Sosial forsterkning og demping av risiko relatert til Smart Grid-teknologi

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Juni 2020

Simen Brandvik Kristensen

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i Samfunnssikkerhet	Vårsemesteret, 2020 Åpen
Forfatter: Simen Branvik Kristensen	
Fagansvarlig: Ole Andreas Hegland Engen **Veileder:** Kenneth Arne Pettersen Gould	
Tittel på masteroppgaven: Sosial forsterkning og demping av cyber-risiko relatert til Smart Grid-teknologi **Engelsk tittel:** Social amplification and attenuation of cyber-risk related to Smart Grid-technology	
Studiepoeng: 30	
Emneord: Sosial forsterkning av risiko, Sosial demping av risiko, Cyber-risiko, Cyberangrep, AMS, Smart Grid, Risikokommunikasjon, Risikopersepsjon	Sidetall: 88 +Vedlegg/annet: 125 Trondheim 25. juni 2020

Forord

Dette prosjektet markerer slutten på to givende studieår innen *samfunnssikkerhet* ved UiS. Gjennom prosjektet har jeg utforsket mediekommunikasjons betydning for risikopersepsjon innen den digitale energisektoren, og drøftet hvorvidt dette kan ha betydning for sosial påvirkning på risiko. Dette viste seg å være en spennende og omfattende utfordring der jeg fikk mulighet til å benytte mye kunnskap jeg har tilegnet meg gjennom et meget spennende masterstudiet.

Da Covid-19 pandemien herjet under dette prosjektets gjennomførelse ble det dessverre ikke mulig å foreta så mange intervju som jeg hadde håpet, og det ble da ikke stort nok grunnlag for å anvende i prosjektet. Men jeg vil rette stor takknemlighet til de informantene som kunne ta seg tid til intervju i en hektisk periode, deres innspill har betydd mye! Og takk til Universitetet i Stavanger som innfridde ekstra tid til å jobbe med prosjektet da jeg støttet på komplikasjoner i datainnsamlingen.

Tusen takk til veileder Kenneth Pettersen Gould for verdifulle innspill og spennende samtaler. Det har blitt satt utrolig stor pris på i en hektisk prosess!

-Simen Brandvik Kristensen, 25. Juni 2020

Sammendrag

Norge er et av verdens ledende land i den digitale utviklingen, en utvikling som også har stor innvirkning på energisektoren, der utviklingen av *Smart Grid* systemer skaper et bærekraftig og fleksibelt kraftnett. Men denne fusjonen mellom kraft og informasjonsteknologi fører også med seg nye utfordringer, da energisektoren blir sårbar for tradisjonelle IT trusler som cyberangrep. Som et resultat blir det et økt behov for å forstå cyberrisiko i sektoren, ikke bare for eksperter, men også for allmennheten da et cyberangrep som rammer kraftnettet kan ha konsekvenser langt utover sektoren.

Hvordan risikoen blir kommunisert kan ha store implikasjoner for persepsjoner, som igjen kan i stor grad diktere sosiale reaksjoner under og etter en uønsket hendelse. Dette prosjektet undersøker derfor hvordan nyhetsmediers risikokommunikasjon angående cybertrusler relatert til Smart Grid systemer har blitt kommunisert til allmennheten. Og hvilke konsekvenser denne kommunikasjonen kan ha for sosial forsterkning av risiko.

For å undersøke denne problemstillingen ble det utført dype dykk i dokumenter angående Smart Grid systemer, samt cybertruslene de står overfor. Og deretter ble det utført en medieanalyse og sentimentanalyse for å kunne, basert på mediers ordvalg, kategorisere artikler som negative eller positive i sine skildringer av Smart Grids. Målet er at dokumenter fra sentrale myndigheter og aktører gir et dypere og informerende innblikk i risikoprofilen, mens media skildringer gir grunnlag for å trekke antagelser om befolkningens risikopersepsjoner. Analysens funn blir drøftet i lys av teoretiske rammeverk som *Normal Accidents Theory* (NAT), *Risk Governance Framework* (IRGC) og *Social Amplification of Risk* (SARF). For å skildre risikoprofilens kompleksitet og usikkerhet, hva risikokommunikasjon kan og bør innebære. Samt hvordan risikokommunikasjon kan ha følger for sosiale reaksjoner og derfor skape ytterligere konsekvenser i møte med en ekstraordinær situasjon.

Prosjektet konkluderer med at mediebildet ikke skildrer cybertrusler den norske energisektoren står overfor på tilstrekkelig vis. Og derfor at befolkningen antageligvis ikke er oppmerksomme på trusselbildet. Denne underkommuniseringen kan ha sosiale konsekvenser utover den initierende hendelsen. Nyhetsmedier har stor innlytelse på risikopersepsjoner, og derfor bør det være større toleranse for å uttrykke usikkerhet. Ved å i større grad skildre cybertrusler som kan ramme energisektoren kan det tenkes at befolkningen blir mer bevisste, og derav skapes en kollektiv beredskap, eller *public resilience.*

Innholdsfortegnelse

1. Innledning **1**
1.1 Bakgrunn 1
1.2 Problemstilling 3
1.3 Tidligere forskning 5
1.4 Faglig relevans 7
1.5 Oppgavens struktur 9

2. Kontekst **10**
2.1 Digitalisering, trusler og muligheter 10
2.2 Systembeskrivelse 13
2.2.1 Strømnettet 13
2.2.2 Smart Grid 15
2.2.3 AMS 17
2.2.4 IoT, Stordata og Skytjenester 18
2.2.5 Elhub 19
2.2.6 SCADA og fleksibelt forbruk 20
2.3 Aktører og lovverk 21

3. Teoretisk rammeverk **26**
3.1 Begrepsavklaring 26
3.1.1 Risiko 26
3.1.2 Verdi, trussel og sårbarhet 27
3.1.3 Sikkerhet og sikkerhet 28
3.1.4 Cybersikkerhet 29
3.2 Kompleksitet og tette koblinger (NAT) 29
3.3 Risikokommunikasjon (IRGC) 32
3.4 Sosial forsterkning av risiko (SARF) 38

4. Metode **43**
4.1 Forskningsdesign 43
4.2 Litteratursøk 44
4.3 Medieanalyse 46
4.4 Kvalitetskriterier 51

5. Empiri **54**
5.1 Smart Grids og trusselbildet 54
5.1.1 Cyberangrep i energisektoren 54
5.1.2 Sikkerhetsmyndigheter og trusselbildet 56
5.1.3 Trusselaktører og angrepsmetoder 60
5.1.4 Oppsummering 61
5.2 Smart Grids og Media 62

5.2.1 Mediebildet 62
5.2.2 Smart Grid i media fra år til år 63
5.2.3 Tematiserte medier 70
5.2.4 Oppsummering 72

6. Drøfting **74**
6.1 Hvilke følger har digitalisering av energisektoren for trusselbildet? 74
6.2 Hvordan blir Cyberrisiko relatert til Smart Grid teknologi belyst i mediebildet? 76
6.3 Hvilken grad av overensstemmelse eksisterer mellom risikoprofilen beskrevet av sentrale myndigheter og risiko som kommuniseres av media? 81

7. Konklusjon **85**
7.1 Forslag til videre forskning 87

8. Litteraturliste **87**

Vedlegg **106**
Vedlegg 1: Medieanalyse 106
Vedlegg 2: Kilder til medieanalyse 116
Vedlegg 3: Sentimentanalyse 120

Figurer

Figur 1: Sammenhengen mellom kommunikasjon, persepsjon og reaksjon.

Figur 2: Nytt kommuniserende kraftnett

Figur 3: Nyskapende kommunikasjonsplattform

Figur 4: Risikotrekanten

Figur 5: Risk Governance Framework

Figur 6: The risk management and stakeholder involvement

Figur 7: The social amplification of risk framework

Figur 8 Utvidelse av SARF modell

Figur 9: Complexities in Identifying, Understanding and Analyzing Criticial Infrastructure Interdependencies

Figur 10: Cyberangrep og sikkerhetshendelser i norsk energisektor

Figur 11: Smart Grid relaterte artikler utgitt etter år

Figur 12: Positiv og negativ vekting av Smart Grid relaterte artikler, 2003-2020

Figur 13: Ulikheter i teknologisk- og økonomisk belysning av Smart Grid teknologi

Figur 14: Effekter av under- og overrapportering av risikokilder

Tabeller

Tabell 1: Medieanalyse

Tabell 2 Positive og negative nøkkelord for sentimentanalyse

Tabell 3: Antall positive stikkord benyttet i artikler fra 2011

Tabell 4: Stikkord relatert til cyberangrep registrert i 2016

Tabell 5: Stikkordsøk i artikler 2018 og 2019

Tabell 6. Skille mellom teknisk- og økonomisk-fokuserte mediekilder.

Tabell 7: Mediers belysning av artikler

1. Innledning

1.1 Bakgrunn

Norge er et av verdens mest digitaliserte land og samfunnets avhengighet av strøm og IKT fortsetter å øke (DSB 2019, s.200). Videre øker interesse og utvikling av Smart Grid teknologi, noe som innebærer fusjonen av IT- og energisektoren. Systemet innebærer enorme muligheter for effektivisering og bærekraft, men fører også med et nytt trusselbilde da energisektoren i større grad blir inkorporert i det digitale landskap. Og blir derav sårbart for IKT-trusler (Mendel 2017).

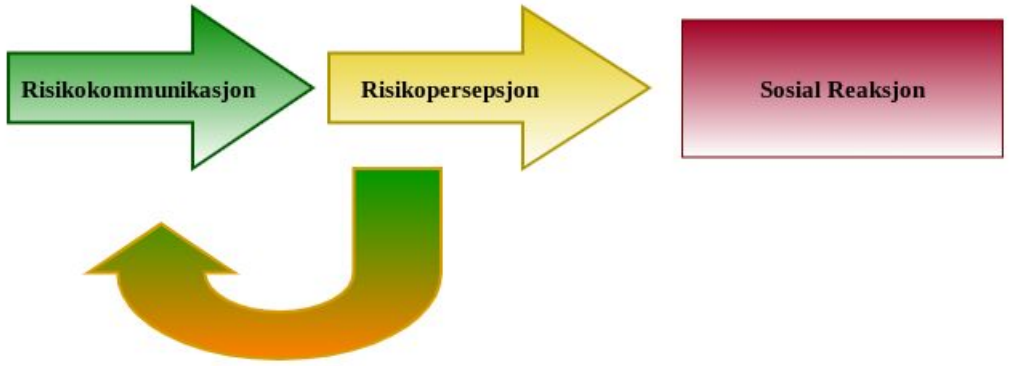
Norge har aldri opplevd et cyberangrep som rammer en hel samfunnssektor (DSB 2019, s.200). Selv om det kan tyde på at kritiske samfunnsfunksjoner da er tilstrekkelig sikret påpeker eksperter at det digitale domenet er preget av stor usikkerhet (NSM 2020). Samtidig har denne følelsen av trygghet resultert i at befolkningen har forventninger om sikker, stabil og avbruddsfri energiforsyning.

Slike følelser og tillit rettet mot myndigheters risikohåndtering og opprettholdelse av samfunnsfunksjoner blir formet gjennom en rekke ulike personlige og sosiale prosesser. Slike persepsjoner er subjektive inntrykk og tolkning av informasjon (Renn 2008, s.93). Persepsjoner om risiko innebærer derfor forventninger om mulige risikohendelser. Når man i liten grad har direkte kontakt med risikokilden vil kommunikasjon være av stor betydning, og nyhetsmedier får potensielt en sentral rolle. Cyberrisiko innen Smart Grid systemer er upersonlig for allmennheten, da individer har liten mulighet til å kontrollere den, og den er kompleks. Dette fører til at informasjonsbehovet om risiko tilfredsstilles gjennom nyhetsmedier, og det er derav grunn til å anta at befolkningens risikopersepsjoner angående Smart Grids er i stor grad påvirket av mediers kommunikasjon. Videre kan risikopersepsjoner ha stor betydning for sosiale reaksjoner i møte med en uønsket hendelse.

Sammenhengen mellom kommunikasjon, persepsjon og sosiale reaksjoner

Dette prosjektet arbeider med antagelsen om at media som kommunikasjonskanal, av en risikokilde den generelle befolkningen ikke har direkte erfaring med, vil være en sentral aktør innen forming av risikopersepsjoner. Videre vil risikopersepsjoner ha en betydelig innvirkning på den sosiale reaksjonen som oppstår i møte med en risikohendelse.

Det er betraktes derfor som essensielt å skildre mediebildets risikokommunikasjon om cybertrusler innen Smart teknologi for å så kunne gjøre antagelser om befolkningens persepsjoner om tema. Da nyhetsmediers belysning av risikoen kan ha direkte konsekvenser for samfunnets reaksjoner i møte med et cyberangrep i norsk energisektor.



Figur 1: Sammenhengen mellom kommunikasjon, persepsjon og reaksjon.

Det erkjennes at kommunikasjonsprosessen går to veier som figur 1 illustrerer. Media setter dagsorden ut i fra informasjonsbehov, og videre informasjonsbehov skapes av respons. Medier vil være relevante og befolkningen vil være informert. Figuren viser til hvordan media og publikum spiller av hverandre, og risikokommunikasjon kan skape persepsjoner som igjen fører til et nytt informasjonsbehov. Med andre ord eksisterer det en tilbakeføring sløyfe mellom medier og befolkning, fremfor en enveisprosess der befolkning er svamper av mediers budskap (Petts et al. 2001).

1.2 Problemstilling

Basert på energisektorens kritikalitet for infrastruktur og samfunnsfunksjoner, samt cyberdomenets økende kriminelle aktivitet og utvidende angrepsflate, kan det tenkes at konsekvenser av et eventuelt vellykket angrep vil ha effekter utover de rent fysiske. Da flere deler inkorporeres i et system øker kompleksiteten og som et resultat blir sikkerhet en betydelig utfordring. Ved å fokusere på risikokommunikasjon med den hensikt å skape en delt kunnskapsflate i samfunnet, kan risikoens sosiale bølge-effekter mitigeres i møte med en uønsket hendelse. Som en sentral kommunikasjonskanal vil nyhetsmedier ha påvirkning på forming av risikopersepsjoner, og derav innflytelse på sosiale reaksjoner.
Det vil derfor være hensiktsmessig å forsøke å besvare følgende problemstilling:

> ***Hvordan kan medias risikokommunikasjon angående cybertrusler i Smart Grids påvirke risiko?***

Digitaliseringen av energisektoren skaper nye muligheter og verdier, men presenterer også nye utfordringer. I takt med Smart Grid utviklingen ekspanderer trusselbildet og angrepsflaten. Risiko beskrivelser fra sentrale myndigheter og aktører reflekterer ekspertise, og er det nærmeste man kommer beskrivelser av en faktisk sikkerhetstilstand. For å senere kunne beskrive mediers risikokommunikasjon som tilstrekkelig eller ikke, er det nødvendig å kartlegge risikoprofilen slik som beskrevet av myndigheter. Første forskningsspørsmål er derfor formulert:

> *Hvilke følger har digitalisering av energisektoren for trusselbildet?*

Videre er media den største kommunikasjonskanalen til den generelle befolkningen. Nyheter videreformidles fra media og tolkes i ulike sosiale kontekster som bidrar til å utvikle persepsjoner om en gitt risiko. For å kunne drøfte eventuelle sosiale reaksjoner i møte med et cyberangrep er det viktig å forsøke å kartlegge eksisterende risikopersepsjoner.
Forskningsspørsmål nummer to blir derfor:

Hvordan blir Cyberrisiko relatert til Smart Grid teknologi belyst i mediebildet?

Videre har undersøkelser vist at mennesker har større grad av tillit, og føler en større grad av sikkerhet dersom en risiko er blitt ansvarlig innrammet, rasjonelt diskutert og gjort kjent. Overensstemmelse mellom sentrale myndigheter og aktørers beskrivelser og mediers belysning viser til åpen kommunikasjon og videreformidling av ekspertise om risikoprofilen. Dersom myndighetenes beskrivelser viser til en større risiko enn profilen formidlet via media, kan det tyde på at befolkningen ikke er oppmerksomme på risikobildet og vil derfor være mindre forberedt på en uønsket hendelse. Overensstemmelse i beskrivelser av risikoprofilen kan derfor ha store implikasjoner for hvordan samfunnet responderer under og etter en uønsket hendelse. Et tredje forskningsspørsmål blir da:

Hvilken grad av overensstemmelse eksisterer mellom risikoprofilen beskrevet av sentrale myndigheter og risiko som kommuniseres av media?

Avgrensning

Målet med prosjektet er å utforske cyber risikoen tilknyttet Smart Grid systemer, og hvordan denne risikoen blir kommunisert gjennom medier. Som kommunikasjonskanal er media et bindeledd mellom allmennheten og hendelser på både nasjonal og internasjonal basis. Informasjonen media vektlegger og presenterer dikterer mye av kunnskapen vi mottar. Og derfor persepsjoner vi skaper og utvikler. Det kan tenkes at dersom informasjonen er mangelfull eller misvisende, kan det ha konsekvenser for samfunnet i møte med en uønsket hendelse.

Problemstilling og forskningsspørsmål viser til energisektoren, trusselbildet, media og myndigheter som interessant for forskningsprosjektet, men det er gjort avgrensninger i gjennomføringen av undersøkelser.

Energisektoren omfatter en rekke aktører og lovverk, og digitalisering av sektoren skaper også et mer omfattende trusselbilde. Dette prosjektet søker ikke å kartlegge truslene i sektoren i sin helhet, men fokuserer heller på tilsiktede cybertrusler da dette viser seg som en

økende bekymring. Videre vil heller ikke prosjektet fokusere på en enkelt virksomhet eller hvordan de tilnærmer seg problematikken, men heller undersøke sårbarheter i sektoren generelt for å videre undersøke hvordan dette kommuniseres gjennom nyhetsmedia. Med myndigheter refereres det til sentrale sikkerhetsmyndigheter, spesielt Nasjonal sikkerhetsmyndighet (NSM), da de har stort fokus på cybersikkerhet. Enkelte offentlige utredninger vil også benyttes for å kartlegge risiko i det digitale landskap.

Media avgrenses til nyhetsmedier og enkelte sentrale aktører innen Smart Grids som bidrar i nyhetsbildet. Denne begrensningen gir mulighet til å generere data fra en rekke ulike kilder for å kunne beskrive belysning av tema, samtidig som det utelukker sosiale medier. Studiet anerkjenner derimot sosiale mediers betydning for kommunikasjonsprosessen og derfor persepsjoner. Men nyhetsmedier betraktes som en større formidler av informasjon relatert til Smart teknologi innen energisektoren.

Avgrensningen gir mulighet til å undersøke en stor, men spesifik kommunikasjonskanals belysning av ny teknologi. Samt hvilken betydning denne belysningen kan ha for persepsjoner.

1.3 Tidligere forskning

Det eksisterer mye foreliggende forskning innen risikopersepsjon, det spenner bredt faglig. Med relevans innenfor blant annet sosiologi, sosialantropologi, psykologi og sikkerhetsfag. Kunnskap om risikopersepsjon er essensielt for vellykket risikokommunikasjon. Viten om hvordan risiko oppfattes og videre kommuniseres er derfor av stor betydning for å videre kunne benytte SARF rammeverket for å predikere potensielle sosial utfall av risiko.

Medias påvirkning på risikopersepsjoner

Health and Safety Executive (HSE) rapport 329/2001 presenterer funn fra et britisk prosjekt som undersøkte medias rolle i risiko amplifikasjon blant befolkningen. Funnene motsier myten om at befolkningen er passive mottakere av informasjon fra eksperter. Tvert i mot

rasjonaliserer man og tolker risiko-informasjon gjennom flere perspektiver og dimensjoner. Personlig erfaring, allmennkunnskap, og formidlet informasjon fra en rekke kommunikasjonskanaler utvider muligheter for differensiering i tolking av informasjon og skaper dynamiske mottakere. Videre viser også rapporten media som dynamiske tolkere og formidlere av informasjon. De søker å respondere til, og reflektere sosiale preferanser og bekymringer, da befolkningen er sofistikerte brukere av media.

HSE rapporten konkluderer med SARF rammeverket presentert på 1980-tallet ikke kan håndtere et fullstendig bilde av medias påvirkning. Rapporten stresser også at media må sees som en mulighet og et redskap framfor et problem (Petts et al. 2001).

Likevel har flere forskningsprosjekter vist til korrelasjon mellom mediadekning og økende grad av risikopersepsjoner. Selv om befolkning er dynamiske mottakere av informasjon spiller medier en viktig rolle innen risikokommunikasjon, spesielt i henhold til risikoprofilen der publikum har mindre personlig erfaring (Frh 2017; Park & Sohn 2013; Kone & Mullet 1994: Gore et al. 2005; Jung & Ha 2016).

HSE rapportens påvirking på dette studiet er dens beskrivelser av kommunikasjon mellom media og befolkning, dens konklusjoner angående SARF rammeverket anerkjennes. Men for dette studiets formål vil rammeverket, særlig dens beskrivelser av risiko forsterkelse og demping i møte med komplekse, usikre og tvetydige risikoer, være et godt analyseverktøy. Det påpekes at Kasperson et al. først presenterte rammeverk supplementeres med Aven og Fjæans (2019) utvidelse av rammeverket.

Usikkerhets-basert tilnærming til risiko

Fjæran og Aven (2019) beskriver i *"Making visible the less visible- how the use of an uncertainty-based risk perspective affects risk attenuation and risk amplification"* hvordan en usikkerhet-basert tilnærming til risiko vil ha følger for eventuell demping og forsterkelse. Gjennom en anlayse av risikokommunikasjons-prosessen angående bruk av Narasin, et fortilsetningstoff, foreslår forfatterne en utvidelse av SARF-rammeverket. Formålet er å gjøre mer omfattende analyser ved å inkludere faser før en uønsket hendelse, da forfatterne påpeker at sosial påvirkning av risiko ofte stammer fra "ikke-hendelser". Disse "fasene" reflekterer

SARF rammeverket, men inkluderer slike usikre "ikke-hendelser", deres responser, eller mangel på responser. Poenget er at negativ risiko, uansett om en uønsket hendelse utspiller seg eller ikke, vil ha visse fortolkninger, persepsjoner og derfor ha en sosial dimensjon (Fjæran & Aven 2019).

Cyber-trusler i kraftsektoren

Det er også gjort studier angående risikopersepsjon mer spesifikt innen informasjonssikkerhet i kraftbransjen. Marie Røyksund (2011) tar for seg hvordan aktører innen kraftforsyningen opplever og håndterer cybertrusler. Studiet påpeker den økende kompleksiteten som resultat av IT og elkrafts fusjon, samt hvordan dette ekspanderer trusselbildet.

Studiets funn påpeker, etter gjentatte intervju, at kraftbransjen oppfatter målrettede dataangrep mot driftskontrollsystem som lite sannsynlig. Tiltak innen sektoren er basert på foreliggende ROS-analyser, interne retningslinjer, samt enkelte myndighetskrav (Røyksund 2011).

Det har skjedd store endringer, særlig teknologisk, siden 2011, og trusselbildet er ytterligere ekspandert i kraftbransjen. Det vil derfor være interessant å se hvordan media belyser denne utviklingen, og hvordan man kan kommunisere slike komplekse risikoer.

1.4 Faglig relevans

Samfunnssikkerhet omhandler et samfunns evne til til å beskytte seg mot og respondere til hendelser som truer fundamentale verdier og funksjoner for innbyggeres liv og helse (Engen et al. 2016, s.30). Norge er en nasjon i endring. Stadig flere integrerte funksjoner og infrastrukturer avhengig for samfunnets velstand og virkning blir digitale. Digitalisering er essensielt i den moderne verden for automatisering, effektivisering og videre verdiskapning, men som en konsekvens blir flere verdier sårbare for digital manipulasjon, spionasje og sabotasje (NSM 2020). Et økende fokus på helhetlige digitale sikringstiltak blir derfor av avgjørende betydning for samfunnets videre funksjonalitet.

Når digitalisering strekker seg lengre i komplekse verdikjeder som inkorporerer alminnelige husstander og hverdagslige objekter gjennom innovativ *smart* teknologi, blir angrepsflaten stor, trusselbildet uoversiktlig, og samtidig derfor i større grad, et linjeansvar blant samtlige borgere.

Sikkerhetsfokus på så omfattende skala krever tilstrekkelig risikokommunikasjon. Kommunikasjon er igjen avhengig av kunnskap om persepsjoner som videre i betydelig grad bygger på media opplysninger.

God beredskap krever gode prediksjoner om hva som kan skje i fremtiden. Kunnskap om hvordan diverse systemer kan rammes og hvilke utfall dette vil ha blir viktig for å gjøre samfunnet robust og resilient i møte med ekstraordinære situasjoner. Dersom samfunnet møter et scenario som man på ingen måte var forberedt på vil sannsynligvis konsekvensene bli mer alvorlige.

Dette er også tanken bak sosial forsterkning og demping av risiko. Dersom mennesker inkorporert i en kompleks, tett koblet verdikjede ikke har noen kunnskap om potensielle hendelser og konsekvenser, er tanken at sosiale reaksjoner forsterker risiko og utgjør ytterligere skade enn først antatt (Kasperson & Kasperson 1996).

Det vil derfor være fruktbart å utføre en komparativ undersøkelse av kommunikasjonskanaler og ekspertvurderinger. Dersom det eksisterer en overensstemmelse mellom disse kan man anta at eksperter og den generelle befolkning har noe kunnskap om potensielle farer med *smart* teknologi. Og derfor at samfunnet i større grad er kapabel til å takle uforutsette hendelser i det komplekse digitale nettverk som er Smart Grid teknologi.

Denne potensielle problematikken vil bli undersøkt gjennom samfunnssikkerhetsfaglig teori, belyst av SARF-modellen, risikokommunikasjon, gjensidig avhengighet og tette koblinger.

1.5 Oppgavens struktur

I dette prosjektet vil fenomenet sosial påvirkning av risiko, med vekt på kommunikasjon og persepsjoner, knyttes til digitaliseringen av energisektoren.

Kapittel 1 vil introdusere denne tematikken, presentere problemstilling og forskningsspørsmål, samt belyse tidligere relevant forskning.

I kapittel 2 vil sette prosjektets kontekst, noe som inkluderer systembeskrivelser, trusler og sårbarheter, aktørbildet og lovverk som er av relevans for energisektoren.

Deretter vil kapittel 3 redegjøre for det teoretiske rammeverket benyttet for å svare på problemstillingen. Og kapittel 4 vil inneholde anvendt metode, samt begrunnelse av valg tatt i forskningsprosessen.

Videre vil kapittel 5 vise til funnene som blir drøftet i lys av teori i kapittel 6.
Til slutt presenterer kapittel 7 konklusjoner trukket basert på prosjektets funn, og gir forslag til videre forskning.

2. Kontekst

2.1 Digitalisering, trusler og muligheter

Digitalisering

Dagens samfunn, og dens medlemmers tilværelse, er betraktelig forskjellig fra tidligere. Gjennom et historisk perspektiv kan strukturelle og sosio kulturelle utviklinger sies å være kontinuerlige drivere for et samfunns modernisering. Men man kan særlig peke på den teknologiske utviklingen som springbrettet som fører samfunn fra det førmoderne, inn i det revolusjonerende, digitale og effektiviserte.

I sin enkleste form kan man forstå begrepet digitalisering som tilretteleggingen for generering og håndtering av data via informasjonsteknologi. Fra det analoge til det digitale (Dvergsdal 2019).

En form for revolusjonerende teknologi finner man i alle historiske epoker, men få har hatt den innvirkningen på verden som man har opplevd de siste 100 årene. Fra Nikola Tesla sine tanker om et verdensomfattende trådløst system på tidlig 1900 tallet, til de første mekaniserte, søkbare systemer på 1930 tallet. Frem til Licklider skjematiserte og populariserte ideen om et "intergalaktisk" nettverk av datamaskiner på 1960 tallet. Og til det store spranget på 1990-tallet da Berners-Lee oppfant verdensveven, har vært store milepæler i den digitale revolusjon (Andrews 2013).

Teknologisk nyskapning har på ingen måter stanset med årene. Internettet ble en altomgripende anvendelse og har forårsaket videre eksplosiv økning innen teknologi. Internett-teknologi påvirker samtlige sektorer i dagens samfunn. Det gir muligheter for å yte smartere og mer effektiv kundeservice, og skaper nye verdier og forretningsmodeller gjennom nettverking, stor data, automatisering og digital kommunikasjon (Schallmo et al. 2018, s.2).

Cyber kriminalitet

Denne digitale transformasjonen kan beskrives som den banebrytende forandringen av hele forretningsverden gjennom ny teknologi basert på internett, som videre har fundamentale implikasjoner for samfunnet i sin helhet. Denne evolusjonen fører med seg mange muligheter, men også økt kompleksitet, tette koblinger, og som et resultat, sårbarheter (Digital21 2018, s.2).

> "*A society that applauds innovation in the world of business can hardly expect to escape innovation in the world of crime*" (Ross 2016, s.121).
>
> -Leon Radzinowicz

Den digitale utviklingen har også hatt enorme følger for ondsinnede handlinger slik som tyveri, svindel, sabotasje og krigføring. Teknologi skaper nye verdier, verdier som kan bli eksponert og utnyttet i et stadig ekspanderende trusselbilde.

Digitalisering binder samfunnet sammen i enorme digitale verdikjeder som, dersom ikke tilstrekkelig sikret, ekspanderer samfunnets angrepsflate. Teknologisk innovasjon byr også på kriminell innovasjon. Digitale angripere i dag kan benytte verktøy for ytre "virkelig", fysisk skade gjennom digitale midler. For eksempel kan smarte høyttalere og hodetelefoner *hackes* og ytre helseskadelig lydsignaler (Carlsen 2019).

Videre blir flere samfunnsviktige strukturer og funksjoner avhengige av hverandre, og omtrent alt avhenger av kraft og IKT. Da disse sektorene fusjoneres i skapelsen av et mer intelligent strømnett og samfunn generelt, kan det tenkes at en uønsket hendelse kan få enorme ramifikasjoner. Ikke begrenset til infrastruktur og materielle verdier, men for liv, helse, samfunnsstabilitet, styringsevne og kultur (DSB 2019, s.29).

Implikasjoner for energisektoren

Denne konteksten, digitalisering og internett med sine sårbarheter, blir i større og større grad introdusert i energisektoren. Norge er verdens mest digitaliserte land (Norsis 2017a), og med den stadige digitale utviklingen vil energidistribusjon bli mer sammensveiset med

informasjon- og kommunikasjonsteknologi. Dette innebærer at to sentrale kritiske, bærebjelker i samfunnet blir gjensidig avhengige og tett koblet (IRGC 2006, s.50). Dette vil kreve en enorm digital kompetanse for å fungere sikkert og som forventet, og for å fostre tillit, forståelse og trygghet blant befolkningen.

I 2016 forårsaket hackere et massivt strømbrudd i Ukraina som rammet flere hundre tusen mennesker (Knudsen 2016). Når strømnettet kan bli felt gjennom digitale broer viser det til en stor samfunnsmessig sårbarhet. At slike sårbarheter vil øke er frykten for fremtiden.

Dagens fokus for utvikling i energisektoren går under fellesbetegnelsen "Smart Grid" (SG). Det omfatter all innovasjon i sektoren og presenterer et nytt generasjons strømnett der ny kommunikasjonsteknologi blir anvendt for å forbedre energiinfrastruktur og distribusjon (Yacout 2013, s.1). Motivasjonen for denne utviklingen er flerfoldig. Miljømessige, samfunnsmessige, teknologiske, og økonomiske fordeler vil bli resultatet av et mer adaptivt, automatisert nett som med bedre evne kan respondere ved utfall eller uforutsette situasjoner (Sæle 2014).

Innovasjonens betydning for trusselbildet

Smart Grid visjonen er fremtiden, men bekymringer følger med. Spesielt to faktorer gir bekymringer, tette koblinger og økt kompleksitet.

For det første, som beskrevet, vil stadig økende koblinger blant infrastrukturer, industrielle kontrollsystemer og smart-teknologi øke sårbarhet for cyberangrep. Dersom verdien er digital kan den kompromitteres via digitale verktøy. Potensielle angrep kan skade systemer som igjen kan forårsake uforutsette kaskadeeffekter grunnet tett koblede systemer og komplekse verdikjeder (NSM 2017, s.9).

For det andre åpner Smart-teknologi et helt nytt marked. Videre utvikling som ofte fokuserer på økonomisk gevinst gjør at sårbarhetsreduserende tiltak ofte kommer i etterkant (Ibid, s.7). Det fleksible nettet med prosumenter og IoT-gjenstander (*Tingenes internett)* videre kompliserer risikobildet og trekker husstander og den allmenne befolkningen mer inn i nettet, dette øker sårbarheten for samfunnet totalt (Mendel 2017).

Det betyr at samfunnssikkerhet blir i større grad et linjeansvar (Skotnes 2017). Gjennom den teknologiske utviklingen og IoT vil gjenstander som sannsynligvis ikke tar særlig hensyn til trusselbildet bli inkorporert. Angrepsflaten blir derfor omfattende og verdikjedene uoversiktlige.

2.2 Systembeskrivelse

2.2.1 Strømnettet

Det norske strømnettet ble konstruert mellom 80 og 120 år tilbake med den hensikt å transportere strøm fra store kraftverk til forbruker (The norwegian smartgrid centre u.å.d). Nettets funksjon er som bindeledd mellom produsent og kunde, samt tilknytning til utenlandske kraftsystemer. Strømnettet er en sentral infrastruktur av ethvert moderne samfunn, det står for produksjon, overføring og omsetning av energi (Energifakta 2019b). Kraftnettet er essensielt i energiforsyning da elektrisk energi ikke produseres der den forbrukes. Kostnader, sikkerhet, leveringskvalitet, miljø og samfunnsaksept er hovedaspekter innen energiforsyning (Sand 2015, s.3). Videre må nettet dimensjoneres for å håndtere variasjon i forbruk. Under vintersesongen må nettet kunne håndtere ekstra energiforsyning, samt være i stand til å importere ekstra kraft over tid, som for eksempel i ekstra tørre år.

Regulering i strømnettet skjer på tre nivå. *Transmisjonsnettet* fungerer som knutepunkt mellom kraftprodusenter og brukere på landsbasis, og styres av Statnett. Dette systemet inkluderer også forbindelser utenfor nasjonale grenser. Videre er det *Regionalnettet* som kobler transmisjons- og distribusjonsnettet, og omfatter produksjon- og forbruksradialer med sterkere spenning.
Distribusjonsnettet omfatter lokale kraftnett som forsyner mindre sluttbrukere. Hverdagslig forbruk kobles opp mot distribusjonsnettet, men større produksjonsanlegg gjerne knyttes til transmisjons- eller regionalnettet (Energifakta 2019b).

Nordmenn er store forbrukere av elektrisk energi, som i større og større grad forsynes av småkraft. Forbruket øker stadig samtidig som samfunnet blir mer avhengig av pålitelig og sikker forsyning. Produksjon må følge tilgang på ressurser, og kilder til fornybar energi som vind, sol og elvekraft lar seg i liten grad regulere. Derav øker behovet for intelligente, fleksible strømnett (The norwegian smartgrid centre u.å.d).

I dagens moderne samfunn er strøm av stor kritikalitet og forsynings mønsteret med fremtidige prediksjoner kan ikke være avhengig av utdatert infrastruktur. Kraftnettet kan med andre ord ikke forventes å tolerere fremtidens nødvendige kapasitet. EU reguleringer, fallende kostnader for fornybar energi, samt forbrukertrender har skapt motivasjon til å erstatte fossil energi, skape energieffektivisering og forbedre forsyningssikkerhet. Tilby bedre leveringskvalitet og økonomisk effektivisering (Sand 2015, s.46; Regjeringen 2018; Hovland 2018).

