UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER:

Høst 2020

FORFATTER:

Magnus Wølner

VEILEDER:

Sissel Haugdal Jore

TITTEL PÅ MASTEROPPGAVE:

Hvordan benytter universiteter og høyskoler risikoanalyser som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser?

EMNEORD/STIKKORD:

Risikoanalyse, risikoanalysemetodikk, beslutningsstøtte, safety, security, NS 5814, NS 5832, usikkerhet.

SIDETALL:

78 (inkludert litteraturliste og vedlegg)

Bærum 16.12.20

Sammendrag

Universitets og høyskolesektoren (UH-sektoren) i Norge får føringer fra kunnskapsdepartementet for hvordan arbeidet med samfunnssikkerhet og beredskap skal prioriteres, og herunder bruk av risikoanalyser som verktøy (Kunnskapsdepartementet, 2019). Studien har til hensikt å vurdere hvordan UH-sektoren benytter risikoanalyser i arbeidet med å beskytte seg mot uønskede tilsiktede hendelser. For å besvare problemstillingen er det etablert forskningsspørsmål som dekker risikoanalysemetodikk sett opp mot anbefalinger i teoretisk bidrag, vurdering av om det skilles mellom safety og security i prosessen, samt om metodikkene fungerer forskjellig i forhold til det å støtte beslutninger. Det er benyttet kvalitativ metode og foretatt semistrukturerte intervjuer av ti informanter, der alle har stilling og ansvar innenfor sikkerhet og beredskap i UH-sektoren. Resultatene ble drøftet opp mot utvalgt teori.

Studien viser at UH-sektoren de siste årene har økt sitt fokus på uønskede tilsiktede hendelser, og det gjennomføres risikoanalyser i dette arbeidet. Risikoanalysene blir riktignok primært brukt for å utarbeide beredskapsplaner, og inngår i liten grad som beslutningsstøtte opp mot tiltak eller handlingsplaner. Analysene er med det lite brukt som underlag for konkrete sannsynlighets eller konsekvensreduserende tiltak. I forhold til valg av metodikk opp mot tilsiktede uønskede hendelser er det en fordeling der ca. halvparten benytter tofaktormodellen, og den resterende halvparten trefaktormodellen. Det varierer i hvilken grad dette er et bevisst valg. Hvilken metodikk og definisjon som legges til grunn er av betydning for kvaliteten i risikovurderingen, og studien viser at det er store skiller i sektoren hva gjelder kompetanse om både vurdering og bruk av risikoanalysemetodikk. Det mangler også kompetanse og fokus på at vurdering av usikkerhet bør inngå i analysene. Større forståelse for og bevissthet om begrepet usikkerhet vil gjøre sektoren i bedre stand til å vurdere fremtidige hendelser og scenarier, der også overraskende og nye trusler kan forekomme. sektoren bør for øvrig ha større fokus på hva som er formålet med risikoanalysene, da det vil sikre et bedre samspill og forståelse mellom beslutningstaker og de som gjennomfører analysene. Det vil også bidra til en mer effektiv risikoanalyseprosess.

Videre viser studien at det ikke foreligger noe organisatorisk skille mellom safety og security, samt at sektoren i stor grad benytter samme metodikk for risikoanalyser av begge områdene.

De to metodikkene har hver sine styrker og svakheter, og ut ifra en totalvurdering har de relativt lik funksjon i forhold til det å støtte beslutninger. Safety metodikk med tilhørende bruk av matrise er enkel og kjent for mange fra tidligere, men får i mindre grad frem de bakenforliggende vurderingene. Security metodikk får til gjengjeld i større grad fram disse vurderingene, men krever samtidig mer kunnskap og erfaring i tillegg til at den ofte er ukjent for beslutningstakerne. Det fremkommer at valg av metodikk i seg selv ikke er det viktigste, men at risikoanalyseprosessen legger grunnlaget for god beslutningsstøtte. Det er en pågående revisjon av Norsk standard 5814 (NS 5814) og denne vil kunne være et viktig bidrag til at UH-sektoren kan vurdere både safety og security hendelser ved bruk av samme metodikk. Det vil kunne styrke sektorens evne til å arbeide enhetlig i arbeidet med samfunnssikkerhet og beredskap.

Det er ulik praksis knyttet til hvordan sektoren dokumenterer og rapporterer de analysene som blir gjennomført. Risikoanalysene bør fremstilles i en helhetlig rapport der også fremgangsmåte, bakgrunnskunnskap og metodikk beskrives. UH-sektoren bør i tillegg til at beredskapsplaner oppdateres, også benytte risikoanalysene som beslutningsstøtte, for å vurdere sannsynlighets- og konsekvensreduserende tiltak opp mot de uønskede tilsiktede hendelsene som blir identifisert. Det at analysene faktisk benyttes som grunnlag for konkret oppfølging i sektoren, må kunne adresseres som det viktigste forbedringspunktet som fremkommer i studien.

Forord

Denne oppgaven setter et endelig punktum for min videreutdanning innen risikostyring og sikkerhetsledelse ved Universitet i Stavanger. Jeg ble i 2018 inspirert av en tidligere kollega til å begi meg ut på denne mastergraden, og det valget har jeg ikke angret på. Etter 11 år i politiet hvorav ni av dem i full turnus, begynte jeg å bli klar for nye utfordringer. De ulike kursene ved UIS har gitt meg solid og relevant faglig påfyll, og har vært et viktig bidrag til at jeg har kunnet begynne i stillingen som ansvarlig for sikkerhet og beredskap ved Handelshøyskolen BI.

Jeg ønsker å takke min arbeidsgiver for økonomisk støtte og fleksible tilpasninger som har gjort det mulig å fullføre dette prosjektet. Jeg har ervervet meg kunnskap som arbeidsgiver i stor grad vil dra nytte av. Min veileder Sissel Haugdal Jore fortjener også en stor takk, da hun har bidratt med viktige innspill som har styrket kvaliteten i prosjektet.

Sist men ikke minst vil jeg takke min flotte kone og nå tobarnsmor Charlotte, som har måttet gi mye av seg selv når jeg har lukket meg inne for å skrive. Det har vært krevende tider med håndtering av pandemi i stillingen på BI, fødsel i august, pappapermisjon og flytting til ny bolig der det er avdekket vesentlige mangler. Med masteroppgave på toppen av dette vil 2020 bli et år jeg sent vil glemme. Jeg er like fullt stolt over nivået på produktet jeg nå leverer, samtidig som jeg føler at jeg har vært til stede for familien min på en god måte.

Innhold

Figurer og tabeller

1.0 Innledning

Å beskytte bygninger og infrastruktur mot security hendelser som terrorisme og andre villede ondsinnede handlinger, har i etterkant av større terrorangrep i flere vestlige land fått et stadig større fokus. Det er sannsynlig at tilsvarende angrep også vil kunne skje i fremtiden (Hegghammer, 2016). I Norge har hendelsene 22. juli 2011 og angrepet i In Amenas i 2013 satt beskyttelse mot slike ondsinnede handlinger på agendaen (Jore & Egeli, 2015, s. 808). I etterkant av slike hendelser har man sett en økning i risikoerkjennelse, og bruken av risikoanalyser inngår som en sentral del i arbeidet med å forebygge uønskede tilsiktede hendelser (Albrechtsen et al., 2017). Risikoanalysene fremstår i denne sammenheng som et nyttig verktøy (Jore et al., 2018).

I Norge fremkommer det av internkontrollforskriften § 5 jfr. § 1 at det stilles krav om at samtlige virksomheter gjennomfører systematiske tiltak, for bl.a. å forebygge uønskede tilsiktede hendelser. Det inkluderer naturligvis også norske høyskoler og universiteter, som også får klare føringer fra kunnskapsdepartementet (KD) for hvordan det skal fokuseres på samfunnssikkerhet og beredskap, og herunder bruk risikoanalyser som verktøy (KD, 2019). Dette arbeidet medfører riktignok noen utfordringer, og det foreligger ingen omforent praksis knyttet til gjennomføring av risikoanalyser opp mot tilsiktede uønskede hendelser. Risikovurderinger inngår som en viktig del av beslutningsstøtte i forhold til blant annet utforming av handlingsplaner og risikoreduserende tiltak.

