DET TEKNISK-NATURVITENSKAPELIGE FAKULTETET

# MASTEROPPGAVE

| | |
|---|---|
| Studieprogram/spesialisering:<br>Risk analysis and governance | *Vårsemesteret, 2023*<br><br>Åpen / ~~Konfidensiell~~ |
| Forfatter: Olav Persson Flatabø | |
| Fagansvarlig ved UiS: Roger Flage | |
| Tittel på oppgaven: Sannsynlighet eller usikkerhet? En undersøkelse av risikokonseptualiseringen tilknyttet cybersikkerhet hos fire virksomheter kritiske for norsk samfunnssikkerhet<br><br>Engelsk tittel: Probability or uncertainty? An examination of the risk conceptualization connected to the cyber security in four organizations critical for Norwegian societal security | |
| Studiepoeng: 30 | |
| Emneord: Risiko, cybersikkerhet, kritisk infrastruktur, usikkerhet, sannsynlighet, NSM, Norges Bank, Petroleumstilsynet, Telenor | Sidetall: 50<br>+ vedlegg/annet:<br><br>Stavanger, *14/6-2023* |

## Sammendrag

Norge, som et av verdens mest digitaliserte land, har gjort enorm nytte av cyberteknologi, men har samtidig åpnet opp for et svært omfattende og komplekst trusselbilde. Et gjennomgående tema i årets trusselvurderinger fra blant andre NSM og PST er at det er særlig utfordrende å vurdere og håndtere cyberrisiko. Momenter som lange leverandørkjeder, hybride trusler og brå teknologisk utvikling fører til at trusselbildet blir svært usikkert. Vi trenger følgelig risikobeskrivelser som reflekterer og tar høyde for dette. Det ble derfor aktuelt å gjøre en undersøkelse av risikokonseptualiseringen hos en rekke virksomheter kritiske for norsk samfunnssikkerhet og hvorvidt de hensyntar usikkerheten i det digitale trusselbildet gjennom følgende problemstilling: *Er risikokonseptualiseringen av cybersikkerheten tilknyttet kritisk infrastruktur i Norge forenlig med usikkerhetsbasert risikoteori?*

Gjennom arbeidet har det blitt tatt utgangspunkt i et usikkerhetsbasert risikoperspektiv som omhandler å definere risiko som konsekvenser med tilhørende usikkerheter, gjerne referert til som «(C, U)». Oppgaven undersøker og vurderer fire ulike virksomheter tilknyttet kritisk infrastruktur i Norge: NSM, Norges Bank, Petroleumstilsynet og Telenor. De er fra vidt forskjellige sektorer, men har til felles at alle er tilknyttet kritisk infrastruktur og har ansvar for tilhørende sikkerhetsarbeid. Metoden som benyttes er dokumentanalyse. Dette gjøres primært gjennom å undersøke hvordan risiko omtales i publikasjoner fra virksomhetene selv.

Oppgaven kommer frem til at NSM og Norges Bank har begge et risikoperspektiv som tilsvarer å konseptualisere risiko som en *kombinasjon av sannsynlighet og konsekvens*. Ut fra usikkerhetsbasert risikolitteratur som trekkes frem i oppgaven, er dette en upassende tilnærming til sikkerhetsrisiko og kan ofte ende i utilstrekkelige og/eller misvisende risikobeskrivelser. Implikasjonene blir forsterket av at cyberrisikobildet er særlig preget av usikkerhet. Videre kommer det frem at både Telenor og Petroleumstilsynet har en tilnærming til risiko som baseres på (C, U)-perspektivet. Med utgangspunkt i informasjonen samlet inn i denne oppgaven, kan man hverken avkrefte eller bekrefte problemstillingen helt kategorisk, ettersom virksomhetene ikke opererer ut fra én felles risikokonseptualisering. Som et resultat konkluderer oppgaven med at Petroleumstilsynet og Telenor sin risikokonseptualisering er *forenlig* med usikkerhetsbasert risikoteori. NSM og Norges Bank gir på sin side uttrykk for risikokonseptualisering som er *uforenlig* med usikkerhetsbasert risikoteori.

# Forord

Etter fem år som student på Universitetet i Stavanger er det vanskelig å ikke å føle på litt vemod når masteroppgaven endelig skal innleveres. Å levere inn denne oppgaven markerer en stor milepæl for meg, men markerer også slutten på både mitt liv som student og som beboer i Stavanger. Det har vært fem svært lærerike år, både med tanke på utdanningen i seg selv, men ikke minst gjennom å ha bodd i en annen by enn hjembyen og bli godt kjent med en helt annen del av landet.

Arbeidet med oppgaven har vært en enormt givende prosess som har bidratt godt til både akademisk og personlig utvikling. Det har riktignok gått litt seigt periodevis, men samlet sett har dette gått langt bedre enn jeg turte å se for meg i forkant av semesteret. Jeg kan nå se tilbake på et veldig interessant prosjekt med masse lærdommer jeg gleder meg til å ta med til den nye jobben i Oslo.

Det er en rekke mennesker jeg ønsker å takke for at semesteret har vært en fryd. I forbindelse med oppgaven ønsker jeg å rette en kjempetakk til min veileder, Roger Flage. Roger har vært en helt super veileder som har gitt gode og grundige tilbakemeldinger på oppgaven hele veien. Han passet også på at jeg kom godt i gang tidlig på semesteret gjennom å foreslå tidsplaner og sette mål. Å komme godt i gang tidlig i semesteret har strengt tatt ikke vært normen for meg de ni foregående semestrene, og jeg har absolutt merket at dette var helt nødvendig for denne oppgaven. Jeg vil også takke mine foreldre for uvurderlig støtte gjennom alle ti semestrene og bidrag til språkvask på oppgaven. Jeg vil til slutt takke mine medstudenter på fRiskrommet, som har stilt opp med godt selskap og støtte gjennom hele semesteret og bidratt godt til å gjøre arbeidet med masteren overkommelig.

# Innholdsfortegnelse

1. Innledning ..... 6
1.1 Bakgrunn ..... 6
1.1.1 Cybertrusler i Norge ..... 6
1.1.2 Norges kritiske infrastruktur ..... 7
1.1.3 Norges kritiske infrastruktur og cybersikkerhet ..... 9
1.1.3 Cybersikkerhet og risikostyring ..... 10
1.2 Problemstilling, avgrensing og formål ..... 10
1.3 Oppgavens struktur ..... 11
2.0 Teori ..... 13
2.1 Generisk risikovitenskap og anvendt risikovitenskap ..... 13
2.2 Safety eller security? ..... 13
2.3 Konsekvenser og assosierte usikkerheter ..... 14
2.4 Alternative risikokonseptualiseringer ..... 16
2.4.1 Mer om risiko som sannsynlighet og konsekvens ..... 17
2.4.2 Mer om alternativer ..... 17
2.4.3 Svakheter knyttet til (C, P) og ISO-perspektiv ..... 18
2.5 Risiko innen sikkerhet og økonomi ..... 19
3.0 Metode ..... 21
3.1 Metodologiske hovedtrekk ..... 21
3.2 Oppgavens utvalg ..... 21
3.3 Fremgangsmåte ..... 22
3.4 Metode for analyse og diskusjon ..... 23
3.5 Validitet og reliabilitet ..... 23
4.0 Informasjonsinnsamling ..... 26
4.1 Nasjonal sikkerhetsmyndighet ..... 26
4.1.1 NSM - RISIKO ..... 26
4.1.2 Nasjonalt digitalt sikkerhetsbilde 2022 ..... 26
4.1.3 Lov om nasjonal sikkerhet (sikkerhetsloven) ..... 27
4.1.4 Veileder for sikkerhetsstyring ..... 29
4.1.5 Risikovurdering av IKT-systemer ..... 30
4.2 Norges bank ..... 30
4.2.1 Finansiell infrastruktur 2022 ..... 31
4.2.2 Ros (2020) ..... 31
4.2.3 TIBER-NO ..... 33
4.2.4 NBIM - policies ..... 34
4.3 Petroleumstilsynet ..... 34

4.3.1 Risikobegrepet i petroleumsvirksomheten ..... 34
4.3.2 Integrert og helhetlig risikostyring i petroleumsindustrien ..... 35
4.3.3 Styringsforskriften ..... 36
4.3.4 SINTEF – regulering av IKT-sikkerhet ..... 37
4.4 Telenor ..... 39
4.4.1 Telenor – Digital sikkerhet ..... 39
4.5 Oppsummerende tabell for virksomhetenes risikoforståelse ..... 42
5.0 Analyse og diskusjon ..... 43
5.1 Hovedtrekk i funnene ..... 43
5.1.1 Vektlegging av risiko ..... 43
5.1.2 Risikoperspektiv hos virksomhetene ..... 44
5.1.3 Er risikoforståelsen hos virksomhetene forenlig med usikkerhetsbasert risikoteori? ..... 48
5.2 Ulikheter og likheter ..... 51
5.3 Implikasjoner rundt å vurdere risiko som sannsynlighet og konsekvens ..... 53
5.4 Validitet og reliabilitet ..... 54
6.0 Konklusjon ..... 56

# 1. Innledning

## 1.1 Bakgrunn

### 1.1.1 Cybertrusler i Norge

Gjennom de siste tiårene har Norge, i likhet med store deler av verden, gått gjennom en digital transformasjon av hele samfunnet. Digitaliseringen har allerede ført til utallige nye muligheter, og det er ingen ende på disse i siktet enda. Utviklingen er imidlertid ikke bare av positiv betydning. Samtidig som vi kan setter pris på alt det gode denne utviklingen har ført med seg, er det et omfattende spekter av alvorlige sårbarheter som nå har tatt stor plass i et voksende trusselbilde for både samfunnssikkerheten og statssikkerheten i Norge. Norge, som et av de mest digitaliserte landene i verden, er særlig utsatt (DSB, 2019).
De enorme forbedringene som følger med digital teknologi, har samtidig ført til at samfunnet har gjort seg svært avhengig av den. For den enkelte er en vellykket hverdag nå betinget av at man for eksempel får kommunisert med venner og familie og planlagt reiseveiene sine. Butikker trenger fungerende betalingsterminaler. Et hotell må ha orden på bookinger og adgangssystemer. Et typisk kontor setter til daglig opp digitale møter og trenger tilgang til fakturainformasjon. Oppgaver som dette gjøres i dag digitalt og henger tett sammen med samfunnets helt avgjørende funksjoner.

I årene før 2014 har hensynet til effektiv statsforvaltning, økonomisk liberalisering og internasjonalisering fått veie tyngst, mens hensynet til sikkerhet har måttet vike. Siden har verdensbildet på ny blitt preget av økende spenning blant verdens stormakter, og staten har vist økt fokus på og vilje til å bedre norsk sikkerhet i takt med verdensbildet (Notaker, 2023). Norge må nå forholde seg til et omfattende trusselbilde. En trussel defineres av SRA som et begrep vanligvis brukt til omtale av risiko som følge av et angrep (SRA, 2018). Dette innebærer et fokus på trusler som vil utnytte sårbarheter der de blir funnet, i motsetning til hendelser som naturkatastrofer, som inntreffer nærmest vilkårlig. I PST sin trusselvurdering blir trussel satt i sammenheng gjennom en trefaktormodell. Modellen setter trussel sammen med sårbarhet og verdi, som sammen utgjør risiko (PST, 2023).

Gjennom PST sin nasjonale trusselvurdering for 2023, får vi vite at etterretningsvirksomhet er blant de alvorlige truslene innen det digitale domenet. Det kommer også frem at det pågår

omfattende etterretningsvirksomhet i Norge på vegne av fremmede stater. PST gir uttrykk for å være sikre på at flere stater har utført dette i Norge det siste året og navngir fire nasjoner: Russland, Kina, Iran og Nord-Korea. Russland og Kina blir videre utpekt som de største trusselaktørene blant fremmede statsmakter. I kontekst av utviklingen vi så gjennom 2022 og frem til nå, er dette et trusselområde som må bli tatt på alvor. Regjeringen sier selv at risikobildet har blitt skjerpet siden invasjonen av Ukraina (Meld St 9 (2022-2023)). Videre har Telenor i sin nyeste rapport om digital sikkerhet meldt om høyere usikkerhet rundt russiske aktører og deres vilje til å angripe norsk infrastruktur (Telenor, 2022). Skal vi tro trusselvurderingene fremlagt, er det ingen mangel på grunner til å investere videre i cybersikkerhet og å være på vakt.

Underleverandører blir også trukket frem som et sentralt trusselområde. Virksomheter benytter seg i stadig høyere grad av underleverandører. Underleverandører kan utgjøre en trussel, ettersom disse kan fungere som en angrepsflate for virksomhetene som hyrer dem inn. Trusselaktører hopper gjerne over gjerdet der det er lavest, og dersom underleverandører innvilges tilganger, samtidig som de ikke opprettholder tilsvarende sikringstiltak, kan dette føre til at virksomheter som i utgangspunktet er godt sikret, får betydelige sårbarheter (PST, 2023).
Det kommer imidlertid et lysglimt frem i NSMs digitale trusselvurdering fra fjoråret: antall vellykkede kompromitteringer hadde sunket, samtidig som antall forsøk hadde økt. Vi må likevel ta dette med en klype salt, ettersom det er usikkert om dette skyldes at vellykkede kompromitteringer blir bedre til å skje uoppdaget (NSM, 2022a).

### 1.1.2 Norges kritiske infrastruktur

For å forstå hva som utgjør Norges kritiske infrastruktur, vil Direktoratet for samfunnssikkerhet og beredskap (DSB) sin kartlegging av samfunnets kritiske funksjoner (DSB, 2016) være en verdifull kilde. Kartleggingen har som formål å være et grunnlagsdokument for samfunnssikkerhet- og beredskapsarbeid. Samtidig som ulike typer virksomheter er fordelt ut i ulike sektorer med forskjellige overlagte myndigheter, står de overfor utfordringer som spenner på tvers av sektorer og nivåer. Gjennom å identifisere kritiske funksjoner og deres funksjonsevne, kan forståelsen rundt fordelingene og sammenhengene blant samfunnets funksjoner settes i system.

DSB viser til NOU 2006:6 for definisjonen av kritisk infrastruktur og grunnleggende behov. Kritisk infrastruktur defineres i NOU 2006: 6 slik: «Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse» *(NOU 2006:6. Kapittel 3)* Videre blir grunnleggende behov beskrevet som trygghet og fysiske behov som vann, mat varme og lignende, (NOU 2006:6). Dersom nedetid for slike funksjoner truer befolkningens sikkerhet og/eller sikkerhetsfølelse innen syv døgn eller mindre, kan funksjonene betegnes som kritiske (DSB, 2016).

I kartleggingen fra DSB blir det definert tre hovedkategorier for kritiske funksjoner:
(1) Styringsevne og suverenitet - denne kategorien beskrives som grunnleggende rammebetingelser for ivaretakelse av samfunnsfunksjonene og defineres av to kritiske funksjoner: (1) styring og kriseledelse og (2) forsvar. Disse skal blant annet hjelpe landet med sikkerhet overfor andre stater, opprettholde kontroll og normale styringsaktiviteter i utfordrende tider. Blant aktørene vil vi finne organisasjonene bak de tre trussel- og risikovurderingene som ble publisert i februar i år (NSM, 2023, PST, 2023, E-tjenesten, 2023): NSM, PST og E-tjenesten.
(2) Befolkningens sikkerhet - omhandler funksjoner avgjørende for beskyttelse av liv og helse, demokratiske rettigheter, miljø, eiendom og materielle verdier. Funksjonene innenfor dette området retter seg mot både trusler og farer som direkte kan virke inn på borgernes sikkerhet, deriblant tjenester innen helse, politi og vern mot naturkatastrofer.
Det er fem funksjoner som utgjør dette området: (1) Lov og orden, (2) Helse og omsorg, (3) Redningstjenester, (4) IKT-sikkerhet og (5) Natur og miljø.
(3) Samfunnets funksjonalitet - dette betegner samfunnets ulike type forsyninger og infrastrukturbaserte tjenester av kritisk nødvendighet. Dette området har blitt omfattende og komplisert, ettersom ulike kritiske områder er avhengige av andre og kan gi videre komplikasjoner for ytterligere kritiske leveranser – for eksempel kraft, ekom og finansielle tjenester, som i utgangspunktet er tre forskjellige funksjonsområder.
Samfunnets funksjonalitet omfatter i alt syv forskjellige funksjonsområder: (1) Forsyningssikkerhet, (2) Vann og avløp, (3) Finansielle tjenester, (4) Kraftforsyning, (5) Elektronisk kommunikasjon, (6) Transport og (7) Satellittbaserte tjenester. Hver av disse har en rekke underkategorier bestående av tilhørende kapabiliteter som blir videre definert i dokumentet.

### 1.1.3 Norges kritiske infrastruktur og cybersikkerhet

Som tidligere nevnt er trusselbildet i det digitale domenet svært omfattende for norsk sikkerhet som en helhet. Denne oppgaven er imidlertid avgrenset til å handle om forholdet mellom kritisk infrastruktur og cybertrusler. Kritisk infrastruktur og cyberdomenet har gjennom de siste tiårene blitt koblet tett sammen. Kritisk infrastruktur preges av kompleksitet og avhengigheter som ofte kan være gjensidig, som blir omtalt som «systems of systems» (Aven, 2016).