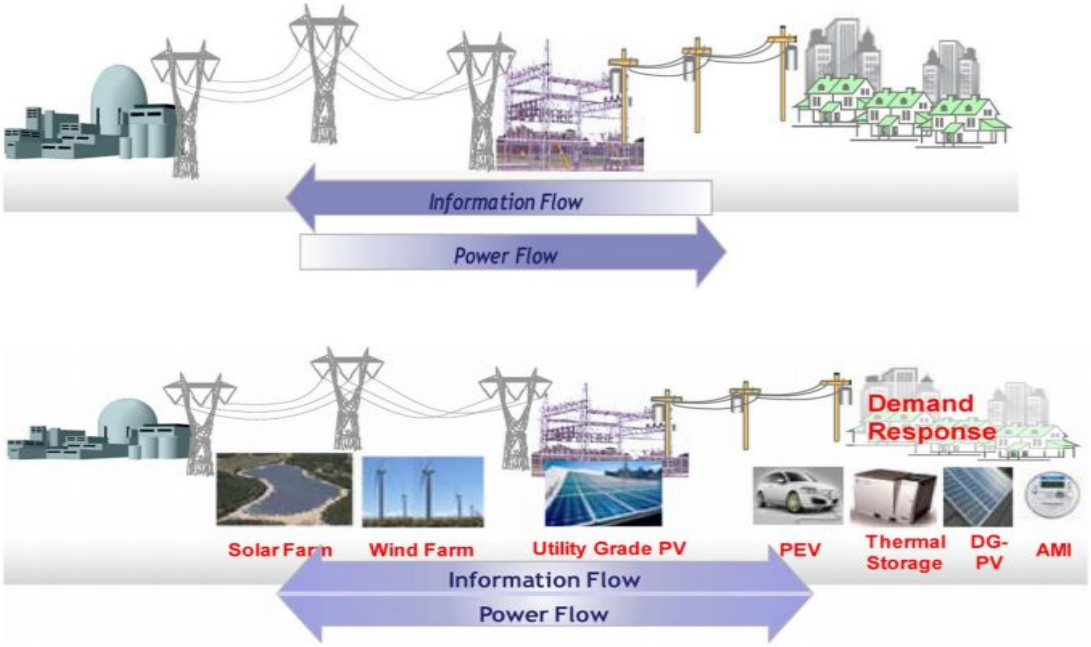
Med dette i fokus forventes kraftnettet å være i kontinuerlig forandring opp mot 2040, og de nordiske transmisjonssystem operatørene (TSO) planlegger oppgraderinger i kraftnettet med en kostnad på inntil 15 milliarder euro frem til år 2028. Investeringene skal øke nettets kapasitet, redusere flaskehalser i systemet og øke integreringen av større mengder fornybar energi, spesielt fra vind (Statnett et al. 2019, s.3).

Høyere andel av periodisk energigenerering, utfaselsen av tradisjonelle generatorer, flere samhandlende komponenter, samt at frekvens- og spenningsstøtte synker fører til at kraftnettet øker i kompleksitet både for operatører og for analysering (ibid, s.4).

Det er derfor ikke bare ønskelig, men en nødvendighet å oppgradere kraftnettet. Nettverket minner om et økosystem. En enorm organisering av teknisk infrastruktur som strekker seg gjennom hele landet og knytter samfunnet sammen gjennom flyt av energi. Det øker stadig i kompleksitet og det utforskes derfor nye metoder for å kunne ha et bærekraftig og stabilt system for fremtiden.

I den forbindelse har sektoren vendt seg i økende grad mot IKT og elektronikk. Slik teknologi har blitt benyttet i kraftsektoren i mange år tidligere gjennom ulike datasystemer. Men

kraftbransjen går fra å være forbrukere av slike IKT løsninger til å bli IT-selskaper selv (Kvande 2017). En økende anvendelse av IKT skal gjøre nettet "smartere". I et holistisk perspektiv er det summen av alle delene som til sammen utgjør et intelligent, automatisert og synkronisert system (Valmot 2011). Dette vil også være den mest kosteffektive måten å oppgradere nettet på da slik teknologi blir stadig mer billig og tilgjengelig.



Figur 2: "Nytt kommuniserende kraftnett" Hentet fra Sand 2015, s.50

Resultatet blir et paradigmeskifte i energisektoren. Nye elektroniske komponenter og digital teknologi gjør det mulig å overvåke og fjernstyre, og derfor vedlikeholde og regulere kraftnettet (The norwegian smartgrid centre u.å.d).

Fra et kraftnett der operatører ikke er klare over strømbortfall enkelte steder før kunder rapporterer, til et nett der bortfall kan observeres og repareres fra kontoret (Litos Strategic Communication u.å, s.7). Og fra et nett av kunder til et nett av prosumenter, der overskuddsenergi kan føres tilbake i systemet (Halden arbeiderblad 2014; Flå 2016).
En innovasjon av teknologi som går under betegnelsen *Smart Grid*.

2.2.2 Smart Grid

Begrepet *Smart Grid* ble introdusert i 2005 som en betegnelse på en nytt generasjon av kraftnett og forbrukere. *Grid* refererer til selve kraftnettet som infrastruktur, mens *Smart* viser til objekter med innebygde operativsystem med mer avanserte data og måle evner (Yacout 2013, s.2).

Smart Grid har en rekke definisjoner. Men alle innebærer økt grad av intelligens i strømnettet gjennom digitalisering og automatisering for større grad av sikkerhet, effektivitet og samfunnsøkonomisk og miljømessig besparelse.

> *"A Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety"*
>
> -Den Europeiske kommisjon 2011 (Lund 2014, s.133)

Enkelt beskrevet kan Smart Grid sies å være fusjonen av internett og kraftnett (Sand 2016, s.4). Et system hvor store deler av anlegg, enheter og komponenter har en IP-adresse (Internet Protocol Address) som muliggjør fjernstyring og observasjon via internett. Med andre ord er det en digitalisering av kraftsektoren. Noe som innebærer en inkorporasjon av sensorer med den hensikt å blant annet måle forskjellige parametere. Sensorene bindes sammen gjennom toveis kommunikasjon, data genereres og tolkes slik at drift kan optimaliseres (Mostue & Moengen 2020, s.6).

Dagens nett er organisert i ulike tjenestesiloer basert på sin respektive funksjonalitet (Olsen 2020, s.18). I tiden fremover vil data fra de ulike vertikalene sammenstilles på en sentralisert plattform og viske ut grensene mellom siloene, og derav gi bedre innsikt i kraftsystemet som helhet (Ibid, s.15). Mer utbredt anvendelse av IT-systemer og teknologi i kraftsektoren vil kjennetegnes med blant annet at større mengder data må genereres og tolkes. Og mer integrering av teknologi som muliggjør fjernstyring og automasjon. Dette byr igjen på en rekke utfordringer sektoren må ta hensyn til. Det blir et større behov for IKT-kompetanse og

vektlegging på IKT for strategisk betydning, og derfor et krav til tilstrekkelig IKT-sikkerhet (ibid, s.15).

Smart Grid visjonen støtter seg på flere ulike teknologier og prinsipper for nettdrift. For dette prosjektets hensikt vil derimot kun de mest sentrale bli på simpel måte gjort rede for, da dette de er de viktigste elementene for å få et overordnet innblikk i morgendagens energisystem. De mest sentrale kan dog sies å være nye automatiske måle- og styringssystemer (ams), ny standardisert kommunikasjon- og databehandlingsplattform (Elhub), tingenes internett (IoT), operasjonelle driftssystemer (SCADA), batteriteknologi og forbrukerfleksibilitet, og bruk av stordata og skybaserte tjenester.

2.2.3 AMS

Automatiske Måle- og Styringssystemer (AMS) er en milepæl for kraftnettet. Fra den 1. januar 2019 ble slike målere installert i alle norske hjem (Olsen 2020, s.4). Det blir etablert en toveis kommunikasjon slik at strømforbruket registreres i sanntid og sendes direkte til distributørene. Dette gir mer og pålitelig data til netteiere, derav kan forsyningssikkerhet forbedres og strømnettet kan monitoreres og styres på en effektivisert måte.

For sluttbrukere betyr dette at man får en avregning etter eget bruk time for time. Det gir økt bevissthet, og fungerer som incentiv for lavere forbruk, samt muligheten til å levere egen produksjon gjennom solceller eller annet utstyr (ibid, s.5).

Summen er at strømbruket blir fordelt på en mer jevn, fordelaktig måte. Dyrere strømpriser når nettets belastning er høy vil føre til at mennesker er mer bevisste på sin oppførsel og som et resultat reduseres faren for overbelastning og strømbrudd. Regulering av eget strømbruk vil også bli videre forenklet gjennom mer smart teknologi, kommunikasjon mellom komponenter og styring via applikasjoner kan tillate oss full overvåkning og fjernstyring av alle elektriske komponenter i husstanden.

Nettselskapene vil være driftsansvarlige for AMS. Grunnet de store mengder data dette systemet leser vil strømforbruk og personvern være underlagt personopplysningsloven for å

ivareta kundenes rettigheter. Det omfatter at lagret data vil bli slettet etter 3 år, samt at leverandører kun kan anvende informasjonen nødvendig for å ta betaling (Nygaard 2019).

2.2.4 IoT, Stordata og Skytjenester

Tingenes Internett betegner smarte, tilkoblede enheter som kan kommunisere med hverandre og et bredere system (Olsen 2020, s.6). Utviklinger innen kommunikasjon-, sensor-, og batteriteknologi gjør det mulig for små datamaskiner å utføre oppgaver som blant annet måling av en rekke ulike parameter. IoT gjenstander kan være "smarte" hverdagslige gjenstander slik som ovner, kjøleskap, fjernsyn og lignende. Eller det kan omfatte mindre sensorteknologi og andre enheter i et større system. Fellesnevneren er at IoT-gjenstander benytter internett for å kommunisere (Øverby 2018). Dette er et viktig aspekt av evolusjonen i energisektoren. Enhver kraftlinje har ulike kapasiteter. Sensorteknologi og IoT gjør det mulig å kontinuerlig og pålitelig overvåke temperatur, ising, vinkel og vibrasjon i kraftlinjene, slik at nettet kan reguleres for å ikke overskride grenser basert på sanntidsinformasjon (Mostue & Moengen 2020, s.44).

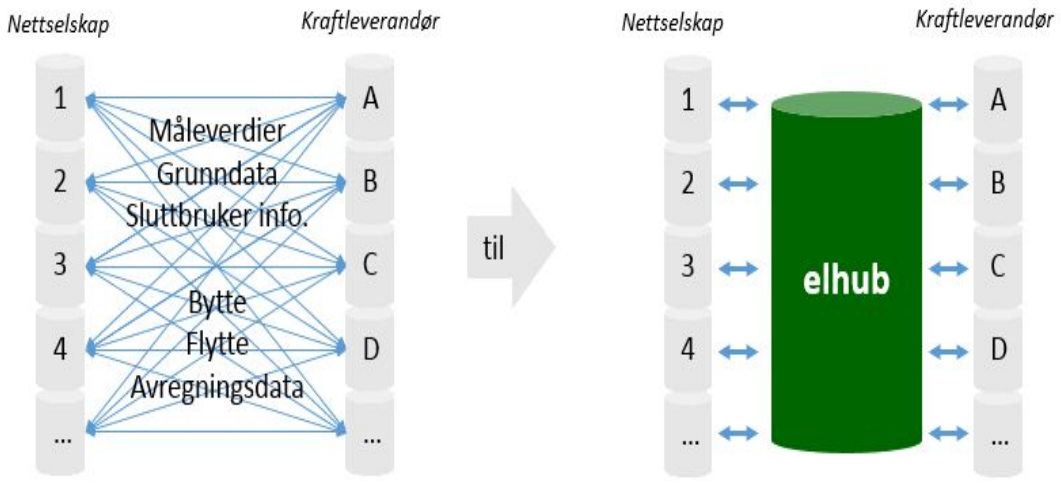
I dag er det flere hundre tusen ulike målepunkter i nettet. Den enorme mengden data disse komponentene genererer og kommuniserer gjennom IoT må så sammenstilles, analyseres og gjøres brukelig for nettdrift. Slike datamengder blir betegnet *Big Data,* eller Stordata (Olsen 2020, s7). Stordata kjennetegnes ved at mengden datasett er så store og komplekse at de ikke lengre kan håndteres av tradisjonelle datahåndteringssystemer. Denne kompleksiteten beskrives ofte av fire egenskaper ved datasettene, også kjent som de fire "V-ene". *Volum* viser til datamengde, *Velocity* (hastighet) refererer til hurtig tilgang av data. *Variety* (variasjon) handler om et stort mangfold i type data, og *Veracity* (sannferdighet) betegner informasjonens reliabilitet og kredibilitet (Olsen 2020, s.7; Mostue & Moengen 2020, s.30).

Slik data har blitt samlet i mange år for overvåkning i driftskontroller, men med økende antall enheter i systemet vil også datamengden øke. Datasett generert vil derfor bli brukt til langt flere analyseformål. Begrensningen her er som nevnt kapasiteten til systemer for å håndtere slike data. Derav blir fokuset på maskinlæring og kunstig intelligens (AI) viktigere også i energisektoren for å gjøre slik data anvendbare (Olsen 2020, s.7).

For å kunne så effektivt som mulig håndtere slike datamengder blir også skytjenester mer anvendt i energisektoren. Innen nettdrift vil tradisjonell lagring av data ikke gi tilstrekkelig mulighet til kontroll over informasjonen. Datasett vil kunne bli analysert raskere slik at selskapene kan utnytte nye driftsmuligheter og bygge skalerbare tjenester. NVE påpeker stor økonomisk nytte ved slike tjenester med tanke på datamengdene som blir produsert fra Smart Grid teknologi, særlig AMS (Ibid, s.8).

2.2.5 Elhub

Økende grad av digitalisering og databehandling krever også fornyelse av kommunikasjon. I februar 2019 ble Elhub startet i Norge (Elhub 2018). Dens funksjon som et IT-system er å effektivisere og standarisere kommunikasjon og enkelte databehandlinger i kraftmarkedet. I henhold til økt anvendelse av IKT systemer har Statnett utviklet en nøytral datahub med krav fra NVE. All måledata og markedsprosesser blir håndtert i systemet, og skaper herved et standard grensesnitt for kommunikasjon som samtlige markedsaktører må forholde seg til. Kommunikasjonsprosessen mellom leverandører, netteiere og eventuelle tredjeparter blir derav forandret til en enklere, delt plattform.



Figur 3: "Nyskapende kommunikasjonsplattform" Hentet fra Elhub 2018

Plattformen mottar og bruker meldinger for å så generere meldinger tilbake til relevante aktører. Elhub omfatter meldinger om blant annet leverandørbytter, målerverdier og endringer av grunndata (Elhub 2018; Olsen 2020, s.6).

Ved å på effektiv måte distribuere måleverdier, effektivisere avregninger, og øke nøytralitet, realiserer plattformen potensialet som ligger i AMS. En rekke tidligere aktør drevne oppgaver blir nå sentralisert i huben, markedsprosesser kan utøves raskere, og med større grad av kvalitet. Elhub har også stor grad av innebygde sikkerhetsmekanismer. Da store mengder potensielt personlig data blir sendt og utvekslet på samme plattform vil tilgangen til slike data bli under mer overenstemt tilsyn. Meldinger blir kryptert og tilgang begrenset, sannsynligvis vil dette resultere i økt personvern (Elhub 2018).

2.2.6 SCADA og fleksibelt forbruk

SCADA, eller *Supervisory Control and Data Aqcuistion,* er datasystemer som i samspill med ulike komponenter gjør det mulig å overvåke og fjernstyre industrielle prosesser (Olsen 2020, s.15). SCADA har vært i bruk i flere år da det benyttes i hovedsak til å drifte høyspentnettet. Datasystemet er innvolvert i for mange deler av nettdriften til at det vil erstattes med det første. Et skifte i en så fundamental del av driften vil by på unødvendig risiko, og det forutsees derfor at det vil være en del av fremtidens nettverk (Andreassen 2017).

SCADA må derimot adapteres til nye verdikjeder i sektoren. Teknologisk innovasjon og økende anvendelse av fornybar energi tillater konsumenter å i tillegg bli produsenter, herav begrepet *Prosumenter.* Enveis-kommunikasjon og distribusjon blir erstattet med en toveis modell der kunder kan legge overskuddskraft tilbake på nettet. For infrastruktur og drift byr dette på utfordringer. Planlegging, drift og stabilitet av distribusjonsnettet kan settes på prøve. Selskaper blir derfor underlagt press for utbygging av infrastruktur for å dimensjonere etter økt forbrukerfleksibilitet.

Denne utfordringen skal møtes til dels med ny batteriteknologi. Ved å inkludere batterier i nettet kan man benytte mellomlagring av energi, og derav gi blant annet mer balansert

forsyning, forbedre spenning- og frekvens kvalitet, og anvende overskuddskraft (Olsen 2020, s.9).

2.3 Aktører og lovverk

Aktører

Den norske energisektoren er preget av et mangfold aktører og offentlig eierskap. De overordnede politiske rammer for energiforvaltning blir satt av Stortinget. Regjeringen har utøvende myndighet som håndheves gjennom ulike departementer.

Ansvaret for vann- og energiforvaltning ligger på Olje- og energidepartementet, som igjen har eieransvar for statsforetakene Enova og Statnett. Enova sin funksjon er å forvalte ressursene i Energifondet, samt fremme miljømessig strukturering av bruk, produksjon og teknologiutvikling innen energi. Statnetts ansvar omfatter bygg og drift av det sentrale strømnettet. Foretaket sitter med majoriteten av eierskapet av sentralnettet og har systemansvaret over tid. Det er derfor deres oppgave å regulere for tilfredsstillende kraftbalanse og leveringskvalitet på nasjonal basis (Energifakta 2017).

Videre ligger ansvaret for forvaltning av innenlandske energiressurser hos Norges vassdrags- og energidirektorat (NVE), de har i tillegg funksjon som nasjonal reguleringsmyndighet for elektrisitetssektoren. NVE er også underlagt Olje- og energidepartementet (Ibid).

NVE har også ansvar for samordning og koordinering av beredskap i møte med ekstraordinære situasjoner. For disse formål ble det opprettet en landsdekkende organisering kalt *Kraftforsyningens beredskapsorganisasjon* (KBO) som omfatter NVE, samt alle eiere og drivere av kraftproduksjon. Detaljerte beredskapsplaner har blitt konstruert for å sikre tilstrekkelig sikkerhet og strømrasjonering under uforutsigbare situasjoner. Videre har NVE i samarbeid med NorCERT (Nasjonalt Cybersikkerhetssenter) dannet er responsteam for sektoren, KraftCERT, med den funksjon å bistå energisektoren både proaktivt og responsivt i møte med IKT- trusler og uønskede hendelser (Vada u.å).

Norges forskningsråd sitter også med en sentral rolle, særlig med tanke på Smart Grid teknologi. Da de har ansvaret for regi av bevilgninger til energiforskning.
Olje- og energidepartementet finansierer forskning og innovasjon i energisektoren gjennom forskningsrådet (Energifakta 2017). Med økende fokus på småkraft av særlig miljømessige formål blir teknologisk muliggjørelse av fleksibilitet i kraftnettet et fokus for forskning. The Norwegian Smartgrid Centre (NSC) mottar bevilgninger for prosjekter gjennom sine medlemmer (the norwegian smartgrid centre, u.å.a).

NSC fungerer som et nasjonalt kompetansesenter for teknologisk og digital innovasjon i energisektoren. Senteret har per juni 2020, 47 medlemmer som omfatter alt fra små kraftselskap, forskningsinstitusjoner, universiteter, teknologi utviklere, og statsforetak som Statnett og store selskap som statkraft (the norwegian smartgrid centre, u.å.c).
Senterets virksomhet omfatter stimulering til forskning, undervisning, kommersialisering og demo-prosjekter (Smartgrids 2016, s.38).
Deres visjon er, gjennom industri og forskning allianser, å implementere ny teknologi for økt fleksibilitet og intelligens i det elektriske energisystemet.

En akselerering av innovative digitale og teknologiske midler i kraftnettet skal redusere behovet for videre investering i infrastruktur, øke forsyningssikkerhet, samt fremme klimavennlig strukturering av systemet (the norwegian smartgrid centre, u.å.b).

Lovverk

Kraftforsyning er en kritisk samfunnsfunksjon. Det skal sikres at sluttbrukere har tilstrekkelig tilgang til elektrisk energi og fjernvarme der det er utbygd. Dette er kritisk både for nasjonens styringsevne og suverenitet, samt befolkningens sikkerhet. Og er derfor en essensiell del av samfunnets grunnleggende behov (DSB 2016, s.17). Grunnet denne kritikaliteten finns det et omfattende juridisk rammeverk for å sikre vedlikeholdt funksjonalitet.

Lovverket skal ivareta samfunnsmessig rasjonell energiforvaltning, effektiv produksjon, distribusjon og bruk av energi, samt sikre viktige hensyn til forsyningssikkerhet, verdiskapning og miljø (Energifakta 2019a).

Politiske konflikter oppstår i forskjellige produksjon- og klima interesser. Det må ofte foretas en rekke avveininger mellom produksjon og miljø. Samfunnet er avhengig av korrekt kraftbalanse, noe som kan kreve ytterligere infrastruktur og naturinngrep. Allmenne interesser som blant annet biologisk mangfold, lokalsamfunn, friluft og landskap kan bli sårbare for slik utbygging (Energifakta 2019a; Vasstrøm et al. 2018). Lovverket skal sørge for at ulike interessenter blir hørt, at tiltak blir satt under offentlig regi, samt ha et velfungerende kraftmarked i fokus.

Elsertifikatloven ble skapt med det formål å øke produksjon av energi fra fornybare energikilder (Energifakta 2019a). Smart Grid teknologi er ikke bare nyttig, men er forutsetning for bærekraftig energiproduksjon i henhold til loven. Et mer fleksibelt, intelligent strømsystem kan ta i bruk eksisterende infrastruktur på en fordelaktig måte slik at videre naturinngrep kan minimaliseres (Smart Innovation Norway 2016).

Videre er det en rekke lover energisektoren må ta hensyn til under planlegging, konstruksjon, og operasjon av produksjon- eller distribusjonsanlegg for elektrisitet og fjernvarme (Energifakta 2019a).

- Plan- og bygningsloven
- Naturmangfoldloven
- Konkurranseloven
- Forvaltningsloven
- Friluftsloven
- Forbrukerkjøpsloven
- Forurensningsloven
- Vannfallrettighetsloven
- Vassdragsreguleringsloven
- Vannressursloven
- Havenergilova

I henhold til dette prosjektet kan spesielt tre lover trekkes frem som mer sentrale for Smart Grid aktører. Energiloven, Kraftberedskapsloven og GDPR.

Energiloven omfatter at energi på alle nivå; produksjon, omdannelse, overføring, distribusjon og anvendelse, gjøres på en samfunnsmessig rasjonell måte. Både allmenne og private verdier skal tas i betraktning. Selve utbyggingen og driften av nettet en monopolvirksomhet, men loven åpner for liberal konkurranse innen produksjon og handel. Energiloven omfatter også reguleringer angående fjernvarme, elektrisk energi, systemansvar, leveringskvalitet, overføringsforbindelser og beredskap (Energifakta 2019a).

Kraftberedskapsforskriften ble opprettet med den hensikt å stille sikkerhetskrav for opprettholdelse av normal forsyning på effektiv måte i, og etter, ekstraordinære situasjoner (NVE 2018, s.3). Forskriften ble revidert og trådte i kraft med nye tiltak for IKT-sikkerhet den 1. januar 2019 (NVE 2019). Revideringen var grunnet den økende digitaliseringen av kraftsektoren og samfunnet forøvrig, noe som har resultert i et endret risiko- og sårbarhetsbildet i energisystemer (NVE 2018, s.3).

Med fusjonen av kraft og IKT blir energimarkedets forsyningssikkerhet avhengig av kontinuerlig operative digitale systemer. Digitalisering resulterer i større nettverk av komponenter, enheter og systemer. For å ivareta tilstrekkelige sikkerhetsmekanismer i en større digital verden, med flere digitale trusler, har kraftbransjen stadig fokusert mer på IKT-sikkerhet over årene (NVE 2019). Den reviderte forskriften er en presisering av sikring og beredskapsplikten i energiloven, og inneholder en blanding av funksjons- og detaljkrav som legger til rette for en helhetlig tilnærming. Og tydeliggjør plikt for grunnsikring for alle informasjonssystemer hos virksomheter med anlegg der svikt kan få betydelige konsekvenser for produksjon, distribusjon eller anvendelse av elektrisk energi og fjernvarme. Den inneholder videre nye plikter for hendelsesrapportering innen sektoren (Ibid).

Med økende digital sårbarhet er Personvernforordningen (GDPR) noe sektoren må forholde seg til. Forordningen fra EU trådte i kraft i energisektoren i mai 2018, den har som formål å sikre de enkelte kunders rettigheter med tanke på innsynsrett, manipulering, redigering og sletting av data, samt en rett til å overføre data fra en leverandør til en annen (Møller & Funes

2017). Persondata er en hvilken som helst opplysning som kan benyttes for å identifisere enkeltpersoner. Slike digitale verdier, i et sårbart nettverk, kan derfor benyttes for uetiske gjerninger. Den nye forordningen skal derfor sikre at behandlingen av slik data skjer på en lovlig, rettferdig og gjennomsiktig måte (Regjeringen 2019b).

Hele fornybarnæringen, med for eksempel de nye smarte strømmålere, må rette seg etter lovgivningen, og Energi Norge har av den grunn fått etablert en veileder for sektorens tilpasning (Møller & Furnes 2017).

3. Teoretisk rammeverk

I dette kapittelet vil sentrale begreper defineres og det teoretiske rammeverket bli avklart. Dette inkluderer uttrykk som risiko, sikkerhet, verdi, trussel, sårbarhet, samt cyber-begrepet. Det teoretiske grunnlaget består av "Social amplification of risk", eller SARF-rammeverket, risikokommunikasjon, samt Charles Perrow sine beskrivelser av komplekse og tett koplede system.

Formålet med valgt teori er å vise til det digitale samfunnets sammensveisede verdier og resulterende økende sårbarheter. Og hvordan slike omfattende risikoprofiler bør kommuniseres for å redusere sosiale konsekvenser av eventuelle ondsinnede handlinger i energisektoren.

3.1 Begrepsavklaring

3.1.1 Risiko

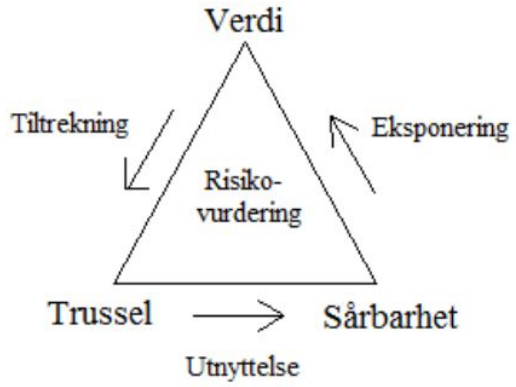
Risikobegrepet kan ha forskjellige konnotasjoner avhengig av fagfelt. Det er derimot hensiktsmessig for denne teksten å inkludere tre elementer. Risiko involverer utfall som har en påvirkning på noe mennesker verdsetter, sannsynlighet av at utfallet forekommer, og en formel for å kombinere disse (Renn 2008, s.2). Usikkerhets aspektet av risiko blir også av betydning, da dette prosjektet i stor grad tar for seg målrettede angrep mot et system. En slik risiko er nærmest umulig å kvantifisere da den avhenger av blant annet aktørenes intensjoner, ressurser og kompetanse (Engen et al. 2016, s.87). Avens formulering adopteres derfor, der risiko forståes *som kombinasjonen av usikkerhet og konsekvens av en gitt aktivitet* (Aven et al. 2016, s.37).

Videre kan risiko vurderes ut i fra flere karakteristikker slik som omfang, utstrekning, varighet, reversibilitet, avstand mellom hendelse og synlige effekter, ødeleggelse av egenkapital og mobilisering potensiale. Slike distinksjoner gjør det mulig å klassifisere risiko

etter grad av kompleksitet, tvetydighet og tilknyttet usikkerhet, som blir en avgjørende faktor for hvilken metodikk som best egner seg for håndtering (Engen et al. 2016, s.83).
Det er også viktig å poengtere at risiko er multidimensjonalt, noe som utdypes i teori kapittelet. En risiko identifiseres i spesifikke sosio kulturelle, politiske og historiske kontekster (Lupton 2013. s,21).

3.1.2 Verdi, trussel og sårbarhet

Som beskrevet ovenfor omhandler en risiko en verdi, en trussel eller fare, og en sårbarhet. Sammenhengen mellom disse illustreres i "risikotrekanten"



Figur 4: "Risikotrekanten" Hentet fra Eskeland Kruke (2017) s.11

En *Verdi* i en sikkerhets kontekst betegner noe man vil beskytte. Dette relateres ofte til liv og helse, miljø, materielle og økonomiske verdier (Engen et al. 2016, s.43). I et teknologisk system vil for eksempel sikker drift og pålitelighet være primær-verdier der fysiske komponenter som muliggjør dette kan betraktes som støttende, sekundær-verdier. Videre kan verdier innebære mer abstrakte ting som egenskaper og kunnskap. En verdi er altså noe man drar en viss nytte av og derfor har identifisert som beskyttelsesverdig. Verdi-identifisering vil derfor bestå av mange subjektive betraktninger og kan variere fra system til system, og kultur til kultur.

Videre er en *Sårbarhet* et systems manglende evne til å virke under og etter uønsket påvirkning. En sårbarhet kan ofte mitigeres gjennom proaktivt arbeid for å skape robuste systemer (Ibid, s.47).

En *trussel* forståes som en passiv eller aktiv handling eller situasjon som utnytter en sårbarhet og eksponerer verdier for skade. Noe med potensialet til å utløse en uønsket hendelse (NOU 2000:24, s.18).

3.1.3 Sikkerhet og *sikkerhet*

Sikkerhetsbegrepet kan simpelt forståes som et fravær fra ulykker, men dette beviser ikke tilstrekkelig sikkerhetstilstand. Det kan også forstås som en trygghet mot farer som kan true noe av verdi, for eksempel liv og helse (Kongsvik et al. 2018, s.20). Videre kan man si sikkerhet handler om tapsforebygging som formulert av Aven, der sikkerhet er et systems evne til å unngå skader eller tap (Ibid, s.21).

Det er viktig å poengtere at sikkerhet, som risiko, er multidimensjonalt. Sikkerhet er en *tilstand,* et fravær av negativ risiko. En *følelse,* at man opplever avstand eller kontroll over en farekilde. Og sikkerhet er en *praksis,* et arbeid for å sikre en kontrollerbar tilstand og en trygghetsfølelse. I denne teksten vil derfor sikkerhet forstås som *en dynamisk ikke-hendelse* som beskrevet av Weick (Besnard & Hollnagel 2012, s.14). Dette viser til et pragmatisk sikkerhetsperspektiv, der sikkerhetsarbeid blir en kontinuerlig, sirkulær prosess for å forebygge uønskede hendelser. Slikt arbeid kan hovedsakelig tilnærmes på to proaktive måter. Ved å hindre at uønskede hendelser oppstår i utgangspunktet, eller ved å etablere barrierer som reduserer verdiens sårbarhet dersom en uønsket hendelse likevel skulle oppstå (Kongsvik et al. 2018, s.22). Barrierer kan forstås som et sett av menneskelige, teknologiske og/eller organisatoriske elementer med den funksjon å forebygge eller stanse et hendelsesforløp. Barriere elementer kan være fysiske, immaterielle, funksjonelle eller symbolske av natur (Kongsvik et al. 2018, s.76; Rosness et al. 2010, s.36).

Forståelse og arbeid med sikkerhet er tofoldig. Engelsk terminologi differensierer mellom *Safety* og *Security*. Der førstnevnte omhandler hendelser som ikke er planlagt eller uønsket, som vanligvis omtales som "uhell". Operatør feil og teknisk svikt faller innenfor denne kategorien. *Security* retter fokus mot bevisste ondsinnede handlinger, slik som for eksempel sabotasje, økonomisk motivert kriminalitet eller terrorisme (Kongsvik et al. 2018, s.26). Det

gjelder altså intenderte handlinger som rammer oss fordi noen har en intensjon om å iverksette dem.

Dette prosjektet vil i hovedsak ta for seg *Security* begrepet, da scenarioet er målrettede tilsiktede handlinger i kraftsektorens digitale domene, og hvilke utfall dette kan føre til.

3.1.4 Cybersikkerhet

Data-, informasjon- og cybersikkerhet blir ofte brukt om hverandre, men skiller seg på enkelte områder. Datasikkerhet omhandler verktøy og tjenester med den funksjon å sikre all digital informasjon, både fra tilsiktede gjerninger og systemsvikt. Informasjonssikkerhet overlapper i stor grad med datasikkerhet, men kan også omfatte analog informasjon. Begrepet omfatter derfor flere aspekter enn datasikkerhet da det også innebærer fysisk sikring, lovverk, beredskapsplaner og lignende.

Cybersikkerhet tar i større grad for seg sikring av enheter og strukturer som baseres på IT, men som ikke nødvendigvis omhandler informasjon på datasystemer. For eksempel virksomheter som benytter IT for produksjon og drift opplever trusler fra internett (Natt 2019). Kraftproduksjon og distribusjon er avhengig av IT systemer og dette prosjektet vil derfor benytte seg av begrepet Cybersikkerhet.

3.2 Kompleksitet og tette koblinger (NAT)

"*Normal Accident Theory"* ble presentert av Perrow i 1984. Det deterministiske perspektivet påpeker hvordan ulykker er uunngåelige i komplekse og tett koblede systemer (Rijpma 1997, s.15). Modernisering byr på effektivisering, men også kompleksitet. Samfunnet blir i større sammenhengende noe som kan føre til at en tilsynelatende kontrollerbar feil kan ha en uforutsett kaskadeeffekt. Mange systemiske risikoer, slik som innenfor informasjon- og kommunikasjonsteknologi, krever synergi mellom flere system og et holistisk perspektiv for

å skape pålitelig, og sikker drift (Renn 2008, s.5). Systemer som underbygger kritiske samfunnsfunksjoner, men er sårbare viser til potensielt farlig teknologi.

Risiko for katastrofe blir mer betydelig, ikke bare for virksomheten og aktørene som drifter systemet, men også for tredjeparts offer og eventuelt fremtidige generasjoner. Den digitale verden fletter flere tidligere isolerte systemer inn i store, ofte globale system. Økt kompleksitet skaper større verdikjeder som igjen byr på kunnskapsutfordringer, sårbarheter kan utnyttes på måter som ikke var mulig tidligere, trusselbildet blir utfordrende å kartlegge. Spørsmålet blir derfor om det er mulig å drifte slik *farlig* teknologi sikkerhetsmessig ansvarlig, eller om et vellykket angrep med resulterende samfunnskrise er kun et spørsmål om tid?

I følge *normale ulykker*-perspektivet kan slike teknologier identifiseres på to strukturelle egenskaper, systemets interaksjoner og koblinger (Engen et al. 2016, s.146). Dette medfører også et styringsdilemma.

Interaktiv kompleksitet betegner systemer der system-deler og komponenter er koblet på ikke-lineære måter, og gjensidig avhengighet mellom enheter kan resultere i at svikt og feil får uforutsette hendelseskjeder (Kongsvik et al. 2018, s.78). Det kan beskrives som det motsatte av typ samlebåndsproduksjon der det vil være direkte linjer mellom komponent "A" og komponent "B" osv. Komponenter krever ikke direkte samspill i produksjonsprosessen, da dette følger en lineær, preskriptiv prosedyre.