1.1 Valg av tema for oppgaven

Forskeren er selv ansatt som ansvarlig for sikkerhet og beredskap ved Handelshøyskolen BI, og har med det både stor interesse for og nytte av denne studien. Forhåpentligvis vil den kunne bidra med viktige konklusjoner også i sektoren for øvrig. Risikoanalyse var tema for et av kursene i masterutdanningen i risikostyring og sikkerhetsledelse ved universitetet i Stavanger (UIS). I dette kurset var det mye fokus på at forståelse for risikobegrepet har betydning når man tar beslutninger, samt viktigheten av hvilke vurderinger og kunnskap som ligger til grunn for fremstilling av risikobildet. Som en del av stillingen ved BI deltok forskeren også på et kurs i sikringsrisikoanalyse metodikk i regi av direktoratet for samfunnssikkerhet og beredskap (DSB). Metodikken som her ble benyttet er noe annerledes enn den som ble presentert i forbindelse med det nevnte kurset ved UIS. Det fremkommer av

styringsdokument for arbeidet med samfunnssikkerhet og beredskap i kunnskapssektoren at risikoanalyser er et viktig verktøy, og at det er av stor betydning at hver enkelt virksomhet foretar egne analyser som er tilpasset eget studiested (KD, 2019, s. 19). Det fremkommer videre at det er viktig at risikoanalysene benyttes som beslutningsgrunnlag ovenfor hendelser som vurderes til risikonivået middels og høy, samt at de tiltak som iverksettes fremgår av en handlingsplan (KD, 2019, s. 19). Det som vekket interesse for studien er der det fremkommer at «*KD har inntrykk av at det er noe usikkerhet mht. hvordan den enkelte virksomhet kan lage en god og hensiktsmessig ROS-analyse*» (KD, 2019, s. 29). Riksrevisjonen har for øvrig nylig rettet kritikk mot sektoren der hovedfunnene er at flere av UH-virksomhetene ikke har gjennomført risikoanalyser, og at risikoer som er vurdert til å ha middels til høy risiko ikke følges opp med tiltak eller handlingsplan (2020).

Forskeren har med det fattet interesse for hvordan arbeidet knyttet til risikoanalyser opp mot særlig tilsiktede uønskede hendelser blir foretatt i UH-sektoren. Det fremkommer dessuten av samfunnssikkerhetsinstruksen at departementene jevnlig må gjennomføre risikoanalyser opp mot både tilsiktede og utilsiktede hendelser, hvilket forutsetter at også de underliggende virksomhetene må gjennomføre slike analyser (KD, 2019, s. 29). Interessen for den eventuelle usikkerheten rundt valg av metodikk for risikoanalyser, samt hvordan disse blir benyttet som beslutningsstøtte for å iverksette tiltak, danner med det bakgrunnen for valg av oppgave. Tema for oppgaven er derfor hvordan universiteter og høyskoler i Norge benytter risikoanalyser for å beskytte seg mot uønskede tilsiktede hendelser.

1.2 Problemstilling og hensikt med studien

For å undersøke hvordan universiteter og høyskoler i Norge benytter risikoanalyser for å beskytte seg mot uønskede tilsiktede hendelser ble følgende problemstilling valgt:

- Hvordan benytter universiteter og høyskoler risikoanalyser som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser?

Med denne problemstillingen vil en belyse hvordan risikoanalysene blir brukt som beslutningsstøtte for videre tiltak og handlingsplan. Som en kommer tilbake til senere i studien er selve formålet med analysene at de skal bidra som beslutningsstøtte. Ordlyden i

problemstillingen som går på «hvordan benytter» innebærer at det må besvares hvordan disse analysene faktisk blir brukt for å sikre seg mot tilsiktede uønskede hendelser.

For å besvare problemstillingen på en dekkende måte ble følgende forskningsspørsmål utviklet:

1. Hvordan samsvarer valg av risikoanalysemetodikk i sektoren med anbefalinger i teoretiske bidrag?

Med dette forskningsspørsmålet vil en kartlegge hvilken metodikk universiteter og høyskoler i Norge benytter i risikoanalyser opp mot tilsiktede uønskede hendelser. Det vil i tillegg belyse hvorvidt studiestedene har et bevisst forhold til hvorfor en gitt metodikk foretrekkes. Slik spørsmålet lyder vil det bli vurdert om valgt metodikk har likheter med det en kan se på som anbefalt metodikk i et teoretisk perspektiv.

2. Skilles det mellom safety- og security hendelser i forhold til valg av metodikk?

Med dette forskningsspørsmålet vil en belyse om virksomhetene i sitt arbeide skiller mellom safety og security, samt om det her benyttes ulike metodikker opp mot de to områdene. Problemstillingen retter seg mot tilsiktede uønskede hendelser og således security, og en avklaring av om det foreligger et skille eller ikke vil være av betydning for å belyse hvilken metodikk som benyttes.

3. Fungerer metodikk opp mot safety og security forskjellig i forhold til det å støtte beslutninger?

Med dette forskningsspørsmålet vil en belyse om metodikken innenfor security fungerer på en annen måte enn metodikken innenfor safety, i forhold til det å ha funksjon som beslutningsstøtte. Slik problemstillingen lyder vil oppgaven undersøke hvordan risikoanalyser benyttes som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser, og dette siste forskningsspørsmålet vil med det være viktig for å vurdere om ulik metodikk har betydning for denne funksjonen.

Som nevnt er det økende fokus på det å bruke risikoanalyser som et ledd i det å beskytte seg mot tilsiktede uønskede hendelser, og studien er med det relevant. Det er også vist til at det er et krav at virksomhetene som er underlagt kunnskapsdepartementet gjennomfører slike. Hensikten med studien er med det også å belyse hvorvidt slike analyser blir gjennomført fordi

det blir stilt som et krav, eller om det i tillegg faktisk blir benyttet som beslutningsstøtte for konkrete tiltak og handlingsplaner. Forhåpentligvis vil studien være et viktig bidrag til bevisstgjøring rundt hvordan risikoanalysene benyttes opp mot arbeidet med sikkerhet og beredskap i sektoren, særlig når det gjelder tilsiktede uønskede hendelser. Resultatet av studien vil trolig heller ikke være unikt for UH-sektoren, men vil være relevant og av interesse for andre som jobber med sikkerhet og beredskap.

1.3 Oppgavens oppbygning

Oppgaven er bygd opp slik at det etter innledningen redegjøres for UH-sektoren i Norge i kapittel 2. Dette gjøres for å sette leseren inn i riktig kontekst ettersom studien retter seg mot denne sektoren. I kapittel 3 redegjøres det for utvalgt og relevant teori som er avgjørende for å kunne besvare problemstillingen. Videre i kapittel 4 blir forskningsdesign og valg av metode fremlagt. Det innebærer også refleksjon fra forskeren over de vurderinger som er gjort knyttet til kvaliteten av studien. Resultater som fremkommer i de gjennomførte intervjuene blir formidlet i kapittel 5. Kapittel 6 omfatter diskusjon der empiri og teori drøftes opp mot hverandre, før det trekkes konklusjon av problemstillingen i kapittel 7.

1.4 Avgrensning

For å besvare problemstillingen så presist som mulig er det avgjørende å foreta noen avgrensninger. Et område som har vært gjenstand for mye debatt er hvorvidt sannsynlighet bør inngå eksplisitt i risikoanalysene. Dette er et stort og omfattende tema som kunne vært gjenstand for problemstilling og oppgave i seg selv. Studien vil derfor ikke gå i dybden på dette temaet, men de mest sentrale momentene rundt bruk av sannsynlighet og usikkerhet blir trukket fram i teorien og andre deler av oppgaven. Det vil med bakgrunn i valgt problemstilling være unaturlig å styre helt unna sannsynlighetsvurderingen, men denne er altså ikke hovedfokus for oppgaven og det er nødvendig å gjøre en avgrensning rundt dette.

De to standardene for risikovurdering NS 5814 og NS 5832 blir trukket frem i oppgaven. Det gjøres oppmerksom på at NS 5814 er under revidering, med den hensikt å vurdere hvordan både tilsiktede og utilsiktede hendelser kan vurderes under samme standard (Standard Norge, 2020). Dette er en pågående prosess der status (november 2020) er at revisjonen har vært ute

på høring, og komitéen er nå i ferd med å implementere høringsinnspillene. Revideringen er relevant å trekke fram med tanke på problemstillingen, men det vil ikke bli redegjort for denne i sin helhet ettersom dette arbeidet ikke er ferdigstilt. Det er riktig nok viktig å trekke dette frem slik at leseren er klar over arbeidet som pågår knyttet til dette.

Videre vil ikke forskerens egen virksomhet utgjøre en del av empirien i studien. Det er vurdert at det er fornuftig å holde denne utenfor da det kan bli for nært opp mot egne oppgaver i virksomheten, samt at Handelshøyskolen BI er en privat stiftelse og dermed ikke får direkte pålegg av KD om å gjennomføre risikoanalyser opp mot tilsiktede uønskede hendelser. Føringer fra KD skilles her mellom «bør» for de private og «skal» for de virksomhetene som er direkte underlagt departementet.

2.0 Universitets- og høyskolesektoren

En vil i denne delen av besvarelsen redegjøre for universitets- og høyskolesektoren i Norge (UH-sektoren), i det studien omfattes av denne. Dette gjøres for at leseren skal forstå hvilken kontekst som ligger til grunn.