Fra DSB sin kartlegging, kommer det tydelig frem at cyberdomenet tar svært stor plass i det norske samfunnet – det er også verdt å notere seg at denne kartleggingen er fra 2016 og utviklingen har ikke bremset siden da. IKT-sikkerhet utgjør en av de fem hovedkategoriene under befolkningens sikkerhet. I tillegg kan det ventes at IKT-hendelser vil ha betydning for samtlige andre funksjoner i varierende grad. Gjennom de siste årene har vi sett cyberhendelser eksempelvis føre til at fly holdes på bakken, forsinkelser i helsetjenester og strømavbrudd (Gjesvik, 2019). Cyberangrep kan true samfunnssikkerheten generelt og statssikkerheten spesielt (DSB, 2019). Hendelsene viser oss at avhengighetene som nå ligger til grunn, kan sette liv og helse i fare.

DSB har videre publisert en rekke analyser av krisescenarioer i 2019. Blant dem finner vi en risikoanalyse som omhandler cyberangrep mot norsk ekom-infrastruktur (DSB, 2019). Blant vurderingen kommer det frem at vi i en tilspisset sikkerhetspolitisk situasjon må regne med ulike typer cyberangrep som blant virkemidlene en fremmed statsmakt benytter seg av mot Norge (DSB, 2019). Hvorvidt Norge befinner seg i en slik situasjon nå, kan diskuteres, men vi har definitivt kommet oss noen skritt nærmere som følge av konflikten i Ukraina – Norges statsminister uttalte i 2022 at Norge hadde kommet i en sikkerhetspolitisk utsatt situasjon (Notaker, 2023).

Dette leder oss inn på hybride virkemidler (også kalt sammensatte) som et særlig alvorlig trusselområde. NUPI (2016) peker på at dette gjerne dreier seg om en kombinasjon av konvensjonelle og ukonvensjonelle metoder for makt og vold. Ofte benyttes begrepet om å kombinere cyberangrep med andre virkemidler. Disse truslene kan komme fra både statlige og ikke-statlige trusselaktører (NUPI, 2016).

Vi har siden fått ny sikkerhetslov fra 2019, som har til hensikt å sikre kritisk infrastruktur. Endringene har inkludert flere endringer i et forsøk på å holde takt med den teknologiske

utviklingen og rollen til privat sektor i et moderne Norge. Blant endringene finner vi muligheten for å underlegge private virksomheter, brede rettslige standarder (for eksempel bruk av «forsvarlig» i stedet for å sette mer konkrete krav) og bestemmelser rettet mot informasjonssystemer og informasjonssikkerhet (Sikkerhetsloven, 2018).

### 1.1.3 Cybersikkerhet og risikostyring

Cybersikkerhet og risikostyring har blitt to fagområder som har fått mye med hverandre å gjøre etter hvert som risikoutviklingen har tatt nye veier og blitt vesentlig høyere. Et tydelig og aktuelt eksempel på viktigheten og relevansen av risikostyring innen forebyggende cybersikkerhetsarbeid, kan vi finne i en risikovurdering utført av NSM i mars 2023 i et brev til Justis- og beredskapsdepartementet. Her har NSM vurdert implikasjonene av applikasjonene TikTok og Telegram på tjenesteenheter, der særlig førstnevnte har vært særlig omstridt i offentlige debatter. Det vises til at applikasjonene har tilknytning til Kina og Russland. Her ble risikoen klassifisert som høy, og til følge vurderer NSM at applikasjonene ikke bør installeres på tjenestetelefoner til ansatte i offentlig sektor, samt private virksomheter tilknyttet sikkerhetsloven. Et gjennomgående tema i bakgrunnen beskrevet er kompliserte og utfordrende trusler som bidrar til et svært usikkert trusselbilde virksomhetene må vurdere og håndtere (NSM, 2023).

## 1.2 Problemstilling, avgrensing og formål

Oppgavens problemstilling lyder slik:

*Er risikokonseptualiseringen av cybersikkerheten tilknyttet kritisk infrastruktur i Norge forenlig med usikkerhetsbasert risikoteori?*

Hva som legges i usikkerhetsbasert risikoteori vil utdypes i teorikapittelet, men vil helt grunnleggende dreie seg om å forstå risiko som å omfatte konsekvenser og assosierte usikkerheter, og med det diskutere hvorvidt virksomhetene hensyntar usikkerhet innenfor deres risikovurderinger og risikostyring knyttet til cybersikkerhet.

Dette bygger opp til tre forskningsspørsmål:

*Vektlegges usikkerhet i virksomhetenes risikobeskrivelser?*

*Jobber virksomhetene ut fra en felles forståelse av risiko i deres cybersikkerhetsarbeid?*

*Hva er implikasjonene ved eventuelle avvikende risikoforståelser?*

Problemstillingen retter seg mot forskjellige virksomheter som direkte eller indirekte forvalter kritisk infrastruktur i Norge og har en sentral rolle innen cybersikkerheten i den forbindelse. Oppgaven er ikke begrenset til én bestemt sektor eller type virksomhet, men tar heller i sikte å undersøke et bredt spekter forskjellige aktører rundt Norges kritiske infrastruktur. Innholdet i oppgaven vil da kunne fortelle oss noe den grunnleggende risikoforståelsen til en rekke virksomheter med sentrale og omfattende roller og innflytelse på norsk samfunnssikkerhet og statssikkerhet.

Metoden som blir benyttet i denne oppgaven er dokumentanalyse av offentlig tilgjengelige dokumenter fra og om virksomhetene. Det er ikke alltid informasjonen i disse dokumentene vil gi tilstrekkelig eksplisitte svar på det som oppgaven tar sikte på å undersøke, ettersom det dreier seg om rimelig spesifikke spørsmål. Det er derfor noen deler av diskusjonen som vil basere seg på tolkninger av betydning bak det som publiseres. Dette medfører visse begrensinger for hvilke betraktninger og slutninger som kan trekkes i oppgaven på enkelte områder. Dette vil drøftes videre i metodekapittelet.

Det er klarligvis ikke gjennomførbart å utarbeide et utvalg som gjør det mulig å trekke konklusjoner for risikostyringen i hele Norge, men resultatene vil kunne gi et inntrykk av noen mulige fellestrekk og forhåpentligvis vil det bli gjort funn om enkeltvirksomheter av stor betydning som i selv kan ha nytte for samfunnssikkerheten.

Formålet med oppgaven er å bidra til å bygge bro mellom usikkerhetsbasert risikoteori og cybersikkerhet slik det praktiseres i viktige deler av samfunnet. Således ble kritisk infrastruktur et naturlig valg, ettersom virksomhetene tilknyttet dette, er definert av å være av avgjørende betydning for norsk samfunnssikkerhet.

## 1.3 Oppgavens struktur

Kapittel 1 (innledning) gjør rede for bakgrunn, hvor forholdet mellom cyberrisiko og norsk kritisk infrastruktur blir beskrevet. I denne delen vil jeg trekke frem ulike trusselvurderinger fra myndigheter og selskaper som kan knyttes opp mot cyber, samfunnssikkerhet og kritisk infrastruktur.

Kapittel 2 (Teori) tar for seg relevant litteratur fra risikovitenskapen, særlig rettet mot grunnleggende teori rundt forståelse av risiko og usikkerhet. Det er under denne delen kjernen av analysen vil knyttes inn. Videre vil teoridelen ta for seg relevante konsepter knyttet til security risk management. Konseptene som velges ut, er avhengig av hva som fremkommer i empiridelen.

Kapittel 3 (Metode) går inn på metodebruken som oppgaven går frem med. Her vil det bli redegjort for hva slags metodikk som blir benyttet, samt teori om valgt metode. Validitet og reliabilitet bak metoden vil også bli diskutert, med bakgrunn i forskningsteori.

Kapittel 4 (Empiri) vil etter planen dreie seg om innholdsanalyse av dokumenter og rapporter som forteller oss om usikkerhet/risikoforståelsen virksomhetene jobber ut fra. Å se på hvordan de forstår risiko, bruk av sannsynligheter og forventningsverdier, og hvorvidt dette støttes av vurdering av usikkerhet og/eller mer helhetlige risikobeskrivelser, er sentrale temaer som trekkes frem. Hva de sier direkte, hvilke kilder de henviser til og rammeverk de benytter seg av vil kunne gi uttrykk for dette.

Kapittel 5 (Analyse og diskusjon) vil undersøke og trekke frem virksomhetens usikkerhet/risikoforståelse, slik det legges frem i kildene fra informasjonsinnhentingen. Likheter og ulikheter på tvers av virksomhetene vil så bli trukket frem og belyst. Dette vil så bli vurdert i lys av usikkerhetsbasert risikoteori, som trukket frem i kapittel 2.

Kapittel 6 (Konklusjon) vil samle sammen hovedtrekkene fra teori, informasjonsinnsamling, analyse og diskusjon. Hovedfunnene fra disse kapitlene vil bli trukket sammen og oppsummert. De viktigste begrensingene understrekes, og så kjernepoengene som har kommet ut av oppgaven bli belyst.

# 2.0 Teori

I dette kapitlet vil ulik teori som har blitt valgt ut for oppgaven bli redegjort for. Kapitelet vil først bygget opp generelt rundt risikovitenskap og sikkerhetsrisiko, for å bygge opp under videre teori om sikkerhetsrisiko. Videre vil usikkerhetsbasert teori bli redegjort for, først gjennom å gjengi selve konseptet. Deretter vil ulike alternative risikokonseptualiseringer bli gjennomgått. Det mest relevante alternativet som omhandler sannsynlighet og konsekvens vil bli gjennomgått mer i dybden, samt implikasjonene av å anvende denne innenfor sikkerhetssammenhenger.

## 2.1 Generisk risikovitenskap og anvendt risikovitenskap

Risikovitenskap defineres som den mest berettigede kunnskapen om risikoanalyse. Dette omfatter konsepter, prinsipper, tilnærminger, metoder og modeller for risikoanalyse. Risikoanalyse er her et samlebegrep for risikoforståelse, risikovurdering, risikopersepsjon, risikokommunikasjon og risikostyring (Aven, 2022 s. 312).

Det blir i Aven (2022) videre trukket et skille mellom det vi kaller generisk risikovitenskap og anvendt risikovitenskap. Kunnskap om generisk risikovitenskap kan sies å ha handle om risikoanalyse i seg selv. Dette kan for eksempel dreie seg om svakhetene bak å blindt stole på sannsynligheter i risikovurderinger. Dette er grunnleggende kunnskap om risikoanalyse som skal kunne anvendes i alle mulige fagområder, deriblant felles betydning i risikoanalyse innen helse, statistikk og økonomi. Anvendt risikovitenskap handler om å kombinere den generiske risikovitenskap sammen med de andre fagdisipliner, der man utvikler og formidler kunnskap spesifikk for anvendelsesområdet (Aven, 2022). Et eksempel på dette kan vi finne i Selvik & Aven (2019). I denne artikkelen drøftes bruk av nullvisjon innen olje og gass, og hvorvidt visjonen kan anvendes innen produksjonstap (Selvik & Aven, 2019).

## 2.2 Safety eller security?

Som en del av teoretisk avgrensing, vil jeg redegjøre for begrepene «safety» og «security» og hvordan de brukes i sikkerhets- og risikolitteraturen. På norsk bruker vi heller begrepet «sikkerhet» til å omhandle begge to. Det hender at security oversettes til sikring, men det er sjeldent at en ser begrepet “cybersikring” benyttes. Disse begrepene utgjør en viktig nyanse som vi ikke har på norsk. Når vi omtaler safety management og security management, har de begge til felles at det handler om beskyttelse, men hva man beskytter seg mot vil være vidt

forskjellig. Dermed blir håndteringen av de to områdene forskjellige fra hverandre og man benytter seg av ulike rammeverk og konsepter for passende praksis.
Som beskrevet i Jore (2019), blir skillet mellom security og sikkerhet bestemt av om det foreligger en intensjon bak trusselen og hvorvidt den er ondsinnet. Dersom det er en ondsinnet og intelligent intensjon bak trusselen, vil trusselen falle inn under security (Jore, 2019). Safety vil da handle om beskyttelse mot diverse ulykker og naturhendelser. På den andre siden kan vi forstå security til å omhandle trusseltyper som terrorisme og sabotasje. Under security vil vi også finne det aller meste innen cyberrisiko, da de fleste trusler er et resultat av tilsiktede handlinger. Denne oppgaven vil derfor dreie om teori knyttet opp mot security, heller en safety, men vil likevel omtale dette som sikkerhet.
En tydelig forskjell mellom risikostyring innen safety og security kommer til uttrykk i Amundrud et al. (2017), hvor det blir trukket et skille mellom hvordan risiko ofte blir omtalt i safety-kontekst, sammenlignet med i en security-kontekst. Innen safety blir risiko ofte definert som kombinasjonen mellom konsekvenser og assosierte sannsynligheter eller usikkerheter, i tråd med (C, U)-konseptet. Security risiko blir på sin side blir gjerne beskrevet gjennom en trefaktormodell med verdi, trussel og sårbarhet, slik vi ser i PST sin nasjonale trusselvurdering. Det blir imidlertid gjort klart i Amundrud et al. (2017) at (C, U)-konseptet ikke er uforenlig med trefaktormodellene, og at det ikke er nødvendig å skille mellom risikodefinisjonene i security og safety (Amundrud et al., 2017).

## 2.3 Konsekvenser og assosierte usikkerheter

Helt grunnleggende blir risiko som et konsept definert som (C, U) i Aven (2022) og det er dette konseptet jeg sikter til når jeg omtaler *usikkerhetsbasert risikoteori/risikoforståelse/konseptualisering* (Aven, 2022). Vi vil da se på en konkret aktivitet som skal vurderes og C vil stå for de faktiske konsekvensene vi knytter til denne aktiviteten i fremtiden. En vanlig forståelse av risiko er at det handler om negative konsekvenser, men det kan også omhandle positive utfall, ofte referert til som muligheter. Risiko og tilhørende konsekvenser kan da omtales og vurderes uavhengig av verdier hos den enkelte. U i konseptet referer til assosierte usikkerheter (Aven, 2022). Usikkerhet defineres kvalitativt på to måter i SRA sin ordliste på:

- "For en person eller grupper personer, å ikke kjenne til den reelle verdien av en mengde eller fremtidige konsekvenser av en aktivitet

- Uperfekt eller ukomplett informasjon/kunnskap om en hypotese, en mengde eller forekomsten av en hendelse" (SRA, 2018, s. 4)

Mange forbinder risiko med konsekvenser og sannsynlighet. Sannsynlighet er snarere et uttrykk for usikkerhet, men etter forståelse av risiko som (C, U) vil man behandle usikkerhet som et grundigere og bredere tema.
Det er imidlertid i noen sammenhenger hvor bruk av sannsynligheter og kvantitative estimater gjør seg mer passende enn andre. Vi kan trekke et skille mellom frekvenstistisk sannsynlighet og subjektive/kunnskapsbaserte sannsynligheter. Vi kan gjøre regning med at dersom vi har en helt vanlig kortstokk, vil man ha en 1/52 sannsynlighet for å predikere kortet på toppen rett og med det angi en frekvenstistisk sannsynlighet på situasjonen. Dette kan vi eksperimentere på gjennom å forsøke å predikere kortet, legge det tilbake og stokke om. En må riktignok gjennomføre dette eksperimentet svært mange ganger for å kunne få resultater av betydning, men man kan da i teorien teste om man kan forvente å predikere rett hver 52 gang. Sannsynligheten vi da uttrykker betegner andelen rette predikasjoner vi kan forvente dersom vi forsøker dette et uendelig antall ganger. Vi vil i praksis benytte oss av frekvenstistiske sannsynligheter i sammenhenger hvor vi har en tilsynelatende repeterbar og stabil situasjon. Vi må likevel merke oss at vi i disse situasjonene gjør en rekke antakelser som forutsetter at estimatet vårt er passende. Dersom man skal si noe om sjansene for å predikere kortet på toppen av en kortstokk, må vi for eksempel anta at det er 52 kort i stokken, at alle ruterne er i stokken og at alle femmerne er i stokken. Dette er ikke nødvendigvis gitt, men er noe man gjerne tar utgangspunkt i uten å ha undersøkt nærmere.
På den andre siden finner vi den subjektive og kunnskapsbaserte sannsynligheter. Dette vil omhandle en subjektiv vurdering av usikkerheten for at en hendelse frem i tid vil forekomme eller ikke, uttrykt gjennom å angi en sannsynlighet (Aven, 2022). En sannsynlighet på 50% vil innebære at man likestiller usikkerheten med å trekke en blå ball ut av en urne med én blå og én rød ball. Når man skal uttrykke usikkerhet i form av en sannsynlighet i sammenhenger som sikkerhet i fremtiden, er det i all hovedsak denne type sannsynlighet en benytter seg av.