Komplekse interaksjoner inngår i større produksjonsprosesser, i systemer som krever at flere kritiske handlinger foregår parallelt. Dette gjør verdikjeden uoversiktlig da komponent "A" kan være avhengig av komponent "E" som igjen er avhengig av andre komponenter. Komponentsvikt i systemet kan derfor, som nevnt, føre til uforutsigbar eskalering. Selve produksjonsprosessen, samt vedlikehold, oppgraderinger, håndtering og drift blir vanskeliggjort av dette faktum (Engen et al. 2016, s.144).

Systemets grad av koblinger viser til tidsavhengige prosesser og sekvenser. Tett koblede systemer er preget av lite *slakk,* som tilsier at antall og prosesser må være mer nøyaktig, og

ressurser kan ikke enkelt erstattes. Tiltak for systemets robusthet og redundans må derfor implementeres i systemets design-fase (Ibid, s.145).

Komplekse systemer er altså preget av blant annet nærhet, flere komplekse sammenhenger og interaksjoner, en vanskelighet i å erstatte deler, tilbakeføringssløyfer, indirekte informasjon og derfor, begrenset forståelse.

Det er videre viktig å bemerke at et systems karakteristikker også er avhengig av kontekst. Grad av interaksjon og koblinger vil variere ut i fra miljøet, eller ut i fra de omgivelser, sosiale og politiske, de sosiotekniske systemene befinner seg i (Ibid, s.146).

Dette fører til et styringsdilemma, da perrow hevder at systemer preget av høy kompleksitet kan kun effektivt styres gjennom en desentralisert organisasjonskultur, mens et tett koblet system krever sentralisert styring. Teknologier preget av begge karakteristikker vil derfor ikke kunne håndteres på ansvarlig vis. På dette grunnlaget påpeker Perrow at storskala ulykker innenfor slike system er uunngåelige (Rosness et al. 2010, s.49).

I henhold til problematikken tatt opp i dette prosjektet vil Perrows beskrivelser kaste lys på den økende grad av kompleksitet og tette koblinger ikke bare på systemskala, men på en overordnet samfunnskala. Samfunnets grad av teknologi øker, noe som tilsynelatende vil fortsette i lang tid fremover. Det moderne samfunn er et sammenvevd, integrert nettverk av mennesker, teknologer, organisasjoner og sektorer som gir et komplekst trusselbilde. Svikt i elektrisitetsforsyning kan raskt bli kritisk for mange mennesker.

Dersom et vellykket tilsiktet angrep i denne sektoren fører til strømbortfall vil høyst sannsynlig tidligere kommunikasjon, og derfor befolkningens risikoforståelse ha enorm innvirkning på hvordan en slik hendelse blir håndtert i krisefasen, samt hvilke bølge-effekter som oppstår i ettertid. Samfunnets systemiske sårbarheter, verdier og trusler må kartlegges og møtes med organisatorisk og teknisk kompetanse for å sikre samfunnets levetid i den digitale alder.

3.3 Risikokommunikasjon (IRGC)

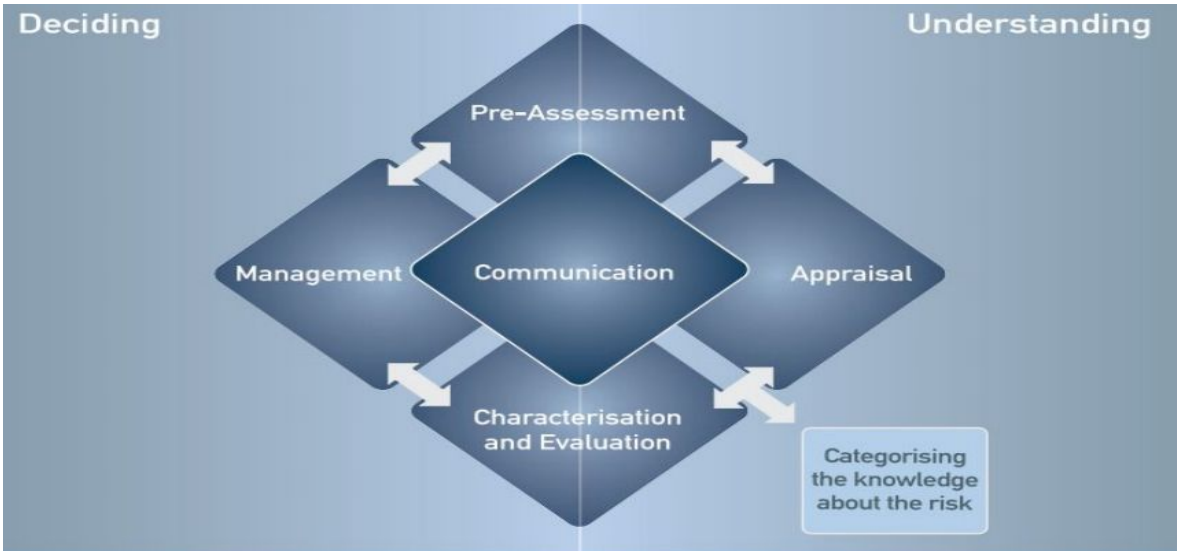
"*The International Risk Governance Council*", forkortet IRGC, har utviklet et omfattende rammeverk for risikostyring. Deres mål er å legge til rette for bedre risikoforståelse og deres vitenskapelige, sosiale og økonomiske kontekst (IRGC 2005, s.2). Rammeverket gir også veiledning til hvordan ulike risikoer bør kommuniseres og håndteres. "*Risk Governance*" eller risikostyring tar for seg identifikasjon, evaluering, ledelse og beslutnngstaking, og kommunikasjon av risiko. Det er metoden samfunn benytter for å nå kollektive besluttninger angående teknologoer og aktiviteter som kan ha ukjente konsekvenser (Renn 2008, s.8).

Dette inkluderer totaliteten av relevante prosesser, regler, aktører og konvensjoner, samt hvordan relevant informasjon samles, analyseres og videreformidles. Prinsipper for god styring er transparens, effektivitet, pålitelighet, bærekraft, rettferdighet, lovlydighet, og politisk og sosial muliggjørelse (IRGC 2005, s.4). På denne måten vil IRGCs rammeverk unngå den rent realistiske, eller objektive risikoforståelsen, å inkludere de sosiale dimensjoner av risiko (Renn 2008, s.3).

IRGCs prosess består av 4 faser; før-vurdering, risikovurdering, karakterisering og evaluering, og håndtering, med risikokommunikasjon som en sentral del i hver fase (Ibid, s.47).

I *Før-vurderings fasen* blir de forskjellige perspektiver angående en gitt risiko klargjort og problemet blir definert, med andre ord skapes konteksten for videre arbeid (Ibid, s.48). Under *Risikovurderingen* utvikles kunnskapsbasen for håndtering og beslutning av risiko, hvordan kan eventuelle negative utfall mitigeres.
Karakterisering og evaluering vil sørge for at vitenskapelig data blir sammenføyd med en forståelse av sosiale verdier for å gjøre de best mulige beslutninger. En diskurs vil karakterisere risiko som enten akseptabel, tolererbar, eller ikke-tolererbar (Ibid, s.149).
Risikohåndtering betegner den prosessen og implementasjonen av midler for å møte de satte risikoakseptkriteriene (Aven 2006, s.16).

Denne prosessen skal reflektere god risikostyring, der formålet er å sikre optimal balanse mellom verdiskaping og unngåelse av ulykker, skader og tap. Dette er beslutninger angående situasjoner med høy risiko og stor usikkerhet (Ibid, s.15).



Figur 5: "Risk Governance Framework" Hentet fra IRGC (2005) s.8

Figur 5 viser til en kontinuerlig, sirkulær prosess der kommunikasjon er sentralt. Effektiv kommunikasjon må vedlikeholdes for suksess i enhver aktivitet under risiko vurdering- og håndterings prosessen (Renn 2008, s.201).

Risikokommunikasjon har utviklet seg fra å være en enveis prosess, en kanal fra eksperter og myndigheter til befolkningen, til en toveis-prosess. Formålet med denne modellen er at de ansvarlige risiko aktørene deltar i diskursen, og derfor læringsprosessen, noe som sørger for å bygge tillit dersom befolkningen føler seg hørt og føler en risiko blir fornuftig adressert og håndtert. Videre er målet med kommunikasjonsprosessen å assistere interessenter i å forstå risiko vurdering og håndterings prosessen, for å komme til de best mulige avgjørelsene. Effektiv praksis for risikokommunikasjon hjelper aktører å ta informerte, rasjonelle beslutninger, som igjen vil bygge tillit fra befolkningen (Ibid, s.202).

Risikokommunikasjon har interne og eksterne aspekter. Sentrale aktører til risiko identifikasjon, vurdering eller håndtering må vite hva risikoen betyr, hvilken rolle de har i

verdikjeden, og deres ansvar. Og ekstern kommunikasjon må sørge for å være informerende og engasjerende (Ibid, s.202).

Effektiv kommunikasjon, eller mangelen på dette, har betydelig påvirkning risikopersepsjoner, og derfor hvordan mennesker møter en gitt risiko. Begrepet risikopersepsjon kan forstås som den subjektive oppfatningen av risiko (Ibid, s.93). Over-dramatisering av en risiko kan føre til unødvendig sosial uro, mens demping av risiko kan føre til at ansvarlige myndigheter mister tillit dersom en ulykke inntreffer. Informasjonen som kommuniseres bør skape og vedlikeholde tillit til aktører, samt reflektere virkeligheten. Risikokommunikasjons funksjon vil være utdanning og opplysning, risikotrening og atferdstilpasning, konfidens og autoritetstro, samt oppfordrelse til deltakelse i risiko-relatert diskurs og håndtering (Ibid, s.203).

For at disse funksjoner av kommunikasjon skal fungere etter hensikt er det viktig å skape en helhetlig risikoforståelse. Aspekter av risiko slik som hvor, hvilken aktivitet, type fenomen, farlige forhold og type omfang (Kongsvik et al. 2018, s.35), bør kommuniseres slik at det reflekterer virkeligheten. Derimot er ikke alltid denne informasjonen tilgjengelig og byr derfor på kunnskapsutfordringer som vanskeliggjør prosessen.
Videre vil spørsmål om risikoen er frivillig eller påtvunget, om effektene er umiddelbare eller langsiktige, omforent kunnskap om risiko eller grad av omstridelse, opplevelse av egenkontroll, kjennskap til potensielle konsekvenser, og måten den kan påvirke individet, altså måten skaden inntreffer, har betydning for befolkningens risikopersepsjon (Ibid, s.34). Jo mer man vet, jo flere tiltak kan man iverksette for å forebygge, eller mitigere skadeomfang. Datainnsamling, dens tolkning og videreformidling blir derfor essensielt både i risikoens fysiske og sosiale dimensjon.

Særlig tre aspekter ved en risiko vanskeliggjør kommunikasjon; kompleksitet, usikkerhet og tvetydighet.
En risikos kompleksitet betegner graden av problematikk i å forutse hvordan deler av et system kan påvirke hverandre. Usikkerhet handler om manglende kunnskap, både om sannsynlighet og konsekvens (IRGC 2005 s.16). Dersom risikoen er preget av både kompleksitet og usikkerhet kan dette føre til tvetydighet. Tvetydighet kan igjen deles i

fortolkende og normativ, der førstnevnte betegner uenighet ved resultatets betydning, mens sistnevnte viser til hvorvidt det eksisterer enighet om risikoen er akseptabel eller ikke (Renn 2008, s.179).

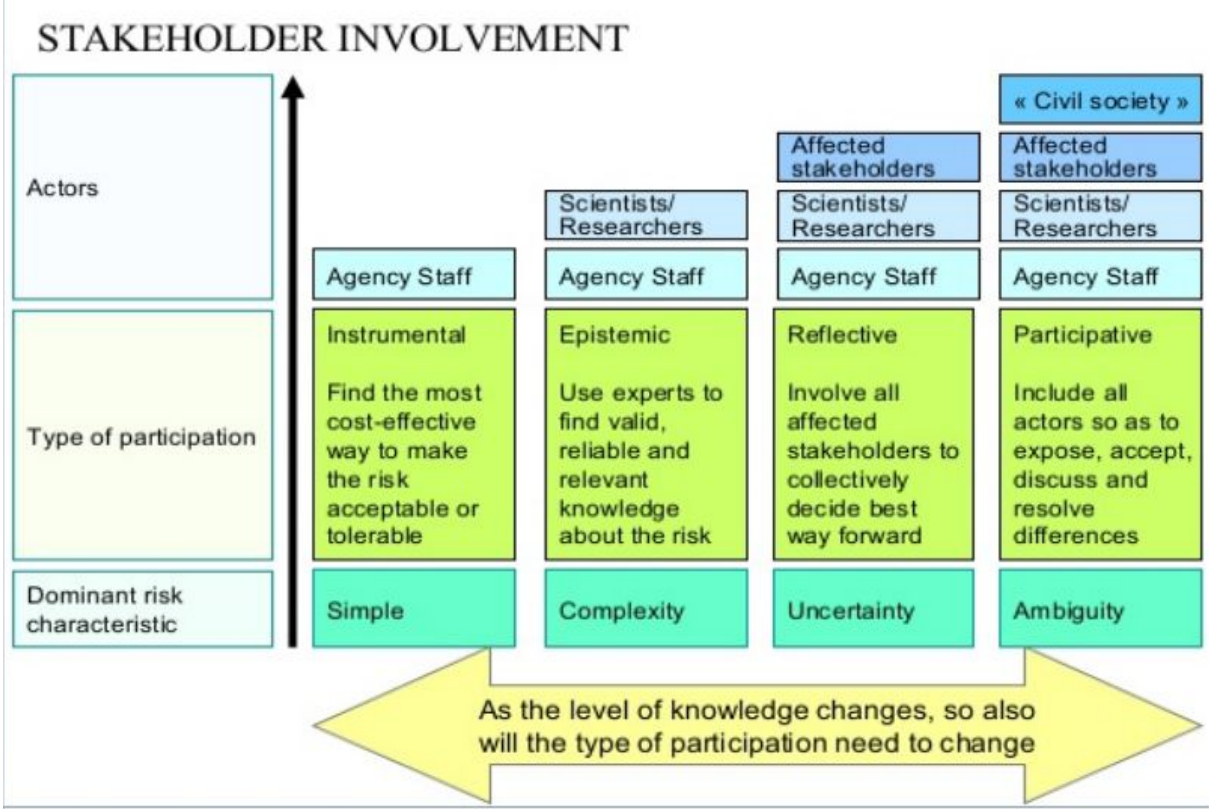
Disse karakteristikkene av risiko bør videre være av betydning for hvordan risikostyringsprosessen vil foregå (Ibid, s.177). En enkel, eller lineær risiko, der det er direkte link mellom risiko og tiltak, vil kunne håndteres gjennom rutinebaserte tiltak. En "instrumentell" form for diskurs vil også være tilstrekkelig, kun direkte involverte aktører trengs for å komme til det ønskede sikkerhetsnivå (Ibid, s.191).

Risiko preget av kompleksitet bør tilnærmes med datainnsamling og ekspert analyser for å fremme en så risiko-informert beslutning som mulig. Målet vil være å skape et robust system i stand til å takle et mangfold med eventuelle påkjenninger. "Epistemisk" diskurs er her anbefalt, noe som betegner en omfattende ekspert-samtale, der formålet vil være å komme til de mest realistiske deskripsjoner eller forklaringer på en eventuell ulykkes-kjede (Ibid, s.192).
For risikoer preget av større grad av usikkerhet bør føre var prinsippet vektlegges.

Risikostyringen bør fokusere på å bygge resiliens, altså systemets evne til å overvåke, forutse, respondere på fleksible måter, og å dra lærdom fra diverse påkjenninger (Kongsvik et al. 2018, s.90). Diskursen rundt risikoen bør være "refleksiv", som omhandler potensielt risikofylte avveininger. Man vil ta for seg spørsmål om hvor mye usikkerhet man er villig til å akseptere for fremtidig innovasjon og vinning. Denne diskursen bør involvere berørte interessenter, eksterne eksperter, samt ansatte (Renn 2008, s.196; Engen et al. 2016, s.129).

Til slutt vil risiko preget av flertydighet løses gjennom en diskurs basert strategi der interessenter i større grad involveres og ekstern sosial kommunikasjon benyttes (Renn 2008, s.182). Formålet blir å nå beslutninger som er akseptabel for de fleste involverte. Man vil fragmentere problemet til mindre deler for å nå konsensus gjennom en "deltakende" diskurs som fokuserer på å nå et mer ensidig narrativ angående risiko. Tvetydighet og verdikonflikter løses gjennom diskurs på større arena som vil involvere alle relevante aktører (Ibid, s.199).

Figur 6 nedenfor illustrerer sammenhengen mellom ulike risiko-aspekter og aktør involvering.



Figur 6: "The risk management and stakeholder involvement" Hentet fra Bruvold 2017, s.27

Uansett risiko-kategorisering vil inklusiv risikostyring handle om deliberasjon (Renn 2008, s.200). Når det kommer til samfunnsrisiko bør et mangfold av aktører være engasjert for å utforske og diskutere så mange sider som mulig. Det bør være en demokratisk prosess, da dette er avgjørende i skapelse av menneskers risikopersepsjoner, og tillitsbygging.

Viktigheten av dette for beslutningstakere er også mangfoldig, Renn (2018) legger vekt på særlig to aspekter. For det første demonstrerer studier innen risikopersepsjon hva som er viktig for mennesker, deres bekymringer, noe som bør tas i betraktning i en politisk agenda. Det viser ikke kun til individuelle subjektive betraktninger, men større kulturelle holdninger som driver handling i møte med potensiell fare. Inkludering av risikos sosiale dimensjoner og kulturelle bekymringer vil derfor være essensielt for å skape ønsket risikotilpassende atferd. Et annet poeng er at politisk styring og regulering av risiko innebærer avveininger. Slike avveininger avhenger av en risikos kontekst og dimensjon. En multidimensjonal

risikoforståelse vil forhindre en forhastet, potensielt skadelig beslutning (Streicher et al. 2018, s.365). En holistisk situasjonsforståelse vil med andre ord forsikre at man tilnærmer seg risiko på en adekvat måte, med "tilstrekkelig forestillingsevne" som beskrevet av Westrum (Kongsvik et al. 2018, s.82). Risikopersepsjoner er kritisk for å formulere og evaluere effektive program for risikokommunikasjon.

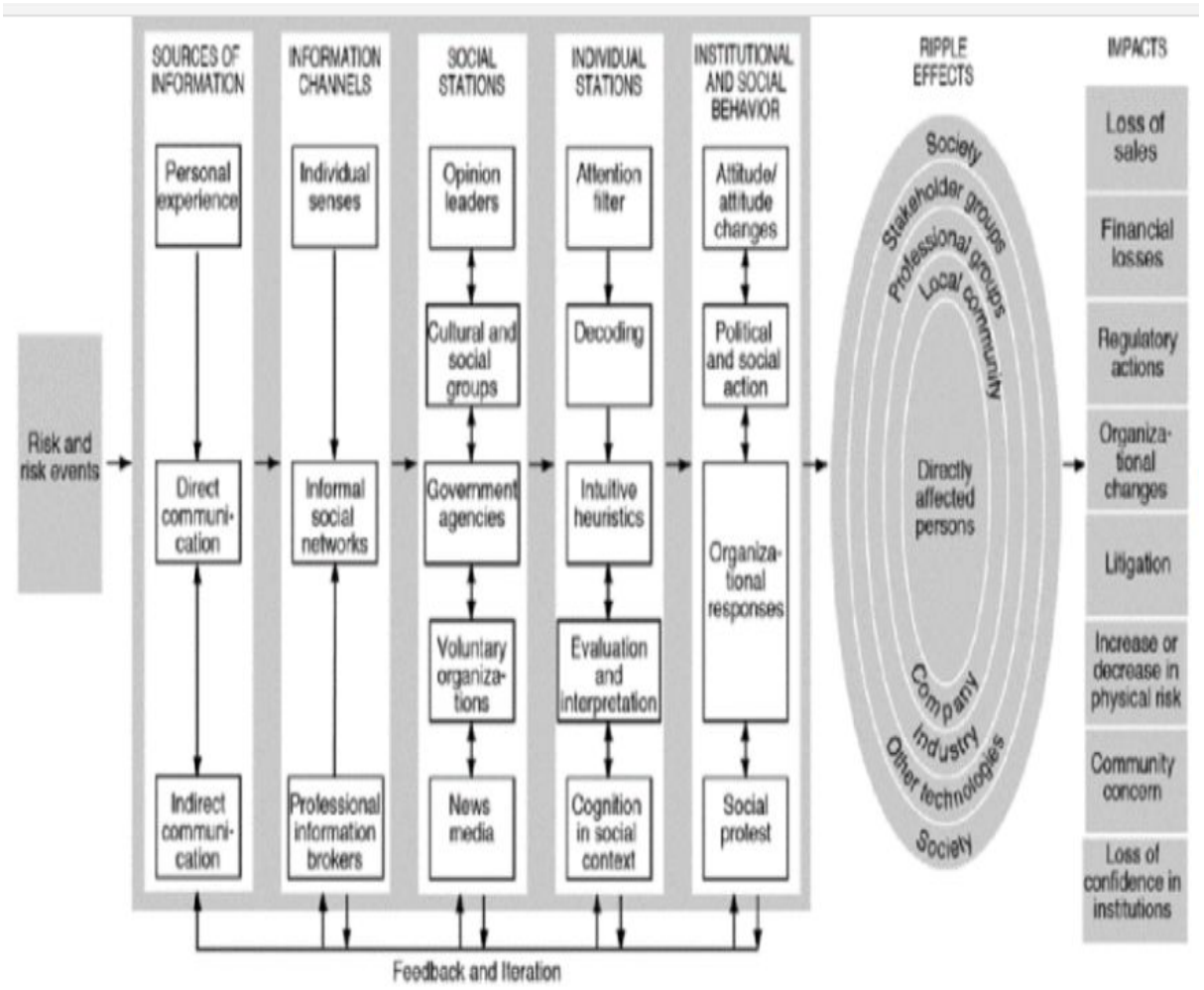
Til slutt må det påpekes at kommunikasjonsprosessen angående risiko i Smart Grid systemer ikke nødvendigvis skal oppfordre til stor atferdsendring blant allmennheten. Det er begrenset med tiltak den generelle befolkningen kan foreta seg, og hovedansvaret ligger på myndigheter og media. Poenget er, sett gjennom et sosiokulturelt læringsperspektiv, at kommunikasjonen skal bevisstgjøre. Ved å adressere risikoprofilen i et reelt lys skapes muligheter for samfunnsmessig utvikling i form av *indre tale,* eller bevisstgjøring. Som legger grunnlaget for introspeksjon, refleksjon og oppmerksomhet. Læring og bevisstgjøring skapes i interaksjonen mellom mennesker, og handler om individene samt kommunikasjonsprosessens kontekst (Myklebust 2017). Og denne kollektive risiko-forståelsen kan igjen føre til *Public Resilience,* som betegner hvordan å i større grad involvere allmennheten i risikobildet gjør samfunnet i stand til å møte et bredt utvalg av uforutsette hendelser på en mer fleksibel måte (Urheim 2015, s.18). Relatert til psykologien kan det sammenlignes med "*Emotional Cushioning",* der individer forbereder seg mentalt på skuffelse slik at man er i en bedre posisjon til å håndtere hendelsen, eller opplever lykke dersom man uslipper den (DiTullio 2019, s.20; Neimark 2007). Her har medier medier en sentral rolle. Selv om mennesker er reflekterende og dynamiske mottakere av informasjon som vist av Petts et al. (2001), har en rekke studier vist en direkte korelasjon mellom nyhetsmedier og risikopersepsjoner (Frh 2017; Park & Sohn 2013; Kone & Mullet 1994: Gore et al. 2005; Jung & Ha 2016). Park og Sohn (2013) viste til hvordan mediedekning om risiko knyttet til kugalskap hadde direkte innflytelse på kunnskap, holdninger og derav risikopersepsjoner. Videre viste deres forskning at når nyhetsmedier dekker informasjonsbehov, reduseres frykten til risikokilden. For best effekt av risikokommunikasjon bør derfor informasjonen være objektiv og informerende, samt spille på åpenhet mellom myndigheter, eksperter, relevante industrier og allmennheten (Park & Sohn 2013).

3.4 Sosial forsterkning av risiko (SARF)

"Social amplification of risk" beskriver hvordan risiko filtreres gjennom individuelle og kulturelle prosesser. Som et rammeverk vil det beskrive fenomenet der informasjonsprosesser, institusjonelle strukturer, gruppe-atferd og individuelle responser former den sosiale opplevelsen av risiko, og derfor påvirker konsekvenser av gitt risiko. Med andre ord utforskes de dimensjoner av risiko utover de rent fysiske.

En fare, eller negativ risiko, samhandler med psykologiske, sosiale, institusjonelle og kulturelle prosesser på måter som resulterer i en forsterkning, eller demping, av offentlig respons relatert til risikoen (Kasperson et al. 1988, s.177).

Sosial forståelse, og derfor påvirkning, av risiko har røtter i den sosiale dimensjonen. Dette inkluderer både direkte, eller personlig kontakt, og indirekte kontakt med risikoen. Dersom man ikke opplever personlig kontakt, lærer man om risikoen gjennom informasjonskanaler, slik som media eller organisasjoner. Slike institusjoner kan forsterke forståelse av risiko til den grad at persepsjoner skapes i fravær fra den faktiske risikoen. På denne måten kan sterke offentlige bekymringer og sosioøkonomiske endringer følge en risiko med tilsynelatende lave fysiske konsekvenser (Chong 2018, s.2).



Figur 7: "The social amplification of risk framework" Hentet fra Kasperson et al. 1988, s.183

"*The social amplification of risk framework*", eller *SARF* for kort, starter med en risiko-relatert hendelse eller aktivitet, slik som for eksempel en uønsket hendelse (Figur 7). Slike risiko-hendelser kan ha varierende *signal verdi* (Gould & Fjæran 2019, s.4), som forsterker eller demper videre sosiale konsekvenser av risikoen. Risiko-signalene kan skapes både gjennom direkte eller indirekte kontakt. Disse signalene blir filtrert gjennom sosiale og individuelle "*amplification stations"*, eller risikopåvirkende stasjoner. Disse kan inkludere forskere, risiko-håndterende institusjoner, media, aktivist organisasjoner, personlige nettverk, og offentlige byråer. Informasjonen generert gjennom disse stasjonene videreformidles gjennom kommunikasjonskanaler. Dette kan igjen påvirke hvordan stasjonene kommuniserer om risikoen og hvordan den blir oppfattet av mottakere, og så videre, som en sirkulær prosess (Kasperson et al. 1988, s.181).

Gjennom denne prosessen vil signalene filtreres (ikke all informasjon blir tatt i betrakting av individet), dekoderes, og det gjøres en meningsdannelse. Sosiale verdier vil også knyttes til informasjonen, og man vil gjennom sosiale eller individuelle aksjoner akseptere, ignorere, tolerere eller forandre risikoen (Ibid).

Denne prosessen vil føre til en form for risiko-tilpasset atferd, som kan ha uforutsette sekundære konsekvenser, eksempelvis miljømessige, økonomiske, politiske eller sosiale. Det kan også bidra til å skape negative assosiasjoner og misnøye for, og derfor forandre holdninger til aktiviteter, teknologier, myndigheter, og lignende (Ibid, s.182). Slike sekundære risiko-konsekvenser kan videre bli tolket av andre sosiale grupper og individer slik at et nytt stadie av sosial påvirkning av risiko oppstår og produserer tertiære konsekvenser. En risiko kan på denne måten gi "bølge" effekter (*Ripple-effects)* å spre seg til andre lokasjoner eller fremtidige generasjoner. Risikoens bølge-effekter betegner ulike atferdsendringer som oppstår i respons til risikokilden. Sekundær effektene blir så oppfattet av ulike sosiale grupper og individer slik at tertiær-effekter oppstår. Derav kan risiko tilknyttet den initierende hendelsen skape bølge-effekter som får konsekvenser for lokalsamfunn, industri, interessenter, storsamfunnet, eller til og med globalt som illustrert i figur 7 (Ibid).

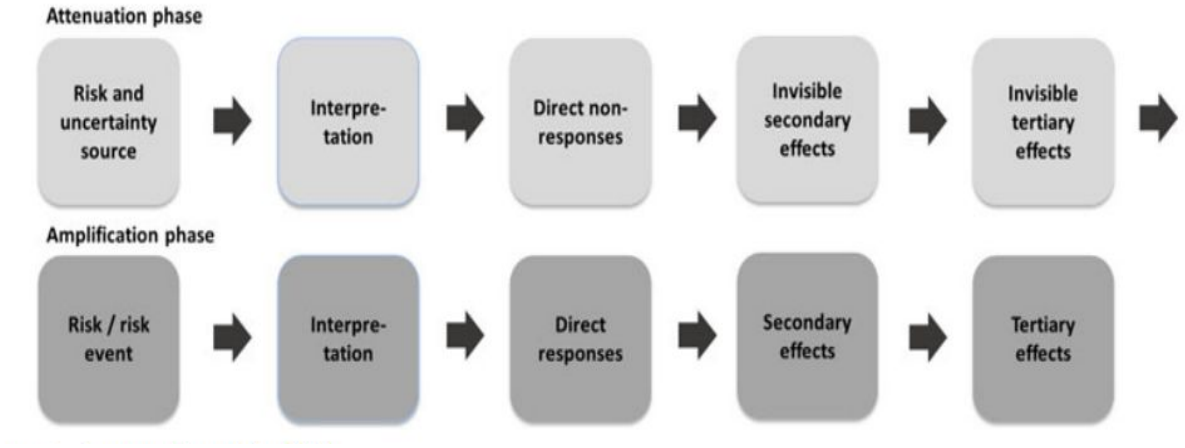
Ifølge Kasperson et al. er det spesielt fire karakteristikker ved informasjon som utgjør om risiko forsterkes eller minskes gjennom den sosiale prosessen. Volum, eller mengde informasjon. Til hvilken grad det er uenigheter om informasjonen presentert. Grad av hysteri eller dramatisering, og de symbolske konnotasjonene ved informasjonen da dette ikke tolkes i isolasjon (Ibid, s.184). Disse elementene modifiserer informasjonen, og derfor risikopersepsjoner.

SARF modellen er altså et rammeverk for å analysere hvordan risikokilder kommuniseres og modifiseres fra sender, gjennom stasjoner og kanaler, til mottaker. Alle nivå i kommunikasjonskjeden, individer, media, og så videre filtrerer informasjonen som videreformidler den med enkelte variasjoner. Denne sosiale dimensjonen av risiko, og de "bølge" effektene dette kan forårsake er en essensiell del av risikostyring og beslutning i dagens verden.

Usikkerhetsperspektiv

Risikoens bølge-effekter vil utspilles i kjølevannet av en uønsket hendelse, men kommunikasjon angående gitt risiko bør være en altomgripende del av prosessen. Fjæran og Aven (2019) påpeker risiko kommunikasjonens rolle i før-vurderingsfasen, før en uønsket hendelse har inntruffet. Nemlig hvordan grad av risiko demping eller overdrivelse påvirker den sosiale reaksjonen i etterkant (Fjæran & Aven 2019, s.1). Dette kan trekkes tilbake til risikotilpassende atferd, hvordan mennesker tolker meldinger og derfor hvor beredt man er i møte med risikoen.

Risiko blir vurdert i henhold til hvordan de ansvarlige aktørene konseptualiserer og beskriver risiko. Deres forståelse påvirker hvordan risiko blir innrammet og har derav konsekvenser for hvilke beslutninger som blir gjort. SARF rammeverket blir dog ekspandert som vist i figur 8 nedenfor.



Figur 8 "Utvidelse av SARF modell" Hentet fra Fjæran & Aven (2019) side 15

Det tradisjonelle SARF rammeverket tar utgangspunkt i en tydelig definert risiko. Denne utvidede modellen påpeker at ved å adoptere er bredere, usikkerhet-basert perspektiv på risiko, som grunnlag for risikovurderinger og håndteringer, kan man redusere sosial overdrivelse betydelig.

Sosial påvirkning av risiko er betydningsfullt da forsterkelse gjør individer i stand til å håndtere risiko og hendelser gjennom risikopersepsjon og dens påvirkning på daglig atferd.

Men på den andre siden kan demping av risiko lede til potensielt store konsekvenser ved at en risiko blir underestimert og derfor utilstrekkelig håndtert.
Denne før-fasen av risiko, hvordan kommunikasjonen og derfor responsen foregår blir sentralt i konteksten av nye moderne og komplekse teknologier som Smartgrids. Positive innvirkninger for miljø, økonomi og samfunn er åpenbare og veletablerte. Hvordan risikoen er forstått, innrammet og kommunisert via myndigheter, media og befolkningen kan derimot ha negative konsekvenser dersom kommunikasjonsprosessen er misforstått og feil vinklet.

Teori og empiri viser ofte at offentlig opinion av en beslutning er mer positiv og akseptert dersom flere stemmer er hørt, flere argumenter er lagt frem, og den rasjonelle, eller saklige informasjonen styrer (Chong 2018, s.12). Risiko kommunikasjonsprosessen bør derfor være omfattende, involverende og transparent (Park & Sohn 2013).

Relatert til ny teknologi kan små ukjente risikoer gjøre stor skade. Risikoer som i mindre grad er kjent, eller komplekse kan skape stor offentlig bekymring. Fordi risikoen vil da i mindre grad la seg kontrollere, noe som da impliserer at andre, potensielt verre uønskede hendelser kan oppstå.

Når man da omtaler *Smart Grids,* et system av enorm samfunnsmessig kritikalitet som igjen avhenger av et system preget av økende kompleksitet og negative trender relatert til cyberkriminalitet, vil det være behov for å ta diskurs om risiko alvorlig. SARF rammeverket vil være behjelpelig i å undersøke kanaler som media og myndigheters risikokommunikasjon angående Smart Grids. Hvordan denne kommunikasjonsprosessen foregår er av betydning for persepsjoner. Hvilke saker media gir oppmerksomhet får betydning for offentligheten, *Agenda-setting*, og hvordan disse sakene belyses, *Framing*, vil ha betydning for offentlig persepsjoner (Parveen et al. 2017, s.4) Videre vil rammeverket gjøre det mulig å drøfte om en uønsket hendelse vil ha betydelige sekundær- og tertiær effekter.

Til slutt må det påpekes at SARF rammeverket har vært under kritikk, blant annet for å over simplifisere hvordan befolkningen oppfatter risikosignaler (Petts et al. 2001). Men rammeverket er likevel et godt verktøy for diskusjon og undersøkelse av hvordan risiko har blitt kommunisert, og derfor prediksjon av sosiale reaksjoner etter en hendelse.

4. Metode

Metodikken anvendt i dette studiet er valgt med det formål å utforske om det eksisterer samsvar, eller diskrepans mellom hvordan risikoprofilen tilknyttet Smart Grids kommuniseres via media og myndigheter til allmennheten. Derav er håpet å kunne dra en konklusjon om risiko vil bli sosialt forsterket eller dempet i møte med en eventuell uønsket hendelse.

Faglitteratur og systembeskrivelser ble hentet og analysert fra legitime sikkerhetsmyndigheter og tidsskrifter, dette gjør opp både teknologiske beskrivelser samt etablering av trusselbildet. Dette kapittelet redegjør for valg av forsknings logikk, metode, og datainnsamling og analyse. Deretter vil kvalitetskriterier, og styrker og svakheter med metodikken redegjøres for.

4.1 Forskningsdesign

Forskningsdesign er en overordnet plan som konstrueres med det formål å besvare problemstilling og forskningsspørsmål. Designet skal linke forskningsobjektet til metoden valgt for undersøkelse (Blaikie & Priest 2019, s.15).
Tre spørsmål er sentrale i designet; hva, hvordan og hvorfor (Ibid, s.36). Hvordan og hvorfor denne metoden er valgt utdypes videre i kapittelet.