Barnehager, grunnskole, kulturskole, videregående opplæring, fagskoleutdanning, høyere utdanning og voksnes læring og kompetansepolitikk utgjør KD sitt ansvarsområde. I tillegg har KD ansvaret for forskning og integrering. Universiteter og høyskoler inngår som KD sine underliggende etater, og Norge har i dag ti universiteter, seks høyskoler og fem vitenskapelige høyskoler med statlig eierskap. Det er også flere private høyere utdanningsinstitusjoner der 17 av disse mottar statlig tilskudd (KD, 2014). Politikkområdet til KD omfatter med det svært ulike virksomheter både i størrelse, oppgaver, eierskap og tilknytningsform til departementet, samt at det omfatter en stor del av befolkningen (KD, 2019, s. 4).

2.1 Samfunnssikkerhet og beredskap i Kunnskapsdepartementets sektor

I Norge har samtlige departementer ansvar for samfunnssikkerhet og beredskap innenfor egen sektor (KD, 2019). For UH-sektoren og øvrige underliggende etater tilligger det overordnede

ansvaret for dette dermed KD. På nettsidene til KD fremkommer det hvilke mål de har for arbeidet opp mot samfunnssikkerhet og beredskap:

> *«Kunnskapsdepartementets overordnede mål for arbeidet med samfunnssikkerhet og beredskap er å forebygge uønskede hendelser, minske konsekvensene av de hendelsene som likevel oppstår og være forberedt på å håndtere alle typer kriser. For at vi skal lykkes med å forvalte dette ansvaret må alle i sektoren være seg sitt ansvar bevisst og arbeide helhetlig, systematisk og kunnskapsbasert med samfunnssikkerhet, basert på et system for risikostyring»* (2020).

Styringsdokument for arbeidet med samfunnssikkerhet i kunnskapsdepartementets sektor er opprettet for å sikre en grundig og regelmessig tilnærming til arbeidet. Styringsdokumentet gjelder for alle aktører og nivåer i sektoren og tydeliggjør ansvarsforhold, tiltak og KD sin oppfølging av arbeidet med samfunnssikkerhet og beredskap. De krav og anbefalinger som fremkommer må tilpasses hver enkelt virksomhet ut ifra styringslinje og tilknytningsform (KD, 2020).

2.2 Risikoanalyser i kunnskapssektoren

Det fremkommer av samfunnssikkerhetsinstruksen at hvert departement jevnlig må oppdatere risikoanalyser av egen sektor, og på bakgrunn av denne iverksette nødvendige tiltak for å redusere risikoen (2017). KDs risikoanalyse av sektoren ligger tilgjengelig på regjeringen sine nettsider. I analysen fremkommer de farer og trusler som er aktuelle, samt at det gis anbefalinger til tiltak som nevnt. Analysen viser et bredt spekter av hendelser, og det er gjerne knyttet til hendelser der mange mennesker er samlet i et begrenset område. Scenariene tar utgangspunkt i krisescenariene som direktoratet for samfunnssikkerhet og beredskap (DSB) la fram i 2015, og i styringsdokumentet beskrives de uønskede hendelsene skoleskyting, pandemi, cyberangrep og hybride trusler. Det fremkommer at dette er scenarioer som virksomhetene kan vurdere å ta inn i egen risikoanalyse i tillegg til eventuelt andre egne scenarier (KD, 2019, s. 16).

I kapittel 7 i styringsdokumentet tydeliggjøres det at de statlige virksomhetene bl.a. skal gjennomføre risikoanalyser knyttet til samfunnssikkerhet. Disse skal utarbeides i en helhetlig

rapport der bl.a. fremgangsmåte og metodikk beskrives. Resultatene fra analysene skal særlig føre til tiltak dersom risikoen vurderes til middels og høy. En handlingsplan er her å foretrekke slik at tiltakene blir synliggjort (KD, 2019, s. 19). De virksomhetene som ikke er direkte underlagt KD oppfordres til det samme. Målet med analysene er at de uønskede hendelsene som kan inntreffe blir identifisert og at tilhørende risiko vurderes for disse, samt at både sannsynlighets- og konsekvensreduserende tiltak fremkommer (KD, 2019, s. 18).

Hver enkelt virksomhet må altså gjennomføre egne risikoanalyser og disse må være tilpasset egen virksomhet hva gjelder størrelse og særpreg. KD anbefaler at risikoanalysene sees i sammenheng med analyser av bl.a. HMS, slik at arbeidet med samfunnssikkerhet blir innarbeidet i den helhetlige virksomhetsstyringen. Samtidig anbefales det at virksomhetene tar scenarioene som DSB beskriver som utgangspunkt. Disse er av omfattende karakter og vil ramme store deler av samfunnet, hvilket innebærer at de er svært aktuelle også for KD sin sektor (KD, 2019, s. 19).

Til bruk i arbeidet med risikoanalyser presenteres både to- og trefaktormodellen i styringsdokumentet som egnet metodikk. Det vil bli redegjort for de to metodikkene i denne studien i kapittel 3. Det følger med en veileder for gjennomføring av risikoanalyser som vedlegg til styringsdokumentet. Her trekkes risikomatrisen fram som et eksempel for å fremstille risiko som en sammenstilling av sannsynlighet og konsekvens (KD, 2019, s. 35).

2.3 Beredskapsrådet

For å styrke arbeidet med samfunnssikkerhet og beredskap i UH-sektoren opprettet KD råd for samfunnssikkerhet og beredskap i 2017. Både statlige universiteter og private høyskoler er representert, samt fagskoler, studentsamskipnader og folkehøyskoler. Den viktigste oppgaven som tilligger rådet er å tilstrebe en enhetlig og hensiktsmessig tilnærming i sektoren innenfor samfunnssikkerhet og beredskap. Det vesentlige er i den forbindelse at virksomhetene har tett dialog om beste praksis og de erfaringer som gjøres. Rådet trekker fram en del sentrale temaer det bør jobbes med, som bl.a. risikoanalyser, beredskapsplaner og øvelser. Rådet har 14 medlemmer og har jevnlige møter for å styrke arbeidet som nevnt (KD, 2020).

3.0 Teori

En vil i denne delen av studien redegjøre for utvalgt og relevant teori. Der det er relevant vil det bli trukket eksempler opp mot UH-sektoren.

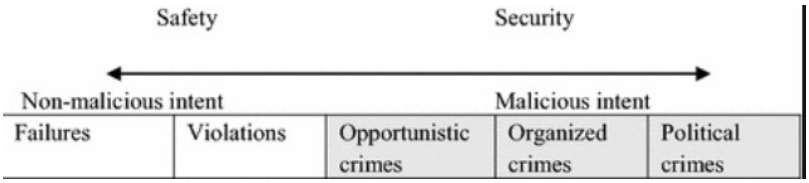
3.1 Safety vs security

I Norge er vi kjent med å benytte ett ord for sikkerhet, men på engelsk brukes gjerne både safety og security. En vil videre i besvarelsen legge den engelske forståelsen til grunn for å kunne skille de to begrepene. Safety forstås som handlinger og hendelser som ikke er planlagt, som f.eks. ulykker, naturkatastrofer og uhell m.m. Innen security er handlingene derimot tilsiktede og uønskede, som f.eks. terror, sabotasje, tyverier m.m. Det innebærer at en angriper vil vurdere både konsekvensene og muligheten for å oppnå den effekten en ønsker (Engen et al., 2016, s. 87). En kan også si at security omhandler ondsinnede handlinger der trusselaktøren vil være strategisk ved bevisst å unngå de barrierer som skal hindre et angrep (Smith & Brooks, 2012, s. 9). Som eksempel fra UH-sektoren kan en trekke fram en bussulykke med studenter som en safety hendelse, mens et bevisst angrep mot studiestedets datasystem vil regnes som security.

På bakgrunn av tilgjengelig forskning kan safety i større grad sees på som en etablert vitenskap enn det security er i dag (Jore, 2019, s. 2). Økt fokus og interesse for å beskytte oss mot terrorisme, spionasje, cyberangrep og andre villede ondsinnede handlinger, har riktignok medført økt oppmerksomhet for security som forskningsområde. Det finnes en rekke definisjoner av security, og det er ingen omforent enighet om hvilken som er best egnet. Tidligere ble begrepet forstått som noe som primært var tilknyttet forsvaret og politiet, men det har nå fått en bredere forankring i ulike sektorer i samfunnet. Security trusler kan forekomme på mange måter og nivåer, og det gjelder ikke bare terrorisme som ofte blir nevnt i den sammenheng. Security omfatter også mer tradisjonell kriminalitet som innbrudd, tyveri og skadeverk (Jore, 2019, s. 7).

Flere forskere har tatt til orde for at det er nødvendig å skille security og safety fra hverandre når det kommer til arbeidet med risiko og krisehåndtering. De relaterer beskyttelse mot terrorisme og andre villede handlinger til security, og beskyttelse fra ikke-villede handlinger til safety (Boholm et al., 2016). Ofte er det begrepet intensjon forskere bruker for å skille

security fra safety. Flere studier innen organisatorisk sikkerhet og ulykker trekker riktignok fram det at intensjon også kan være til stede innenfor safety. Ulykker forekommer sjelden tilfeldig, men som et resultat av for lite fokus på sikkerhet. Menneskelig intensjon kan ha betydning for årsaken til at ulykker finner sted (Perrow, 1999; Reason, 1990). Eksempelvis kan en virksomhet med viten og vilje ta snarveier for å oppnå økonomisk gevinst, hvilket medfører at ulykker oppstår som følge av regelbrudd. Intensjon spiller med det en rolle innenfor både safety og security, og et mer presist skille mellom disse vil være at trusselaktøren innenfor security har en ondsinnet vilje (Jore, 2019, s. 15). Figuren under illustrerer hvordan feil og regelbrudd kan innebære intensjon, men at safety og security skilles ved det som kalles ondsinnet vilje.



