonener i hovedsak innledes ved at trusselaktørene utnytter relativt enkle sårbarheter ved systemet som sosial manipulering, utdatert programvare, svake og gjenbrukte passord eller manglende to-faktorautentisering (NSM, 2023, s. 18-23; NVE, 2022, s. 20-26; PST, 2023, s. 15-18)

Sett opp mot Reasons (1997, s. 2-6) teorier om organisatoriske ulykker skyldes uønskede hendelser i komplekse systemer i hovedsak en kombinasjon av aktive, menneskelige feil og underliggende latente forhold ved virksomheten. I den forbindelse vektlegger Reason at

enkeltindividet i mange tilfeller ikke innehar forutsetningene for å lykkes, men likevel blir trukket frem som syndebukker når kriser oppstår. Herunder presiserer Perrow (1999, s. 70) at så lenge mennesker fremdeles ansettes i høyteknologiske systemer vil individuelle feil forekomme. Som ansvarlig forvalter for sikkerhetsstyringen skal NVE imidlertid immunisere systemet mot menneskelige enkeltfeil og opprettholde et sikkerhetsnivå i henhold til etablerte sikkerhetsmålsetninger. I tråd med tradisjonelt samfunnssikkerhetsarbeid sikres målsetningene i stor grad gjennom ulike lag av barrierer og sikkerhetstiltak. Reasons sveitserostmodell problematiserer imidlertid forekomsten av latente feil i et dybdeforsvar. På overordnet nivå legger Reason til grunn at en virksomhet utvikler flere lag av barrierer mellom verdiene virksomheten ønsker å beskytte og identifiserte trusler. Videre er det mangfoldet av de ulike barrierene som i dybden danner systemer som skal beskytte mot uønskede og sikkerhetstruende hendelser. I kombinasjon med aktive feil begått i den «skarpe enden» av virksomheten, er det de latente svakhetene i systemet som vil fremme brudd på optimal praksis og legge til rette for at en potensiell trussel får muligheten til å penetrere seg gjennom kraftforsyningens ulike lag av sikkerhetstiltak (Reason, 1997, s. 5-15).

Sett i sammenheng med kraftsystemet vil sårbarheter oppstå der latente svakheter og underliggende feil får utvikle seg ubemerket i dybdeforsvaret av barrierer. På denne måten legges forholdene til rette for at en mulig uønsket hendelse eller en svikt i leveransesikkerheten får utspille seg. I lys av oppgavens kontekst er det nærliggende å trekke paralleller til sårbarhetsflatene som har fått utvikle seg i kjølvannet av samfunnsdigitaliseringen over tid. Herunder fremhever flere av informantene driftssystemenes økende eksponering mot det åpne nettet som en sikkerhetsutfordring som i kombinasjon med en enkeltfeil fra en systemoperatør vil kunne få massive konsekvenser for driftskontinuiteten, og potensielt gå utover den samlede leveransesikkerheten. I takt med den teknologiske utviklingen løfter NSM (2023, s. 24) samtidig frem viktigheten av enkeltindividets sikkerhetsbevissthet og betydningen av en god sikkerhetskultur på virksomhetsnivå.

All den tid kraftforsyningen vil absorbere potensielle svakheter og sikkerhetshull hos digitale underleverandører er det nærliggende å legge til grunn at det eksisterer en rekke uoppdagede sårbarheter i det digitale dybdeforsvaret. Disse sårbarhetsflatene vil under gitte omstendigheter kunne utnyttes av ondsinnede trusselaktører. Slik vil den digitale transformasjon kunne forsterke de latente sikkerhetshullene i kraftsektorens digitale barrierer,

som i kombinasjon med et tilspisset trusselbilde vil kunne forårsake en total eller delvis penetrasjon av etablerte sikkerhetstiltak. Samtidig fremhever informantene – i tråd med klassiske faktorer innenfor risikopersepsjon – faren ved at de digitale truslene ofte vies mindre oppmerksomhet og nedprioriteres i det forebyggende sikkerhetsarbeidet sammenlignet med konkrete fysiske farer med mer håndgripelige konsekvenser (NVE, 2022, s. 20-26).

Som følge av at cyber-fysiske-systemer i stadig større grad integreres i kraftforsyningen vil et målrettet tilslag mot et system eller mot en latent sårbarhet i et system imidlertid kunne gi fysiske, så vel som digitale utslag. Herunder vil mindre avvik kunne få store og uoversiktlige ringvirkninger, og i takt med at skillet mellom den fysiske og digitale verden viskes ut vil systemene kunne utvikle nye sårbarhetsflater. All den tid sikkerhetstiltak i mange tilfeller utgjøre en betydelig utgift som ikke nødvendigvis harmonerer med private organisasjoners målsetning om profittmaksimering, frykter NSM samtidig at nødvendige sikkerhetsinvesteringer vil nedprioriteres som et resultat av svakere økonomiske tider. Et redusert fokus på sikkerhet vil i ytterste konsekvens kunne gå utover samfunnets samlede motstandsdyktighet og resiliens. Parallelt med Russlands angrepskrig i Ukraina og den voksende internasjonale konfliktflaten beskriver NSM at summen av komplekse og ekspanderende cybersårbarheter bygger opp under risikoen for koordinerte og tverrsektorielle cyberoperasjoner mot strategiske mål og sikkerhetsinteresser innenfor norsk kraftsektor (NSM, 2023, s. 7-14; NVE, 2021, s. 4-6 & 10-20).

6.4 – Sårbarhetsreduserende tiltak og barrierer

For å redusere den totale risikoen vektlegger VTS-modellen at det samlede risikobildet vil reduseres til den grad man evner å redusere enten trusselen, verdien eller sårbarheten ved et system (Engen et al., 2021, s. 101-103). All den tid trusselen mot norsk energisikkerhet i hovedsak utgjøres av eksterne trusselaktører utenfor NVEs kontroll eller virkeområde, peker de iboende sårbarhetene ved kraftsystemet seg ut som det mest hensiktsmessige fokusområdet for NVEs sikkerhetsstyring, til tross for at det naturligvis ikke finnes noe definert fasitsvar på hvilket sikkerhetsnivå som vil være tilstrekkelig. Uten å gå i dybden på hvordan identifiserte sårbarheter kan reduseres foreslår likevel FFI gjennom BAS3-prosjektet, NVE gjennom ulike fag- og eksternrapporter og Justis- og beredskapsdepartementet gjennom sin NOU om *digital sårbarhet* en rekke sårbarhetsreduserende tiltak og grunnprinsipper for sikkerhetsstyringen av kraftforsyningen.

Sett opp mot sårbarhetsflatene som følger i kjølvannet av samfunnsdigitaliseringen fremheves blant annet behovet for en kombinasjon av tekniske, organisatoriske og juridiske barrierer. I den forbindelse vises det til nødvendige sikkerhetstiltak som fastsatte sikkerhetskrav, standardiserte veiledninger innenfor IKT-sikkerhet, strategiske styringssystemer og kunnskapsbasert tilsynsvirksomhet. I takt med at det legges opp til stadig tettere koblinger mellom kraftforsyningens drift- og forretningssystemer og en økt bruk av digitale underleverandører vil det samtidig stilles større krav til den tekniske arkitekturen, redundante løsninger og faglig veiledning på området. På denne bakgrunn anbefaler NVE at virksomheter i kraftforsyningen som tar en høyere risiko i forbindelse med digitaliseringsinitiativer, samtidig må styre risikoen ved å investere i egnede IKT-sikkerhetstiltak, prosedyrer og tilstrekkelig beredskap. For å fremme god risikostyring oppfordrer informantene samtidig til stimulering mot god sikkerhetskultur, bevisstgjøring av ansatte på relevante trusler og sårbarhetshetsflater, samt utvikling av digitale rammeverk med tilhørende sjekklister og rutiner (NOU 2015:13, s. 142-145; NVE, 2021, s. 16-20).