## 2.4 Alternative risikokonseptualiseringer

Akkurat hvordan en definerer risiko i seg selv varierer mye. I Aven (2012) kan vi se en historisk kartlegging av utviklingen av risikokonseptualisering. Kartleggingen omfatter begrepet helt tilbake til 1600-tallet, men denne oppgaven vil rette seg inn på risikoforståelse i nyere tid. Kartleggingen illustrerer seks ulike forståelser (D1-D6) av risikobegrepet siden den tid (Aven, 2012):

- D1 – Risiko som en forventningsverdi. Risikoen vil da omhandle enten forventet tap eller forventet nytte. Dette er en relativt enkel tilnærming til risiko, ettersom man kun står igjen med et enkelt tall som en tallfestet forventning. Dette kan nyanseres litt dersom man forholder seg til forventet nytte, da man også kan ta litt mindre konkrete faktorer med i betraktning.
- D2 – Risiko som sannsynligheten for et tap. Denne definisjonen vil samtidig ikke reflektere nyansene bak ulike grader for konsekvenser, gitt at tapet forekommer. Med utgangspunkt i denne tilnærmingen, er sannsynlighet alene pekt ut som den passende måten å betegne usikkerhet på.
- D3 – Risiko som konsekvenser og assosierte usikkerheter. Dette betegner en retning som har hatt en overgang fra å forholde seg til sannsynligheter, over til å hensynta et bredere perspektiv på risiko gjennom usikkerhetsdimensjonen. Etter det nye perspektivet er sannsynlighet ikke lenger en del av definisjonen, men det kan samtidig benyttes for å bidra til å uttrykke usikkerhet (men ikke som en nødvendighet).
- D4 – Risiko som usikkerhet. Dette innebærer et perspektiv som setter varians og avvik i fokus allerede eksisterende data, som et utgangspunkt for å forstå risikoen fremover i form av en forventningsverdi. Dette kan rette seg mot historisk data for aktiviteten som vurderes eller data fra lignende aktiviteter og benyttes gjerne av økonomer.
- D5 – Risiko som objektiv usikkerhet. Denne retter seg mot sammenhenger vi vi har en kjent og objektiv sannsynlighetsfordeling å forholde oss til og forutsetter målbar usikkerhet. Definisjonen blir «tom» i tilfeller hvor vi forholder oss til subjektive sannsynligheter.
- D6 – Risiko kan defineres gjennom tre ulike perspektiver: (1) Risiko som hendelse eller konsekvens, (2) konsekvenser og assosierte usikkerheter og (3) definisjonen fra ISO «the effect of uncertainty on objectives». Denne brede tilnærming tar sikte på å

være pragmatisk og fleksibel i møte med vidt forskjellige problemstillinger innen risiko (Aven, 2012, s. 39-41).

### 2.4.1 Mer om risiko som sannsynlighet og konsekvens

Blant de seks forskjellige kategoriene, finner vi at D2, som omhandler sannsynlighet og konsekvenser fortsatt er nokså utbredt. Dette kan omfatte både å se på risiko som å bestå av disse to temaene eller at de skal kombineres matematisk gjennom enkel multiplisering. Det kan uttrykkes som (C,P) og (C*P). Dette er vanligere i de mer teknisk- og naturvitenskapelige fagområdene vi finner blant ingeniører, helse og statistikk. Gjennom en slik tilnærming tar man ofte utgangspunkt i at risiko er objektivt og kan måles og utregnes (Lupton, 2013).

### 2.4.2 Mer om alternativer

Vi kan videre se i ISO 31000:2018 (del av D6) at risiko defineres som effekten av usikkerhet på målsetninger (ISO, 2018). Denne definisjonen kritiseres i Aven (2022), men blir den blir samtidig også vist til blant definisjonene av risiko i SRA sin ordliste (SRA, 2018) Det utdypes videre at risiko vanligvis uttrykkes som en kombinasjon av risikokilder, mulige hendelser, konsekvenser og deres *likelihood*. Det blir imidlertid presisert at det med likelihood menes et begrep bredere enn slik sannsynlighet, slik det ofte må oversettes på andre språk (ISO, 2018), deriblant norsk.

Utenfor usikkerhetsbasert risiko, kan man ofte finne definisjoner av sikkerhetsrisiko som ser slik ut (Amundrud et al, 2017, s. 287, min oversettelse):

1. «Risiko = f(verdi, trussel, sårbarhet), hvor f avgir en funksjon
2. Risiko = verdi x trussel x vulnerability
3. Risiko = trussel x (sårbarhet og konsekvens)
4. Risiko = trussel x sårbarhet x konsekvens»

Dette dreier seg om forskjellige måter å illustrere de ulike variablenes forhold til hverandre, med utgangspunkt i en trefaktormodell. Det kommer videre frem i Amundrud et al (2017) at trefaktormodeller ikke behøver å være uforenlig med en usikkerhetsbasert tilnærming til risiko (Amundrud et al. 2017)

### 2.4.3 Svakheter knyttet til (C, P) og ISO-perspektiv

Alle disse definisjonene har til felles at de ikke fanger opp usikkerhet i tilstrekkelig grad. Den tydeligste svakheten med disse tilnærmingene er at kunnskapsstyrken som ligger til grunn for vurderingene av de ulike variablene, ikke blir reflektert som en del av metoden. Dette vil innebære at man etter disse metodene, ikke vil skille mellom et svakt og et sterkt kunnskapsgrunnlag.

Aven og Kristensen (2019) peker på følgende faktorer som kan brukes til å vurdere hvorvidt kunnskapsgrunnlaget er sterkt:

1. «Rimeligheten bak antakelser gjort
2. Mengden og relevansen av data/informasjon
3. I hvilken grad det er enighet blant eksperter
4. I hvilken grad fenomenene involvert er forstått og treffsikre modeller eksisterer
5. i hvilken grad kunnskapen har blitt grundig undersøkt» (Aven & Kristensen, 2019, s. 6, min oversettelse)

I en sammenheng med cybersikkerhet, som er et særlig komplisert og teknisk område, vil det for eksempel være svært begrensende for en passende risikoforståelse, dersom vi ikke skiller på vurderinger gjort av lekfolk og cybereksperter.

Som vi ser blant de overnevnte definisjonene for sikkerhetsrisiko og (C*P)-perspektivet, kan vi se at mange kan omgjøre risiko til et rent kvantitativt tema med matematiske formler. Dette innebærer å omgjøre våre vurderinger av de ulike faktorene til forventningsverdier, vi vil da stå igjen med ett tall å forholde oss til.

Matematiske tilnærminger til risiko ser vi hyppig bruk av i risikomatriser, hvor vi er avhengige av å kategorisere konsekvenser og sannsynlighet. Dette fører til tydelige begrensninger på konsekvensaksen. Aven (2022) peker på at konsekvensene bak en hendelse ofte ikke vil bli passende representert gjennom ett enkelt punkt. Samme hendelse kan ha et bredt spekter av konsekvenser, og med det ha behov for en mer nyansert fremstilling (Aven, 2022).

Eksempelvis kan et vellykket phishing-forsøk både ha alt fra minimale eller ingen konsekvenser for driften, og det kan også åpne døren for et løspengevirus som setter en hel virksomhet ut av spill og medføre enorme tap, slik vi så hos Norsk Hydro i 2019.

Vi kan videre finne en svakhet gjennom å se for oss en normalfordeling bestående av ulike konsekvenser knyttet til en bestemt hendelse. Dersom vi skal derivere én verdi ut av dette, vil

dette tallet kunne være nøyaktig det samme som en helt ulik fordeling, men som har samme sentrum. Hvordan fordelingen faktisk ser ut kan imidlertid være svært viktig informasjon. Fordelingen kan ha formen av en bjelle, mens den andre kan være langt mer horisontal. Den mer horisontale fordelingen kan innebære en betydelig større muligheter for alvorlige og/eller ekstreme utfall, som bør tas med i betraktning (Aven, 2019).
Et annet problem med å behandle risiko som regnestykker er at det kan føre til at ulike reelle forhold mellom ulike faktorer ikke gjenspeiles i formelen. Bruk av risikomatriser med (C*P)-perspektivet til grunn vil for eksempel anta en lineær avstand mellom de forskjellige kategoriene for sannsynlighet og konsekvens. Dette trenger imidlertid ikke å reflektere virkeligheten – i virkeligheten kan de faktisk forholdene være nærmere eksponentielle eller logaritmiske, og alt imellom. Tar man utgangspunkt i en slik misvisende modell, kan det lede at blir overbevist om å rangere ett tiltak over det andre, mens effekten reelt sett er motsatt (Aven, 2015). Vi kan i slike sammenhenger se at upassende bruk av risikoanalysemetoder kan lede til verre enn tilfeldige beslutninger, og med det kunne være verre enn nytteløst (Cox, 2008).

## 2.5 Risiko innen sikkerhet og økonomi

Kjernetemaet i denne oppgaven er forståelse av risiko og usikkerhet. Risiko kan forstås på mange måter. Dette kan være upraktisk, men kan samtidig være nødvendig i sammenhenger hvor man forholder seg til risiko vidt forskjellig. Et typisk eksempel på dette kan være hvordan en porteføljeforvalter tar kalkulerte risikoer med store porteføljer og medfølgende usikkerheter, mens en annen risikoekspert kan jobbe med HMS-risiko ute på en oljeplattform. De har til felles at de begge jobber med risiko, men anvendelsområdene setter tydelig preg på hvordan risiko operasjonaliseres.

Dette leder oss inn på spennet mellom risikoanalyse innen økonomisk styring og risikoanalyse innen sikkerhet. Aven & Vinnem (2007) trekker frem *expected utility theory* (EUT) som helt sentralt innen økonomisk teori. EUT har til hensikt å gi et logisk grunnlag for å ta beslutninger ut fra hvilke alternativer som har størst *forventet nytte*. Med utgangspunkt EUT skal man estimere sannsynligheter og tallfeste nytten bak ett eller et sett med utfall og videre komme frem til forventningsverdier for nytten i alternativene (Aven & Vinnem, 2007).

Videre blir porteføljeteori trukket frem som sentralt i håndtering av økonomisk risiko. Porteføljeteori trekker frem systematisk risiko og usystematisk risiko som konsepter i risikostyring.

Utgangspunktet i dette perspektivet er at man har en portefølje av prosjekter med medfølgende usikkerheter i hver av dem. Systematiske risikoer er risikoer som har innvirkning på hele porteføljen, mens usystematisk risiko er forbundet med risiko som gjelder enkeltprosjekter. Ved tilfeller der antallet prosjekter i porteføljen blir høyere og fordelt på mange nok forskjellige områder, vil den usystematiske risikoen komme til ha mindre og mindre betydning for det samlede resultatet. I slike sammenhenger kan det da være fornuftig å vurdere og håndtere risiko gjennom matematiske formler og forventningsverdier (Abrahamsen et al, 2004).

Hvorvidt risiko gjennom forventningsverdier er en passelig tilnærming i alle sammenhenger, er imidlertid ikke gitt. I Abrahamsen et al (2004) blir det drøftet hvorvidt bruk av forventningsverdier, slik vi blant annet kan se i EUT, benyttes i forbindelse med sikkerhetsstyring (safety). Eksempler på vanlige variabler som blir benyttes innen sikkerhetsstyring er Fatal Accident Rate (FAR), Potential Loss of Life (PLL) og Expected Net Present Value (E[NPV]).

Gjennom artikkelen kommer det frem at bruk av forventningsverdier gjør seg passende under systematisk risiko med en stor og bred portefølje, som et hovedkontor som finansielt sett må forholde seg til fremtidige markedssvingninger. Dette er imidlertid ikke alltid like passende når en vurderer risiko. Risiko knyttet til sikkerhet kan føre til store avvik fra forventningsverdiene festet til ett prosjekt, og dersom porteføljen ikke er stor nok, må usystematisk risiko vektlegges mer. Verdiene som står på spill i ulykker, kan omhandle skade på helse og miljø – enheter som ikke objektivt kan bli gitt en nytteverdi. Konsekvensene som følger en ulykke, kan også være svært uforutsigbare. Vi må ta i betraktning at forventningsverdier må settes basert på en rekke antakelser om fremtiden som kan ha varierende hold i seg (Abrahamsen et al, 2004, s. 351-352).

# 3.0 Metode

## 3.1 Metodologiske hovedtrekk

Metodologisk kan oppgaven beskrives som en serie av case-studier. Case-studier har en sentral posisjon innen samfunnsvitenskapelig forskning. Det er ingen konsensus om én klar definisjon av tilnærmingen, men kan beskrives som en «kritisk, kvalitativ eller anti-positivistisk tilnærming som gjør det mulig å gripe ved det særegne ved mennesker og samfunn» (Andersen, 1997. s 10).

Dette er i hovedsak en kvalitativ oppgave. Mens kvantitative metoder tar i bruk data i form målbare enheter, vil kvalitative metoder rette seg mot informasjon og mening som ikke kan tallfestes eller måles. Oppgaven har til formål å undersøke virksomhetene i dybden og utvikle en helhetlig forståelse av risikoforståelsen, så langt som kildene muliggjør det, og kan sies å for det meste å være forenlig med beskrivelsen av kvalitative metoder beskrevet i Dalland (2017 s. 53).

Den kan imidlertid også ha et visst preg av den kvantitative siden, ettersom noe av oppgaven også kan fungere som en slags «stikkprøve» av denne type virksomheter, og samlet kan funnene gi en indikasjon for andre lignende virksomheter. De skal imidlertid ikke benyttes som grunnlag for videre *statistisk* generalisering for en større populasjon, ettersom dette ikke er passende for case-studier (Yin, 2009). At man tar for seg to, eller en håndfull med case-studier, gjør ikke at en kan se bort fra problemene knyttet til statistisk representativitet (Andersen, 1997). Eventuelle teorier om hvordan øvrige virksomheter forstår og styrer risiko, må alternativt gjøres gjennom *analytisk* generalisering (Yin, 2009).

## 3.2 Oppgavens utvalg

Oppgaven tar sikte på å undersøke risikostyringen av cybersikkerhet tilknyttet kritisk infrastruktur i Norge. Gjennom oppgaven blir fire forskjellige virksomheter undersøkt. Resultatene skal kunne ha vekt i seg selv, da virksomhetene som undersøkes er av stor betydning i seg selv med sentrale roller i norsk samfunnssikkerhet. Videre kan resultatene bidra til å gi oss et inntrykk av hvordan praksisen foregår ellers i virksomheter med lignende roller, men resultatene er ikke ment til å kunne generaliseres ut mot en større gruppe virksomheter. Virksomhetene har blitt valgt ut fra deres relevans til tematikken i oppgaven. Det har ikke vært én bestemt standardisert metode for valg av metoder, men snarere

helhetlige vurderinger rundt virksomhetene og åpne kilder som har avgjort utvalget. Blant vurderingene som la til grunn ble det særlig vektlagt deres rolle og hvorvidt offentlig tilgjengelige publikasjoner gjør det gjennomførbart å besvare problemstillingen. Kriteriene kan oppsummeres slik:

- Virksomhetene betraktes som store (>100 ansatte per NHO sin definisjon)
- Virksomhetenes er forvalter kritisk infrastruktur
- Virksomhetene har en sentral rolle i egen sektor
- Virksomhetene er ansvarlige for sikkerheten i infrastrukturen de er tilknyttet
- Det må finnes offentlige tilgjengelige publikasjoner som
    - Er publisert pålitelige kilder som omhandler virksomhetene eller publisert av virksomhetene selv
    - Omhandler risiko, risikostyring og cybersikkerhet
    - Eksplisitt eller implisitt belyser virksomhetenes risikostyring og risikoforståelse

## 3.3 Fremgangsmåte

Valget av kildene til datainnsamling har primært foregått gjennom søk på relevante nettsider, der virksomhetene omtaler seg selv, eller omtales av andre. De fleste dokumentene kunne undersøkes ved grundig gjennomgang for relevant tematikk, mens andre dokumenter som var lange og tvilsomt relevante, ble det benyttet gjennomgang av innholdsfortegnelse, samt søk på følgende nøkkelord: *usikkerhet*, *risikostyring*, *risikovurdering*, *risiko*, *sannsynlighet* og *kunnskap*.

Valg av teori har vært et resultat av en iterativ prosess, der valg av konsepter som skal brukes til analysen har vært avhengig av hva som har vært å finne av relevant informasjon, og valg av kilder til informasjonsinnsamling har vært avhengig av at det er relevante konsepter innen usikkerhetsbasert risikoteori å evaluere disse opp mot. Følgelig har problemstillingen blitt justert flere ganger gjennom skrivingen.

## 3.4 Metode for analyse og diskusjon

Fremgangsmåten som har vært utgangspunkt for informasjonsinnsamling kan betegnes som dokumentundersøkelse/innholdsanalyse. Jacobsen (2000) peker på tre ulike sammenhenger der det er passende med slik dokumentundersøkelse: (1) når det er umulig eller svært vanskelig å samle inn primærdata, (2) når vi øsker å få tak i hvordan andre har fortolket en viss situasjon eller hendelse og/eller (3) når vi ønsker å få tak i hva mennesker faktisk har gjort og sagt (Jacobsen, 2000. s 163-164). Jeg tenker at de to siste poengene gjør seg særlig relevante for informasjonsinnsamlingen i denne oppgaven.

Da jeg skulle vurdere hva slags metodebruk jeg skulle gå frem med, gikk de første tankene i retning av intervju direkte med utvalgte virksomheter. Det var imidlertid særlig to utfordringer som førte til at jeg foretrakk dokumentundersøkelse: (1) det kan bli utfordrende å snakke ut detaljert om egen sikkerhet til bruk i en oppgave som skal offentliggjøres og (2) å diskutere risiko helt grunnleggende kan bli i overkant abstrakt dersom man har tatt en bestemt risiko for gitt, slik at det blir vanskelig å få frem gode svar fra mennesker utenfor fagområdet. På bakgrunn av dette valgte jeg å gå frem med dokumentundersøkelse som metode, og så kom frem til at virksomhetene oppga god og tilstrekkelig informasjon på de fleste områder dersom man kan trekke slutninger på hva som sies både eksplisitt og implisitt. Det ble derfra vurdert at intervjuprosesser vil medføre lite hensiktsmessige komplikasjoner til oppgaveskrivingen.

Det teoretiske innholdet i kapittel 2 vil anvendes for å vurdere hvorvidt innsamlet informasjon om risikoforståelse er kompatibelt med usikkerhetsbasert risikoforståelse. Teorien drøfter både usikkerhetsbasert risikoforståelse og ulike alternativer, som vil bli brukt til å knytte begreper opp mot ulike momenter som kommer frem av informasjons-innsamlingen, samt medfølgende styrker og svakheter.