Figur 1: Skille mellom safety og security (Jore, 2019, s. 6).

Et annet skille er at innen safety så kan en si at det er akseptert at det å produsere varer og tjenester innebærer et gitt nivå av risiko. Det medfører større kunnskap og tilgang på historiske data som kan brukes i risikoanalyser og risikostyringen av virksomheten. Det gjør at en har bedre forutsetninger for å vite hvilke tiltak man kan iverksette for å redusere risikoen til en gitt aktivitet. Innenfor security er derimot ikke risikoene nødvendigvis knyttet til produksjonen. Det innebærer svært begrenset tilgang på data, samt stor usikkerhet knyttet til hvilken risiko eller trussel som kan bli den neste. Det vil også være langt mer krevende å vurdere aktuelle scenarioer, ettersom virksomhetene har langt mindre kunnskap om disse sammenliknet med safety. Enhver risikovurdering innebærer usikkerhet, men denne vil være større innenfor security knyttet til hvem, hva, hvor, hvordan og når kommer det neste angrepet (S. Jore, 2019, s. 8). Som eksempel fra sektoren kan en trekke fram at en i de fleste utdanninger har gode muligheter for å risikovurdere hvilke ulykker som kan finne sted, men når det gjelder security kan et studiested bli valgt som mål mer tilfeldig. Angriperen ønsker kanskje ikke å ramme sektoren i seg selv, men samfunnet i sin helhet.

Kvantitative metoder har i større grad blitt benyttet innen safety, ettersom det er vanskelig å gjøre kvantitative beregninger innen security. Aven & Renn forklarer her at kvalitative metoder i kombinasjon med vurderinger fra eksperter ofte vil være å foretrekke for å beskrive og risikovurdere security hendelser (2009). Bruk av kvalitative tilnærminger er hensiktsmessig ettersom mange security hendelser gjerne aldri eller sjelden forekommer. Det vil like fullt være en del security hendelser hvor en har god tilgang på data, som f.eks. innbrudd, tyverier og cyberkriminalitet. Ettersom truslene i realiteten kommer fra utenfor virksomheten vil risikovurderingene i stor grad basere seg på trusselvurderinger som kommer fra myndighetsnivå. De vil med det ikke være tilpasset den enkelte virksomhet, men på et generelt nivå (Jore, 2019, s. 8). Figuren under viser en liste over de mest sentrale forskjellene mellom security og safety. Denne er ikke uttømmende.

The nature of the risk	Safety Risk related to production and profit, often well-known risks	Security Strategic humans, dynamic threat, often rooted in causes outside the organization
Type of intent	Non-malicious intent	Intentional, malicious
Historical data	Historical data often exist that are applicable for prediction of future trends	Data sources problematic, historic trends not always good predictors of the future
Types of risk assessment	Quantitative probabilities and frequencies of safety-related risks are often utilized	Qualitative (expert-opinion based) likelihood of security-related risks
Possibility for mitigation	Organization has knowledge about possible risk scenarios and measures	Threats and measures may be symbolic, organizations often lack means

Figur 2: Forskjeller mellom security og safety (Jore, 2019, s. 9).

Forskjellene mellom de to områdene medfører ulik bruk av verktøy og metoder innenfor bl.a. risikoanalyser og standarder. Å vurdere en security trussel innebærer noe annet enn det å vurdere en safety trussel ettersom truslene som skal vurderes i stor grad er ukjente, samt at de innebærer et bredt spekter av scenarioer. Innen safety er truslene i større grad kjent i tillegg til at antall mulige scenarioer er mer begrenset (Kriaa et al., 2015). Til tross for den økende interessen og flere standarder og retningslinjer innen security, så foreligger det ingen omforent beste praksis innen dette feltet som angår bl.a. risikoanalysemetodikk. Tilnærmingen varierer med det mellom både de ulike landene og i ulike sektorer (Maal et al., 2017). Det er pågående debatt rundt hvorvidt security er så særegent at det krever egen

tilnærming, eller om dette i større grad kan baseres på kunnskap fra safety feltet (Amundrud et al., 2017; Jore & Egeli, 2015).

De to feltene har også flere likheter, bl.a. når det gjelder risikoanalysemetodikk, ettersom begge analyserer trusler, sårbarheter, konsekvenser og sannsynligheten for at hendelsen skal finne sted (Piètre-Cambacédès & Bouissou, 2013). Videre spiller også menneskelige handlinger en viktig rolle innenfor både safety og security, og konsekvensene kan bli like. Eksempelvis vil en brann på et universitet forårsaket av et uhell kunne innebære de samme konsekvensene som om brannen bevisst var påsatt. Tiltak som iverksettes innenfor det ene feltet kan påvirke sikkerheten knyttet til det andre, og en bør med det se safety og security i forhold til hverandre (Jore, 2019, s. 11). Som eksempel kan det å innføre security tiltak rundt et studiested medføre hindringer for en ambulanse som skal rykke ut til en mer ordinær safety hendelse som f.eks. hjertestans.

Jore forklarer at de fleste definisjoner som finnes av security bygger på å få fram forskjellen fra safety, samt hva security ikke er (2019, s. 12). Jore definerer security på følgende måte:

> *"Security can be defined as the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking.*
>
> *Security risk management includes assessing and reducing the likelihood and consequences of possible attacks with various types of risk-reducing measures, for example, through critical infrastructure protection and by building organizational and societal resilience"* (2019, s. 15).

Det vil senere i oppgaven bli redegjort for de to risikoanalysemetodikkene to- og trefaktormodellen, men det kan i denne sammenheng nevnes at det største skillet mellom de to metodikkene går på hvordan bruken av sannsynlighet inngår eksplisitt eller ikke. Trefaktormodellen skiller seg her ut ved at den ikke eksplisitt uttrykker sannsynligheten for et angrep, slik man ofte har gjort ved mer tradisjonell metodikk innenfor safety. En kan med det si at stridens kjerne står rundt bruken av sannsynlighet eller ikke når det gjelder villede

ondsinnede handlinger (Jore & Egeli, 2015, s. 808). Jore & Egeli har i sine studier av ulike interessenter i norsk petroleumssektor undersøkt behovet for forskjellig risikoanalysemetodikk når det gjelder analyser opp mot safety og security, samt i hvilken grad sannsynlighet bør inngå som vurdering i disse (2015, s. 810). Funn i studien viser at eksperter innen safety hevder at en også innen security kan benytte sannsynlighet, så lenge disse innebærer subjektive vurderinger basert på tilgjengelig bakgrunnskunnskap. De hevder videre at det å velge helt forskjellig risikoanalysemetodikk innenfor safety og security vil innebære en risikostyring som ikke gir en helhetlig tilnærming. Sett fra security sitt ståsted er det argumenter for at bruk av sannsynlighet innenfor dette feltet ikke er egnet, ettersom trusselaktøren vil ha intensjon og kapasitet. Trusselaktøren kan med det være fleksibel og tilpasse angrepet slik en vil. Enkelte vektlegger med det at de to områdene safety og security er så forskjellige at behovet for ulik risikoanalysemetodikk er tilstede (Jore & Egeli, 2015, s. 807). Figuren under oppsummerer de viktigste funnene i studien som her ble trukket fram.

Research themes	Example of questions	Results
Is there a need for specific methodology for security risk management	Do you or your company use the same risk analysis methodology for safety and security risk analysis? Is there a need for a risk analysis methodology designed exclusively for security?	9 out of 15 informants are in favour of specific risk management methodology for the area of security. All informants working exclusively with security supported this argument.
Are probabilities applicable in security risk analysis	How do you and your company define security risk? Do you use probability in the analysis? What is your opinion on the use of probabilities in security risk management?	8 out of 15 informants claim that probabilities cannot be used in security risk analysis. All informants working exclusively with security supported this argument.

Figur 3: Oppsummering av funnene i studien til Jore & Egeli (Jore & Egeli, 2015, s. 810).

Jore & Egeli konkluderer i sin studie med at det på tross av at metodikkene er ulike så vil de innebære en form for vurdering av sannsynlighet. De hevder med det at tilnærmingene innenfor security må være kompatibel med standarden for risikostyring innenfor safety, og at de vurderingene som foretas av sannsynlighet må synliggjøres. Sannsynlighetsvurdering må være bygget på et subjektivt og kunnskapsbasert perspektiv. Videre forklarer Jore & Egeli at det uavhengig av hvilken metodikk som velges, så er det å foreta risikoanalyser opp mot security meget krevende (2015, s. 807).

