DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:
Risikostyring og sikkerhetsledelse

Vårsemesteret, 2022

Åpen / ~~Konfidensiell~~

Forfatter: Christian Andersen Halle

.....
(signatur forfatter)

Fagansvarlig: Sissel Haugdal Jore

Veileder(e): Sissel Haugdal Jore

Tittel på masteroppgaven:
Hvordan utvikle «etterretningstrussel» som del av en risikovurdering.

Engelsk tittel:
Establishing the intelligence threat as part of a risk assessment.

Studiepoeng: 30

Emneord:
Risikovurdering, risikoanalyse,
etterretningstrussel, totalforsvaret

Sidetall: ..... 69 ...

+ vedlegg/annet: ... 12 ...

Stavanger, ... 09.05.2022 ...
dato/år

Forord

Veien frem til denne oppgaven startet i 2019 og har vært både interessant og utfordrende. Jeg har ved siden av studiet byttet stilling i Forsvaret, pusset opp huset, oppdratt en valp og fått gleden av å bli pappa for første gang. Det som startet som et ønske om faglig og akademisk påfyll for videre karriere i Forsvaret har ført til en stor interesse for fagfeltet. Med denne interessen kom det også til slutt et karrierebytte ut av Forsvaret for å jobbe fulltid med risiko og sikkerhet.

Uten familien min ville det aldri blitt noen masteroppgave. Mor og far er fantastiske støttespillere som de har vært siden jeg ble født. Cathrine har tatt i ekstra hjemme, hjulpet meg til å prioritere studiene og vært stresset på mine vegne mange ganger. Henriette kom til verden underveis og har gitt meg mer glede enn jeg trodde var mulig. En spesiell takk må også gå til hunden min Millie, som har vært en god samtalepartner på mang en tur i skogen.

Lars Østby og Morten Grønning har gitt meg ekstra støtte gjennom studiene med mange gode samtaler om både fag og annet.

Rico Behlke har vært en meget god sparringpartner og korrekturleser.

Ronny Windvik ved FFI har støttet oppgaven som ekstra veileder, sparringpartner, frustrasjonsventil og kompis. Teamet som har vært tilgjengelig for meg på FFI for faglig støtte og diskusjoner har også vært usedvanlig hjelpsomme. Tusen takk Kjell Olav og Monica!

Til slutt må jeg takke Sissel Jore som har veiledet meg. Jeg ba spesifikt om henne hovedsakelig fordi hun imponerer meg faglig, og litt fordi hun jobber mye med tilsiktede handlinger. Der andre har vært fornøyd har Sissel påpekt forbedringspotensialet, og det har jeg hatt behov for.

Sammendrag

Etterretningstrusselen i Norge har vært høy over lengre tid ifølge myndighetene. Totalforsvarskonseptet er revitalisert i de senere årene og omfatter blant annet en rekke strategiske kommersielle avtaler for støtte til Forsvaret. Kommersielle aktører i totalforsvaret, som blant annet behandler sikkerhetsgradert informasjon eller er av betydning for grunnleggende nasjonale funksjoner, har gjennom sikkerhetslovens funksjonelle krav fått et større ansvar for å skape et forsvarlig sikkerhetsnivå for nasjonen.

Aktørene som har strategiske avtaler med Forsvaret blir naturlige etterretningsmål, noe sikkerhetsmyndighetene også er tydelige på i åpne rapporter. Disse aktørene benytter normalt sett risikovurdering til å etablere eget risikobilde, og må i lys av sikkerhetsloven identifisere etterretningstrusselen som del av denne vurderingen. Oppgaven har som formål å se på egnetheten av risikovurdering og funksjonelt lovverk i jobben med å skape et forsvarlig sikkerhetsnivå. Oppgaven benytter en kvalitativ case-studie av risikovurderingsprosessen til to av Forsvarets strategiske logistikkpartnere for å besvare problemstillingen som er:

I hvor stor grad sikrer risikovurderinger hos Forsvarets strategiske logistikkpartnere, et forsvarlig sikkerhetsnivå mot etterretningstrusler?

Casen beskriver hvordan etterretningstrusselen blir identifisert og vurdert av kommersielle aktører i dag. Metodikken de benytter er drøftet gjennom tre forskningsspørsmål opp mot et bredt landskap bestående av teori om etterretning, funksjonelle reguleringsregimer, risiko og risikovurdering er beskrevet.

Oppgaven konkluderer med at de kommersielle aktørene gjennomfører mindre formelle risikovurderinger på området enn forventet. Deres pragmatiske tilnærming fører ikke nødvendigvis til et for dårlig risikonivå, men det er mindre kontroll på risikobildet enn det kunne ha vært. Avslutningsvis i oppgaven foreslås mulige forbedringer i metodikken som benyttes i dag, og det pekes på områder for mulig videre forskning.

Hvordan utvikle «etterretningstrussel» som del av en risikovurdering.

Innhold

1. Introduksjon

Trusselen fra etterretning har vært vedvarende høy i Norge over tid. Utfordringen med å risikovurdere etterretningstrusselen har opptatt meg under studiene. Dagens funksjonelle sikkerhetslov legger ansvaret for å få et forsvarlig sikkerhetsnivå på den enkelte virksomhet i betydelig større grad enn loven den erstattet. Virksomheter som omfattes av sikkerhetsloven må derfor vurdere risiko og iverksette tiltak mot alt fra naturkatastrofer til trusselen fra terrorister, kriminelle og spioner. Særlig etterretningstrusselen fremstår som vanskelig å vurdere og evaluere, ettersom den ikke nødvendigvis har et kortsiktig mål og i motsetning til andre ondsinnede aktører aktivt søker å holde sine aktiviteter skjult også etter gjennomføringen. Derfor ønsker jeg å se på hvordan risikovurdering av etterretningstrusselen gjennomføres i dag. Relevant teori vil benyttes til å evaluere metodikken som den benyttes og om mulig peke på forbedringer.

1.1. Risikovurdering av etterretningstrussel

Norsk Standard sin 5830-serie er myntet på risikovurdering og -analyse av tilsiktede uønskede handlinger (NS 5830, 2012, s. 1). Denne beskriver risikoen som en kombinasjon av verdi, trussel og sårbarhet. Forskerne Brooks og Smith fra Edith Cowan University definerer i sin bok Security Science, trusselen for tilsiktede handlinger som en kombinasjon av intensjon og kapabilitet. De definerer videre intensjonen som en kombinasjon av et ønske og et forventet utfall, mens kapabiliteten defineres som en kombinasjon av kunnskap og ressurser (Smith & Brooks, 2013, s. 64). Sammenligner man etterretningsaktøren med andre aktører som utfører tilsiktede, uønskede handlinger så kommer egenarten tydelig frem. Utfallet en etterretningsorganisasjon ønsker å oppnå kan i motsetning til de andre ha et langt perspektiv der det ikke er en kortsiktig vinning eller oppmerksomhet som er vesentlig. Etterretningsaktøren er som regel opptatt av å skjule både handlingen og effekten av handlingen sin, i motsetning til de andre rasjonelle trusselaktørene. En terrorist ønsker å skape frykt og er derfor avhengig av oppmerksomhet, sabotøren ønsker ødeleggelse, mens den kriminelle ønsker vinning og er klar over at handlingen vil være synlig så snart den er gjennomført. Ettersom etterretningsaktørene historisk er statlige er tilgangen på ressurser og kunnskap betydelig større enn for en kriminell organisasjon eller en terrororganisasjon. Trusselen fra en etterretningsaktør er med andre ord helt forskjellig fra trusselen fra andre ondsinnede aktører, både i intensjon og kapabilitet.

Det kan være vanskelig for et privat firma å analysere seg frem til etterretningsaktørens faktiske intensjon og kapabilitet er, mest sannsynlig vanskeligere enn å analysere andre ondsinnede aktører. Eksempelvis har myndighetene et insentiv for å dele så mye som mulig av kunnskapen de har om terrorister og kriminelle, da det å spre kunnskapen kan bidra til å skape et mest mulig robust samfunn. Når det gjelder etterretningstrusselen så har aktørene så store ressurser at de sannsynligvis vil endre sine metoder dersom sikkerhetsmyndighetene deler for mye kunnskap om dem. Det er dermed bedre å holde kortene tett til brystet og kunne overvåke, enn å åpne opp og bli utsatt for nye og ukjente metoder. I tillegg er det lettere å forutse hva de mulige målene for en kriminell eller en terrorist er, enn det er å forutse hva som er av interesse for en etterretningsorganisasjon. Den kriminelle er i stor grad interessert i lett omsettelige verdier, mens terroristen er interessert i å skape frykt og følger ofte trender i type angrep. Det er vanskeligere å forutse hva en etterretningsorganisasjon kan velge å angripe i virksomheten, da det kan være informasjon som kun har verdi i et større bilde enn det firmaet selv klarer å forstå.

1.2. Tema

Risikofagfeltet har utviklet seg betraktelig fra et tidlig fokus på naturkatastrofer og organisatoriske ulykker til også å fokusere på tilsiktede handlinger fra rasjonelle aktører. Sikkerhetsloven pålegger den enkelte virksomhet å skape et forsvarlig sikkerhetsnivå. Der myndighetene tidligere har gitt klare føringer for tiltak som må gjennomføres i et deterministisk regelverk, er det nå opp til den enkelte virksomhet å analysere seg frem til de riktige tiltakene i det nye funksjonelle regelverket. Dette gjør at sikkerhetsloven nå tar inn over seg den raske endringstakten i sikkerhetssituasjonen i verden, men det skaper utfordringer for virksomhetene som nå må ta ansvar for risikovurderingene som legges til grunn for å skape det forsvarlige sikkerhetsnivået.

Med en høy etterretningstrussel mot norske interesser og norske virksomheter er det interessant å undersøke hvordan man metodisk vurderer risikoen for at en etterretningsaktør gjennomfører innhentingsaksjoner. Oppgavens tema er derfor:

Hvordan utvikle «etterretningstrussel» som en del av en risikovurdering.

1.3. Forsvarets logistikkpartnere som etterretningsmål

Totalforsvarsbegrepet omfatter gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunnet i hele krisespekteret fra fred til væpnet konflikt (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 10). Beredskapsplanleggingen er en del av det de sivile og militære skal samarbeide om i konseptet, og for Forsvaret er det behov for langsiktige avtaler innen visse områder for å sikre beredskapen. Forsvarets logistikkorganisasjon (FLO) forvalter av den grunn avtaler innen logistikken med det som kalles sivile strategiske samarbeidspartnere (Forsvaret, 2020). Den første av disse ble inngått i 2015 med Wilh. Wilhelmsen (Lorentsen, 2015), mens avtaler med Grieg og Bring har kommet til i henholdsvis 2017 (Grande, 2017) og 2018 (Engebretsen, 2019). De strategiske logistikkpartnerne er spesielt viktige for Forsvarets operative evne innen mottak av allierte, samt transport av personell og etterforsyning av mat og drivstoff (Endregard, 2019, s. 78) i forbindelse med sikkerhetspolitiske kriser eller krig. Dermed inngår de sivile leverandørene i den stående militære beredskapen i krig og fred i kontraktens varighet og blir innlemmet i den militære enden av totalforsvaret på en annen måte enn andre sivile bedrifter med kortere militære kontrakter.

Den tradisjonelle forståelsen av logistikk handler om prosesser som kobler sammen aktiviteter for å flytte og lagre varer (Jahre & Persson, 2011, s. 67). Militær logistikk kan defineres som «… aktiviteter og ressurser som organiseres og benyttes for å fremskaffe og understøtte militære kapasiteter i operasjoner.» (Elvemo & Jakobsen, 2020). Logistikken i forbindelse med militære operasjoner er et viktig etterretningsmål ettersom man ved å vite hvor ressursene som skal understøtte operasjoner forflyttes, lettere kan forutse hva den militære operasjonsplanen er. Dette kan man se ved å følge krigen som foregår i Ukraina i disse dager, der kunnskap om etterforsyningene og logistikken til de russiske styrkene kan ha gitt vestlig etterretning og de ukrainske lederne klare indikasjoner på når og hvor angrepene vil konsentrere seg. Det samme så man i forkant av krigen der det ble offentliggjort etterretningsinformasjon om den russiske oppbyggingen i nærområdet (Altman, 2021). Denne informasjonen kan ha kommet blant annet fra etterretning om logistikken til de russiske styrkene, da dette ville ha gitt informasjon om hvilket materiell som ble flyttet og hvor det ble flyttet til. For en mulig motstander vil Forsvarets logistikkpartnere være mulige

etterretningsmål for å få informasjon og kunnskap om forflytninger av norske og allierte styrker. Noe som er vesentlig for å ha en grad av kontroll på hva Norge og North Atlantic Treaty Organization (NATO) eller andre allierte foretar seg i deres nærområde. Denne typen informasjon vil være av vesentlig betydning dersom en fremmed makt skulle vurdere å angripe Norge, eller om de er redde for at våre allierte skal angripe dem.

1.4. Samfunnets avhengighet av nettbaserte løsninger

Cecilie Daae, direktør for Direktoratet for samfunnssikkerhet og beredskap (DSB), skrev i 2019 at Norge var et av landene i verden som hadde kommet lengst i digitalisering av samfunnsfunksjonene (DSB, 2019, s. 8). Utviklingen har fortsatt i stor fart siden den gang og samfunnet er i stadig større grad avhengig av nettbaserte løsninger for å fungere. Informasjon lagres og deles digitalt og gjennom Covid-19 pandemien har stadig flere gjennomført stadig mer av jobben sin via internett. Daae skrev videre at digitaliseringen av samfunnet brakte med seg «nye sårbarheter som vi foreløpig neppe fullt ut forstår dybden i og omfanget av». Det er stor fare for at vi ville oppleve uventede hendelser ettersom det er vanskelig å fullt ut ha oversikt over avhengighetene (DSB, 2019, s. 8) som kommer som en følge av lange og kompliserte verdikjeder. En ytterligere utfordring med utviklingen er at det kanskje ikke er tid til å få oversikt over avhengigheter og sårbarheter, da utviklingen fortsetter i høyt tempo. Siden 2019 har man i Norge startet utrullingen av det digitale 5G-nettet som øker kompleksiteten ytterligere, og som det kun er noen få som forstår omfanget av.

Avhengigheten av nettbaserte løsninger, sammen med kompleksiteten og de mange avhengighetene i verdikjeder, skaper sårbarheter. Disse sårbarheter er det vanskelig å ha kontroll på og de kan gi trusselaktører muligheter til å kompromittere virksomhetene. Med mindre virksomhetene selv jobber godt med å forstå sårbarhetene og iverksetter tiltak. I dette domenet opererer etterretningsaktørene med sine statlige ressurser. Private firma, og ikke minst de som er tilknyttet totalforsvaret, har en stor utfordring når de skal skape forsvarlig sikkerhet i møte med denne trusselen.

1.5. Problemstilling

Andre staters etterretningstjenester er interessert i Norges beredskap og aktørene som er del av denne beredskapen. Alle virksomheter som har en rolle i beredskapen er potensielle etterretningsmål og må av den grunn ta med etterretningstrusselen i sine risikovurderinger når de skal oppnå et forsvarlig sikkerhetsnivå. Dette er en vanskelig trussel å vurdere ettersom aktørene ikke opererer med samme logikk som andre rasjonelle aktører. Så for å forstå etterretningstrusselen må virksomhetene forstå sin rolle som del av totalforsvaret på kort og lang sikt. De må videre forstå hva motstanderen kan ønske å avdekke av informasjon og hvilke kapabiliteter de statlige etterretningsaktørene har tilgjengelig. Virksomhetene forvalter ikke bare sikkerhet for seg selv og sine egne verdier, men også en del av sikkerheten til hele den norske beredskapen.

Totalforsvaret er avgjørende for Norge i vår respons på et angrep mot nasjonen. Forsvarets strategiske logistikkpartnere er av sentral betydning for en militær respons og er av den grunn sannsynlige etterretningsmål. Ettersom sikkerhetsloven pålegger dem å skape et forsvarlig sikkerhetsnivå er det interessant å undersøke hvordan de metodisk utvikler etterretningstrusselen som del av en risikovurdering.

Den raske utviklingen innen data og internettbasert teknologi skaper stadig større sårbarhetsflater som kan utnyttes av aktører med ondsinnede intensjoner. Tempoet i utviklingen og kompleksiteten i verdikjedene vanskeliggjør risikovurderingene som må ligge til grunn for gode sikkerhetstiltak. Det er mange ondsinnede aktører som utnytter den såkalte cyberdimensjonen og statlig etterretning har i flere land vært svært aktive i mange år. Statlige aktører har med sin tilgang på kunnskap og ressurser muligheter til å utvikle metoder og «våpen» til bruk i cyberdomenet. Dette vanskeliggjør ytterligere jobben til virksomhetene som søker å beskytte seg og skape et tilfredsstillende sikkerhetsnivå.

Oppgavens problemstilling er derfor:

I hvor stor grad sikrer risikovurderinger hos Forsvarets strategiske logistikkpartnere, et forsvarlig sikkerhetsnivå mot etterretningstrusler?

1.6. Studiets innretning

For å svare på denne problemstillingen har Forsvarets strategiske logistikkpartnere blitt forespurt om å delta som «caser» ved å la meg gjennomføre dybdeintervjuer om hvordan risikovurderingene blir utviklet. Disse «casene» har jeg deretter analysert for å se på likhetstrekk og forskjeller i tilnærmingen til risikovurderinger i dette lille, men sentrale, miljøet i totalforsvaret.

1.6.1. Forskningsspørsmål

Det har blitt utarbeidet tre forskningsspørsmål for å svare på oppgavens problemstilling.

- Hvordan forholder firmaene seg til et funksjonelt lovverk som sikkerhetsloven?

Dette spørsmålet undersøker firmaenes rolleforståelse som underlagt sikkerhetsloven grunnet sin rolle i totalforsvaret. Det utforsker hvordan firmaene forholder seg til sikkerhetsloven og dens funksjonelle tilnærming som skyver ansvaret for å treffe de riktige tiltakene ned til dem som kommersielle aktører, herunder hvordan forsvarlig sikkerhet forstås.

- I hvilken grad er risikovurderingsprosessen slik den er i dag relevant for å identifisere etterretningstrusler?

Spørsmålet ser nærmere på prosessen for risikovurdering som del av risikostyringen. Det undersøker hvordan prosessen er forankret og med hvilken hyppighet vurderingene oppdateres. Videre utforskes kunnskapsbasen vurderingene baserer seg på og hvordan firmaenes prosesser stemmer overens med teorier om risikovurdering.

- Hvilken metodisk tilnærming har firmaene til risikoanalyse, og hvordan forstås de sentrale begrepene; som sannsynlighet, konsekvens, sårbarhet og verdi?

Her undersøkes begrepsforståelsen og eventuell bruk av metodikk som baserer seg på norske standarder.

Jeg vil videre i studien drøfte funnene som kommer frem gjennom undersøkelsen av disse tre forskningsspørsmålene opp mot relevant teori. Drøftingen vil belyse egnetheten av funksjonelle lovverk for å oppnå ønsket sikkerhetsnivå i totalforsvaret, og egnetheten av standard risikovurderinger mot etterretningstrusler hos kommersielle aktører. Til slutt vil studien forhåpentlig kunne peke på mulige forbedringer i den metodikken som er benyttet for risikovurdering.

2. Bakgrunn

Jeg vil i dette kapittelet utdype noe av bakgrunnen for problemstillingen oppgaven tar for seg. Etterretningstrusselen i Norge i dag vil bli beskrevet med bakgrunn i de ugraderte rapportene som gis ut av Norges hemmelige tjenester. Etterretningstjenesten gir årlig ut en ugradert rapport som heter FOKUS, Politiets sikkerhetstjeneste (PST) utgir Nasjonal trusselvurdering, mens Nasjonal sikkerhetsmyndighet (NSM) gir ut rapporten Risiko. Ser vi disse i sammenheng kan vi danne oss et mer sammensatt bilde av flere nasjonale trusler, også etterretningstrusselen. Videre vil jeg i kapittelet beskrive totalforsvarskonseptet som gir rammen for de strategiske logistikkpartnernes deltakelse i den norske beredskapen. Til slutt vil jeg definere to begreper som er sentrale i problemstillingen: etterretningstrussel og risikovurdering.

2.1. Dagens etterretningstrussel i Norge

Stater benytter seg av etterretningsaktivitet blant annet for å skaffe seg innsikt i sensitive norske sikkerhetspolitiske spørsmål (PST, u.d.). Selv om etterretningstrykket mot Norge har vedvart over tid, har det hatt mindre fokus i offentligheten etter den kalde krigen ble avsluttet. Både Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) har påpekt etterretningstrusselen i sine ugraderte, offentlige vurderinger. PST har allerede i sin første offentlige trusselvurdering et eget avsnitt som beskriver at etterretningsvirksomheten mot norske interesser er på et høyt nivå (PST, 2004). Etterretningstjenesten peker også mot etterretningstrusselen i sin første versjon av FOKUS, når de beskriver at utenlandske etterretningstjenester utnytter seg av det digitale rommet til etterretningsvirksomhet (Etterretningstjenesten, 2011, s. 31). Både PST og Etterretningstjenesten fremhever etterretningstrusselen i årene som følger, men fra 2016 kan det synes som trusselen kommer høyere på agendaen. Etterretningstjenesten skriver at trusselen har vært økende i flere år (Etterretningstjenesten, 2016, s. 82), mens PST setter etterretning som første punkt i sin trusselvurdering for første gang (PST, 2016, s. 6). FOKUS 2019 tydeliggjør utfordringen ved å gi etterretningsvirksomhet mot Norge et eget kapittel, der det tidligere hadde blitt beskrevet i sammenheng med andre utfordringer (Etterretningstjenesten, 2019, ss. 12-19). Etterretningstjenesten er de senere år tydelige på at særlig Russland og Kina gjennomfører betydelige etterretningsoperasjoner mot norske interesser, noe PST har beskrevet i flere år.

Målene beskrives som både offentlige og sivile, og har knytning til alt fra høyteknologi og forskning til forsvar og beredskap.

Digitaliseringen skaper stadig nye muligheter og sårbarheter og Etterretningstjenesten, PST og Nasjonal sikkerhetsmyndighet (NSM) har i flere år vært klare på at statlige aktører benytter seg av samfunnets økende digitalisering i etterretningssammenheng. Allerede i trusselvurderingen i 2009 skriver PST at det er flere stater som er «i ferd med å bygge opp en betydelig kapasitet innen datanettverkoperasjoner» (PST, 2009). Dette har bare økt i takt med samfunnets digitalisering og i 2021 skriver Etterretningstjenesten at russiske og kinesiske etterretningstjenester er spesielt aktive i det digitale rom (Etterretningstjenesten, 2021, s. 16). NSM sier at det digitale risikobildet er skjerpet sammenlignet med 2020 som var et år med mye aktivitet (NSM, 2021, s. 7), mens PST skriver at operasjoner i cyberdomenet vil «utgjøre den største delen av russisk og kinesisk etterretningsaktivitet mot Norge» (PST, 2021). Sårbarhetene i de digitale verdikjedene er så mange og sammenhengene tidvis så komplekse, at det er vanskelig å holde sikkerhetstiltakene oppdaterte og relevante. Trusselaktørene kan benytte seg av kjente sårbarheter der oppdateringer ikke er gjennomført enda, ukjente sårbarheter, leverandørangrep eller forskjellige former for manipulasjon for å oppnå sine mål. De statlige aktørene som sikkerhetstjenestene advarer mot er sofistikerte og har store organisasjoner, som ytterligere vanskeliggjør risikostyringen i bedrifter som utsettes for denne typen oppmerksomhet.

2.2. Totalforsvaret

Totalforsvaret er et begrep som mange har et forhold til, men innholdet i begrepet har endret seg vesentlig siden det først ble beskrevet under den kalde krigen. For å belyse oppgavens problemstilling må totalforsvarskonseptet belyses.