## 3.5 Validitet og reliabilitet

Som en del av oppgaven må validiteten og reliabiliteten bak forskningsdesignet vurderes. Yin (2009) trekker frem fire ulike områder som bør vurderes for evaluering av case-studier: (1) konstruktvaliditet, (2) intern validitet, (3) ekstern validitet og (4) reliabilitet.

Yin (2009) peker på tre ting som kan øke konstruktivvaliditeten innen case-studier: flere beviskilder, etablere beviskjeder og få nøkkelinformantene til å gjennomgå utkast til informasjonsinnsamlingen (Yin, 2009). Denne oppgaven vil forholde seg til et begrenset

antall kilder fra hver aktør, da dette oppgaven tar for seg et tema som kan sies å være for de spesielt interesserte. Petroleumstilsynet som case er imidlertid et unntak, da vi kan finne flere og forskjellige typer kilder som underbygger deres forhold til risiko og usikkerhet.

Intern validitet er et tema som blir særlig relevant når formålet med oppgaven er å forklare hvordan og/eller hvorfor x har ledet til y. Denne oppgaven er heller en deskriptiv studie, der vi snarere undersøker y i seg selv, som da vil betegne virksomhetenes risikoforståelse. Videre blir *slutninger* trukket frem som et viktig tema for intern validitet. Hver gang oppgaven omtaler noe som ikke direkte observeres, må det konkluderes på basis av det grunnlaget man har. Man må i disse spørsmålene være kritisk med tanke på om disse slutningene faktisk stemmer, og om alle alternativer har blitt vurdert. Dette blir et særlig viktig tema i de tilfeller der virksomhetene implisitt uttrykker risikoforståelse, og må bli adressert når man skal trekke slutninger i analyse og diskusjon av funnene gjort.

Gjennom å diskutere oppgavens eksterne validitet, kommer vi tilbake til tematikken rundt hvorvidt det er passende å bruke resultatene til generalisering. Ekstern validitet er et typisk utfordrende område for case-studier, da enkelttilfeller eller små utvalg skaper svake generaliseringsgrunnlag. Mens mer kvantitative metoder kan sikte seg inn på statistiske generaliseringer, vil man med case-studier generalisere gjennom analytisk generalisering. Denne oppgaven har imidlertid som formål å studere disse virksomhetene og at funnene om virksomhetene selv skal være av interesse og stå på egne bein, gitt virksomhetenes sentrale roller i norsk sikkerhet. Det er på ingen måte gitt at funnene skal kunne være gjeldende for et større antall virksomheter, og flere virksomheter bør undersøkes dersom en ønsker å skape et mer helhetlig bilde av hvordan praksisen foregår i lignende virksomheter og/eller fagområder i Norge for øvrig.

Reliabilitet omhandler oppgavens *etterprøvbarhet* og hvorvidt en tilsvarende undersøkelse utført av noen andre hadde landet på funn og resultater, med hensikt om å minimere feil og partiskhet fra forfatterens side. Dette vil da handle om å repetere undersøkelsen, og ikke utføre samme metode på nytt med nye aktører (Yin, 2009).

Gjennom informasjonsinnsamlingen er det som nevnt i all hovedsak offentlig tilgjengelige publikasjoner fra virksomhetene selv som blir benyttet. Ved enkelte anledninger blir det benyttet relevant regulering eller forskningsrapporter som omhandler virksomhetene, ment for å supplere det virksomhetene alt har publisert. Med utgangspunkt i slike kilder, er det

etter min vurdering ingen grunn til å feste noe særlig tvil til kildene. Det vil likevel være viktig å presisere skillet mellom det som kommer frem eksplisitt og det som kommer frem implisitt fra kildene. Det som kommer frem implisitt, vil da nettopp være avhengig av en tolkning. Denne tolkningen trenger ikke nødvendigvis å være lik for alle, og det vil derfor være viktig å understreke poenger som baseres på en tolkning og skille de fra poengene som virksomhetene eksplisitt trekker frem selv.

# 4.0 Informasjonsinnsamling

## 4.1 Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) et direktorat som står med et sektorovergripende ansvar for det forebyggende sikkerhetsarbeidet i Norge og er det nasjonale fagmiljøet for cybersikkerhet. Etter 2019 er direktoratet underlagt Justis- og beredskapsdepartementet. (Regjeringen, u.å.a) blant virkemidlene til NSM, driver NSM aktivitet innen rådgivning, tilsyn og kontroll med hensikt om å sikre Norges infrastruktur. Det er også en del av direktoratet kalt Nasjonalt cybersikkerhetssenter (NSCS) som fungerer som et partnerskap mellom offentlige og private virksomheter som skal rette seg direkte mot cybersikkerhet og teknisk sikkerhet (NSM, 2022).
NSM har i utgangspunktet ansvaret for tilsyn for etterlevelse av sikkerhetsloven hos underlagte virksomheter, men i praksis delegeres tilsynsansvaret til relevante tilsynsmyndigheter i sektorene virksomhetene tilhører (BAHR, 2019).

### 4.1.1 NSM - RISIKO

NSM står bak én av de tre trussel- og risikovurderingene som gis ut årlig av de nasjonale sikkerhetstjenestene. Den siste vurderingen fremlagt av NSM heter Risiko 2023 og tar for seg det nåværende trusselbildet Norge står overfor, innenfor deres ansvarsområde.

Risiko som et begrep benyttes svært ofte i denne rapporten. Det gis en mengde med tips om faktorer som bidrar til økt risiko for tiden, slik som økt avhengighet og kompleksitet, bruk av underleverandører, Norges økte ansvar innen energiforsyning og Kina og Russland som trusselaktører. Det blir videre trukket frem en rekke risikomitigerende tiltak som skal kunne bidra til økt kjennskap og håndtering av de viktigste risikomomentene. Rapporten sier imidlertid lite om metodemessige og konseptuelle aspekter ved risiko og usikkerhet i seg selv. Det vi kan implisitt trekke ut fra risikoforståelsen i bunn, er at dette ikke behandles som et strengt kvantitativt tema. Gjennom rapporten blir risiko ikke omtalt gjennom kvantitative estimater, men snarere beskrevet gjennom ord (Risiko 2023).

### 4.1.2 Nasjonalt digitalt sikkerhetsbilde 2022

NSM har også en annen årlig publikasjon som mer direkte retter seg mot digital sikkerhet kalt Nasjonalt digitalt risikobilde 2022. Også i denne rapporten blir risiko et sentralt begrep som stadig knyttes mot aktuelle temaer. Risikoforståelse blir beskrevet som helt avgjørende og

blir på et punkt omtalt i samme setning som usikkerhet, men uten at dette utdypes videre. Begrepet sannsynlighet blir brukt ved flere anledninger, men knyttes aldri direkte opp mot risikoforståelse, og det vises heller aldri til bruk av konkrete sannsynligheter eller sannsynlighetsgrader (NSM, 2022).

I tilsvarende publikasjon for 2021 finner vi også mye av det samme – risiko, risikovurdering og risikostyring som stadig blir omtalt og vektlagt, men uten videre diskusjon av risiko. Videre blir begrepet sannsynlighet benyttet oftere her, og «sannsynligvis» benyttes ved flere anledninger til å beskrive digitale sikkerhetstrusler frem i tid (NSM, 2021). Det er verdt å nevne at nevne at disse påstandene ikke står alene, og underbygges av årsakene til disse vurderingene, men kunnskapsstyrken i seg selv blir ikke eksplisitt karakterisert.

### 4.1.3 Lov om nasjonal sikkerhet (sikkerhetsloven)

Jeg vil trekke frem sikkerhetsloven som et eget relevant tema for å beskrive risikostyringen rundt kritisk infrastruktur. Sikkerhetsloven har som formål å fremme Norges samfunnssikkerhet og statssikkerhet. I henhold til § 1-2 gjelder sikkerhetsloven for offentlige organer på alle nivåer for offentlig organisering. Som en del av endringene fra den eldre sikkerhetsloven, finner vi at andre virksomheter kan nå utpekes til å bli underlagt sikkerhetsloven dersom de:

> «a. behandler sikkerhetsgradert informasjon
>
> b. råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner
>
> c. driver aktivitet som har avgjørende betydning for grunnleggende nasjonale funksjoner.» (Sikkerhetsloven, 2018)

Gjennom disse kravene finner vi at private virksomheter også kan underlegges sikkerhetsloven dersom de oppfyller ett eller flere av de overnevnte kravene. Dette er en av endringene som kom med den nye sikkerhetsloven, som trådte i kraft i 2019.
Videre vil underleverandørene tilknyttet underlagte organer og virksomheter kunne bli underlagt. Særlig punkt C om grunnleggende nasjonale funksjoner (GNFer) blir relevant i denne oppgaven. Sikkerhetsloven definerer GNFer som «tjenester, produksjon og andre

former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2018) Det er også denne definisjonen som blir vist til i NSMs rapport Risiko 2023.

Sikkerhetsloven inneholder også en rekke føringer for hvordan risikostyringen i en underlagt virksomhet skal gjennomføres. Til å begynne med skal NSM legge til rette for informasjonsutveksling for trusler og sikkerhet. Selv utgir NSM, sammen med PST og E-tjenesten, trusselvurderinger for innenfor egne ansvarsområder. Dette kan bidra med å gjøre bidra til å bedre kunnskapsgrunnlaget når virksomheter skal utføre risikovurderinger. Kapittel fire i sikkerhetsloven stiller krav til vurdering av risiko. Etter § 4-2 er virksomheten pålagt til å regelmessig utføre risikovurderinger, som et fundament for forebyggende sikkerhet. De er videre pålagt til å gjennomføre sikkerhetstiltak og øvelser i tråd med risiko vurdert, samt å dokumentere denne prosessen.

Kapittel fem i sikkerhetsloven omhandler informasjonssikkerhet, og gir overordnede føringer på hvordan en underlagt virksomhet skal beskytte skjermingsverdig informasjon. Hvor streng beskyttelsen skal være, bestemmes gjennom et kategoriseringssystem, der vi finner fire kategorier for hvor sensitiv informasjonen er:

a. STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger
b. HEMMELIG dersom det kan få alvorlige skadefølger
c. KONFIDENSIELT dersom det kan få skadefølger
d. BEGRENSET dersom det i noen grad kan få skadefølger. (Sikkerhetsloven, 2018)

Personer som skal ha tilgang på skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere må bli sikkerhetsklarert på nivå tilsvarende graderingen på informasjonen. (Virksomhetssikkerhetsforskriften)
Blant forskriftene som supplerer sikkerhetsloven, finner vi virksomhetssikkerhetsforskriften fra 2019. Denne forskriften stiller ytterligere og mer spesifikke krav til underlagte virksomheter.
Kravene til risikovurderinger tilknyttet beskyttelse av skjermingsverdige verdier utdypes i virksomhetssikkerhetsforskriften § 12:

«Når en virksomhet vurderer risiko, skal den ta hensyn til

a. hvilken betydning virksomhetens skjermingsverdige verdier har for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser
b. hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for
c. sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe
d. hvilke sårbarheter som er knyttet til de skjermingsverdige verdiene
e. konsekvensen av sikkerhetstruende virksomhet for de skjermingsverdige verdiene
f. i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal.» (Virksomhetssikkerhetsforskriften, 2019)

Videre blir krav til håndtering av gitt risiko utdypet i § 13:

«Når en virksomhet skal håndtere en risiko, skal den vurdere

a. om risikoen er akseptabel
b. å endre sårbarheten til de skjermingsverdige verdiene ved grunnsikringstiltak og påbyggingstiltak
c. hvordan virksomheten kan påvirke konsekvensene som kan inntreffe dersom de skjermingsverdige verdiene rammes, for eksempel ved å endre redundansen eller iverksette tiltak for skadebegrensning og gjenopprettelse
d. å gjøre seg mindre avhengig av andre virksomheter
e. å håndtere risikoen på andre måter.» (Virksomhetssikkerhetsforskriften, 2019)

### 4.1.4 Veileder for sikkerhetsstyring

NSM har også publisert i veileder innen sikkerhetsstyring (NSM, 2020). I denne publikasjonen står risiko og risikostyring i sentrum, som en del av sikkerhetsstyringssystemet

underlagte virksomheter er pålagt å ha på plass. Kapittel 2 stiller krav til at virksomhetene må jevnlig og kontinuerlig vurdere risiko knyttet til skjermingsverdige verdier og opprettholde et forsvarlig sikkerhetsnivå i takt med dette. Det blir vist til § 12 og § 13 i virksomhetssikkerhetsforskriften om risikovurdering og risikohåndtering, som blant annet pålegger virksomhetene å foreta sannsynlighetsvurderinger for sikkerhetstruende virksomhet. Lenger ned spesifiseres det at vurdering av sannsynlighet og konsekvens anbefales i flere kapitler (NSM, 2020).

### 4.1.5 Risikovurdering av IKT-systemer

Man kan videre finne en veileder fra NSM for risikovurdering av IKT-systemer. Veilederen er rettet mot ugraderte systemer og kan blant annet anvendes både innenfor IKT og industrielle kontrollsystemer (OT).

Veilederen skriver nærmere om risiko i kapittel 2. Risiko defineres som «usikkerhet rundt måloppnåelse». Risikostyring blir videre definert som å «sikre at virksomheten når sine mål og retter fokus mot de aktiviteter som er mest kritisk for å nå målene», mens risikovurdering som begrep dekker risikoidentifisering, risikoanalyse og risikoevaluering.

NSM diskuterer videre ulike tilnærminger til risiko. Fra Norsk Standard 5814:2008 blir risiko beskrevet som et uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse. Denne definisjonen blir imidlertid beskrevet som utfordrende grunnet bruk av tallverdier for sannsynlighet og konsekvens i forbindelse med svak kunnskapsgrad.

De går videre til å diskutere trefaktormodell for risiko, basert på Norsk Standard 5832:2014, hvor risiko defineres slik: «uttrykk for forholdet mellom truslene mot en gitt verdi og denne verdiens sårbarhet overfor den spesifisert trusselen». NSM foretrekker denne modellen, men har med hensikt utelatt vurdering av sannsynlighet, som ellers kan inngå i en slik tilnærming. Dette blir begrunnet med at tallfesting av sannsynligheten for at en hendelse skal inntreffe, kan være utfordrende (NSM, 2020).

## 4.2 Norges bank

Norges bank er sentralbanken i Norge og er en av de viktigste aktørene i Norges økonomi på nasjonalt nivå. Norges Bank har som hovedformål å fremme finansiell stabilitet og et

effektivt og sikkert betalingssystem. I egen rapport peker de på fire virkemidler i arbeidet mot målene: (1) Overvåke betalingssystemet og annen finansiell infrastruktur og bidra til beredskaps- løsninger, (2) føre tilsyn med interbanksystemer, (3) legge til rette for et stabilt og effektivt system for betaling, avregning og oppgjør mellom foretak med konto i banken og (4) utstede sedler og mynter og sørge for at de kan fungere effektivt som betalingsmiddel (Norges bank, 2022a).
Banken er organisert gjennom tre øvre organer: (1) Representantskap, (2) Hovedstyre og (3) Komite for pengepolitikk og finansiell stabilitet. Underlagt hovedstyret finner vi Norges Bank Investment Management (også kjent som Statens pensjonsfond utland eller Oljefondet), Norges Bank Administrasjon og Norges Bank Sentralbankvirksomheten (Norges Bank, 2022b).

### 4.2.1 Finansiell infrastruktur 2022

Norges Bank har i sin rapport om finansiell infrastruktur 2022 omtalt sentrale aspekter av finansielle tjenester i Norge. Blant de viktigste punktene som tas opp, finner vi cybersikkerheten.
Norges Bank beskriver trusselbildet mot Norges finansielle sektor som alvorlig og økende. Norges egen nasjonalforsamling har blitt utsatt for alvorlige cyberhendelser de siste årene. Vi ser samtidig russiske cyberangrep aktivt bli benyttet i angrep rettet mot kritisk infrastruktur i Ukraina (Norges Bank, 2022c). Dette kan riktignok ikke sammenlignes med hendelsene i Norge, men gi et perspektiv på de sårbarhetene og konsekvensene gjennomdigitaliserte samfunn kan bli introdusert til. Noen av de mest alvorlige sårbarhetene i cyberdomenet er digital kartlegging og sabotasje av kritisk infrastruktur. Dersom infrastruktur rammes, kan dette få konsekvenser for kritiske transaksjonsfunksjoner, samt sensitiv informasjon. Angrepet på SolarWinds fra 2020 understreker farene knyttet opp mot bruk av underleverandører og hvordan dette kan sette digital infrastruktur på spill (Norges Bank, 2022c).

### 4.2.2 Ros (2020)

I vurderingen av trusselbildet blir det vist til en modell fra Ros (2020), som viser den potensielle utviklingen fra en cyberhendelse til en systemkrise. Modellen er trukket ut fra en publikasjon som tar for seg systematisk risiko innen den finansielle sektoren. Jeg vil skrive utdypende om denne publikasjonen, ettersom innholdet i denne kan fortelle oss mye om

Norges Bank sitt syn på cyber risiko og assosierte temaer. Publikasjonen er på engelsk, så de delene som blir referert til er oversatt av meg.

Modellen inndeler forløpet i fire hoveddeler: Kontekst, sjokk, forsterkning og systemkrise. Som en del av kontekstsfasen tar Ros (2020) for seg definisjonen av cyberrisiko. Her kommer det frem at de tar i bruk Expected Utility Theory (EUT) som et utgangspunkt for å definere cyberrisiko. Cyberrisiko blir således definert som et produkt av en hendelses sannsynlighet og tilhørende konsekvenser.
I denne fasen anvender man en sannsynlighetsbasert risikovurdering med følgende formel: cyberrisiko = cybertrussel x sårbarheter x verdier x konsekvenser / mottiltak. Ligningen tar da for seg en estimert sannsynlighet for en hendelse, estimert verdier knyttet til verdier og medfølgende konsekvenser, og eventuelt risikomitigerende tiltak.
Dette er tilsynelatende en rent kvantitativ tilnærming, der man er avhengig av å omgjøre alle faktorene til tallverdier, og man vil til slutt stå igjen med ett tall som skal anslå cyberrisikoen. Det blir imidlertid forklart at tilnærmingen er en matematisk formel, men skal bli brukt for å illustrere faktorenes forhold til hverandre, og ikke bli brukt som en ren kvantitativ tilnærming (Ros, 2020).