I tråd med Besnard et. al (2018, s. 27-40) vil en god sikkerhetskultur blant annet karakteriseres av evnen til å identifisere utfordringer som oppstår i skjæringsfeltet mellom ulike enheter og til å sikre effektiv samhandling mellom ulike fagområder, på tross av organisatoriske ulikheter. Herunder foreslår Justis- og beredskapsdepartementet at NVE i fellesskap med relevante interesseorganisasjoner bør utarbeide utfyllende veiledere på «beste praksis» og stimulere til å etablere mer ressurssterke og operative fagmiljøer innen IKT-sikkerhet og IKT-hendelseshåndtering. Fagmiljøene vil blant annet kunne fungere som kontaktpunkt ut mot andre sektorer, organisere kurs og øvelser, samt legge til rette for rask informasjonsutveksling om erfarte hendelser, aktuelle trusler og mulige avbøtende tiltak. Videre fremheves viktigheten av brede risiko- og sårbarhetsanalyser i forkant av bruksendringer, ved system- og organisasjonsendringer og i forbindelse med teknologiskifter (NOU 2015:13, s. 143-145). For å skaffe oversikt og kontroll over aktuelle trusler og sårbarheter vektlegger NVE betydningen av et helhetlig styringssystem og en omfattende tilsynsvirksomhet. På bakgrunn av det store mangfoldet av digitale underleverandører på feltet foreslås det samtidig å etablere en overordnet oversikt over leverandører og en ordning for godkjenning, eksempelvis gjennom krav til sertifisering og standardiserte sikkerhetskrav til tjenesteutsettingen. Slik vil det være enklere for den enkelte virksomhet å kartlegge og analysere relevante sårbarheter hos aktuelle underleverandører (NVE, 2022, s. 18-26). Sluttelig løfter FFI – gjennom sine strategier for redusert sårbarhet i kraftsektoren – frem

behovet for digital kompetanseheving og opplæring til beredskapspersonell og systemoperatører, behovet for samhandling og felles løsninger på tvers av virksomheter, samt viktigheten av et økt fokus på feiloppretting og reetablering etter ekstraordinære hendelser og fysiske enkeltpåkjenninger (FFI, 2001, s. 21-25).

På den andre siden beskriver informanten tilknyttet den digitale sikkerhetssektoren at sofistikerte sikkerhetstiltak i mange tilfeller vil medføre en stor økonomisk kostand og kunne føre til redusert brukervennlighet. En redusert brukervennlighet kan bidra til å komplisere systemdriften og på denne måten åpne opp for nye risikoer og sårbarheter ved at systemoperatørene finner nye og sikkerhetstruende snarveier. På denne bakgrunn understreker informanten viktigheten av at alle sikkerhetstiltak og sikkerhetsstrategier baseres på underliggende risikoanalyser og at man finner frem til en balansegang mellom akseptert risiko, nødvendige sikkerhetstiltak og brukervennlige systemer.

7.0 – KONKLUSJON

Alt i alt fremhever informantene at interstatlig etterretningsvirksomhet, med evne til å tilpasse seg potensielle barrierer og iverksatte mottiltak, vil utgjøre den største security-trusselen mot norsk kraftforsyning som en konsekvens av tilspisningen i det sikkerhetspolitiske landskapet. Herunder løfter relevante statlige sikkerhetsmyndigheter, som PST, NSM og Forsvarets etterretningstjeneste, frem russisk etterretningsvirksomhet som den mest aktuelle enkeltstående trusselaktøren mot norske sikkerhetsinteresser og samfunnskritisk infrastruktur. I den forbindelse forventes det at norske virksomheter og demokratiske institusjoner vil utsettes for et bredt spekter av sammensatte virkemidler, rekognoseringsaktivitet og digitale nettverksoperasjoner som et ledd i interstatlig etterretningsvirksomhet. Eksempelvis gjennom komplekse cyberangrep, påvirkningsoperasjoner eller digital spionasje. Sett i sammenheng med samfunnsdigitaliseringen har det samtidig åpnet seg en rekke nye sårbarhetsflater i kjølvannet av den teknologiske utviklingen. I takt med at organisasjoner, teknologi og fysiske enheter koples sammen på måter som tidligere var utenkelig forsterkes det gjensidige avhengighetsforholdet mellom mennesker og maskiner. I den forbindelse fremheves det store mangfoldet av digitale underleverandører, den tiltagende eksponeringen av sentrale driftssystemer mot det åpne nettet, økende avhengighet til IKT- og elektroniske kommunikasjonssystemer, tvetydige sikkerhetskrav og knapphet på kompetent personell som

sikkerhetskritiske sårbarhetsflater for kraftsektoren i sin helhet (NOU 2015:13; NVE, 2021; NVE, 2022).

Til tross for at de forretningsmessige og samfunnsøkonomiske gevinstene ved integrasjonen av ulike systemer beskrives som for store til å jobbe mot utviklingen, er informantene likevel samstemte om at den digitale transformasjonen åpner for en bredere eksponering mot digitale trusselagenter. Følgelig vil samfunnsdigitaliseringen stille større krav til en kunnskapsbasert risikohåndtering og en helhetlig sikkerhetsstyring. Som beskrevet i en rekke sentrale styringsdokumenter utgjør kraftforsyningen samtidig en helt essensiell samfunnsfunksjon for opprettholdelsen av en rekke andre kritiske samfunnsfunksjoner og infrastrukturer (DSB, 2016). Skadepotensialet og samfunnsrisikoen som følger i kjølvannet er dermed enormt og utgjør en vesentlig sikkerhetsutfordring for den norske samfunnssikkerheten. Sett opp mot problemstillingen er det med andre ord naturlig å legge til grunn at samfunnsdigitaliseringen på den ene siden bidrar til praktiske løsninger, robuste sikkerhetssystemer og effektivisering, men på den andre siden åpner for nye sårbarhetsflater for samfunnets grunnleggende verdier, systemer og funksjoner. Slik tjener den digitale utviklingen både som grunnlag for nye sårbarheter og som virkemiddel for å begrense dem. Sett i sammenheng med dagens foreliggende trusselbilde mot norske sikkerhetsinteresser legger disse moderne sårbarhetsflatene til rette for et bredere handlingsrom og nye angrepsflater for ondsinnede trusselaktører som datakriminelle eller utenlandsk etterretningsvirksomhet (NVE, 2022).

Som en konsekvens av den antatte russiske målsetningen om å sette europeisk energisikkerhet under press og den tiltagende energikrisen Europa står i, vil norsk olje- og energisektor samtidig få en stadig større sikkerhetspolitisk betydning for resten av Europa i tiden fremover (Etterretningstjenesten, 2023, s. 28-32; NOU2023:3, s. 33). I takt med økende internasjonalisering og den voksende sikkerhetspolitiske verdien vil naturligvis også trusselbildet mot norsk energiinfrastruktur skjerpes. Følgelig vil det som tidligere var energipolitikk i større grad smelte sammen med, og underordnes, norsk sikkerhetspolitikk. Til tross for at PST (2023) vurderer den fysiske sabotasjerisikoen som relativt liten, bemerkes det at en ytterligere tilspisning av den sikkerhetspolitiske situasjonen er å forvente og at enkeltstående sabotasjehandlinger mot strategiske mål i Norge kan bli et aktuelt scenario dersom Russlands vilje til å eskalere konflikten med NATO og vesten tiltar. I så fall forutsetter PST at en potensiell sabotasjehandling sannsynligvis vil gjennomføres på en måte som gjør det krevende å tilskrive handlingen til aktøren som står bak, og i den anledning

løftes det digitale domenet frem som en spesielt eksponert angrepsflate for digital etterretningsvirksomhet (PST, 2023, s. 17-21).