Totalforsvarskonseptet ble utviklet i etterkant av den andre verdenskrig og var en måte å bygge et sterkt forsvar i en liten nasjon med stort og langstrakt areal. Konseptet var myntet på krig og man så for seg en total krig på samme måte som når tyskerne invaderte, og baserte seg på at samfunnets totale ressurser skulle støtte Forsvaret i en kamp for nasjonen. Denne versjonen av det norske totalforsvaret er beskrevet som «en vel planlagt væpnet dugnad»

(Håkenstad, 2019, s. 25) og ved et krigsutbrudd ville sivilt personell massemobiliseres både til Forsvaret og til sivil beredskap. Ved den kalde krigens slutt var det tilsynelatende ikke lenger behov for dette konseptet som i sin helhet handlet om det sivile samfunnets støtte til Forsvaret i tilfelle krig.

Etter den kalde krigen ble samfunnssikkerheten satt stadig mer i fokus. Med dette fokuset kom også behovet for militær støtte under sivile kriser mer frem. Moderniseringen av totalforsvarskonseptet førte da med seg at de totale ressursene som er tilgjengelige i krig, også skal kunne brukes ved kriselignende hendelser i fredstid (Forsvarsdepartementet og Justis- og beredskapsdepartementet, 2018, s. 10). En del av det nye konseptet er Forsvarets langsiktige strategiske avtaler med kommersielle leverandører som skal levere til Forsvaret i fred, krise og krig. På denne måten blir Forsvaret og noen av dets viktigste sivile leverandører integrert i hverdagen og kan støtte hverandre i alle deler av et krisespektrum. Dette gir åpenbare fordeler i samvirket, men fører også til at disse leverandørene blir mer interessante som etterretningsmål da de er tett knyttet til Norges forsvarsevne.

2.3. Avgrensninger

2.3.1. Risikovurdering

ISO 31000 definerer risikovurdering som risikoidentifikasjon, risikoanalyse og risikoevaluering. NS 5830 definerer risikovurdering som en helhetsvurdering av verdi, trussel og sårbarhet. Risikoanalysen er i NS 5830 opphøyet til å inneholde risikovurdering, strategivurdering og tiltaksvurdering, og ettersom dette strider mot resterende standarder har benevnelsen blitt «sikringsrisikoanalyse» i NS 5832. NS 5814 definerer i sin siste versjon, risikovurdering som rammer for vurderingen, identifisering av uønskede hendelser, risikoanalyse og risikoevaluering.

Forståelsen av «risikovurdering» i denne oppgaven følger ISO 31000, og inkluderer dermed risikoidentifikasjon, risikoanalyse og risikoevaluering. Dette da det gir uttrykk for den metodiske og analytiske tilnærmingen som benyttes i å utvikle etterretningstrusselen som faktor. Rammene rundt legges som regel av en ledelse, mens strategien og tiltakene kommer som konsekvenser av identifikasjon, analyse og evaluering av risiko.

2.3.2. Etterretningstrussel

Begrepet etterretningstrussel benyttes i de åpne rapportene til PST og Etterretningstjenesten, men har ikke en blitt definert av noen av dem. Etterretningsdoktrinen beskriver etterretning som «… resultatet av statlig sanksjonert innhenting, analyse og vurdering av data og informasjon, som er generert åpent eller fordekt og utarbeidet for å gi fortrinn i beslutningsprosesser» (Forsvaret, 2021, s. 20). Grunnet mangelen på en allment akseptert definisjon på begrepet etterretning benyttes begrepene etterretningsorganisasjon, etterretningsvirksomhet og etterretningsanalyse i doktrinen (Forsvaret, 2021, s. 18). Det som truer den enkelte organisasjon som gjennomfører en risikovurdering, og som kan motvirkes med tiltak, er innhentingen som er en del av etterretningsvirksomheten.

Etterretningen blir i doktrinen beskrevet som «statlig sanksjonert» (Forsvaret, 2021, s. 20), men for en organisasjon er det ingen grunnleggende forskjell på om innhentingstrusselen er statlig sanksjonert eller ikke. Industrispionasjen har i hovedsak de samme særegenhetene som den statlige etterretningsinnhentingen, og en beskrivelse av spionasje er at det er aktivitet som søker å skaffe informasjon gjennom fordekte og ulovlige metoder (Smith & Brooks, 2013, s. 193).

Etterretningstrusselen er i oppgaven forstått som trusselen for fordekt og ulovlig innhenting av informasjon fra en privat eller statlig sanksjonert organisasjon. Trusselen innebefatter for en virksomhet aktører med kapabilitet, mulighet og intensjon til å rokke ved konfidensialiteten, integriteten eller tilgjengeligheten på virksomhetens informasjon.

3. Teori

Dette kapittelet vil gå gjennom teori relatert til sentrale deler av problemstillingen i oppgaven. Funksjonelle lovverk beskrives og ses opp mot sin motsats i regelbaserte lovverk, med et blikk på utfordringene som skapes for lovverkene med økende kompleksitet. Videre blir etterretningsteori belyst, med ekstra fokus på innhentingen som følge av definisjonen jeg legger til grunn for etterretningstrusselen. Russisk bruk av etterretning blir også brukt som eksempel slik at vi kan forstå en eventuell motstander. Risiko og usikkerhet blir belyst for å skape en teoretisk forankring til fagfeltet. Avslutningsvis blir risikovurderingen beskrevet med fokus på prosessen og de faktorene som legges til grunn i analysen i de norske standardene NS5814 og NS5832.

3.1. Funksjonelle lovverk som regulering av sikkerhetsrisiko

For å kunne gå inn i problemstillingen må vi forstå hva funksjonelle lovverk er og hvordan de virker. Sikkerhetsloven er et slikt lovverk og i forslaget til lovvedtak som ble lagt frem angående denne i 2017 sto det at «… det gjennomgående stilles funksjonelle krav til sikkerhetstiltak.» (Prop. 153 L (2016-2017), s. 8). Jeg vil videre se på hvilke utfordringer kompleksiteten i dagens samfunn bringer med seg for slike reguleringsregimer.

Reguleringsregimer som lovverk kan være funksjonelle eller deterministiske i sin tilnærming til det de regulerer. Innen risikofaget kan forskjellen beskrives som at lovverkene kan være risikostyrte eller regelstyrte. Regelstyrte, eller deterministiske, lovverk legger strenge føringer for hvilke tiltak som skal innføres. Eksempelvis er det en rekke sikkerhetstiltak som skal være til stede for at en flyplass skal få lov til å være operativ. Disse kravene er enkle å følge og det er enkelt for myndighetene å kontrollere hvorvidt lovverket er fulgt. Risikostyrte, eller funksjonelle, lovverk legger få om noen føringer for hvilke tiltak som skal innføres. Det er funksjonelle krav som ligger til grunn og disse kravene «… beskriver hva som skal oppnås, istedenfor hvilke løsninger som skal benyttes.» (Njå, Sommer, Rake, & Braut, 2020, s. 75). Det er tilstanden som skal oppnås som er vesentlig og risikoen som møter det enkelte firma som styrer tiltakene.

Sikkerhetsloven er et funksjonelt lovverk som har som formål «å trygge Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser» (Sikkerhetsloven, 2018, ss. §1-1 a)) og «å forebygge, avdekke og motvirke sikkerhetstruende virksomhet» (Sikkerhetsloven, 2018, ss. §1-1 b)). Loven sier at organisasjonene som er underlagt loven skal opprette «et forsvarlig sikkerhetsnivå» (Sikkerhetsloven, 2018, ss. §4-3). Slike reguleringsregimer bygger på en antakelse om at organisasjonene som underlegges loven selv har kompetansen og kunnskapen som skal til for å forstå risikoen de står ovenfor nå og i fremtiden (Jore & Moen, 2015, s. 679). Gjennom denne forståelsen og kjennskapen til egen organisasjon og egne sårbarheter skal hver enkelt organisasjon bruke den mengden ressurser de har behov for til å sette inn de nødvendige tiltak. Hver enkelt organisasjon vil oppfylle lovverkets krav ved å benytte riktig type og mengde midler, mens de lar en akseptabel restrisiko gjenstå. En av fordelene med slike reguleringsregimer er at det skal føre til en riktig ressursbruk, der forskjellene mellom ulike organisasjoner tas til følge. Det er eksempelvis ikke det samme behovet for sikkerhetstiltak si en gågate i en småby som Otta som det er på Karl Johans gate i Oslo.

Deterministiske lovverk baserer ofte sine regler på faktiske hendelser og er sånn sett et reaktivt lovverk. Funksjonelle lovverk kan derimot være forutseende og endre sikkerhetstiltak i takt med endringer i risikobildet, gitt at organisasjonene har den forutsatte kompetansen og kunnskapen. Dette skaper potensielt et lovverk som er agilt og passer bedre i en hurtig omskiftelig verden, men dersom kompetanse og kunnskap ikke er på plass så er det ikke sikkert at man har kontroll på sikkerheten.

Myndighetenes muligheter for oppfølging av funksjonelle lovverk kan være en utfordring da det er vanskelig å gi en beskrivelse av hva som er godt nok. Et lovverk som inneholder et sett med regler, gjør at myndighetene kan revidere organisasjoners tiltak etter en sjekkliste. Inspektøren kan bedømme om lovverket er overholdt ved å kontrollere om de riktige tiltakene er innført i henhold til loven, og ved manglende overholdelse vil straff kunne følge. Dette er ikke mulig med et funksjonelt regelverk ettersom det ikke er mulig å lage enkle sjekklister som vil gi et fasitsvar på om loven er overholdt eller ikke. Håndhevelse av lovverket med eventuelle straffer er svært krevende om ikke umulig, og inspektørenes rolle har endret seg til å bli rådgivende (Jore & Moen, 2015, s. 680). Dette er ressurskrevende for myndighetene

ettersom en inspektør må ha vesentlig høyere kompetanse med et funksjonelt lovverk. Samtidig vil en inspeksjon eller oppfølging ta betydelig lenger tid siden inspektøren vil være avhengig av å «… besitte veldig høy systemkompetanse.» (Njå, Sommer, Rake, & Braut, 2020, s. 75). Vedkommende må forstå organisasjonens oppbygging, sikkerhetssituasjon og infrastruktur, for å kunne si om ressursbruken og tiltakene er i henhold til lovens intensjon.

Vi kan med andre ord si at et funksjonelt reguleringsregime i teorien skaper et agilt og moderne lovverk som tar høyde for alle trusler man er kjent med i dag og kan utsettes for i fremtiden. Det var beskrevet i lovforslaget at loven skulle være en «… dynamisk og fleksibel rammelov …» som skulle sette «… myndigheter og virksomheter bedre i stand til å sikre disse sentrale nasjonale interessene mot et trussel- og risikobilde i stadig og rask endring.» (Prop. 153 L (2016-2017), s. 7). Utfordringen er at oppnåelsen av sikkerheten står og faller på kompetansen hos de som skal følge lovverket, og de som eventuelt skal følge opp om lovverket overholdes. Denne forutsetningen skaper et stort behov for personell med kunnskap om risikovurderinger og en økt ressursbruk av spesialister som forstår de enkelte farene som kan inntreffe. Dette utfordres blant annet av den økende kompleksiteten i verden.

3.1.1. Kompleksitet og hvordan det utfordrer regulering

Ordet kompleks defineres i Store norske leksikon som «… et sammenhengende hele av innbyrdes selvstendige deler …» eller «… sammensatt av mange elementer eller mangesidig.» (Rzadkowska, 2021). Ut fra ordet kompleks kommer kompleksitet som samme leksikon definerer som «… sammensatt eller innviklet.» (Eilertsen & Persvold, 2019). Disse definisjonene gir en pekepinn på hva man mener når man sier at systemer og verden i sin helhet blir stadig mer kompleks.

Innen risikofaget var det Perrow som gjorde kompleksitet til et populært begrep, som del av sin Normal Accident Theory (Perrow, 1984). Han beskriver systemer der komponenter som ikke hører sammen i prosessen har en nærhet som kan skape uforutsette interaksjoner. Jo oftere disse interaksjonene kan forekomme, jo mer komplekst er systemet. Motsatsen til komplekse systemer er ifølge Perrow lineære systemer der komponentene har avstand til hverandre dersom de ikke skal interagere.

Nancy Leveson beskriver at kompleksitet kommer i mange forskjellige former som alle eksisterer i systemene vi mennesker bygger og benytter. Hun mener at noen av disse systemene nå er så komplekse at bare noen få eksperter kan forstå dem, og at det ikke er sikkert at de engang vil ha forståelse for hva systemet potensielt kan gjøre. Tre relevante eksempler hun trekker frem er; kompleksiteten i hvordan systemkomponenter virker sammen, kompleksiteten som oppstår av endringer over tid, og kompleksiteten i at årsak og virkning ikke henger sammen på en enkel og lineær måte. Disse kaller hun henholdsvis interaktiv, dynamisk og ikke-lineær kompleksitet (Leveson, 2017, s. 4). Den interaktive kompleksiteten øker etter hvert som det er flere systemkomponenter som gjør flere aktiviteter samtidig. Komponentene i et datasenter skaper eksempelvis en høyere kompleksitet enn komponentene i en gammel fabrikk. Den dynamiske kompleksiteten er også stadig økende ettersom endringene i systemer kommer hyppigere. Det er eksempelvis flere endringer på operativsystemer, noe de fleste av oss ser på oppdateringer på mobiltelefonen. For hver oppdatering er det komponenter som er avhengige av prosessen i operativsystemet som også må endres og kompleksiteten økes. Forutsigbarheten i årsak og virkning vil bli mindre etter hvert som annen kompleksitet øker, og den ikke-lineære kompleksiteten øker dermed også. Utfordringen Leveson peker på er at vi mennesker ender med å bygge systemer som er utenfor vår egen fatteevne siden kompleksiteten blir så stor at vi ikke klarer å forutse alle mulige utfall.

Økende kompleksitet gjør regulering vanskelig. Med få eksperter som er i stand til å forstå et gitt system, og med en verden som endrer seg stadig raskere, er det vanskelig å opprettholde gode, deterministiske lovverk. Lovverkene er i hovedsak reaktive og vil sannsynligvis ikke klare å lage regler som er relevante for å skape sikkerhet ettersom antakeligvis ikke vil holde følge med utviklingen. Men kompleksiteten skaper utfordringer for funksjonelle lovverk også. Nettbaserte løsninger har som regel lange verdikjeder med kompleksitet i alle ledd. Det er en høy grad av interaktiv kompleksitet i hvordan de forskjellige komponentene i en nettbasert verdikjede fungerer. Det er videre en utfordring med dynamisk kompleksitet da det stadig kommer nye løsninger og forbedringer på gamle systemer, og tidvis enkeltløsninger for å få gamle komponenter i et system til å fungere sammen med nyere deler av systemet. Det er ikke enkelt å holde kontroll på årsak-virkningssammenhenger, og komponenter som interagerer i et betydelig høyere tempo enn de mekaniske systemene som Perrow i sin tid beskrev. Alt dette

utfordrer den grunnleggende antakelsen som ligger til grunn for funksjonelle reguleringsregimer, nemlig at den enkelte organisasjon har kunnskap og kompetanse nok til å selv velge de beste tiltakene, basert på risikovurderinger, for å skape et forsvarlig sikkerhetsnivå. Det er derfor ikke slik at man bør bruke et utelukkende funksjonelt eller deterministisk reguleringsregime, man er avhengig av å bruke elementer av begge og finne balansen mellom de to (Jore & Moen, 2015, s. 677).

3.2. Etterretning

For å kunne belyse oppgavens problemstilling på må man ha en forståelse for hva etterretning er. Her vil jeg beskrive teori angående hva etterretning som fenomen er og hvordan bruken har endret seg over tid i takt med utviklingen i verden. Det er dessuten vesentlig å være klar over forskjeller i bruk av etterretning på tvers av nasjoner, og jeg vil særlig nevne hvordan Russland bruker sine etterretningstjenester.

3.2.1. Definisjon av etterretning

Etterretning er omtalt som verdens nest eldste yrke (Knightley, 1986), men å definere etterretning er derimot ikke enkelt. Forfatteren John le Carré skal ha sagt at etterretning er informasjonsinnhenting som gjøres i hemmelighet (Andrew, Aldrich, & Wark, 2020, s. 1), men i dagens informasjonssamfunn er ikke det en definisjon som gir verdi. Ofte assosieres etterretning med statlige aktører og en definisjon fra National Security Act fra 1947 legger vekt på at etterretning er informasjon som relaterer seg til kapabilitetene, hensiktene og aktivitetene til andre nasjoner, organisasjoner og personer (Warner, 2020, s. 5). For at en definisjon av etterretning skal gi mening er det ikke nok å vektlegge bare informasjonen. Etterretningens formål er å gi beslutningsstøtte og da er det ikke nok med informasjon alene. Informasjonen må analyseres og presenteres for å kunne gi verdi, og før det er mulig må man innhente riktig informasjon. Forsvarets fellesoperative doktrine beskriver etterretning som «systematisk innhenting og bearbeiding av data og informasjon som angår utenlandske forhold» og presiserer at «Begrepet etterretning brukes om produktet, aktiviteten og organisasjonen som utøver aktiviteten» (Forsvaret, 2019, s. 139). Etterretningsbegrepet benyttes for flere institusjoner enn bare Forsvaret i Norge, da blant annet Politiet og Tollvesenet benytter etterretning mot eksempelvis kriminelle aktører eller terrorister. Definisjonen i Forsvarets etterretningsdoktrine ble derfor i 2021 oppdatert til «… resultatet av

statlig sanksjonert innhenting, analyse og vurdering av data og informasjon, som er generert åpent eller fordekt og utarbeidet for å gi fortrinn i beslutningsprosessen.» (Forsvaret, 2021, s. 20).

3.2.2. Endring i etterretningsbruk over tid

Etterretning var i Norge et rent militært anliggende som ble brukt på taktisk nivå, frem til midten av andre verdenskrig (Forsvaret, 2021, s. 17). På det militære taktiske nivået benyttes da også etterretningen til å gi et fortrinn på slagmarken ved å kjenne fiendens posisjoner, metoder, kapasiteter og så videre. Dermed kan man, ved å kjenne sine egne styrker og svakheter, velge taktikken som vil føre til seier. Dette er klassisk militær etterretning som Sun-Tzu beskrev i sin «Art of War», hvor det kjente sitatet «If you know your enemy and know yourself, you need not fear the result of a hundred battles.» kommer fra (Giles, 2000, s. 11). Men etterretning har over tid, i nasjoner med lengre historie enn Norge, vært mer enn en ren militær disiplin. Både England og Frankrike hadde personer tilknyttet hoffet som hadde som hovedoppgave å samle inn etterretninger om konspirasjoner og mulige invasjoner på 15- og 1600 tallet (Omand, 2019, s. 39). Under andre verdenskrig ble forgjengeren til dagens Etterretningstjeneste formet i eksil i London som Forsvarets overkommandos andre avdeling (Forsvaret, 2021, s. 17). Under den kalde krigen var det i stor grad militære behov som skulle dekkes av etterretningen. NATO og Norge ønsket å ha en så stor kontroll som mulig på hva Sovjet gjorde når det kom til utplassering av styrker og våpenprogrammer (Omand, 2019, s. 42). Etter murens fall ble det mindre behov for denne typen etterretninger, mens det politiske maktapparatet i større grad så et behov for etterretninger som kunne hjelpe i beslutningsprosesser i en hurtig omskiftelig verden. Dagens Etterretningstjeneste er først og fremst til støtte for beslutningstakere i regjeringen og departementene. Dette fører til en vesentlig endring over tid på hva som er interessant å innhente etterretninger om. Det er da viktig å forstå at en etterretningstrussel fra en stat ikke lenger er en trussel kun mot informasjon som kan benyttes militært.

3.2.3. Russisk etterretning

Det er, som Sun-Tzu forteller oss, et behov for å kjenne fienden. Når det er etterretningstrusselen i Norge vi ser på er det ifølge Etterretningstjenesten, Russland og Kina som utgjør våre største motstandere (Etterretningstjenesten, 2022, s. 6). Disse to landene er beskrevet som at de benytter alle statens virkemidler for å understøtte statens mål

(Etterretningstjenesten, 2022, s. 8). Det er tettere knytninger mellom staten og næringslivet i både Russland og Kina enn i vestlige land, og det er sannsynlig at deres etterretningstjenester gjennomfører oppdrag som henter ut informasjon til støtte for firmaer kommersielt. Deres etterretningstjenester er av den grunn med på å hente inn informasjon og gjennomføre aksjoner for flere formål enn å gi beslutningstakerne støtte. Russland beskrives av noen som at de anser seg å være i en pågående politisk og kulturell krig med vesten. Denne følelsen av å være i en krig kan være med på å gjøre russisk etterretningstjenester betydelig mer aggressive og risikovillige enn sine vestlige motparter (Galeotti, 2017). Det å sikre den informasjonen som man selv anser som vesentlig for militære forhold mellom Norge og Russland vil derfor sannsynligvis ikke være nok.

At stater som Russland benytter alle statens virkemidler til å oppnå statens mål er med på å skape den komplekse trusselen som i senere år har blitt omtalt som hybridkrig, hybride trusler eller sammensatte trusler. Dette fenomenet er enkelt forklart at en stat benytter seg av alle sine muligheter for å påvirke en annen nasjon, på tvers av politiske og militære virkemidler. Et kjent tilfelle av dette er den russiske påvirkningen av det amerikanske presidentvalget i 2016 (Congressional Research Service, 2021, s. 18). Vi har også sett Russland bruke sammensatte trusler mot Ukraina både når de annekterte Krim i 2014 og før de invaderte i 2022. For å kunne utføre mange av disse typene trusler er de avhengige av tilgang på informasjon og data som gir påvirkningsmuligheter (Kveberg, Alme, & Diesen, 2019), ikke bare eventuelle militære fortrinn. Det er dermed av interesse for russisk etterretning å skaffe seg tilganger og informasjon som kan være interessant en gang i fremtiden. Dette gjør det veldig vanskelig å analysere seg frem til hva som skal sikres, ettersom vi ikke vet hva som er av interesse.

Russland har over tid satset på etterretning i det digitale domenet (Etterretningstjenesten, 2021, s. 16) og er regnet som meget kapable på området. Eksempelvis er en enhet som er tilknyttet den russiske etterretningsorganisasjonen GRU omtalt i litteratur som APT28 eller «Fancy Bear». Denne gruppen er attribuert som en av to som hacket demokratene i USA i forbindelse med valget i 2016 (Congressional Research Service, 2021, s. 17). Denne enheten har også offentlig blitt pekt på som de som sannsynligvis sto bak dataangrepet mot Stortinget i 2020 (PST, 2020). En annen gruppe som også ligger under GRU er omtalt som «Sandworm» (Congressional Research Service, 2021, s. 17) og står bak et cybervåpen kalt Cyclops Blink

(NCSC, 2022), som senest var omtalt i Dagbladets artikkel 14. april 2022 (Halvorsen, 2022). Russland har i tillegg flere enheter som spesialiserer seg innen det digitale rom, og flere etterretningsorganisasjoner enn GRU, så trusselen fra russisk etterretning i det digitale rom er meget stor.

3.2.4. Etterretningsprosessen

Skal man beskytte seg mot etterretningstrusler så må man forstå prosessen som fører fra oppdragsgivers ønsker til innhenting, analyse og etterretningsprodukter. Denne prosessen er kontinuerlig, noe som gjør truslene vanskelige å beskytte seg mot med periodevise risikovurderinger.

Hele etterretningsprosessen er beskrevet i det såkalte etterretningshjulet med styring, innhenting, bearbeiding og fordeling som en kontinuerlig og syklisk prosess (se figur 1). Produktet skal som Forsvarets definisjon sier, gi et fortrinn i beslutningsprosesser og er derfor beskrevet som beslutningsstøtte. Verden er dynamisk, og beslutningstakerne vil ha behov for å gi nye styringssignaler basert både på endringer i situasjonen og etterretningsproduktet de har fått. Etterretningsprosessen er av den grunn ikke er en ensporet prosess som følger de fire trinnene i en repeterende syklus. Det vil være behov for styringssignaler og dialog mellom og internt i trinnene gjennom hele prosessen.