3.3 Hva er risiko?

Det finnes en rekke ulike definisjoner av risiko og vi kan alle ha ulik forståelse eller aksept for risiko. På fritiden vår finner enkelte glede i å kjøre på ski ned bratte fjell, mens andre er mer risikoaverse og oppsøker ikke slik risiko bevisst. Risiko kan dreie seg om ting som både er positivt og negativt. Denne studien dreier seg om tilsiktede uønskede handlinger og en kan med det forstå at vi forbinder dette med noe negativt. For å kartlegge og beskrive risiko er det av stor betydning for kvaliteten i risikovurderingen at en har klart for seg hvilken definisjon som legges til grunn. Risikoen skal uttrykkes og presenteres for både beslutningstakere og ulike stakeholders, og en bør ha felles forståelse av begrepet risiko for å kunne ta gode beslutninger (Aven, 2008, kapittel 1 og 2). Aven forklarer at risiko kan defineres på flere måter:

C x P (konsekvens multiplisert med sannsynlighet)

C, P (kombinasjon av konsekvens og tilhørende sannsynlighet)

C, U (kombinasjonen av mulige fremtidige hendelser/konsekvenser og tilhørende usikkerhet)

(2008)

Definisjonen der risiko er produktet av sannsynlighet og konsekvens er en tradisjonelt mye brukt forståelse som legges til grunn (Engen et al., 2016, s. 78). Aven baserer sine lærebøker på definisjonen C, U der også bakgrunnskunnskapen inngår som et sentralt element. En kan benytte sannsynlighet for å beskrive hvor trolig det er at noe vil inntreffe med tilhørende konsekvenser, men her må bakgrunnskunnskapen og usikkerhet knyttet til dette kommuniseres (Aven, 2008, kapittel 2). Et klassisk eksempel er spillet der en får gevinst ut ifra hvilken verdi terningen viser. Dersom spilleren mangler bakgrunnskunnskap om terningen vil dette nærmest umuliggjøre en vurdering av sannsynligheten for å vinne.

I Norge har vi særlig to standarder som definerer risiko på noe ulike måter, henholdsvis Norsk standard (NS) 5814 og 5832. I NS 5814 defineres risiko som «*et uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse*» (Standard Norge, 2008). Slik vi forstår dette utgjør risiko her kombinasjonen av sannsynlighet og konsekvens, og ordlyden uønsket hendelse viser at det innebærer noe negativt. En kan her merke seg at sannsynlighet

inngår eksplisitt. I NS 5832 er risiko definert som *«forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet ovenfor den spesifikke trusselen»* (Standard Norge, 2012). Her er sannsynligheten bevisst utelatt (Busmundrud et al., 2015, s. 15). En vil i forbindelse med redegjørelse av risikoanalysemetodikk senere i besvarelsen komme tilbake til definisjonene som de to standardene er bygget på.

3.4 Usikkerhet

Slik det fremkommer i kapittel 3.3 er det usikkerhet knyttet til det å vurdere fremtidige hendelser, og det å inkludere usikkerhet inn i security planlegging er derfor viktig. I vurderingen av risiko er det naturlig å omtale eller å stille spørsmål om hvor stor eller høy denne er. Sannsynlighet er her en måte å uttrykke usikkerheten på, hvilket betyr at vi gjør en vurdering av hvorvidt vi tror at et scenario faktisk kan skje (Aven, 2015, s. 42). Det er her viktig å være klar over begrensningene knyttet til dette, da beregningene gjøres med bakgrunn i en kunnskap hvor det ligger en rekke forutsetninger til grunn. Forutsetninger og bakgrunnskunnskap må fremkomme i risikoanalysene da de både kan inneholde feil og være basert på svært begrenset kunnskap (Aven, 2015, s. 43). Som eksempel opp mot UH-sektoren kan en vurdere sannsynligheten og tilhørende usikkerhet for en skoleskyting (PLIVO) som lav. Samtidig har man begrenset bakgrunnskunnskap fra Norge å vurdere dette på, og de forutsetninger som ligger til grunn bør med det fremkomme i analysen.

Aven understreker at det er viktig å være oppmerksom på at liten usikkerhet ikke nødvendigvis betyr liten risiko (2015, s. 44) . Dette kan illustreres slik det fremkommer i tabell 1 under ved at en ser for seg et scenario der en bare har to mulige utfall, i dette tilfellet 0 eller 1 omkomne. Slik det fremkommer har alternativ A og B ulik usikkerhetsfordeling, og en leser at A innebærer høyere usikkerhet enn B. Men når vi ser på risiko med sine to komponenter konsekvens og usikkerhet vil vi med sikkerhet vurdere alternativ B til å ha størst risiko.

Mulig utfall (antall omkomne)	Sannsynlighetsfordeling alternativ A	Sannsynlighetsfordeling alternativ B
0	0,5	0,001
1	0,5	0,999

Tabell 1: Sannsynlighetsfordeling alternativ A og B (Aven, 2015, s. 44).

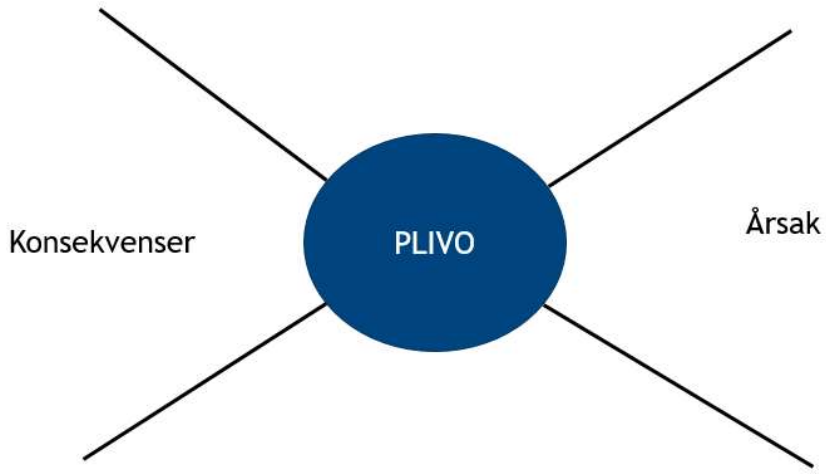
Usikkerhet er altså av betydning og det er de siste årene en rekke ulike perspektiver på risiko, der bruk av begrepet usikkerhet foretrekkes fremfor sannsynlighet. Aven forklarer at bakgrunnen for dette er at sannsynlighet må sees på som et verktøy for å beskrive usikkerheten, og at en ikke utelukkende kan basere seg på dette ene verktøyet (2014, s. 1). I de eldre perspektivene på risiko ble ikke det uforutsette og de potensielt større overraskelsene vektlagt, slik en i dag gjør ved å fokusere på bakgrunnskunnskap. Ved ensidig fokus på sannsynlighet vil en utelukke viktige aspekter ved risiko og usikkerhet. Ved igjen å se hen til scenarioet med skoleskyting vil en kunne si at det er uheldig dersom man legger for stor vekt på sannsynlighet, og hevder at det er lav sannsynlighet for at slikt skal skje i Norge. Konsekvensene vil like fullt være meget alvorlig, og med begrenset bakgrunnskunnskap kan en argumentere for at tilhørende usikkerhet er høy. For sektoren er dette relevant ved at en bør ha et videre perspektiv på risiko og med det går utover det å beregne og vurdere sannsynligheter.

Et viktig aspekt for å vurdere risikoen er nettopp styrken på bakgrunnskunnskapen. Som eksempel kan en trekke fram tilfeller der en har samme beregning av sannsynlighet for to situasjoner, men der bakgrunnskunnskapen som sannsynlighetsvurderingen bygger på er vidt forskjellig. En svak bakgrunnskunnskap tilsier mer usikkerhet enn høy grad av kunnskap. Om dataene som ligger til grunn er relevant for problemstillingen vil naturligvis også påvirke usikkerheten. Det vil derfor være uheldig å kun ta beslutninger basert på vurderinger av sannsynligheter, ettersom bakgrunnskunnskapen vil kunne være ulik. Dessuten vil beregninger av sannsynlighet ofte være bygget på antagelser og vurderinger som en ikke ensidig matematisk kan si med sikkerhet er korrekt. Antagelser og forutsetninger som blir lagt til grunn vil ha stor påvirkning på beregning av sannsynligheten (Aven & Krohn, 2014, s. 1). For å unngå at en overser uforutsette og overraskende hendelser må en benytte seg av et bredere perspektiv enn utelukkende å forholde seg til sannsynligheter. Perspektivene der bakgrunnskunnskapen som foreligger vektlegges er et viktig bidrag for ikke å overse slike uforutsette hendelser (Aven & Krohn, 2014, s. 2). Mange eksperter innen security velger ikke å benytte sannsynlighet i vurderinger av risiko og sårbarhet, og argumenterer for at det ikke er egnet som beslutningsstøtte. Like fullt bør det for å kunne vurdere og prioritere ulike tiltak fremkomme en vurdering av sannsynligheter. Styrken på bakgrunnskunnskapen kan her vurderes kvalitativt og synliggjøres. Hvordan styrken på bakgrunnskunnskapen her vurderes er lite omtalt og vurdert når det gjelder security forhold (Askeland et al., 2017, s. 196).