På den andre siden påpeker NSM (2023) at «sikkerhet» i mange tilfeller oppfattes som en relativt snever tekniske funksjon som ikke nødvendigvis harmonerer med virksomhetenes «kjernevirksomhet» eller det private næringslivets målsetning om profittmaksimering. I takt med svakere økonomiske tider og økende privatisering av samfunnsfunksjonene kan det følgelig være fristende for virksomhetene å senke sikkerhetsnivået eller å lempe på risikovurderingene, for å heller kunne allokere ressursene til andre produksjonsmessige formål og kortsiktig profitt. Sett hen til næringslivets stadig mer sentrale rolle i arbeidet med nasjonale sikkerhetshensyn vil sikkerhetsutfordringer for den enkelte virksomhet imidlertid kunne forplante seg og få ringvirkninger for samfunnets samlede motstandsdyktighet. Følgelig kan det tenkes at den økonomiske logikken om profittmaksimering og kostnadsbesparende tiltak i flere tilfeller vil kunne kollidere med nasjonale sikkerhetshensyn, og på denne måten bidra til å bygge opp under de voksende digitale sårbarhetsflatene (NSM, 2023).

Sett i lys av kraftsektorens økende avhengighet til digitale verdikjeder utgjør sårbarhetene til eksterne underleverandører en sentral sikkerhetsutfordring som vil absorberes av kraftsektoren i sin helhet. Følgelig vil det heller ikke være tilstrekkelig å utvikle sikkerhetstiltak for egne systemer, men det vil samtidig stilles krav til en oversikt over underleverandører og eventuelle «sikkerhetshull» (DSB, 2020; NVE, 2022). Herunder slår flere nasjonale sikkerhetsmyndigheter fast at potensielle nettverksoperasjoner i hovedsak forventes å rette seg mot relativt enkle sårbarheter ved systemene som utdatert programvare, svake og gjenbrukte passord eller manglende to-faktorautentisering (NSM, 2023; PST, 2023). Samtidig viser undersøkelser fra USA at de digitale leverandørkjedene tjente som inngangsporten til systemene for angriper ved majoriteten av de digitale tilslagene mot amerikanske virksomheter (Ponemon Institute, 2019). Med andre ord er det nærliggende å legge til grunn at relativt enkle sårbarhetsreduserende tiltak, sikkerhetsstrategier og barrierer vil kunne bidra til å styrke sikkerhetsnivået rundt kraftforforsyningens sentrale systemer betraktelig, til tross for et skjerpet trusselbilde og endrede rammebetingelser. I tråd med systemperspektivet og VTS-modellen bør det således være et selvstendig poeng å redusere kartlagte sårbarhetsflater mest mulig, all den tid de latente sårbarhetene vil bidra til å

problematisere sikkerhetsstyringen, fremme brudd på optimal praksis og menneskelig svikt, og på denne måten skape utfordringer for den norske samfunnssikkerheten i sin helhet.

Samlet sett vil samfunnsdigitaliseringen ligge til grunn for utviklingen av en rekke digitale sårbarhetsflater som vil bidra til å komplisere sikkerhetsstyringen av kraftforsyningen som system. Sett i lys av utviklingen i det sikkerhetspolitiske landskapet er dette sårbarhetsflater, som i takt med den voksende konfliktflaten mellom vestlige demokratier og autoritære regimer, vil kunne utnyttes av ondsinnede trusselaktører. Både av kriminelle grupperinger, men kanskje først og fremst av interstatlig etterretningstjenester som et ledd i hybride virkemiddeloperasjoner. På overordnet nivå vil dagens geopolitiske uroligheter og sikkerhetspolitiske usikkerhet med andre ord skjerpe trusselbildet mot norske samfunnsfunksjoner generelt, og energi- og kraftsektoren spesielt. PST (2023) og NSM (2023) presiserer imidlertid i sine offentlige trusselvurderinger at det er liten grunn til å forvente fysiske sabotasjeaksjoner mot norsk infrastruktur i det inneværende året, men at de digitale sårbarhetsflatene er mer eksponert enn tidligere for målrettede anslag og nettverksoperasjoner. Når det sagt beskriver flere av informantene en rekke sårbarhetsreduserende tiltak og barrierer som vil kunne begrense skadevirkningene ved et potensielt tilslag og redusere de digitale sårbarhetsflatene. I lys av VTS-modellen er dette sikkerhetstiltak som ved implementering vil bidra til å redusere den totale risikoen mot kraftforsyningens systemer og styrke dybdeforsvaret mot latente svakheter og underliggende feil.

Sett i sammenheng med «systemperspektivet» har jeg gjennom oppgaven etablert at kraftforsyningen utgjør et samlet system med en overordnet visjon om å ivareta samfunnets behov elektrisk energi gjennom et velfungerende el-system. Rammebetingelsene systemet opererer under vil imidlertid forandres i takt med samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen. På denne måten vil endrede rammevilkår kunne bidra til å skape nye og forsterke aktuelle sårbarhetsflater for kraftforsyningens tilgjengelighet og leveransesikkerhet. Disse sårbarhetsflatene må NVE og tilknyttede KBO-enheter dimensjonere for i sikkerhetsstyringen av kraftsystemet gjennom relevante virkemidler, tekniske og organisatoriske barrierer og sårbarhetsreduserende tiltak for å ivareta kraftforsyningens definerte krav til funksjon og ytelse.

Alt i alt kan det følgelig konkluderes med at samfunnsdigitaliseringen har bidratt til å skape nye rammebetingelser og sårbarhetsflater for kraftforsyningen som system. I lys av dagens sikkerhetspolitiske situasjon har trusselbildet mot disse sårbarhetsflatene naturligvis skjerpet seg. På samfunnsnivå vil et større bortfall av kraftleveranser kunne gå på bekostning av funksjons- og samhandlingsevnen til tilknyttede kritiske samfunnsfunksjoner og responderende beredskapspersonell. En vedvarende svikt vil med andre ord kunne utløse en kaskade av eskalerende feil og få massive ringvirkninger for den helthetlige samfunnssikkerheten. I takt med at samfunnsdigitaliseringen har skapt et bredere handlingsrom for potensielle trusselaktører, peker oppgavens funn samtidig på at samfunnet og kraftvirksomhetene kun innehar en begrenset evne til å beskytte og forsvare kraftforsyningens digitale sårbarhetsflater mot det foreliggende trusselbildet innenfor rammene av dagens sikkerhetspolitiske situasjon. Det er følgelig nærliggende å legge til grunn at disse sårbarhetsflatene utgjør en potensiell sikkerhetsutfordring for befolknings grunnleggende behov og for storsamfunnet i sin helhet. På denne bakgrunn anbefaler NVE at alle virksomheter som tar en høyere risiko i forbindelse med digitaliseringsinsentiver bør styre risikoen ved å aktivt investere i beredskap, prosedyrer og egnede sikkerhetstiltak og legge til rette for en proaktiv tilnærming til sikkerhetsstyringen. Samtidig fremheves viktigheten av en god sikkerhetskultur, digital kompetanseheving, aktiv bruk av redundans og oppdaterte risiko- og sårbarhetsanalyser på området.