Etterretningsprosessen starter i modellen med styring fra beslutningstakerne. Denne styringen gir hvilke problemstillinger som ønskes belyst og hvilken informasjon det er behov for, og innhentingen av data og informasjon som kan bidra til å belyse problemstillingene blir så iverksatt. Innhentingsprosessen defineres i NATO doktrine som «… the exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for use in the production of intelligence." (NATO, 2016, ss. 4-1). Kilder kan i denne sammenhengen være alt fra åpent tilgjengelig informasjon, via mennesker til IKT systemer, og disse «utnyttes» ved at informasjon hentes fra dem.

Informasjonen som er innhentet gjøres tilgjengelig for analytikere. Som gjennom «… collation, evaluation, analysis, integration and interpretation.» (NATO, 2016, ss. 4-1) gjør

større mengder data og informasjon fra flere ulike kilder om til etterretning som kan rapporteres tilbake til beslutningstakerne. Disse etterretningene søker å være prediktive ved å belyse ulike tolkninger av informasjonen som har blitt hentet inn. Med dette blir flere ulike fremtids scenarier vurdert i forhold til sin sannsynlighet.

Etterretningsprosessen avsluttes ikke etter at hjulet har gått en runde, men fortsetter kontinuerlig ved at man henter inn ytterligere informasjon som skal søke å bekrefte eller avkrefte scenariene som er utarbeidet. Styringen til innhentingsapparatet kommer da både fra beslutningstakerne og analytikerne som har et ønske om ytterligere innhenting. I modellen beskrives dette som Intelligence Requirement Management and Collection Management (IRMCM), og det er dette som sørger for at etterretningsprosessen er kontinuerlig i sin natur.

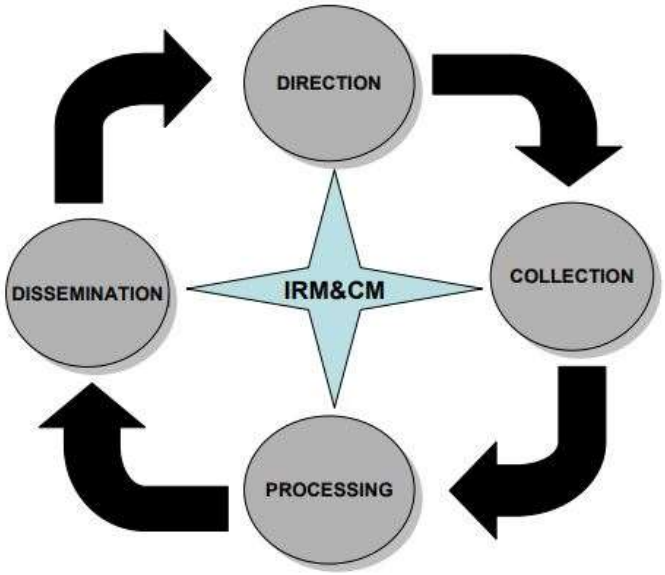


Figure 2: The Intelligence Cycle

Figur 1 – Etterretningshjulet (AJP-2, s4-2)

3.2.5. Innhenting

Jeg har i oppgaven definert etterretningstrusselen for de aktuelle firmaene som en trussel for fordekt og ulovlig innhenting, og vil derfor gå nærmere gjennom innhentingsfasen av etterretningshjulet. I Figur 1 er denne beskrevet som «Collection» og tar styringssignaler fra etterretningsledelsen, fremvist som «Direction» i figuren. Det som hentes inn sendes deretter videre til prosessering, men det er ikke slik at etterretningshjulet går endimensjonalt rundt.

Sentralt i figuren ligger IRMCM som styrer etterretningsbehovet og innhentingsbehovet fortløpende. Her går signalene mellom de fire delene av hjulet kontinuerlig slik at analytikerne eksempelvis kan påvirke hvilken informasjon som skal hentes inn ut fra hvilke behov de har i sin pågående analyse.

Innhentingsledelse er også et selvstendig fagfelt innen etterretningen ettersom man må forstå sensorene som kan hente inn informasjon for å benytte riktig innhentingsressurs på et gitt oppdrag. En metode for å analysere hvilke ressurser som skal benyttes for å hente inn informasjon er «targeting»-metodikk. Denne metodikken beskrives i NATO som en prosess for utvelgelse og prioritering av mål, der målene klassifiseres som «… facility, individual, virtual entity, equipment or organization (FIVE-O) …» (NATO, 2021, ss. 1-1), og selv om det ikke er gitt at andre følger samme doktrine er det antakelig at prosessen ligner. Når målene er klassifisert og vurdert velger man så de beste midlene til å skape den ønskede effekten. Effekten i etterretningssammenheng vil være å hente ut den informasjonen man ønsker til bruk i etterretningsanalyse eller som en del av de mulige sammensatte truslene som kan benyttes mot en stat. Bruken av «targeting»-metodikken er med på å gjøre at etterretningsorganisasjoner analyserer hele store nettverk og verdikjeder for å finne den beste metoden for å finne informasjonen de ønsker. Eksempelvis er det sannsynlig at man analyserer hele totalforsvaret for å finne informasjon som kan gi beslutningsstøtte, eller sårbarheter som kan utnyttes som en del av de sammensatte truslene.

For å finne gode tiltak som kan forhindre etterretningen i størst mulig grad må staten og private aktører analysere mulige trusselaktører. Til dette er det naturlig å benytte risikovurderinger på samme måte som man gjør mot kriminalitet, sabotasje og terrorisme. Denne delen av risikofaget kalles ofte «security» og ser spesielt på risikoer som følge av handlinger som gjennomføres med vilje av rasjonelle aktører. Risiko for tilsiktede handlinger har blitt definert som trusselen mot en gitt verdi og verdiens sårbarhet mot trusselen (Engen, et al., 2017, s. 87). Risikoen beskrives for hver verdi man ønsker å beskytte, og det kreves analyse av de aktørene som kan utgjøre en trussel mot verdien og sårbarheten verdien har ovenfor trusselen. Ettersom en rasjonell aktør vil kunne endre sin fremgangsmåte i forhold til de sikkerhetstiltakene de møter er dette en meget dynamisk risiko. Trusselaktørenes evne til å omgå eller forsere de tiltak må derfor også vurderes.

3.3. Risiko og usikkerhet

Begrepene risiko og usikkerhet er viktige for problemstillingen for å sikre at man har et klart forhold til hva som legges i dem. Dette er begreper de fleste har et forhold til i det daglige, men alle legger ikke det samme i begrepene. Forståelsen fra dagligtale reflekterer heller ikke hva begrepene må inneholde for å belyse denne problemstillingen på en god måte.

Risiko er i dagligtale forbundet med faren for at et tap eller en annen uønsket hendelse inntreffer. Ser man derimot på risiko med akademiske øyne så er det flere ulike definisjoner på risiko. Disse skaper forskjellige forutsetninger for en videre analyse og vurdering av risikoene man står overfor. Uten en klar formening om hva man legger i begrepet kan beslutningstakerne baserer sine beslutninger på feil forståelse og risikoanalyser som fokuserer på feil områder. Eksempelvis uttalte professor Terje Aven etter rapporten til 22. juli kommisjonen ble publisert at samfunnet ville gamble og benytte sine ressurser feil dersom den rådende risikotenkningen ble videreført (Aven, 2012b). Den rådende tenkningen Aven kritiserte var å definere risiko som et produkt av sannsynligheten og konsekvensen for en uønsket hendelse.

En klassisk definisjon av risiko (R) er at risiko er et produkt av sannsynlighet (P) og konsekvens (C). Denne definisjonen har en realfaglig bakgrunn da faktorene kan beskrives i tall og risikoen matematiske regnet ut med formelen (R=C*P). Sannsynligheten er et tall mellom 0 og 1, der 0 viser at hendelsen er utelukket mens 1 viser at hendelsen er garantert. Konsekvensene er en tallfestet verdi som beskriver størrelsen på utfallet. Utfallet kan være mange forskjellige størrelser, eksempelvis antallet skade eller drepte eller en kroneverdi som blir vunnet eller tapt. Gjennom å multiplisere sannsynlighet og konsekvens for alle mulige utfall av en hendelse får man en forventet verdi som gir et risikotall som kan benyttes. Denne metoden gjør det enkelt å sammenligne risikoer, men blir blant annet kritisert for å ikke gi nok fokus på utfall som har en kombinasjon av høy konsekvens og lav risiko. Derfor er en annen relatert definisjon at risiko er knyttet til konsekvensene av en aktivitet og tilhørende sannsynlighet (Aven, 2015, s. 41) som beskrives (R=C, P). Risiko er i denne definisjonen fortsatt tenkt som en kvantitativ størrelse da konsekvensene normalt angis i en numerisk verdi

og sannsynlighet er et matematisk begrep som angis av tall mellom 0 og 1. Risikotallet man får ved å multiplisere de to faktorene er dog ikke like vesentlig i denne definisjonen.

Aven sin kritikk i 2012 var rettet mot et manglende forhold til usikkerhet og kunnskapsstyrke i analysene som ble gjennomført. Han beskriver risiko som en «… kombinasjon av konsekvensene C av aktiviteten og tilhørende usikkerhet U (vi vet ikke hva C vil bli).» (Aven, 2015, s. 42). Denne definisjonen av usikkerhet beskrives (R=C, U). Usikkerheten kan uttrykkes som sannsynlighet i denne definisjonen også, men den har med seg perspektivet om at det er usikkerhet rundt hva konsekvensen blir. Dersom man regner ut risikoen med dette perspektivet kommer kunnskapsstyrken inn som en faktor. Det er i denne sammenhengen viktig å vite hvilken kunnskap sannsynligheten bygger på, for konsekvensen man har valgt. Dette legger en dimensjon oppå tallene som blir presentert dersom risikoen regnes ut kvantitativt. Definisjonene Aven derfor legger til grunn, og som viser hans motsats til den «foreldete tenkningen» (Aven, 2012b), er at risiko er kombinasjonen av konsekvensene av en aktivitet og den tilhørende usikkerheten. Når denne risikoen skal beskrives gjøres det for den enkelte utvalgte konsekvens og dens tilhørende sannsynlighet og kunnskapsstyrken konsekvensen og sannsynligheten er basert på (Aven, 2015, s. 60).

Det er ingen entydig definisjon på usikkerhet (Njå, Sommer, Rake, & Braut, 2020, s. 48), men for NS-ISO 31000:2018 definerer like fullt risiko som virkningen av usikkerhet knyttet til mål. Usikkerheten gjennomsyrer på mange måter hele risikobegrepet. Det er usikkerhet i fortiden vi har hentet kunnskap og erfaring fra, i nåtidens utregning eller analysere og beskrivelse av risikoen, og i fremtiden i forhold til hvilke faktorer som vil endre seg og hvilke hendelser som vil inntreffe. Direktoratet for samfunnssikkerhet og beredskap (DSB) benytter i Nasjonalt risikobilde 2014 en tabell med fire hovedkilder til usikkerhet i risikoanalysen som er beskrevet av Elvik.

Figur 1 – Usikkerhetskilder (DSB, 2014, s. 22)

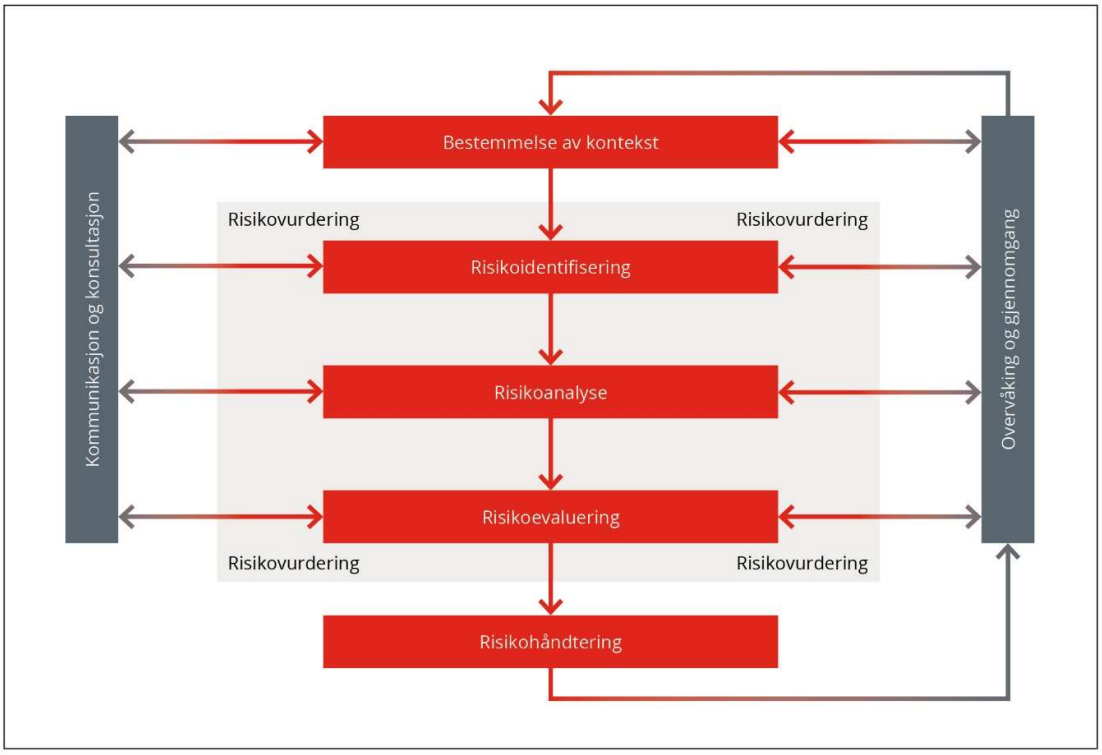
Disse fire beskriver usikkerheten i både fortiden, nåtid og prediksjonen av fremtiden. I tillegg er det usikkerhet om hva som faktisk kommer til å skje og hvilke konsekvenser det vil ha.

Statistisk usikkerhet viser til usikkerheten som stammer fra datautvalget analysen baserer seg på. Dataene skal være et representativt utvalg, men for eksempel kan tilfeldige variasjoner i datasettet sannsynliggjøre sammenhenger som ikke egentlig finnes. Det er i tillegg vanskelig å ha kontroll på alle faktorene som avgjør hvorvidt dataene er representative, og om alle relevante faktorer er observert og gjort rede for i datainnsamlingen. Teoretisk usikkerhet er usikkerheten vedrørende holdbarheten av forklaringsmodellene og forutsetningene som ligger til grunn for teorien som er anvendt. Det er vesentlig å tydeliggjøre alle forutsetninger og antakelser som ligger til grunn for analysen, men hvilken effekt eventuelle feil har er vanskelig å forutse. Metodeteknisk usikkerhet viser til usikkerheten ved om metoden som er valgt er hensiktsmessig for å gi forutsigbarhet. Eksempelvis kan en analysemetode som baserer seg på en kausal-tankegang, basert på en direkte årsak og virkningseffekt, komme frem til feil konklusjoner i et tilfelle der systemet som analyseres er mer komplekst enn analytikerne forstår. Kontekstuell usikkerhet er usikkerheten om hvor sensitiv modellen vår er for endringer i forutsetningene. Med tiden vil forutsetninger og faktorer endre seg, men det er usikkert hvor mye disse endringene vil endre utfallet.

3.4. Risikovurdering

Risikovurdering står helt sentralt i analysen av problemstillingen ettersom det er i denne prosessen at etterretningstrusselen skal utvikles som faktor. En teoretisk tilnærming til risikovurderingsprosessen må beskrives for å kunne vurdere metoden som benyttes av virksomhetene. Risikovurderingsprosessen er sterkt knyttet til standardene som benyttes og risikoperspektivene som ligger i modellene som benyttes i dem. Av den grunn vil jeg eksemplifisere trinnene i risikovurderingen med hjelp av de norske standardene NS5814 og NS5832. Disse to standardene er delvis divergerende ettersom 5832 har et hovedfokus på å håndtere «… tilsiktede uønskede handlinger.» (NS 5832, 2014, s. 2), som kan beskrives som et rent «security» perspektiv. Denne standarden beskriver risiko som en kombinasjon av faktorene verdi, sårbarhet og trussel. På den andre siden er 5814 en standard som har sitt fundament innen «safety» verden, og frem til sin revisjon i 2021 forholdt den seg til risiko som en kombinasjon av sannsynlighet og konsekvens. I sin siste versjon, NS5814:2021, har standarden hatt som mål å «… gjenspeile utviklingen i risikoforståelse …» (NS 5814, 2021, s. vii) blant annet ved å ha et klarere forhold til usikkerhet. Dessuten ønsker man med standarden å synliggjøre sammenhengen mellom NS5814 og NS5832, ved å ta med verdi, trussel og sårbarhetsfaktorene.

Risikovurderingen er et element av den totale risikostyringsprosessen som er visuelt fremstilt i figur 2. Risikostyringen er «alle tiltak og aktiviteter som gjøres for å styre risiko» (Aven, 2015, s. 13) i en organisasjon. Overordnet skal organisasjonen gjennom risikostyring få kontroll på sitt eget risikobilde ved å fastsette sin egen kontekst, identifisere, analysere og evaluere risikoer, og sette inn tiltak for å håndtere risikoen. Prosessen er illustrert på en måte som tydelig viser at dette er en kontinuerlig og ikke-lineær prosess. Denne måten å se risikovurdering på er lik som i NS5814 og NS-ISO31000, mens NS5832 divergerer i sin begrepsbruk. NS5832 benytter seg av begrepet «sikringsrisikoanalyse» som består av igangsetting, sikringsrisikovurdering, vurdering av strategi og vurdering av tiltak. Grunnleggende dekkes de samme delene av sikringsrisikostyring i NS5832 og risikostyring i NS5814, med unntak av at verdivurderingen er en sentral del av «sikringsrisikovurderingen».



Figur 2 – Risikostyringsprosessen (Justis- og beredskapsdepartementet, 2019, s. 6)

3.4.1. Risikoidentifikasjon

Selve risikovurderingen starter, som vi ser i figur 2, med risikoidentifikasjon som består av identifisering av ulike trusler, farer og muligheter organisasjonen står ovenfor i rammen som er gitt. Denne identifiseringen må benytte seg av den beste tilgjengelige kunnskapen og det er anbefalt å dra nytte av kunnskapen til alle interessentene (NS-ISO 31000, 2018, s. 11). For å få frem alle de mulige uønskede hendelsene kan gruppen benytte bakgrunnsinformasjon som historiske data for egen organisasjon eller andre tilsvarende organisasjoner. Videre kan det være at myndighetene, akademia eller ulike interesseorganisasjoner har publisert informasjon som er nyttig. Det er også fornuftig å gjennomgå tidligere analyser som er gjort på området, og i tillegg bruke ulike teknikker for å identifisere mulige farer som ikke har inntruffet enda. Analytikerne kan benytte seg av forskjellige teknikker som «brainstorming» og scenariobygging for å skape seg et best mulig bilde av alle truslene. Brainstorming bygger på at man skal åpen opp for muligheter man kan se for seg, men som ikke nødvendigvis finnes i dataene og kunnskapen man benytter. Alle ideer skal frem og vurderes seriøst. Scenariobyggingen kan bygge videre på enten en «brainstorm» eller andre data, og forsøker å

beskrive hvilke hendelser et handlingsforløp kan føre til. Det er uansett hvilke teknikker man benytter seg av vesentlig at man samler analytikere i åpne og ærlige diskusjoner for å identifisere så mange relevante trusler som mulig i dette trinnet.

3.4.1.1. Verdi

NS5814 beskriver risikoidentifikasjonen med utgangspunkt i at verdiene som skal beskyttes er beskrevet i det første trinnet av risikostyringen. NS5832 har som sagt verdivurderingen som sitt første trinn i sikringsrisikovurderingen. Verdiene er uansett viktige å ha kontroll på og for å gå nærmere inn på verdivurderingen er det viktig å se nærmere på verdibegrepet i seg selv.

Verdi er gjerne i hverdagen forbundet med penger og en monetær verdi. Begrepet er også gjennom filosofien, forbundet med alle ting. Mennesker, objekter, handlinger og tilstander kan alle tillegges verdi, og ofte skilles det mellom det som har verdi i seg selv og det som har en verdi med bakgrunn i å være et middel for å realisere verdi (Sagdahl, 2019). Verdiene som forvaltes av en virksomhet er mange og veldig ulike. Informasjon er en verdi, og i dagens samfunn kanskje den viktigste verdien en virksomhet har. Systemene der informasjonen lagres og deles har også en viss egenverdi, men ved bortfall av et datanettverk er det ofte større verdi i informasjonen enn i systemet. Det samme kan til en viss grad sies om personer, da deres verdi i en sikringsrisikoanalyse øker ut fra hvilken tilgang de har til informasjon. En utfordring med vurdering av verdier er at man må forholde seg til mer enn sin egen verdisetting. Man kan som virksomhet forvalte verdier på vegne av andre virksomheter, lokalsamfunnet eller nasjonen. Ofte kategoriserer man konsekvensklasser som «liv og helse», «informasjon», «operativ evne», «omdømme» og «økonomi» (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 32) for å kunne operasjonalisere verdivurderingen ytterligere.

I sin beskrivelse av risikovurdering benytter Smith og Brooks begrepet «criticality» heller enn verdi. De beskriver at man skal rangere alle ressurser, mennesker og informasjon, etter hvor kritiske de er for organisasjonens evne til å oppnå sine mål (Smith & Brooks, 2013, s. 66). Mens i NS5830, som beskriver terminologien som benyttes i NS5832, er verdien beskrevet som en ressurs. Ressursen kan være materiell som infrastruktur, eller immateriell som omdømme og informasjon. Det som gjør verdien interessant for risikovurderingen er at den kan utsettes for påvirkning som har negative konsekvenser for de som eier, forvalter eller drar

nytte av den (NS 5830, 2012, s. 4). Verdivurderingen er som Brooks og Smith beskriver angående «criticality», en identifikasjon av alt som skal beskyttes for å sikre at organisasjonen kan oppnå sine mål. En viktig presisering beskrives i NS5832, da vurderingen skal ta inn over seg «… alle verdier den [organisasjonen] eier, forventer å eie i fremtiden eller forvalter for andre eiere.» (NS 5832, 2014, s. 6). Når listen over verdier som skal beskyttes mot etterretningstrusler skal lages må dermed alle verdier vurderes, også verdier som forvaltes av organisasjonen for andre eiere eller nasjonen. Dette er også reflektert i NS5814 der det beskrives at «Overordnede verdier og interesser kan spenne fra nasjonale sikkerhetsinteresser og samfunnsverdier til virksomhetens egne interesser.» (NS 5814, 2021, s. 5).

NS5832 beskriver i tillegg til verdivurderingen en fastsettelse av hvor godt en verdi skal fungere under eller etter en påvirkning som neste trinn etter verdivurderingen (NS 5814, 2021, s. 6). Det er ikke mulig å sikre alt fullt ut så en slik vurdering er nødvendig for den senere risikoevalueringen, og ligger sammen med verdivurderingen i en tidligere fase av risikostyringen i NS5814.

3.4.1.2. Trussel

Identifikasjonen av uønskede hendelser skal finne farer og trusler som kan gå ut over de verdiene som skal beskyttes, uavhengig av om de er grunnet naturlige fenomener, teknisk svikt eller menneskelige handlinger. NS5814 benytter trusler som begrep på tilsiktede hendelser og kunnskapen som skal benyttes for å analysere dem kan være tidligere hendelser, trender, etterretningsinformasjon og trusselvurderinger (NS 5814, 2021, s. 6). Hendelser som skal gå videre til analysetrinnet må kunne føre til en tap i verdi. De må også være representativt for de risikoene som er identifisert og relevante for objektet som analyseres. Hendelsene kan utvikles videre til mer detaljerte scenarier dersom det er behov for en mulighet for en mer detaljert vurdering. I NS5832 er trusselvurderingen beskrevet som en identifikasjon og beskrivelse av mulige trusselaktører. Som del av denne beskrivelsen kommer en vurdering av intensjonen og kapasiteten disse aktørene innehar.