Hva

Studieobjektet er et komplekst fenomen som krever forskjellige analysemetoder. Fenomenet som undersøkes er kommunikasjons påvirkning på risikopersepsjoner og hvordan ulike persepsjoner kan ha følger for sosial påvirkning av risiko. Det ble derfor ansett som hensiktsmessig å benytte et *eksplorerende* design da det tillater mer flyt mellom empiri og teori, samt legger til rette for en kontinuerlig læringsprosess gjennom hele prosjektet (Blaikie & Priest 2019, s.89; Sand 2019). Videre er logikken benyttet *abduktiv* da det gir de beste

muligheter for eksplorasjon og deskripsjon. I følge Blaikie og Priest (2019) vil en abduktiv tilnærming også være best egnet til å beskrive fenomenet gjennom forståelse og foreslå grunner av et fenomen, fremfor å gi konkrete forklaringer og årsaker (Blaikie & Priest 2019, s.99). Det er en logikk som fokuserer på meninger, fortolkelser, motiver og intensjoner, og i et studie av kommunikasjon og subjektive oppfatninger vil det være hensiktsmessig.

Hvordan

Dette prosjektet benyttet seg av triangulering, kombinasjon av kvalitativ og kvantitativ metode. Målet var å belyse risikokommunikasjons aspektet fra ulike vinkler for å kunne trekke mer objektive konklusjoner angående mediers belysning av tema. Datagenerering besto av et omfattende litteratursøk av relevante dokumenter, samt artikler som tar for seg Smart Grid teknologi. Analysemetoder besto av kvalitative innholdsanalyser, og kvantitative sentimentanalyser av medieartikler. Trianguleringen, eller *Mixed Methods,* gjør det mulig å skape dype beskrivelser av fenomenet med et kvantitativt, konkret grunnlag (Blaikie & Priest 2019, s.214).

4.2 Litteratursøk

Da oppgaven dekker en bred tematikk, fra tekniske systembeskrivelser, det digitale kraftnettets trusselbildet, og risikos dimensjoner er det hensiktsmessig å inkludere tilsvarende omfattende litteratur. Metodikken anvendt er derfor primært i form av dokument- og innholdsanalyser. Litteraturen består i hovedsak av bøker, artikler, kronikker, internettsider, og foredrag.

Det har blitt gjort et utdypende søk for foreliggende kilder om *Smart Grid* konseptet og visjon, og om arbeid innen denne sektoren reflekterer tilstrekkelig sikkerhetstilstander. Beskrivelsene vil finne sin tyngde og reliabilitet i ekspertvurderinger om slike høyrisikoteknologier.

I følge Jacobsen (2005) er sekundærkilder godt egnet i situasjoner hvor man ønsker å tilegne seg data om hvordan andre har tolket gitte situasjoner og hendelser, eller når man søker fakta om hva mennesker faktisk har sagt eller gjort. Derfor vil sekundærkilder være mer fruktbart da persepsjoner, som subjektive oppfatninger, blir en gjengivelse av andres erfaringer og oppfatninger.

Dokumentanalysen utført er i stor grad kvalitativ som viser til en systematisk gjennomgang av litteraturen med det formål å kategorisere og registrere det innholdet som er av relevans for å besvare problemstillingen.

Da de fleste tidsskrifter i dag er digitalisert kan man anta at en vesentlig del av befolkningen får informasjon fra de samme kildene uavhengig av bosted. Prosjektet tar derfor utgangspunkt i at nyhetsmedier har i stor grad lik og omfattende innflytelse på individer uavhengig av deres bosted. Og derfor at befolkningen ikke har drastisk ulike risikopersepsjoner i henhold til Smart Grid teknologi. Videre vil en bredere inkludering av tidsskrifter generere mer data som igjen gir et mer fullstendig og kredibelt analyse av mediebildet.

For å finne relevant data ble standard søkemotorer som Google, Google Scholar og Yahoo benyttet, samt Universitetsbibliotekets program Atekst (Retriever).
Bestemte søkeord avgrenset søket til relevante artikler og dokumenter angående Smartgrid-teknologi, digitalisering av kraftsektoren, nye trusler denne innovasjonen medfører, aktører innenfor sektoren og lovverk disse må rette seg etter. Og hvordan sikkerhetsrelatert arbeid, slik som barrierer, blir implementert for å beskytte kritiske verdier.

Analysen av innsamlet sekundærdata var tofoldig. For det første ble det gjennomført innholdsanalyser. Disse ble sammenstilt i en kvalitativ metaanalyse der hensikten var å skaffe et overblikk og sammenstille tidligere forskning innen sikkerhet og Smart Grids. Beskrivelser av prosjektets fenomener er derfor en omfattende kombinasjon av enkeltstudier for å sikre et helhetlig forskningsbilde der flere perspektiver blir drøftet. Både tekniske systembeskrivelser og vurderinger fra sikkerhetsmyndigheter støtter seg på dette. Dette prosjektet får faglige

tyngde fra mange dokumenter, både sikkerhetsvurderinger fra myndigheter og tekniske dokumenter fra ulike sentrale aktører i energisektoren og forskere innen ulike institusjoner.

Den andre analyseprosessen besto av media- og sentimentanalyse der formålet var å forstå medias risikokommunikasjon til den bredere befolkningen om både de positive og negative egenskapene assosiert med Smart Grids. En slik kvantitativ innholdsanalyse av media ga mulighet til å systematisk telle og klassifisere ulike aspekter av artikler, i dette tilfellet stikkord.

4.3 Medieanalyse

I forsøket på å skape et bilde av risikoforståelse og kommunikasjon fra media til befolkningen har en kvantitativ medieanalyse og sentimentanalyse, eller opinion analyse blitt anvendt. Hensikten var å identifisere, kvantifisere og studere subjektiv informasjon som meninger, følelser og evalueringen (Chong 2018). Dette er hensiktsmessig da risikopersepsjon ofte skapes gjennom indirekte kontakt med kilden. Media er en enorm kommunikasjonskanal som sprer sin melding og sitt budskap til den generelle befolkningen, hvordan media da velger å ramme inn et tema vil da trolig ha følger for offentlig opinion.

Nyhetsmedier er for mange hovedkilden for informasjon og nyhetssaker. Som kommunikasjonskanal fungerer de på mange måter som knutepunkt mellom verden og allmennheten. Det medier formidler får befolkningen kunnskaper om. Måten medier belyser risiko tilknyttet ny teknologi som Smart Grids, vil derav være av betydning for befolkningens persepsjoner. Dersom medier feilinformerer og misrepresenterer risikoprofilen er det grunn til å tro at sosial risiko vil bli påvirket i møte med en uønsket hendelse. Er allmennheten klare over at energisektoren kan bli utsatt for tilsiktede cyberangrep? Er befolkningen oppmerksomme på det digitale landskaps kompleksitet? Og er man bevisst på hvilke konsekvenser et vellykket angrep kan ha, ikke bare for dem som individer, men for samfunnet i sin helhet?

For å skape et bilde på risikopersepsjoner knyttet til Smart Grids å besvare disse spørsmålene er det hensiktsmessig å analysere hvordan medier kommuniserer risikoprofilen. Gjennom en sentimentanalyse er formålet å undersøke ulike elementer av artikler, spesielt ordforrådet. Analysemodellen skal forsøke å belyse hva sender av risikokommunikasjonen vil oppnå med artikkelen, hvordan ordvalget påvirker artikkelens budskap, samt hvilken effekt artiklene kan ha på mottaker (Tørdal 2017).

Medieanalysen omfatter i hovedsak kilder hentet via søkemotoren A-tekst, men inkluderer også enkelte kilder hentet gjennom enkle Google-søk. Formålet var å skaffe et overordnet bilde på hvordan informasjon om Smart Grid teknologi blir belyst i både lokale og riksdekkende nyhetsmedier, samt gjennom internettsøk. Kildene består derfor av aviser og magasiner, samt enkelte artikler fra andre relevante aktører (Infosec, Forskning og Addsecure) som var fremtredende resultat av internettsøket. Kildene anvendt er presentert i tabellen nedenfor og hver artikkel er videre utdypet i vedlegg 1 (medieanalyse).

Riksdekkende medier	Lokalaviser
Teknisk Ukeblad	Sunnmøreposten
NRK	Romsdal Budstikke
Aftenposten	Moss avis
ABC Nyheter	Avisa Nordland
ITB aktuelt	Adressavisen
VG	Halden arbeiderblad
E24	Trønder-avisa
Dine penger: Forbruker	Trønderbladet
Morgenbladet	Bergens tidende
Nationen	Harstad Tidende
Klassekampen	Oppland arbeiderblad
Computerworld	Opdalingen
Volt	Aura avis
Finansavisen	

NTB
Byggfakta
Arkitektur N
Forskning.no
Addsecure
Sintef Infosec

Tabell 1: Medieanalyse

Av disse kan 12 beskrives som tematisk fokuserte da de dekker hendelser og nyheter av begrenset omfang; Teknisk ukeblad, ITB aktuelt, Dine penger: Forbruker, E24, Computerworld, Volt, Finansavisen, Arkitektur N, Byggfakta, Forskning, Sintef infosec, og Addsecure.

Sentimentanalyse

Ved å telle en egenskap ved disse dokumentene, i dette tilfelle ordforråd, kan man avgjøre om dokumentet på negativ eller positiv måte belyser tema (Sander 2019a), dette vil igjen gjøre det mulig å formulere en tolkning av befolkningens holdning til en gitt risiko.
Denne analyseprosessen ble utført ved å se etter forhåndsbestemte nøkkelord;

Positive nøkkelord	Negative nøkkelord
Smart	Hacking
Nyttig	Ondsinnet
Lønnsomt	Datainntrenger
Trygghet	Katastrofe
Effektiv	Skade
Verdiskapning	Angrep
Gunstig	Trussel
Prosumer	Kompleksitet
Intelligent	Ødeleggelse

Gevinst	Sabotasje
Bedre	Avbrudd
Forsyningssikkerhet	Strømbortfall
Strømoverskudd	Sårbarhet
Fleksibilitet	Cyber-trusler/sårbarheter
Reduksjon	Misbruk

Tabell 2 "Positive og negative nøkkelord for sentimentanalyse"

Nøkkelord ble valgt ut i fra deres negative og positive, konnotasjoner og assosiasjoner. Ordene ble også analysert i sin kontekst, for eksempel kan ordet *reduksjon* være brukt i både negative og positive beskrivelser, men for dette studiet hører det med reduksjon for miljøbelastning, strømforbruk, økonomisk bekostning og lignende.

Alle "negative" nøkkelord viser til en fare, en trussel eller en uønsket hendelse som kan ramme det digitale kraftnettet. Mens "positive" nøkkelord refererer til samfunnsmessig, økonomisk eller miljømessig gevinst man kan tjene på implementasjon og anvendelse av smartgrid-teknologi.

For å holde sentimentanalysen relevant og spisset ble antall valgte nøkkelord begrenset til 30. Nøkkelordene kunne også eventuelt bli påbygget ut i fra dens kontekst. For eksempel kunne ordet *angrep* inngå i ord som *angrepsflate, angriperne og angrepet.* Dersom et "positivt" stikkord ble brukt i en negativ setning, eller i en setning uten relevans til Smart-teknologi, ble det ikke registrert i analysen.

I totalt 75 avis og nettavis artikler ble de forhåndsdefinerte nøkkelordene registrert 1080 ganger. Som tidligere beskrevet ble det ikke sett nødvendig å avgrense media til regionale tidsskrifter da befolkningen i større grad enn tidligere kan tenkes å få nyheter fra like kilder. Nyhet- og informasjonsbildet som dekker saker om Smart Grid-teknologi ble funnet gjennom aviser, søkemotoren Google og gjennom databasen a-tekst (retriver). Artiklenes relevans ble

determinert gjennom Smart Grid-teknologisk knyttede søkeord som *Smart Grid, ams, elhub, fleksibel strøm,* og lignende.

Det ble analysert i alt 75 artikler fra 33 forskjellige tidsskrifter. For studiets hensikt ble tidsskriftene delt i to kategorier: Allmenne- og tematiserte tidsskrifter.
Allmenne tidsskrifter omfatter de lokale og nasjonale riksdekkende tabloidaviser, eller nyhetsmedia. Altså de tidskrifter som dekker nyheter av all slags tema og omfang. Mens tematiske tidsskrifter betegner de mer faglige rettede tidsskriftene. Kilder som fokuserer på teknologi, næringsliv, politikk og lignende.
Denne kategoriseringen sees nødvendig da det kan tenkes at de allmenne tabloidene ikke går i samme dybdenivå som de faglige. De tematiserte tidsskriftene vil sannsynligvis avdekke sårbarheter og trusler på en mer vitenskapelig og omfangsrik måte.

Ut i fra denne kategoriseringen kan man dele de 33 tidsskriftene inn i 21 allmenne og 12 tematiserte tidsskrifter. Av disse 12 er 8 teknologisk eller økonomisk fokuserte, og resterende består av andre tematiserte tidsskrifter.

Analyseprosessen er tredelt. Først ble litteratursøket utført ved å begrense artikler til de med relevans for temaet Smart Grids. Deretter ble artikler som var av relevans analysert i sin helhet slik at tekstens kontekst ble forstått. På denne måten unngikk prosjektet å telle stikkord som ikke var av kontekstuell betydning. Det tredje steget besto å telle antall stikkord i sin totalitet og vurdere deres belysning hver for seg. Med andre ord ble stikkord som ble brukt i en relevant tekst, men likevel brukt på urelevante måter i en setning, luket bort.

På denne måten ble det forsikret at stikkordene ble brukt i beskrivelse av teknologi og, eller tilknyttede sårbarheter. Basert på dette kunne enkelte artikler sies å uttrykke sterkere bekymringer rettet mot sikkerhetsutfordringene smart Grid-teknologi poserer. Andre artikler belyser teknologien som innovativ og påpeker samfunnsmessig gevinst, mens noen artikler beskriver teknologien fra både positive og negative sider.

For å eliminere gråsoner og skape pålitelighet i den kvantitative analyseprosessen ble det gjort klare skiller mellom kategoriene *Negativ, Positiv,* eller *Både positiv og negativ.* Artikler

som ble kategorisert *Positiv* inneholder *kun* positive stikkord i relevant kontekst. I likhet inneholder *Negative* artikler 100% negative stikkord. Dersom en artikkel belyste Smart Grid teknologi hovedsakelig positivt, men uttrykte en eller flere bekymringer ble den kategoriset *Både positiv og negativ.*

Analysen omfattet 75 artikler fra 33 ulike nyhetskilder. Totalt ble 1080 stikkord registrert, derav var 753 *positive*, og 327 hadde *negative* konnotasjoner. Basert på denne kategoriseringen kunne 53 artikler sies å bære positivt budskap, 5 negative, og 17 viste både positiv og negativ belysning av Smart Grid teknologi (Se Vedlegg 3).

4.4 Kvalitetskriterier

For å skape systematisk og transparent forskning må kvalitetskriterier som validitet, reliabilitet og overførbarhet sikres (Leung 2015). Disse kriteriene, samt styrker og svakheter med valgt metode drøftes i denne seksjonen.

Validitet

Validitet, eller gyldighet, omhandler relevansen av metoder og data brukt, og dens egnethet til å besvare forskningsprosjektets problemstilling (Leung 2015). Problemstilling og forskningsspørsmål ble forandret flere ganger underveis i forskningsprosessen. Tematikken ble gjort klar fra begynnelsen, men hvordan data skulle analyseres og hvilken metodikk ble anvendt har blitt revidert underveis. For eksempel skulle intervju være en sentral del av både forming og innhold av prosjektet. Men grunnet komplikasjoner hadde bare to av totalt åtte kontaktede virksomheter innen Smart Grid teknologi mulighet til å disponere informanter. Datagrunnlaget ble derav for magert og prosjektet måtte styrkes ytterligere gjennom litteratursøk og analyser. De to foretatte intervjuene var likevel av stor nytte til å bekrefte antagelser angående system-teknologi og hvordan aktører innen sektoren oppfatter risikobildet.

Videre ble metodetriangulering betraktet som en styrke da en kvantitativ analyse kunne legge grunnlaget for å drøfte på et mer konkret grunnlag enn kun antagelser og innholdsanalyser. Formålet var å gjengi et bilde av mediers belysning av Smart Grid systemer, og derav hvordan risikoprofilen kommuniseres til det bredere samfunn. Ved å etablere stikkord og analysere artikler deretter var målet å detektere følelser som frykt, engasjement, usikkerhet og lignende. Sentimentanalysen har likevell noen potensielt store svakheter som prosjektet anerkjenner og har tatt i betraktning. Blant annet at ulike mennesker kan uttrykke følelser på forskjellige måter. For eksempel kan noen plussord som i seg selv indikerer forbedring, som *effektiv,* benyttes for å uttrykke frykt. Som for eksempel "hackere blir mer effektiv". Ethvert forhåndsdefinerte nøkkelord ble derfor analysert i sin kontekst. Det kan fortsatt tenkes at inkludering av flere nøkkelord ville vært mer hensiktsmessig for analysen, men utvalget ble ansett som tilstrekkelig i kombinasjon med dokumentanalyser.

Det anerkjennes også at media ikke er synonymt med offentlig opinion. I dagens globale informasjonsverden kan ikke mennesker betraktes som ureflekterende mottakere av medias budskap. Det eksisterer toveiskommunikasjon gjennom en rekke digitale medier som former persepsjoner og tillit. Likevel kan man anta at tradisjonelle nyhetsmedier og tabloider fortsatt opptar en enorm del av mediebildet. Mange mennesker får fortsatt store mengder informasjon gjennom tv, radio og aviser. Det argumenteres derfor for at tradisjonell media i det minste har et stort bidrag i formingen av visse persepsjoner.

Ved å benytte dokumentstudie og innholdsanalyse er det mulig å dekke et bredt utvalgt av ekspertvurderinger blant både sikkerhetsmyndigheter, produsenter og driftere av SG-teknologi. Videre blir det mulig å kartlegge media- belysning og kommunikasjon over tid, samt skille mellom ulike tidsskrifter. Et omfattende utvalg av slikt kvalitativt materiale ble også verdifullt for å berike å rettferdiggjøre tekniske systembeskrivelser. Deres verdi, avhengigheter, koblinger og sårbarheter.

Reliabilitet

Reliabilitet, eller pålitelighet, handler om forskningens repliserbarhet (Ibid). Hvordan sammenhengen mellom empiri, analyse og resultat skaper et koherent og gjentagbart resultat. Analyse resultatenes pålitelighet var i fokus gjennom hele prosessen. Resultater dratt fra

omfattende innholdsanalyser ble faktasjekket gjennom andre sammenlignbare kilder, og enkelte systembeskrivelser ble i tillegg bekreftet gjennom samtaler med eksperter.

Likevel kan måling og analyse alltid by på feil. Dette var en frykt spesielt innen sentimentanalysen da analysering av konkrete stikkord i forskjellige kontekster av og til måtte ty til subjektive betraktninger. Nemlig om stikkordene ble brukt i en relevant setning. Derfor anerkjenner prosjektet at personlig *bias* kan forårsake enkelte variasjoner i spesielt kvantitative målinger. Det ble derfor gjort klare skiller mellom kategorier for å minimere gråsoner.
Metodetriangulering ble ansett som en styrke da innholdsanalyser og sentimentanalysen kunne spille på hverandre, og drøftinger kunne bli gjort ut i fra et mer objektivt innblikk i mediebildet.

Overførbarhet

Prosjektets hensikt er å tolke begivenheten *sosial demping og forsterking av risiko innen smart grid teknologi* ved bruk av veletablerte teoretiske rammeverk. Håpet var da å konstruere nye ideer å trekke pragmatiske konklusjoner. Å gi mening til hendelser relatert til en større kontekst (Danermark et al. 2002, s.80).

Denne logikken, som alle andre, har sine begrensninger. Det er ingen faste kriterier som gjør det mulig, på en definitiv måte, å bekrefte validiteten av trekte konklusjoner. Slutninger blir trekt ut i fra beste mulige forklaring.

Ved omfattende datainnsamling og utdypende analyse gjennom samfunnssikkerhetsfaglige teoretiske rammeverk var håpet å nå en koherent og gyldig konklusjon. Dette prosjektet omfatter både observerbare elementer samt mer abstrakte strukturer. Absolutte sannheter er sjeldne i samfunnsvitenskapen, konklusjoner dratt må derfor betraktes som “kvalifisert gjetting” (Persson 2019).

De fleste kvalitative studier fokuserer på et spesifikt fenomen eller problem innen visse kontekstuelle rammer, og generaliserbarhet blir derav påvirket (Leung 2015). Likevel lar et omfattende litteratursøk og innholdsanalyser det mulig å gi et overordnet innblikk i det

digitale trusselbildet, ikke bare i energisektoren. Hovedfokuset er på truslene cyberkriminalitet poserer for sektoren, men gjennom belysning av tette koblinger og kompleksitet kan det tenkes at beskrivelser av trusselbildet er overførbart til andre kritiske strukturer som avhenger av IT-løsninger. Videre gjør en pragmatisk tilnærming og analyse av mediebildet det mulig å vise til årsak-effekt sammenhenger mellom kommunikasjon gjennom media og dens påvirkning på risikoprofiler.

Resultatene vil ikke være gyldige for alle sektorer og kommunikasjonsprosesser, men håpet er at trekke konklusjoner kan adopteres til andre sammenlignbare systemer og sosiale kontekster, og forhåpentligvis bidra til videre forskning.

5. Empiri

I dette kapittelet presenteres funn fra dokumenter og artikler.
Først vil trusselbildet kartlegges i henhold til myndigheters beskrivelser for å vise til cyberrisiko i energisektoren. Deretter vil observasjoner fra medieanalysen presenteres for kunne skildre mediers belysning av Smart Grid teknologi.

For prosjektets formål er det nyttig å kartlegge trusselbildet som beskrevet av ulike myndigheter og sikkerhetseksperter da slike beskrivelser belyser omfanget av cyberrisiko. Medieanalysen vil så utdype hvordan ulike tidsskrifter portreterer det samme tema. Da hypotesen er at grad av overenstemmelse mellom risikoprofilene vist av myndigheter og media vil ha direkte påvirkning på risiko er dette skillet nødvendig. Med andre ord, er det store forskjeller mellom risikoprofilen beskrevet av sikkerhetsmyndigheter, og risikoprofilen som blir kommunisert via media til allmennheten?

5.1 Smart Grids og trusselbildet

5.1.1 Cyberangrep i energisektoren

Dokumenterte cyberangrep direkte rettet mot energiinfrastruktur er fortsatt relativt sjeldne (Desarnaud 2017, s.16). Cyberangrep som indirekte har påvirket sektoren har hendt tidligere, men ingen med så omfattende konsekvenser som man opplevde i Ukraina 2015 (Johansen 2016; McLellan 2016; Olsen 2020, s.19).

Imidlertid er man klar over at cyberkriminalitet øker samt at energisektoren i større grad, med IKT, er kjernen av kritiske funksjoner i samfunnet (Hotvedt & Saugstad 2017; NSM 2019, s.10; Desarnaud 2017, s.27). Angrep kan derfor tenkes å få mer alvorlige konsekvenser i takt med digitaliseringen. Nedenfor beskrives få, men store angrep som har indirekte eller direkte forårsaket skade i sektoren. Listen er ikke utfyllende, men illustrerer sårbarheter.

SQL Slammer

Slammer betegner et datavirus angrep fra 2003 som resulterte i tjenestenekt blant flere systemer (DDoS). Viruset var ikke rettet mot en spesifikk virksomhet, men spredte seg gjennom flere tusen datamaskiner (Grimes 2019), før det til slutt infiserte og kompromitterte dataparameter-display hos Davis-Besse atomkraftverk i USA. Datasystemet samlet sanntidsdata fra flere kritiske enheter i kraftverket for å kunne overvåke tilstand. Systemet var nede i flere timer, men fikk ingen ytterligere konsekvenser. Likevel viser hendelsen til hvordan kritisk infrastruktur kan bli påvirket av datavirus gjennom en usikret tilkobling til et tredjeparts selskap. Resterende av Davis-Besse sine nettverkssystemer var segregert og sikret slik at viruset ikke ville forårsaket større skade (Desarnaud 2017, s.16).

Stuxnet

Et sofistikert datavirus som benyttet seg av flere *Zero-day*[1] sårbarheter i 2010 infiserte datamaskiner som opererte programmerte logiske styringssystemer (PLS) i Natanz, Iran (Ibid). Viruset fikk tilgang på sentrale enheter i kraftverket og fortsatte å ødelegge nesten

[1] Betegner sårbarheter som er ukjent, eller ikke håndtert, av de som arbeider med å redusere risiko. Da sårbarheten er ukjent kan den utnyttes av cyber angripere, også kjent som *Zero-day exploit.*

1000 sentrifuger benyttet for fordeling av uran (Ibid; Frøystad 2017). Hendelsen viser at selv isolering av nettverk, *Airgap*[2], ikke alltid sikrer systemet mot angrep.

Black Energy

I 2015 ble tre energiselskaper i Ukraina utsatt for noe man tidligere ikke trodde kunne skje. Cyberangrep rammet strømnettet og slo ut 30 transformatorstasjoner, 80.000 boliger og bedrifter. Flere hundre tusen mennesker fikk sin strømtilførsel avbrutt uten forvarsel i desember måned (Desarnaud 2017, s.18; Johansen 2016; McLellan 2016; Olsen 2020, s.19). Gjennom sosial teknisk manipulasjon og *Spear-phishing,* som er "fisking" etter sensitiv digital informasjon, fikk angriperne tilgang til et nærliggende nettverket. Fra her kunne de benytte digitale bakdører for å få tilgang til større deler av systemet. Iot komponenter og datasystemer som SCADA er som regel operert via standard dataprogrammer slik som *Windows,* og dog utsatt for standard skadevare[3] (McLellan 2016).

2020

I mars 2020 uttalte selskapet ENTSO-E at de hadde nylig funnet tegn til et vellykket cyberangrep i sine kontor nettverk. Selskapet er ansvarlig for koordineringsmekanismer som leverer energi gjennom EU og består av 42 driftere av kraftverk i 35 europeiske land. Det kompromitterte nettverket var tilstrekkelig segregert og ikke tilkoblet operasjonelle energioverføring-systemer. Angrepet ble derfor isolert til mindre IT systemer (Lyngaas 2020).

Angrepet illustrerer likevel noen store bekymringer. Nemlig at et digitalt innbrudd kan over tid gå oversett. I et så sentralt selskap kan man anta at sikkerhet er en prioritet. Et slikt angrep i mindre ressurssterke selskap kan derfor eventuelt aldri bli oppdaget.

I mai 2020 ble deler av Storbritannias kraftverk hacket. Selskapet Elexon er et ledd mellom kraftstasjoner og distribusjonsselskaper. Deres datamaskiner og nettverk ble kompromittert som resulterte i at ansatte ble utestengt fra sine systemer (Clowes 2020).

[2] *Air Gap/Wall:* Metode innen nettverkssikkerhet som handler om å fysisk isolere nettverkssystemer fra usikre nettverk, slik som det offentlige internettet.
[3] Fellesbetegnelse på programvare skapt med den hensikt å stjele, ødelegge, og manipulere data eller systemer.

I sum viser angrepene til et utsatt system med store samfunnsverdier, der kompleksitet og tette koblinger gjennom et stadig ekspanderende digitalt system utfordrer energisektoren, og påpeker sårbarheter man tidligere ikke var klar over.

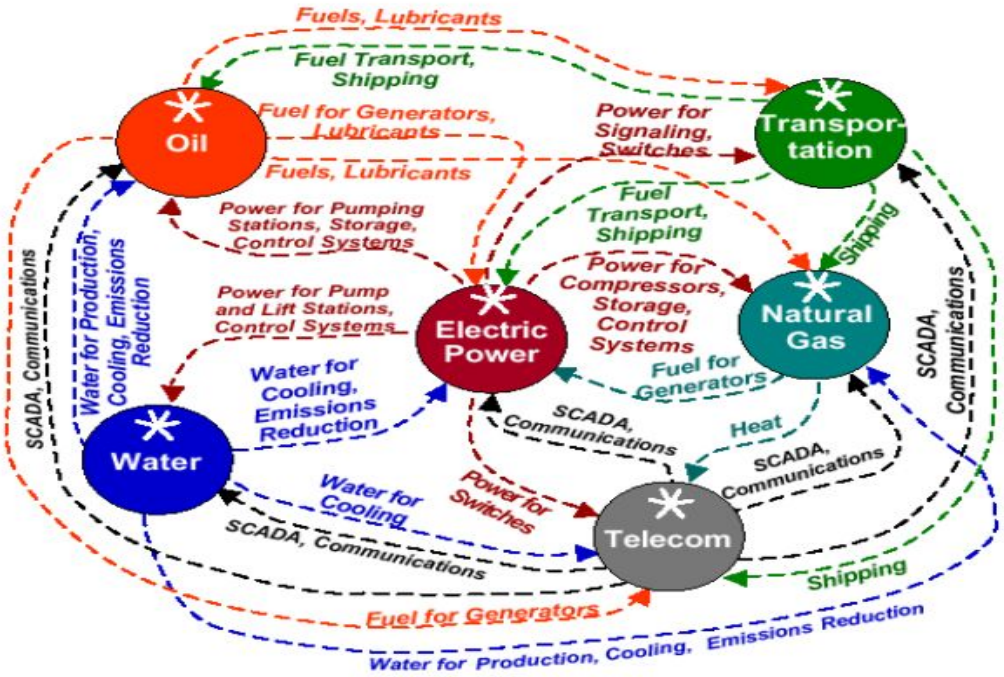
5.1.2 Sikkerhetsmyndigheter og trusselbildet

De sentrale sikkerhetsmyndighetene Politiets sikkerhetstjeneste (PST), Etterretningstjenesten og Nasjonal sikkerhetsmyndighet (NSM) påpeker de samme bekymringene innenfor den digitale utviklingen (PST 2020; E-tjenesten 2020; NSM 2020).

Digitalisering knytter private hjem til offentlige og militære sektorer i enorme digitale økosystem karakterisert av uoversiktlige verdikjeder og tverrsektorielle, til og med internasjonale, avhengigheter (NSM 2019, s.23). Kompleksiteten som medfølger øker sårbare innganger trusselaktører kan benytte. Digital inntrengelse, kartlegging og sabotasje av kritisk infrastruktur blir ansett som en av de mest alvorlige hendelsene som kan ramme vårt samfunn i dag (PST 2020, s.1). Videre blir det vanskeligere å kartlegge de komponentene og programvarene som faktisk gjør oss sårbare (Ibid, s.5). Økende avhengighet av IKT-løsninger fører til at de som kontrollerer norsk elektronisk kommunikasjon (ekom) sitter med stort ansvar, og kompromittering av deres virksomhet kan bli katastrofalt for samfunnet.

Norge har sjeldent opplevd betydelige avbrudd i kritisk infrastruktur (DSB 2019, s.200). Men risiko øker da digitalisering og anvendelse av mer skybaserte tjenester gjør virksomheter og samfunnet mer sårbart for spionasje, spesielt med tanke på personvern (Olsen 2020, s.19).

Gjennom smart-teknologi knyttes flere systemer til hverandre og samfunnet blir mer til en sammenhengende enhet. Et system kan defineres som tekniske delsystemer, slik som infrastrukturer, eller det kan vise til større organisatoriske systemer som samfunn og nasjoner (Maal et al. 2017, s.16). Systemer og mennesker kommer nærmere og nærmere hverandre, og avhengigheten øker gjennom IoT, digitalisering og systemintegrasjon (NOU 2015, s.54). Smart-teknologi resulterer derfor i et mer tett koblet samfunn, og svikt i et Smart Grid system kan ha alvorlige kaskadeeffekter og fatale konsekvenser for samfunnet som helhet.



Figur 9: "Complexities in Identifying, Understanding and Analyzing Criticial Infrastructure Interdependencies" Fra Sand 2015, s.7

Figur 9 illustrerer kompleksiteten i å identifisere, forstå og analysere gjensidige avhengigheter mellom kritiske infrastrukturer. Kompleksiteten medfører også at systemer som isolert sett er tilstrekkelig sikret blir gjort sårbare gjennom svakere enheter i verdikjeden (DSB 2019, s.197).

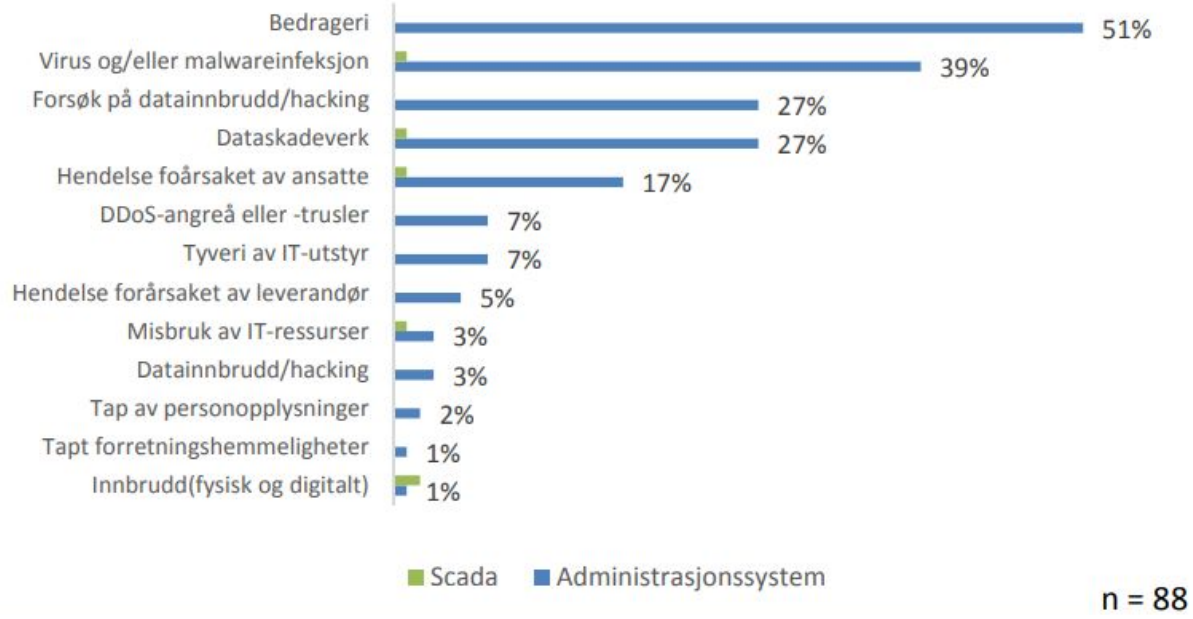
NSM påpeker også kompleksiteten i det digitale landskap. De aller fleste sektorer og funksjoner er avhengig av kraft og IKT (NSM 2020, s.10). Videre digitalisering og bruk av teknologi skaper et overvåkningssamfunn som man ikke kjenner omfanget av (Ibid, s.32). I følge NSM er digitale verdikjeder dynamiske da de etableres i hovedsak ut i fra kostnadseffektivitet for de ulike virksomhetene, og hvor det finnes markedsmuligheter (Ibid, s.33). Smart teknologi åpner et nytt marked der aktører kan tilby IoT-komponenter som har minimal eller ingen sikkerhet og øker derfor risikoen for misbruk (Ibid, s.36; NSM 2018, s.27).

Tette koblinger og ukjente avhengigheter gir store utfordringer for beredskap og hendelseshåndtering (Ibid, s.38). Nettverket har blitt mer integrert og komplekst, og det blir i

større grad benyttet på måter infrastrukturen ikke var opprinnelig designet for (IRGC 2007, s.6).