7.1 – Forslag til videre forskning

Basert på oppgavens funn ville det for videre forskning vært interessant å undersøke hvordan identifiserte sårbarhetsflater kan begrenses og reduseres gjennom implementasjon av ulike former for forebyggende og redundante tiltak. På denne måten vil man kunne åpne for et bredere innblikk i kraftforsyningens sentrale utviklingsområder og etablere forståelse for hvordan sikkerhetssystemene og barrierene kan videreutvikles. Samtidig vil det foreliggende trusselbildet mot kraftforsyningen naturligvis være i kontinuerlig endring og utvikle seg i takt med det sikkerhetspolitiske landskapet. Det kunne med andre ord vært interessant å gjennomført en oppfølgingsstudie om hvordan virksomheter og KBO-enheter innenfor energisektoren har opplevd utviklingen i trusselbildet. Herunder om virksomhetene har opplevd en reel økning i antallet tilslag eller alvorligheten i registrerte sikkerhetsavvik som følge av den sikkerhetspolitiske utviklingen. Studien kunne tatt utgangspunkt i en kvantitativ tilnærming og sammenlignet statistiske data om sikkerhetsavvik og registrere tilslag mot trender i den sikkerhetspolitiske utviklingen. På denne måten kunne man forsøkt å kartlegge

eventuelle korrelasjoner mellom det presentere trusselbildet og hyppigheten av faktiske forsøk på tilslag eller kartleggingsvirksomhet mot norsk energisektor.

Videre ville det vært interessant å gå i dybden på de ulike KBO-enhetenes tilnærming til sikkerhetsstyringen av egne anlegg. Herunder hadde det vært aktuelt å undersøke i hvilket omfang KBO-enhetene har tilpasset sitt beredskapsforberedende arbeid til utviklingen i trusselbildet og til hvilken grad enhetene ivaretar og oppfyller kraftberedskapsforskriftens krav til sikringstiltak og risikovurderinger. Studien kunne tatt utgangspunkt i en kvalitativ tilnærming og samlet inn informasjon om sikringen av et representativt utvalg anlegg gjennom kvalitative intervjuer, deltakende observasjon og supplerende dokumentanalyser. Kartlagte sikringstiltak ved de ulike anleggene vil videre kunne sees opp mot kraftberedskapsforskriftens lovfestede krav til sikring og sikkerhet. På denne måten vil man kunne undersøke og analysere i hvilken utstrekning kraftberedskapsforskriftens definerte krav til sikringstiltak og risikovurderinger faktisk ivaretas, og om det foreligger store sikkerhetsavvik på området. Samtidig vil man også kunne sammenligne de ulike KBO-enhetens sikringstiltak opp mot hverandre og slik avdekke om det er noen typiske mønstre av sikkerhetsavvik eller sikkerhetshull som går igjen hos flere av de sentrale virksomhetene på feltet.

Litteraturliste

Anholt, R. & Boersma, K. (2018). *From Security to Resilience: New Vistas for International Responses to Protracted Crises*. Hentet fra: https://beta.irgc.org/wp-content/uploads/2018/12/Anholt-et-al-for-IRGC-Resilience-Guide-Vol-2-2018.pdf

Beck, U. (1992). *Risk Society; Towards a New Modernity*. London: Sage Publications.

Besnard, D., Boissières, I., Daniellou, F. & Villena, J/ Institute for an Industrial Safety Culture (ICSI). (2018). *Safety culture: From understanding to action*. Toulouse: Institut pour une culture de sécurité industrielle. Hentet fra: https://www.icsi-eu.org/sites/default/files/2020-07/Icsi_cahier_EN_safety-culture_2017.pdf

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

Bredesen, M. G. & Reichborn-Kjennerud, E. (2016, 13. mars). Hybrid krigføring – hva er det? Hentet fra (lest 30.01.23): https://www.nupi.no/publikasjoner/innsikt-og-kommentar/hvor-hender-det/hhd-2016/hybrid-krigfoering-hva-er-det

Burke, W. W. & Litwin, G. H. (1992). A causal model of organizational performance and change. *Journal of Management*, *18*(3), 523–545. https://doi.org/10.1177/014920639201800306

Dalen, M. (2011). *Intervju som forskningsmetode – en kvalitativ tilnærming* (2. utg.). Oslo: Universitetsforlaget AS.

Dalland, O. (2017). *Metode og oppgaveskriving* (6.utg.). Oslo: Gyldendal akademisk

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

Direktorat for samfunnssikkerhet og beredskap. (2016). *Samfunnets kritiske funksjoner*. Hentet fra: https://www.dsbinfo.no/DSBno/2017/tema/samfunnets-kritiske-funksjoner/?page=2

Direktoratet for samfunnssikkerhet og beredskap. (2020). *Risikostyring i digitale verdikjeder*. Hentet fra: https://www.dsb.no/rapporter-og-evalueringer/risikostyring-i-digitale-verdikjeder/

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

Etterretningstjenesten. (2022). *Fokus 2022.* Hentet fra: https://www.etterretningstjenesten.no/publikasjoner/fokus

Etterretningstjenesten. (2023). *Fokus 2023.* Hentet fra: https://www.etterretningstjenesten.no/publikasjoner/fokus

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

Forsvaret forskningsinstitutt. (2001). *En sårbar kraftforsyning - Sluttrapport etter BAS3* (FFI/RAPPORT-2001/02381). Hentet fra: https://www.ffi.no/publikasjoner/arkiv/en-sarbar-kraftforsyning-sluttrapport-etter-bas3

Forsvaret forskningsinstitutt. (2018). *Lavintensivt hybridangrep på Norge i en fremtidig konflikt.* Hentet fra: https://www.ffi.no/publikasjoner/arkiv/lavintensivt-hybridangrep-pa-norge-i-en-fremtidig-konflikt

Forsvaret forskningsinstitutt. (2023a). Forsvarets forskningsinstitutt - Vi gjør kunnskap og ideer til et effektivt forsvar. Hentet fra (lest: 10.02.23): https://www.ffi.no/om-ffi

Forsvaret forskningsinstitutt. (2023b). Beskyttelse av samfunnet (BAS). Hentet fra (lest 20.03.23): https://www.ffi.no/forskning/prosjekter/beskyttelse-av-samfunnet

Gould & Bieder. (2020). *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice*. Toulouse: Springer Cham

Grønmo, S. (2015). *Samfunnsvitenskapelige metoder* (2. utg.). Oslo: Fagbokforlaget

Grønmo, S. (2023, 16 januar). Kvalitativ metode. I S. Dahlum (red.). Hentet fra (lest 25.01.23): https://snl.no/kvalitativ_metode

Heyerdahl, A. (2022a). From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway. *European Security*, *32*(1), 147-169. https://doi.org/10.1080/09662839.2022.2070006

Heyerdahl, A. (2022b). Risk assessment without the risk? A controversy about security and risk in Norway. *Journal of Risk Research, 25*(2), 252-267. https://doi.org/10.1080/13669877.2021.1936610

Jacobsen, D. I. (2016). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. (5. utg). Oslo: Høyskoleforlaget

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2010). *Introduksjon til samfunnsvitenskapelig metode* (4. utg.). Oslo: Abstrakt.