En trussel er, når man ser på tilsiktede handlinger, en spesifikk type ondsinnet handling som kan ramme objektet for risikovurderingen som gjennomføres. Truslene kan kategoriseres ut fra type handling som gjennomføres, eksempelvis kriminalitet, sabotasje, terrorisme og

spionasje (Njå, Sommer, Rake, & Braut, 2020, s. 258). Trusselen kan defineres som et produkt av intensjon og kapabilitet (Smith & Brooks, 2013, s. 64). Der intensjonen videre brytes ned til en kombinasjon av trusselaktørens ønske og forhåpning, mens kapabiliteten er sammensatt av ressursene og kunnskapen aktøren besitter. En veileder fra PST, NSM og POD fra 2015 peker på historikk, tilstedeværelse, intensjon og kapasitet som fire relevante faktorer (NSM, PST og POD, 2015, s. 16). For å vurdere trusselen skal man vurdere om det er noen historikk på lignende hendelser tidligere mot tilsvarende bedrifter og hvorvidt noen trusselaktører er til stede i området som virksomheten ønsker å beskytte. Videre skal man vurdere intensjonen og kapasiteten til de mulige trusselaktørene for å ha et grunnlag for å beskrive trusselen. Det kan i tillegg være fornuftig å analysere aktørenes målvalg for å få et forhold til sannsynligheten for at en handling vil bli gjennomført (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 32). Trusselen utvikles ofte videre til scenarioer for lettere å kunne analysere videre. Disse scenarioene må være relevante, konsistente og plausible sier veilederen (NSM, PST og POD, 2015, s. 18), ellers vil de ikke være nyttige i den videre analysen.

3.4.2. Risikoanalyse

Risikoanalysen er neste del av risikovurderingsprosessen og skal ta de identifiserte farene og analysere disse for å skape et risikobilde. Risikoanalyser kan gjennomføres på ulike måter og kategoriseres ofte i forenklede, standard og modellbaserte analyser (Aven, Røed, & Wiencke, 2017, s. 16). Forenklede risikoanalyser er som regel kvalitative og gjennomføres med få involverte som deltar i en relativt uformell gjennomgang. Analysen består som regel av gruppediskusjoner som skaper en konsensus i gruppen for hva risikoen forbundet med den enkelte fare er. Denne typen analyser fører som regel til en presentasjon av risikoene på en grov skala, der risikoene betegnes i bolker som liten og stor. Standard risikoanalyser er noe mer formelle og benytter seg av anerkjente risikoanalysemetoder som grovanalyser og andre modeller, for å utvikle risikoene. Disse analysene kan være kvalitative eller kvantitative og fører ofte til en presentasjon av risikobildet i risikomatriser. Modellbaserte analyser identifiserer og kvantifiserer risiko, ved hjelp av modeller som eksempelvis regner ut sannsynligheten for alle mulige konsekvenser av en hendelse. De modellbaserte risikoanalysene er derfor i hovedsak kvantitative analyser som baserer seg på en strukturert gjennomgang av årsak og virkning.

3.4.2.1. Sårbarhet

Sårbarhetsanalysen ligger som første del av risikoanalysen i NS5814 (NS 5814, 2021, s. 7). NS5832 har ikke et klart skille mellom risikoidentifikasjon og risikoanalyse, men det legges stor vekt på sårbarhetsanalysen som en av de tre faktorene metodikken hviler på.

Sårbarhet kan beskrives som mottakeligheten for et scenario (Ezell, 2007), og beskrives i de norske standardene som analyseobjektets «… manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning» (NS 5830, 2012, s. 5). Denne beskrivelsen gjenspeiler også sårbarhetsutvalget sin rapport fra 2000 der det også påpekes at sårbarhet er knyttet opp mot tap av verdi, og at det sårbare systemet eksempelvis kan være staten, et firma eller enkeltstående datasystemer (NOU, 2000). Sårbarheten når vi ser på etterretningstrusselen beskriver i hvilken grad en aktør kan utføre en handling uten å bli stanset. Dette er avhengig av hvilke sikringstiltak som er iverksatt, men også av aktørens evne til å omgå tiltakene. Dette skiller sårbarhetsvurderingen for tilsiktede handlinger fra sårbarhetsanalyser innen safety-faget. Barrierer i safety-perspektivet kan svekkes over tid eller ikke være dimensjonert for en gitt hendelsen, men vil ellers fungere mot det de er ment for. Når trusselen kommer fra en rasjonell aktør, kan derimot alle typer tiltak i teorien omgås eller forseres. Sårbarhetsanalysen i security-perspektivet er derfor avhengig av en forståelse av de barrierene og tiltakene som er implementert, og aktørens ressurser og kapabilitet til å omgå eller forsere disse (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 33).

Sårbarhetsanalysen eller -vurderingen skal vurdere hvor sårbare verdiene som skal beskyttes er for at en uønsket hendelse skal inntreffe. Gjennom vurderingen skal man se om det finnes eksisterende sikringstiltak eller barrierer som kan forhindre de truslene og farene som er identifisert. Videre kartlegges eventuelle svakheter som kan føre til at en hendelse får utvikle seg og ha uønskede effekter. Analysene kan gjøres med hjelp av en gjennomgang på objektet dersom det er et fysisk objekt, en såkalt «site survey». En annen teknikk som kan benyttes er en versjon av «targeting» som tidligere er beskrevet som en metodikk innen innhentingsledelsen i etterretning (Smith & Brooks, 2013, s. 68). Det er uansett viktig for sårbarhetsvurderingen å forstå sine egne verdier og truslene som truer dem. Når man vurderer

etterretningstrusselen er det eksempelvis viktig å sette seg i trusselaktørens situasjon og se på sine egne systemer med deres briller, der våre sårbarheter fremstår som deres muligheter.

3.4.2.2. Sannsynlighet

NS 5814 baserer seg på at risiko er en kombinasjon av usikkerhet eller sannsynlighet og konsekvens. Det kan benyttes tallfestede verdier for sannsynlighet og konsekvens, men det er også mulig å beskrivelse faktorene i prosa. Dersom faktorene ikke er tallfestet er det normalt å lage bolker av sannsynlighet og konsekvens som er beskrevet som eksempelvis stor, middels og lav/liten.

Sannsynlighetsbegrepet er sentralt i dette perspektivet på risiko, enten som del av definisjonen eller som en metode for å belyse usikkerhet. Sannsynlighet er i dagligtale et begrep som uttrykker hvor trolig det er at en hendelse oppstår, men det er usikkert om det finnes en «korrekt» sannsynlighet for ulike hendelser. Den matematiske sannsynligheten for et utfall er et tall mellom 0 og 1 der 0 viser at utfallet er umulig mens 1 viser at utfallet er garantert. Denne typen sannsynlighet er en frekvensfortolkning (Aven, Røed, & Wiencke, 2017, s. 46) og henviser til antallet ganger et utfall inntreffer dersom hendelsen gjennomføres et stort antall ganger. Denne typen sannsynlighet kalles på engelsk «probability» og det er mulig å regne seg frem til den korrekte sannsynligheten for at ulike hendelser oppstår. I en risikoanalyse vil det være vanskelig å definere et eksperiment som vil kunne gjentas i det uendelige, og tidsenheter benyttes derfor ofte for å angi sannsynligheten. Ser man eksempelvis på flomfare kan man beskrive sannsynlighet som x ganger per år, tiår eller lignende. Et annet engelsk begrep for sannsynlighet er «likelihood» og det fører til en annen fortolkning av sannsynlighet. Likelihood kan sies å være subjektive sannsynligheter, som også kalles kunnskapsbasert sannsynlighet er da et uttrykk for analytikerens usikkerhet i forhold til et utfall (Aven, Røed, & Wiencke, 2017, s. 46). Denne typen sannsynlighet vil oppdateres fortløpende etter hvert som ytterligere kunnskap, data og informasjon legges til. Sannsynligheten kan fortsatt uttrykkes som et tall, men dette tallet vil ikke bli likt uavhengig av hvilken analytiker som gjennomfører analysen. Sannsynligheten i en risikovurdering er todelt da man både må forholde seg til sannsynligheten for at hendelsen inntreffer og sannsynligheten for at hendelsen har en gitt konsekvens.

Sannsynlighetsvurderingen i risikoanalysen skal beskrive hvor trolig det er at en uønsket hendelse inntreffer. Denne beskrivelsen er en subjektiv oppfatning som er avhengig av blant annet kunnskapsstyrken i analysegruppen og hvor godt bakgrunnsmaterialet analysen bygge på er. Sannsynligheten for ulykker som ikke er tilsiktede kan til en viss grad analyseres med hjelp av historiske data og statistikk, mens det for tilsiktede handlinger i hovedsak er en kvalitativ vurdering. NS5832 har tilsynelatende ikke et klart forhold til sannsynligheten ved de forskjellige scenarioene, men denne er avhengig av vurderingene av verdi, trussel og sårbarhet. Det mangler slik sett bare den eksplisitte beskrivelsen av sannsynlighet dersom man følger denne metodikken. NS5814 har i siste revisjon tatt med perspektivet rundt tilsiktede handlinger og faktorene verdi, trussel og sårbarhet, som ofte kalles trefaktormodellen. I standardens beskrivelse av sannsynlighetsvurdering foreslås en systematisering av sannsynlighet for tilsiktede hendelser. Gjennom denne beskriver man sannsynligheten for at en verdi vil angripes og sannsynligheten for at et angrep vil lykkes dersom angrepet finner sted.

3.4.2.3. Konsekvens

Konsekvenser er følger, virkninger eller resultater av noe som skjer (Henriksen & Tranøy, 2021). I risikoanalyse er konsekvenser mulige følger av den uønskede hendelsen som analyseres. Konsekvenser, som nevnt i beskrivelsen av verdifaktoren, vil være av flere typer som eksempelvis liv og helse, omdømme, verdier eller skade på miljøet. De trenger ikke bare være direkte følger av en hendelse, men kan være indirekte konsekvenser. For eksempel er de direkte konsekvensene av Covid-19 pandemien helsemessige, men det har i tillegg vært vesentlige indirekte konsekvenser for økonomien blant annet på grunn av utfordringer ved å frakte varer over landegrenser. Konsekvensene kan beskrives på flere måter i en risikoanalyse, enten med tall eller med ord, og det kan oppstå flere konsekvenser for en enkelt hendelse.

Når konsekvenser benyttes i en risikoanalyse så er det vesentlig å være klar over hvordan konsekvensen som analyseres er fastsatt. En uønsket hendelse som har konsekvenser for liv og helse kan, ut fra hvordan andre faktorer spiller inn, føre til 100 døde eller 1 skadet. Eksempelvis vil det være store forskjeller i konsekvensen for liv og helse av en boligbrann utfra tidspunktet det brenner. Konsekvensen kan fastsettes på flere måter i analysen. Man kan

velge å benytte den mest sannsynlige konsekvensen ut fra en sannsynlighetskartlegging av alle mulige konsekvenser. Alternativt kan man velge seg ut de konsekvensene som ansees som de verste mulige for å sikre seg best mulig mot et «worst case»-scenario, eller et gjennomsnitt av alle mulige konsekvenser sett opp mot sannsynligheten for de forskjellige utfallene.

NS5832 har ingen åpen vurdering av konsekvensene for en gitt risiko, men i verdivurderingen vil det som regel finnes et forhold til konsekvensdimensjonen. Verdi- og trusselvurderingen skal føre til valg av scenarioer som videreutvikles, og når disse skal velges skal de være «… relevante for videre analyse.» (NS 5832, 2014, s. 6). For å sikre at man velger de mest relevante scenarioene er det vesentlig å ha et forhold til hvilke konsekvenser den enkelte verdi kan utsettes for. Dette stemmer også overens med tankegangen rundt «criticality», eller kritikalitet på norsk, som ble beskrevet i underkapittelet om verdi.

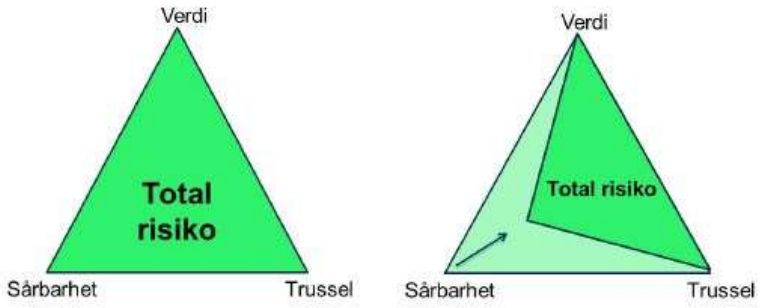
Risikoanalysen i NS5814 har konsekvensanalysen som integrert del. Konsekvensene de forskjellige uønskede hendelsene kan få for de beskrevne verdiene må analyseres og kan beskrives på flere måter gjennom antall, omfang eller varighet av tap, eventuelt grad av tap for mer abstrakte konsekvenser. Men det er påpekt at det er et behov for å vurdere risikoer opp mot hverandre og at det da er behov for å benytte samme typer og kategorier av konsekvenser (NS 5814, 2021, s. 6). Dette er en utfordring når det kommer til å beskrive mulige konsekvenser av en etterretningstrussel. En uønsket hendelse i det perspektivet har ikke nødvendigvis konsekvenser for objektet selv da de kan være en vei inn til andre mål, som er funnet ved hjelp av targeting metodikken. Det kan også være at eventuell informasjon som blir hentet ut først har en konsekvens dersom en konflikt oppstår en gang i fremtiden. Hvordan denne typen konsekvenser kan vurderes med samme type og kategori som mer umiddelbare konsekvenser med tap av liv eller monetære verdier er vanskelig.

3.4.3. Risikoevaluering

Risikoevalueringen er siste ledd av risikovurderingen og skal sammenstille og presentere analysene som er gjort i de to foregående leddene. Dette er punktet der analytikerne skal gi beslutningstakerne grunnlaget for å ta beslutninger for videre risikohåndtering. De to aktuelle norske standardene kan gi ganske ulike visualiseringer av risikoen som er analysert ettersom

NS5814 legger hovedvekt på sannsynlighet og konsekvens, mens NS5832 forholder seg til de tre faktorene; verdi, trussel og sårbarhet. Begge metodene skal likevel presentere et risikobilde, og sine anbefalinger, til beslutningstakerne for videre risikohåndtering.

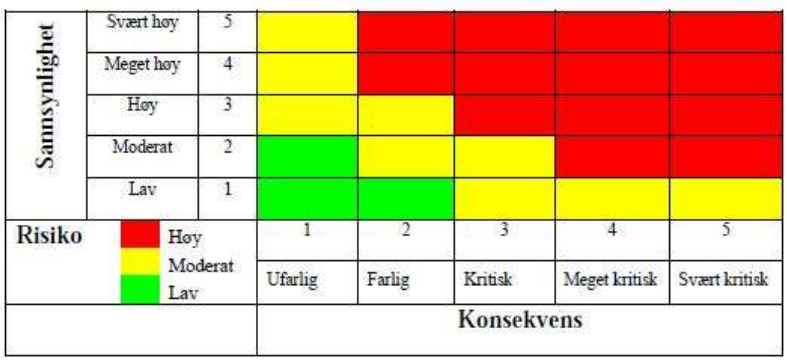
NS5832 beskriver at man etter vurderingene av verdi, trussel og sårbarhet skal vurdere såkalt «ren risiko». Dette er ikke en kvantitativ størrelse, men en kvalitativ vurdering av risikoen. Det er vanskelig å anslå en aktør sin intensjon og kapasitet nøyaktig så det er viktig å være tydelig på at dette er subjektive vurderinger med den usikkerheten som medfølger (NSM, PST og POD, 2015, s. 19). Hvert scenario som er valgt skal beskrives med et risikonivå der alle faktorvurderingene er med, og usikkerheten i alle vurderinger og konklusjoner beskrives (NS 5832, 2014, s. 6). Sikringsrisikobildet visualiseres som i figur 3 med bakgrunn i de tre faktorene. Man må ikke kvantifisere faktorene for å sette opp trekantene grafisk, men det vil være et behov for å kunne sammenligne den totale risikoen for de forskjellige scenarioene slik at beslutningstakerne kan prioritere. I figur 3 er det også visualisert hva som skjer med risikoen ved å innføre tiltak for å minimere sårbarheten i et scenario.



Figur 3 – Risikotrekanten (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 34)

NS 5814 beskriver risikoevalueringstrinnet noe mer utførlig enn NS5832. Det er naturlig da det er et selvstendig trinn i risikovurderingen, men ikke i sikringsrisikovurderingen. Dette trinnet starter med en vurdering av oppnåelsen av sikkerhetsmål som er gitt som del av rammene for selve risikovurderingen. Vurdering og rangering av identifiserte risikoer skal legges frem sammen med forslag til tiltak. Kunnskapsgrunnlaget til analysen og den metodiske prosessen beskrives også, for å gi beslutningstakerne en forståelse for kunnskapsstyrken i analysen. En av visualiseringene som ofte brukes i denne sammenhengen

er en risikomatrise som illustreres i figur 4. Risikoene plasseres i matrisen og sammenlignes og rangeres naturlig i de to dimensjonene: konsekvens og sannsynlighet. Det er også mulig å visualisere effekten det har å innføre tiltak, på konsekvensene eller sannsynligheten for en hendelse.



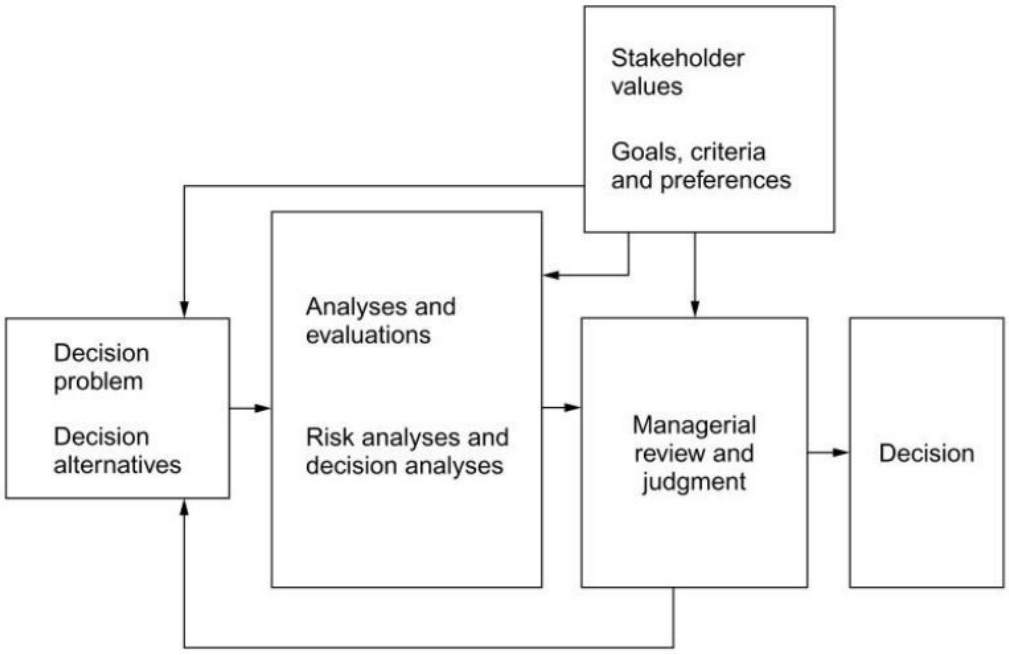
Figur 4 – Eksempel på risikomatrise (Busmundrud, Maal, Kiran, & Endregard, 2015, s. 31)

Begge metodene for visualisering av risiko har sine klare utfordringer. Risikotrekantens manglende visualisering av sannsynligheten for en gitt risiko er en svakhet. Dessuten er det vanskelig å raskt sammenligne ulike risikoer gitt at alle vurderingene av faktorene er grunnleggende subjektive og kvalitative. Risikomatrisen på sin side skaper et bilde av risikoene sett opp mot hverandre, men bildet blir en grov forenkling. Matrisen kan vanskelig fremstilles med en god forståelse for usikkerheten som ligger i de ulike risikovurderingene. Man må i tillegg velge mellom å presentere de konsekvensene som er mest sannsynlige, gjennomsnittlige eller «worst case». Sammenligningen blir forenklet der det for beslutningstakeren kan være viktigere å se de mest sannsynlige konsekvensene og vurdere dem opp mot mindre sannsynlige scenarioer, som i verste fall har veldig store konsekvenser.

Utfordringene til de to visualiseringsmetodene er viktig å være kjent med, men ingen av de norske standardene legger opp til at utelukkende en visuell fremstilling skal danne beslutningsgrunnlaget. Viktigheten av skriftlig dokumentasjon er beskrevet i NS5814, hvor det legges vekt på at det skal være «… mulig å følge resonnementene i risikovurderingen.» (NS 5814, 2021, s. 11) i dokumentasjonen, mens NS5832 beskriver at sikringsrisikobildet skal presenteres med hensikten «… å gi et best mulig beslutningsgrunnlag for videre sikringsrisikostyring.» og er tydelig på at visualisering ikke er et behov (NS 5832, 2014, s. 7).

At det likevel er fokus på visualisering av risikoer er fordi beslutningstakere ofte ønsker en enkel fremstilling av den totale vurderingen. Det er ekspertene som skal forholde seg til detaljene, mens beslutningstakerne ikke skal bruke tid på å sette seg så detaljert inn i alle analyser. Beslutningstakerne må likevel kjenne begrensningene i de ulike presentasjonene.

En normal beslutningsprosess er visualisert i figur 5 og viser at beslutningsproblemet, i vårt tilfelle hvilke risikohemmende tiltak som skal iverksettes, ikke er en enkel lineær prosess. Beslutningstakerne må i tillegg til ekspertenes analyser og vurderinger ta inn over seg behovene og ønskene til alle «stakeholders», eller interessenter. De må i tillegg se på de totale målene for organisasjonen, og eventuelle preferanser i forhold til verdier som åpenhet eller miljø. Selve det å fortolke de risikovurderingene som er gjort er med andre ord langt fra det vanskeligste beslutningstakerne gjør. Det er sannsynlig at de ser forbi en enkel visualisering i form av en matrise eller en risikotrekant, og forstår hva som ligger bak. Det vesentlige er nok en åpen og ærlig dialog mellom analytikerne og beslutningstakerne der alle antakelser og eventuelle bias blir lagt frem, slik at beslutningen tas mest mulig opplyst.



Figur 5 – Beslutningsprosess (Aven, 2012a, s. 114)

3.4.4. Oppsummering

Det teoretiske rammeverket for oppgaven er relativt stort da det kreves breddeforståelse for å besvare problemstillingen. Det er et behov for en teoretisk bakgrunn innen funksjonelle reguleringsregimer ettersom sikkerhetsloven er en lov som baserer seg på funksjonelle krav. Den enkelte organisasjons kunnskap, kompetanse og ressursbruk vil av den grunn påvirke sikkerhetsnivået i totalforsvaret. Denne typen regulering utfordres i dag ikke bare av kunnskapsbehovet i den enkelte organisasjon, men også av kompleksiteten i samfunn og teknologi. Videre er det et behov for en forståelse av etterretningsbegrepet og hvordan normale etterretningsoperasjoner styres. Her har jeg tatt utgangspunkt i NATO sine etterretningsdoktriner, med en antakelse om at våre motparter har lignende prosesser innen sin etterretning. Noe informasjon om russisk bruk av etterretning er også tatt med for å sette søkelys på en av hovedaktørene man står ovenfor i domenet. Innhentingstrinnet i etterretningshjulet er ytterligere belyst med teori ettersom jeg har definert at etterretningstrusselen primært handler om innhenting for den enkelte bedrift. Det er behov for teori angående risikobegrepet og usikkerhetsdimensjonen også før teorien rundt risikovurderingen kunne legges frem. Teorien rundt risikovurderinger er beriket med eksempler fra de norske standardene NS5814 og NS5832 for å trekke frem hva som anses som vesentlig i prosessen dersom man benytter seg av en av disse.