På verdensbasis antas enheter som forskjellige samfunnstjenester benytter å øke fra 485 millioner i 2013 til 1,53 milliarder i 2020 (Olsen 2020, s.7). IoT teknologi i kraftnettet er tallrike, liten, og spredt utover hele nettet. Dersom en ondsinnet aktør skulle få urettmessig tilgang til kun en slik komponent, kan inntrengelsen benyttes som en digital "dør" til andre komponenter og systemet i sin helhet (Øverby 2018). NSM har påvist slike tverrsektorielle digitale sårbarheter gjennom foretatte inntrenger tester. Ved flere anledninger har testene påvist at gjennom å kompromittere enheter via internett har de kunnet få tilgang til større deler av systemet (NSM 2019, s.20). NSM sine *"hackere"* trengte seg inn i en offentlig virksomhets systemer ved å benytte en IoT gjenstand som drev kontorenes kjøkken. "*Angriperne"* benyttet enheter som en digital "bro" og fikk deretter tilgang på hele systemet (NSM 2018, s.27). NSM anslår at innen 2020 vil opp til 25% av alle digitale angrep utnytte IoT gjenstander (NSM 2017, s.30).

Videre viser en undersøkelse av Norges vassdrags- og energidirektorat (NVE) fra 2015 at kun 11 av 81 nettselskaper uttrykker bekymring for sikkerhetsrisiko angående AMS innføringen (Olsen 2020, s.19). I løpet av 2015 ble minst 20% av virksomheter rammet av virus, med mulig store mørketall. En rapport med hensikt å kartlegge cyberrisiko i energisektoren ble gjennomført av NVE i 2017 (Azam 2017). Figur 10 viser antall cyberangrep og sikkerhetshendelser som har rammet sektoren ifølge undersøkelsen.



Figur 10: "Cyberangrep og sikkerhetshendelser i norsk energisektor" Hentet fra Azam 2017, s.13

Av 88 undersøkte bedrifter rapporterte 39% å få sine systemer infisert av virus og skadevare, 27% rapporterte om hacking-forsøk, og 27% om skadeverk (Azam 2017, s.12). Videre viser rapporten til at administrasjonssystemene er mest utsatt, men enkelte tilfeller hadde hendt der SCADA systemene ble utsatt for cyberangrep. Driftskontrollsystemer som SCADA anses som mest alvorlig da et vellykket cyberangrep kan mørklegge store deler av systemet slik som i Ukraina 2015 (Ibid). Ingen av hendelsene opplevd i norsk energisektor fikk enorme konsekvenser. 69% rapporterer ingen konsekvenser, og 19% rapporterte mindre alvorlige driftsavbrudd der kun 2% førte til økonomiske tap. Ingen driftsavbrudd fikk direkte konsekvenser for sluttbrukere (Ibid, s.15).

Videre viser rapporten til vanskeligheter med å i det hele tatt vite at systemer er infisert. Blant 46% av de utsatte virksomhetene ble sikkerhetshendelsen oppdaget ved tilfeldighet, mens 40% oppdaget kompromittering gjennom rutinemessig arbeid (Azam 2017, s.17).

Til slutt beskriver Direktoratet for samfunnssikkerhet og beredskap (DSB) at Telenors kjerneinfrastruktur er godt sikret, men det finnes derimot ingen alternativer. Et bortfall vil ramme de fleste sektorer i samfunnet og potensielt få få svært store konsekvenser (DSB 2019 s.207). Regjeringen påpeker viktigheten av å redusere denne kritikaliteten av

kjerneinfrastrukturen da samfunnsverdiene den underbygger blir ansett som for høy (NOU 2015, s.16).

5.1.3 Trusselaktører og angrepsmetoder

Kripos beskriver IKT-kriminalitet som et reelt samfunnsproblem. Tall fra NorCERT registrerte omtrent 20.000 cybertrusler i 2018, derav 5000 var saker som måtte undersøkes videre (NSM 2019, s.10).

Trusselaktører spenner bredt innen motivasjon, kapasitet og intensjon i det digitale landskap. Såkalte *Script Kiddies*[4] og sosiale hackere betegner ofte individer eller mindre grupper med den motivasjon å teste grenser, eller å se hva de kan få til (NOU 2015, s.54). De benytter som regel sosial manipulasjon eller eksisterende digitale metoder for å oppnå tilgang til systemer.

Hacking for å trenge inn i ulike digitale systemer blir enklere å utføre for aktører som har motivasjon og vilje. Et enkelt søk på Google, eller fritt tilgjengelige nettlesere som "skjuler" brukerens identitet og IP-adresse slik som TOR[5], gir en mengde av resultater. "How-to" guider innen digital kriminalitet og "Crime-as-a-service" som er et marked der kriminelle tjenester som datatyver, botnett og tjenestenektangrep fritt selges og kjøpes over internett (NOU 2015, s.55).

Videre inneholder aktørbildet mer ressurssterke aktører som arbeider for større organiserte grupper eller stater. Politisk motivasjon gjennom digital terrorisme, militære motivasjoner gjennom spionasje, eller økonomiske verktøy som svindel er stadig økende trusler. Såkalte *Hacktivister* utgjør også en del av trusselbildet, og omfatter politisk motiverte grupper som de omtalte "Anonymous" (Sands 2016).

[4] Betegner en uerfaren trusselaktør som benytter programmer, eller "manus" skapt av andre for å angripe datasystem og nettverk.
[5] Et informasjonssystem, eller *Internet browser,* som er tilgjengelig for alle og gir anonymitet på internett ved å sende internett-trafikk gjennom et verdensomspennende datanettverk.

Skadevarene (*malware)* disse aktørene benytter er mangfoldige og kategoriseres ut fra intensjon og spredningsform. Felles er at de utnytter teknologiske sårbarheter for å få urettmessig tilgang til enhetene de infiserer (NOU 2015, s.54).
Gjenstander koblet til nettverk blir sårbare for sikkerhetssvakheter i andre tilkoblede komponenter, systemet er derfor kun så sterkt som sitt svakeste ledd. En inntrenger kan derfor infisere en komponent, skadevaren sprer seg, og hackeren vil få tilgang til større deler av systemet (NOU 2015, s.46). Her er frykten blant annet at en angriper kan tilegne seg operatør adgang og derav fjernavkoble strømmen (Lillesund 2009). Da samhandling og avhengigheten av ulike komponenter i systemet øker kan cyberangrep og virus i en komponent true hele virksomheter, og gi ringvirkninger på samfunnsskala. I det digitale samfunn må man tenke at "små tuer kan velte store lass" (NVE 2019).

Innen Smart Grids er også såkalte "*in-the-middle*" angrep en trussel. Her vil angriperen injisere seg i kommunikasjonsledd mellom kommuniserende enheter uten å bli oppdaget. Deretter kan inntrengeren av økonomiske grunner manipulere strømmåledata, eller sabotere systemet ved å styre skillebrytere, stanse drift, eller ødelegge distribusjonsutstyr (Pettersen 2015, s.22). Innen Smart Grid systemer kan ofte kommunikasjonsveier mellom enheter være lange og befinne seg i områder med manglende fysiske barrierer, som trådløse koblinger og fiberforbindelser, som er sårbare for inntrengelse uten fysisk tilkobling. Noe som øker sårbarheten for slike type angrep (ibid).

5.1.4 Oppsummering

Det må belyses at Smart Grid teknologi kan også drastisk forbedre sikkerheten i energisektoren på flere måter. Systemet tillater operatører å bruke en mer proaktiv tilnærming da systemet blir overvåket. Fjernstyring åpner også for å isolere kompromitterte komponenter og enheter for å unngå kaskadeeffekter. Smart Grids er også automatisert til den grad at det kan detektere, analysere og respondere på forstyrrelser uten menneskelig interaksjon (Westlund 2007). Cyberrisiko blir trukket fram særlig da tradisjonelle IKT trusler og cyberangrep er relativt nye for energisektoren.

Basert på empiri har den digitale utviklingen hatt betydningsfull innflytelse på trusselbildet innenfor energisektoren. Det kan oppsummeres gjennom følgende hovedtrekk:

- Omfattende digitalisering er nødvendig for å drifte fremtidens smarte nett. Men flere komponenter øker system kompleksitet, skaper uoversiktlige verdikjeder og utvider angrepsflaten.
- Økt digitalisering knytter sammen samfunnet og cybersikkerhet blir utfordrende på virksomhets-, myndighets-, teknologisk-, og generelt på samfunnsnivå.
- Cyberangrep viser til at innebygd sikkerhet ikke alltid er tilstrekkelig. Tradisjonelle sikringsmekanismer benyttet i sektoren kan omgåes av ondsinnede aktører.
- Samtlige sikkerhetsmyndigheter uttrykker bekymringer, og kartlegging av cybersikkerhets-hendelser viser at mange norkse kraftselskap har opplevd tilsiktede angrep mot sine systemer.
- Ulike aktører og leverandører vektlegger sikkerhet forskjellig og kan skape mulige svakheter i verdikjeden.
- Cyberangrep blir enklere å utføre, vanskeligere å spore, og et tilsynelatende "friskt" system kan allerede være smittet.
- Norsk energisektor har så langt ikke opplevd hendelser med store konsekvenser, men cyberrisiko er preget av stor usikkerhet.

5.2 Smart Grids og Media

5.2.1 Mediebildet

Omtrent i 2010 kommer begrepet "Smart Grid" mer frem i det norske mediebildet, men fokuset ligger hovedsakelig på visjonen, planer og investering (Fredriksstad blad 2010; Bergens tidende 2010; Gram 2010; Sørlie 2010; Sprenger 2010).

Man kan på godt grunnlag anta at den generelle befolkningen er oppmerksomme på at digitale angrep er et fenomen. De fleste tabloider dekker omfattende cyberangrep. *Stuxnet* i

Iran 2010, Yahoo i 2013, strømutfall i Ukraina 2015, Netflix, Spotify, Twitter og Amazon i 2016, Wannacry 2017, Helse Sør-øst 2018, og Hydro i 2019 (E-tjenesten 2020, s.78).

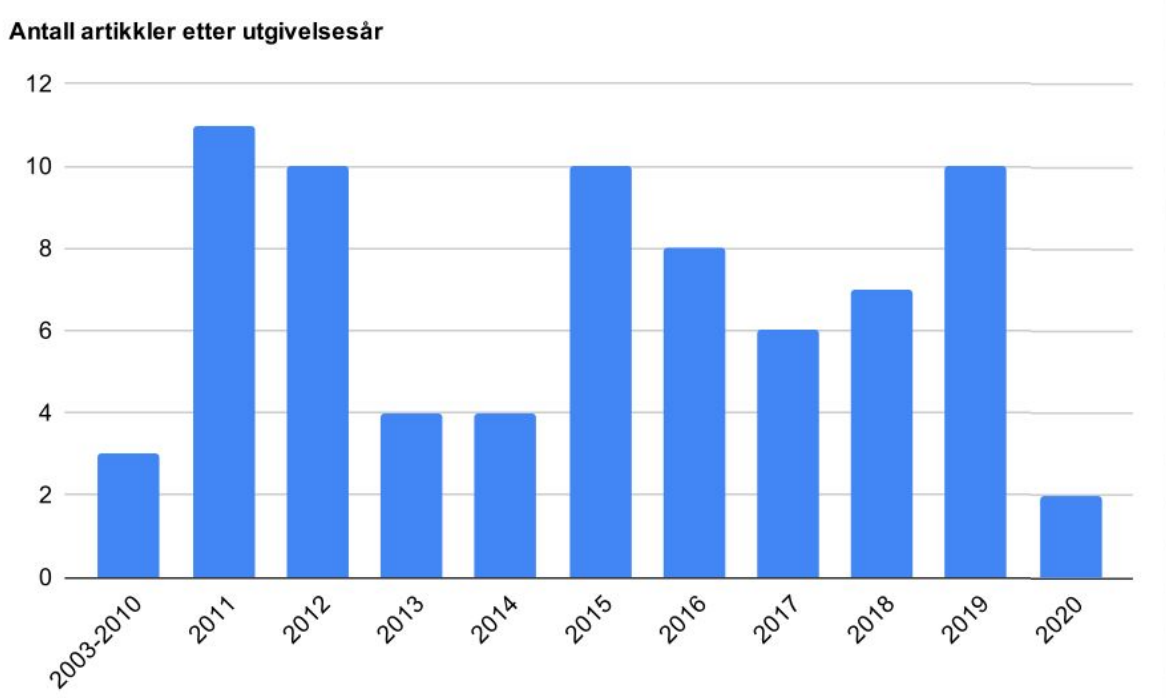
Men om det belyses tilstrekkelig at energisektoren og kritisk infrastruktur er utsatt for cyberangrep er mer utfordrende å anta. Blant annet viser NVE rapporten at til tross for flere angrepsforsøk i norsk energisektor førte kun 2% av registrerte hendelser til mediedekning (Azam 2017, s.17).

Da nyhetsmedier er en stor faktor i forming av risikopersepsjoner i form av indirekte kontakt med risikokilder, vil en skildring av mediebildet relatert til Smart Grid teknologi være nyttig for å videre predikere sosiale reaksjoner i møte med cyber hendelser.

Analysen gjennomført består av totalt 75 artikler fra år 2003 til og med 2020. Gjennom innhold- og sentimentanalyser kan 5 sies å være negativ i den form at bekymringer om risiko trekkes utelukkende frem. 53 av artiklene har en mer positiv belysning av tema, og 17 artikler trekker frem både trusler og muligheter (Se vedlegg 1 og 3 for full medieanalyse og sentimentanalyse).

5.2.2 Smart Grid i media fra år til år

I dette prosjektet ble beskrivelser av Smart Grid begrepet og relatert teknologi analysert i 75 artikler fra totalt 33 ulike kilder. Kildene viser at begrepet ble benyttet i nyhetsmedia allerede i 2003 (Farmakis 2003), og i 2009 ble det uttrykt bekymringer for fremtidige sårbarheter. En drastisk økning av informasjon forekommer så to år senere i 2011.



Figur 11: "Smart Grid relaterte artikler utgitt etter år"

Første artikkel er fra tidskriften *Verdens Gang* (VG) i 2003. Artikkelen legger vekt på hvordan Smart Grid teknologien vil skape toveiskommunikasjon mellom produsenter og konsumenter som på sikt vil gi billigere strøm (Farmakis 2003). Computerworld beskriver så i 2009 hvordan fremtidens energisystem kan bli sårbart for hacking (Lillesund 2009). Artikkelen ble også publisert gjennom VG.

2011

Oppsamlede artikler fra den kraftige informasjon økningen i 2011 viser hovedsakelig optimisme. Lokale nyhetsaviser som Trønderavisa, Halden arbeiderblad og Trønderbladet belyser tema gjennom beskrivelser av økt effektivitet, forbrukerfleksibilitet og videre verdiskapelse (Halden arbeiderblad 2011; Kvitnes 2011; Falstad 2011; Trønderbladet 2011). Trønderavisa beskriver også begynnelsen på demoprosjekter i Steinkjer som håper på positive miljøeffekter og mindre nødvendige investeringer i kraft-infrastrukturen (Trønder-avisa 2011).

Antall ganger positive stikkord blir benyttet i 2011	
Smart	47
Lønnsomt	5
Effektiv	14
Intelligent	4
Bedre	14
Fleksibilitet	4
Reduksjon	8

Tabell 3: Antall positive stikkord benyttet i artikler fra 2011

Kilder: Falstad 2011; Halden Arbeiderblad 2011; Kvitnes 2011; Ystrøm 2011; Trønder-avisa 2011; Kirknes 2011; Nilsen 2011; Trønderbladet 2011; Valmot 2011a; Valmot 2011b; Lie 2011

Ordbruket fra artikler i 2011 viser at Smart Grid teknologi blir hovedsakelig belyst gjennom sine egenskaper som et mer intelligent, fleksibelt og effektivt system som vil være lønnsomt for samfunnet på sikt.

Den teknologisk fokuserte tidskriften Teknisk Ukeblad viser også hovedsakelig optimisme i 2011. I likhet med lokalavisene beskrives Smart teknologi i strømnettet som beste mulighet til forbedret stabilitet i fremtidens nett, lavere strømpriser for sluttbrukere grunnet AMS og IoT teknologi, og økt driftssikkerhet (Valmot 2011a; Valmot 2011b; Lie 2011).
Det uttrykkes også enkelte bekymringer dette året. Tidskriften Computerworld beskriver tverrsektorielt arbeid mellom IT og energi og påpeker nye utfordringer fusjonen vil medføre både på virksomhet- og systemnivå (Kirknes 2011).

2012

2012 viser et lignende mediebildet som året før. Lokalavisene Halden arbeiderblad og Bergens tidende beskriver hvordan smartere strømnett vil gi store gevinster for sluttbruker da det åpner for større grad av egenregulering, samt hvordan inkorporering av Smart-teknologi i strømnettet minsker nødvendigheter for utbygging av infrastruktur (Øyehaug 2012; Mordt 2012).

Videre beskriver de tematiserte tidsskriftene Arkitektur N og E24 hvordan Smart Grids støtter en bærekraftig byutvikling og hvordan distributører kan tilby mer tjenester basert på data fra ams. Store muligheter for økonomisk gevinst (Mogensen & Brattli 2012; Midtsæther 2012).

Igjen påpekes enkelte bekymringer gjennom blant annet Teknisk Ukeblad som beskriver scenario der kraftnettet kan bli utsatt for cyberangrep som følge av ams målere. Artikkelen viser til større bekymringer enn tidligere sett gjennom språkbruk. Ordet *hacking* og *angrep* blir registrert 9 ganger, *sabotasje* og *kompleksitet* 2, og *katastrofe* blir nevnt. Samtidig vises det til at sannsynligheten for et vellykket angrep ikke blir ansett som stor, og nettets effektivisering som følge av teknologiutviklingen er nødvendig (Hamnes 2012).

2013 og 2014

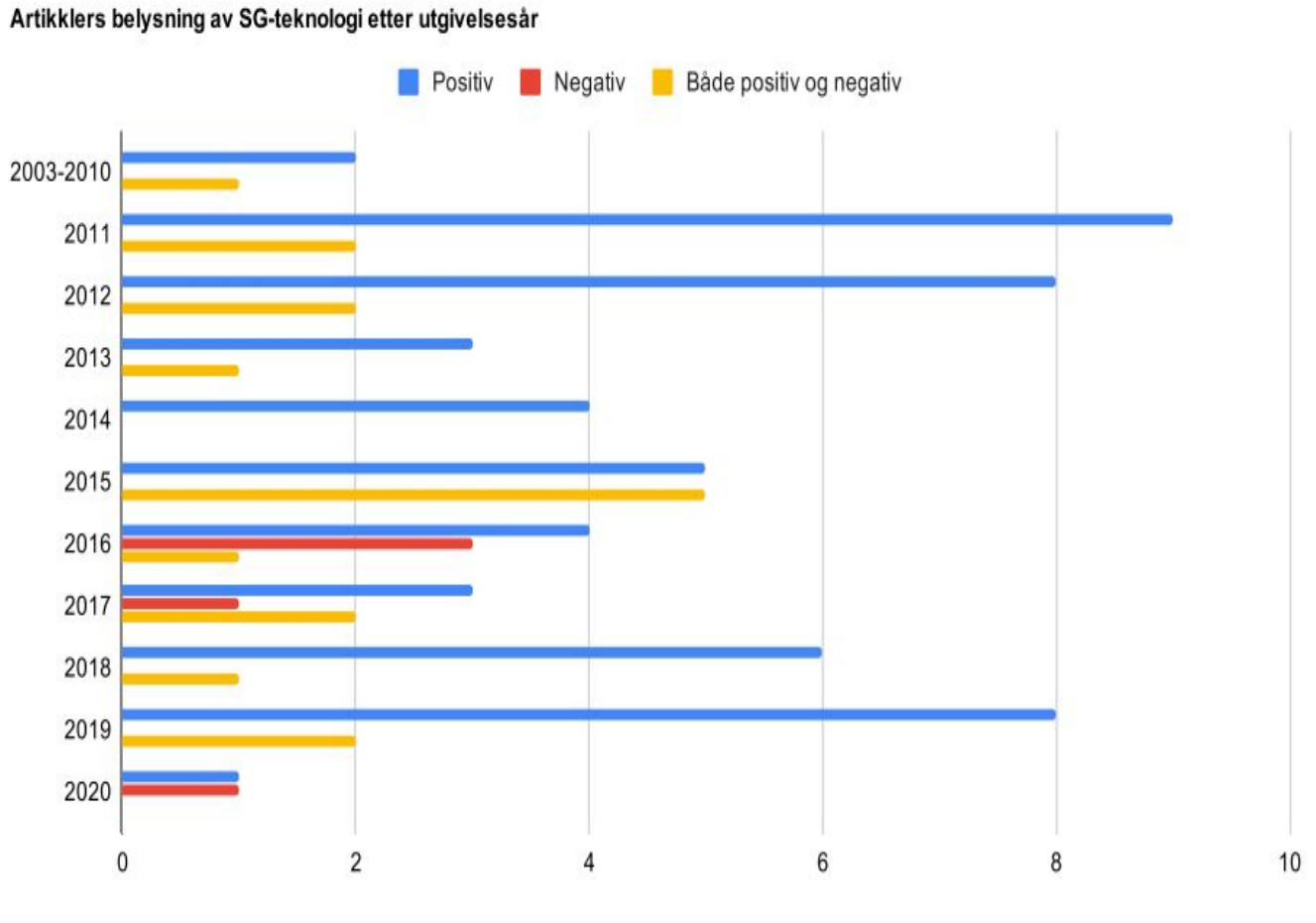
Videre viser funn at informasjonen rundt Smart Grids blir mindre omtalt i media årene 2013 og 2014. Artiklene hentet viser igjen til en optimistisk belysning av tema. VG beskriver teknologien som nødvendig for økt anvendelse av småkraft i energisektoren (Dyb 2013), og E24 påpeker AMS som et fundament for smart-revolusjonen (Valmot 2013).
Ulike lokalaviser påpeker hvordan teknologien gir bedre nettdrift, øker driftssikkerhet, og legger til rette for sluttbrukere (Avner & Tønnessen 2014; Karlsen 2014; Halden arbeiderblad 2014; Romsdal budstikke 2014).
Teknisk ukeblad betoner igjen begge sider av saken ved å påpeke investeringskostnader og umoden teknologi (Sprenger 2013).

Utvikling fra 2015

Mediebildet viser hovedsakelig positiv belysning fra 2003 til og med 2014. Spesielt de allmenne nyhetskilder som dekker et bredt omfang av saker viser mer optimistiske beskrivelser. Bekymringer i mer allmenn media uttrykkes ikke betydelig før 2015 og 2016 (Nystrøm 2015; Lohne et al. 2016; Johansen 2016). Da det trekkes frem at cyberrisiko er en økende fare for energisektoren ved videre teknologiutvikling.

Figuren nedenfor viser hyppigere artikler som er både positiv og negativ, og rent negative, spesielt fra 2015. Særlig rent negativ vekting øker fra år 2016.

Bekymring for økende cyber-risiko i energisektoren har blitt påpekt tidligere enn 2015, men hovedsakelig i tematiserte tidsskrifter slik som *Teknisk Ukeblad, Volt* og *Computerworld*. Før 2015 var beskrivelser av Smart Grid teknologi som påpekte sårbarheter i systemet, også mer fokusert på nødvendigheten av utviklingen. Figur 12 viser artikler belysning av Smart Grid teknologi år for år.



Figur 12: "Positiv og negativ vekting av Smart Grid relaterte artikler, 2003-2020"

Datautvalget viser til to trender. For det første er 60% av alle analyserte artikler som vektes *rent negativt* fra 2016. Og for det andre omtales bekymringer i økende grad fra allmenne nyhetskilder.

2015 viser en jevn fordeling av positiv, og både positive og negative beskrivelser av Smart Grid teknologi. Positive beskrivelser blir kommunisert spesielt via lokalaviser og næringslivs baserte tidsskrifter. I likhet med tidligere år beskrives nødvendigheten av innovasjon i energisektoren for å støtte fremtidens nettdrift og stabilitet, hvordan større datamengder gir

videre verdiutvikling. Og hvordan Smart-teknologien fungerer som et "springbrett" ikke bare mot smarte nettverk, men smarte byer og regioner (Myhre 2015; Braaten 2015; Yndestad 2015).

Fagskriftene Volt og ITB aktuelt skildrer hvordan angrepsforsøk på norsk infrastruktur øker, hvordan smart teknologi skaper sårbarheter innen de fleste sektorer. Samt hvordan markedet fører til utfordringer innen regulering og implementering (ITB aktuelt 2015; Pettersen 2015; Nystrøm 2015; Volt 2015).

Overveldende negative beskrivelser trekkes frem i hele mediebildet i 2016, i etterkant av de omfattende konsekvensene av cyberangrepet på Ukrainas energisektor.
Hendelsen viser til at media i større grad får cyberrisiko innen energisektoren på dagsorden. I 2013 og 2014 er beskrivelsene av teknologien overveldende positiv, med unntak av noe usikkerhet rundt utrullingen av AMS (Sprenger 2013). I 2016 blir bekymringer, spesielt med tanke på ondsinnede angrep, mer tydelig uttrykt.

Antall ganger stikkordene *Hacking, Angrep* og *Cyber- trusler* og *sårbarheter* blir registrert i 2016	
Hacking	19
Angrep	31
Cyber- trussel/sårbarhet	14

Tabell 4: Stikkord relatert til cyberangrep registrert i 2016

Kilder: Flå 2016; Volt 2016; Braathen 2016; Aura avis 2016; Yndestad 2016; Johansen 2016; Brunmark 2016; Lohne et al. 2016

I Januar trekkes denne hendelsen frem i Aftenposten, med ytterligere beskrivelser om hvordan Norge er sårbar for en lignende hendelse. ABC nyheter beskriver i juni en øvelse utført av Nkom som avslørte sårbarheter innen cyberdomenet i norsk Ekom og energisektor. Videre belyser VG ekspertvurderinger med vekt på hvordan Smart teknologi skaper kompleksitet i digitale verdikjeder som gir en økt angrepsflate (Lohne et al. 2016; Brunmark 2016; Johansen 2016).

2017-2020

Etter 2016 fortsetter en del blandet belysning av Smart Grid risiko. I januar 2017 beskriver NRK hvordan økende cyberkriminalitet er en økende bekymring for nasjonen med over 22.000 dataangrep mot norske bedrifter og etater. Det legges vekt på at hver enkelt datamaskin blir del av et større nettverk med betydning for sikkerhet, og hvordan kompromittering av systemer innen strøm og tele er en større bekymring (Hotvedt & Saugstad 2017). Tematiserte tidskrifter uttrykker også bekymringer for sårbarheter i strømnettet, men påpeker også hvordan sektorer jobber på lag mot en nødvendig utvikling (Frøystad 2017; Grøtan 2017; Nickelsen 2017).

Belysning av cyberrisiko i mediebildet dempes tilsynelatende årene 2018 og 2019. Fokus på Smart teknologi sitt potensialet til forbedring og effektivisering blir igjen mer fremtredende i mediebildet.

Positive og negative stikkord fra artikler 2018 og 2019	
Bedre	17
Effektiv	8
Forsyningssikkerhet	7
Hacking og Angrep	8
Trussel og Sårbarhet	3

Tabell 5: Stikkordsøk i artikler 2018 og 2019

Kilder: Hovland 2019a-d; Hovland 2018; Gustaffson 2019; Michalsen 2019; Jordheim 2018; Lorentzen 2018; E24 2018; VG 2018; Jystad 2019; Laberg 2019; Høeg & Belgaux 2019; Brøndbo 2019; Bersvendsen 2018; NTB 2018

Mer bredt dekkende nyhetsmedier som Adressavisen og VG beskriver i 2018 hvor Smart utviklingen og IoT teknologi er på vei, og hvordan det er en viktig prioritet for nasjonen (Bersvendsen 2018; VG 2018).

Tematiske tidsskrifter, spesielt økonomisk fokuserte, som E24 viser også en stor optimisme i 2018 og 2019 der bærekraftig systemutvikling, ny IoT teknologi og innføring av AMS vil lede til bedre og billigere strøm for kunder over tid (Hovland 2019a; Lorentzen 2018; Hovland 2019b; Hovland 2019c; Hovland 2019d).

Mer teknologisk fokuserte nyhetsmedier fortsetter derimot en mer nyansert belysning ved å trekke frem de potensielle sårbarhetene utviklingen medfører (Høeg & Belgaux 2019; Gustaffson 2019).

I 2020 er datamaterialet for magert til å si noe om trender i mediebildet, men av utvalgte kilder stammer begge fra lokalaviser der *Adressavisen* legger beskriver PSTs årlige trusselrapport med bekymringer for hacking av Smart teknologi. Og *Moss avis* beskriver positive aspekter som bærekraft, økonomisk for sluttkunder (Adressavien 2020; Buraas 2020).

5.2.3 Tematiserte medier

Nyhetsmedier støtter seg ofte på fageksperter. Saker som omhandler kultur, politikk, teknologi eller næringsliv er ofte omfattende og dersom medier ønsker å gi dypere beskrivelser søkes ekspertise fra ulike sektorer. Ulikheter i medias belysning av Smart Grid teknologi kan derfor tenkes i stor grad å være påvirket av fagfeltet ekspertisen er hentet fra, samt hvilke tema tidskriften begrenses til. Med andre ord vil som regel teknologiske tidsskrifter benytte tekniske eksperter i sin skildringer, beskrivelser av norsk næringsliv benytter økonomer, og lignende.
Det kan forårsake ulikheter i tidsskriftets belysning av det samme tema, og derav kan det antas at allmennheten vil ha ulike risikopersepsjoner avhengig av hvilke mediekilder de får informasjon fra.

De 75 artiklene innhentet for medieanalyse stammer fra 33 ulike tidsskrifter. Av disse var 12 *tematiserte medier,* kilder som begrenser sitt omfang av nyhetsdekning. Blant disse kan igjen 8 skilles ved å ha enten et teknologisk eller økonomisk fokus.

Teknologisk fokusert	Økonomisk fokusert
Teknisk Ukeblad	Byggfakta
ITB aktuelt	Finansavisen
Computerworld	E24
Volt	Dine penger: forbruker

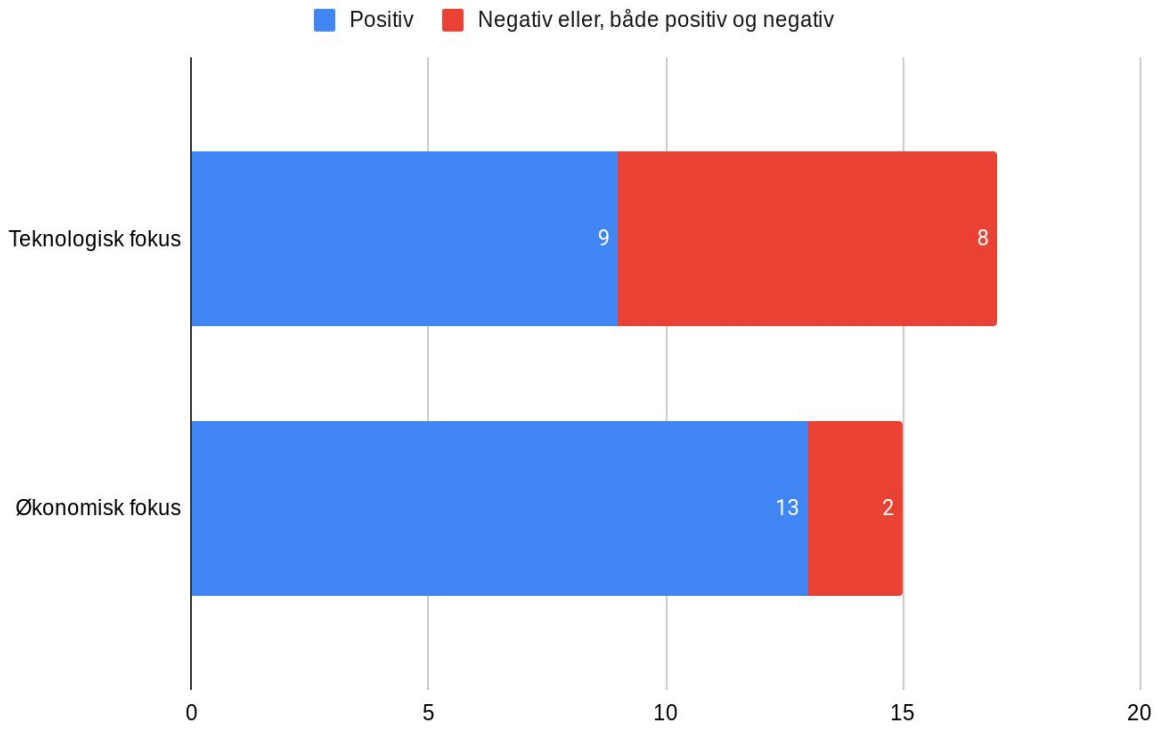
Tabell 6. Skille mellom teknisk- og økonomisk-fokuserte mediekilder.

De fire utelatte tematiserte kildene omfatter *Forskning*, *Arkitektur N*, *Addsecure* og *Infosec* (sintef). *Forskning* dekker et bredt spekter av hendelser innen vitenskap og kan derav sies å være tematisert, men ikke videre begrenset. *Arkitektur N* publiserer artikler relatert til arkitektur, landskap og interiør, men har liten relevans som kilde sett bort fra artikkelen analysert. *Addsecure* og *Infosec* publiserer innlegg som er av relevans for sikkerhet og Smart Grid, og bidrar derfor i nyhetsbilde, men de er ikke utelukkende en mediekilde.

Teknisk ukeblad publiserer artikler spesifikt innen teknologi, energi og industri. *ITB aktuelt* har fokus på integrerte tekniske bygginstallasjoner. *Volt* (Voltmag) dekker nyheter relatert til kraftproduksjon, transmisjon og distribusjon, elektroteknikk og automatisering. Videre er *Computerworld* norges ledende kilde til IT-nyheter.

De økonomisk fokuserte kildene tar for seg norsk næringsliv, privatøkonomi, børsen og spesifikt bygg- og anleggsnæring.

Til sammen omfatter disse kildene 32 artikler, hvorav 15 er fra økonomisk fokuserte kilder, og 17 fra teknologiske.



Figur 13: Ulikheter i teknologisk- og økonomisk belysning av Smart Grid teknologi.

Av de 17 artiklene fra teknologisk fokuserte nyhetskilder belyses 9 som *positiv,* mens 8 inneholder beskrivelser som gir artikkelen *negativ*, eller *både positiv og negativ* skildring av Smart Grid teknologi. Av de økonomisk fokuserte viser derimot 13 artikler til *positive* beskrivelser, og 2 som *negative,* eller både og.

Dette viser et skille da økonomisk fokuserte kilder beskriver Smart Grid teknologi positivt i 87% av de analyserte artiklene, i motsetning til teknologisk fokuserte kilder som presenterer teknologien rent positivt i 53% av artiklene.

Derav kan det antas at det er betydelige forskjeller i allmennhetens risikopersepsjon relatert til Smart Grid teknologi avhengig av hvilke kilder man tilegner seg informasjon fra.

5.2.4 Oppsummering

Medie- og sentimentanalyse viser til en mediebildet der Smart Grid teknologi ikke kommer tydelig frem, spesielt tilhørende trusler og sårbarheter. Av 75 artikler stammer 36 fra

tematiserte tidsskrifter som kan antas å ikke ha samme rekkevidde, eller publikum. 32 av disse stammer igjen fra kilder med enten et økonomisk eller teknologisk fokus, som har betydning for hvordan Smart Grids skildres. De allmenne lokal- og riksdekkende medier tar for seg Smart teknologi i 44 artikler fra 2003 til 2020.

Mediers belysning av artikler		
Positiv	Negativ	Både positiv og negativ
53	5	17

Tabell 7: Mediers belysning av artikler

Av de 75 analyserte artiklene var 53 optimistiske i sine skildringer av Smart Grid innovasjonen, 17 artikler inneholdt mer nyanserte beskrivelser. Og 5 artikler påpeker kun bekymringer.