Jore, S. H. (2015). Challengers of building societal resilience through organizational security risk management. *Working on Safety.*

Jore, S. H. (2019a). The conceptual and scientific demarcation of security in contrast to safety. *European journal for security research*, *4*(1), s. 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. H. (2019b). The multifaceted aspect of uncertainty – the significance of addressing uncertainty in the management of the transboundary wicked problem of terrorism. *Proceedings of the 29th European safety and reliability conference*, s. 4044-4051. https://doi.org/10.3850/978-981-11-2724-3.

Justis- og beredskapsdepartementet. (2017). *Risiko i et trygt samfunn — Samfunnssikkerhet.* (Meld. St. 10 (2016-2017)). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Kvale, S., Brinkmann, S., Anderssen, T. M., & Rygge, J. (2015). *Det kvalitative forskningsintervju* (3. utg.). Oslo: Gyldendal akademisk.

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

Nasjonal sikkerhetsmyndighet. (2023). *Risiko 2023 - Økt uforutsigbarhet krever økt beredskap.* Hentet fra: https://nsm.no/getfile.php/13125471676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

Njå, O., Sommer, M., Rake, E. & Braut, G. (2021). *Samfunnssikkerhet – analyse, styring og evaluering.* Oslo: Universitetsforlaget.

NOU 2006:6. (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.* Oslo: Justis- og politidepartementet Hentet fra: https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

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

https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2023:3. (2023). *Mer av alt – raskere*. Oslo: Olje- og energidepartementet. Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2023-3/id2961311/

Norsk senter for forskningsdata (NSD). (2022). Hentet fra (lest 10.01.23): https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/

Norges vassdrags- og energidirektorat. (2008, 03. desember). Kraftforsyningsberedskap og KBO. Hentet fra (lest 28.01.23): https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/

Norges vassdrags- og energidirektorat. (2012). *Veiledning til forskrift om beredskap i kraftforsyningen.* Hentet fra: https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/veiledning-til-kraftberedskapsforskriften/

Norges vassdrags- og energidirektorat. (2013, 10. juni). Kraftforsyningens beredskapsorganisasjon (KBO). Hentet fra (lest 25.01.23): https://www.nve.no/energi/tilsyn/kraftforsyningsberedskap-og-kbo/organisering-av-kraftforsyningsberedskap/kraftforsyningens-beredskapsorganisasjon-kbo/

Norges vassdrags- og energidirektorat. (2021). *IKT-sikkerhetstilstanden i kraftforsyningen 2021*. (NVE-rapport 19/2021). Hentet fra: https://publikasjoner.nve.no/eksternrapport/2021/eksternrapport2021_19.pdf

Norges vassdrags- og energidirektorat. (2022). *Risikostyring av IKT-sikkerhet i leverandørkjeder*. (NVE-rapport 17/2022). Hentet fra: https://publikasjoner.nve.no/eksternrapport/2022/eksternrapport2022_17.pdf

NRK. (2022, 26. september). Gassrørledningen Nord Stream. Hentet fra (10.03.23): https://www.nrk.no/nyheter/gassrorledningen-nord-stream-1.13828304

Olje- og energidepartementet. (2021, 12. oktober). Kraftforsyningen. Hentet fra (lest 14.02.23): https://www.regjeringen.no/no/tema/energi/beredskap-i-energisektoren/kraftforsyningen1/id2353809/

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies.* (2. utg). New York: Basic Books.

Persson, C. P. (2019, 03. april). Abduksjon: Metoden for å finne den beste forklaringen. Hentet fra: https://forskning.no/om-forskning-samfunnsvitenskap/abduksjon-metoden-for-a-finne-den-beste-forklaringen/1317339

Politiets sikkerhetstjeneste. (2023). *Nasjonal trusselvurdering - 2023*. Hentet fra: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2023/

Ponemon Institute. (2019). *The Cost of Third-Party Cybersecurity Risk Management.* Hentet fra: https://www.censinet.com/wp-content/uploads/Ponemon-2019-The-Economic-Impact-of-Third-Party-Risk-Management.pdf

Qu, S. Q. & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, *8*(3), s. 238-264. Hentet fra: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2058515

Eriksen, J., Rake, E. L. & Sommer, M. (2018). *Beredskapsanalyse - En innføring*. Høgskulen på Vestlandet og Universitetet i Stavanger: Cappenlen Damm Akademisk

Reason, J. (1997). *Managing the risks of organizational accidents*. New York: Ashgate Publishing

Renn, O. (2008). *Risk governance. Coping with uncertainty in a complex world*. London: Earthscan.

Roe, E. & Schoulman, P. R. (2008). *High Reliability Managment: Operating on the Edge.* Stanford: Stanford University Press.

Rossignol, N., Delvenne, P. & Turcanu, C. (2015). Rethinking Vulnerability Analysis and Governance with Emphasis on a Participatory Approach. *Risk Analysis*, *35*(1), s. 129 – 140. Hentet fra: https://pubmed.ncbi.nlm.nih.gov/24924802/

Standard Norge. (2014). *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse* (NS 5832:2014). Hentet fra:

https://www.standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=718202

Statsministerens kontor. (2022, 31. oktober). Regjeringen styrker Forsvarets beredskap i Norge. Hentet fra (lest 10.01.23): https://www.regjeringen.no/no/aktuelt/regjeringen-styrker-forsvarets-beredskap-i-norge/id2942769/

Thurén, T. (2009). *Vitenskapsteori for nybegynnere* (2.utg). Oslo: Gyldendal Akademisk

Unruh, G. og Kiron, D. (2017). *Digital transformation on purpose*. Hentet fra: https://sloanreview.mit.edu/article/digital-transformation-on-purpose

US. Department of Homeland Security. (2015) *The future of smart cities; cyber-physical infrastructure risk.* Hentet fra: https://www.researchgate.net/publication/281086433_The_Future_of_Smart_Cities_Cyber-Physical_Infrastructure_Risk

Wolf, M. og Serpanos, D. (2018). *Safety and Security in Cyber–Physical Systems and Internet-of-Things Systems*. Hentet fra: https://www.researchgate.net/publication/322190542_Safety_and_Security_in_Cyber-Physical_Systems_and_Internet-of-Things_Systems

Yin, Robert K.. (2017). *Case study research: design and methods* (6. utg.). Los Angeles: SAGE publications.

VEDLEGG

Vedlegg 1: Informasjonsskriv om forskningsprosjektet

Informasjon om forskningsprosjekt

Universitet i Stavanger - Institutt for sikkerhet, økonomi og planlegging

Vil du delta i forskningsprosjektet

***Norsk kraftforsyning i møte med fremtidens trusselbilde og moderne sårbarhetflater*?**

Dette informasjonsskrivet beskriver forskningsprosjektet *Norsk kraftforsyning i møte med fremtidens trusselbilde og moderne sårbarhetsflater*. Prosjektet inngår som en del av min masteroppgave i samfunnssikkerhet ved Universitet i Stavanger, våren 2023. I dette informasjonsskrivet ønsker jeg å informere om målsetningene ved forskningsprosjektet og hva en deltakelse vil innebære for deg.

Oppstartdato: 01.01.23
Ferdigstillelse: 15.06.23

Målsetning med forskningsprosjektet

Kraftforsyningen utgjør en essensiell komponent i opprettholdelsen av en rekke grunnleggende samfunnsfunksjoner og en svikt i leveransesikkerheten vil resultere i massive konsekvenser for det norske samfunnet i sin helhet. Den sikkerhetskritiske avhengigheten er på mange måter total i den forstand at samfunnet vil oppleve en spontan stans innenfor de fleste samfunnssektorer i øyeblikket kraftforsyningen opphører, og flere kritiske samfunnsfunksjoner vil umiddelbart eller i løpet av kort tid svikte. På bakgrunn av samfunnsdigitaliseringen, dagens sikkerhetspolitiske uroligheter og den sikkerhetspolitiske utviklingen har imidlertid trusselbildet mot kraftforsyningen endret seg gjennom de siste årene.