Ut fra teorien mener jeg å se et behov for at den enkelte organisasjon i totalforsvaret har utledet hva sikkerhetsloven betyr for dem, særlig med tanke på begrepet forsvarlig sikkerhet. Jeg forventer videre at de har et klart forhold til etterretningstrusselen og ser dens egenart. Uavhengig av hvorvidt de ser på etterretningstrusselen alene eller som del av mange risikoer, forventer jeg at de gjennom en viss bruk av en eller begge de norske standardene gjennomfører risikovurderinger som gir dem et klart bilde av risikoen for etterretningsinnhenting.

4. Metode

Dette kapittelet vil redegjøre for metodebruken i oppgaven og hvorfor den er valgt, og med det vil studiens styrker og svakheter belyses. Valgene jeg har tatt underveis vil bli beskrevet sammen med endringer som har kommet til underveis i prosjektet for å skape en forståelse rundt oppgaven og hvordan den har blitt til.

4.1. Forskningsdesign

Temaet oppgaven tar for seg er hvordan man kan utvikle trusselen fra etterretning som del av en risikovurdering. Dette temaet er som beskrevet i innledningen videre spisset til en problemstilling som ser på hvordan dette gjøres hos de strategiske logistikkpartnerne til Forsvaret, og i hvor stor grad det skaper det ønskede sikkerhetsnivået som det er krav til i sikkerhetsloven. Denne typen problemstilling, der man ønsker å gå i dybden på en prosess utforskes best med hjelp av kvalitative metoder. «Kvalitativ metode er særlig hensiktsmessig hvis vi skal undersøke fenomener som vi ikke kjenner særlig godt, og som det er forsket lite på, og når vi undersøker fenomener vi ønsker å forstå mer grundig.» (Johannesen, Tufte, & Christoffersen, 2010, s. 32). Det er vanskelig å belyse en problemstilling som ønsker å svare på hvordan noe gjøres med hjelp av kvantitative metoder, da det er lite relevant å hente inn data som på et eller annet vis kan tallfestes. Svaret på en slik problemstilling vil naturlig være en subjektiv vurdering med bakgrunn i data som samles inn, ikke et objektivt og tallfestet svar.

Jeg har valgt å benytte en abduktiv forskningsstrategi. Blaikie beskriver at mens induktiv strategi kan besvare «hva», og deduktiv og retroduktiv strategi kan besvare «hvorfor», så kan abduktiv strategi besvare begge. Metoden besvarer i motsetning til deduktiv metode «hvorfor» med kunnskap heller enn årsaker (Blaikie, 2010, s. 89). For å belyse problemstillingen i denne oppgaven er det mer ønskelig å søke kunnskapen enn årsakene, ettersom årsakene kan være så mange og komplekst sammensatt. For å utvikle denne kunnskapen ønsker jeg å forstå motivene og intensjonene som ligger bak valgene firmaene tar, som er en annen fordel ved å benytte abduktiv metode (Blaikie, 2010, s. 89).

For å få relevant empiri på hvordan etterretningstrusselen utvikles som del av en risikovurdering ble en modell med casestudie valgt. «Caseundersøkelser består kort sagt i å

samle så mye informasjon (data) som mulig om et avgrenset fenomen (casen).» (Johannesen, Tufte, & Christoffersen, 2010, s. 86). Denne oppgavens tema er å se på hvordan risikovurderinger blir gjennomført i en relevant «case», særlig med tanke på etterretningstrusselen. Blant annet grunnet pålagte nasjonale begrensninger under Covid-19 pandemien var det ikke mulig å finne et passende tidspunkt for å observere risikovurderingsprosesser. Ønsket var derfor å gjennomføre dybdeintervjuer i en eller flere organisasjoner som befant seg innenfor et segment der etterretning var en reell del av trusselbildet. Dette ville belyse metodikken som ble benyttet fra mer enn ett firma slik at det ville være mulig å generalisere noe. Dersom kun et firma hadde blitt valgt ville det blitt mer utfordrende å generalisere ettersom det er vanskelig å vite om de er representative for sammenlignbare firma, eller om de gjør risikovurderinger på en annen måte.

4.2. Utvelgelse av organisasjoner for casestudien

Som del av utviklingen fra tema til problemstilling måtte det en utvelgelse til for å finne hvilke firmaer eller organisasjoner jeg ønsket å studere risikovurderingsprosessen i. Organisasjonene som skulle forespørres måtte være klare etterretningsmål, og det måtte være sannsynlig at de selv var klar over at de var etterretningsmål. Dersom de ikke hadde en forståelse for at de kunne være utsatt for etterretningsinnhenting ville det ikke være noen grunn til å tro at de hadde risikovurderinger som inkluderte denne risikoen. Organisasjoner eller firmaer som anser seg selv som etterretningsmål vil naturlig ha et avklart forhold til risikoen, og en risikovurdering av etterretningstrusselen er dermed forventet. I datainnsamlingen har jeg ønsket å få belyst metoden som ble brukt til denne vurderingen, og refleksjonene rundt prosessen.

Jeg har i oppgaven definert etterretningstrusselen til å innebefatte industrispionasje. Definisjonen jeg benytter i teorikapittelet, fra Etterretningsdoktrinen, beskrev etterretning som statlig sanksjonert. For meg var det derfor ønskelig å velge organisasjoner som ville være av interesse for en statlig etterretningstjeneste når jeg skulle finne mulige caser. Det norske totalforsvarskonseptet var for meg et naturlig sted å se etter mulige organisasjoner som både er etterretningsmål og er kjent med det selv. En stat som ønsker å kjenne til hva Norge foretar seg som nasjon i et krise- eller krigsscenario vil anse totalforsvaret som et etterretningsmål. Dette konseptet er beskrevet i litteratur og stortingsmeldinger, og ettersom Norge utgjør

NATO sin nordøstre flanke mot Russland vil det norske totalforsvaret sannsynligvis benyttes dersom NATO ønsker å foreta seg noe mot Russland fra norsk territorium. Totalforsvaret er dermed et sannsynlig etterretningsmål for Russland. Gjennom informasjonsinnhenting mot deler av totalforsvaret vil de både kunne få varsling mot en eventuell offensiv handling fra NATO, og ha en viss kontroll på forsvaret av Norge dersom de selv skulle ha intensjoner om en offensiv.

Det er også nærliggende å tenke at det vil være lettere å hente inn informasjon fra en sivil organisasjon som har kommersielle mål, enn fra en organisasjon som er statlig og skapt for å motstå en fiende. Med andre ord er det sannsynligvis lettere å hente inn informasjon fra sivile deler av totalforsvaret enn de statlige, og i særdeleshet enklere enn å hente inn informasjon fra Forsvaret. Samtidig er det Forsvarets bevegelser og planer som er de mest interessant å få kontroll på. Logistikk er nødvendig for å forflytte og forsyne en hvilken som helst militær styrke, uavhengig av hvilken intensjon den har. Får man problemer med logistikken sin så vil kampavdelingene lenger fremme i striden få problemer. Manglende mat, drivstoff eller ammunisjon vil effektivt stoppe en militær styrke som er i krig. Dette har vært tydelig gjennom hele krigen i Ukraina, der russiske fremrykninger stadig har stoppet opp grunnet mangelfull logistikk (Listou & Ekstrøm, 2022). Av disse grunnene anser jeg Forsvarets strategiske logistikkpartnerne som ettertraktede etterretningsmål for en fiende. Det er sannsynlig at disse partnerne vil ha informasjon som gir indikasjoner på hva Forsvaret og eventuelt NATO har planer for å gjøre. Dersom man har kontroll på hva som forflyttes hvor i en militær sammenheng, vil etterretningsanalytikere kunne skape et bilde på hvor eventuelle offensiver vil komme.

4.3. Utvelgelse av intervjuobjekter

Forsvaret hadde strategiske kontrakter, som var offentlig kjent, med tre logistikkfirma da jeg startet på denne masteroppgaven. Ettersom dette var firma som sannsynligvis var etterretningsmål, og som sannsynligvis var klar over at de var det, ble alle tre firmaene forespurt om å la meg intervjue personell fra dem for å hente inn data. Alle firmaene var i utgangspunktet positive til å stille med informanter som kunne belyse problemstillingen i oppgaven. Det viste seg likevel at et av firmaene valgte å ikke delta. De to andre firmaene stilte velvillig opp, men ved begge firmaene ble antallet informanter redusert av ulike grunner.

Noen av informantene sluttet i sine stillinger og det var ingen som da kunne belyse prosessene som de hadde deltatt i på samme måte. Det var i tillegg noen informanter som hadde en sterk knytning til IKT og sikkerhetsstyring innen IT, men som ikke ville være i stand til å belyse risikovurderingen. Oppgaven er derfor basert på en informant fra hvert av de to firmaene. Disse satt i ledende stillinger i eget firma og hadde god kjennskap og erfaring fra risikovurderingene som var gjennomført de senere årene. De var i tillegg kjent med de ulike prosessene som spiller inn i den totale risikostyringen som risikovurderingene var del av i konsernet for øvrig. Det lave antallet informanter er en svakhet i oppgaven. Det er lite sannsynlig å få fullt generaliserbare data fra et utvalg på to firmaer med en informant i hvert firma. På den andre siden satt de to informantene sentralt i risikoarbeidet i sine firma, og to av tre firma i segmentet er intervjuet. Man må derfor kunne anta at deres metoder og betraktninger representerer andre sammenlignbare firma der de sammenfaller. Jeg ønsket i oppgaven å gå i dybden på få firma i et lite segment, heller enn å gå bredere ut og sammenligne med ulike typer firma. På denne måten kunne jeg få en grundigere forståelse for metodene de benytter, og tankegangen som ligger bak. Med to av tre mulige firma med i studien mener jeg at jeg har god mulighet til å få dypere innsikt enn i en mer overfladisk studie med mange informanter.

4.4. Utvelgelse av teori og avgrensninger

Tidlig i oppgaven har jeg valgt å definere hva jeg legger i definisjonene risikovurdering og etterretningstrussel. Begge avgrensningene mener jeg er nødvendige for å sikre at intervjuobjektene, leserne og jeg alle har den samme forståelsen av hva det er som belyses. Definisjonen på etterretningstrussel viste seg viktig i intervjusammenheng da det i de uformelle samtalene før intervjuene ble stilt spørsmål fra respondentene om jeg ønsket at de skulle skille på statlig etterretning og industrispionasje. Definisjonen ble da lagt frem og det var enighet om at det ville være et vanskelig og kunstig skille å legge til grunn. Definisjonen av risikovurdering er ansett som vesentlig for å kunne benytte standardene NS5832 og NS5814 som eksempler. Disse har noe forskjellig terminologi, men ved å benytte definisjonen er det mulig å trekke frem gode eksempler fra begge standardene underveis.

Hvilke områder det er behov for å belyse teori fra er vurdert fortløpende gjennom prosessen med å skrive oppgaven. Det er relativt mye teori som er belyst, men alt er vurdert til å være

vesentlig for å kunne drøfte problemstillingen. Det er et vanskelig tema som krever en god forståelse for både etterretning og risiko, men også en dypere forståelse for innhentingsdelen av etterretningshjulet og risikovurdering.

4.5. Beskrivelse av studie

Før intervjuene startet utviklet jeg en intervjuguide i to versjoner. Den ene versjonen var myntet på intervjuobjektene, som skulle få denne tilsendt i forkant av intervjuene for å ha mulighet til å forberede seg. Den andre guiden var myntet på meg selv og var betydelig mer detaljert. Tanken med dette var å sikre at intervjuene kunne foregå semistrukturert, men at jeg hadde noen tema som måtte bli belyst selv om de ikke lå eksplisitt i intervjuguiden som var sendt ut.

Valget om å sende ut intervjuguiden i forkant kan føre med seg utfordringer for oppgaven. Oppgaven skal se på hvordan de strategiske logistikkpartnerne gjennomfører sine risikovurderinger opp mot etterretningstrusselen. Når intervjuobjektene er kjent med spørsmålene i forkant er det mulig at de velger å gi svar som gjør at det fremstår som om prosessene deres er bedre enn de i realiteten er. På den andre siden er ikke oppgaven ute etter å avdekke feil og mangler hos firmaene, men se i hvor stor grad intensjonen i sikkerhetsloven kan oppnås med bruk av risikovurderinger. Dersom firmaene legger frem en metode som er forbedret i forhold til den de benytter til daglig, så vil målet med oppgaven fortsatt oppnås. Fordelen med å sende ut intervjuguiden i forkant var at intervjuobjektene hadde tid til å forberede seg til intervjuet. Dermed gikk en mindre del av tiden i intervjuene med til at de skulle tenke seg om eller forsøke å huske hvordan de gjennomfører risikovurderinger. Det var også lite behov for å få ytterligere svar ettersendt på epost, da det var få spørsmål de ikke hadde svar på. Fordelene med å sende ut intervjuguiden ble vurdert til å veie tyngre enn ulempene. Det var heller ingen klare tegn til at noen av intervjuobjektene forsøkte å pynte på realiteten i hvordan risikovurderingene blir gjort.

Intervjuene ble gjennomført i lokalene til firmaene med kun meg selv og respondenten til stede. Intervjuene ble tatt opp med opptaker etter avtale og skriftlig samtykke fra respondentene. Før opptakeren ble skrudd på hadde vi en uformell prat der jeg blant annet

presenterte meg selv, min bakgrunn og bakgrunnen for min interesse for temaet. Respondentene presenterte også seg selv og sin bakgrunn før vi skrudde på opptakeren, slik at de kunne være trygge på at disse opplysningene ikke ville komme i transkriptet og med det en ytterligere sikring av anonymitet. Disse uformelle samtalene skapte, sammen med det at dette var en-til-en samtaler, en god og åpen atmosfære før intervjuet som gjorde selve intervjuprosessen enklere. Utfordringen med å intervjue alene er at det er vanskelig å notere ned relevante poenger samtidig som man konsentrerer seg om intervjuet og å få en god samtale. Dette var enklere for meg grunnet opptakeren som gjorde at jeg ikke var redd for å gå glipp av noe av det som ble sagt, og kunne fokusere på samtalen og de viktige oppfølgingsspørsmålene. Etter intervjuene er de transkribert og sendt til respondenten slik at de har kunnet sjekke dette. I forbindelse med denne sjekken ble også respondentene bedt om å komme med ytterligere opplysninger dersom de mente det var noe relevant som ikke hadde kommet frem. Transkriptene er videre blitt analysert ved at jeg har kodet teksten for å kunne trekke ut essensen av hva de har fortalt om risikovurderingsprosessen. Den kodede teksten har jeg deretter kondensert ned for å forsøke å komme til essensen i hva datainnsamlingen forteller meg. De tekstutdragene jeg satt igjen med i hver kategori har til slutt blitt sett opp mot hverandre for å finne likheter og ulikheter i de to firmaenes metoder.

En av utfordringene i datainnsamlingen til prosjektet har vært at informasjonen det er behov for å samle inn for å belyse problemstillingen, grenser opp mot sikkerhetsgradert informasjon. For å sikre en åpen dialog har jeg derfor hatt med meg en kopi av egen sikkerhetsklarering til intervjuene. Et ønsket resultat av dette var at intervjuobjektene følte seg komfortable med at jeg kunne håndtere eventuell informasjon som var gradert, på en god måte. Dette førte til at de fortalte så åpent som de kunne i forhold til graderingen på lokalene. Jeg valgte så å fjerne informasjon som kom frem i intervjuene fra transkriptene dersom jeg enten var usikker på om den kunne bli tolket som gradert, eller kunne være referanser til sikringstiltak. Dette var uansett ikke informasjon som var relevant for oppgaven og det har ikke ført med seg noen utfordring i den videre analysen av informasjonen.

Min bakgrunn som offiser, med bakgrunn fra både logistikk og etterretning, er en utfordring i forbindelse med dette studiet. Firmaene har strategiske avtaler med Forsvaret og min bakgrunn kan føre til at intervjuobjektene føler seg usikre. De kan være mindre villige til å

legge frem forhold de selv er usikre på om Forsvaret ville like, uavhengig av om det er i brudd med kontrakter eller ei. Det har derfor vært et poeng for meg å være så åpen og ærlig med dem som mulig, og å forsikre dem om at dersom det kommer frem noe kritikkverdig så vil det ikke beskrives med mindre det er relevant for oppgaven.

4.6. Oppgavens reliabilitet og validitet

Reliabilitet er et mål på hvor pålitelige dataene som er samlet inn i forbindelse med oppgaven er. Det kan bli sett på som en utfordring for reliabiliteten for denne oppgaven at intervjuobjektene har fått spørsmålene på forhånd. Dette gjør at de kan velge om de vil svare ærlig på spørsmålene eller heller å skape et bilde av en bedre prosess. Jeg mener derimot at jeg ved å sende ut intervjuguiden på forhånd økte reliabiliteten til oppgaven. Med et ønske om å gå i dybden var det et behov for å la intervjuobjektene forberede seg. Dette gjorde at de kunne svare og utdype på alle spørsmålene, og hadde hatt mulighet til å reflektere rundt begrepene jeg ønsket å diskutere. En annen utfordring er at det kun er et intervjuobjekt i hvert firma ettersom det da ikke var mulig å se svarene opp mot hverandre internt i et firma, og på den måten bekrefte prosessen. Her mener jeg også at utsendingen av intervjuguiden i forkant styrker reliabiliteten, ettersom intervjuobjektene hadde muligheten til å diskutere med andre internt og dermed fremstille et riktig bilde av prosessen på vegne av flere enn seg selv. Det som teller for påliteligheten av dataene som er hentet inn om prosessen er at de to firmaene i stor grad svarer sammenfallende. De beskriver en relativt lik prosess i hverdagen, med noen forskjeller som blant annet er grunnet konsernstruktur og -føringer. Det ble i tillegg stilt oppklarende spørsmål som ikke var kjent på forhånd, underveis i intervjuene. Ingen av respondentene viste da tegn til at de svarte unnvikende eller måtte tenke seg ekstra om for å svare noe som passet i en oppdiktet prosess. Reliabiliteten i oppgaven bedømmes derfor som god, men med klare forbedringspotensialer uten pandemiens begrensninger. Det hadde eksempelvis vært interessant å kunne overvære risikovurderingsprosessen fullt ut i begge firma, for å se hvordan det faktisk gjøres.

Hvorvidt en oppgave er valid er en betegnelse på «… hvor godt, eller relevant, data representerer fenomenet.» (Johannesen, Tufte, & Christoffersen, 2010, s. 69). Spørsmålet er om dataen er gode til å beskrive det generelle fenomenet som studeres. Eksempelvis er det en utfordring at dataene er samlet inn ved hjelp av kun ett intervju per respondent. Dersom jeg

har misforstått noe angående prosessen eller konteksten firmaene jobber i så er det ikke sikkert at det har blitt fanget opp. For å øke validiteten har jeg derfor bedt om skriftlige rettelser og tilføyelser fra respondentene til både transkriptene av intervjuene og empirikapittelet. Oppgaven er å belyse risikovurdering for etterretningstrusler som gjennomføres hos de strategiske logistikkpartnerne til Forsvaret. Ettersom to av de tre firmaer som faller inn i denne kategorien har deltatt i undersøkelsen er det sannsynlig at dataene som er hentet inn beskriver fenomenet godt, og dermed har en høy grad av validitet.

En annen form for validitet er beskrevet som ytre validitet og måler hvilken grad resultatet kan «… overføres i rom og tid.» (Johannesen, Tufte, & Christoffersen, 2010, s. 357). Denne oppgavens ytre validitet er det vanskelig å bedømme, men det er mulig å gjøre seg noen betraktninger. Det er lite sannsynlig at disse firmaene har en vesentlig annerledes prosess enn andre sammenlignbare firma i Norge. Firmaer som er etterretningsmål, og selv er klar over det, vil måtte forholde seg til denne trusselen i sine risikovurderinger. Med en relativt ny sikkerhetslov er det lite sannsynlig at andre firmaer enten har vesentlig mer eller mindre kompetanse og fokus på hvordan de skal skape et forsvarlig sikkerhetsnivå. På den andre siden er det usikkert om firma som ikke har den knytningen til Forsvaret som de strategiske partnerne har, vil velge å ansette en så stor andel med Forsvars-bakgrunn. Muligheten for å generalisere resultatene til andre firmaer er dermed usikker ettersom det er mange faktorer som spiller inn på hvordan et firma vil forholde seg til etterretningstrusselen. Med kun to informanter er det også vanskelig å påstå at det er stor mulighet for generalisering.

5. Empiri

Empirien som er funnet i case-studiene presenteres i dette kapittelet. Noen overordnede betraktninger beskrives, deretter belyses funnene knyttet til spørsmålstillingene som ble benyttet i intervjuguiden. Kapittelet avsluttes med en beskrivelse av en metode som er generalisert ut fra de to casene.

5.1. Funn

Gjennom de to casene som er belyst fremkommer det et bilde av at risikovurderinger i hovedsak har to fokus, overholdelse av lov- og kontraktspålagte føringer og kommersielle hensyn opp mot omdømme og lønnsomhet. Respondenten fra firma A kommenterer at «… den nye sikkerhetsloven legger mye ansvar over på den sivile aktøren …», men sier også at «… vi tar utgangspunkt i de kravene som ligger i de sikkerhetsavtalene vi har.». Firma B bekrefter tankegangen når de sier at «Vi oppfyller egentlig sikkerhetsloven gjennom å ha den dokumentasjonen som [Forsvarsmateriell] FMA industrisikkerhet stiller [krav om] til oss.». Dette gjør ikke at firmaene nødvendigvis har dårlig sikkerhet når det kommer til etterretningstrusselen, men det er ikke enkelt å studere risikovurderingene for å forstå hvilke tiltak som er iverksatt med bakgrunn i en god forståelse for trusselen. Firmaene ser sin egen mangel på kompetanse i møtet med denne typen trussel og lener seg av den grunn i stor grad på offentlige organer som skal inneha ekspertisen. Det er i tillegg en stor grad av tiltro til egne IT-leverandørers skikkethet i forhold til trusselen i cyberdomenet.

Ingen av firmaene jobber med risikoanalyse basert på NS 5830 serien, men begge har et klart forhold til hva de legger i faktorene verdi, sårbarhet og trussel. Begge forholder seg til risikovurderingssystemer internt i konsernene som er basert på sannsynlighet og konsekvens, og dermed forholder seg mer til NS 5814. Firma B er tydelig på at de baserer seg på siste versjon av NS 5814, og dermed har med seg forståelsen for samtlige faktorer. Konsernstrukturene de strategiske partnerne er del av er store og komplekse med en mengde underenheter. Det er en stor grad av både interaktiv og dynamisk kompleksitet i verdi- og beslutningskjedene internt i konsernene. Dette gjør at noen av vurderingene som gjøres ikke ble belyst i intervjuene. Disse gjøres i andre deler av samme konsern, ofte med innspill fra de strategiske logistikkpartnerne, som bare må stole på at det er gode beslutninger.

5.2. Rolleforståelse

Begge firmaene beskriver totalforsvaret som bruken av nasjonens samlede ressurser i forsvaret av Norge. De beskriver konseptet som sier at en liten nasjon med et så stort areal ikke klarer å forsvare seg med militære kapasiteter alene, men må trekke på alle relevante ressurser i samfunnet. De ser seg som del av totalforsvaret blant annet med bakgrunn i kontraktene de har med Forsvaret, men det er også visse forskjeller i forståelsen av egen rolle. Egen rolle i sivile kriser er et område der de har en ulik oppfatning, da firma A ser seg selv som en selvstendig og naturlig del av totalforsvarskonseptet mens firma B kun beskriver seg som en del av det i den grad Forsvaret velger å benytte seg av dem. Noe av forskjellen synes å komme fra ulikheter mellom firmaene, ettersom det ene eier en del infrastruktur som de anser som viktig i Forsvarssammenhengen, men det kan også ha bakgrunn i forskjellig forståelse for totalforsvarskonseptet.