For å supplere usikkerhetsvurderingen med en kvalitativ vurdering av styrken på bakgrunnskunnskapen, har Flage og Aven riktignok foreslått kriterier for hvilke momenter som her kan ligge til grunn for dette i risikovurderinger (Askeland et al., 2017, s. 197). Det vil ikke bli redegjort for disse kriteriene videre i oppgaven, men det kan nevnes at bakgrunnskunnskapen kan vurderes som enten lav, medium eller høy. Høy bakgrunnskunnskap vil med det innebære lav usikkerhet, og motsatt vil lav bakgrunnskunnskap føre til dertil høy usikkerhet (Askeland et al., 2017, s. 197). For UH-sektoren som skal vurdere risikoen for et bredt spekter av security hendelser, vil fokus på usikkerhet og bakgrunnskunnskap kunne utgjøre et viktig bidrag til å rangere risikoene med tilhørende tiltak.

3.5 Hva er en risikoanalyse?

Målet med en risikoanalyse er at den skal kartlegge og beskrive risiko. *«Vi snakker om at risikoanalysen skal presentere et risikobilde»* (Aven, 2008, s. 13). Aven viser her til bow-tie modellen for å illustrere dette risikobildet. I figur 4 under vises en bow-tie modell for en uønsket tilsiktet hendelse i form av en skoleskyting, også kjent som pågående livstruende vold (PLIVO). Den uønskede hendelsen fremkommer her i midten av figuren og en sentral del av risikoanalysen er at disse initierende hendelsene blir identifisert (Aven, 2008, s. 13). Til venstre fremkommer mulige årsaker, og til høyre konsekvensene av hendelsen. På begge sider vil det her kunne fremkomme både sannsynlighets- og konsekvensreduserende barrierer (Aven, 2008, s. 14). Ser vi hen til eksempelet med PLIVO som er relevant for UH-sektoren kan en tenke seg at en mulig årsak for en slik hendelse kan være radikalisering, samt at konsekvensene kan innebære titalls drepte mennesker. De ulike barrierene vil her være tiltak for å påvirke risikoen. En risikoanalyse vil med det ha som mål å beskrive hele eller deler av en bow-tie modell. Det finnes ulike metoder for hvordan en går fram for å gjøre dette, og det er av betydning hva resultatene av analysen er tenkt brukt til (Aven, 2008, s. 14).



Figur 4: Bow-tie modell for en PLIVO hendelse (Aven, 2008, s. 13).

3.5.1 Hensikt med risikoanalyser

Det er flere grunner til at en gjennomfører risikoanalyser, og som nevnt vil disse først og fremst ha som mål å presentere et risikobilde. Analysene vil også gi grunnlag for å sammenlikne forskjellige tiltak og deres påvirkning eller effekt på risikoen. Det vil også kunne fremkomme kritiske funksjoner eller aktiviteter som er av betydning (Aven, 2008, s. 15). En rekke virksomheter er underlagt strengt regelverk der gjennomføring av risikoanalyser er lovpålagt. Risikoanalyser gjennomføres med det av mange for å oppfylle de krav som er gitt av myndighetene (Aven, 2008, s. 16). Aven trekker her fram at det er uheldig dersom dette er motivasjonen i seg selv, ettersom det medfører at resultatene fra analysen ikke blir brukt i sin helhet (Aven, 2008, s. 16). «*Poenget med en risikoanalyse er å gi et underlag for å kunne ta gode beslutninger»* (Aven, 2008, s. 16). Å treffe beslutninger kan være krevende i det ulike hensyn mellom bl.a. økonomi og sikkerhet må veies opp mot hverandre. Virksomhetene i UH-sektoren vil som eksempel gjerne være bundet av stramme budsjetter, og trenger grunnlag for å vurdere hvilke sikkerhetstiltak de skal prioritere. Risikoanalysene vil her kunne være et viktig grunnlag for å komme fram til beslutninger som ivaretar denne balansen, samt sikrer at virksomhetens øvrige mål oppnås på best mulig måte (Aven, 2008, s. 16).

3.5.2 Risikoanalyseprosessen

Risikoanalyseprosessen blir som regel fremstilt ved de tre fasene planlegging (forberedelser), risikovurdering (gjennomføring) og risikohåndtering (bruk). I planleggingsfasen av risikoanalyser er det sentralt at man nøye vurderer hva som er formålet. Analysen skal bringe på banen ulike momenter som legges til grunn for beslutninger som skal tas, og mangel på avklaring av formålet vil ikke gi et godt beslutningsgrunnlag (Aven, 2008, s. 43). «*Hvordan analysen og dens resultater skal brukes i beslutningsprosessen må være tydelig*» (Aven, 2008, s. 45). Ser man hen til bow-tie modellen er det vesentlig at de som skal gjennomføre analysene og beslutningstaker/leder avklarer om analysen skal dekke hele eller deler av denne. Som eksempel kan det være at ledelsen ved en høyskole eller et universitet ønsker en risikoanalyse som beslutningsstøtte, for å vurdere hvilke sikringstiltak de bør iverksette for å redusere konsekvensene av en bilbombe utenfor deres lokaler. Poenget er her at beslutningstaker/ledelse må være tydelig på hva analysen skal belyse og hva det ønskes beslutningsstøtte til. Det har også betydning for hvilken metodikk som velges, samt hvordan arbeidet organiseres og hvilken ressursbruk det medfører (Aven, 2008, s. 44). Aven trekker her fram at erfaring viser at det brukes mest tid på fasen med selve risikovurderingen, og for lite til både planlegging og risikohåndteringen. Sistnevnte er den fasen der analysene faktisk tas i bruk som beslutningsstøtte. En fordeling der det brukes 1/3 av ressursene i hver av de tre fasene, vil slik Aven forklarer det gi en prosess som er bedre balansert (2008, s. 44).

Risikovurderingen består av risikoanalyse og risikoevaluering der resultatene fra risikoanalysen evalueres. Risikoanalyse + risikoevaluering= risikovurdering. I prosessen med en risikoanalyse vil det å identifisere mulige initierende hendelser være noe av det viktigste som gjøres. Aven trekker her fram at «*det du ikke har identifisert, kan du ikke håndtere*» (2008, s. 55). Av det kan vi forstå at det vil være vanskelig for universiteter og høyskoler å iverksette sannsynlighets- eller konsekvensreduserende tiltak opp mot uønskede hendelser som en ikke har identifisert. Videre består risikovurderingen av både årsaks- og konsekvensanalyse, og risikobildet presenteres med bakgrunn i dette (Aven, 2008, s. 57–59). Det finnes en rekke ulike måter risikoen kan presenteres på og risikomatrise er en av dem (Aven, 2008, s. 61–65). I risikoevalueringen vurderes det hvorvidt risikoen er for høy eller akseptabel m.m. (Aven, 2008, s. 67).

Det er risikoanalysen og diskusjonen knyttet til resultatene av disse, som skal gjøre at analytikerne kan presentere risikobildet. Ledere og beslutningstakere vil så bruke risikobildet som grunnlag for å håndtere risikoen. I denne fasen vil de ulike tiltakene og virkemidlene vurderes for enten å redusere, optimalisere, overføre eller beholde risiko (Aven, 2008, s. 20). De ulike tiltakene må vurderes opp mot både hvilke positive og negative effekter de kan innebære (Aven, 2008, s. 71). Det er mange ulike hensyn som må veies opp mot hverandre, bl.a. økonomi, overordnet strategi og ulike dilemmaer m.m. Aven understreker at analysene ikke gir beslutningen i seg selv, men gir et grunnlag for at beslutninger kan tas (Aven, 2008, s. 70).

3.5.3 Risikoanalysemetodikk

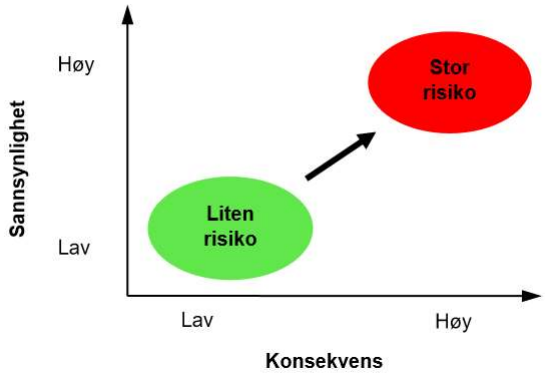
En vil i denne delen av besvarelsen redegjøre for de to risikoanalysemetodikkene to- og trefaktormodellen.