På bakgrunn av den tiltagende utviklingen i risikobildet ønsker jeg derfor å undersøke hvordan sikkerhetsstyringen av norsk kraftforsyning påvirkes av samfunnsdigitaliseringen sett i lys av dagens sikkerhetspolitiske uroligheter, og til hvilken grad trusselbildet har endret seg i

takt med den sikkerhetspolitiske situasjonen. Herunder ønsker jeg å kartlegge på hvilken måte sikkerheten rundt norsk kraftsektor påvirkes av samfunnsutviklingen, hvordan beredskapen innrettes etter forventet utvikling i det fremtidige trusselbildet og i hvor stor utstrekning samfunnsdigitaliseringen har åpnet for nye sårbarhetsflater rundt den norske kraftforsyningen.

Oppgaven vil spesielt fokusere på hvordan NVE som ansvarlig forvalter, og enheter som faller inn under Kraftforsyningens beredskapsorganisasjon (KBO-enheter) oppfatter, vurderer og håndterer den ekstraordinære utviklingen i risikobildet. Videre vil identifiseringen av potensielle sårbarheter i opprettholdelsen av leveransesikkerheten stå sentralt. På overordnet nivå inviterer forskningsprosjektet til en kartlegging av samfunnsdigitaliseringens innvirkning på sikkerheten rundt norsk kraftproduksjon, samtidig som tematikken også legger premissene for en vurdering av relevante sikkerhetspolitiske faktorers betydning for utviklingen i trusselbildet.

Hvorfor får du spørsmål om å delta?

For å innhente pålitelig og relevant informasjon ønsker jeg å komme i kontakt med informanter med kjennskap til driften av kraftforsyningen som system, kunnskap om sikkerheten rundt kraftforsyningen eller generelt bred innsikt i oppgavens tematikk for øvrig. Intervjuene er relatert til forskningsprosjektet og har til hensikt å belyse relevante informasjonsbehov.

Herunder vil informasjonen fra intervjuene bli brukt til å:

1. Bidra til å belyse oppgavens forskningsspørsmål i kombinasjon med andre kilder til empiriske data.

2. Supplere gjennomførte dokumentanalyser i forbindelse med forskningsprosjektet

3. Underbygge aktuelle funn og konklusjoner i oppgaven.

Det er frivillig å delta

Din deltakelse vil enhver tid være frivillig og uten økonomisk vederlag. Du har rett til å kontrollere innsamlet informasjon om deg og har på ethvert tidspunkt anledning til å trekke deg fra prosjektet uten videre negative konsekvenser. Hvis du ønsker å trekke deg fra

prosjektet, vil informasjonen din bli slettet. Samtlige informanter som bidrar i prosjektet vil anonymiseres.

Ditt personvern – hvordan oppbevares og brukes dine opplysninger

Innhentet informasjon vil kun benyttes for formålene beskrevet i dette informasjonsskrivet. Opplysningene vil behandles konfidensielt og i samsvar med personvernregelverket. Opplysninger som kan identifisere deg vil bli anonymisert i masteroppgaven. Informantene vil ikke kunne gjenkjennes i en publikasjon.

Hva gir rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

Hvor kan jeg finne ut mer?

Har du spørsmål knyttet til forskningsprosjektet, ønsker gjennomlesning av sitater og øvrige data, eller vil trekke deg fra prosjektet kan du ta kontakt med:

- **Faglig ansvarlig for veiledning av masteroppgaven:**
  Claudia Morsut, førsteamanuensis ved Universitetet i Stavanger
  E-post: claudia.morsut@uis.no
  Telefon: 51 83 13 31

- **Ansvarlig forsker som utfører intervjuene:**
  Bjørn Henrik Lundqvist
  E-post: 267532@uis.no

- **Personvernombud ved UiS:**
  Rolf Jegervatn.
  E-post: personvernombud@uis.no
  Telefon: 51 83 30 81

- **NSD - Norsk senter for forskningsdata AS**
  E-post: personverntjenester@nsd.no
  Telefon: 55 58 21 17

Hvis du har spørsmål knyttet til vurderingen som er gjort av personverntjenestene fra SIKT, kan du ta kontakt via: personverntjenester@sikt.no eller telefon: 73 98 40 40.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?

Prosjektet vil etter planen avsluttes 15.06.23. Etter prosjektslutt vil datamaterialet med dine personopplysninger slettes.

På oppdrag fra Universitetet i Stavanger har SIKT – Kunnskapssektorens tjenesteleverandør vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Vedlegg 2: Vedlegg til informasjonsskriv med samtykkeerklæring

VEDLEGG TIL INFORMASJONSSKRIV
Samtykkeskjema for deltakelse i intervjuer

Hva innebærer det for deg å delta?

Som beskrevet i informasjonsskrivet ønskes det å gjennomføre et kvalitativt intervju av deg i kraft av din funksjon eller faglige innsikt. For å belyse oppgavens problemstilling og tilhørende forskningsspørsmål vil jeg gjennom forskningsprosjektet benytte meg av semistrukturerte intervjuer. Dette innebærer at en overordnet intervjuguide danner rammene for intervjuet, men at spørsmål, tematikk og tilnærming vil kunne tilpasses det enkelte intervju. Slik legges det til rette for at informanten kan gå i dybden på temaene informanten selv vurderer som betydningsfulle. Intervjuet vil anslagsvis vare i **40-60 minutter.**

Tidspunkt og sted for intervju

Dersom du samtykker til å delta i forskningsprosjektet vil vi i samråd avtale tid og sted for intervjuet. Jeg ser for meg å gjennomføre intervjuet i perioden april-mai 2023. Dato og klokkeslett avtales nærmere med deg. Intervjuet kan enten gjennomføres ved fysisk oppmøte, over digital videokonferanse eller pr. telefon.

Rettigheter som informant

Jeg har blitt gjort kjent med målsetningene ved forskningsprosjektet og informasjonsarket ovenfor. Jeg har forstått hensikten med intervjuet og at:

- Min deltakelse i intervjuet er frivillig. Jeg forstår at jeg ikke får betalt for min deltakelse.

- Jeg kan trekke tilbake samtykket og avslutte deltakelsen når som helst, eller nekte videre deltakelse uten noen form for negativ konsekvenser

- Jeg forstår at jeg kan trekke hele intervjuet, deler av intervjuet eller annen informasjon som er gitt når som helst uten uheldige konsekvenser, selv etter at intervjuet mitt er avsluttet.

- Jeg har rett til å få informasjonen jeg har bidratt med rettet eller korrigert.

- Jeg har rett til å sende en klage til ansvarlig for databeskyttelse (Personvernombud ved UiS Rolf Jegervatn. E-post: personvernombud@uis.no. Telefon: 51 83 30 81) eller det norske datatilsynet (https://www.datatilsynet.no/en/) vedrørende behandlingen av mine personopplysninger.

- Deltakelse i prosjektet innebærer å stille til et intervjue om oppgavens tema. Intervjuet vil vare i ca. 45 minutter.

- Intervjuet vil bli tatt opp på lyd for å sikre notoritet ved datainnsamlingen. Kun forskeren som utfører intervjuet vil ha tilgang til lydfilen, som vil bli lagret i en kryptert datamappe. Ingen innspilte lyddata lagres utover prosjektets slutt.