Synet på trusler har blitt endret etter hvert som samfunnet har endret seg. I lys av den teknologiske utviklingen blir trusler kategorisert i tre kategorier: (1) naturhendelser, (2) ulykker og (3) villede handlinger. Det blir også vist til en annen tilnærming som kan bidra til å ytterligere nyansere begrepet ved å tillegge det tre dimensjoner: (1) Agent - kilden til trusselen, (2) motiv - villet eller ikke og (3) lokasjon - ekstern eller intern.
Cybertrusler blir kategorisert ytterligere ved menneskelige og ondsinnede handlinger, der man vurderer kapasitet, hensikt og mulighet hos trusselaktøren. Et venndiagram bestående av de tre faktorene benyttes for å kunne karakterisere status på risikoen.

Artikkelen har en egen seksjon som adresserer usikkerhet som et eget tema. Usikkerhet blir beskrevet som en noe man knytter til ufullkommen eller ukjent informasjon. Usikkerhet kan deles inn i to hovedkategorier: «known unknowns» og «unknown unknowns». Sistnevnte beskriver en grunnleggende uvitenhet, begrensing av kunnskap eller uforutsigbarhet knyttet til fremtiden.
(1) Tvetydighet - usikkerhet knyttet til sannsynlighet, grunnet manglende informasjon
(2) Epistemisk - ufullkommen informasjon eller kunnskap

(3) Aleatorisk - iboende variasjon i det som undersøkes
(4) Interaksjon - uforventet interaksjon mellom flere hendelser, som hver for seg kunne vært forutsett (Ros, 2020. s 34-35)

Usikkerhet blir så trukket frem noe som kan begrense tilliten en har til egne beslutninger når en jobber ut fra utilstrekkelig informasjon eller eventuelle konsekvenser er uklare. Man må da lene seg på subjektiv dømmekraft. Som et resultat kan man oppleve at involverte blir svært lite risikovillige, som kan lede til uforutsigbare beslutninger og såkalt «herding behaviour», som igjen kan lede til økt volatilitet under sikre side (Ros, 2020).
Videre skrives det at avhengigheten finanssektoren har til informasjon fører til muligheter for trusselaktørene. Trusselaktørene kan forsøke å kontrollere eller manipulere informasjonene som når beslutningstakere i virksomhetene. Dette er ventet å bli en økende utfordring fremover, som kan føre til økt usikkerhet og mer utnyttelse av vellykkede cyberangrep (Ros, 2020).

### 4.2.3 TIBER-NO

Norges Bank jobber nå med å ta i bruk et nytt rammeverk kalt TIBER-NO (Norges Bank, 2022b), en norsk implementering av en TIBER-EU, et rammeverk utarbeidet av EUs sentralbank. TIBER står for Threat Intelligence-based Ethical Red Teaming. Dette er et rammeverk som benyttes til å øve seg på å håndtere cybertrusler fra reelle trusselaktører gjennom såkalt «red teaming». Dette innebærer å øve på cyberhendelser gjennom å simulere trusselaktørene, og skal bidra til å hjelpe en virksomhet med å vurdere egen cybersikkerhet. Slike øvelser vil teste virksomhetene i fulle scenarioer og vil utgjøre en mer helhetlig test, sammenlignet med penetrasjonstester (ECB, 2018).
I selve rammeverket blir risiko tatt opp ofte. Risiko blir i første omgang hyppig omtalt i forbindelse med risiko knyttet til testene i seg selv, slik som risiko for at testene utføres på feil premisser. Videre er kapittel 6 dedikert til risikostyring for TIBER-tester. Det kommer frem at risikoer knyttet til personer, systemer og prosesser i testen blir identifisert, analysert og mitigert. En risikovurdering bør gjennomføres i forkant og etablere forhåndsregler for risikostyring gjennom tester. Det blir i en rekke andre sammenhenger nevnt begreper som risiko, risikovurdering, risikostyring og risikomitigering, men uten å gå nærmere inn på metodikk eller risikoforståelse (ECB, 2018).

### 4.2.4 NBIM - policies

NBIM har på sin side også publisert noen policies som tar for seg informasjonssikkerhet, sikkerhet og risikostyring. Her blir bruk og viktigheten av risikostyring trukket frem, men utdypende informasjon om tilnærming til risiko i seg selv blir ikke gjennomgått i dybden (Norges Bank, 2022)

## 4.3 Petroleumstilsynet

Sikkerheten innen norsk olje- og gassvirksomhet har i det siste vært et hyppig omtalt tema, særlig gjennom det siste året. Dette har blitt av interesse for denne oppgaven, da norsk olje- og gassvirksomhet har blitt omtalt som kritisk infrastruktur ofte det siste året, i takt med at geopolitiske spenninger har blitt verre og mistanker om spionasje har blitt et stort tema. Eksempelvis kan vi se olje- og gassrørledninger bli betegnet som kritisk infrastruktur i en artikkel fra regjeringen om NATO og sikkerhet (Regjeringen, 2022). Norsk olje og gass benytter seg også i svært stor grad av OT-teknologi til å utføre omfattende operasjoner, hvilket medfølger dramatiske sårbarheter, skal vi tro en forskningssjef fra Sintef Digital, som har hevdet at muligheten for å sprenge en oljeplattform ved å overta kontrollsystemene på land har blitt en reell risiko (DN, 2022).
Vi kan videre på denne sektoren i lys av områdene for kritisk infrastruktur i NSB sin karlegging. I kategoriene for forsyningssikkerhet og kraftforsyning blir forvaltningsorganer og selskaper knyttet til olje trukket frem under «ansvar og involverte» (DSB, 2016).

Sentralt bak myndighetene som regulerer petroleumsvirksvirkosomhetene i Norge, finner vi Petroleumstilsynet. Petroleumstilsynet har nylig blitt underlagt Olje- og energidepartementet og har ansvaret for å legge premisser for oppfølging av sikkerheten hos regulerte virksomheter (Regjeringen, u.å.b). Petroleumstilsynet er også et direktorat som utvikler og formidler kunnskap om egne fagområder, som da vil omfatte veiledning til risikostyring og sikkerhet (Petroleumstilsynet, u.å).

### 4.3.1 Risikobegrepet i petroleumsvirksomheten

Petroleumstilsynet har publisert et eget dokument som direkte adresserer risikobegrepet, hva vi legger i det og hvordan det bør brukes. Dokumentet motiveres av at det årlig skjer hendelser som har hatt potensiale til å utvikle seg til storulykker, og at virksomhetene alltid må ivareta hensyn til forsvarlighet og kontinuerlig forbedring av sikkerhet.

Petroleumstilsynet ønsker å bidra til dette gjennom å øke risikoforståelse. Det blir trukket frem to sentrale aspekter bak risikobegrepet: (1) usikkerhet om konsekvensene og (2) konsekvenser av virksomheten. Dette formuleres videre til at «risiko er konsekvensene av virksomheten, med tilhørende usikkerhet (Petroleumstilsynet, 2016. s 7).
Petroleumstilsynet diskuterer videre bruk av sannsynlighet i risikobegrepet, men at dette er en del av det «tidligere risikobegrepet». Erfaringer har vist et behov for å unngå slike «mekaniske» vurderinger av risiko, fordi usikkerheter kamufleres av slik praksis. Sannsynligheter er imidlertid ikke nødvendigvis uheldig å bruke. Gitt en mer helhetlig forståelse av usikkerheten rundt, kan sannsynligheter utgjøre et godt bidrag til å beskrive risiko i sammenhenger så høy usikkerhet at angivelse av sannsynlighet er meningsløst. Med det «nye risikobegrepet» vil man tidvis operere med sannsynligheter, men oppmerksomheten rettes mer mot hva sannsynlighetene inneholder. (Petroleumstilsynet, 2016)
Petroleumstilsynet går nærmere inn på usikkerhet rundt konsekvensene som tilknyttet risikobegrepet. Risiko blir beskrevet som mangel på informasjon, manglende forståelse eller kunnskap. Dette kan rette seg mot effekter av virksomheten, eksisterende og potensielle tilstander, bruk av modeller, antakelser og risikoreduserende tiltak. Det nevnes to spørsmål en kan stille seg for å vurdere usikkerhet knyttet til en beslutning: (1) Har vi tilstrekkelig kunnskap til å ta en god beslutning? og (2) Hvordan ta gode besleutninger i lys av usikkerheten som eksisterer? (Petroleumstilsynet, 2016. s 8).

### 4.3.2 Integrert og helhetlig risikostyring i petroleumsindustrien

Petroleumstilsynet har selv publisert en rapport i 2018 som tar for seg viktigheten av og gjeldende prinsipper for risikostyring innen norsk petroleumsvirksomhet. Rapporten har til formål å bidra til god balanse mellom god sikkerhet og god økonomisk verdiskapning, og peker også på at disse ofte går hånd-i-hånd. Risikostyring blir trukket frem som løsningen på å finne denne balansen. Rapporten retter seg imidlertid ikke direkte mot cybersikkerhet, men snarere risikostyring i seg selv (Petroleumstilsynet, 2018).
Petroleumstilsynet skriver at usikkerhet handler om mangel på kunnskap og at man følgelig må «Tvile seg frem til større forståelse av usikkerhet» (Petroleumstilsynet, 2018. s 14).
Usikkerhet blir i kapittel 3 trukket frem som en hovedkomponent av risikobegrepet, og det blir vist til krav fra § 17 i styringsforskriften om risikoanalyse, hvor det foreligger krav om vurdering av usikkerhet. Usikkerhetsbegrepet vil videre redegjort for. Usikkerheten vil handle om hva som kan skje, hyppigheten, årsaker og konsekvensene som følger.

Kunnskapsstyrken er et sentralt moment som må vurderes. Den kan være god eller mindre god og må klargjøres når man skal ta hensyn til usikkerhet. Dersom dette ikke hensyntas, vil dette kunne føre til at beslutninger fattes basert på et urealistisk bilde av risiko. Når en avgjør hvilken kraft risikovurderingene skal ha, bør kunnskapsstyrken vektlegges. Når enn man gjør en vurdering eller fatter en beslutning knyttet til fremtiden, må dette baseres på en rekke premisser og antakelser. Mengden og kvaliteten som ligger til grunn for disse antakelsene, kan variere. De kan også være helt feil. Gjennom å hensynta usikkerheten og vurdere kunnskapen, kan man adressere og ta høyde for medfølgende svakheter, feil og mulige overraskelser (Petroleumstilsynet, 2018).

### 4.3.3 Styringsforskriften

Også i styringsforskriften som gjør seg gjeldene for petroleumsvirksomhet, kan vi se behandling og risiko stå som et sentralt og gjennomgående tema for å sikre mennesker, miljø og materiell. Denne forskriften retter seg også mot risikostyring i seg selv, og ikke direkte mot risikostyring av cybersikkerhet.

Kapittel 2 tar for seg risikostyring hos underlagte virksomheter. § 4 setter krav til at virksomhetene skal velge løsninger og barrierer og som reduserer sannsynligheten for uønskede hendelser. Disse skal velges ut fra enkeltvis og samlet vurdering.

I § 9 ser vi at krav til akseptkriterier til risiko for blant annet personellrisiko. Operatørene skal sette disse selv – ikke myndighetene. Akkurat hvordan et risikoakseptkriterium kan settes kan variere, både kvalitativt – for eksempel gjennom en forventningsverdi eller en ALARP-tilnærming. Gjennom en evaluering av bruk av akseptkriterier (Proactima, 2020) ser vi at akseptkriteriene fungerer i praksis gjennom at bransjen typisk fastsetter et statisk kvantitativt mål på forventet Fatal Accident Rate (FAR-verdi). Forventet FAR-verdi uttrykker antall forventede dødsfall per 100 millioner eksponerte timer og et risikoakseptkriterium vil sette et øvre tak på dette (Proactima, 2020). Fra Preventor (2021) kommer det frem at tilnærmet alle norske operatører fastsetter de samme FAR-verdiene for de ansatte generelt og de mest eksponerte gruppene på henholdsvis 10 og 20. Disse har heller ikke endret seg på i overkant av 20 år, til tross for at sikkerhetsnivået har blitt betydelig bedre (Preventor, 2021).

Som nevnt ovenfor, finner vi også i § 17 krav til bruk av risikoanalyser. Risikoanalysene skal gi et nyansert og helhetlig bilde av risikoen. De skal videre ta for seg storulykkerisiko og

miljørisiko som følger aktivitetene hos virksomheten. Det stilles videre enn rekke mer konkrete krav til innholdet i risikoanalysene:
«Risikoanalysene skal

a. identifisere fare- og ulykkessituasjoner,

b. identifisere initierende hendelser og klarlegge årsakene til hendelsene,

c. analysere ulykkessekvenser og mulige konsekvenser, og

d. identifisere og analysere risikoreduserende tiltak, jf. rammeforskriften § 11 og denne forskriften § 4 og § 5.

Risikoanalyser skal utføres og inngå som en del av beslutningsgrunnlaget, blant annet når en skal

a. identifisere behovet for og funksjon til nødvendige barrierer, jf. § 4 og § 5,

b. identifisere spesifikke ytelseskrav til barrierefunksjoner og barriereelementer, herunder hvilke ulykkeslaster som skal legges til grunn for utforming og drift av anlegget/innretningen, systemer og/eller utstyr, jf. § 5,

c. utforme og plassere områder,

d. klassifisere systemer og utstyr, jf. aktivitetsforskriften § 46,

e. vise at hovedsikkerhetsfunksjonene ivaretas,

f. fastsette operasjonelle betingelser og begrensninger,

g. velge definerte fare- og ulykkessituasjoner.» (Styringsforskriften, 2010. § 17)

### 4.3.4 SINTEF – regulering av IKT-sikkerhet

SINTEF har 2021 publisert en rapport som omhandler regulering av IKT-sikkerhet i petroleumsindustrien (SINTEF, 2021). Rapporten tar for seg gjendelende regelverk og forventningene fra myndighetenes side for IKT-sikkerhet i petroleumssektoren.

I petroleumssektoren trekker man et skille mellom to hovedområder for cyberteknologi: IT og OT. Enkelt forklart går skillet mellom IKT-teknologien som benyttes i kontorsammenheng

(IT), mens IKT-teknologien som benyttes direkte i industriell sammenheng (OT). Skillet mellom disse teknologiområdene går mellom en såkalt demilitarisert sone, som illustrert i rapporten. På hver sin side av denne kan vi finne kontor/IT på IT-siden, og drift, kontroll, prosess – logikk og prosess felt på OT-siden. OT skiller seg fra IT ved at OT medfører fysiske endringer knyttet til utstyr og prosesser, og blir da også omtalt som industrielle IKT-systemer. Det pekes på at det ikke er noen entydig definisjon på IKT-sikkerhet, men at sikkerhetsmålene i en NOU fra 2018 uttrykkes gjennom CIA-konseptet - konfidensialitet, integritet og tilgjengelighet. Prioriteringen av disse tre områdene er imidlertid ulik for IT og OT.  Dette delkapittelet retter seg mot sikkerhet innen både vanlig IT og OT innen norsk petroleumsvirksomhet (STINFEF, 2021).

Rapporten dekker videre bakgrunn og trusselbildet for sektoren. Med tanke på risikobildet for cybersikkerhet, er petroleumsvirksomhet i Norge blant de særlig utsatte områdene. En trusselvurdering fra E-tjenesten viser at nettangrep kan rette seg mot industrielle kontrollsystemer, og med det virke inn på fysiske systemer og prosesser i virksomhetene. Det pekes på at Regjeringen har i Nasjonal strategi for digital sikkerhet (2019) formulert tre forventninger til cybersikkerhetsarbeider: (1) virksomheter skal ha en risiko basert tilnærming til digital sikkerhet, (2) myndigheter og virksomheter deler informasjon og kunnskap om trusler, sårbarheter, hendelser og tiltak og (3) myndighetene bistår virksomhetene med råd og veiledning for å bidra til kunnskapsgrunnlaget til virksomhetene (SINTEF, 2021).

Begrepet «risikobasert» forklares videre i rapporten. Begrepet innebærer ikke at man utelukkende baserer beslutninger på analyser og vurderinger av risiko, men heller at styringen skal være *risikoinformert.* SINTEF går videre inn på forsiktighetsprinsippet, som kommer til anvendelse fordi man legger til grunn at risikovurderinger har sine begrensninger og svakheter. Med dette som utgangspunkt, blir kunnskap og usikkerhet i forutsetningene vektlagt i regelverket, slik som i § 11 av rammeforskriften, peker på en tilnærming til risiko der en fokuserer på usikkerhetsaspektet av begrepet (SINTEF, 2021).

I delkapittel 1.4 blir det listet opp en rekke definisjoner på ulike begreper som benyttes i rapporten. Blant dem finner vi definisjon på risiko, som er hentet fra Petroleumstilsynet. Definisjonen på risiko går slik: «konsekvensene av virksomheten med tilhørende usikkerhet» (SINTEF: 2021. s 9) og viser til en veileder fra Petroleumstilsynet som referanse. Usikkerhet blir videre definert slik: «dreier seg om mangel på informasjon, manglende forståelse eller mangel på kunnskap» (SINTEF, 2021. s 9).