Tofaktormodellen

Forvarets forskningsinstitutt (FFI) har vurdert metodikkene to- og trefaktormodellen i forhold til risikovurderinger av tilsiktede uønskede hendelser (2015, s. 3). En vil komme tilbake til vurderingene de kom fram til, men tofaktormodellen blir her presentert med bakgrunn i NS 5814 og redegjørelsen fra FFI.

Tofaktormodellen er en metodikk som har sitt opphav i NS 5814 (Busmundrud et al., 2015, s. 3). Det vises til kapittel 3.3 der NS 5814 definerer risiko som et *«uttrykk for kombinasjonen av sannsynligheten for og konsekvensene av en uønsket hendelse»* (Standard Norge, 2008). FFI omtaler denne metodikken som sannsynlighet og konsekvens-tilnærmingen (Busmundrud et al., 2015, s. 9). Tofaktormodellen har lang tradisjon hva gjelder risikoanalyser av safety hendelser innen blant annet industrien, men man har sett en økning i bruken av denne metodikken også opp mot security (Busmundrud et al., 2015, s. 27). Figur 5 under viser hvordan risiko i denne metodikken utgjør funksjonen av sannsynlighet og konsekvens av en uønsket hendelse. En kan her se at lav sannsynlighet og lav konsekvens utgjør liten risiko. Samtidig vil det ved å se hen til denne metodikken medføre at hendelser med lav

sannsynlighet og høy konsekvens, vil kunne utgjøre samme risiko som en mindre alvorlig hendelse som kan skje oftere (Busmundrud et al., 2015, s. 27).



Figur 5: Sammenhengen mellom konsekvens, sannsynlighet og risiko (Busmundrud et al., 2015, s. 27).

Slik en forstår står sannsynlighetsbegrepet her relativt sentralt, og en vurdering av denne vil være av betydning. Statistikk og annen relevant data i forbindelse med cyberangrep ved et studiested vil som eksempel kunne utgjøre et viktig grunnlag for å vurdere sannsynligheten. Konsekvensene kan også vurderes ved bruk av samme tallmateriale, men samtidig kan det være vanskelig å vurdere hvilke indirekte konsekvenser som også kan oppstå. Når det gjelder tilsiktede uønskede handlinger vil kvantitativ vurdering av sannsynlighet være krevende og som regel uegnet. Det vil like fullt kunne gjøres gode kvalitative vurderinger av de ulike scenarioene (Busmundrud et al., 2015, s. 28).

FFI deler tofaktormetodikken inn i de fire fasene objektkartlegging/verdivurdering, trusselvurdering/scenariobeskrivelse, sårbarhetsvurdering og vurdering av risiko (Busmundrud et al., 2015, s. 28). Forsvarsbygg gjennomfører prosessen ved å nedsette en arbeidsgruppe på tre til seks personer, i tillegg til ulike fageksperter som velges ut ifra det område som skal analyseres. I fasen for objektkartlegging/verdivurdering kartlegges objektet i sin helhet, og her inngår elementer som bl.a. beliggenhet, bygningsmasse og infrastruktur. I verdivurderingen kartlegges virksomhetens verdier, og dette kan dreie seg om bl.a. sensitiv informasjon eller spesielle bygninger som er særlig viktig å beskytte (Busmundrud et al.,

2015, s. 28). For UH-sektoren kan dette være relevant i form av f.eks. bygninger eller lokaler, som huser viktig forskning eller sensitiv kjemisk prosessteknologi av stor betydning.

Videre vil det i fasen for trusselvurdering og scenariobeskrivelse bli identifisert hvilke aktuelle farer og uønskede hendelser som kan forekomme. En støtter seg her til ulike kilder og fagmiljøer for å kunne si noe om trusselen, og en kan her nevne bl.a. Politiets Sikkerhetstjeneste (PST), Norsk Sikkerhetsmyndighet (NSM) og etterretningstjenesten. Scenariobeskrivelsen tar utgangspunkt i trusselvurderingen og gir eksempler på hendelser som kan finne sted (Busmundrud et al., 2015, s. 29). I NS 5814 omtales dette som identifikasjon av farer og trusler (2008).

I fasen for sårbarhetsvurdering gjøres det en vurdering av hvorvidt en trusselaktør faktisk vil kunne ha muligheten til å gjennomføre en uønsket handling, og der ikke allerede etablerte tiltak er egnet til å stanse angrepet (Busmundrud et al., 2015, s. 29). Et viktig moment som her fremkommer er mulighet, og vil avhenge av trusselaktørens kapasitet i form av bl.a. trening, kunnskap og metode den eller de har tilgang til. De allerede etablerte sikringstiltak kan her vurderes ved å bruke tidsregnskapet. Hvor lenge vil f.eks. et gitt objekt klare å stå imot et angrep fra en gitt aktør (Busmundrud et al., 2015, s. 29). For UH-sektoren vil det være lite naturlig å snakke om å stå imot et angrep, men en vurdering av responstid fra nødetater kan være et fornuftig moment å vektlegge i sårbarhetsvurderingen.

Videre vil det i konsekvensvurderingen fremkomme hvilket utfall en ser for seg at et angrep vil få. Det legges da til grunn at eksisterende sikringstiltak ikke er gode nok eller er fraværende. «*Konsekvensen av en gjennomført handling uttrykkes da som funksjon av bortfall av objektets tilknyttede verdi*» (Busmundrud et al., 2015, s. 29). En kan her se for seg at ulike typer materiell blir ødelagt eller at liv og helse blir rammet, og det gjøres konsekvensvurdering av de ulike scenarioene (Busmundrud et al., 2015, s. 29).

I den siste fasen som er vurdering av risiko blir aktualiserte konsekvenser vurdert opp mot sannsynlighet. Berørte verdier utgjør en del av konsekvensene og trusler og sårbarheter inngår

i sannsynlighetsvurderingen. Det er her kvalitative vurderinger som ligger til grunn ettersom trusselaktørens intensjon og kapasitet er vanskelig å beregne (Busmundrud et al., 2015, s. 29).

For å rangere konsekvensene har forsvarsbygg utviklet et konsekvensskjema som vist i tabell 4 under. En kan her se at risikoen rangeres fra ufarlig til katastrofalt. Som en ser er nedetid, kompromittering av informasjon, personskader og økonomi kriterier som legges til grunn for å vurdere konsekvensene.

Betegnelse	Driftsforstyrrelser / skade
1 UFARLIG	a) Ingen nedetid. Få eller små endringer i forhold til operativ evne b) Kompromittering av informasjon UGRADERT c) Ingen personskader d) Økonomiske konsekvenser opptil 100 000 kr
2 FARLIG	a) Nedetid < 1 døgn. Viktig funksjon[1] kan ikke opprettholdes, eller ekstraordinære tiltak må iverksettes for å håndtere situasjonen b) Kompromittering av informasjon BEGRENSET c) Få mennesker blir skadet, mindre personskader d) Økonomiske konsekvenser 100 000 – 1 000 000 kr
3 KRITISK	a) Nedetid 1 døgn til 1 uke. Flere viktige funksjoner kan ikke opprettholdes eller omfattende ekstraordinære tiltak må iverksettes for å håndtere situasjonen b) Kompromittering av informasjon KONFIDENSIELT c) Inntil 1 person omkommer og/eller flere alvorlige personskader d) Økonomiske konsekvenser 1 000 000 – 50 000 000 kr
4 MEGET KRITISK	a) Nedetid mer enn 1 uke. Vital funksjon[2] kan ikke opprettholdes b) Kompromittering av informasjon HEMMELIG c) Død/alvorlig masseskade > 5 personer d) Økonomiske konsekvenser 50 000 000 kr –>
5 KATASTROFALT	a) Nedetid mer enn 1 år. Vital funksjon kan ikke opprettholdes b) Kompromittering av informasjon STRENGT HEMMELIG c) Massedød d) Økonomiske konsekvenser 100 000 000 kr –>

Tabell 2: Konsekvensskjema (Busmundrud et al., 2015, s. 30).

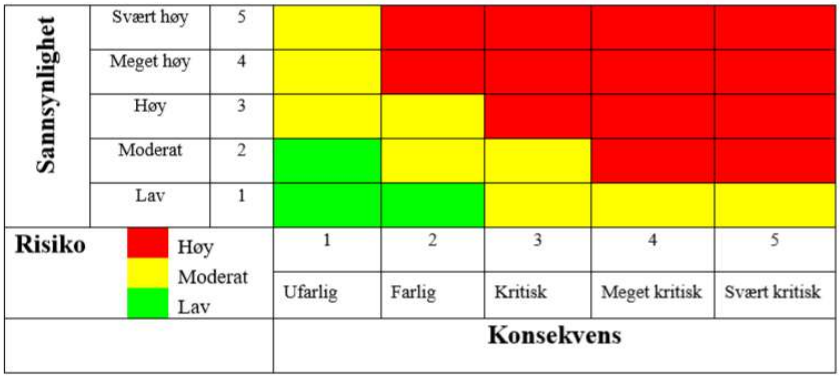
På tilsvarende måte vurderes sannsynligheten for at en gitt hendelse finner sted ved bruk av en tabell som vist i tabell 3 under. Vurderingene er her i stor grad kvalitative og basert på subjektive antagelser. (Busmundrud et al., 2015, s. 30).