- Transkripsjoner fra intervjuet vil bli protokolert i en intervjuprotokoll. Jeg har rett til å få tilgang til og innsyn i intervjuprotokollen og eventuelt komme med rettelser og/eller tilføyelser til denne. Ingen intervjuprotokoller vil bli lagret utover prosjektets slutt.

- Jeg forstår at jeg ikke vil bli identifisert med navn i noen rapporter, og at min konfidensialitet som deltaker i denne studien forblir sikker.

- Personopplysninger vil ikke bli delt på nett eller til tredjeparter og vil kun samles inn og administreres av prosjektpartnerne i henhold til EUs generelle databeskyttelsesforordning. Ved å signere dette samtykkeskjemaet godtar jeg at mine personopplysninger kan brukes i denne forskningen.

- All innhentet informasjon vil utelukkende bli brukt i forskningssammenheng.

- Jeg har lest og forstått informasjonen som er gitt.

- Jeg har fått en kopi av dette samtykkeskjemaet.

Dersom du velger å delta på intervju er det ønskelig at du signerer vedlagt samtykkeerklæring.

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet "*Norsk kraftforsyning i møte med fremtidens trusselbilde og moderne sårbarhetsflater "*, og har fått anledning til å stille spørsmål.

Jeg samtykker til:

☐ å delta i intervju

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet 15.06.2023

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Intervjuguide for informanter tilknyttet kraftsektoren

Intervjuguide

Masteroppgave i samfunnssikkerhet

Universitet i Stavanger – våren 2023

Vedlagt er en overordnet intervjuguide utarbeidet til utvalgte intervjuobjekter. Intervjuguiden danner rammene for et semistrukturert intervju og er utviklet på bakgrunn av masteroppgavens problemstilling og tilhørende forskningsspørsmål. De forhåndsdefinerte spørsmålene er imidlertid supplert med utfyllende og sonderende oppfølgingsspørsmål. Den utformede intervjuguiden tar følgelig utgangspunkt i åpne spørsmål hvor svaralternativene ikke nødvendigvis er gitt i forkant og har med andre ord ikke blitt fulgt mekanisk gjennom intervjuene. Det enkelte intervju ble tilpasset intervjuobjektet utefra faglig funksjon, erfaring og kunnskapsfelt.

1.0 – Problemstilling og forskningsspørsmål:

«Hvordan påvirkes sikkerheten rundt norsk kraftforsyning av samfunnsdigitaliseringen, sett i lys av dagens sikkerhetspolitiske situasjon?»

Sentrale forskningsspørsmål:

- *F1: Hvilke kilder til risiko utgjør trusler mot levereansesikkerheten for norsk kraftforsyning?*
- *F2: Hvilke sentrale sårbarheter foreligger i opprettholdelsen av leveransesikkerheten til norsk kraftforsyning?*
- *F3: Hvordan påvirkes trusselbildet mot og sårbarhetsflatene ved norsk kraftforsyning av samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen?*
- *F4: Hvordan kan identifiserte sårbarheter reduseres?*

2.0 – Intervju

Innledning

Kort presentasjonsrunde og beskrivelse av prosjektet.

Del I – Kraftforsyningen som system

Kraftforsyningen som kritisk samfunnsfunksjon

1. Redegjør for din funksjon og tilknytning til kraftforsyningen som kritisk samfunnsfunksjon.

2. Beskriv kraftforsyningen som kritisk samfunnsfunksjon.
- På hvilken måte utgjør kraftforsyningen en kritisk samfunnsfunksjon?
- Hvilke sikkerhetskritiske avhengigheter eksisterer mellom kraftforsyningen og andre kritiske samfunnsfunksjoner og infrastrukturer?

Sårbarhetsflater og trusselbildet mot kraftforsyningen

3. Hvilke sentrale sårbarheter foreligger i opprettholdelsen av kraftforsyningen som kritisk samfunnsfunksjon?
- Hvilke digitale sårbarhetsflater foreligger?
- Hvilke fysiske sårbarhetsflater foreligger?
- Hvordan har sårbarhetsflatene utviklet seg de siste årene?
- Hvilke sårbarhetsflater utpeker seg som de mest kritiske for kraftforsyningen som helhetlig system?

4. Hvordan vil du beskrive det foreliggende trusselbildet mot norsk kraftforsyning?
- Hvilke naturlige og ikke-intenderte farer eksisterer?
- Til hvilken grad oppfattes ondsinnede og målrettede trusselaktører som en eksisterende trussel mot kraftforsyningen?
- Aktuelle fysiske trusler?
- Aktuelle digitale trusler?

Sikkerhetsstyring av kraftforsyningen

5. På hvilken måte jobber dere med sikkerhetsstyring av kraftforsyningen?

- Hva legger virksomheten i begrepet sikkerhetsstyring?
- Kan du beskrive hvordan din virksomhet sikrer god sikkerhetsstyring?
- Hva opplever du at virksomheten gjør riktig ved sikkerhetsstyringen?
- Hvordan gjennomføres sikkerhetsstyringen i praksis?
- Opplever dere utfordringer eller problemstillinger knyttet til sikkerhetsstyringen av kraftforsyningen som system?
- Barrierer, sikkerhetstiltak, strategier?
- Hvilke funksjoner er involvert i den daglige risikostyringen? Hvilket ledernivå er involvert?
- Gjennomføres det jevnlig evalueringer av iverksatte barrierer og sikkerhetstiltak?

6. Til hvilken grad utgjør cyber-fysiske systemer en forutsetning for driften av den norske kraftforsyningen?
- På hvilken måte avhenger kraftforsyningen av cyber-fysiske systemer?
- Medfører integrasjonen av cyber-fysiske systemer en økt sårbarhet for kraftforsyningen som system?
- Har dere oversikt over digitale leverandører og underleverandører på feltet?

Del II – Samfunnsdigitalisering og sikkerhetspolitiske faktorer

Samfunnsdigitaliseringens og sikkerhetspolitiske faktorers innvirkning på sikkerheten

7. På hvilken måte påvirker den økende samfunnsdigitaliseringen sikkerhetsstyringen av kraftforsyningen som kritisk samfunnsfunksjon?
- Har den økende samfunnsdigitaliseringen ført til nye sårbarhetsflater?
- Har den økende samfunnsdigitaliseringen ført til nye trusselagenter?
- Er sikkerhetsstyringen innrettet etter det voksende digitale trusselbildet?
- Hvilken sammenheng et det mellom kartlagte trusler og den etablerte beredskapen?

8. På hvilken måte virker den sikkerhetspolitiske utviklingen inn på sikkerheten rundt den norske kraftforsyningen?
- Hvilke sikkerhetspolitiske faktorer er sentrale for trusselbildet mot norsk kraftforsyning?
- Til hvilken grad har dere justert sikkerhetsstyringen som følge av den sikkerhetspolitiske utviklingen?

9. Hvordan ser du for deg den fremtidige utviklingen i trusselbildet mot norsk kraftforsyning?
- Hvilken rolle spiller samfunnsdigitaliseringen for utviklingen i trusselbildet?

- Hvilken rolle spiller den sikkerhetspolitiske situasjonen for utviklingen i trusselbildet?

10. På hvilken måte har trusselbildet og sårbarhetsflatene endret seg i takt med samfunnsdigitaliseringen?
- Foreligger det noen utfordringer i leverandørkjedene når det gjelder digital sikkerhet?
- Har dere gjort dere noen tanker om hvordan disse utfordringene best kan løses?
- Til hvilken grad vil en skadevare eller en svikt i leverandørkjedene påvirke deres sikkerhetsstyring?
- Til hvilken grad foregår det kunnskaps- og erfaringsdeling mellom virksomheten og underliggende leverandørkjeder?