## 4.4 Telenor

Telenor er Norges største leverandør av digitale tjenester innen mobil, fastnett og TV-tjenester. Selskapet er en kommersiell aktør innenfor elektroniske kommunikasjonsnett og -tjenester, og både største tilbyder og infrastruktureier. Selskapet har tilknytning svært mange områder på DSB sin oversikt over kritisk infrastruktur, men kan hovedsakelig plasseres under elektroniske kommunikasjonstjenester, inn under samfunnets funksjonalitet. I samme oversikt blir Telenor maritim radio navngitt i forbindelse med redningstjeneste, og infrastrukturen kobles til funksjonaliteten av andre kommersielle teleoperatører og Nødnett, som blant annet er avgjørende for kommunikasjon for nødetatene (DSB, 2016). Selskapet er børsnotert, samtidig som staten eier i overkant av halve selskapet (Regjeringen, u.å.c).

### 4.4.1 Telenor – Digital sikkerhet

I likhet med de overnevnte sikkerhetstjenestene, publiserer også Telenor en sikkerhetsrapport på årlig basis. Den siste i skrivende stund tar for seg trusselbildet i 2022. Rapporten adresserer mange av temaene vi ser fra de andre trusselvurderingene. Vi står overfor et nytt verdensbilde nå som krig har brutt ut i Europa, og vi må som følge derav gjøre regning med høyere usikkerhet knyttet til evne og vilje hos russiske aktører. Vi ser en stadig økning av cyberkriminalitet, samtidig som kjente sårbarheter blir flere. Alt dette akselereres av en teknologisk utvikling som ikke viser tegn til å avta. Behovet for å håndtere usikkerhet i en volatil verden understrekes (Telenor, 2022).

Fra tilsvarende rapport året før, viser Telenor til en pyramide som kartlegger de ulike trusselaktørene. Fra topp til bunn, rangeres de slik: (1) Stater, (2) kontraktører, (3) organisert kriminalitet, (4) politisk motiverte «hacktivister og (5) enkeltkriminelle og svindlere. Trusler kan også komme gjennom samarbeid på tvers av de forskjellige nivåene (Telenor, 2021. s. 23).

Telenor går nærmere inne på risiko og risikoforståelse i kapittel 2 i 2022-rapporten. "Tradisjonelle" risikovurderinger er ikke lenger tilstrekkelig for det digitale domenet, og det er blitt behov for mer helhetlige tilnærminger til digital sikkerhet. I takt med at kompleksiteten øker, øker også behovet for å utvikle ny kunnskap. Det redegjøres for beslutningsgrunnlaget for risikostyring, som skal inneholde en beskrivelse av omfang, kontekst og kriterier, samt en risikovurdering som består av identifikasjon, analyse og

evaluering av risiko. Virksomhetene vil så vurdere videre akseptabel risiko og eventuelt risikomitegerende tiltak.

Sannsynlighet som begrep benyttes knapt gjennom hele rapporten, og brukes ikke til å betegne risiko. En seksjon i kapittel 2 tar for seg usikkerhet og er relevant nok til at det er verdt å gjengi i sin helhet:

«En grunnleggende usikkerhet i risikovurderinger er at vi ikke kjenner fremtiden. Trusselbildet er dynamisk og kan endre seg raskt på grunn av ytre faktorer slik som politisk klima, trusselaktørers intensjoner og evner og nye sårbarheter som kan utnyttes. Denne usikkerheten presenteres gjerne i form av sannsynligheter for hva som kan skje og tilhørende konsekvenser.

Det er usikkerhet knyttet til kunnskapsgrunnlaget for analysen. Relevant informasjon er historiske data og erfaringer og eksperimenter og modell- data i eksempelvis konsekvensvurderinger. Kilder til usikkerhet ligger i selve datagrunnlaget, men også at modeller eller data ikke er tilgjengelig. I mange tilfeller inngår eksperters vurderinger. Det kan være større eller mindre grad av enighet mellom eksper- tene, og subjektive ekspertvurderinger kan være påvirket av menneskelige faktorer, partiskhet og gruppedynamikk. Som nevnt tidligere, lar komplekse systemer seg ikke beskrive ved enkeltkomponenter og oversiktlige sammenhenger mellom dem. Dette gir usikkerhet knyttet til systemforståelsen og interne og eksterne avhengigheter og sammen- koblinger, der også tid er en kritisk faktor. På grunn av kompleksitet kan det være nødvendig å gjøre antakelser og avgrensninger som representerer til dels sterke forenklinger. Samlet sett kan disse usikkerhetsfaktorene gi et kunnskapsgrunnlag som er ufullstendig og skjevt. En systematisk vurdering av usikkerhet og hvor godt kunnskapsgrunnlaget er, må inngå og kommuniseres overfor beslutningstakerne.» (Telenor, 2022. s 9).

Føre-var-tilnærming blir videre nevnt i forbindelse med risikohåndtering. Kompleksitet og usikkerhet som vi nå har sett en drastisk økning av, vil innebære et økt behov for resiliens. Der vi finner meget høy usikkerhet, samtidig som det dreier seg om meget alvorlige konsekvenser, kan føre-var bli en nødvendig risikohåndteringsstrategi. Det kan for eksempel innebære å fatte beslutninger målrettet mot å redusere avhengigheter, slik at et eventuelt bortfall ikke fører forutsette og uforutsette konsekvenser for virksomheten (Telenor, 2021).

Gjennom 2021-rapporten ser Telenor ut til å gi uttrykk for en annerledes forståelse av risiko. Risiko, risikovurderinger og risikostyring omtales hyppig gjennom hele rapporten. Holistisk

og risikostyrt tilnærming til sikkerhet vektlegges, men usikkerhet utover sannsynlighet blir ikke tydelig adressert.

## 4.5 Oppsummerende tabell for virksomhetenes risikoforståelse

Videre følger en tabell som oppsummerer kjernefunnene i informasjonsinnsamlingen som vil tatt opp videre i analyse og diskusjon. Tabellen tar for seg hver av de fire virksomhetene og hvorvidt de (1) viser at de vektlegger risikostyring, (2) om de implisitt eller eksplisitt konseptualisere risiko og (3) hva er hovedtrekkene i risikokonseptualiseringen? Den siste kolonnen er basert på neste kapittel.

| Virksomhet | Vektlegging av risikostyring | Konseptualisering av risiko | Forståelse av risiko i tråd med (C,U) – konsekvenser og assosierte usikkerheter? |
|---|---|---|---|
| NSM | Klart vektlagt i flere publikasjoner | Ingen tydelig eksplisitt konseptualisering | Bruk av sannsynlighet i forskrift. Denne blir også henvist til i veileder – gir uttrykk for et (C, P)--perspektiv |
| Norges Bank | Klart vektlagt gjennom rapport og bruk av rammeverk | Ingen tydelig eksplisitt konseptualisering | Bruk av sannsynlighet uten videre forklaring – kan tyde på (C, P) -perspektiv |
| Petroleumstilsynet | Klart vektlagt i flere publikasjoner | Klare eksplisitt konseptualisering | Tydelig definerer risiko som konsekvenser med tilhørende usikkerhet – i tråd med (C,U) |
| Telenor | Klart vektlagt i rapport | Risiko konseptualisere, men noe utydelig | Knytter usikkerhet og vurdering av kunnskapsgrunnlag til å tenke nytt på risiko – tyder på (C,U) |

# 5.0 Analyse og diskusjon

Dette kapittelet vil bestå av en analyse og diskusjon av informasjonen samlet inn i kapittel 4. Først vil fokuset på risiko hos virksomhetene bli gjennomgått, hvor det også blir vist til hvor dette kommer fra. Deretter vil perspektivene på risiko bli redegjort for, både eksplisitt og implisitt, slik det har kommet frem hos virksomhetene. Risikoperspektivene som virksomhetene har gitt uttrykk for, vil så bli gjennomgått og diskutert i lys av teorien lagt frem i teorikapittelet, med hensikt om å besvare hvorvidt perspektivene er forenlig med teorien. Implikasjonene av dette vil så bli diskutert i neste delkapittel. Avslutningsvis vil oppgavens validitet og reliabilitet bli drøftet mer konkret.

## 5.1 Hovedtrekk i funnene

### 5.1.1 Vektlegging av risiko

I samtlige virksomheter undersøkt i kapittel 4, kan vi se at risiko som begrep, samt relaterte begreper som risikostyring og risikovurdering, er et gjennomgående sentralt tema innen cybersikkerhetsarbeidet.

Det tydeligste eksempelet på dette er NSM sin årlige publikasjon med navngitt «Risiko». Dette vektlegges videre gjennom de andre publikasjonene undersøkt i oppgaven, samt reguleringer som sikkerhetsloven og virksomhetssikkerhetsforskriften, hvor en finner krav til jevnlige risikovurderinger, samt innholdet i vurderingene.

Fra Norges Bank var det særlig tre kilder av interesse for oppgaven: (1) rapport om finansiell infrastruktur (2022), (2) Ros (2020) og (3) rammeverket TIBER. Alle tre har til felles å diskutere risiko knyttet til trusselaktører hyppig, samt omtale risikostyring som sikkerhetsstrategien. I tillegg finner vi Norges Bank sine veiledere for risikostyring og sikkerhetsstyring blant deres policier. Til tross for at risikoforståelse ikke redegjøres for, signaliserer en egen veileder for risikostyring et klart fokus på risiko.

Petroleumstilsynet har selv flere publikasjoner som direkte tar for seg viktigheten av risikoforståelse og hvorfor vi driver med risikostyring. Blant mange relevante kilder, gjør veilederen for integrert og helhetlig risikostyring seg særlig relevant.

Hensikten med å trekke frem bruk og vektlegging av risiko hos virksomhetene er å tydeliggjøre relevansen og viktigheten å ha en klar, ryddig og passende konseptualisering og

tilnærming til risiko. Forståelse av risiko en legger til grunn vil ha betydelige implikasjoner for hvordan en vurderer og styrer risiko. Når det er et klart mønster av at risiko, risikovurderinger og risikostyring omtales såpass ofte i sikkerhetsarbeidet, er det tydelig at virksomhetene vil ha fordel av en passende og felles definisjon av risiko i bunn.

### 5.1.2 Risikoperspektiv hos virksomhetene

Gjennom kildene jeg har funnet for NSM, er det utfordrende å finne en klar konseptualisering av risiko. At NSM har en utfyllende rapport kalt «Risiko», men uten å klart definere hva de legger i begrepet, er noe påfallende. Blant funnene er det noe som tyder på at de ikke er konsekvente i hvordan de forholder seg til risiko. På den ene siden kan vi finne et fokus på sannsynligheter i sammenhenger hvor andre aspekter ved konteksten bak beskrives, men kunnskapsstyrken ikke adresseres. Rapportene Risiko 2023 og Nasjonalt digitalt sikkerhetsbilde 2021 og 2022 er eksempler på dette. Det er imidlertid noen nyanser bak det norskesannsynlighetsbegrepet, som beskrevet i teorikapittelet, nemlig at dette ikke skiller mellom det vi på engelsk forstår som «likelihood» og «probability». Med andre ord trenger ikke sannsynlighet i disse sammenhengene å referere til en rent kvantitativ verdi, men kan også vise til en kvalitativ klassifikasjon, som i sammenhenger hvor beskrivelser av risiko utover å kun estimere risiko, kan være mer passende.

Vi ser videre et uttrykt fokus på sannsynligheter gjennom sikkerhetsloven og virksomhetssikkerhetsforskriften, hvor NSM står på reguleringssiden. Kapittel 5, som omhandler ulike graderinger kan være for å legge premissene for risikostyring av informasjonssikkerhet, der man kategoriserer ulike konsekvensgrader for GNFer i Norge. Det blir videre i virksomhetssikkerhetsforskriften stilt krav til vurdering av risiko i forbindelse med skjermingsverdige verdier i §12. Underlagte virksomheter skal vurdere deres betydning for landets GNFer, sårbarheter, trusler og mulige konsekvenser, men mest interessant for oppgaven er kravet om å vurdere *sannsynlighet* i § 12 c). Relevansen av denne reguleringen understøttes også av at de er forholdsvis nye (2019), samt at en veileder fra 2020 viser til § 12 i veiledning for risikostyring.

NSM sin diskusjon av risiko kan imidlertid gi inntrykk av en mer nyansert forståelse av risiko. I deres veileder om risikovurdering av IKT-systemer, definerer NSM risiko som

«usikkerhet rundt måloppnåelse», som muligens er ment til å samsvare med risikodefinisjonen gitt av ISO (D6) av de ulike risikokonseptualiseringene i teorikapittelet.

NSM går nærmere inn på bruk av sannsynligheter i risikovurderinger knyttet til sikkerhet. De peker på en forståelse fra Norsk Standard som definerer risiko som kombinasjon av sannsynlighet og konsekvens. NSM påpeker at bruk av sannsynlighet og konsekvens i tallverdier kan være utfordrende i tilfeller med lav kunnskapsstyrke. NSM foretrekker å benytte seg av en trefaktormodell, hvor de har unnlatt å inkludere sannsynlighet, grunnet vanskeligheter med å tallfeste sannsynlighet for at en hendelse inntreffer. Akkurat hva NSM mener med det første utsagnet er noe tvetydig – det kan både bety at NSM mener at sannsynlighet ikke bør benyttes, og at kun at det ikke skal kvantifiseres. Med tanke på hva de skriver under trefaktormodellen, tyder det på at bruk av sannsynligheter i selv bør unngås.

I Norges Bank var det noe mer knapphet på kildene som kunne fortelle oss noe om risiko og cybersikkerhet. Informasjonsinnsamlingen har i hovedsak blitt sentrert rundt innholdet i rapporten deres om finansiell infrastruktur (2022). Det er heller ikke en klar eksplisitt konseptualisering i denne rapporten.

Rapporten beskriver risikobildet rundt cybersikkerhet og trekker i den anledning frem en modell basert på Ros (2020). Modellen beskriver forløpet fra en cyberhendelse frem til en systemkrise. I denne modellen er sannsynlighet et av momentene som trekkes frem under cyberrisiko, sammen med sårbarhet. Cyberrisiko beskrives som økende, men uten forklaring på hva de legger i dette eller uttrykk for evaluering av usikkerhet eller kunnskapsstyrke.

Norges Bank sin anvendelse av Ros (2020) gjør at vi videre implisitt kan trekke ut noe om deres tilnærming til risiko, gjennom innholdet i denne artikkelen. Rapporten, som omhandler systematisk risiko i den finansielle sektoren. Når cyberrisiko skal defineres i rapporten, blir det tatt utgangspunkt i EUT og det leder til en forståelse av risiko som sannsynlighet og konsekvenser. Det blir videre foreslått en sannsynlighetsbasert risikovurdering bestående av en i utgangspunktet matematisk ligning. Man vil i en slik sammenheng bruke forventningsverdier for å sette opp ligningen samt stå igjen med en forventningsverdi som en

slags «risk score» for å uttrykke risiko. Tilnærmingen blir imidlertid nyansert noe ved at det påpekes at tilnærmingen ikke er strengt kvantitativ.

Ros (2020) dedikerer videre et eget delkapittel til å redegjøre for og diskutere usikkerhet. Fokuset kan tyde på en bredere tilnærming til usikkerhet utover sannsynlighet. Dette kommer til uttrykk særlig gjennom første formen for usikkerhet, som omhandler usikkerhet knyttet til manglende informasjon som ligger bak angitte sannsynligheter. Vi ser videre at usikkerhet blir vektlagt innen risiko ettersom at det blir beskrevet hvordan involverte forholder seg til sammenhenger med høy usikkerhet. Det kommer likevel ikke klart frem at usikkerhet kobles inn i noen grunnleggende risikokonseptualisering etter min vurdering.

Etter gjennomgang av risikorelaterte publikasjoner fra og om Petroleumstilsynet, kommer det frem et klart mønster av tydelig og eksplisitt konseptualisering av risiko. De er tydelige på både viktigheten av risikostyring, og understreker også betydningen av å ha en god forståelse av akkurat hva risikobegrepet bør innebære. I Petroleumstilsynets veileder for integrert og helhetlig risikostyring kommer dette frem ved flere anledninger. I denne rapporten vektlegges usikkerhet som sentralt i risikobegrepet. Kunnskapsstyrken blir trukket frem som sentralt under usikkerhet og noe en må ta høyde for når man skal ta risikoinformerte beslutninger. Denne veilederen gjelder riktignok for risikostyring av sikkerhet generelt, og er ikke rettet direkte mot risikostyring av cybersikkerhet. Gjennom rapporten til SINTEF (2021) blir det demonstrert at disse prinsippene gjør seg gjeldene for risikostyring av cybersikkerhet også, både innen IT og OT. Denne rapporten tar for seg hvordan petroleumsreguleringen virker inn på cybersikkerheten i petroleumssektoren. Det vises til Petroleumstilsynets konseptualisering av risiko, som kan fortelle oss at risikoperspektivet til Petroleumstilsynet kommer til anvendelse også innen cybersikkerheten.

Vi ser videre at risikokonseptualiseringen underbygges gjennom grundig gjennom Petroleumstilsynets rapport om risikobegrepet. Rapporten adresserer begrepet og hva det bør inneholde direkte. Også her blir risiko definert som bestående av to hovedelementer: «konsekvensene av virksomheten og tilhørende virksomhet». Bruken av sannsynlighet blir videre knyttet til en eldre forståelse av risikobegrepet, og kritiseres for å være en mekanisk tilnærming til risiko som ikke reflekterer usikkerhet bak angitte sannsynligheter. Sannsynligheter beskrives som en et tidvis godt virkemiddel for å beskrive risiko, men utilstrekkelig alene å ikke beskrive usikkerheten rundt.