Hovedpunktene fra utførte analyser kan oppsummeres i følgende punkter:

- Nyhetsmedier viser oppmerksomhet rundt potensielle sårbarheter allerede i 2009, men slike aspekter får ikke stor oppmerksomhet før 2015 og 2016.
- Før 2015 var bekymringer hovedsakelig uttrykt i tematiske medier, spesielt de teknologiske.
- Etter cyberangrepet i Ukraina, desember 2015, observeres en drastisk økning rent negative skildringer. Flere allmenne nyhetskilder beskriver trusler og sårbarheter assosiert med Smart Grid systemer.
- I 2018 og 2019 dempes risikobeskrivelser i mediebildet og Smart Grids nødvendighet for samfunnet blir igjen fokus.
- Et betydelig skille av risiko-beskrivelser eksisterer mellom tematiserte medier der økonomiske nyhetsmedier tenderer å skildre teknologiutviklingen i et mer positivt lys enn de teknologisk fokuserte.

6. Drøfting

I dette kapittelet vil data presentert i kapittel 5 drøftes i lys av det teoretiske rammeverket og tidligere forskning. Strukturen i kapittelet vil følge forskningsspørsmålene. Da drøftingen vil lede opp til svaret på prosjektets problemstilling som presenteres i konklusjonen, kapittel 7, nemlig *hvordan kan medias risikokommunikasjon angående cybertrusler i Smart Grids påvirke risiko?*

6.1 *Hvilke følger har digitalisering av energisektoren for trusselbildet?*

Digitaliseringen av kraftnettet vil neppe stoppe opp. Effekten av Smart teknologi og verdiutviklingen det medfører er av enorm gunstig samfunnsmessig og økonomisk effekt. Videre er intelligente strømnett en global satsing og visjon (Smartgrids 2016; Lund 2014; Litos Strategic Communication u.å), som medfører et press til å henge med, og ikke bli etterlatt i en utdatert digital verden. Effektene fra Smart Grid systemer vil også bidra til å nå felles mål om en grønnere verden satt av EU. Billigere og ren energi, bærekraftig infrastruktur og industri, bærekraftige byer, ansvarlig forbruk og produksjon, klimakontroll, og bevarelse av økosystemer er Eus bærekraft mål som denne utviklingen vil ha direkte innflytelse på (United nations u.å). Men denne utviklingen må støttes opp av andre drivere enn teknologi. "Smart" teknologi må følges av tilsvarende smarte sikkerhetstiltak for å virkeliggjøre og vedlikeholde fremtidens systemer.

Beskrivelser fra myndigheter, spesielt NSM og NVE, viser til et trusselbilde i dynamisk utvikling. NSM beskriver en omfattende og usikker risikoprofil i det digitale landskap der økt omfang av komponenter, enheter og systemer sammenknyttes i et enormt kommunikasjonssystem. Digitale relasjoner blir tettere både innad i ulike sektorer og tverrsektorielt på ulike nivå, som omfatter private og offentlige funksjoner. Dette får følger både for individer og virksomheter, samfunnet og til og med globalt.
Med andre ord blir internett et helt nytt domene der angrepsflaten er stor og oversikt over sårbarheter er utfordrende å kartlegge.

Myndigheter beskriver hvordan disse sårbarhetene vil være en utfordring for hele samfunnet, også for drivere av kritisk infrastruktur (NSM 2019; NSM 2020; NOU 2015; PST 2020). Da tradisjonelle IKT-trusler i større grad blir en bekymring for energisektoren gjennom utviklingen av Smart Grids øker cyberrisiko. Tilsiktede digitale angrep er en økende trend (NSM 2019, s.10), samtidig som de blir enklere å utføre og vanskeligere å spore. Samtidig viser innsamlet data at denne cyber risikoen allerede har hatt konsekvenser for energisektoren, og spesielt angrepet i Ukraina illustrerer større konsekvenser slike hendelser kan ha for samfunnet.
Til slutt viser empirien at innebygde sikkerhetstiltak ikke alltid holder følge med angrep metodikkens utvikling. Systemer har blitt kompromittert selv med tilstrekkelig isolering (airgaps) (NSM 2018; Frøystad 2017). Det vises til bekymringer for at avhengigheten av nettverk teknologi har økt raskere enn mekanismer til å tilstrekkelig sikre det (Khurana & Lu 2010; Line et al. 2011).

Systembeskrivelser og følgende risikoprofil viser til energisektoren som en potensielt farlig teknologi (Engen et al .2016, s.139). Som påpekt er energisektoren vital for samfunnets verdier, og potensielle utfall av et omfattende cyberangrep vil ikke begrenses til energisektoren, men påvirke samfunnets som helhet og få direkte konsekvenser for andre-grads offer.

I følge Perrows *Normal Accident Theory* (NAT) viser beskrivelser av NSM og NVE til et system der en ulykke er kun et spørsmål om tid. Høy interaktiv kompleksitet eksisterer tydelig i det digitale domenet da det er utfordrende å kartlegge årsak, virkning og videre potensielle kaskadeeffekter. Kommunikasjon og avhengigheter innad i systemet er ikke lineære, men viser derimot til komplekse sammenhenger og interaksjoner. Avhengigheten mellom samfunnsfunksjonene effektiviserer, men kan også by på sårbarheter som rask kan forplante seg i en uoversiktlig verdikjede (NSM 2020, s.8). Utstrakt bruk av ny Smart-teknologi skaper et overvåkningssamfunn det er utfordrende å kartlegge (Ibid, s.32). Videre vises *tette koblinger* til tidsavhengige prosesser og liten grad av slakk i systemet (Engen et al. 2016, s.145). Energi produseres ikke der den forbrukes, og strømnettets kapasitet må reguleres etter forbruk. Energidistribusjon tillater liten slakk i den form at både private og offentlige sluttbrukere trenger kontinuerlig tilførsel.

I følge Perrow viser denne kombinasjonen av system-karakteristikker til at systemet ikke kan håndteres på ansvarlig vis, og derfor at storskala ulykker er uunngåelige (Rosness et al. 2010, s.49). Det må belyses at det eksisterer teorier som, *Høypålitelige Organisasjoner* (HRO) der det hevdes at slike styringsdilemma kan, og har blitt, unngått (Ibid, s.57; Kongsvik et al. 2018, s.80). Men dette prosjektet poengterer systemske koblinger og kompleksitet i henhold til tilsiktede trusler. Slike trusler bærer et særegent preg av usikkerhet da aspekter som aktør intensjon, kapasitet og vilje blir av betydning.

For å summere har digitalisering av energisektoren ført med seg større grad av kompleksitet og tette koblinger. Trusselbildet har derav blitt mer omfattende. Cybertrusler som preger energisektoren i dag er preget av kompleksitet og usikkerhet. Noe som igjen gjør risikokommunikasjon til en utfordring (Renn 2008).

6.2 Hvordan blir Cyberrisiko relatert til Smart Grid teknologi belyst i mediebildet?

Sammenhengen mellom sosiale reaksjoner, persepsjoner og tidligere risikokommunikasjon er betydelig. Noe som viser til mediers store ansvar i å portrettere et informerende risikobilde, spesielt risiko som mennesker opplever gjennom indirekte kontakt.

Mediebildet

Av 1080 telte nøkkelord i 75 artikler ble 753 positive, og 327 negative ord registrert i relevant kontekst. Dette gav videre en inndeling av 53 positive, 5 negative, og 17 både positive og negative belyste artikler. Denne kategoriseringen viser til et mediebildet med følgende hovedtrekk:

- Nyhetsmedier beskriver egenskaper og fordeler ved teknologien allerede i 2003, før selve *Smart Grid* begrepet blir introdusert (Farmakis 2003; Yacout 2013, s.2)
- Potensielle sårbarheter som utviklingen medfører blir ikke betydelig uttrykt før 2015, og spesielt 2016.

- Etter angrepet i Ukraina øker negative beskrivelser i allmenne nyhetsmedier.
- Mer positive beskrivelser blir igjen mer sentrale i årene 2018 og 2019
- Tematiserte, spesielt teknologisk fokuserte tidsskrifter skildrer teknologien mer nyansert.

Mediebildet viser hovedsakelig til positiv belysning av Smart Grid-teknologi da omtrent 70% av artikler ikke skildret bekymringer. Videre viser omtrent 23% til både positive og negative beskrivelser. Det kan derfor antas at allmennheten har en hovedsakelig positiv holdning til teknologiutviklingen. Oppmerksomhet rundt potensielle cybertrusler vil antageligvis sterkt avhengige av hvilke mediekilder man benytter, da teknologisk fokuserte kilder tenderer til å skilder teknologien mer nyansert.

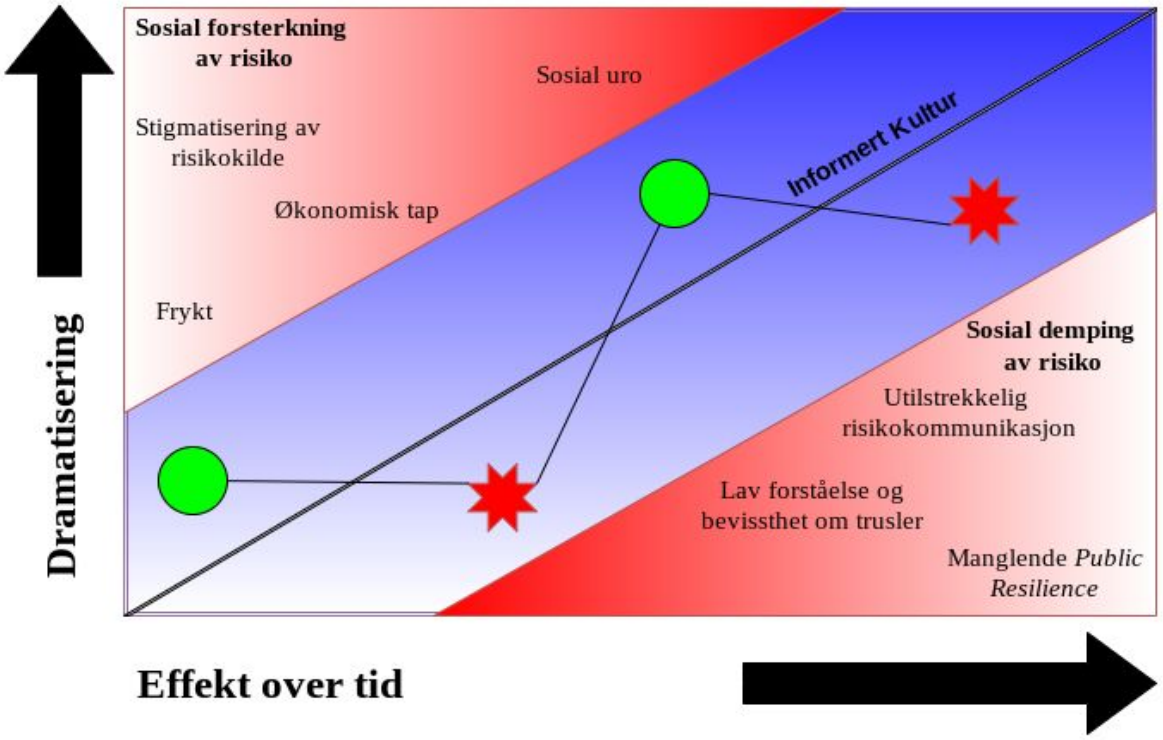
Nyhetsmediers betydning

> *"The relationship between citizens and politicians, between the represented and the representative, depends essentially on what happens in this media-centered communication space … It is in the media space that political battles of all kinds are fought, won, and lost … Media politics works … as an alternative form of sociopolitical presence, using the input of grassroots power"* (Chong 2018, s.1)
>
> -Castells, M. 2004

Nyhetsmediers makt ligger i å forme en virkelighet. De gjenspeiler den ikke, men filtrerer og konstruerer saker for videre formidling til befolkningen. Tidligere forskning viser at oppmerksomheten media gir til risikokilder og hendelser kan forme offentlig persepsjoner i stor grad (Jung & Ha 2016; Frh 2017; Park & Sohn 2013). Medias *Agenda* og *framing* (Parveen et al. 2017) vil derfor ha betydning for individers persepsjoner, noe som igjen knyttes til sosial forsterkelse og demping av risiko. En ujevn balanse i nyhetsrapportering, eller en feil representasjon av risiko kan derfor være av betydning for sekundær- og tertiær effekter av risiko etter den initielle hendelsen.

Medier har her et ansvar for å formidle trusselbildet på en forsvarlig og informerende måte. Reflektere trusler teknologien kan medføre, men unngå beskrivelser som skaper hysteri, sinne

og frykt, da en rekke forskning viser direkte korelasjon mellom mediedekning og risikopersepsjoner (Park & Sohn 2013; Kone & Mullet 1992; Gore et al. 2005). Dersom en risiko blir dempet i mediebildet kan reaksjoner blir forsterket i møte med en hendelse. Da graden av risikoforsterkelse kan være en reaksjon på grad av tidligere risiko demping (Fjæran & Aven 2019), vil nyhetsmediers belysning og kommunisering av Smart- teknologi være av stor betydning i møte med en fremtidig hendelse. Nyhetsmedier bør anses som et kommunikasjonsverktøy. Risikokommunikasjon kan fungere som en *symbolsk sikkerhetsbarriere* (Rosness et al. 2010, s.100), med den hensikt å skape en kollektiv bevissthet rundt cybertruslene.



Figur 14: "Effekter av under- og overrapportering av risikokilder"

Figur 14 viser til effekten risikokommunikasjon kan ha over tid. Dersom cybertrusler relatert til Smart Grids skulle blitt presentert med stort volum og en dramatisk tilnærming, ville dette høyst sannsynlig skapt frykt og stigmatisering av risikokilden. Stor grad av dramatisering ville derfor ført til sosial forsterkning av risiko. Som et resultat kunne Smart Grid teknologi blitt kontroversiell og mangle offentlig aksept, i likhet med teknologier slik som atomkraftverk (Kasperson & Kasperson 1996, s.100).

På den andre siden vil underrapportering av disse cybertruslene føre til en generell uoppmerksomhet og sosial demping av risiko. Derav blir det en "gjemt fare" som i møte med en initierende hendelse kan få betydelige konsekvenser for sosiale reaksjoner (Fjæran & Aven 2019; Kasperson & Kasperson 1996, s.104).

En *informert kultur* refererer her til et publikum og en befolkning med risikopersepsjoner som reflekterer større grad av oppmerksomhet, både rundt verdier og sårbarheter. En slik kultur, og *public resilience* vil antageligvis på best måte formes gjennom en god balansering av over- og underrapportering i mediebildet, det vil si, belysning av både fordeler og ulemper med teknologien.

Persepsjoner bør i større grad formes av en delt informasjonsflate, med tettere kunnskapsgap mellom myndigheter og allmennheten, for best mulig samfunnsmessig beredskap blant samtlige aktører. Dette bør oppnås gjennom en kommunikasjonsflyt der risiko meldinger konstrueres for å treffe en trygg, men oppmerksom sone.

Som påpekt av Kasperson (1988) vil informasjonsflyten innenfor dette rommet preges av en eller flere karakteristikker; volum, tvetydighet, dramatisering og symbolske konnotasjoner. Videre vil tillit til informasjonskilden være av betydning om informasjonen fører til forsterkning eller demping. Dersom det eksisterer høy grad av tillit til de rapporterende og håndteres av risiko, kan en større mengde volum og dramatisering foregå uten å skape hysteri (Urheim 2015, s.16). I Norges åpne demokrati har nordmenn stor tillit til offentlige virksomheter og myndigheter samt de tjenester de tilbyr (NSM 2020, s.8). Det er derfor grunn til å tro at mediebildet kan i større grad kommunisere usikkerhet uten negative sosiale konsekvenser. Som en kommunikasjonskanal bør media betraktes som et verktøy og i større grad benyttes til denne hensikten.

Risiko i mediebildet

Hendelser som får større konsekvenser blir også trukket mer frem i lokalaviser og riksdekkende medier, som vist av negative beskrivelser fra 2016. Dette viser til Ukraina angrepet som en hendelse med stor signal-verdi (Gould & Fjæran 2019, s.4). Slike hendelser

viser til en risiko som tidligere har vært mindre forstått. Når en hendelse gir så omfattende konsekvenser som i Ukraina øker informasjonsbehovet rundt lignende hendelser, og økende risikoperspesjoner følger. Samfunnet blir mer bevisstgjort på at cyberangrep kan ramme energisektoren på meget omfattende måter, og økende kompleksitet samt risikokildens usikkerhet skaper et videre kunnskapsbehov. Som tidligere påpekt var Ukraina situasjonen av unikt omfang. At risikoen forsterkes i mediebildet det neste året kan derfor være som årsak av tidligere demping av cyberrisiko i sektoren (Fjæran & Aven 2019).

Demping av risiko i mediebildet i påfølgende år er vanskeligere å påpeke konkret. En forklaring kan være sosial drift (Gould & Fjæran 2019), der et langvarig fravær fra farer gir økt tillit til de som håndterer risiko. Denne tryggheten man føler, og derfor demping av risiko, kan være et resultat av at Norge har blitt spart fra cyberangrep som har ramifikasjoner på samfunnsnivå.

Videre kan det tenkes at ethvert krise fenomen har et geografisk territorium, som vil føre til høyest grad av engasjement, diskurs og offentlig bekymring blant menneskene dette territoriet omfatter. Derav kan krisens "levetid" antas å minske jo lengre man beveger seg fra området. Da mennesker har en tendens til å *minimalisere* påvirkning fra negative hendelser for å hurtigst mulig returnere til en form for normaltilstand (Dege 2020; Rathus 2006, s.262).

Med andre ord kan Norge være preget av langvarig "trygghet" og derav dempet risiko. Dempet risiko og en følelse av trygghet kan skape en "blindhet" for visse farer og trusler (Engen et al. 2016, s.157), som igjen kan resultere til at dersom et vellykket cyberangrep inntreffer kan effekten av tidligere demping av risiko øke sosial forsterkning (Fjæran & Aven 2019).

Videre kan det tenkes at eksperter har større toleranse for å uttrykke sårbarheter og manglende kunnskap enn media. Da det ikke eksisterer noe alternativ til utviklingen i energisektoren, samfunnet kan ikke være frakoblet, og sårbarhetene som følger vil være uunngåelig. Denne mangelen på valgfrihet kan være en faktor i mediers belysning. Dette virker som en logisk beslutning, men det kan likevel få uforutsette konsekvenser da det

sannsynligvis betyr at allmennheten ikke er oppmerksomme på truslene som eksisterer i den digitale energisektoren.

6.3 Hvilken grad av overensstemmelse eksisterer mellom risikoprofilen beskrevet av sentrale myndigheter og risiko som kommuniseres av media?

Empirien viser til liten grad av overensstemmelse mellom risikoprofilen skildret av myndigheter og belysning fra media. Dette kan da tyde på at befolkningens risikopersepsjoner ikke samstemmer med trusselbildet, og kanskje er de fleste ikke klar over til hvilken grad energisektoren er sårbar for cyberangrep.

Sosial forsterkning av risiko

Dette studiet poengterer at dersom allmennheten ikke er klar over at cyberangrep i sektoren kan forekomme vil sosiale reaksjoner bli sterkere enn om befolkningen var bevisst. Det relateres til *Public Resilience*, og psykologiske fenomener som *Emotional Cushioning*. Dersom en risiko som kan ha enorme konsekvenser for samfunnet ikke har blitt tilstrekkelig kommunisert, og derfor ikke gjort bevisst, kan det tenkes at befolkningen ikke har forberedt seg mentalt på mulige konsekvenser.

I scenarioet *vellykket cyberangrep mot norsk energisektor* kan bølge-effektene antas å bli betydelige da risikoprofilen ikke blir helhetlig belyst i mediebildet utenom i respons til en ekstraordinær hendelse. Det er sannsynlig, basert på medieanalyse, at den generelle befolkningen som får sin informasjon fra allmenne nyhetskilder, ikke er oppmerksomme på cybertruslen og hvordan den kan påvirke dem direkte. Belyst av SARF rammeverket vil den initierende risiko hendelsen være et vellykket cyberangrep som får store konsekvenser. Siden allmennheten lærer om risiko og hendelser gjennom informasjonssystemer, særlig risiko man ikke har personlig erfaring med, blir media en kritisk aktør. Volumet av informasjon og dens grad av dramatisering vil ha stor innflytelse på risikopersepsjoner, og derfor om risikoen blir dempet eller forsterket (Kasperson & Kasperson 1996, s.98). Graden av demping eller forsterking vil igjen påvirke omfanget av bølge-effektene. Dersom risikoen forsterkes, som er

det mest tenkelige scenarioet, kan dette føre til sekundær effekter som langvarige negative persepsjoner, negative følger for økonomi, politisk og sosialt press, sosial uro eller konflikt, omfattende regulatoriske endringer, og følger for annen teknologi utvikling (Ibid, s.99). En ekstraordinær hendelse i energisektoren kan derav tenkes å få betydelige følger for offentlig aksept av Smart Grids og annen Smart-teknologi. Store endringer i regelverk kan forekomme som resultat av politisk press, noe som kan holdte eller bremse utviklingen. Og det kan få omfattende økonomiske følger da investeringer i sektoren minskes.

I forhold til mediebildet analysert kan dette betraktes som et sannsynlig utfall av en initierende hendelse da risikoen virker å ha blitt dempet over tid. Og som påpekt av Fjæran og Aven (2019) kan grad av forsterkning være direkte påvirket av langvaring demping før risikohendelsen.

Disse sekundær-effektene blir videre oppfattet av sosiale grupper og individer slik at risikoprofilen forsterkes og produserer tertiær-effekter, derav *bølge,* eller *Ripple* effekten (Kasperson et al. 1988, s.182). I forhold til Smart Grid teknologi kan et hackerangrep eksponere sårbarheter befolkningen ikke tidligere var klar over, sekundær-effektene fører til stigmatisering av teknologien som videre kan spre seg til andre samfunn og fremtidige generasjoner. Slik kan Smart Grid teknologi bli et sentralt og kontroversielt tema for energiproduksjon og distribusjon i likhet med atomkraftverk. For å begrense slike effekter argumenterer dette prosjektet derfor at risikoprofilen bør være mer nyansert i mediebildet slik at allmennheten er klare over risikoen assosiert med slike teknologier.

Risikokommunikasjon har som formål å opplyse, oppfordre tilpasning av atferd, skape tillit til myndigheter, og gjøre kommunikasjonsprosessen mer inklusiv (Renn 2008, s.203). Gjennom disse egenskapene blir samfunnet i helhet mindre sårbart. En opplyst befolkning er motstandsdyktig, vellykket risikokommunikasjon skaper *Public resilience* (Urheim 2015, s.18).

Myndigheter kan ikke predikere alle mulige ekstraordinære situasjoner som kan ramme systemet. Derfor vil en beredskapsplan aldri være fullt dekkende. Ved å skape resiliens blant befolkningen og skape transparens og involvering i risikobildet vil et bredere spekter av

hendelser kunne håndteres på en bedre måte. Poenget er ikke at ethvert individ kan utøve store forskjeller for cybersikkerhet i det private, men derimot å skape en samfunnsmessig *indre tale,* nemlig å bevisstgjøre allmennheten slik at sosiale bølge-effekter av risiko kan mitigeres.

Videre kan det tenkes, grunnet det digitale landskaps kompleksitet, at flere samfunnsmedlemmer som har en viktig samfunnsrolle og en betydning for den helhetlige digitale sikkerheten, likevel ikke er klar over sårbarheter i andre sektorer enn de de jobber innenfor. Med andre ord, de gjensidige avhengighetene som eksisterer i det digitale domenet. Sikkerhet blir i større grad et linjeansvar, som påvist kan mindre delsystemer benyttes for digital inntrengelse til større systemer (Skotnes 2017, NSM 2020).

De foretatte analysene sett gjennom SARF kan tyde på en problematikk. Ifølge Kasperson et al. (1988) starter rammeverket med en initierende hendelse. Signalene denne hendelsen genererer vil så formidles gjennom en rekke prosesser som informasjonskilder og kanaler, sosiale- og individuelle stasjoner, samt institusjonelle og mindre grupperinger. Før signalene ender opp med å få visse konsekvenser som vil ha bølgeeffekter utover den rammede sektoren. Et cyberangrep i energisektoren kan få direkte konsekvenser for strømproduksjon og distribusjon. Videre kan dette skape bølge-effekter og derav få konsekvenser for lokalsamfunnet, industrien, interessenter, teknologiutvikling, og til og med storsamfunnet. Effektens resonans vil kunne minskes dersom hendelsen signaler ble prosessert gjennom riktige kanaler og stasjoner, på en god måte. Dette studiet hevder at nyhetsmedier ikke har blitt brukt tilstrekkelig som et kommunikasjonsverktøy, og derfor at en hendelse i norsk energisektor vil ha potensielt store bølge-effekter.

Det kan derfor foreslås en alternativ kommunikasjonsmetode i media, som vil fremme flere aspekter ved risikoprofilen på en bedre måte, og derav skape større grad av resiliens blant befolkningen.

Hvordan kommunisere det man ikke vet?

Det er ingen fasit på hvordan media bør kommunisere risikoprofilen, men det må påpekes noen hensyn ut i fra risikoens egenskaper og påvirkning på risikopersepsjoner.

For det første kan man gå ut i fra at risikoen vil oppleves som høy for de fleste. Da risikoen er påtvunget, effektene av en hendelse vil sannsynligvis være umiddelbare og inntreffe mange samtidig, og det er en relativt "ny" risiko med potensialet til å ramme omtrent alle samfunnsfunksjoner. Videre vil befolkningen oppleve liten egenkontroll av faren, og kunnskap om potensielle angrep og utfall er preget av usikkerhet (Kongsvik et al. 2018, s. 34).

For det andre viser beskrivelser til en usikker og kompleks risiko. Kompleks i den forstand at det er utfordrende å få oversikt over potensielle konsekvensers utfall. Og preget av usikkerhet da det er vanskelig å forutsi om en tilsiktet hendelse vil inntreffe (Bruvold 2017, s.27; Renn 2008). Det kan derfor tyde på at aktør samarbeid og informasjon bør inneholde ikke bare berørte interessenter, eksperter og ansatte, men også allmennheten. Risikoen kan tilnærmes med en *deltakende* diskurstype der formålet er å avsløre, diskutere og løse uenigheter innen risikovurdering og håndtering (Engen et al. 2016, s.129).

Implementering av sikkerhetstiltak er hovedsakelig forbeholdt eksperter og myndigheter, men som beskrevet omhandler problemstillingen å kommunisere en kompleks, usikker og delvis normativ tvetydig risikoprofil. Utfordringen blir da å kommunisere en risiko på en rettskaffen og informerende måte, uten å skape hysteri. Da risikoen omhandler ondsinnede aktører er usikkerheten stor, og i det er kan være vanskelig å balansere mellom forsterkning og demping av risiko i media. Omfattende rapportering om sårbarheter og konsekvenser av hacking i energisektoren kan resultere i redusert tillit til myndigheter og aktører som håndterer risiko, mens demping av risiko kan føre til en sosial drift og mindre oppmerksomhet rundt risikoen, som igjen kan føre til sterkere reaksjoner i møte med en hendelse i sektoren (Fjæran & Aven 2019; Gould & Fjæran 2019). Media har derfor et ansvar i å "lukke gapet" mellom ekspertkunnskap og befolkningen.

En utfordring ved å kommunisere risiko relatert til tilsiktede angrep er at når all informasjon er tilgjengelig, har angrepet allerede skjedd, eller allerede blitt avverget. Risikokommunikasjonen handler derfor hovedsaklig om opplysning fremfor adferdsendring blant befolkningen. Graden av følt egenkontroll av risikoen vil derfor betraktes som lav blant

befolkningen og kan skape uro. Hvordan man konstruerer risiko meldinger vil derfor være av stor betydning.

Usikkerhet i media

Formålet med å formidle en usikker og ukontrollerbar risiko til befolkningen kan virke unyttig. På en side kan det skape unødvendig frykt og mistillit. Men på en annen side kan det føre til økt oppmerksomhet rundt trusselen og økt grad av tillit til myndigheter ved å synliggjøre tiltak som blir utført. Risikokommunikasjon som dekker informasjonsbehovet på en god måte og øker kunnskap kan også redusere frykt og bekymringer (Park & Sohn 2013). Mens effekten av risiko forsterkning i mediebildet som forekommer kun i etterkant av hendelser kan føre til økt uro.

I dag viser mediebildet hovedsakelig en optimisme rundt Smart Grid teknologi, videre har ikke en tilsiktet hendelse med store konsekvenser rammet energisektoren i Norge.
Studiet vil derfor oppfordre til et mer nyansert mediebildet for å gjøre befolkningen oppmerksomme på cybertruslene som eksisterer i sektoren. Ved å fokusere på tiden før en risiko hendelse, og anerkjenne kunnskap begrensninger og usikkerhet, kan resultere i et mer nyansert risikobilde. Ved å adoptere et usikkerhets-basert perspektiv (Fjæran & Aven 2019; Pidgeon & Fischhoff 2011) også i mediebildet, kan befolkningen på bedre måte forventes å takle konsekvenser av et potensielt angrep. Derav vil risikoens bølge-effekter minskes, og konsekvenser som økonomiske tap, tap av omdømme og tillit, samt sosial uro kan bli betraktelig mindre enn dersom risikoen har vært dempet i forkant.

7. Konklusjon

Sammenhengen mellom risiko- kommunikasjon, persepsjoner og reaksjoner er utfordrende å kartlegge. Foretatte analyser gir ingen konkrete svar på hvordan mediers risikokommunikasjon vil påvirke sosiale reaksjoner, men gir grunnlag for videre betraktninger.

Første del av analysen tok for seg risikoprofilen i henhold til myndigheter som viste til en kompleks og usikker risiko. Disse aspektene av risikoen formidles i liten grad i mediebildet i del to av analysen. Noe som kan tilsi at nyhetsmediers belysning av risikoen ikke er tilstrekkelig og kan derfor ha negativ konsekvens for risikoens bølge-effekter i etterkant av et cyberangrep.

Mediebildet i dag viser til mer optimisme i sine skildringer av Smart Grid teknologi, med unntak av mer teknologisk fokuserte tidsskrifter. Og risikokommunikasjon om cybertrusler innen Smart Grids ser ut til å være mager bortsett fra i direkte respons til en ekstraordinær hendelse som Ukraina. Hendelsen har derimot tilsynelatende blitt glemt da Norge aldri har opplevd noe lignende. Basert på mediebildet kan det antas at befolkningen ikke er klare over de teknologiske sårbarhetene som eksisterer, samt hvilke konsekvenser et cyberangrep kan ha for samfunnet.

Prosjektets problemstilling lyder; -*Hvordan kan medias risikokommunikasjon angående cybertrusler i Smart Grids påvirke risiko?*
Det er som sagt vanskelig å gi et konkret svar, men foretatte analyser kan tyde på følgende:

Det norske samfunn befinner seg i tiden *før* en initierende hendelse, og hvordan risikoen velges å rammes og videreformidles til befolkningen i dette stadiet kan være av enorm betydning for den sosiale responsen under og etter et potensielt cyberangrep. Dersom risikoen ikke formidles i større grad i media kan dette få konsekvenser for tillit til myndigheter, økonomi og videre teknologiutvikling. Slike bølge-effekter kan sannsynligvis mitigeres ved å tolerere mer beskrivelser av risikoprofilens utfordrende aspekter, slik som kompleksitet, usikkerhet og tvetydighet.

Dette prosjektet oppfordrer derfor til mer nyanserte beskrivelser i mediebildet, noe som kan oppnåes ved å adoptere et mer usikkerhets-basert perspektiv.
Media har enorm påvirkning på risikopersepsjoner som oppleves gjennom indirekte kontakt. Ved å anerkjenne sin betydning å tilrettelegge for mer nyanserte beskrivelser av risikoprofilen kan det ha positive innvirkninger på sosiale reaksjoner i det norske samfunnet dersom et angrep i energisektoren får katastrofale konsekvenser. For å akseptere risiko må det

eksistere tillit til myndigheter og sentrale aktører. Som en kommunikasjonskanal av stor betydning har nyhetsmedia en sentral rolle når det kommer til å bygge tillit og dekke kunnskapsgapet mellom eksperter og befolkning. Risikoprofilen som blir omtalt er derimot preget av stor usikkerhet og kompleksitet, noe som gjør god kommunikasjon til en utfordring. Ved å inkludere et usikkerhets-basert perspektiv i nyhetsmedia kan informasjonen om cyberrisiko i sektoren dekkes på en fornuftig måte, uten å skape unødvendig sosial uro. Videre kan slik transparent kommunikasjon skape en større grad av samfunnsmessig motstandsdyktighet som kan ha positive effekter på å vedlikeholde tillit til myndigheter dersom et angrep får store konsekvenser. Å fokusere på, og å kommunisere usikkerhets-aspektet ved risikoen kan gi gode resultater ved å introdusere et "sunt nivå" av risiko forsterkelse som igjen kan skape sterkere grad av *public resilience.* Her har nyhetsmedia et ansvar overfor allmennheten.

7.1 Forslag til videre forskning

Mye tidligere forskning viser til sterke relasjoner mellom risikokommunikasjon i media og allmenn risikopersepsjon. Å fremstille risikoprofiler på en nyansert måte vil derfor være av nødvendighet for å skape god offentlig beredskap, samt å skape "sunne" persepsjoner blant befolkningen. Dette prosjektet påpeker at medier bør ha større toleranse for å uttrykke usikkerhet slik at "sunne" holdninger skapes og sosiale reaksjoner i etterkant av en potensiell hendelse vil minimeres. Hvordan man skal konstruere slike risiko meldinger for best mulig respons vil være av nødvendighet for risikokommunikasjon i tiden fremover.

8. Litteraturliste

Adressavisen (2020) "Har du ovner som fjernstyres, kan du bli et hacker-offer"
Hentet fra:
https://www.adressa.no/pluss/nyheter/2020/02/05/Har-du-ovner-som-fjernstyres-kan-du-bli-et-hacker-offer-21004208.ece

Andreassen, J. (2017) "SCADA / DMS / AMS / NIS: Begreper som har gått ut på dato?"
Hentet fra:
https://blogs.esmartsystems.com/no/scada-dms-ams-nis-begreper-som-har-gatt-ut-pa-dato

Andrews, E. (2013) "Who invented the internet?"
Hentet fra: https://www.history.com/news/who-invented-the-internet

Aven, T. (2006) "Risikostyring: Grunnleggende prinsipper og ideer"
(1.utgave) Oslo: Universitetsforlaget

Aven, T., Boyesen, m., Njå, O., Olsen, K.H & Sandve, K. (2016) "Samfunnssikkerhet"
(7.utgave) Oslo: Universitetsforlaget

Avner, T. & Tønnessen,T. (2014) "Nå lysner det for smart strømbruk"
Hentet fra:
https://app.retriever-info.com/go-article/02000220140214167053 7/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Aura Avis (2016) "Nye målere gjør slutt på maset"
Hentet fra:
https://app.retriever-info.com/go-article/055147201609246b5ee935932a3be61b9c55c568b5a2e1/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Azam, N. (2017) "Informasjonssikkerhetstilstanden i energiforsyningen"
Hentet fra: http://publikasjoner.nve.no/rapport/2017/rapport2017_74.pdf

Bergens Tidende (2010) "Snart smekk fullt i Drotningsvik"
Hentet fra:
https://app.retriever-info.com/go-article/02002120100223849e38627eff2d8404565299eaab5414/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light

Besnard, D. & Hollnagel, E. (2012) "I want to believe: some myths about the management of industrial safety" (DOI 10.1007/s10111-012-0237-4)

Bersvendsen, T. (2018) "Smarte byer trenger fremoverlente byggherrer"
Hentet fra:
https://app.retriever-info.com/go-article/020001201811062992d5c61e79758ab50398a5fcd9adb5/null/archive/search?sessionId=0547cc32-4e18-4468-9206-ea4800c14618&&theme=light

Blaikie, N. & Priest, J. (2019) "Designing social research"
(3. utgave) Cambridge: Polity press.