11. Til hvilken grad har dere måttet tilpasse deres beredskapsforberedende- og forebyggende arbeid til utviklingen i trusselbildet?
- Hvilken kobling er det mellom kartlagte digitale trusler og den etablerte digitale beredskapen?

12. Hvordan kan identifiserte sårbarheter reduseres?
- Konsekvenser ved en svikt?
- Alternative løsninger ved bortfall?
- Fremtidige barrierer og sikkerhetstiltak?
- Til hvilken grad er det forholdsmessig å innføre flere barrierer og styrke eksisterende sikkerhetstiltak?

Annet:
Aktuelle dokumenter: forskrifter, instrukser, lovgivning, rammeverk, retningslinjer, etc.

- Er det flere momenter enn hva som har vært tema i intervjuet du tenker er av relevans hva gjelder sikkerheten rundt norsk kraftforsyning?
- Med tanke på anonymisering i oppgaven – hva ønsker du å omtales som?

Avsluttende kommentarer

Har du noen tilføyelser eller er det noe mer du vil legge til?
Informasjon om gjennomlesning av notater. Takk for deltakelsen.

Vedlegg 4: Intervjuguide for informanter tilknyttet FFI og den digitale sikkerhetssektoren

Intervjuguide

Masteroppgave i samfunnssikkerhet
Universitet i Stavanger – våren 2023

Vedlagt er en overordnet intervjuguide utarbeidet til intervjuobjektene fra Forsvarets Forskningsinstitutt og den digitale sikkerhetssektoren. Intervjuguiden danner rammene for et semistrukturert intervju og er utviklet på bakgrunn av masteroppgavens problemstilling og tilhørende forskningsspørsmål. De forhåndsdefinerte spørsmålene er imidlertid supplert med utfyllende og sonderende oppfølgingsspørsmål. Den utformede intervjuguiden tar følgelig utgangspunkt i åpne spørsmål hvor svaralternativene ikke nødvendigvis er gitt i forkant og har med andre ord ikke blitt fulgt mekanisk gjennom intervjuene. Det enkelte intervju ble tilpasset intervjuobjektet utefra praksis, erfaring og kunnskapsfelt.

1.0 – Problemstilling og forskningsspørsmål:

«Hvordan påvirkes sikkerheten rundt norsk kraftforsyning av samfunnsdigitaliseringen, sett i lys av dagens sikkerhetspolitiske situasjon?»

Sentrale forskningsspørsmål:

- *F1: Hvilke kilder til risiko utgjør trusler mot levereansesikkerheten for norsk kraftforsyning?*
- *F2: Hvilke sentrale sårbarheter foreligger i opprettholdelsen av leveransesikkerheten til norsk kraftforsyning?*
- *F3: Hvordan påvirkes trusselbildet mot og sårbarhetsflatene ved norsk kraftforsyning av samfunnsdigitaliseringen og den sikkerhetspolitiske utviklingen?*
- *F4: Hvordan kan identifiserte sårbarheter reduseres?*

2.0 – Intervju

Innledning

Kort presentasjonsrunde og beskrivelse av prosjektet.

Del I – Utviklingen i trusselbildet mot norske sikkerhetsinteresser og norsk samfunnssikkerhet

1. Hvordan har trusselbildet mot norsk samfunnssikkerhet og norske sikkerhetsinteresser utviklet seg i kjølvannet av det siste årets sikkerhetspolitiske uroligheter?
- Hvilke områder påvirkes mest?
- Hvilke sentrale sikkerhetsutfordringer har blitt forsterket i kjølvannet av krigen i Ukraina?
- Hvordan møter det norske samfunnet disse utfordringene?

2. Hvilke sikkerhetspolitiske faktorer bidrar til å true den norsk samfunnssikkerheten?

3. Hva er de største sårbarhetsflatene for det norske samfunnet, sett i lys av det siste årets sikkerhetspolitiske uroligheter?
- Hvorfor er disse sårbarhetsflatene mest eksponert?
- Kan de beskyttes? På hvilken måte?

4. Er det segmenter ved det norske samfunnet som er mer utsatt for det siste årets endringer i trusselbildet enn andre?
- Hvilke?
- Hvorfor er disse segmentene mer eksponert enn andre?
- På hvilken måte er norske sivile virksomheter eksponert for endringene i trusselbildet?
- Hvilke metoder benyttes mot norske sivile virksomheter?
- Hvilke trusselaktører står bak?
- Til hvilken grad er norske virksomheter eksponert for interstatlig påvirkning?

5. På hvilken måte har samfunnsdigitaliseringen bidratt til å utvikle nye sårbarhetsflater for den norske samfunnssikkerheten?
- Hvilke digitale sårbarhetsflater er mest eksponert?

- Til hvilken grad utgjør digitale verdikjeder, underleverandører og tjenesteutsetting en sårbarhetsflate for den norske samfunnssikkerheten?
- Hvordan påvirkes de digitale sårbarhetsflatene av den sikkerhetspolitiske utviklingen?

Del II – Utviklingen i trusselbildet mot norsk kraftforsyning

6. Til hvilken grad skyldes dagens energikrise i Europa ringvirkninger fra krigen i Ukraina?
- Hvordan påvirker energikrisen Norge?
- Hvordan påvirkes norsk energisikkerhet og norsk energipolitikk?

7. Har trusselbildet mot norsk kraftforsyning forandret seg det siste året?
- På hvilken måte?
- Hvem er de største trusselaktørene?

- Hvis ja:
- Til hvilken grad er forandringene i trusselbildet en konsekvens av energikrisen i Europa og Russlands angrepskrig i Ukraina?

8. Hvordan vil fremtidens trusselbilde påvirke norsk kraftforsyning?
- Hvordan påvirkes sikkerheten rundt kraftforsyningen av forandringene i trusselbildet?

9. Hvilke sentrale sårbarheter foreligger i opprettholdelsen av leveransesikkerheten til norsk kraftforsyning?
- Hvilke fysiske sårbarhetsflater foreligger?
- Hvilke digitale sårbarhetsflater foreligger?
- Til hvilken grad utgjør sårbarhetsflatene en digitaliseringskonsekvens?

Del III – Reduksjon av sårbarhetsflater

10. Hvordan kan sårbarhetsflatene som følger i kjølvannet av samfunnsdigitaliseringen begrenses og reduseres?
- Sårbarhetsreduserende tiltak?
- Barrier? Harde/myke?

11. Hvordan kan sårbarhetsflatene som følger i kjølvannet av den sikkerhetspolitiske utviklingen begrenses og reduseres?
- Sårbarhetsreduserende tiltak?
- Barrier? Harde/myke?

12. Hvordan kan sårbarhetsflatene ved den norske kraftforsyningen begrenses og reduseres?
- Sårbarhetsreduserende tiltak?
- Barrier? Harde/myke?

Annet:

Aktuelle dokumenter: forskrifter, instrukser, lovgivning, rammeverk, retningslinjer, etc.

- Er det flere momenter enn hva som har vært tema i intervjuet du tenker er av relevans hva gjelder sikkerheten rundt norsk kraftforsyning?
- Med tanke på anonymisering i oppgaven – hva ønsker du å omtales som?

Avsluttende kommentarer

Har du noen tilføyelser eller er det noe mer du vil legge til?

Informasjon om gjennomlesning av notater. Takk for deltakelsen.