Vi ser videre at myndighetene stiller krav til risikostyringen gjennom styringsforskriften. I § 4 stilles det konkrete krav til virksomhetenes risikostyring, deriblant krav til å redusere sannsynligheten for uønskede hendelser. Bruk av sannsynlighet i denne sammenhengen kan etter min vurdering tolkes på flere måter. Implisitt kan dette tolkes over i et fokus på at en nødvendigvis skal operere sannsynligheter i sammenheng med risikostyring. På den andre siden kan vi tolke denne bruken av sannsynlighetsbegrepet til å kun peke på at virksomhetene skal drive med risikomitigerende aktiviteter, men at bruken av begrepet ikke nødvendigvis innebærer noen betydning for risikokonseptualiseringen. Vi ser også at det i samme forskrift stilles krav til bruk av risikoakseptkritierier. Akkurat hva et risikoakseptkriterium innebærer er imidlertid ikke gitt. Dette kan innebære kvantitative forventningsverdier, og det er nettopp det som har blitt standard praksis blant operatørene i norsk petroleumsvirksomheter.

Blant kildene benyttet for delkapittelet om Telenor, var det noe knapt med kilder som kan fortelle oss om risikoforståelsen til Telenor, men rapporten deres Digital Sikkerhet 2022 gir noen svært relevante innspill. Innledningsvis blir grad av usikkerhet brukt til å beskrive risikobildet rundt Russland som et resultat av krigen i Europa, fremfor å for eksempel snakke om økt sannsynlighet for russiske operasjoner. I rapporten har de et eget kapittel som retter seg mot en «ny» forståelse av risiko. Fokus på kunnskap og beslutningsgrunnlag vektlegges videre, som kan videre tyde på et fokus på kunnskapsstyrke. Kompliserende elementer som øker usikkerheten blir trukket frem, slik som lange leverandørkjeder og en geopolitisk volatil tid. Det listes videre opp en rekke punkter som risikovurdering bør ta høyde for, som avsluttes med at det er en rekke kilder til usikkerheter knyttet til risikovurderingen og peker på kunnskapsbehov.

Usikkerhet som et eget tema drøftes videre. Ulike faktorer som kan påvirke usikkerheten trekkes frem. De skriver så at usikkerhet presenteres gjerne i form av sannsynligheter og tilhørende konsekvenser. Dette gir et klart uttrykk for en risikoforståelse som går ut på at sannsynlighet kan være et virkemiddel for å kommunisere usikkerhet, og erstatter ikke usikkerhet som en del av risikobegrepet. Kunnskapsgrunnlaget blir særlig trukket frem som et sentralt usikkerhetsmoment, og nevner blant annet mangel på data, enighet blant eksperter, partiskhet og kompleksitet. Alt dette støtter opp under en bred og helhetlig tilnærming til risiko. Dette blir videre trukket ut i praktiske eksempler der fokuset på usikkerhet kontra sannsynlighet illustreres: føre-var og økt vekt på resiliens. Dette er begge strategier som gjør seg passende i sammenhenger preget av alvorlige konsekvenser og høy usikkerhet –

sammenhenger der å angi sannsynligheter ofte kan bli upassende og misvisende. Rapporten markerer det som ser ut til å være en overgang hos Telenor sin risikoforståelse innen sikkerhetsarbeid. Dette kommer frem gjennom å se på overgangen fra fokuset på sannsynlighet tilsvarende rapport fra 2021, over til det helhetlige og usikkerhetsorienterte risikoperspektivet i 2022.

### 5.1.3 Er risikoforståelsen hos virksomhetene forenlig med usikkerhetsbasert risikoteori?

Samlet sett vil jeg argumentere for at kildene fra NSM (delkapittel 4.1) antyder en konseptualisering som dreier seg om et utgangspunkt i sannsynlighet og konsekvens, som kan kobles til (C, P)-konseptet (eller D2 under alternative konseptualiseringer). Dette er i hovedsak basert på bruken av sannsynlighet og konsekvenser uten videre vurdering av usikkerhet i § 12 c) i virksomhetssikkerhetsforskriften, samt henvisning til denne i veileder for sikkerhetsstyring. Det er imidlertid vært å bemerke at det kommer aldri helt eksplisitt fram, heller ikke trusselvurderingene som hyppig omtaler risiko.

Det er likevel noen nyanser av denne forståelsen som kommer frem gjennom veileder for risikovurdering av IKT-systemer. Her blir det trukket frem to risikodefinisjoner, en tilsvarende (C, P) og trefaktormodell, samt en ytterligere definisjon som blir benyttet innledende – risiko som usikkerhet knyttet til måloppnåelse. Bruk av sannsynligheter i tilknytning til lav kunnskapsstyrke blir trukket frem som en betydelig utfordring i drøftingen av de to førstnevnte. Å vurdere kunnskapsstyrken som ligger til grunn er et kjerneelement i risikobeskrivelsen knyttet til risiko konseptualisert som (C, U).

Ut fra det som har blitt lagt frem, ser det ut til at det NSM presenterer er forskjellige konseptualiseringer av risiko fra de ulike kildene. Dette kan tyde på at NSM enten har endret tilnærmingen sin til risiko eller at de ikke er konsekvente.

Norges Bank sin konseptualisering og hvorvidt usikkerhet vurderes kommer heller ikke helt eksplisitt frem på noe punkt i deres publikasjon om cybersikkerhet og finansiell infrastruktur. Dette må snarere tolkes implisitt. Det som kan fortelle oss mest om deres risikoforståelse,

finner vi i modellen basert på Ros (2020) og videre inn i artikkelen fra Ros (2020). Sannsynlighet står som et av få punkter å vurdere risiko ut fra. Dette gir et tydelig tegn på at man nødvendigvis forholder seg til bruk av sannsynlighet innen sikkerhetsrisiko. Det er videre ingen andre faktorer listet opp i modellen som gir oss en ide om en grundigere vurdering av usikkerhet utover å angi en sannsynlighet. I dette tilfellet blir det også relevant å nevne at sannsynlighetsbegrepet kan både være angitt kvantitativt og kvalitativt.

Videre kan det risikorelaterte innholdet i Ros (2020) fortelle oss noe om Norges Bank sin tilnærming til risiko, i og med at de har valgt å anvende nettopp denne artikkelen. Innledende om risiko blir cyberrisiko definert i tråd med (C, P)-perspektivet, med utgangspunkt i EUT. EUT, som omtalt i teorikapitlet, er svært vanlig å anvende innen økonomistyring, men premissene til grunn for risikostyring av økonomi og sikkerhet kan være svært ulike. EUT vektlegger sannsynligheter og bruk av forventningsverdier for å tallfeste nytteverdier, som kan hjelpe oss med å rangere beslutningsalternativer. Med EUT som utgangspunkt vil en (C, P)-konseptualisering fremstå logisk. Dersom man anvender denne logikken i en sikkerhetssammenheng, kommer vi tilbake til utfordringene knyttet til usikkerhet. Å tallfeste faktiske og mulige økonomiske tap knyttet til en investering vil by på langt færre utfordringer enn om man skal angi eller utregne forventningsverdier knyttet til et digitalt angrep fra ukjente trusselaktører i omfattende og komplekse systemer. Grunnlaget for bruk av slike forventningsverdier kan være svært varierende, og disse variasjonene blir ikke reflektert dersom man driver risikostyring på basis av EUT. Usikkerhet blir likevel gått inn på i Ros (2020), og det blir diskutert hvordan dette kan påvirke risikostyringen, men dette inngår tilsynelatende ikke i selve risikoperspektivet. Av det som har kommet frem her, kan det tolkes til at Norges Bank deler sitt syn på risiko med en artikkel som benytter seg i hovedsak av (C, P)-perspektivet.

Petroleumstilsynet er på sin side svært klare på sin konseptuelle tilnærming til risiko. Av kildene trukket frem i oppgaven er Petroleumstilsynet tydelige og konsekvente i å definere risiko mer eller mindre ordrett slik (C, U)-perspektivet defineres i Aven (2022) eller D3, som beskrevet i teorikapittelet. Veileder for integrert og helhetlig risikostyring og rapport om risikobegrepet trekker begge frem sentrale momenter som ligger i kjernen av en usikkerhetsbasert risikoforståelse.  Disse kildene retter seg ikke mot cybersikkerhet i seg selv, men vi kan knytte disse sammen gjennom publikasjonen fra SINTEF, som viser Petroleumstilsynets risikoperspektiver anvendes innen regulering av cybersikkerhet.

Begrensningene knyttet til bruk av sannsynlighet bygger videre på en overgang fra det eldre (C, P)-perspektivet, over til det usikkerhetsbaserte (C, U)-perspektivet. Begrensingene knyttet til sannsynlighet og motivasjonen til å fokusere på usikkerhet drøftes videre og forteller oss eksplisitt at Petroleumstilsynet ikke bare benytter seg av (C, U), men gir også uttrykk for å være godt kjent med hvorfor dette er viktig.

Det kan samtidig være verdt å nevne kravet til bruk av akseptkriterier fra styringsforskriften rettet mot underlagte virksomheter. Samtidig som akseptkriterier ikke nødvendigvis må være kvantitative forventningsverdier, ser vi at det har blitt en bransjestandard som går ut på at så å si alle norske operatører setter kvantitative forventningsverdier knyttet til sikkerhetsrisiko, slik som vi ser med FAR-verdier. Disse verdiene er riktignok satt av operatørene selv, men kan sies å være et resultat av kravene stilt fra myndighetssiden. Disse verdiene retter ikke direkte mot cybersikkerhet, men i og med at OT-sikkerhet har implikasjoner for FAR-verdiene, kan dette gjennom tolkning knyttes sammen.

Gjennom kildene undersøkt knyttet til Telenor, kommer det etter min vurdering ikke frem en helt klar risikokonseptualisering, men heller at Telenor i sin rapport Digital Sikkerhet 2022 viser tegn til en usikkerhetsbasert tilnærming til risiko. Telenor sin omtale av økt usikkerhet fremstår tidlig som et tegn på at risikoforståelsen bygger på usikkerhet som et sentralt moment i risikobegrepet. Dette utgjør det som Telenor omtaler som å tenke nytt om sikkerhet – en mer helhetlig tilnærming til risiko. Dette markerer en overgang fra en tilsynelatende mer snever og sannsynlighetsorientert tilnærming som ble gitt uttrykk for i 2021. Tilnærmingen som uttrykkes i 2021-rapporten om digital sikkerhet kan tolkes til å implisitt være i tråd med en (C, P)-tilnærming, som skiller seg drastisk fra slik risiko omtales i Digital Sikkerhet 2022.

Usikkerhet og kunnskapsstyrke og deres betydning for risiko blir videre omtalt grundig i 2022-rapporten. Utsagnet «usikkerheten presenteres gjerne i form av sannsynligheter for hva som kan skje og tilhørende konsekvenser» kan i det minste fortelle oss at Telenor har et fokus på usikkerhet, men akkurat hvordan de forholder seg til bruk av sannsynlighet kan være litt mer åpent for tolkning. Utsagnet høres kanskje kjent ut med tanke på (C, U)-definisjonen om konsekvenser og assosierte usikkerheter, men innholdet er ikke det samme. I tråd med (C, U)-konseptet er ikke sannsynlighet nødvendigvis galt å benytte seg av for å kommunisere usikkerhet, så lenge man er kjent med begrensningene bak. Hensyn til kunnskapsstyrken, som en helt sentral svakhet bak å sette for stor tillit til angitte sannsynligheter, demonstrerer Telenor godt at de er kjent med gjennom påfølgende avsnitt om usikkerhet og

kunnskapsgrunnlag. Etter min vurdering gir dette klare signaler om at Telenor tilnærmer seg risiko med basis i en (C, U)-forståelse av begrepet. At Telenor videre i mer praktiske eksempler viser til tilfeller der en må vektlegge usikkerhetsgrad forteller oss at denne konseptualiseringen forlenges til strategisk tekning i sikkerhetsarbeidet.

## 5.2 Ulikheter og likheter

Jeg vil i dette delkapittelet redegjøre for likheter og ulikheter på tvers av de fire utvalgte virksomhetene og med det besvare forskningsspørsmålet oppgitt i førstekapittel: *jobber virksomhetene ut fra en felles forståelse av risiko i deres cybersikkerhetsarbeid?*

Samlet sett vil jeg si at resultatene åpner for å plassere de fire virksomhetene i to forskjellige kategorier av risikoforståelse: (C, P) og (C, U). De ulike virksomhetene gir imidlertid varierende grad av uttrykk for å tilhøre enten den ene eller andre kategorien, men det kommer klart frem fra alle virksomhetene hvilken av disse to risikoperspektivene de står nærmest.

Norges Bank og NSM blir begge plassert under kategorien for (C, P)-perspektivet. Norges Bank legger tilsynelatende svært lite vekt på usikkerhet, samtidig som de trekker frem sannsynlighet som et av få elementer som utgjør cyberrisiko. Artikkelen de viser til i sin modell for cyberhendelser ser ut til å, til tross for å omtale usikkerhet i et eget kapittel, definerer risiko som en kombinasjon av sannsynlighet og konsekvenser, som er kjernen av et (C, P)-perspektiv. NSM er i likhet med Norges Bank å kategorisere inn under (C, P)-kategorien. Dette er hovedsakelig grunnet mønsteret av sannsynlighetsfokus som funnet i de ulike kildene fra delkapittelet om NSM, fremfor usikkerhet eller andre momenter tilknyttet usikkerhet. NSM kan likevel plasseres et sted imellom grunnet deres drøfting rundt begrensinger rundt sannsynlighet i én av kildene, men dette synet reflekteres ikke i deres omtale av risiko i øvrige kilder.

Petroleumstilsynet og Telenor er å finne i kategorien rundt (C, U)-perspektivet. Petroleumstilsynet er virksomheten som helt klart har den tydeligste konseptualiseringen av risiko, og kan finnes i flere av kildene trukket frem i denne oppgaven. De er også svært konsekvente i hvordan dette defineres, og videre drøfting av svakhetene bak sannsynlighet og viktigheten bak å fokusere på usikkerhet forteller oss at de har en god forståelse av hvor betydelig vektlegging av usikkerhet og kunnskapsstyrke er i sikkerhetssammenhenger.

Telenor er ikke like eksplisitte i deres risikokonsepttulariseringer, men det er likevel et gjennomgående eksplisitt fokus på usikkerhet i 2022-rapporten deres. Kunnskapsgrunnlaget blir også trukket frem som sentralt, og vil med det etter min tolkning befinne seg sammen med Petroleumstilsynet i kategorien for et usikkerhetsbasert risikoperspektiv. En annen interessant parallell er at begge ser ut til å omtale dette usikkerhetsbaserte risikoperspektivet som noe overgangen til noe nytt, mens det mer snevre synet tilhører fortiden. I kapittelet hvor Telenor diskuterer helhetlig risikotilærming og usikkerhet, er kapittelet kalt «vi må tenke nytt om digital sikkerhet», mens Petroleumstilsynet skriver om bruk av sannsynlighet som noe som ble gjort tidligere, men har vist seg å være utilstrekkelig.

Samlet sett vil jeg si det er godt grunnlag for å konkludere med at virksomhetene *ikke* jobber ut fra en felles forståelse for risiko. Blant de fire virksomhetene jobber to og to ut fra en mer eller mindre felles forståelse for risiko, men skillet på tvers av disse to gruppene er betydelig. Norges Bank og NSM på én side og Petroleumstilsynet og Telenor på den andre siden kan plasseres henholdsvis på hver sin side av (C, P)-perspektivet og (C, U)-perspektivet.

Akkurat hvorfor det forskjeller og hvorfor de er som beskrevet i delkapittelet over, er ikke helt rett-frem spørsmål å svare på dersom man skal ta utgangspunkt i kildene i denne oppgaven, ettersom det kun er Petroleumstilsynet og Telenor som motiverer sitt valg av risikotilnærming, gjennom å drøfte usikkerhet og helhetlig risikotilnærming. Det er muligens ikke tilfeldig at akkurat de to virksomhetene som skriver om viktigheten av sin konseptuelle tilnærming til risiko er de to samme virksomhetene som i denne oppgaven har blitt plassert under (C, U)-perspektivet. At noen i virksomheten har satt seg ned og sett kritisk på hvordan man forholder seg til sikkerhetsrisiko, vil lede en inn på en bredere perspektiv, som må omhandle noe mer enn sannsynlighet og konsekvenser. På den andre siden med Norges Bank og NSM ser vi ingen av dem som omtaler noen form for begrunnelse og/eller viktigheten bak å bruke sannsynlighet som en av to dimensjoner av risikobegrepet.

Sikkerhet er viktig i alle de ulike sektorene virksomhetene tilhører, og risiko står sentralt i sikkerhetsarbeidet hos alle. Som tidligere nevnt, kan ulike risikoforståelse være mer eller mindre passende, avhengig av sammenhengen, men sammenhengen her er felles for alle sammen: sikkerhetsrisiko. Sammenhengen med hensyn til risikotilnærming er lik, til tross for at virksomhetene tilhører vidt forskjellige sektorer.

Akkurat med Norges Bank, kan en institusjon i finanssektoren ha risikostyringsprinsipper som er mer forenlig med økonomistyring, da det antagelig er svært mange økonomer i bildet. Dette kan for eksempel ha kommet av at økonomer blir satt å jobbe med sikkerhet, eller at det blir lagt føringer for risikostyring i hele virksomheten, som kommer fra økonomer. Hvorfor NSM til å begynne med ikke klart konseptualiserer risiko samtidig som virksomheten primært jobber med sikkerhet, er ikke lett å finne et svar på. Når dette dreier seg om såpass store og sentrale virksomheter, er det etter alt å dømme uheldig og ingen gode argumenter for å holde videre på et (C, P)-perspektiv.