Firmaene forholder seg begge til Sikkerhetsloven, men er usikre på om det er fattet vedtak i departementet om deres status. Det anser begge som mindre vesentlig ettersom kontraktene de har med Forsvaret gir tydelige føringer om at de skal forholde seg til loven, og stiller spesifikke krav til dem. Ingen av firmaene har selvstendig vurdert hva som ligger i begrepet «forsvarlig sikkerhetsnivå» som anvendes i loven. De har med andre ord ikke en eksplisitt vurdering de kan evaluere egen sikkerhet opp mot, og de synes å mene at de selv ikke har kompetanse til å gjøre en slik vurdering opp mot loven og egen rolle i en totalforsvarssammenheng. Begge er av den oppfatning at dette er noe Forsvaret må ha bedre forutsetninger for å definere. Forsvarlig sikkerhet er slik de ser det oppnådd når de følger de kravene som er pålagt, og har den påkrevde dokumentasjonen som er beskrevet i kontraktene de har med blant annet Forsvarsmateriell (FMA) angående industrisikkerhet. Overvekten av de ansatte i firmaene har bakgrunn fra Forsvaret og de ser seg i stand til å operasjonalisere kravene som stilles med bakgrunn i sin erfaring. Respondenten i firma B sier at de har «… mest hell med å ansette folk som har vært med i Forsvaret før.» og utdyper at «Det er greit å ha folk som er bevisst [sikkerhetssituasjonen], og det er noe som bygges opp over tid …». Firma A har også «… folk med ganske god innsikt i sikkerhetsspørsmål. Gjennom lang militær karriere, operativ karriere …». Så med bakgrunn i kontrakten og personellets forståelse for sikkerhetssituasjonen med bakgrunn i erfaring fra Forsvaret, mener de at de

oppfyller kravene til forsvarlig sikkerhet uten selv å måtte vurdere nøyaktig hva som ligger i begrepet.

Det er ingen tvil om at firmaene ser seg selv som etterretningsmål. De benytter de åpne trusselvurderingene fra Politiets sikkerhetstjeneste (PST), Etterretningstjenesten og Nasjonal Sikkerhetsmyndighet (NSM) for å gjøre sine egne vurderinger i denne sammenheng. Som respondenten fra firma B sier så er «… virksomheter i rammen av totalforsvaret, eller som støtter Forsvaret […] er en aktør som kan bli angrepet.» Begge firmaer er også klar over forsøk på etterretningsinnhenting mot et firma i kategorien som ble avdekket i sammenheng med dataangrepet på Stortinget i 2021. Firmaene ser at de er truet av både statlige og kriminelle aktører, samtidig som ingen av dem utelukker at de har konkurrenter som kan benytte ulovlige midler i sine ønsker om informasjon. De har med andre ord en klar formening om at det eksisterer en etterretningstrussel som del av det totale risikobildet de opererer i.

5.3. Utarbeidelse av risikovurderinger

Firmaene beskriver begge at risiko er noe de jobber med kontinuerlig og at det ved hendelser eller spesielle oppdrag vil gjennomføres analyser relativt hyppig. Firma A beskriver en mer formalisert prosess opp mot selskapets styre, der risikobildet presenteres og diskuteres med en hyppighet som er styrt av situasjonen de er i. Ved normal drift vil det si at risikobildet forankres med styret kvartalsvis, mens det eksempelvis ved større øvelser kan være så ofte som ukentlige møter. Respondenten forteller at «… er vi inne i store komplekse operasjoner så kan vi ha inntil en ukes frekvens […] Hvis det er mer stabil drift så kan det være at hvert styremøte så har vi en vurdering.» For firma B sin del er det noe mindre formelt, men ved at daglig leder, som også er konsernsjef, deltar aktivt i vurderingene har man en god forankring. De gjennomfører også vurderinger når styret ønsker og har senest gjennomført en vurdering angående den pågående krisen i Ukraina. Styret ønsket å vite hvordan dette kunne påvirke selskapet og respondenten forteller at de skulle lage en «one-slider» med analyse om hvordan situasjonen kan påvirke konsernet. Respondenten beskriver at de har «… tro på små intense gjennomføringer [av risikovurderinger] regelmessig …» heller enn «… et kjempestort prosjekt som skal holde på i flere år …».

Ingen av firmaene beskriver utarbeidelsen av risikovurderingene som en spesielt formell eller formalisert prosedyre. Det er lite bruk av normale risikovurderingsverktøy som feiltreanalyse eller bowtie, men de har en noen egne verktøy de benytter gjennomgående. Begge benytter seg av egne maler og programvare som konsernet stiller krav til. Felles for disse synes å være at de er utarbeidet med bakgrunn i vurdering av kommersiell risiko og forholder seg til risiko som en sammenheng mellom sannsynlighet og konsekvens. Ingen av firmaene beskriver noen egen metodikk for etterretningstrusselen. De vurderer tilsynelatende risiko for tilsiktede handlinger likt som andre risikoer. Firma A beskriver at de alltid utarbeider scenarioer som representerer «worst case» og «best case», samt et som kan beskrives som mest sannsynlig. Dette gjøres gjerne ved at de «… sitter […] rundt bordet og tenker - hva er det verste som kan skje? Så får man som regel et samstemmig bilde av hva man mener er det verste, og så likeledes på de andre [scenarioene] …». Dette hjelper dem med å forholde seg til usikkerheten som ligger i det å forutse fremtidige hendelser. De involverer bredt og diskuterer hyppig med eget styre for å forankre og motvirke gruppetenkning. Alle typer risiko og forskjellige konsekvenser beskrives på samme måte og visualiseres i en type risikomatrise, der konsekvensene måles opp mot hverandre basert på erfaring i arbeidsgruppen. Firma B har en lignende tilnærming, men den enkelte analyse virker ikke som den nødvendigvis har med seg de tre scenarioene eksempelvis. For å se konsekvenser på tvers av kategorier har de utarbeidet en matrise som sammenligner de forskjellige utfallene med en kommersiell risiko der konsekvensen beskrives som tap av verdi.

5.4. Usikkerhet og kompleksitet

Når usikkerheten beskrives så var det ikke usikkerhet tilknyttet risikovurderingene som først ble definert. Informanten fra firma A tenkte først og fremst på forskjellen mellom risiko og usikkerhet med en tanke om at usikkerhet kunne være både positivt og negativt, mens risiko var negativt. De ble derfor ledet inn på at usikkerhet kunne være viktig i forhold til analysene og vurderingene som gjøres i risikoarbeidet. Etter denne presiseringen av spørsmålsstillingen fremhever begge firmaene usikkerheten rundt kunnskapen til de som gjennomfører analysene som en kilde til usikkerhet. Datakvaliteten og relevansen i dataene man benytter seg av beskrives også som en kilde til usikkerhet i analysene. I tillegg var de bevisste på at faktorene som påvirker fremtiden er ukjente og derfor skaper usikkerhet. Pandemien ble henvist til som et eksempel på denne typen usikkerhet av informanten fra firma B. Ingen av informantene beskrev valg av metode eller metodens egnethet, som en kilde til usikkerhet.

Kompleksitet var et tema som ikke ble eksplisitt diskutert med firmaene, men de beskriver begge en situasjon der kompleksiteten fører med seg usikkerhet. Informantene beskriver at de ikke selv i sine firma har kunnskapen og kompetansen til å gjøre vurderinger innenfor eksempelvis IT-sikkerhet. Begge firma beskriver også en hverdag som er preget av korte tidsfrister og mange faktorer de ikke selv føler de har kontroll over. Dette fører til at man, som informanten i firma A sier, «… må akseptere at det ligger en del usikkerhet i de vurderingene du gjør …».

5.5. Faktorene

5.5.1. Verdi

Begge firmaene beskriver at de har definert sine verdier som del av å benytte ISO 9001 basert kvalitetssystem. Firma A beskriver at de med tanke på etterretningstrusselen i hovedsak ser på kommersiell verdi og forsvarets robusthet som verdiene de må forholde seg til og beskytte. De er i tillegg opptatt av omdømmerisiko og eget omdømme som verdi. Dette gjenspeiler seg i firma B som har definert fire verdier i jobben med ISO 9001, som er omdømme, personell, informasjon, og informasjons- og kommunikasjonsteknologi (IKT). Begge firmaene har et forhold til hvilke verdier de forvalter i den enkelte operasjon de er del av, men uten at det er spesifikt vurdert eller beskrevet. Ut fra det de beskriver så ser de i stor grad på informasjonen de besitter som en verdi de forvalter på vegne av Forsvaret. I den grad denne er videre vurdert i forhold til risiko for eget firma er den satt inn som del av en eller flere av de større risikoene som omdømme og kommersiell verdi. Særlig firma A fremhever også at de er så integrerte i militære planer og operasjoner at de må søke å tenke som Forsvaret gjør slik at de ikke kompromitterer den militære robustheten. Respondenten sier at de er «… såpass integrert i militære planer og militære operasjoner at vi må ha en voldsom årvåkenhet på det, og må tenke som Forsvaret tenker.».

5.5.2. Trussel

Trusselforståelsen utvikles i begge firma gjennom bruk av eksterne kilder og i stor grad ekstern kunnskap. Begge firmaene beskriver at de benytter de ugraderte publikasjonene til PST, Etterretningstjenesten og NSM for å forstå hva etterretningstrusselen mot eget firma kan være og innebære. Det er også beskrevet en tett dialog med Forsvaret gjennom FMA og FLO i

hovedsak. Firmaene er tett integrert i en koordineringscelle i FLO-systemet der de har tilgang til etterretningsinformasjon som deles internt i Forsvaret. Kontakten med FMA angående industrisikkerhet beskrives også som tett og gir tilsynelatende noe ekstra forståelse for etterretningstruslene. Begge firma beskriver at en av grunnene til å ha en overvekt av ansatte med militær bakgrunn, er at disse er i stand til å forstå det trusselbildet de opererer i som del av totalforsvaret.

Cybertrusler har firmaene en viss erfaring med og det er påvist forsøk på inntrenging i nettverkene til en aktør i sektoren nylig. Truslene i dette domenet har firmaene selv ikke kompetanse til å vurdere, men begge beskriver konsernenes IT-ressurser som meget robuste. Informantene fra begge firma har en generell forståelse for hvilke typer trusselaktører som kan operere mot dem i domenet, og de har stort fokus på de typiske forsøkene som «phishing» eposter i begge firma. Begge firmaene fremhever at etterretningstrusselen kan være både statlig og privat. Respondenten i firma B sier at «… om det ikke er en statlig aktør så kan det være en konkurrent som prøver å finne ut hva er vår strategi …», mens intervjuobjektet i firma A påpeker «… at det er en viss kontakt mellom de som driver med egentlig kriminelt motivert inntrengningsoperasjoner og statlige etterretningsaktører.».

5.5.3. Sårbarhet

Firmaene beskriver at de innen sårbarhet, når det kommer til nettverkstrusler må stole på de konserneide IT-ressursene de benytter. Det er ikke mulig for dem å ha god nok forståelse for systemene, avhengighetene og kompleksiteten, til å skape seg sin egen sårbarhetsforståelse. Det er likevel IT-ressurser som er i samme konsernstruktur som jobber med sårbarhetsforståelsen, og begge firmaene beskriver disse som meget kompetente og med et klart mål om å holde en høy sikkerhet. Eksempelvis beskrives bruk av såkalt penetrasjonstesting og bruk av «red team» for å aktivt lete etter sårbarheter. De konserneide IT-ressursene samarbeider i tillegg med nasjonale statlige organer som NSM. Sårbarhetsforståelsen utvikles ifølge informantene gjennom disse samarbeidene med både statlige og private sikkerhetsleverandører, men informanten i firma B innrømmer at «… vi har nok ikke vært flinke nok til å gå inn og dypdykke på sårbarhet …». Ingen av firmaene beskriver noen egen sårbarhetsforståelse myntet på etterretningstrusselen, men er klare på at IT-ressursenes samarbeid med myndighetene gir dem dette for cyberdomenet.

5.5.4. Konsekvens

Konsekvensene er for begge firmaene utviklet gjennom scenarioutvikling. Firma A beskriver sin utvikling av scenarioer som beskriver «worst case», «best case» og noe midt imellom. Informanten i firma B beskriver at de utvikler scenarioer for forskjellige typer risiko, men at det ikke nødvendigvis er flere forskjellige konsekvenser som utvikles i disse scenarioene. Begge firmaene påpeker at de som kommersielle firmaer er opptatt av konsekvenser med tanke på pengeverdi. En konsekvens som påfører firmaet et tap i omdømme vil kunne føre med seg store tap av verdier i neste omgang, og det er derfor omdømmerisiko fremheves av begge firma som vesentlig. Begge firma er opptatt av konsekvensene som kan ramme Forsvaret og som det ikke kan festes en verdi til som konsekvens utenfor firmaet selv. Likevel oppleves begge firma som tydelige på at det for dem internt er de monetære verdiene som må vurderes. Er ikke avtalene lønnsomme så vil ikke en kommersiell aktør stå i dem, uavhengig av eventuelle konsekvenser for Forsvaret. Noen utviklet forståelse av konsekvensene som kommer fra etterretningstrusler får jeg ikke en forståelse for at noen av firmaene har.

5.5.5. Sannsynlighet

Når de skal beskrive sannsynlighet begynner informantene med å beskrive en statistisk sannsynlighet som kan tallfestes. Informanter fra firma B ville tidligere beskrevet sannsynlighet som «… ett tall fra null til en …», men etter å ha jobbet med sikkerhet var det en mer kvalitativ og kunnskapsbasert størrelse. For å beskrive sannsynligheten benyttet firmaet seg nå av begrepene lav, middels, høy og svært høy, og de forsøkte å se sannsynligheten for etterretningstrussel opp mot indikatoranalyser. Disse indikatorene skulle hjelpe dem med å se endringer i sannsynligheten underveis i en situasjon eller operasjon. Firma A beskrev også at sannsynlighet var kunnskaps- og erfaringsbasert i deres risikovurderinger. De utviklet de forskjellige konsekvensscenarioene først og forsøkte deretter å oppnå en type konsensus i gruppen for hvor stor sannsynligheten var for de forskjellige scenarioene. Dette hjalp dem både med å beskrive sannsynligheten og å raffinere scenarioene de hadde beskrevet. Sannsynligheten for forsøk på etterretningsinnhenting anså firmaene som veldig høy basert på de ugraderte rapportene fra de hemmelige tjenestene. Firma B påpeker at «Vi ser at [et annet tilsvarende firma] ble angrepet i fjor, indirekte via Stortinget. Så at det skjer er uten tvil.». Firma A bekrefter også at de har fått vite at de er «… et høyt prioritert etterretningsmål for fremmed etterretning.».

5.6. Generell tilnærming til risikovurdering

Informantene beskriver en pragmatisk tilnærming til risikovurderinger når det gjelder etterretningstrusler. Der de opplever at de ikke har kompetanse eller innsikt nok til å gjøre egne vurderinger velger de å stole på eksterne aktører. Dette kommer særlig frem i forhold til faktorene sårbarhet og trussel, hvor de i all hovedsak ser til myndighetene og sine egne konserns IT-ressurser. Når de opplever at myndighetene forteller dem at de er etterretningsmål så tar de det for gitt og vurderer sannsynligheten som høy. Sannsynlighet og konsekvens, og eventuelt andre faktorer i risikovurderingen, utvikles deretter i egne risikoscenarioer for etterretningstruslene.

Begge informantene oppleves som de skulle ønske at de hadde ressursene og kunnskapen til å ta et større eierforhold til denne delen av risikovurderingen. Informanten fra firma A sier at «Drømmesituasjonen ville jo ha vært å ha […] en ressurs som jobber hele tiden med risiko.». Dette forstås også som et ønske om å ha større kunnskap om metodikk innen risikovurderinger, for det synes ikke som det er noen systematisk bruk av risikovurderingsverktøy i firmaene. Informanten i firma B kommenterte da også at han skulle ønske NSM kunne utvikle enkle og billige e-læringskurs innen temaet. På den måten ville alle typer bedrifter i Norge ha tilgang på bedre kunnskap og ville bidra til å gjøre totalforsvaret mer robust.

6. Drøfting

Jeg vil i dette kapittelet belyse problemstillingen og forskningsspørsmålene i oppgaven, med hjelp av informasjonen som har kommet frem i empirien og teorien som er beskrevet. Det første forskningsspørsmålet vil jeg drøfte opp mot egnetheten av funksjonelle lovverk i møtet med en etterretningstrussel. De to neste forskningsspørsmålene vil drøftes med tanke på hvor egnet standard risikovurdering er for et kommersielt firma som skal vurdere trusselen fra etterretningsaktører. Til slutt vil jeg drøfte mulige forbedringer i metodikken som benyttes, med tanke på å forbedre sikkerhetsnivået som oppnås.

6.1. Egnethet av funksjonelle lovverk for å oppnå et forsvarlig sikkerhetsnivå i totalforsvaret

Sikkerhetsloven er et funksjonelt regelverk som pålegger alle organisasjoner som er underlagt det, å opprette et forsvarlig sikkerhetsnivå. Lovens formål er å «… trygge … nasjonale sikkerhetsinteresser» og «å forebygge, avdekke og motvirke sikkerhetstruende virksomhet» (Sikkerhetsloven, 2018). Totalforsvaret og alle aktørene som er del av det, utgjør en nasjonal sikkerhetsinteresse og må følge lovverket for å oppnå et forsvarlig sikkerhetsnivå. Hvor egnet et slikt lovverk er til å oppnå det ønskede sikkerhetsnivået vil drøftes i dette avsnittet.

6.1.1. Hvem er underlagt lovverket

Sikkerhetsloven sier at organisasjonene som er underlagt loven skal opprette «et forsvarlig sikkerhetsnivå» (Sikkerhetsloven, 2018, ss. §4-3). Organisasjoner som er del av totalforsvaret, som de strategiske logistikkpartnerne kan underlegges loven helt eller delvis gjennom et vedtak i Forsvarsdepartementet (Sikkerhetsloven, 2018, ss. §1-3).

De strategiske logistikkpartnerne som case studiene har blitt gjennomført hos, er bevisst sin egen rolle i totalforsvaret. Denne rollen har de som følge av sine kontrakter med Forsvaret og den er særlig tydelig i forbindelse med beredskapen opp mot en eventuell krig som leverandører av logistikktjenester. At dette fører med seg at de er underlagt sikkerhetsloven er de klare på, men ingen av dem er sikre på om det er fattet vedtak i Forsvarsdepartementet på at de er underlagt loven. Det er med andre ord ikke sikkert at disse firmaene er underlagt sikkerhetsloven gjennom vedtak i departementet. De mener dog at dette har lite å si ettersom

de har sikkerhetsavtaler som del av kontraktene med Forsvaret. Disse sikkerhetsavtalene er basert på og utledet fra sikkerhetsloven, og bestemmelsene som ligger i avtalene er derfor antatt å gi føringer for hva som må gjøres for å oppnå forsvarlig sikkerhet. På den andre siden har ingen av dem selv analysert og definert hva sikkerhetsloven betyr for dem eller selv beskrevet hva de regner som et forsvarlig sikkerhetsnivå. Det virker heller ikke som de har blitt revidert av noen tilsynsmyndighet på sin etterlevelse av loven ettersom de er usikre på om det er fattet vedtak på at de er direkte underlagt loven. Alt i alt er forholdet til sikkerhetsloven noe uklart selv om begge firmaene svarer at de er underlagt og etablerer et forsvarlig sikkerhetsnivå ved å følge kravene i kontraktene de har med Forsvaret. Denne uklarheten mener jeg myndighetene eller Forsvaret burde fjernet ved å være tydeligere med sine overordnede forventninger til firmaene i forhold til lovverket.

Hvorvidt de er underlagt lovverket med et vedtak eller ei har muligens ikke så mye å si for sikkerhetsnivået til disse firmaene, all den tid de anser seg selv som underlagt. Men situasjonen belyser likevel en utfordring for bruken av funksjonelt lovverk. Myndighetene må i dette tilfellet definere hvilke enkeltorganisasjoner som er underlagt loven, selv om det ikke nødvendigvis er noe klart skille på hvilke organisasjoner som har en stor nok del av norske sikkerhetsinteresser. Det er i sikkerhetslovens tilfelle en «gråsone» med organisasjoner som har en binding til norske sikkerhetsinteresser, men som departementet må vedta om skal underlegges lovverket. Denne gråsonen av organisasjoner skaper mulige sårbarheter som kan utnyttes av en motstanders etterretningstjeneste. Interessen for totalforsvaret vil kunne gjøre at de følger en targeting metodikk og finner informasjonen de ønsker, eller vektorer videre inn til bedre beskyttet informasjon. Departementet må dermed, for å skape et helhetlig forsvarlig sikkerhetsnivå, ha en god forståelse for alle verdier og verdikjeder i totalforsvaret. De definerer gjennom vedtakene sine, hvor sikkerhetstiltakene starter og slutter i det helhetlige systemet. Funksjonelt lovverk innen sikkerhet skal skape samfunnssikkerhet gjennom en forståelse for og etterlevelse av lovverket, hos alle relevante aktører og deriblant private selskap. De private selskapene selv kan ha et insentiv til å definere seg selv ut av målgruppen for loven ettersom det er kostnadsdrivende å gjennomføre tiltak og verdiene de sikrer ikke nødvendigvis er deres egne.

En annen utfordring som kommer tydelig frem er at firmaene ikke selv har definert skriftlig hva de legger i det sentrale begrepet i loven – «et forsvarlig sikkerhetsnivå». Funksjonelle lovverk er som Jore og Moen påpeker vanskeligere for myndighetene å følge opp da de ikke kan inspisere overholdelsen av regler. Rollen til inspektøren har av den grunn blitt en mer ressurs og kunnskapskrevende rådgiverrolle (Jore & Moen, 2015, s. 680). Dersom de strategiske logistikkpartnerne er underlagt loven så har de tydeligvis ikke blitt inspisert, eller rådgitt, i forhold til om de oppfyller lovens krav. Dette kan være fordi myndighetene ikke har nok ressurser med den riktige kompetansen til å gjennomføre gode inspeksjoner med grunnlag i sikkerhetsloven. Det er en krevende rolle å inspisere eller rådgi firmaer innenfor funksjonelt regelverk, da det krever tid og kunnskap. For å kunne bedømme om lovverket er fulgt må organisasjonens oppbygning, ressurssituasjon og infrastruktur være kjent, samtidig som den sikkerhetsmessige konteksten må forstås. Med den stadig økende kompleksiteten i verden er denne oppgaven stadig vanskeligere. Den interaktive kompleksiteten som ligger i lange verdikjeder og komplekse organisasjoner som konsernene de strategiske logistikkpartnerne er del av, må forstås og sikres på en egnet måte og med riktig ressursbruk. Ikke-lineær kompleksitet vil også være en faktor som en eventuell inspektør må ta stilling til ettersom konsernstrukturene kan skape endringer som ikke er basert på det sikkerhetsbilde som Forsvarsdepartementet er interessert i.

Uavhengig av om Forsvarets strategiske logistikkpartnere er underlagt sikkerhetsloven med vedtak eller ikke, er det utfordringer ved bruken av lovverket som belyses. Er de definert utenfor av departementet så har de likevel en klar rolle i totalforsvaret og er innenfor det de hemmelige tjenestene definerer som etterretningsmål i åpne vurderinger. Er de definert innenfor, og vedtak er fattet så er det lite sannsynlig at det har blitt fulgt opp med inspeksjoner eller rådgivning på gjennomføringen av risikostyringen som skal føre til et forsvarlig sikkerhetsnivå. Skulle denne typen inspeksjon komme så er det som belyst over, en rekke utfordringer som møter inspektøren for å få god nok kunnskap til å vurdere hvorvidt loven følges.