Brunmark, K. (2016) “Beredskapen sviktet under cyberangrep”
Hentet fra:
https://www.abcnyheter.no/nyheter/2016/06/28/195225967/beredskapen-sviktet-under-cyberangrep

Braaten, F. (2015) “Så smarte kan byene bli”
Hentet fra:
https://app.retriever-info.com/go-article/020002201511292554513/null/archive/search?sessionId=61a23cb5-ff28-47d9-b7d3-f4812c0553dd&&theme=light

Braathen, F. (2016) “Seks områder Norge bør satse på”
Hentet fra:
https://app.retriever-info.com/go-article/02000120160108ad1cbe93a5e820bcfbaf6b721394ff90/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Bruvold, J.A. (2017) “Hvordan kan vi kommunisere det vi ikke vet? En kvalitativ studie om risikoforståelse og risikokommunikasjon i en terrorismekontekst”
Hentet fra: https://publications.ffi.no/nb/item/asset/dspace:2658/17-00182.pdf

Brøndbo, M. (2019) “Vil dele ut kortene på nytt”
Hentet fra:
https://app.retriever-info.com/go-article/055017201902232244 66/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Buraas, M. (2020) “Strømnettet og batterienes plass i det”
Hentet fra:
https://app.retriever-info.com/go-article/05523702002001 03151bf7800d8f0cf0d2ca2d03b54101fe/null/archive/search?sessionId=fe9f06ab-1f52-4229-895b-24241e061410&&theme=light

Carlsen, H. (2019) “Høyttalere og hodetelefoner kan brukes som akustiske våpen”
Hentet fra:
https://www.nrk.no/urix/hoyttalere-og-hodetelefoner-kan-brukes-som-akustiske-vapen-1.14657296

Chong, Mark. (2018) “The social amplification of haze-related risks on the Internet”
Hentet fra:
https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=5342&context=lkcsb_research

Clowes, E. (2020) “Key part of electricity network hit by cyber attack “
Hentet fra:
https://www.telegraph.co.uk/business/2020/05/14/key-part-electricity-network-hit-cyber-attack/

Danermark, et al. (2002) “Explaining society: an introduction to critical realism in the social sciences”
Routledge (kapittel 4)

Dege, M. (2020) "The Psychology of Global Crises: State Surveillance, Solidarity and Everyday Life"
Hentet fra:
https://networks.h-net.org/node/73374/announcements/6133880/psychology-global-crises-state-surveillance-solidarity-and

Desarnaud, G. (2017) "Cyber attacks and energy infrastuctures: Anticipating risks"
Hentet fra:
https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf

Digital 21 (2018) "Digitalisering forutsetter sikkerhet – verdiskapende cybersikkerhet bør være et fellesgode- Innspill fra ekspertgruppe 5: Digital sikkerhet"

DiTullio, M.C. (2019) "The moderating role of emotional cushioning between the greif intensity of perinatal loss and relationship satisfaction among women"
Hentet fra:
https://www.semanticscholar.org/paper/The-Moderating-Role-of-Emotional-Cushioning-Between-DiTullio/cb2b761c24f0cff6c4d83f447b0423eabbae72ca

DSB (2016) "Samfunnets kritiske funksjoner"
Hentet fra: https://www.dsb.no/rapporter-og-evalueringer/samfunnets-kritiske-funksjoner/

DSB (2019) "Analyser av krisescenarioer 2019"
Hentet fra: https://www.dsb.no/rapporter-og-evalueringer/analyser-av-krisescenarioer-2019/

Dunwoody, S. (1992) "The Media and Public Perceptions of Risk: How Journalists Frame Risk Stories"
Hentet fra:
https://www.researchgate.net/publication/240320481_The_Media_and_Public_Perceptions_of_Risk_How_Journalists_Frame_Risk_Stories

Dvergsdal, H. (2019) "Digitalisering"
Hentet fra: https://snl.no/digitalisering

Dyb, P.O. (2013) "Fremtiden er elektrisk"
Hentet fra: https://www.vg.no/nyheter/meninger/i/0mdp2/fremtiden-er-elektrisk

Energifakta Norge (2017) "Statlig organisering"
Hentet fra: https://energifaktanorge.no/om-energisektoren/statlig-organisering/

Energifakta Norge (2019a) "Det juridiske rammeverket"
Hentet fra:
https://energifaktanorge.no/regulering-av-energisektoren/det-juridiske-rammeverket/

Energifakta Norge (2019b) "Strømnettet"
Hentet fra: https://energifaktanorge.no/norsk-energiforsyning/kraftnett/

Energix (2019) “En oppsummering av Forskningsrådets workshop 22. august 2019 om status for arbeid med cybersikkerhet i energisektoren “
Hentet fra:
https://www.forskningsradet.no/contentassets/fde911cb10ff493b8eeb83bd17311601/forskningsradet-workshop-22082019--cybersikkerhet-i-energisektoren-rev.2.0.pdf

Engen, O.A.H., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E. & Pettersen, K.A. (2016) “Perspektiver på samfunnssikkerhet“
(utgave 1) Oslo: Cappelen Damm Akademisk

Elhub (2018) “Hva og hvorfor”
Hentet fra: https://elhub.no/om-elhub/hva-og-hvorfor/

EPFL IRGC (2017) “Governing cybersecurity risks and benefits of the Internet of Things: Connected medical & health devices and connected vehicles”
Hentet fra:
https://irgc.org/wp-content/uploads/2018/09/IRGC.-2017.-Cybersecurity-in-the-IoT.-Workshop-report.pdf

Eskeland Kruke, M.H. (2017) “Beskyttelse av sensitiv informasjon En studie av norske nettselskapers beskyttelse av sensitiv informasjon”
Hentet fra:
https://munin.uit.no/bitstream/handle/10037/11344/thesis.pdf?sequence=1&isAllowed=y

E-tjenesten (2020) “Fokus 2020”
Hentet fra: https://forsvaret.no/fokus

E24 (2018) “Oslo er en av verdens fremste smartbyer”
Hentet fra:
https://e24.no/betalt-innhold/bak-tallene/oslo-er-en-av-verdens-fremste-smartbyer/23921687

Falstad, S.H. (2011) “Steinkjer nasjonal test arena for energisystem”
Hentet fra:
https://app.retriever-info.com/go-article/020080201106241020 55b5b40d4ee911d0b5ce0e9ebec6/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Farmakis, N. (2003) “Snart kan du få billig nattstrøm”
Hentet fra https://www.vg.no/nyheter/innenriks/i/3jj90d/snart-kan-du-faa-billig-nattstroem

Flyvbjerg, B. (2004) “Five misunderstandings about case-study research”
Seale, S., Gobo, G., Gubrium,J.F. & Silverman, D. (eds.), Qualitative Research Practice. London and Thousand Oaks, CA: Sage 2004: side 420-434

Frh, H. (2017) “Risk Perception as Media Effect”
Hentet fra: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118783764.wbieme0139

Flå, J.I. (2016) Vil utnytte sola og vinden

Hentet fra:
https://app.retriever-info.com/go-article/055156201607066d89835579c85fe0b1e7c33433db79c4/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light

Fredriksstad blad (2010) "De satser på energi Halden tar mål av seg til å bli fylkets teknologi-motor"
Hentet fra:
https://app.retriever-info.com/go-article/055230201002181116784689/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light

Frøystad, C. (2017) "Cybersikkerhet og strømnettet"
Hentet fra:
https://infosec.sintef.no/informasjonssikkerhet/2017/10/cybersikkerhet-og-stromnettet/
Gore. M,L., Siemer, W.F., Shanahan, J.E., Schuefele, D. & Decker, D.J. (2005) "Effects on risk perception of media coverage of a black bear-related human fatality"
Hentet fra: https://www.jstor.org/stable/3785078?seq=1

Gould, K.P. & Fjæran, L. (2019) "Drift and the Social Attenuation of Risk"
Hentet fra:
https://www.researchgate.net/publication/335163131_Drift_and_the_Social_Attenuation_of_Risk

Gram, T. (2010) "Inngangsintervju: Må satse på kompetanse"
Hentet fra:
https://app.retriever-info.com/go-article/055015201003192396 34/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light

Grimes, R.A. (2019) "SQL Slammer 16 years later: Four modern-day scenarios that could be worse"
Hentet fra:
https://www.csoonline.com/article/3337179/sql-slammer-16-years-later-four-modern-day-scenarios-that-could-be-worse.html

Grøtan, T.O. (2017) "Hva skjer hvis vi mister kontroll over strømnettet vårt?"
Hentet fra:
https://forskning.no/sikkerhet-kronikk-politikk/kronikk-hva-skjer-hvis-vi-mister-kontroll-over-stromnettet-vart/1162015

Gustaffson, E. (2019) "Er det farlig å digitalisere strømnettet?"
Hentet fra: https://www.addsecure.no/is-the-smart-grid-dangerous/

Hamnes, P.N. (2012) "Slik kan hackere mørklegge Norge"
Hentet fra: https://www.tu.no/artikler/slik-kan-hackere-morklegge-norge/243247

Halden arbeiderblad (2011) "AMS"
Hentet fra:
https://app.retriever-info.com/go-article/055153201102268b1a082cea35c8851e4e9311becc4f31/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Halden Arbeiderblad (2014) "Nytt intelligent energisystem"
Hentet fra:
https://app.retriever-info.com/go-article/055153201403213cd92da25117f709a57291ddc623454d/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light

Hollnagel, E., Lundberg, J. & Rollenhagen, C. (2009)
"What-You-Look-For-Is-What-You-Find – The consequences of underlying accident models in eight accident investigation manuals"
Hentet fra:
https://www.sciencedirect.com/science/article/pii/S0925753509000137

Hotvedt, S.K. & Saugstad, S.V. (2017) "Cyberangrep mot Norge øker sterkt"
Hentet fra: https://www.nrk.no/norge/cyberangrep-mot-norge-oker-sterkt-1.13326267

Hovland, K.M. (2018) "Ruster opp kraftnettet for milliarder: – Et historisk høyt nivå"
Hentet fra:
https://e24.no/olje-og-energi/i/gPm10B/ruster-opp-kraftnettet-for-milliarder-et-historisk-hoeyt-nivaa

Hovland, K.M. (2019a) "Tror nytt strøm-system vil gi lavere priser"
Hentet fra: https://e24.no/olje-og-energi/i/J1abr4/tror-nytt-stroem-system-vil-gi-lavere-priser

Hovland, K.M. (2019b) "Vindkraft sto for 14 prosent av Europas strøm"
Hentet fra:
https://e24.no/olje-og-energi/i/4dPqgE/vindkraft-sto-for-14-prosent-av-europas-stroem

Hovland, K.M. (2019c) "Nytt datasystem samler kraftbransjen: Slik påvirkes din strømregning"
Hentet fra:
https://e24.no/olje-og-energi/i/EoVpyA/nytt-datasystem-samler-kraftbransjen-slik-paavirkes-din-stroemregning

Hovland, K.M. (2019d) "Kraftbransjen forsvarer dagens strømmarked: – Det beste for kunden over tid"
Hentet fra:
https://e24.no/olje-og-energi/i/JorLR6/kraftbransjen-forsvarer-dagens-stroemmarked-det-beste-for-kunden-over-tid

Høeg, E. & Belgaux, C. (2019) "Smartbyens blindveier"
Hentet fra: https://morgenbladet.no/aktuelt/2019/09/smartbyens-blindveier

IFP Energies Nouvelles (2018) "Smart City: Energy challenges facing sustainable cities"
Hentet fra:
https://www.ifpenergiesnouvelles.com/article/smart-city-energy-challenges-facing-sustainable-cities

IRGC (2005) "An introduction to the IRGC Risk Governance Framework"

Hentet fra: https://irgc.org/risk-governance/irgc-risk-governance-framework/

IRGC (2006) "Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures" (White paper)
https://irgc.org/wp-content/uploads/2018/09/IRGC_WP_No_3_Critical_Infrastructures.pdf

IRGC (2007) "Managing and reducing social vulnerabilities from coupled critical infrastructures" (Policy brief)
Hentet fra: https://irgc.org/wp-content/uploads/2018/09/IRGCinfra_site06.11.07-2.pdf

Irges, M. (u.å) "Informasjonssikkerhet, cybersikkerhet og IT sikkerhet- hva er forskjellen?"
Hentet fra: http://mortenirgens.com/?p=769

ITB aktuelt (2015) "Hva skjer hvis en hel by blir mørk?"
Hentet fra: https://www.itbaktuelt.no/2015/03/12/hva-skjer-hvis-en-hel-by-blir-mork/

Jacobsen, D.I. (2005) "Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskapelig metode"
(Utgave 2.) Kristiansand: Høyskoleforlaget

Johannessen, T.S. (2019) "Mikronett: Powerhouse skal forsyne hele Brattørkaia med strøm"
Hentet fra:
https://www.tu.no/artikler/mikronett-powerhouse-skal-forsyne-hele-brattorkaia-med-strom/459343

Johansen, P.A. (2016) "De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet"
Hentet fra:
https://www.aftenposten.no/verden/i/WOlg/de-sa-det-var-umulig-naa-klarer-russiske-hackere-aa-slaa-av-stroemnettet?

Jordheim, H. (2018) "Nå kommer smarthus-løsninger alle har råd til"
Hentet fra:
https://www.dinepenger.no/forbruker/stroempriser/naa-kommer-smarthus-loesninger-alle-har-raad-til/24227660

Jung, E.H. & Ha, J.H. (2016) Effect of Television News Viewing on Risk Perception: Focusing on the Coverage of Mad Cow Disease in South Korea
Hentet fra: http://communicationandhealth.ro/upload/number9/EUNHWA-JUNG.pdf

Jystad, P.T. (2019) "Boksen som får NHO-sjefen til å glise bredt"
Hentet fra:
https://app.retriever-info.com/go-article/0551482019110547c70c1648ef21c93603d99b521211bf/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Karlsen, J. (2014) "Smart teknologi stopper strømbrudd"
Hentet fra:
https://app.retriever-info.com/go-article/0200152014111399109/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Kasperson, R.E. & Kasperson, J.X. (1996) “The Social Amplification and Attenuation of Risk”
Hentet fra:
https://training.weather.gov/wdtd/courses/woc/core/crisis-comms-sm/risk-assess/presentation_content/external_files/Social%20Amplification%20of%20Risk_1996.pdf

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. & Ratick, S. (1988) “The Social Amplification of Risk A Conceptual Framework”
Hentet fra:
https://www.researchgate.net/publication/279397338_The_social_amplification_of_risk

Khurana, H., & Lu, N. (2010) “Smart-Grid Security Issues”
Hentet fra: https://www.researchgate.net/publication/224110557_Smart-Grid_Security_Issues

Kibar, O. (2017) “ En av tre mangler sikkerhetsrutiner mot cyberangrep”
Hentet fra:
https://www.dn.no/teknologi/en-av-tre-mangler-sikkerhetsrutiner-mot-cyberangrep/2-1-140472

Kirknes, L. (2011) “Smart strøm med komplikasjoner”
Hentet fra:
https://app.retriever-info.com/go-article/02009320110916515fb9662261ac8b175659c2c159f5e5/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Knudsen, E. (2016) “For første gang skal hackere ha forårsaket et massivt strømbrudd”
Hentet fra:
https://www.tek.no/nyheter/nyhet/i/GGev3q/for-frste-gang-skal-hackere-ha-forarsaket-et-massivt-strmbrudd

Kone, D. & Mullet, E. (1994) “Societal Risk Perception and Media Coverage”
Hentet fra:
https://www.researchgate.net/publication/15053654_Societal_Risk_Perception_and_Media_Coverage

Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I.A., Hovden, J. & Schiefloe, P.M. (2018) “Sikkerhet i arbeidslivet”
(1.utgave) Bergen: Fagbokforlaget

Kvande, L.H. (2017) “Fyller på med dataanalytikere”
Hentet fra:
https://app.retriever-info.com/go-article/02012220170320869095 90c8a386109a341ef2388d1aba/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light

Kvitnes, Ø. (2011) “leder ann i it-boom”
Hentet fra:
https://app.retriever-info.com/go-article/05515320110226b88e80e64101db5c7e8ba8eae649c402/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Laberg, B. (2019) "Grønn energisatsing på Svalbard"
Hentet fra:
https://app.retriever-info.com/go-article/02016020191008c59ef00b0f68e1b3d396e3ecc9e477a0/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Leiknes, E.J. (2011) "Informasjonssikkerhet i komplekse systemer"
Hentet fra: https://brage.bibsys.no/xmlui/handle/11250/182086

Leung, L. (2015) "Validity, reliability, and generalizability in qualitative research"
Hentet fra: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4535087/

Lie, Ø. (2011) "FoU skal gi enklere nettdrift"
Hentet fra:
https://app.retriever-info.com/go-article/055015201110271151537 5/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Line, M.B., Tøndel, I.A., & Jaatun, M.G. (2011) "Cyber Security Challenges in Smart Grids"
Hentet fra:
https://www.researchgate.net/publication/254056200_Cyber_security_challenges_in_Smart_Grids

Lillesund, M. (2009) "Hackere kan kutte strømmen"
Hentet fra: https://www.vg.no/forbruker/teknologi/i/JVvXm/hackere-kan-kutte-stroemmen

Lohne, J., Holm-Nilsen, S., & Hansen, N.R. (2016) "Slik kan hjemmet ditt bli hacket"
Hentet fra: https://www.vg.no/forbruker/i/zn5r1/slik-kan-hjemmet-ditt-bli-hacket

Lorentzen, M. (2018) "«Tingenes internett» inntar Norge: Men det er usikkert hvor fort det blir penger av det"
Hentet fra:
https://e24.no/teknologi/i/0np27o/tingenes-internett-inntar-norge-men-det-er-usikkert-hvor-fort-det-blir-penger-av-det

Fjæran, L. & Aven, T. (2019) "Making visible the less visible – how the use of an uncertainty-based risk perspective affects risk attenuation and risk amplification"
Journal of Risk Research
https://doi.org/10.1080/13669877.2019.1687579

Litos Strategic Communication (u.å) "the SMART GRID: an introduction"
Hentet fra: https://www.energy.gov/oe/downloads/smart-grid-introduction-0

Lund, H. (2014) "Renewable Energy Systems: A Smart Energy Systems Approach to the Choice and Modeling of 100% Renewable Solutions"
(2.utgave) Academic Press, USA.

Lupton, D. (2013) "Risk"
(2.utgave) New York: Routledge

Lyngaas, S. (2020) “European power grid organization says its IT network was hacked”
Hentet fra: https://www.cyberscoop.com/european-entso-breach-fingrid/

Maal, M., Isaachsen, M., & Torget, K. (2017) “Tverrsektoriell sårbarhet: Hvordan få oversikt over sårbarhet i kritiske samfunnsfunksjoner?”
https://www.ffi.no/publikasjoner/arkiv/tverrsektoriell-sarbarhet-hvordan-fa-oversikt-over-sarbarhet-i-kritiske-samfunnsfunksjoner

Mandag Morgen (2010) “Prosumenter, det nye e-ordet”
Hentet fra: https://www.dagensperspektiv.no/prosumenter-det-nye-e-ordet

McLellan, C. (2016) “How hackers attacked Ukraine's power grid: Implications for Industrial IoT security”
Hentet fra:
https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/

Mendel, J. (2017) “Smart Grid Cyber Security Challenges: Overview and Classification”
Hentet fra:
https://www.researchgate.net/publication/316938222_Smart_Grid_Cyber_Security_Challenges_Overview_and_Classification

Michalsen, G.L. (2019) “Mange snakker om kunstig intelligens. Tina Skagen og kollegene gjør noe med det”
Hentet fra:
https://e24.no/naeringsliv/i/J1V3kJ/mange-snakker-om-kunstig-intelligens-tina-skagen-og-kollegene-gjoer-noe-med-det

Midtsæther, A. (2012) “Nord-trøndere tester det smarte strømnettet: Nå kommer intelligente strømmålere”
Hentet fra:
https://e24.no/privatoekonomi/i/70joRo/nord-troendere-tester-det-smarte-stroemnettet-naa-kommer-intelligente-stroemmaalere

Mogensen, M. & Brattli, K.S. (2012) “Klar for det klimanøytrale livet?”
Hentet fra:
https://app.retriever-info.com/go-article/0551902012032227a9879ddd0f5593a69dbf32a8b762c4/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Mordt, H. (2012) “Nye strømmålere gir dyrere - og billigere - strøm”
Hentet fra:
https://app.retriever-info.com/go-article/055153201209191bf71cbfb4b422b363ecbd9f413d9091/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Mostue, L. & Moengen, T. (2020) “Digitalisering av energisektoren: Anbefalinger om forskning og innovasjon”

Hentet fra:
https://smartgrids.no/wp-content/uploads/sites/4/2020/04/Energi21_Digital21_2020-%E2%80%93-Digital-versjon-LQ-%E2%80%93-Enkeltsider.pdf

Muller, L.P, Friis, K. & Gjesvik, L. (2017) "Cyberangrep- hvem har ansvaret?"
Hentet fra: https://www.nrk.no/ytring/cyberangrep-_-hvem-har-ansvaret_-1.13377001

Myhre, A. (2015) "Kommentar: Smarte nordmenn = smart strømmarked?"
Hentet fra:
https://e24.no/naeringsliv/i/G1Ey0l/kommentar-smarte-nordmenn-smart-stroemmarked

Myklebust, H. (2017) "Sosiokulturelt læringssyn"
Hentet fra: https://laeringsglede.wordpress.com/2017/10/20/sosiokulturell-laeringsteori/

Møller, U. & Furnes, S. (2017) "Veileder for tilpasning til ny personopplysningslov"
Hentet fra:
https://www.energinorge.no/fagomrader/strommarked/nyheter/2017/veileder-for-tilpasning-til-ny-personopplysningslov/

Natt, T.H. (2019) "Datasikkerhet"
Hentet fra: https://snl.no/datasikkerhet

Neimark, J. (2007) "The Optimism Revolution"
Hentet fra:
https://archive.vn/20120531064842/http://psychologytoday.com/articles/index.php?term=20070424-000004&page=1#selection-1253.0-1253.23

Neuman, W.L. (2014) "Social research methods: qualitative and quantitative approaches"
(7. utgave) Boston: Pearson

Nickelsen, T. (2017) "Mer sol og vind i strømnettet"
Hentet fra:
https://app.retriever-info.com/go-article/020093201703035181643 9/null/archive/search?sessionId=0547cc32-4e18-4468-9206-ea4800c14618&&theme=light

Nilsen, J. (2011) "Regner på risiko i kraftnettet"
Hentet fra:
https://app.retriever-info.com/go-article/05501520110929c521ca5113952e5091defd00698fff90/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Nordstrøm, J. (2018) "Mange selskaper henger ikke med"
Hentet fra:
https://e24.no/naeringsliv/datasikkerhet/sikkerhetsekspert-mange-selskaper-henger-ikke-med/24378768

NorSIS (2017a) "Hvordan inkludere alle innbyggere i det digitale samfunn?"
Hentet fra: https://norsis.no/inkludere-innbyggere-digitale-samfunn/

NorSIS (2017b) “Cyberangrep mot Norge øker sterkt”
Hentet fra: https://norsis.no/cyberangrep-norge-oker-sterkt/

NorSIS (2018) “Et sikkert digitalt Norge krever en helhetlig tilnærming”
Hentet fra: https://norsis.no/et-sikkert-digitalt-norge-krever-en-helhetlig-tilnaerming/

NOU 2000:24 (2000) “Et sårbart samfunn Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet”
Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2000-24/id143248/sec2

NOU 2006:6 (2006) “Når sikkerheten er viktigst: Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner”
Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

NOU 2015:13 (2015) “Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden”
Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NS 5830:2012. “Samfunnssikkerhet: Beskyttelse mot tilsiktede uønskede handlinger; Terminologi” Oslo: Standard Norge

NSM (2017) “Risiko 2017: Risiko og sårbarheter i en ny tid- en vurdering av sårbarheter og risiko i Norge”
Hentet fra:
https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

NSM (2018) “Risiko 2018: Verdifulle individer Verdifulle virksomheter Verdifull infrastruktur”
Hentet fra:
https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

NSM (2019) “Risiko 2019: Krafttak for et sikrere Norge”
Hentet fra:
https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

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

NTB (2018) “ABB leverer miljøvennlig teknologi til smarte kraftnett i Stavanger Informasjonssjef Smartgrid Ansvarlig, ABB i Norge”
Hentet fra:
https://app.retriever-info.com/go-article/05501320180824ntbinfono20180824177501761/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

NVE (2015) “Alle strømkunder skal få smart strømmåler (AMS) innen 1. januar 2019. Nettselskapene er ansvarlige for å installere de nye målerne”
Hentet fra: https://www.nve.no/stromkunde/smarte-strommalere-ams/

NVE (2018) “Foreløpig tilleggsveileder til kraftberedskapsforskriften”
Hentet fra:
https://www.nve.no/media/7598/forel%C3%B8pig-tilleggsveileder-kraftberedskapsforskriften.pdf

NVE (2019) “Kraftberedskapsforskriften har trådt i kraft”
Hentet fra:
https://www.nve.no/nytt-fra-nve/nyheter-sikkerhet-og-energiforsyningsberedskap/kraftberedskapsforskriften-har-tradt-i-kraft/

Nygaard, N.G. (2019) “AMS-måler: Slik fungerer din automatiske strømmåler”
Hentet fra: https://xn--strm-ira.no/ams-str%C3%B8mm%C3%A5ler

Nystrøm, S. (2015) “Økt kunnskap for et sikrere samfunn”
Hentet fra;
https://app.retriever-info.com/go-article/05517920150918823e4ae61e838e5572413c698e16b67c/null/archive/search?sessionId=61a23cb5-ff28-47d9-b7d3-f4812c0553dd&&theme=light

Næringslivets sikkerhetsråd (2019) “Kriminalitets- og sikkerhetsundersøkelsen i Norge 2019”
Hentet fra:
https://www.nsr-org.no/getfile.php/1312949-1568794843/Bilder/Krisino/KRISINO%20rapport%202019%20low.pdf

Olsen, P.C. (2020) Nettdrift anno 2020: Digital disrupsjon i energisektoren
Hentet fra: https://response.esmartsystems.com/last-ned-gratis-nettdrift-anno-2020

Otuoze, A.O., Mustafa, M.W., & Larik, R.M. (2018) “Smart grids security challenges: Classification by sources of threats”
Hentet fra:
https://www.researchgate.net/publication/323008907_Smart_grids_security_challenges_Classification_by_sources_of_threats

Park, J. & Sohn, A. (2013) “The Influence of Media Communication on Risk Perception and Behavior Related to Mad Cow Disease in South Korea
Hentet fra: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3767106/

Parveen, H., Chitrapu, S., Tripathi, D. & Das, B. (2017) “Texts: Framing, Agenda-setting”
Hentet fra:
https://www.researchgate.net/publication/319879263_Texts_Framing_Agenda_Setting

Pentz, B. (2015) “Frykter ikke hackere tross daglige angrep”

Hentet fra:
https://forskning.no/sikkerhet-universitetet-i-stavanger-partner/frykter-ikke-hackere-tross-daglige-angrep/459576

Persson, C.P. (2019) "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

Pettersen, P. (2015) "Cyber Security Dag"
Hentet fra:
https://app.retriever-info.com/go-article/05527220150619b796574f3955abcd70a68cd275fd782a/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light

Petts, J., Horlick-Jones, T. & Murdock, G. (2001) "Social amplification of risk: The media and the public"
Hentet fra:
https://www.academia.edu/2796566/Social_amplification_of_risk_The_media_and_the_public

PF Energi (2018) "Cybersikkerhet i kraftbransjen"
Hentet fra: https://www.polyteknisk.no/moter/cybersikkerhet-i-kraftbransjen/

Pidgeon, N. & Fischhoff, B. (2011) "The role of social and decision sciences in communicating uncertain climate risks"
Hentet fra:
https://www.researchgate.net/publication/50877022_The_Role_of_Social_and_Decision_Sciences_in_Communicating_Uncertain_Climate_Risks

PST (2020) "Nasjonal trusselvurdering 2020"
Hentet fra:
https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/

Rapley, T. (2004) "Interviews" C. Seale et al. (red) Qualitative research practice. London: Sage publications.

Rathus, S.A. (2006) "Psychology: Concepts and Connections, Brief Version" (8.utgave) USA: Cengage Learning

Renn, Ortwin (2008) "Risk Governance: Coping with uncertainty in a complex world" (1.utgave) New York, Usa: Earthscan Publishing

Renn, O. & Levin, D (2010) "Trust and Credibility in Risk Communication"
Hentet fra:
https://www.researchgate.net/publication/279396741_Trust_and_credibility_in_risk_communication

Renn, O., Slovic, P., Brown, H.S., & Emel, J. (2010) "The social amplification of risk"

Hentet fra:
https://www.researchgate.net/publication/279397338_The_social_amplification_of_risk

Renn, O (2018) "Implications for risk governance"
Kapittel 16. s.345-369. Fra:
Streicher, B., Raue, M. & Lermer, E. (Red). (2018) "Psychological Perspectives on Risk and Risk Analysis: Theory, Models, and Applications"
(1.utgave) New York: Springer Publishing

Regjeringen (2018) "Norges miljø- og klimasamarbeid med EU"
Hentet fra:
https://www.regjeringen.no/no/tema/europapolitikk/tema/miljo-og-klima1/id686218/

Regjeringen (2019a) "Digital sikkerhet er en grunnleggende forutsetning"
Hentet fra:
https://www.regjeringen.no/no/aktuelt/digital-sikkerhet-en-grunnleggende-forutsetning/id2640917/

Regjeringen (2019b) "Ny personopplysningslov"
Hentet fra:
https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/ny-personopplysningslov/id2340094/

Rijpma, J.A. (1997) "Complexity, tight-coupling and reliability: Connecting normal accidents theory and high reliability theory"
(utgave 5) Oxford: Blackwell publishers Ltd.

Romsdal budstikke (2014) "Smartere strømforsyning"
Hentet fra:
https://app.retriever-info.com/go-article/02005820141126d920a410be1cbe95c9add6b212a71103/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light

Ross, I. (2016) "Exposing fraud: Skills, process and practicalities"
(1.utgave) England: Wiley

Rosness, R., Grøtan, T.O., Guttormsen, G., Herrera, I.A., Steiro, T., Størseth, F., Tinmannsvik, R.K. & Wærø, I. (2010) "Organisational accidents and resilient organisations: six perspectives"
(2.utgave) SINTEF Technology and Society.

Røyksund, M. (2011) "Informasjonssikkerhet i kraftforsyningen"
Hentet fra: https://uis.brage.unit.no/uis-xmlui/handle/11250/184580

Sander, K. (2019a) "Dokumentanalyse/Innholdsanalyse"
Hentet fra:
https://estudie.no/dokumentanalyse/

Sander, K. (2019b) "Eksplorerende design"

Hentet fra: https://estudie.no/eksplorerende-design/

Sand, K. (2015) "Det norske strømnettet og smartgrid, hvordan fungerer energidistribusjonen i dag?"
Hentet fra: https://www.natursekken.no/binfil/download2.php?tid=2103925

Sand, K. (2016) "Hvordan henger elkraft og IKT sammen?"
Hentet fra:
https://smartgrids.no/wp-content/uploads/sites/4/2016/02/K-Sand_Smartgrids-intro.pdf

Sands, G. (2016) "What to Know About the Worldwide Hacker Group 'Anonymous'"
Hentet fra:
https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302

Schallmo, D., Boardman, L. & Williams, C.A. (2018) "Digital transformation of business models- best practice, enablers, and roadmap"
I "International Journal of Innovation Management Vol. 21, No. 8"
DOI: 10.1142/S136391961740014X

SmartGrids (2016) "National and Regional Smart Grids initiatives in Europe"
(2.utgave) European technology platform for the electricity networks of the future

Smart Innovation Norway (2016) "Storsatsing på framtidas digitale kraftnett"
Hentet fra:
https://www.smartinnovationnorway.com/nyheter/storsatsing-pa-framtidas-digitale-kraftnett/

Simonovich, L. (2020) "Are utilities doing enough to protect themselves from cyberattack?"
Hentet fra:
https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/

Skotnes, R.Ø. (2017) "Cybersikkerhet en samfunnsverdi vi alle må beskytte"
Hentet fra:
https://www.aftenbladet.no/meninger/debatt/i/2QOO4/cybersikkerhet-en-samfunnsverdi-vi-alle-ma-beskytte

Sprenger, M. (2010) "Nettselskapene må investere 80 milliarder på 10 år"
Hentet fra:
https://app.retriever-info.com/go-article/05501520100527244013/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light

Sprenger, M. (2013) "Full usikkerhet rundt AMS"
Hentet fra:
https://app.retriever-info.com/go-article/05501520130124158891 92/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Statnett, Fingrid, Energinet, & Svenska kraftnat (2019) "Nordic Grid Development Plan 2019"

Hentet fra:
https://www.statnett.no/contentassets/61e33bec85804310a0feef41387da2c0/nordic-grid-development-plan-2019-for-web.pdf

Sørlie, J.E. (2010) "Avtale med Microsoft"
Hentet fra:
https://app.retriever-info.com/go-article/0551532010051995ea0960b7956d62cbce1325a116ef8e/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light

Sæle, H. (2014) "Smart Grids"
Hentet fra: https://www.sintef.no/prosjekter/smart-grids/

The norwegian smartgrid centre (u.å.a) "FoU"
Hentet fra: https://smartgrids.no/fou/

The norwegian smartgrid centre (u.å.b) "Vedtekter"
Hentet fra: https://smartgrids.no/senteret/vedtekter/

The norwegian smartgrid centre (u.å.c) "Medlemmer"
Hentet fra: https://smartgrids.no/senteret/medlemmer/

The Norwegian Smartgrid Centre (u.å.d) "Om Smartgrid"
Hentet fra: https://smartgrids.no/senteret/about-smartgrid/

Trønder-avisa (2011) "Smartrevolusjon for strømdistribusjon"
Hentet fra:
https://app.retriever-info.com/go-article/020080201109139885 8a3915d2a9f3fd7de7d096066489/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Trønderbladet (2011) "Ny regning fra Trønderenergi"
Hentet fra:
https://app.retriever-info.com/go-article/0551062011100600102444ff937ad2c57abfdbf9b1ca86/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Tørdal, R.M. (2017) "Analysemodeller"
Hentet fra:
https://ndla.no/nb/subjects/subject:14/topic:1:103867/topic:1:185606/resource:1:99541

United Nations (u.å) "Envision2030: 17 goals to transform the world for persons with disabilities"
Hentet fra: https://www.un.org/development/desa/disabilities/envision2030.html

Urheim, M.O. (2015) "Risikokommunikasjon og risikopersepsjon: En kvalitativ studie av terrorvarselet sommeren 2014 og dens implikasjoner for videregåendeelever i Bergen"
Hentet fra:
https://munin.uit.no/bitstream/handle/10037/9655/thesis.pdf?sequence=1&isAllowed=y

Vada, P.A. (u.å) "Forsyningssikkerhet og beredskap"

Hentet fra:
https://www.energinorge.no/fagomrader/strommarked/kraftsystemet/forsyningssikkerhet-og-beredskap/

Valmot, O.R. (2011a) "Hvordan få næringsbygg til å bruke mindre energi"
Hentet fra:
https://app.retriever-info.com/go-article/05501520111020a5a466697c73c5d313a17739a79a2424/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Valmot, O.R. (2011b) "Kobler fiber og strøm"
Hentet fra:
https://app.retriever-info.com/go-article/055015201111111011652184/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Valmot, O.R. (2013) "Så smart blir boligen"
Hentet fra: https://e24.no/teknologi/i/6j4zWW/saa-smart-blir-boligen

Vasstrøm, M., Lysgård, H.K. & Haaland, H. (2018) "Konflikter i vinden"
Hentet fra: https://www.dagsavisen.no/debatt/konflikter-i-vinden-1.1204396