## 5.3 Implikasjoner rundt å vurdere risiko som sannsynlighet og konsekvens

Med utgangspunkt i funnene presentert i oppgaven, ser vi at perspektivet på risiko som en kombinasjon av sannsynlighet og konsekvens blir anvendt innen cybersikkerhet i kritisk infrastruktur i Norge. For å få en ide av implikasjonene som ligger bak en slik tilnærming til sikkerhetsrisiko, kan vi se på teorien rundt usikkerhetsbasert risikoperspektiv, som presentert i teorikapittelet. Akkurat hvilken tilnærming en bør ha til risiko, kan variere ut ifra sammenhengen. Med utgangspunkt teorien presentert, er det i sikkerhetssammenhenger utilstrekkelig å benytte seg av sannsynligheter uten å vurdere usikkerheten som ligger bak, og det er nettopp dette som blir tilfelle dersom man går frem med et (C, P)-perspektiv på risiko. Om dette handler om å angi en prosentandel eller beskrive «svært sannsynlig» og lignende, kan usikkerheten som ligger bak både være svært høy eller svært lav, samtidig som tallet eller beskrivelsen er det samme.

Innledningsvis i oppgaven ble noen hovedtrekk i cyberrisikobildet trukket frem. Det ble nevnt en drastisk teknologisk utvikling, kombinert med økt kompleksitet og avhengigheter, hybride trusler og bruk av lange, uoversiktlige kjeder av underleverandører. Grunnen til at disse momentene var viktig å ta med i denne oppgaven, er å poengtere usikkerheten som ligger bak trusselbildet i cyberdomenet. Disse momentene viser at risikobildet fremover er svært komplekst og uforutsigbart. Denne usikkerheten bør reflekteres i risikovurderingene som gjøres innen cybersikkerhet.

Vi ser for eksempel at Norges Bank benytter seg av sannsynlighet, og ikke usikkerhet, som en del av cyberrisiko. Det samme gjelder NSM sine krav/anbefalinger om risikovurderinger. Man kan da stille spørsmål om hvor nyttig det vil være å nødvendigvis angi sannsynligheter for cyberrisiko, uavhengig av usikkerheten som ligger til grunn. Det kan være mulig å justere opp sannsynlighetene dersom man har dårlig kunnskapsstyrken er lav, men dette blir en lite informativ og unyansert fremstilling. En slik fremstilling vil ikke skille mellom risikoer vi helt enkelt ikke kjenner godt nok til og risiko som vi har god kjennskap til, og som likevel er å anse som for høy. Dette kan påvirke beslutningstakere til å anta at en har kunnskap en ikke har, og dermed påvirke beslutningen. Eksempelvis kan det hende at det neste trinnet burde være å utvikle mer kjennskap til et bestemt fenomen, men grunnet upassende metodebruk, blir risikoen heller ansett som for høy og unødvendige tiltak implementeres for å redusere risikoen som et resultat. Dette er aspekter som ved risiko som kan dekkes dersom en adresserer *usikkerheten*. Med bakgrunn i risikobildet beskrevet tidligere, vil det etter min vurdering sjeldent være passende å benytte seg av sannsynligheter for å beskrive risiko innen cybersikkerhet.

## 5.4 Validitet og reliabilitet

Oppgavens validitet og reliabilitet har blitt omtalt i metodekapittelet, men da mer rettet mot oppgavens metodevalg generelt, samt definisjoner av de metodologiske begrepene. I denne delen vil oppgavens validitet og reliabilitet bli drøftet mer konkret og spesifikke poenger i oppgaven vil bli trukket frem.

Hvorvidt oppgavens funn kan generaliseres er et interessant tema til tross for at dette ikke var oppgavens egentlige hensikt. Samtlige virksomheter spiller sentrale roller i å sikre Norges infrastruktur, så funnene gjort av virksomhetene direkte er ment til å være viktige i seg selv. Funnene indikerer likevel at det i det minste ikke er gitt at risikokonseptulaseringen i denne type virksomheter er forenlig med (C, U)-perspektivet, som er å anbefale innenfor risikostyring av sikkerhet. I denne oppgaven ble to av fire virksomheter assosiert med et (C, P)-perspektiv på risiko. Dette kan forteller oss i det minste at dette faktisk er gjeldende i et fåtall virksomheter og kan videre tyde på at dette er et utbredt problem i andre norske virksomheter, men grunnet få virksomheter i utvalget er det ikke grunnlag for å konkludere med at dette gjelder i nærheten av halvparten av lignende virksomheter.

Reliabiliteten i oppgaven er etter min oppfatning forholdsvis god med tanke på kildebruken. Kildene brukt i oppgaven er i all hovedsak hentet direkte fra virksomhetene selv. Det er noen kilder som omhandler virksomheten, men de har alle en mer supplerende rolle. Det imidlertid noen poenger som måtte trekkes basert på hva det blir gitt uttrykk for, heller enn det eksplisitt skrives om. Dette var i varierende grad nødvendig i undersøkelsen av alle virksomhetene bortsett fra Petroleumstilsynet. Tilfellene der slutninger og betraktninger har vært basert på tolkning av noe som kommer frem implisitt, har blitt poengtert tydelig. Eksempler på dette er for eksempel når kildene som virksomhetene henviser til blir undersøkt for å fortelle oss noe om hva virksomhetene kan mene om risiko. Bruk av sannsynlighet har også vært et sentralt poeng for å undersøke virksomhetenes forhold til usikkerhet, til tross for at dette ofte inkluderer noen utsagn som direkte retter seg mot usikkerhet i seg selv. Samtidig som disse tolkningene understrekes og begrunnes der de forekommer, er det ikke gitt at en annen hadde kommet trukket de samme slutningene basert på samme informasjonsgrunnlag.

# 6.0 Konklusjon

Gjennom oppgavens undersøkelse av NSM, Norges Bank, Petroleumstilsynet og Telenor kommer det frem risiko, risikovurdering, risikostyring er elementter som vektlegges og omtaltes hyppig av samtlige virksomheter. Gjennom videre undersøkelse og vurderinger kommer oppgaven frem til at risikokonseptualiseringen i to av virksomhetene tyder på å ikke være forenlig med usikkerhetsbasert risikoforståelse: NSM og Norges Bank. En fellesnevner hos begge virksomhetene er tydelig og gjentatt fokus på bruk av sannsynlighet for å beskrive risiko, samtidig som usikkerhet knyttet til vurderingene ikke beskrives. Som et resultat kan NSM og Norges Bank karakteriseres med et (C, P)-perspektiv, som innebærer å definere risiko som en kombinasjon av sannsynlighet og konsekvens. Dette pekes på av litteraturen benyttet i teorikapitlet som problematisk i sikkerhetssammenhenger, og også innen cybersikkerhet, da et (C, P)-perspektiv ikke fanger opp usikkerheten som ligger bak. Lange leverandørkjeder, hybride trusler og rask teknologisk utvikling er kompliserende risikoområder i cybertrusselbildet som underbygger viktigheten av å ta usikkerhet, og særlig kunnskapsstyrke i betraktning.

Petroleumstilsynet og Telenor gir derimot klare tegn til å inkludere usikkerhet som et sentralt moment i sin risikokonseptualisering. Petroleumstilsynet er riktignok tydeligere på dette området, men også hos Telenor tyder det på at man jobber ut fra en definisjon av risiko som konsekvenser og tilhørende usikkerhet, slik som (C, U)-konseptet usikkerhetsbasert risikoteori anbefaler for risikostyring av sikkerhet.

Som et resultat ser vi at kun to av de fire virksomhetene ser ut til å ha et risikoperspektiv som er forenlig med usikkerhetsbasert risikoteori, og vi kan med det også se at de fire store og sentrale virksomhetene har risikoperspektiver som ikke er forenlige med hverandre.

# REFERANSELISTE


Amundrud, Øystein, et al. "How the Definition of Security Risk Can Be Made Compatible with Safety Definitions." *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 231, no. 3, June 2017, pp. 286–94, https://doi.org/10.1177/1748006X17699145

Anthony (Tony) Cox Jr, Louis. "What's Wrong with Risk Matrices?" *Risk Analysis*, vol. 28, no. 2, 2008, pp. 497–512, https://doi.org/10.1111/j.1539-6924.2008.01030.x

Aven, Terje. *Risk Analysis*. John Wiley & Sons, 2015.

Aven, Terje and Thekdi, Shital. *Risk Science*. Routledge, 2022.

Aven, Terje, and Kristensen, Vidar. "How the Distinction between General Knowledge and Specific Knowledge Can Improve the Foundation and Practice of Risk Assessment and Risk-Informed Decision-Making." *Reliability Engineering & System Safety*, vol. 191, June 2019, p. 106553, https://doi.org/10.1016/j.ress.2019.106553.

BAHR, 2019. *Kan Din Virksomhet Bli Omfattet Av Den Nye Sikkerhetsloven? — Advokatfirmaet BAHR*. https://bahr.no/newsletter/kan-din-virksomhet-bli-omfattet-av-den-nye-sikkerhetsloven

Dalland, Olav. *Metode Og Oppgaveskriving*. Gyldendal akademis, 2017.

DN, 2022. *"Ruster Opp Cybersikkerheten i Norsk Olje- Og Gass – Frykter Fysiske Skader Fra Digitale Angrep (+)."* *Www.Dn.No*, 4 Apr. 2022, https://www.dn.no/teknologi/lundin/cyberangrep/cybersikkerhet/ruster-opp-cybersikkerheten-i-norsk-olje-og-gass-frykter-fysiske-skader-fra-digitale-angrep/2-1-1194103.

DSB, 2016. *Samfunnets Kritiske Funksjoner*. https://www.dsbinfo.no/DSBno/2017/tema/samfunnets-kritiske-funksjoner

DSB, 2019. *Analyse av krisescenarioer. Pdf*. https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf Accessed 16 Mar. 2023.

E-tjenesten, 2023. *FOKUS. https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/_/attachment/inline/c1a9a458-aa1d-4bf6-a558-9cec57acde8f:9b2050d897a2b2db1bddc8e505db7b666e608b98/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf*

ECB, 2018. *TIBER-EU FRAMEWORK – How to Implement the European Framework for Threat Intelligence-Based Ethical Red Teaming*.

*Forskrift Om Helse, Miljø Og Sikkerhet i Petroleumsvirksomheten Og På Enkelte Landanlegg (Rammeforskriften) - Lovdata*. https://lovdata.no/dokument/SF/forskrift/2010-02-12-158 Accessed 3 May 2023.

*Forskrift Om Styring Og Opplysningsplikt i Petroleumsvirksomheten Og På Enkelte Landanlegg (Styringsforskriften) - Lovdata*. https://lovdata.no/dokument/SF/forskrift/2010-04-29-611 . Accessed 27 Apr. 2023.

*Forskrift Om Virksomheters Arbeid Med Forebyggende Sikkerhet (Virksomhetsikkerhetsforskriften) - Lovdata*. https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053 Accessed 13 Apr. 2023.

Gjesvik, Lars, 2019. *NUPI_Report_5_2019_Gjesvik.Pdf*. https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2598280/NUPI_Report_5_2019_Gjesvik.pdf?sequence=1&isAllowed=y Accessed 16 Mar. 2023.

*Id3-Regulering-Av-Ikt-Sikkerhet.Pdf*. https://www.ptil.no/globalassets/fagstoff/prosjektrapporter/ikt-sikkerhet/id3-regulering-av-ikt-sikkerhet.pdf Accessed 28 Apr. 2023.

Jacobsen, Dag Ingvar. *Hvordan Gjennomføre Undersøkelser?* 2000.

*Lov Om Nasjonal Sikkerhet (Sikkerhetsloven) - Lovdata*. https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven Accessed 13 Apr. 2023.

Lupton, Deborah. *Risk, Second Edition*. Routledge, 2013.

*Nasjonal-Strategi-for-Digital-Sikkerhet.Pdf*. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf Accessed 1 May 2023.

Norges Bank, 2022a. *Finansiell stabilitet - eit hovudmål*. 23 Mar. 2023, https://www.norges-bank.no/tema/finansiell-stabilitet/finansiell-stabilitet-hovudmal/

Norges Bank, 2022b. *Organisering og styring*. https://www.norges-bank.no/tema/Om-Norges-Bank/Organisering-styring/

Norges Bank, 2002c. *Finansiell infrastruktur 2022. https://www.norges-bank.no/contetassets/7437af41dbd94dbfaee9e7f0d231a3ba/finansiellinfrastrutur_2022.pdf?v=08/08/2022123229*

Norges Bank, 2022d. *Policy---Security.Pdf*. https://www.nbim.no/contentassets/b29376a53d074feb9a1713c0603e8b74/policy---security.pdf

Notaker, Hallvard. "Nasjonal sikkerhet eller økonomisk effektivitet? Norges evne til å avdekke hybride trusler i samtidshistorisk perspektiv." *Internasjonal Politikk*, vol. 81, no. 1, Feb. 2023, pp. 115–41, https://doi.org/10.23865/intpol.v81.5157.

NOU:2006:6, 2006. "NOU 2006: 6." *012001-020038*, 5 Apr. 2006, https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/.

NSM, 2020. *Risikovurdering Av IKT-Systemer.Pdf*. https://nsm.no/getfile.php/136603-1625054089/NSM/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf Accessed 23 May 2023.

NSM, 2020. *Veileder-i-Sikkerhetsstyring.Pdf*. https://nsm.no/getfile.php/132933-1591350417/NSM/Filer/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf Accessed 13 Apr. 2023.

NSM, 2022. *Nasjonalt digital trusselbilde 2022 Pdf*. https://nsm.no/getfile.php/1312007-1667980738/NSM/Filer/Dokumenter/Rapporter/NDIG2022_online.pdf. Accessed 14 Apr. 2023.

NSM, 2023. *Risiko 2023 - Nasjonal Sikkerhetsmyndighet.Pdf*. https://nsm.no/get-file.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf Accessed 14 Apr. 2023.

NSM, 2021. *Nasjonalt digitalt risikobilde 2021.Pdf*. https://nsm.no/getfile.php/137495-1635323653/NSM/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_en-keltside.pdf Accessed 14 Apr. 2023.

NUPI, 2016. "Hybrid Krigføring – Hva Er Det?" *NUPI Skole*, https://www.nupi.no/publikasjoner/innsikt-og-kommentar/hvor-hender-det/hhd-2016/hybrid-krigfoering-hva-er-det Accessed 16 Mar. 2023.

Petroleumstilsynet u.å., *Petroleumstilsynets Rolle Og Ansvarsområde*. https://www.ptil.no/om-oss/rolle-og-ansvarsomrade/ Accessed 7 June 2023.

Petroleumstilsynet, 2016. *Risikobegrepet i petroleumsvirksomheten Pdf*. https://www.ptil.no/contentassets/1b253609b7b940069e0acd005861c7ca/risikorapport-2016-nett.pdf Accessed 26 May 2023.

Preventor 2021, *Ptil-Toleransegrenser-Rapport-Rev2.Pdf*. https://www.ptil.no/contentassets/4deea346d8cb4008a2eef488f85313ae/ptil-toleransegrenser-rapport-rev2.pdf Accessed 30 May 2023.

Proactima, 2020. *Bruk-Av-Risikoakseptkriterier---En-Evaluering.Pdf*. https://www.ptil.no/contentassets/4deea346d8cb4008a2eef488f85313ae/bruk-av-risikoakseptkriterier---en-evaluering.pdf. Accessed 27 Apr. 2023.

Regjeringen, 2022. *NATO styrker arbeidet med å beskytte kritisk infrastruktur*." *Regjeringen.no*, 14 Oct. 2022, https://www.regjeringen.no/no/aktuelt/fminmoteokt22/id2935130/.

Regjeringen, u.å.a, *"Nasjonal sikkerhetsmyndighet*." *Regjeringen.no*, 3 May 2019, https://www.regjeringen.no/no/dep/fd/organisering-og-ledelse/etater-og-virksomheter-under-forsvarsdepartementet/tilknyttet-virksomhet/nasjonal-sikkerhetsmyndighet/id451444/.

Regjeringen, u. å.b, *"Petroleumstilsynet*.", 28 July 2006, https://www.regjeringen.no/no/dep/aid/om-arbeids-og-inkluderingsdepartementet/etatstyring/underliggende-etater/petroleumstilsynet/id85809/

Regjeringen, u.å.c, "Telenor ASA." *Regjeringen.no*, 16 Dec. 2022, https://www.regjeringen.no/no/dep/nfd/org/etater-og-virksomheter-under-narings--og-fiskeridepartementet/selskaper/telenor-asa/id2951813/.

SINTEF. *12 ting du må vite om cybersikkerhet*. 22 Mar. 2022, https://www.sintef.no/sistenytt/2021/12-ting-du-ma-du-vite-om-cyberangrep-og-cybersikkerhet/.

Svein, S. Andersen, 1997. *Case-Studier Og Generalisering*. Fagbokforlaget Vigmostad & Bjørke AS,

Telenor, 2021. *Digitalsikkerhet2021.Pdf*. https://www.telenor.no/binaries/om/digital-sikkerhet/digitalsikkerhet2021.pdf. Accessed 19 Apr. 2023.

Telenor, 2022. *Digital_sikkerhet_2022.Pdf*. https://www.telenor.no/binaries/om/digital-sikkerhet/2022/Digital_sikkerhet_2022.pdf. Accessed 16 Mar. 2023.

Yin, Robert K. *Case Study Research*. SAGE, 2009.