6.1.2. Bruken av krav fra kontrakter

Gjennom case-studien har det kommet frem at firmaene i hovedsak forholder seg til krav som fremgår av enkeltkontrakter de har med Forsvaret, heller enn å forsøke å definere hva et

forsvarlig sikkerhetsnivå er. Firmaene har ikke en dokumentert beskrivelse av hva de mener ligger i begrepet «forsvarlig sikkerhetsnivå», men har fortsatt en forståelse av hva dette sikkerhetsnivået er. Denne forståelsen er i stor grad basert på at de har en overvekt av ansatte med bakgrunn fra Forsvaret, som har denne forståelsen med seg fra sin tidligere karriere. Respondenten i firma A beskriver at de «… tar utgangspunkt i de kravene som ligger i de sikkerhetsavtalene vi har.», og fremgangsmåten bekreftes av respondenten i Firma B som forteller at «Vi oppfyller egentlig sikkerhetsloven ved å ha den dokumentasjonen som FMA industrisikkerhet stiller [krav om] til oss.».

Dette er en utfordring for bruken av et funksjonelt lovverk i totalforsvaret. Det ligger en antakelse til grunn for funksjonelle lovverk, om at de som underlegges dem har kompetansen og kunnskapen som skal til for å forstå risikoen (Jore & Moen, 2015, s. 679). Utfordringen i dette tilfellet er at firmaene bekrefter at de er underlagt sikkerhetsloven, men er usikre på i hvilken grad. Dette fører til at de ikke selvstendig setter seg inn i loven, men velger å forholde seg til de bestemmelser som kreves av dem i forbindelse med sikkerhetsavtaler de har undertegnet. Det forsvarlige sikkerhetsnivået er basert på de ansattes situasjonsforståelse og krav som er gitt dem fra Forsvaret i kontrakter. Slik sett kan man si at de omgår den funksjonelle delen av lovverket og forholder seg til et sett med krav som de antar at der en operasjonalisering gjort av Forsvaret. Dermed forholder firmaene seg i stor grad til et deterministisk reguleringsregime, selv om de er underlagt et funksjonelt lovverk. Sikkerhetsloven «legger jo mye ansvar over på den sivile aktøren» kommenterer respondent A, men firmaene velger å skyve ansvaret over til Forsvaret igjen.

Jore og Moen beskriver i tillegg at hverken funksjonelle eller deterministiske regelverk vil fungere alene, men at de er komplementære og man må derfor finne en balanse mellom de to (Jore & Moen, 2015, s. 677). Uavhengig av om firmaene er underlagt loven ved vedtak i Forsvarsdepartementet kan dette med andre ord være en fornuftig tilnærming. De sivile aktørene har et forhold til hvilken type kompetanse som er nyttig å ha for å forstå konteksten de jobber i, mens Forsvaret har omsatt et funksjonelt regime til regler som kan følges og kontrolleres. Noe som likevel gjør at det er vanskelig for denne tilnærmingen å oppnå et forsvarlig sikkerhetsnivå i møtet med etterretningstrusselen, er behovet for kompetanse og kunnskap i det leddet som skal omsette lovverket til tiltak. Tiltakene som kreves av firmaene

gjennom sikkerhetskontraktene er basert på Forsvarets kompetanse og kunnskap, de er ikke tilpasset den enkelte organisasjon. Tiltakene er dermed ikke nødvendigvis de riktige for å oppnå den ønskede tilstanden. Dessuten er det usannsynlig at kravene endrer seg fortløpende, og mye av fordelen med funksjonell regulering faller bort. Funksjonelle regelverk skal skape en sikkerhet som tar høyde for trusler man i dag ikke er kjent med, ved at kompetansen og kunnskapen i den enkelte organisasjon benyttes til å finne de riktige tiltakene. Når man oppfyller sikkerhetsloven ved å følge deterministiske krav fra kontrakter blir tilnærmingen mindre agil. I møtet med en etterretningstrussel som har en kontinuerlig innhentingsledelse og som aktivt søker å omgå alle barrierer, gir en slik tilnærming potensielt et lavere sikkerhetsnivå.

Nå er verden noe mer kompleks enn drøftingen så langt har lagt til grunn. Det er ikke slik at disse selskapene ikke har selvstendige risikovurderinger selv om de ikke er sikre på om de er underlagt sikkerhetsloven. Firmaene er del av større konsern som har standardiserte risikovurderinger som del av sine rutiner. Begge har også IT-ressurser internt i konsernet som de benytter seg av og som jobber aktivt med alle typer trusler i det digitale rom.

Funksjonelle lovverk har en utfordring i møtet med etterretningstrusselen, men neppe i noen større grad en deterministiske lovverk ville hatt. Utfordringen for å skape et forsvarlig sikkerhetsnivå er å finne balansen i bruken av de to regimene. I de ledd som skal operasjonalisere det funksjonelle over i krav og regler som skal følges, må involveringen være bred slik at kunnskapen og kompetansen til å finne de riktige reglene sikres. Videre må man se på en oppfølging av lovverket ute hos de private aktørene i totalforsvaret, som både reviderer hvorvidt man følger pålagte regler og ser på forståelse og prosess for de områdene man må dekke selv. Denne typen oppfølging må gå mer i dybden enn denne oppgaven har gjort for å følge forståelsen og vurderingene helt ned til der de måtte dannes i konsernstrukturen.

6.2. Egnethet av normale risikovurderinger mot etterretningstrussel i kommersielle selskap

Risikovurderingsprosessen er en del av risikostyringen der risiko som treffer organisasjonen skal identifiseres, analyseres og evalueres. For å skape et fullstendig bilde av risikoen et firma opererer i må denne prosessen identifisere trusler i hele spekteret fra naturkatastrofer og menneskelig svikt, til målrettede angrep som terror og etterretning. Min påstand er at etterretningstrusselen er særlig vanskelig å vurdere på grunn av etterretningens egenart, der målet ofte er å holde hele hendelsesforløpet skjult. Ressursene disse aktørene har er også potensielt betydelig større enn andre aktører, da det i hovedsak er statlig sanksjonerte aktører som utgjør trusselen. Spørsmålet er hvor egnet metodene for risikovurdering er når det kommer til å identifisere og analysere etterretningstrusselen.

Etterretningsprosessen er beskrevet som en kontinuerlig prosess, som blant annet visualiseres av etterretningshjulet. Det er i teorikapittelet også påpekt at det også internt i innhentingsprosessen pågår fortløpende vurderinger som styrer behovet for informasjonsinnhenting. I møte med en trusselaktør som jobber kontinuerlig for å kompromittere de verdiene firmaene skal beskytte, er det viktig at risikovurderingsprosessen ikke foregår med for lange tidsintervaller. Dersom man eksempelvis velger en løsning der man gjennomfører en større risikovurdering i året, vil sannsynligvis sikkerhetsnivået være betydelig senket rett før hver vurdering. Dette påpeker begge firmaene også i intervjuene når de forklarer at de gjennomfører mindre risikovurderinger hyppig. Disse vurderingene gjennomføres med bakgrunn i oppdrag og operasjoner som større NATO øvelser. Men firmaene trekker også frem at de gjør egne vurderinger grunnet endring i sikkerhetssituasjonen generelt, som Ukraina-krigen, eller andre hendelser som synes relevante som når det offentliggjøres informasjon om større dataangrep mot norske interesser. Der firmaene beskriver en forskjell er i de periodene de ikke gjennomfører mindre risikovurderinger av disse grunnene. Firma A har da en planmessighet knyttet til styremøtene som går kvartalsvis, noe firma B tilsynelatende ikke har. De beskriver også at de fortsatt gjennomgår risikobildet med konsernsjefen med en viss grad av hyppighet, men beskriver ikke samme regelmessighet.

Ingen av firmaene beskriver at de gjennomgår helheten i risikobildet regelmessig. De oppdaterer deler av bildet med bakgrunn i de mindre vurderingene de gjør fortløpende. Firma B hadde siste store gjennomgang i 2019. Dette kan være en utfordring i møtet med en etterretningsaktør. Sårbarheter i firmaene som ikke synliggjøres av oppdrag eller situasjoner som oppstår, kan forbli uavdekket i lengre perioder. Den proaktive muligheten en risikovurdering kan gi dersom den gjennomføres regelmessig på helheten, om ikke annet helheten i en trusselkategori, faller delvis bort når man gjennomfører vurderinger basert på ytre påvirkning som operasjoner og hendelser.

6.2.1. Identifikasjon

Risikoidentifikasjonen skal avdekke trusler, farer og mulighetene som organisasjonene står ovenfor. I denne oppgavens problemstilling er det etterretningstruslene som er de aktuelle truslene firmaene står ovenfor og skal identifisere.

Viktigheten av kunnskapsdimensjonen i forståelsen av risiko har Aven løftet frem. Som beskrevet i teorien beskriver da også NS-ISO 31000 at det er anbefalt å nytte kunnskap fra alle interessenter. For risikovurderinger i totalforsvaret er det vanskelig å avgrense hvem som er interessentene, men dersom man benytter kunnskap kun fra eget firma er det mest sannsynlig ikke dekkende. For å få kunnskap som kan hjelpe dem med å identifisere risiko benytter da også firmaene statlige ressurser de har tilgjengelig. De har et forhold til Forsvaret og mottar informasjon gjennom koordineringscellen de er del av i FLO-systemet. Dessuten benytter de seg av åpne trusselvurderinger fra sikkerhetstjenestene, og firma A beskriver også direkte kontakt med noen av disse tjenestene.

For å identifisere risiko har jeg fremhevet vurderingene av verdi og trusler i teoridelen, med bakgrunn i de norske standardene. Når det gjelder verdivurderingen så skal jo denne i henhold til teorien identifisere og gradere alle verdiene firmaene eier eller forvalter. Denne vurderingen skal føre til en liste over de verdiene som skal beskyttes, og vil ofte rangeres etter det Smith og Brooks kaller «criticality» (Smith & Brooks, 2013, s. 66). Denne eksersisen er ikke enkel for et firma i totalforsvaret, da de er nødt til å forstå verdien de forvalter for nasjonens forsvar i både nåtid og fremtidige scenarioer. Dessuten må disse verdiene rangeres

etter hvor kritiske de er, også i sammenligning med egne verdier som kun angår firmaet eller konsernet de er en del av. Firmaene jeg har undersøkt for oppgaven har begge et forhold til verdibegrepet og har i forbindelse med ISO 9001 definert verdiene. De identifiserte verdiene er overordnede for selskapet og omfatter eksempelvis omdømme og informasjon. Disse verdiene benytter de når de risikovurderer operasjoner for Forsvaret også, og firma A påpeker viktigheten av å beskytte verdien som ligger i Forsvarets robusthet. For en verdivurdering opp mot en spesifikk trussel som etterretningstrusselen så fremstår det som beskrives som noe grovmasket. Informasjonen som firmaene besitter med bakgrunn i sine kontrakter med Forsvaret er de veldig opptatt av å beskytte, men om de har andre verdier som er interessante for en etterretningsaktør i forhold til Forsvaret virker de ikke sikre på. Dette er også veldig vanskelig å svare på og firma B påpeker også utfordringen med at de får gradert informasjon som de må operasjonalisere gjennom ugraderte kanaler.

Trusselvurderingen utvikles med bakgrunn i ugraderte trusselvurderinger fra sikkerhetstjenestene, informasjon de får direkte fra Forsvaret og fra åpne kilder. De mottar også tidvis informasjon direkte fra sikkerhetstjenestene, som ikke er offentlig kjent. Det fremstår som at begge firmaene basert på dette har relativt god og grundig forståelse for trusselaktørene med deres intensjon og kapasitet. Det at de har mulighet til å diskutere trusselbildet åpent med Forsvaret i koordineringscellen trekkes frem av begge firma som viktig. Dessuten er det tydelig at de med den kompetansebakgrunnen personellet deres har, evner å omsette de åpne rapportene til noe mer enn et overordnet bilde på trusselsituasjonen.

Risikoidentifikasjonen er utfordrende for disse kommersielle firmaene når det kommer til etterretningstrusselen som angriper verdier som forvaltes på vegne av Forsvaret. Det å forstå denne typen verdier er vanskelig, og det er i tillegg vanskelig å forstå hvordan en etterretningsorganisasjon tenker. For å fullt ut forstå intensjonen til en statlig etterretningsaktør vil man måtte forstå seg selv og sin rolle i totalforsvaret slik som etterretningstjenesten ser det. De benytter sannsynligvis en versjon av targeting og kan derfor se firmaene på flere måter. Firmaet kan være et mål i seg selv for å få informasjon som kan være en indikator på militær aktivitet, eller en vei inn til andre organisasjoner eller annen informasjon som ligger videre i verdikjeden. Utfordringen for særlig verdivurderingen er derfor å se og forstå hele spekteret av verdier som kan være truet. Firmaene synes å være gode

på de overordnede verdiene for seg selv og Forsvaret, og på de spesifikke verdiene som kommer som følge av eksempelvis større øvelser. Der det kan fremstå som metodene deres skaper mindre kontroll er i de detaljerte verdiene som har lengre tidshorisont. Detaljene rundt verdiene som skaper Forsvarets robusthet på lang sikt vil det være vanskelig å ha kontroll på med metodene som er beskrevet.

6.2.2. Analyse

Risikoanalysen skal skape et mer detaljert bilde av risikoene som er identifisert. Aven, Røed og Wiencke klassifiserte risikoanalyser i forenklede, standard og modellbaserte analyser (Aven, Røed, & Wiencke, 2017, s. 16) som beskrevet i teoridelen. Firmaene beskriver sine metoder på en måte som best passer med de forenklede analysene, da de i stor grad baserer seg på gruppediskusjon og en konsensus i gruppen. Når det er sagt så beskriver de scenarioutvikling som del av risikoanalysen, der en risiko ofte utvikles i flere scenarioer for å se både de mest sannsynlige og de verst tenkelige utfallene. Så selv om ingen av firmaene beskriver bruk av analysemetoder som normalt inngår i grovanalyser, så gjennomfører de analyser som kan beskrives som også kan gå inn under beskrivelsen som er gitt av standardanalyser i teoridelen.

Jeg har i teoridelen trukket frem sårbarhetsvurderingen, i tillegg til sannsynlighets- og konsekvensanalysen, som del av risikoanalysen. Vurderingen av sårbarhet skal avdekke i hvor stor grad en verdi kan motstå en trussel. Dette er en svært vanskelig vurdering å ta av en etterretningstrussel ettersom det er lite kunnskap om hvilke kapabiliteter en slik aktør har. Det er en grunn til at disse tjenestene i Norge kalles de hemmelige tjenestene, da de forsøker å holde så mye informasjon om egne metoder, kapabiliteter og kapasiteter hemmelig. Firmaene beskriver også at dette er noe de selv i liten grad har kompetanse til å vurdere, men de gjør fortsatt de vurderingene de kan ved å ettergå verdikjeder og bruke «red team». Begge firmaene beskriver at særlig cyberdomenet er vanskelig, men konsernressurser innen IT fremstår som svært kompetente og profesjonelle. De benytter metoder som såkalt «penetrasjonstesting», der en innleid part forsøker å trenge inn i systemene for å avdekke sårbarheter.

Sannsynlighet kan være et kvantifisert begrep eller en beskrivelse av en subjektiv vurdering i risikosammenheng. Begge respondentene beskriver da også at de i hovedsak anser sannsynlighet for å være et tall mellom 0 og 1, men at de benytter seg av kunnskapsbasert vurdering av sannsynlighet i denne sammenhengen. For å kunne fylle en kunnskapsbasert sannsynlighetsvurdering med noe mer mening for beslutningstakerne er det viktig å ha et forhold til kunnskapsstyrken i vurderingen. Hvor god kunnskapen til analysegruppen er og hvor god informasjon som ligger til grunn for analysen bør man ha en viss kontroll på. Begge firmaene har en overvekt av ansatte med militær bakgrunn, som gir dem bakgrunnskunnskap om sikkerhetssituasjonen og etterretningstrusselen. Men det er også fare for en grad av gruppetenkning dersom analysegruppen har en for lik bakgrunn og ikke utfordres av andre perspektiver. Dette kan for firmaene føre til at de legger litt for stor vekt på mageføIelsen, all den tid de ikke nytter seg av mer strukturerte analysemetoder enn scenariobygging. Sannsynligheten for at etterretningstrusler mot firmaene skal materialisere seg er uavhengig av analysemetoden følt som høy i begge firmaene. De uttrykker at de ikke vurderer dette selv, men lytter til myndighetene som forteller dem at de er utsatt. Jeg opplever at dette er basert på mer analyse enn de er klar over selv, da de har lest og vurdert de åpne trusselvurderingene for å komme til konklusjonen om at de er svært utsatte.

Konsekvensdimensjonen er vanskelig når det gjelder kommersielle selskap som er del av totalforsvaret gjennom avtaler med Forsvaret. For å skape et forsvarlig sikkerhetsnivå kan de ikke forholde seg kun til konsekvensene de opplever selv som firma. Konsekvenser for Forsvarets robusthet, som firma A beskriver det, er også en vesentlig faktor i analysen. Begge firmaene benytter seg i større eller mindre grad, av scenariobygging som fører til en sannsynlig konsekvens og en «worst case» konsekvens. Dette er en styrke ettersom det er viktig å ha et forhold til hvordan konsekvensen som er beskrevet er utarbeidet, som jeg beskrev i teoridelen. De beskriver ikke hvordan de analyserer konsekvensene av eventuelle etterretningsaksjoner mot dem, men forsøker å sette alle konsekvensene i sammenheng med de overordnede verdiene til konsernet. De bekrefter at de som kommersielle aktører hovedsakelig er opptatt av konsekvenser som kan måles i kroner og øre, men at eventuelle konsekvenser for Forsvaret også vil ha det. Dersom de er ansvarlige for en konsekvens som treffer Forsvaret så vil det ha en omdømmekonsekvens for firmaet, som i neste omgang har en kommersiell konsekvens.

Risikoanalysene til firmaene kan synes enkle og noe overfladiske ettersom de beskriver dem som gruppediskusjoner som ender med en konsensus. Men det ligger mer til grunn gjennom bruk av eksterne kilder til kunnskap, scenariobygging og vurderinger tatt med bakgrunn i erfaring fra både Forsvaret og private firma. Det som er vanskelig å vurdere er i hvor stor grad de forstår sin plass i risikoen som treffer totalforsvaret i sin helhet. På den ene siden er de opptatt av Forsvarets robusthet og av å ikke kompromittere gradert informasjon de har tilgang til. På den andre siden er de tydelige på at det er den kommersielle konsekvensen de er opptatt av og alle konsekvenser for Forsvaret blir til en viss grad sett på med disse brillene. Satt på spissen kan det synes som de, selv om de ser sin egen rolle i totalforsvaret og forstår risikobildet de er en del av, ser på Forsvaret som en hvilken som helst kunde og ikke tar et selvstendig ansvar for å minimere risiko som ikke har konsekvenser for dem selv.

6.2.3. Evaluering

Risikoevalueringen drar sammen informasjonen fra risikoidentifikasjonen og risikoanalysen og skal presentere et beslutningsgrunnlag for beslutningstakerne. Her benytter begge firmaene seg av systemer som er implementert i konsernene og som tar utgangspunkt i en visualisering basert på sannsynlighet og konsekvens. Firma A forklarer et system der konsekvensdimensjonen må gjøres sammenlignbar når den skal inn i systemet, og at det gjør at alle risikoer må uttrykkes med en kostnad som risiko. Informanten beskriver videre at de til enhver tid jobber aktivt med de 10 risikoene som er ansett som størst. Firma B forklarer ikke nøyaktig hvordan dette gjøres i konsernet, men har beskrevet en tabell de benytter for å sammenligne konsekvenser mellom kategorier som liv og helse, og kostnader.

Ingen av de to firmaene beskriver bruk av risikotrekanten som et visualiseringsverktøy, mens firma A er tydelige på at de bruker risikomatriser. Slike matriser kan kritiseres for å være sterkt forenklende og ikke gi et godt beslutningsgrunnlag (Jacobsen, Thorkildsen, & Eikeland, 2018). Dette synes ikke å være en utfordring i firmaene da de beskriver prosessene som veldig inkluderende med leddene over. Firma A beskriver sine gjennomganger av risiko med styret som en åpen diskusjon og på denne måten blir risikomatrisen kun en liten del av det totale produktet som beslutningstakerne får. Utfordringen jeg opplever at begge firmaene har er at de må sammenligne risikoer av svært forskjellig art, og med svært forskjellige konsekvenskategorier, opp mot hverandre for å få beslutninger på hva som skal prioriteres. Da

blir tilsynelatende de kravene som er gitt i forskjellige kontrakter med Forsvaret førende for hvilke tiltak som blir iverksatt.

De normale risikovurderingene som er beskrevet blant annet i norske standarder er utviklet for en gitt type risikoer, men firmaene jeg har fått intervjue i prosjektet benytter seg grunnleggende av de samme metodene uavhengig av type risiko. Hvor egnet dette er for å oppnå forsvarlig sikkerhet kan diskuteres, men firmaene følger ikke standardene slavisk. Selv om begge har en hovedvekt på å vurdere sannsynligheten og konsekvensen av forskjellige risikoscenarioer, benytter de seg også av faktorene verdi, sårbarhet og trussel. De henter den informasjonen de kan for å skape best mulig forutsetninger for gode beslutninger. Men utfordringen er også mangelen på hyppigere risikovurderinger som i større grad følger de beskrevne trinnene og metodene. Det kan synes som de baserer seg vel mye på informasjonen de får og vurderingene de tar med bakgrunn i egen erfaring. Dette fungerer godt i mange sammenhenger, men det er usikkert om de utfordrer seg selv og sine vurderinger nok til å avdekke andre trusler og sårbarheter enn de er kjent med fra før.

6.3. Mulig forbedring i metodikk

Metodikken firmaene benytter er relativt lite formell i det at den ikke benytter seg av normale risikoanalyseverktøy, men baserer seg i stor grad på konsensus basert på åpne diskusjoner i gruppen. Hyppigheten av risikovurderingene er varierende, men med operasjoner og hendelser øker takten. Dette medfører at de i stor grad vurderer mindre områder av det store risikobildet og oppdaterer bildet litt og litt. Ingen av firmaene forholder seg vesentlig annerledes til etterretningstrusselen enn de gjør til andre trusler, men de skaffer seg så klart kunnskap og bakgrunnsinformasjon fra myndighetene. I denne delen av drøftingen vil jeg løfte særlig tre områder der det er en mulighet for forbedring av metodikk. Dette er bruk av enkle verktøy, den kontinuerlige risikovurderingsprosessen, og en økt forståelse av helhet.

Firmaene har noen verktøy som er standard i egne konsern, men dette er slik jeg ser det i hovedsak visualiserings verktøy. De er ikke designet for å identifisere trusler firmaene ikke allerede har et forhold til. Prosessen firmaene beskriver for å identifisere verdier og trusler ligger i det som kan betegnes som en forenklet risikoanalyse (Aven, Røed, & Wiencke, 2017,

s. 16). De utvikler scenarioer med bakgrunn i etterretningsinformasjon de har mottatt, og baserer seg på vurderingene til Forsvaret og egen forståelse. Dette gir antatt en god forståelse, men det er som nevnt i teorien en fare for gruppetenkning. Bruk av enkle risikoanalyseverktøy til å utfordre sine egne antakelser vil kunne sikre firmaene i større grad når det gjelder å avdekke risikoer. Eksempelvis kan det være nyttig å gå gjennom de overordnede verdiene som er identifisert og vurdere kritikaliteten for den enkelte av dem for firmaet og for totalforsvaret. En slik nedbryting som ikke er operasjonsavhengig, kan i tillegg ses på i flere bolker av tidshorisonter som kort, midlere og lang sikt. En slik vurdering ville ikke nødvendigvis gitt en endring i dagens tiltak, men vil kunne føre til et mer nyansert syn på enkelte verdier. Denne dypere forståelsen av verdiene kunne igjen skape mer av det funksjonelle lovverk ønsker da ny informasjon kan ses opp mot en eksisterende vurdering og raskt føre til endringer i tiltak.