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

Volt (2015a) "Ny sikkerhetsarkitektur"
Hentet fra:
https://app.retriever-info.com/go-article/05527220150417d016f0e97ec708b00f7784ca2dfd39a9/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light

Volt (2015b) "Neste steg"
Hentet fra:
https://app.retriever-info.com/go-article/05527220150417fd0a18254420254633f6e602e680a2ac/null/archive/search?sessionId=61a23cb5-ff28-47d9-b7d3-f4812c0553dd&&theme=light

Volt (2016) "Smarte nett gir uante muligheter"
Hentet fra:
https://app.retriever-info.com/go-article/05527220160205b9e642b2409910b66fe2084c6a74d700/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Westlund, D. (2007) "The Essential Role of Cyber Security in the Smart Grid"
Hentet fra:
https://electricenergyonline.com/energy/magazine/312/article/The-Essential-Role-of-Cyber-Security-in-the-Smart-Grid-.htm

Yacout, D. (2013) "An introduction to Smart Grid"
Hentet fra:
https://www.researchgate.net/publication/280723223_An_Introduction_to_Smart_Grid

Yndestad, H. (2015) “Fra «Smart Teknologi»,til «Smarte Regioner»”
Hentet fra:
https://app.retriever-info.com/go-article/020031201501072916f03655b8e0ecce22113c4db8376b/null/archive/search?sessionId=61a23cb5-ff28-47d9-b7d3-f4812c0553dd&&theme=light

Yndestad, H. (2016) “Når nettene blir smarte”
Hentet fra:
https://app.retriever-info.com/go-article/02003120160902e3a7608679fffc54bdba7380a7de3e83/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Ystrøm, B. (2011) “Viktig for statsbygg”
Hentet fra:
https://app.retriever-info.com/go-article/0551532011041681186a61b394a48412d142cf3431066d/null/archive/search?sessionId=40833ddd-d92c-4ed3-b691-a851d4cc020f&&theme=light

Øverby, H. (2018) “Tingenes Internett”
Hentet fra: https://snl.no/tingenes_internett

Øyehaug, O. (2012) “Boksen som sparer strøm”
Hentet fra;
https://app.retriever-info.com/go-article/020021201212191004997/null/archive/search?sessionId=ca77fb35-a264-4dc1-888f-43f34f2dd086&&theme=light

Åsberg, E. (2020) “Dra nytte av digitaliseringen: Fire norske nettselskaper og Connected Grid”
Hentet fra:
https://response.esmartsystems.com/dra-nytte-av-digitaliseringen-fire-norske-nettselskaper-og-connected-grid?hsCtaTracking=2e53fd26-b122-4de5-a32f-2918e602c995%7C3f85ca23-a114-4a8e-897d-90a8e5c2ef37

Vedlegg

Vedlegg 1: Medieanalyse

NR.	Tidsskrift/Publikasjon	Tittel	Årstall	Belysning av tema basert på stikkord og kontekst	Artikkelenes hovedtrekk
1	Teknisk Ukeblad	Slik kan hackere mørklegge Norge	2012	Både positiv og negativ	Beskriver scenario der deler av kraftnettet kan hackes via ams målere, men påpeker at det er usanssynlig. Samtidig beskrives økonomisk og samfunnsmessig effektivisering pga ams.
2	NRK	Cyberangrep mot Norge øker sterkt	2017	Negativ	NorCert registrerte 22.000 cyberangrep i 2016 og det øker årlig. Påpeker norske myndigheters frykt for angrep i olje- og energi sektoren.
3	Addsecure	Er det farlig å digitalisere strømnettet?	2019	Både positiv og negativ	Flere kritiske infrastrukturer blir koblet sammen over internett og gjort sårbare. Samtidig er samfunnet avhengig av denne utvikling av smart teknologi.
4	Aftenposten	De sa det var umulig. Nå klarer russiske hackere å slå av strømnettet	2016	Negativ	Beskriver hvordan hackere stengte strømmen i Ukraina i desember 2015. Inneholder også ekspertuttalelser om at slike angrep kan skje i Norge.
5	ABC Nyheter	Lammet strømnettet og ekom i nasjonal øvelse: Beredskapen sviktet under cyberangrep	2016	Negativ	Beskriver en øvelse av Nkom som avslørte store sårbarheter i Ekom og energisektorens cybersikkerhet.
6	Forskning.no	Hva skjer hvis vi mister kontroll over strømnettet vårt?	2017	Både positiv og negativ	Økt digitalisering av energi-infrastrukturen skaper bekymringer for angrep. Påpeker samtidig at

					forskere, myndigheter og industrien jobber på lag og har gjort mye for sektorens motstandsdyktighet.
7	SINTEF INFOSEC	Cybersikkerhet og strømnettet	2017	Både positiv og negativ	Lister opp flere tilsiktede angrep innen energisektoren. Digitalisering lar oss gjøre mer med mindre ressurser. Framtiden tillater oss ikke å være frakoblet.
8	ITB aktuelt	Hva skjer hvis en hel by blir mørk?	2015	Både positiv og negativ	Beskriver SG-teknologi forbedring av eksisterende infrastruktur, men påpeker at sårbarheter og angrepsforsøk øker.
9	Verdens Gang	Fremtiden er elektrisk	2013	Positiv	Beskriver behovet for bærekraftig bruk av småkraft, og derav nytten av smart teknologi, også i strømnettet.
10	E24	Nord-trøndere tester det smarte strømnettet: Nå kommer intelligente strømmålere	2012	Positiv	Smarte hus og strømnett er ikke lengre bare en visjon. Enkelt og effektivt for kunder, distributører kan tilby mer tjenester basert på data fra ams. Store muligheter for økonomisk gevinst.
11	E24	Tror nytt strøm-system vil gi lavere priser	2019	Positiv	Elhub, datasystemet som samler data fra ams. Er strømsparende, økonomisk gunstig, skaper bedre konkurranse, og makt til kundene.
12	Verdens Gang	Slik kan hjemmet ditt bli hacket	2016	Negativ	Smart teknologi i alle sektorer skaper enorme digitale kjeder som igjen gir økt angrepsflate. NSM bekymret.
13	Verdens Gang	Hackere kan kutte strømmen	2009	Både positiv og negativ	Smart strømsparing er åpent for angrep. Men nevner Smart Grid som et mer intelligent system som reduserer strømtopper og forbedrer kommunikasjon.
14	E24	“Mange snakker om kunstig intelligens. Tina	2019	Positiv	Gjennom kunstig intelligens og droner vil eSmart levere løsninger for

		Skagen og kollegene gjør noe med det”			kraftbransjen, med store behov for oversikt og utvikling. Selskapene kan derfor vedlikeholde mer fornuftig, og sikre en smart strømforsyning
15	E24	Så smart blir boligen	2013	Positiv	AMS er et fundament for smart-revolusjonen. En plattform for nyttig, smart og lønnsom utvikling.
16	Dine penger: forbruker	Nå kommer smarthus-løsninger alle har råd til	2018	Positiv	Smart teknologi vil gi deg kontinuerlig oversikt over strømforbruket. Tusenvis av kroner kan spares i strømutgifter.
17	E24	Ruster opp kraftnettet for milliarder: -Et historisk høyt nivå	2018	Både positiv og negativ	Rekordhøye investeringer i kraftnettet. Overgang til mer grønn småkraft. Drifts utfordringer med økt kompleksitet.
18	E24	“Tingenes Internett” inntar Norge: Men det er usikkert hvor fort det blir penger av det	2018	Positiv	Smart-teknologi og IoT gir nye muligheter. Men usikkerhet når investeringene vil gi økonomisk utbytte.
19	Verdens Gang	Snart kan du få billig nattstrøm	2003	Positiv	SG-teknologi åpner for toveiskommunikasjon og bedre strømregulering.
20	E24	Oslo er en av verdens fremste smartbyer	2018	Positiv	Smart-teknologi gjøre livet enklere og bedre. Lister opp funksjoner slik teknologi utøver i smarte byer.
21	Verdens Gang	Smarte byer- hva er det egentlig?	2018	Positiv	Hver enkelt smart-teknologi komponent utgjør nødvendigvis ikke enorm forskjell. Men sammenkobling gjennom IoT skaper en teknologisk holisme for framtiden.
22	E24	Vindkraft sto for 14 prosent av Europas strøm	2019	Positiv	Øking av energi fra fornybare kilder i Europa skyldes bla. utbygging av vindparker, mens økningen i distribusjon kan knyttes til oppgradering av kraftnettet, og smarte strømmålere

23	E24	Nytt datasystem samler kraftbransjen: Slik påvirkes din strømregning	2019	Positiv	Elhub gjør at strømkunder kan betale forskjellig pris time for time. Statnett, NVE og regjeringen håper på nye tjenester og smartere strømbruk.
24	E24	Kraftbransjen forsvarer dagens strømmarked: -det beste for kunden over tid	2019	Positiv	Kundeklager angående dyr strøm i 2003 og 2010. AMS og Elhub vil gi kunder mer kontroll.
25	E24	Tappet kraftselskap for 2,3 milliarder	2012	Både positiv og negativ	Påpeker frykt for utro tjenere i kraftbransjen. Men hevder "fjern hacking" blir vanskeligere i slike systemer. Og påpeker en optimisme innen sikkerhetsmekanismer relatert til ams.
26	E24	Kommentar: Smarte nordmenn = Smart strømmarked?	2015	Positiv	Vi er helt avhengige av strøm, kapasitet kan bli problematisk uten videre innovasjon. Smart Grid er løsningen, teknologier eksisterer og er klar til bruk.
27	Moss Avis	Strømnettet og batterienes plass i det	2020	Positiv	Smart strømstyring legger til rette for bærekraftig energiproduksjon. Billigere for kunder og mer miljøvennlig.
28	Avisa Nordland	Boksen som får NHO-sjefen til å glise bredt	2019	Positiv	Smart grid vil bidra til å løse klimautfordringer. Smart teknologi vil tillate oss å vokse i takt med kunders behov.
29	Byggfakta	Grønn energisatsing på Svalbard	2019	Positiv	Svalbard satser stort på sol og vind gjennom batterier og fleksibel strøm. En test av slik teknologi har hittil vært svært givende.
30	Adressavisa	Har du ovner som fjernstyres, kan du bli et hacker-offer	2020	Negativ	Trekker frem PST rapport som viser bekymring for det digitale trusselbildet. Særlig med tanke på IoT og kritisk infrastruktur. Sensore og mange IoT gjenstander er ikke laget med tanke på angrep. Det

					trengs bedre tverrsektorielt samarbeid.
31	Morgenbladet	Smartbyens blindveier	2019	Både positiv og negativ	Kappløp om å bli "smartest". Norge har store forutsetninger for å få til gode, smarte løsninger. Samtidig eksisterer det usikkerhet om hva som er målet med å bli smart, og risiko det involverer.
32	Nationen	Vil dele ut kortene på nytt	2019	Positiv	Delvis urelevant tematisk artikkel, men nevner utbyggelse av smart grid og dens gunstige funksjon for klimautslipp.
33	Klassekampen	Et smartere strømnett	2010	Positiv	Smart Grids for sikring mot strømbrudd, høye kraftpriser, og i tillegg gi kraftig stimulans til både energieffektivisering og produksjon av alternativ energi.
34	Halden Arbeiderblad	ams	2011	Positiv	Beskriver fordelen der smart grids gjør forbrukere til produsenter.
35	Halden Arbeiderblad	Leder ann i it-boom	2011	Positiv	IT-prosjekter i kø i kraftbransjen. AMS skaper muligheter.
36	Halden Arbeiderblad	Viktig for Statsbygg	2011	Positiv	Statsbygg inngår samarbeid med NCE Smart Energy Markets. Prosjektet skal gi økt kunnskap om energiforbruk samt incentiv bærekraftighet.
37	Trønder-avisa	Steinkjer nasjonal test arena for energisystem	2011	Positiv	NTE kjører demoprosjekt i Steinkjer. Bedre utnyttelse av energimengde. Positivt for klima, samt minimerer behov for nye investeringer i strømnettet.
38	Trønder-avisa	Smartrevolusjon for strømdistribusjon	2011	Positiv	SmartGrid som paradigmeskifte innen strømdistribusjon. Helt ny måte å tenke på når det gjelder produksjon, distribusjon og forbruk.
39	Computerworld	Smart strøm med	2011	Både positiv og negativ	Strøm- og IT- ingeniøre må bli samkjørt. Alt kobles

		komplikasjoner			sammen og vi blir sårbare. Men gir et mer fleksibelt nett med muligheter for fjernovervåkning.
40	Teknisk Ukeblad	Regner på risiko i kraftnettet	2011	Både positiv og negativ	ROS-analyser av ekstraordinære situasjoner i kraftnettet. Sannsynligheter er umulig å kvantifisere, men det arbeides kontinuerlig med sikkerhet.
41	Trønderbladet	Ny regning fra Trønderenergi	2011	Positiv	Gjennom nye IT-løsninger forventer Trønderenergi å øke driftssikkerhet og oppnå økonomiske besparelser. De får også en plattform som er forberedt på Smart grid inkorporasjonen.
42	Teknisk Ukeblad	Hvordan få næringsbygg til å bruke mindre energi	2011	Positiv	Smart strømstyring er det billigste alternativet for å forbruke mindre energi, noe det blir krav til i tiden fremover.
43	Teknisk Ukeblad	FoU skal gi enklere nettdrift	2011	Positiv	Driftsmargin har blitt mindre i kraftnettet de siste årene. Teknologiutvikling i retning Smart grid er beste mulighet for å holde nettet stabilt.
44	Teknisk Ukeblad	Kobler fiber og strøm	2011	Positiv	AMS sammen med sensorer gir lavere strømregning og redusert belastning. Summen av SG er at man kan øke driftssikkerheten, forlenge levetiden på ulike komponenter og redusere kostnadene.
45	Trønder-avisa	Næringsklynger skal skape vekst	2012	Positiv	Arenaprogrammet. Målet er at de deltakende bedriftene skal bli smartere sammen. Stor optimisme for videre teknologisk innovasjon.
46	Arkitektur N	klar FOR det klimanøytrale livet?	2012	Positiv	Tar for seg bærekraftig byutvikling. Hvordan skal vi leve “lettere”? Innen energisektoren er svaret klimanøytral forsyning gjennom smart grid.
47	Computerworld	Fremtidens	2012	Positiv	Jo mer effektivt vi utnytter

		kraftnett med ny teknologi			ressursene, jo mer lønnsomt blir det å bygge ut kapasiteten ytterligere. Smart grids er en løsning.
48	Trønder-avisa	NTE får 10 mill. i statsstøtte	2012	Positiv	NTE får støtte for testprosjekt av nye avanserte strømmålere. Slik teknologi vil være et gjennombrudd for smart teknologi.
49	Teknisk ukeblad	FRYKTER LITEN GEVINST AV AMS	2012	Positiv	Frykter at investeringer i ams vil gi økt pris for kunder, men må gjøres fra et samfunnsøkonomisk perspektiv. Ingen sikkerhets- eller drifts-trusler nevnes med tanke på ams/smart grid.
50	Halden Arbeiderblad	Nye strømmålere gir dyrere - og billigere - strøm	2012	Positiv	Etablering av et smartere strømnett vil gi store gevinster da forbruker kan tilpasse bruk etter prising på døgnet. God investering for fremtiden.
51	Bergens Tidende	Boksen som sparer strøm	2012	Positiv	Smart grids gir muligheten til å koble ut deler av strømforbruket når belastningen er stor. Denne investeringen gjør at man slipper videre investeringer i kraftnettets infrastruktur.
52	Teknisk ukeblad	FULL USIKKER RUNDT AMS	2013	Både positiv og negativ	Mer positiv enn negativ. Men påpeker en bekymring om for store investeringskostnader og umoden teknologi.
53	Teknisk ukeblad	*Kraftbransjen stoler ikke på moderne IT*	2013	Positiv	Optimistisk rundt SG-teknologi og påpeker at det er nødvendig investering for fremtiden. Tittelen på artikkelen viser kun til forskjeller i grad av optimisme mellom IT- og Kraftsektoren.
54	Aftenposten	Nå lysner det for smart strømbruk	2014	Positiv	SG-teknologi gir bedre overvåkning og styring av distribusjonsnettet.
55	Halden arbeiderblad	Nytt intelligent	2014	Positiv	SG legger til rette for

		energisystem			“prosumenter”. NCE SEM og Statsbygg har inngått forskningssamarbeid for videre utvikling.
56	Harstad tidende	Smart teknologi stopper strømbrudd	2014	Positiv	AMS og SG ble testet på to skoler. Ga positive resultater.
57	Romsdals budstikke	Smartere strømforsyning	2014	Positiv	Statnett tester ut SG-teknologi. Gjør det mulig å koble ut systemet fragmentert, framfor å mørklegge hele steder.
58	Sunnmøreposten	Fra «Smart Teknologi»,til «Smarte Regioner»	2015	Positiv	Smart Grid er del av en større innovasjon, Smarte byer. Samling av stordata gir tilgang til felles data i sanntid, noe som igjen fører til en tverrfaglig analyse av store regionale datamengder der trender optimaliserer ressurser over tid.
59	Volt	Starten på en ny æra	2015	Positiv	Smartmålere som sensor for å overvåke nettet. Innsamlet data gir innsikt slik at videre fremskritt kan gjøres pålitelig, effektivt og sikkert.
60	Volt	Ny sikkerhetsarkitektur	2015	Både positiv og negativ	Bedriften NES har utviklet en ny sikkerhetsplattform for SG. Mer optimistisk enn negativ, men anerkjenner manglende eksisterende sikkerhet i enkelte SG komponenter.
61	Volt	Neste steg	2015	Både positiv og negativ	SG som nødvendig investering for miljø, økonomi og samfunn. Påpeker enkelte utfordringer med tanke på regulering og implementeringsstrategi.
62	Volt	Cyber Security dag	2015	Både positiv og negativ	Smart teknologi innen alle sektorer gjør oss sårbare. Men dette anerkjennes og arbeides kontinuerlig med. Beskriver også typer trusler mot kommunikasjon på smart grid.
63	Oppland Arbeiderblad	Økt kunnskap for	2015	Både positiv og	Kommunikasjonsteknologie

		et sikrere samfunn		negativ	r og programvare-apper på digitale enheter gjør oss sårbare for angrep. Men fagmiljøet innen IKT sikkerhet vokser.
64	Trønder-avisa	Lokal Energisikkerhet	2015	Positiv	Wenas vil gi trøndere tryggere og mer stabil strømtilførsel gjennom småkraft og SG.
65	Aftenposten	Så smarte kan byene bli	2015	Positiv	Smart teknologi vil bli tvunget mer og mer frem av ren nødvendighet. Artikkelen gir en "utopisk" beskrivelse av den smarte fremtiden, dette inkluderer strøm.
66	Opdalingen	Vil utnytte sola og vinden	2016	Positiv	"On-grid" kunder, eller prosumenter, vil kunne få gode tilbud i Oppdal, Rennebu, Gauldal, Røros, Skaun, Klæbu og Trondheim.
67	Volt	Smarte nett gir uante muligheter	2016	Positiv	Smarte nett og ny teknologi åpner for nye gode muligheter. Maskinlæring vil automatisere beslutningsprosesser.
68	Adresseavisen	Seks områder Norge bør satse på	2016	Positiv	Konsernsjef i Sintef, snakker om hvordan teknologien endrer norsk industri og om nye vekstmuligheter. SG blir positivt nevnt.
69	Aura avis	Nye målere gjør slutt på maset	2016	Positiv	AMS sparer strøm og gir sikrere og mer fleksibel forsyning. Smart strøm gir fordeler både for kundene, kraftsystemet og klimaet.
70	Sunnmørsposten	Når nettene blir smarte	2016	Både positiv og negativ	Skeptisk til Smart-kappløpet. Synkronisert, tverrsektoriell teknologi blir egne organismer som optimaliserer etter egne mål. Hvem skal eie og beskytte stordata? Maskiner sitter i førersetet.
71	Finansavisen	Fyller på med	2017	Positiv	Kraftprodusenter går fra å bruke It som

		dataanalytikere			kontorstøttesystemer til å bli IT-selskaper. AMS og Elhub vil effektivisere.
72	Computerworld	Mer sol og vind i strømnettet	2017	Positiv	Norge sløser enorme mengder strøm fra vind og sol. SG teknologi skal stanse dette.
73	Halden arbeiderblad	Kan huset bli mer intelligent enn meg?	2017	Positiv	Smart Energy-konferansen i 2017. Fokus på sikkerhet og tillit i smarte nett. Et helhetlig risikoperspektiv virker mer optimistisk enn negativt.
74	Adresseavisen	Smarte byer trenger fremoverlente byggherrer	2018	Positiv	Urbanisering øker, byer fortettes og krever effektiv arealutnyttelse. Anvendelse av SG-teknologi er essensiell for å møte krav til effektiv areal- og energieffektivitet.
75	NTB	ABB leverer miljøvennlig teknologi til smarte kraftnett i Stavanger Informasjonssjef Smartgridansvarlig , ABB i Norge	2018	Positiv	Smart strøm er en milepæl for kraftbransjen, og for miljøet.

Vedlegg 2: Kilder til medieanalyse

Linker er satt opp i tabellens (vedlegg 1) rekkefølge.

(1) https://www.tu.no/artikler/slik-kan-hackere-morklegge-norge/243247
(2) https://www.nrk.no/norge/cyberangrep-mot-norge-oker-sterkt-1.13326267
(3) https://www.addsecure.no/is-the-smart-grid-dangerous/
(4) https://www.aftenposten.no/verden/i/WOlg/de-sa-det-var-umulig-naa-klarer-russiske-hackere-aa-slaa-av-stroemnettet
(5) https://www.abcnyheter.no/nyheter/2016/06/28/195225967/beredskapen-sviktet-under-cyberangrep
(6) https://forskning.no/sikkerhet-kronikk-politikk/kronikk-hva-skjer-hvis-vi-mister-kontroll-over-stromnettet-vart/1162015
(7) https://infosec.sintef.no/informasjonssikkerhet/2017/10/cybersikkerhet-og-stromnettet/
(8) https://www.itbaktuelt.no/2015/03/12/hva-skjer-hvis-en-hel-by-blir-mork/
(9) https://www.vg.no/nyheter/meninger/i/0mdp2/fremtiden-er-elektrisk
(10) https://e24.no/privatoekonomi/i/70joRo/nord-troendere-tester-det-smarte-stroemnettet-naa-kommer-intelligente-stroemmaalere
(11) https://e24.no/olje-og-energi/i/J1abr4/tror-nytt-stroem-system-vil-gi-lavere-priser
(12) https://www.vg.no/forbruker/i/zn5r1/slik-kan-hjemmet-ditt-bli-hacket
(13) https://www.vg.no/forbruker/teknologi/i/JVvXm/hackere-kan-kutte-stroemmen
(14) https://e24.no/naeringsliv/i/J1V3kJ/mange-snakker-om-kunstig-intelligens-tina-skagen-og-kollegene-gjoer-noe-med-det
(15) https://e24.no/teknologi/i/6j4zWW/saa-smart-blir-boligen
(16) https://www.dinepenger.no/forbruker/stroempriser/naa-kommer-smarthus-loesninger-alle-har-raad-til/24227660
(17) https://e24.no/olje-og-energi/i/gPm10B/ruster-opp-kraftnettet-for-milliarder-et-historisk-hoeyt-nivaa
(18) https://e24.no/teknologi/i/0np27o/tingenes-internett-inntar-norge-men-det-er-usikkert-hvor-fort-det-blir-penger-av-det
(19) https://www.vg.no/nyheter/innenriks/i/3jj90d/snart-kan-du-faa-billig-nattstroem
(20) https://e24.no/betalt-innhold/bak-tallene/oslo-er-en-av-verdens-fremste-smartbyer/23921687
(21) https://www.vg.no/annonsorinnhold/smart/komplett/472-smarte-byer-hva-er-det-egentlig
(22) https://e24.no/olje-og-energi/i/4dPqgE/vindkraft-sto-for-14-prosent-av-europas-stroem
(23) https://e24.no/olje-og-energi/i/EoVpyA/nytt-datasystem-samler-kraftbransjen-slik-paavirkes-din-stroemregning
(24) https://e24.no/olje-og-energi/i/JorLR6/kraftbransjen-forsvarer-dagens-stroemmarked-det-beste-for-kunden-over-tid
(25) https://e24.no/teknologi/i/G1Ebmq/tappet-kraftselskap-for-23-milliarder
(26) https://e24.no/naeringsliv/i/G1Ey0l/kommentar-smarte-nordmenn-smart-stroemmarked
(27) https://app.retriever-info.com/go-article/05523702001031 51bf7800d8f0cf0d2ca2d03b54101fe/null/archive/search?sessionId=0eae6e36-ab75-4255-9043-afae50045b69&&theme=light

(28) https://app.retriever-info.com/go-article/0551482019110547c70c1648ef21c93603d99b521211bf/null/archive/search?sessionId=0eae6e36-ab75-4255-9043-afae50045b69&&theme=light
(29) https://app.retriever-info.com/go-article/02016020191008c59ef00b0f68e1b3d396e3ecc9e477a0/null/archive/search?sessionId=0eae6e36-ab75-4255-9043-afae50045b69&&theme=light
(30) https://www.adressa.no/pluss/nyheter/2020/02/05/Har-du-ovner-som-fjernstyres-kan-du-bli-et-hacker-offer-21004208.ece
(31) https://app.retriever-info.com/go-article/055126201909276985498 6/null/archive/search?sessionId=0eae6e36-ab75-4255-9043-afae50045b69&&theme=light
(32) https://app.retriever-info.com/go-article/05501720190223224466/null/archive/search?sessionId=0eae6e36-ab75-4255-9043-afae50045b69&&theme=light
(33) https://app.retriever-info.com/go-article/0550102010081945487/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(34) https://app.retriever-info.com/go-article/055153201102268b1a082cea35c8851e4e9311becc4f31/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(35) https://app.retriever-info.com/go-article/05515320110226b88e80e64101db5c7e8ba8eae649c402/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(36) https://app.retriever-info.com/go-article/0551532011041681186a61b394a48412d142cf3431066d/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(37) https://app.retriever-info.com/go-article/02008020110624102055b5b40d4ee911d0b5ce0e9ebec6/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(38) https://app.retriever-info.com/go-article/020080201109139885 8a3915d2a9f3fd7de7d096066489/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(39) https://app.retriever-info.com/go-article/02009320110916515fb9662261ac8b175659c2c159f5e5/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(40) https://app.retriever-info.com/go-article/05501520110929c521ca5113952e5091defd00698fff90/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(41) https://app.retriever-info.com/go-article/0551062011100600102444ff937ad2c57abfdbf9b1ca86/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(42) https://app.retriever-info.com/go-article/05501520111020a5a466697c73c5d313a17739a79a2424/null/archive/search?sessionId=667fd528-c7b9-4baf-9b2e-647272a3c9d8&&theme=light
(43) https://app.retriever-info.com/go-article/05501520111027197bc178c8d8bf9deb5b935d0b180934/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(44) https://app.retriever-info.com/go-article/05501520111110daa569f7d8e856654b75b91447174919/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light

(45) https://app.retriever-info.com/go-article/020080201203056728ea827596be2d44063529e472e29c/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(46) https://app.retriever-info.com/go-article/0551902012032227a9879ddd0f5593a69dbf32a8b762c4/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(47) https://app.retriever-info.com/go-article/0200932012042713320775/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(48) https://app.retriever-info.com/go-article/020080201205038f5452cbb90dea92d1e19cadee513f32/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(49) https://app.retriever-info.com/go-article/0550152012053113618276/null/archive/search?sessionId=7c9e68fc-a35c-4088-abc4-eecdb3acb2fd&&theme=light
(50) https://app.retriever-info.com/go-article/055153201209191bf71cbfb4b422b363ecbd9f413d9091/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(51) https://app.retriever-info.com/go-article/0200212012121910049 97/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(52) https://app.retriever-info.com/go-article/0550152013012415889192/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(53) https://app.retriever-info.com/go-article/0550152013092618118314/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(54) https://app.retriever-info.com/go-article/0200022014021416705 37/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(55) https://app.retriever-info.com/go-article/055153201403213cd92da25117f709a57291ddc623454d/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(56) https://app.retriever-info.com/go-article/0200152014111399109/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(57) https://app.retriever-info.com/go-article/02005820141126d920a410be1cbe95c9add6b212a71103/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(58) https://app.retriever-info.com/go-article/0200312015010729 16f03655b8e0ecce22113c4db8376b/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(59) https://app.retriever-info.com/go-article/055272201502130a8a1e425e7958633efd9769abe1347d/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(60) https://app.retriever-info.com/go-article/05527220150417d016f0e97ec708b00f7784ca2dfd39a9/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(61) https://app.retriever-info.com/go-article/05527220150417fd0a18254420254633f6e602e680a2ac/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(62) https://app.retriever-info.com/go-article/05527220150619b796574f3955abcd70a68cd275fd782a/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light

(63) https://app.retriever-info.com/go-article/05517920150918823e4ae61e838e5572413c698e16b67c/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(64) https://app.retriever-info.com/go-article/0200802015110639246f0f3fd6d74772454dbf3070ba15/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(65) https://app.retriever-info.com/go-article/020002201511292554513/null/archive/search?sessionId=79da5825-95ae-42e1-a605-171e8200d1ea&&theme=light
(66) https://app.retriever-info.com/go-article/055156201607066d89835579c85fe0b1e7c33433db79c4/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(67) https://app.retriever-info.com/go-article/05527220160205b9e642b2409910b66fe2084c6a74d700/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(68) https://app.retriever-info.com/go-article/02000120160108ad1cbe93a5e820bcfbaf6b721394ff90/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(69) https://app.retriever-info.com/go-article/055147201609246b5ee935932a3be61b9c55c568b5a2e1/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(70) https://app.retriever-info.com/go-article/02003120160902e3a7608679fffc54bdba7380a7de3e83/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(71) https://app.retriever-info.com/go-article/0201222017032086909590c8a386109a341ef2388d1aba/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(72) https://app.retriever-info.com/go-article/02009320170303518164 39/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(73) https://app.retriever-info.com/go-article/0551532017021631b1847ecb3314d03d8d7edce54f6205/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(74) https://app.retriever-info.com/go-article/020001201811062992d5c61e79758ab50398a5fcd9adb5/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light
(75) https://app.retriever-info.com/go-article/05501320180824ntbinfono2018082417750 1761/null/archive/search?sessionId=668559df-9704-4489-8526-7868fa2d02ce&&theme=light

Vedlegg 3: Sentimentanalyse

Stikkord og kategorisering av sentimentanalyse.
Artikelnummer slik som vist i vedlegg 1 "*Medieanalyse*"

Del 1: Artikkel 1-25

	Artikkel nr.																								
Stikkord	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
Smart	6	0	6	0	0	1	2	3	5	10	0	0	2	5	12	3	2	0	0	26	34	1	5	1	0
Nyttig	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Lønnsomt	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
Trygghet	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Effektiv	1	0	0	0	0	2	0	0	0	0	0	0	0	0	2	0	1	0	0	1	1	0	1	0	0
Verdiskapning	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0
Gunstig	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
Prosumer	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Intelligent	0	0	0	0	0	0	0	0	0	1	0	0	2	1	1	0	0	0	0	0	3	0	0	0	0
Gevinst	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	1	0	0	0	0	0	0	1
Bedre	0	0	1	0	0	1	0	1	3	4	2	0	0	0	6	0	1	0	2	2	4	0	4	1	0
Forsyningssikkerhet	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0
Strømoverskudd	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0
Fleksibilitet	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0
Reduksjon	1	0	0	0	0	1	0	0	0	1	0	0	1	0	1	0	0	0	0	2	0	1	2	0	1
Hacking	9	2	2	8	4	0	0	1	0	0	0	7	4	0	0	0	0	0	0	0	0	0	0	0	2
Ondsinnet	2	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Datainntrenger	3	2	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Katastrofe	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Skade	3	0	0	1	1	7	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Angrep	9	11	6	7	22	16	13	3	0	0	0	2	2	0	0	0	0	0	0	0	0	0	0	0	0
Trussel	0	1	1	0	2	9	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Kompleksitet	2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0
Ødeleggelse	1	0	2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sabotasje	2	5	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Avbrudd	1	0	0	6	1	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0
Strømbortfall	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sårbarhet	3	0	0	0	1	2	2	1	0	0	0	4	5	0	0	0	0	0	0	0	0	0	0	0	0
Cyber-trussel/ sårbarhet	1	4	0	1	10	4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Misbruk	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Del 2: Artikkel 26-50

	Artikkel nr.																								
Stikkord	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**
Smart	13	1	4	5	0	30	1	14	2	7	2	5	7	15	0	1	2	1	5	2	1	3	3	3	3
Nyttig	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	1	1	1	0	1
Lønnsomt	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	1	0	1	1	0	0	0
Trygghet	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Effektiv	4	0	2	1	0	0	1	1	0	0	1	0	0	2	1	1	6	0	3	0	0	1	1	0	0
Verdiskapning	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
Gunstig	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Prosumer	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Intelligent	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0	1	0	0	1	0	0	0	0	0	0
Gevinst	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2
Bedre	1	0	0	1	0	1	0	2	0	0	0	1	0	0	0	0	6	1	6	0	0	0	1	0	0
Forsyningssikkerhet	0	0	0	5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Strømoverskudd	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0
Fleksibilitet	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0
Reduksjon	6	2	0	2	0	0	0	3	0	0	0	0	0	0	0	0	5	0	3	0	5	0	0	0	0
Hacking	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Ondsinnet	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0

Datainntrenger	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Katastrofe/ Krise	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Skade	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Angrep	0	0	0	0	3	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0
Trussel	0	0	0	0	3	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0
Kompleksitet	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Ødeleggelse	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sabotasje	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Avbrudd	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
Bort/ Ut-fall	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
Sårbarhet	0	0	0	0	1	2	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
Cyber-trussel/ sårbarhet	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Misbruk	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Del 3: Artikkel 51-75

	Artikkel nr.																								
Stikkord	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**
Smart	3	1	6	24	3	5	3	22	8	6	5	1	1	1	22	0	10	3	8	12	1	2	6	6	5
Nyttig	0	0	1	3	0	1	0	0	0	1	2	1	1	1	0	1	11	1	0	0	0	1	0	2	1
Lønnsomt	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Trygghet	0	0	0	0	0	0	0	0	0	0	0	0	1	2	0	0	0	1	0	0	0	0	0	0	0
Effektiv	0	0	0	1	0	0	0	2	8	2	10	0	0	0	1	0	5	1	0	0	0	2	0	3	1
Verdiskapning	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	3	1	0	1	0	0	0	0	0
Gunstig	0	0	0	0	0	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Prosumer	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Intelligent	0	0	1	0	3	1	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0
Gevinst	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Bedre	1	0	1	5	1	0	0	0	2	0	1	1	0	0	0	0	8	0	0	0	0	2	0	0	0

Forsyningsikkerhet	1	0	0	1	0	4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
Strømoverskudd	0	0	0	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0
Fleksibilitet	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	3	1	1	0	0	1	0	0	0
Reduksjon	2	0	3	0	0	1	0	0	0	0	1	0	0	1	0	0	3	0	0	1	0	0	0	0	1
Hacking	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
Ondsinnet	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Datainntrenger	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Katastrofe/Krise	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Skade	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Angrep	0	0	0	0	0	0	0	0	0	2	0	25	1	0	0	0	0	0	0	0	0	0	0	0	0
Trussel	0	1	0	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0	0	0	0	0	0	0	0
Kompleksitet	0	0	0	0	0	0	0	1	0	0	3	0	0	0	0	0	0	0	0	1	0	0	0	0	0
Ødeleggelse	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
Sabotasje	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Avbrudd	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
Bort/ Ut -fall	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sårbarhet	0	0	0	0	0	0	0	0	0	0	0	4	2	0	0	0	0	0	0	0	0	0	0	0	0
Cyber-trussel/ sårbarhet	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0
Misbruk	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0