Muligheten for å dokumentere enkelte analysetrinn ved å benytte verktøy som kritikalitetslister bringer meg til neste forbedringsområde. Etterretningshjulet beskriver en kontinuerlig prosess der organisasjonen hele tiden evaluerer og korrigerer seg selv og produktene som produseres. I møte med denne typen aktører er det et kontinuerlig arbeid som er må gjøres for å identifisere, analysere og evaluere risikoer. Dette gjør begge firmaene i stor grad, men det er to aspekter ved deres kontinuerlige arbeid jeg mener kan vurderes. Hyppigheten av risikovurderinger øker i tider der det er operasjoner, øvelser eller andre hendelser som krever det. Dette er fornuftig, men vil kunne gjøres mer effektivt ved å ha et etablert risikobilde for etterretningstrusselen som all ny informasjon sjekkes opp mot. Det er ikke nødvendigvis behov for en fullstendig gjennomgang av hele risikobildet til firmaene, men et risikobilde som eksempelvis tar inn over seg alle ondsinnede handlinger. Dette bildet vil antatt ha en større endringstakt og dynamikk enn risikoer for naturkatastrofer og organisatoriske ulykker. Det er også fornuftig å involvere bredt for å etablere dette bildet, slik at annen kunnskap og andre vinklinger utfordrer firmaets eksisterende antakelser.

Det siste området jeg mener kan forbedres er det å se på helheten. Det er behov for en klar forståelse av risikovurderingene gjort av andre som har innvirkning på risikobildet. Firmaene synes for det første å ha en stor grad av tillit til sine samarbeidspartnere på risikoområdet, som egne IT ressurser, uten å kunne forklare meg hva disse konkluderer med når det gjelder

etterretningstrusselen. Dette er ikke nødvendigvis noe problem for sikkerheten som skapes, men for et firma underlagt sikkerhetsloven anser jeg det som fornuftig å ha denne kunnskapen. Det vil blant annet sørge for at det ikke er misforståelser mellom leddene i hva som skal sikres. Det er også viktig å se helheten utenfor egen organisasjon. Dersom man etablerer et risikobilde for etterretningstrusselen spesifikt, eller villede handlinger mer generelt, er det viktig å ha en helhetstankegang. Man må ta inn over seg hele totalforsvaret ettersom trusselaktøren kan antas å gjennomføre en type targetinganalyse for å finne veier til informasjon. Som del av totalforsvaret og verdikjedene i totalforsvaret kan dermed sikkerhetshull i firmaene bli benyttet for å kompromittere andre elementer i kjeden. Uten denne helhetstankegangen vil det være vanskelig å skape forsvarlig sikkerhet for totalforsvaret selv om den enkelte organisasjon gjør det den kan for å sikre seg selv.

7. Konklusjon og forslag til videre forskning

Jeg har med oppgaven ønsket å belyse i hvor stor grad risikovurderinger som gjøres hos de strategiske logistikkpartnerne skaper et forsvarlig sikkerhetsnivå mot etterretningstrusler. Svaret på det er det på ingen måte to streker under.

Jeg etablerte tre forskningsspørsmål for å svare på problemstillingen.

Det første var hvordan firmaene forholdt seg til et funksjonelt lovverk som sikkerhetsloven. Her fant jeg at firmaene hadde en etablert rolleforståelse i forhold til totalforsvaret og de sa at var underlagt sikkerhetsloven. Ingen av dem hadde brutt ned føringene som gis i loven og sett selvstendig på hva det kunne bety for dem, og jeg mener forholdet til sikkerhetsloven er noe uklart. De forholder seg til en rekke kontrakter og sikkerhetsavtaler de har med Forsvaret, som alle inneholdt krav var utledet fra sikkerhetsloven. Slik sett kan man si at de forholdt seg til en funksjonell lov ved å oppfylle kravene i deterministiske kontrakter. Tanken er at de ved å oppfylle kravene skaper et forsvarlig sikkerhetsnivå. Dette illustrerer en utfordring ved at de kommersielle aktørene selv må ha kunnskap og kompetanse nok til å oppfylle en funksjonell lov. De må velge, og ha mulighet til, å benytte ressurser til å gjøre den analytiske jobben. Samtidig må staten ha kunnskap og ressurser til å følge opp lovverket ved å utfordre og støtte firmaene i jobben.

Det andre forskningsspørsmålet var i hvilken grad risikovurderingsprosessen var egnet til å identifisere etterretningstrusler. Dette var ikke så enkelt å konkludere på ettersom prosessen som beskrives i firmaene verken følger teorien eller standardene slavisk. Gjennom analysen av intervjuene har jeg likevel kommet til at de gjennomfører alle leddene i en risikovurdering. De gjennomfører risikovurderinger på mindre deler av risikobildet med en situasjonsbestemt hyppighet. Bruken av informasjon fra statlige aktører, og en overvekt av ansatte med forsvarsbakgrunn, fører til at firmaene har kunnskapen til å identifisere etterretningstrusler. Risikovurderingene er godt forankret i begge firma og det er tydelig at vurderingen av etterretningstrusselen fører til risikoreduserende tiltak i firmaene. Utfordringen for å identifisere etterretningstrusler med risikovurderinger er helheten utenfor firmaene, da risikovurderinger naturlig er sentrert rundt firmaet selv og det er vanskelig å forstå en stor nok helhet.

Det siste forskningsspørsmålet var hvilken metodisk tilnærming firmaene hadde til risikovurderingene. Begrepsforståelsen var god innenfor risikovurderingenes sentrale begreper, men som sagt ble ingen standarder fulgt slavisk. Det var likevel klart at firmaenes utgangspunkt var at risiko var et uttrykk basert på sannsynlighet og konsekvens, og at alle typer risiko til slutt ble vurdert opp mot hverandre i en og samme mal.

Alt i alt vil jeg konkludere med at de strategiske logistikkpartnerne gjør mye godt arbeid for å skape et forsvarlig sikkerhetsnivå. De gjør det ikke nøyaktig i henhold til teorien og er mer pragmatiske i sin tilnærming enn jeg hadde forutsett. Dette utfordrer bruken av teori og standarder som jeg hadde forventet å finne. Jeg mener de har et forsvarlig sikkerhetsnivå mot etterretningstrusler som er rettet mot deres verdier eller verdiene som forvaltes av dem for totalforsvaret, jeg er derimot mer usikker på om totalforsvaret har et forsvarlig sikkerhetsnivå mot en etterretningstrussel. Etterretningsaktører jobber med et helhetsbilde når de søker å finne informasjonen de har behov for og det er vanskelig å etablere en like helhetlig sikkerhet for et løselig definert totalforsvar. Lovverket legger til grunn at forsvarlig sikkerhet for nasjonens interesser skapes ved at alle organisasjonene underlagt loven etablerer forsvarlig sikkerhet selv. Denne sikkerheten skal også være basert på vurderinger rundt verdier som forvaltes for andre. Utfordringene er at det er vanskelig å definere hva et forsvarlig sikkerhetsnivå er, det er vanskelig å si hvem som bør endre på noe for å forbedre den overordnede sikkerheten. Det er kanskje ingen som har nok helhetsforståelse til å ta ansvar for at den helhetlige sikkerheten.

Videre forskning innen oppgavens tema kan gå både i bredden og dybden. Det kunne vært interessant å se på forsvarlig sikkerhet i totalforsvaret fra statens side, og se på hvilke muligheter staten har til å sikre at sikkerhetsnivået er tilstrekkelig. Det kan også være interessant å dykke ned i vurderingene som gjøres i de strategiske logistikkpartnerne. Både ved å observere risikovurderingsprosessen og å forfølge vurderingene firmaene baserer seg på fra egne IT ressurser og de statlige aktørene som utformer kravene som stilles i kontrakter.

Bibliografi

Altman, R. (2021, november 21). *Russia preparing to attack Ukraine by late January: Ukraine defense intelligence agency chief*. Hentet april 26, 2022 fra Military Times: https://www.militarytimes.com/flashpoints/2021/11/20/russia-preparing-to-attack-ukraine-by-late-january-ukraine-defense-intelligence-agency-chief/

Andrew, C., Aldrich, R. J., & Wark, W. K. (2020). Introduction - What is intelligence? I C. Andrew, R. J. Aldrich, & W. K. Wark, *Secret Intelligence - A Reader* (ss. 1-3). New York: Routledge.

Aven, T. (2012a). *Foundations of Risk Analysis.* Chichester: Wiley-Blackwell.

Aven, T. (2012b, august 20). *Risikotenkningen er fullstendig foreldet.* Hentet mars 22, 2022 fra Stavanger Aftenblad: https://www.aftenbladet.no/meninger/i/PEdl5/risikotenkningen-er-fullstendig-foreldet

Aven, T. (2015). *Risikostyring.* Oslo: Universitetsforlaget.

Aven, T., Røed, W., & Wiencke, H. S. (2017). *Risikoanalyse.* Oslo: Universitetsforlaget.

Blaikie, N. (2010). *Designing Social Research.* Cambridge: Polity Press.

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* Kjeller: Forsvarets forskningsinstitutt.

Congressional Research Service. (2021). *Russian Military Intelligence: Background and Issues for Congress.* Washington DC: Congressional Researvh Service. Hentet fra https://crsreports.congress.gov/product/pdf/R/R46616

DSB. (2014). *Nasjonalt risikobilde 2014.* Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

DSB. (2019). *Analyser av krisescenarioer.* Tønsberg: Direktoratet for samfunnssikkerhet og beredskap.

Eilertsen, A., & Persvold, A. Z. (2019, juni 11). *kompleksitet*. Hentet april 11, 2022 fra Store norske leksikon: https://snl.no/kompleksitet

Elvemo, L., & Jakobsen, R. (2020, juni 14). *Hva er militær logistikk?* Hentet april 26, 2022 fra Stratagem: https://www.stratagem.no/hva-er-militaer-logistikk/

Endregard, M. (2019). Totalforsvaret i et sivilt perspektiv. I P. M. Norheim-Martinsen (red), *Det nye totalforsvaret* (ss. 62-80). Oslo: Gyldendal Norsk Forlag.

Engebretsen, N. F. (2019, juni 4). *Bring - Fra brev til beltevogner for Forsvaret*. Hentet april 6, 2022 fra Bring: https://www.bring.no/magasinet/ehandel-og-logistikk/fra-brev-til-beltevogner-for-forsvaret

Engen, O. A., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E., & Pettersen, K. A. (2017). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm AS.

Etterretningstjenesten. (2011). *FOKUS.* Oslo: Etterretningstjenesten.

Etterretningstjenesten. (2016). *FOKUS.* Oslo: Etterretningstjenesten.

Etterretningstjenesten. (2019). *FOKUS.* Oslo: Etterretningstjenesten.

Etterretningstjenesten. (2021). *FOKUS.* Oslo: Etterretningstjenesten.

Etterretningstjenesten. (2022). *FOKUS.* Oslo: Etterretnignstjenesten.

Ezell, B. C. (2007, juli). Infrastructure Vulnerability Assessment Model (I-VAM). *Risk Analysis*, ss. 571-583. Hentet april 12, 2022 fra https://www.researchgate.net/publication/6198799_Infrastructure_Vulnerability_Assessment_Model_I-VAM#:~:text=The%20Infrastructure%20Risk%20Analysis%20Model%20%28IRAM%29%20introduced%20by,The%20result%20is%20a%20rank%20ordering%20of%20vulnerability.

Forsvaret. (2019). *FFOD.* Oslo: Forsvarsstaben.

Forsvaret. (2020, oktober 12). *Forsvarets logistikkorganisasjon*. Hentet april 6, 2022 fra Forsvaret: https://www.forsvaret.no/om-forsvaret/organisasjon/forsvarets-logistikkorganisasjon

Forsvaret. (2021). *Forsvarets Etterretningsdoktrine.* Oslo: Forsvarssjefen.

Forsvarsdepartementet og Justis- og beredskapsdepartementet. (2018). *Støtte og samarbeid - En beskrivelse av totalforsvaret i dag.* Oslo: Forsvarsdepartementet og Justis- og beredskapsdepartementet.

Galeotti, M. (2017, mai 12). *Russian intelligence is at (political) war.* Hentet april 14, 2022 fra NATO Review: https://www.nato.int/docu/review/articles/2017/05/12/russian-intelligence-is-at-political-war/index.html

Giles, L. (2000). *Sun Tzu on th Art of War.* Leicester: Allandale Online Publishing.

Grande, A. (2017, mai 15). *DN - Forsvaret tyr til sivile for å bli mer effektive*. Hentet april 6, 2022 fra DN: https://www.dn.no/shipping/forsvaret/grieg-gruppen/forsvaret-tyr-til-sivile-for-a-bli-mer-effektive/2-1-84580

Halvorsen, T. (2022, april 14). *Russisk cybervåpen funnet i Norge*. Hentet april 14, 2022 fra Dagbladet: https://www.dagbladet.no/nyheter/russisk-cybervapen-funnet-i-norge/75858022

Henriksen, A. H., & Tranøy, K. E. (2021, januar 10). *Konsekvens.* Hentet mars 23, 2022 fra Store Norske Leksikon: https://snl.no/konsekvens

Håkenstad, M. (2019). Den væpnede dugnaden - totalforsvaret under den kalde krigen. I P. M. Norheim-Martinsen, *Det nye totalforsvaret* (ss. 25-40). Oslo: Gyldendal.

Jacobsen, I. M., Thorkildsen, A., & Eikeland, L. (2018, februar 28). *Helhetlig risikostyring og visualisering av risikobildet - grunnlag for best mulig beslutningsstøtte*. Hentet april 26, 2022 fra bouvet.no: https://www.bouvet.no/bouvet-deler/metode-for-helhetlig-risikostyring-og-visualisering-av-risikobildet

Jahre, M., & Persson, K. G. (2011). Logistikk og ledelse av forsyningskjeder. I K. G. Persson, & H. (. Virum, *Logistikk og ledelse av forsyningskjeder* (ss. 52-68). Oslo: Gyldendal Akademisk.

Johannesen, A., Tufte, P. A., & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag AS.

Jore, S. H., & Moen, A. (2015). A discussion of the risk-management and the rule-compliance regulation regimes in a security context. I A. Nowakowski, *Saftey and Reliability: Methodology and Applications* (ss. 677-684). London: Taylor & Francis Group.

Justis- og beredskapsdepartementet. (2019). *Veileder til samfunnssikkerhetsinstruksen.* Oslo: Justis- og beredskapsdepartementet.

Knightley, P. (1986). *The Second Oldest Proffesion: Spies and Spying in the Twentieth Century.* New York: W.W. Norton & Company.

Kveberg, T., Alme, V., & Diesen, S. (2019). *Defence against foreign influence.* Kjeller: Forsvarets forskningsinstitutt.

Leveson, N. G. (2017). *Engineering a Safer World.* Cambridge: The MIT Press.

Listou, T., & Ekstrøm, T. (2022, mars 28). *Russland i Ukraina: uten logistikk skjer det lite på slagmarken*. Hentet april 23, 2022 fra Stratagem: https://www.stratagem.no/russland-ukraina-logistikk/

Lorentsen, M. (2015, mars 20). *E24 - Wilh. Wilhelmsen skal øke Forsvarets beredskap: -En historisk avtale*. Hentet april 6, 2022 fra E24: https://e24.no/naeringsliv/i/MRAROJ/wilh-wilhelmsen-skal-oeke-forsvarets-beredskap-en-historisk-avtale

NATO. (2016, februar). AJP-2. *Allied Joint Doctrine for Intelligence-, Counterintelligence and Security*. NATO Standardization Office.

NATO. (2021, november). AJP-3.9. *Allied Joint Publication for Joint Targeting*. NATO Standardization Office.

NCSC. (2022). *Advisory - New Sandworm malware Cyclops Blink replaces VPNFilter.* National Cyber Security Center (UK).

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

NOU. (2000). *NOU 2000:24 - Et sårbart samfunn.* Oslo: Instilling fra utvalg oppnevnt ved kongelig resolusjon 3. september 1999.

NS 5814. (2021, april). *Krav til risikovurderinger*.

NS 5830. (2012, juni). *Samfunnsikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Terminologi*.

NS 5832. (2014, november). *Samfunnssikkerhet - Beskyttelse mot tilsiktede uønskede handlinger - Krav til sikringsrisikoanalyse*.

NS-ISO 31000. (2018, november). *Risikostyring - Retningslinjer*.

NSM. (2021). *Risiko 2021 - helhetlig sikring mot sammensatte trusler.* Oslo: Nasjonal sikkerhetsmyndighet.

NSM, PST og POD. (2015, september 30). *Veileder i terrorsikring.* Hentet fra PST: https://www.pst.no/globalassets/artikler/utgivelser/veileder-i-terrorsikring.pdf

Omand, S. D. (2019). Et historisk tilbakeblikk. I S. Stenslie, L. Haugom, & B. H. Vaage (red.), *Etterretningsanalyse i den digistale tid - en innføring* (ss. 33-50). Bergen: Fagbokforlaget.

Perrow, C. (1984). *Normal accidents: living with high risk technologies.* New York: Basic Books.

Prop. 153 L (2016-2017). (u.d.). *Lov om nasjonal sikkerhet (sikkerhetsloven).* Oslo: Forsvarsdepartementet.

PST. (2004, februar 2). *Trusselvurdering 2004*. Hentet april 6, 2022 fra PST: https://pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2004/

PST. (2009, mars 13). *Trusselvurdering 2009*. Hentet april 6, 2022 fra PST: https://pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2009/

PST. (2016). *Trusselvurdering.* Oslo: Politiets sikkerhetstjeneste.

PST. (2020, desember 8). *Datainnbruddet mot Stortinget er ferdig etterforsket*. Hentet fra PST: https://www.pst.no/alle-artikler/pressemeldinger/datainnbruddet-mot-stortinget-er-ferdig-etterforsket/

PST. (2021, februar 8). *Nasjonal trusselvurdering 2021*. Hentet april 6, 2022 fra PST: https://pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/

PST. (u.d.). *PST - Spionasje*. Hentet april 6, 2022 fra PST: https://pst.no/alle-artikler/artikler/trusler/spionasje/

Rzadkowska, J. (2021, november 7). *kompleks*. Hentet april 11, 2022 fra Store norske leksikon: https://snl.no/kompleks

Sagdahl, M. S. (2019, juni 20). *verdi*. Hentet april 12, 2022 fra Store norske leksikon: https://snl.no/verdi

Sikkerhetsloven. (2018, juni 1). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Hentet april 16, 2022 fra Lovdata: https://lovdata.no/LTI/lov/2018-06-01-24

Smith, C. L., & Brooks, D. J. (2013). *Security Science - The Theory and Practice of Security.* Oxford: Butterworth-Heinemann.

Warner, M. (2020). Wanted - A definition of 'intelligence'. I C. Andrew, R. J. Aldrich, & W. K. Wark, *Secret Intelligence - A Reader* (ss. 4-12). New York: Routledge.

VEDLEGG 1 – Intervjuguide

Søk å forstå firmaets resonnement og prosess – dette er viktigere enn rene fakta svar.

Egen definisjon på etterretningstrussel:

Etterretningstrusselen er i oppgaven forstått som trusselen for fordekt og ulovlig innhenting av informasjon fra en privat eller statlig sanksjonert organisasjon. Trusselen innebefatter for en virksomhet aktører med kapabilitet, mulighet og intensjon til å rokke ved konfidensialiteten, integriteten eller tilgjengeligheten på virksomhetens informasjon.

Innledning til intervjuet

Introdusere meg selv og min interesse for risikovurderingsfaget og tematikken rundt etterretningstrusselen.

Få informasjon om respondenten – hvilken stilling sitter vedkommende i, hvor lenge har vedkommende innehatt stillingen, hva er rollen til vedkommende i risikovurderingsprosessen, hvilken utdanning har vedkommende generelt og spesifikt rettet mot risiko?

Tydeliggjøre at oppgaven ser på metode, ikke på resultatet av vurderingen eller tiltakene som er gjennomført.

Når gjennomførte vedkommende sist en risikovurdering av denne tematikken?

Hva legge respondenten i begrepet totalforsvaret?

Overordnede spørsmål

Rolle/rolleforståelse

Hvilken rolle anser du at firmaet har opp mot totalforsvaret?

Ikke del av – hvilken rolle har firmaet i en krise/krig opp mot Forsvaret?

Del av – hvordan beskriver du rollen firmaet har i totalforsvaret og hva har det å si for dere?

Hvordan forholder firmaet seg til den nye sikkerhetsloven?

Underlagt? Er det fattet vedtak i departementet?

Hvordan definerer dere «forsvarlig sikkerhetsnivå»? Hvordan kom dere frem til denne definisjonen?

Ligger det eksplisitte krav i kontrakten med Forsvaret, hva angår risikovurdering/risikostyring?

Hva legger du i begrepet risikovurdering?

Hva legger du i begrepet etterretningstrussel?

Er firmaet et etterretningsmål? Hvem har definisjonsmakten på dette?

Har Forsvaret eller firmaet definisjonsmakt? Og hvis det er firmaet, hvem – ledelsen eller de som utarbeider risikovurderinger?

<u>Metodikk</u>

Hvordan definerer dere usikkerhet?

FFI2015/00923 – utfordring for FB metoder at usikkerhet ikke beskrives

Statistisk, teoretisk, metodeteknisk og kontekstuell usikkerhet

Hvordan representeres denne i risikoevalueringen? Hvilken rolle spiller usikkerheten i risikoevalueringen?

Hvordan definerer dere sannsynlighet?

FFI2015/00923 – utfordring for FB metoder at 5830-serien ikke forholder seg eksplisitt til sannsynlighet

SN-ISO 73:2009 – mål for hvor stort potensial det er for at noe kan skje, uttrykt som et tall mellom 0 og 1, hvor 0 er en umulighet og 1 er absolutt sikkerhet

NS-ISO 31000:2018 – potensialet for at noe kan skje (ikke rent matematisk; «likelihood» heller enn «probability»

NS 5814:2021 – hvor trolig det er at en hendelse vil inntreffe (i 2008 både tall eller ord, og frekvens kan benyttes)

Frekvensbasert eller kunnskapsbasert?

Hvor ofte utarbeides og revideres risikovurderingene?

Er det en kontinuerlig prosess der all relevant informasjon og alle relevante hendelser utnyttes til forbedring og læring?

Hvilken teoretisk forankring legges til grunn for risikovurderingen?

Hvilke standarder benyttes i firmaet i denne sammenheng?

Hvilken forankring har risikovurderingen i firmaet?

Hvem deltar i utarbeidelse og revisjon av risikovurderingene?

Samarbeider dere med noen i forbindelse med utviklingen av risikovurderinger angående etterretningstrusselen?

Hvor henter dere informasjonen som legges til grunn for vurderingene?

Hvilke åpne kilder, organisasjoner som Rederiforbundet og evt. egne møter med sikkerhetsmyndighetene

Hvilke risikoanalyseredskaper benytter firmaet i forbindelse med etterretningstrusselen?

Feiltreanalyse, hendelsestreanalyse, kost/nyttevurderinger, usikkerhetsanalyse, verdianalyse, kunnskapsstyrkeanalyse el.

Spørsmål til NS 583x-serien

Hvordan utvikles verdiforståelsen?

Intern, ekstern, kort og lang sikt

Hvordan utvikles trusselforståelsen?

Hvordan utvikles sårbarhetsforståelsen?

Hvordan forholder du deg til sannsynlighet i denne tilnærmingen?

Representeres den eksplisitt?

Hvordan evalueres risikoen opp mot andre risikoer?

Sannsynlighet/konsekvensdimensjon

Spørsmål til NS 5814

Hvilken versjon benyttes?

2008 eller 2021?

Hvordan utvikles scenariene?

Hvordan utvikles konsekvensdimensjonen?

Interne, eksterne, kort og lang sikt

Hvordan utvikles og beskrives sannsynligheten?

Hvordan evalueres risikoen opp mot andre risikoer?

Hvordan evalueres de forskjellige konsekvensdimensjonene opp mot hverandre?

Avsluttende spørsmål

Ser du muligheter til forbedring av metodikken dere benytter?

For hele risikostyringen eller etterretningstrusselen spesifikt?

Er det noen spørsmål jeg burde ha stilt for å bedre belyse problemstillingen?

Er det noen ytterligere opplysninger du vil komme med i sakens anledning?