Grad av sannsynlighet	Beskrivelse	Kriterier for sannsynligheten
1 *Lav*	Kriteriene - mer detaljert beskrivelse	✓ Tilstedeværelse av verdi ✓ Trusselaktørens intensjon og kapasitet ✓ Fravær av aktive sikringstiltak ✓ Fravær av passive sikringstiltak ✓ Historiske data ✓ Trendrapporter
2 *Moderat*		
3 *Høy*		
4 *Meget høy*		
5 *Svært høy*		

Tabell 3: Tabell for kriterier og grad av sannsynlighet (Busmundrud et al., 2015, s. 30).

Som en ser av tabell 3 er det en rekke ulike kriterier som inngår i vurdering av grad av sannsynlighet. I tillegg til det som er nevnt om verdi og trusselaktør, ser en også at vurdering av sikringstiltak, historiske data og trendrapporter har betydning for den totale vurderingen av sannsynligheten.

Slik også forsvarsbygg gjør er det ved bruk av tofaktormodellen vanlig at resultatene presenteres i en risikomatrise, som vist under i figur 6.



Figur 6: Risikomatrise for bestemmelse av risiko ut fra konsekvens og sannsynlighet (Busmundrud et al., 2015, s. 31).

Matrisen viser nivåsetting av risiko ut fra konsekvens og sannsynlighet og er en av flere måter å visualisere resultatene fra risikoanalysen på. De ulike scenarioene kan her settes inn etter konsekvensklasse. Fargeinndelingen kan tilpasses virksomheten ut ifra hvilke risikoakseptkriterier de har satt (Busmundrud et al., 2015, s. 31).

Trefaktormodellen

Innenfor security utgjør den såkalte trefaktormodellen en annen forståelse av risiko, som dekker elementene verdi, trussel og sårbarhet (Amundrud et al., 2017, s. 287). Denne modellen har sitt opphav etter angrepene 22. juli og i In Amenas, ettersom særlig disse hendelsene medførte økt fokus på det å beskytte seg mot terrorisme (Jore & Egeli, 2015, s. 808). NSM, Politidirektoratet (POD) og PST har utviklet en veileder i terrorsikring som legger trefaktormodellen til grunn. Denne er i det vesentlige basert på NS 5832 (NSM et al., 2015). En vil redegjøre for trinnene som inngår i denne prosessen.

I verdivurderingen definerer NS 5830 verdi som: *«en ressurs som, hvis utsatt for uønsket påvirkning, vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen»* (Standard Norge, 2012). Verdivurderingen innebærer en kartlegging og rangering av de verdiene virksomheten ønsker å sikre, og eksempler kan her være bygninger, personell, gjenstander, omdømme eller sensitiv informasjon (NSM et al., 2015). Sett opp mot UH-sektoren vil verdivurderingen medføre en bevisstgjøring i forhold til hvilke verdier studiestedene innehar, og hvilke som kan være et egnet mål for aktører som ønsker å true disse. For å identifisere verdiene tar en utgangspunkt i leveransene som virksomheten skaper gjennom ulike prosesser, og som igjen er avhengig av ulike ressurser for å kunne leveres. For å finne leveransene kan en spørre seg hva er det virksomheten produserer? Prosessene kan fremkomme ved å stille spørsmålet hvordan blir virksomhetens leveranser produsert? Ressursene utgjør med det verdiene som må ivaretas ved egnede sikringstiltak (NSM, 2016). For å trekke fram et eksempel fra UH-sektoren kan en illustrere leveranse, prosess og verdi som vist i figur 7 under. I figuren fremkommer utdanning som en viktig leveranse, og kunnskap som en prosess som styrer leveransene. Forskning blir med det identifisert som en verdi som kan utsettes for uønsket påvirkning og på denne måten gi negative konsekvenser for utdanningen som er leveransen.

Figur 7: eksempel på identifisert verdi gjennom leveranse og prosess.

Verdivurderingen er av stor betydning for den totale kvaliteten på risikoanalysen, og det bør i denne fasen gjøres grundige undersøkelser av virksomheten ved bl.a. å intervjue ledere og medarbeidere med solid kunnskap. De identifiserte verdiene vil danne grunnlag for prioritering og vurdering av ressurser til sikringstiltak (NSM et al., 2015). Norske studiesteder vil ha ulike verdier som bør beskyttes, så en kan her se denne tilnærmingen som viktig for at tiltakene som iverksettes er tilpasset den enkelte høyskole eller universitet.

Verdivurderingen leder videre til fasen for fastsettelse av sikringsmål. I dette trinnet ser man på hva man ønsker å oppnå med fremtidige sikringstiltak. *«Det skal fastsettes mål for hva som er ønsket eller akseptabel tilstand for verdiene under eller etter en uønsket hendelse»* (NSM et al., 2015, s. 17). For å se til et eksempel som kan være relevant for UH-sektoren kan en her tenke seg at et studiested setter seg som sikringsmål at det ikke skal komme kritiske eller sensitive forskningsdata på avveie etter et forsøk på spionasje eller liknende. Sikringsmål vil være av betydning for å kunne vurdere hvorvidt de iverksatte tiltak har ønsket effekt.

I fasen for trusselvurdering definerer NS 5830 trussel som en *«mulig uønsket handling som kan gi en negativ konsekvens»* (2012). Trusselaktør defineres som en «*kjent eller ukjent aktør (person, organisasjon, land eller annen) som forbindes med en trussel»* (Standard Norge, 2012). Trusselvurderingen tar utgangspunkt i verdiene som det er ønskelig å beskytte, og beskriver det gjeldende trusselbildet. Den bør også ta for seg hvordan trusselvurderingen kan endres, samt et tidsperspektiv som også dekker framtiden. Det kan riktignok være vanskelig å vurdere dagens trusler opp mot fremtidige. *«Hovedfokuset er på reelle og potensielle trusselaktørers intensjon og kapasitet til å ramme virksomheten»* (NSM et al., 2015, s. 17). Med intensjon menes bl.a. om trussel aktøren har uttalt en vilje om å ramme den aktuelle virksomheten, eller man antar at aktøren har et ønske om dette. Det kan her nevnes politisk, ideologisk eller personlig motivasjon. Med kapasitet menes om trusselaktøren faktisk innehar evne til å ramme virksomheten, det være seg f.eks. kompetanse og utstyr (NSM et al., 2015, s. 17). Det kan være krevende å vurdere både intensjon og kapasitet. I 22. juli rapporten fremkommer det at PST i en trusselvurdering fra 2007 bl.a. vurderte at ingen i det høyreekstreme miljøet i Norge har kapasitet til å utgjøre noen vesentlig trussel mot det norske samfunnet. Rapporten antyder at PST trolig har vurdert at miljøene trenger organisering for å kunne bruke den kapasiteten som trengs for å gjennomføre alvorlige terrorhandlinger (NOU

2012:14. (2012), s. 52). I dag vet vi at det ikke medfører riktighet. For å vurdere trusselbildet må det innhentes relevant informasjon fra flere kilder. Det vil være avhengig av virksomheten, men egne erfaringsdata kan benyttes i tillegg til offentlige publiseringer. PST publiserer bl.a. en årlig trusselvurdering som kan brukes som utgangspunkt (NSM et al., 2015, s. 17). For UH-sektoren kan det her være krevende å foreta en trusselvurdering knyttet til f.eks. et scenario med skoleskyting, da det i PST sin årlige trusselvurdering ikke fremkommer konkrete vurderinger knyttet opp mot dette. I Norge har vi heldigvis lite erfaringsdata å basere vurderinger på knyttet til dette, men en må naturligvis kunne se det som en rimelig antagelse at sektoren er særlig utsatt for slike trusler.

Videre foretas vurdering og valg av scenarier på bakgrunn av både verdi- og trusselvurderingen. NSM definerer scenario som *«en tenkt situasjonsbeskrivelse, hvor en trusselaktør gjennomfører et terrorangrep»* (NSM et al., 2015, s. 18). Med det kan vi forstå at en må vurdere relevante måter en trusselaktør kan velge å skade verdiene til virksomheten. Det innebærer at scenarioet faktisk er realistisk og at det kan skje (NSM et al., 2015, s. 18). En scenariobeskrivelse av et ufo-angrep mot UH-sektoren vil de fleste kunne erkjenne at er lite realistisk og følgelig ikke bør vurderes. Hensikten med å vurdere scenarier er at det vil kunne synliggjøre sårbarhetene som kan utnyttes, og det forenkler med det sårbarhetsvurderingen som er neste trinn i prosessen. NSM definerer sårbarhetsvurdering som *«en vurdering av virksomhetens sårbarhet overfor identifiserte trusler mot identifiserte verdier»* (2015, s. 18). Med det kan vi forstå at et studiested kan vurderes som sårbart dersom det har liten evne til å stå imot uønskede hendelser, og vanskelig vil kunne klare å opprettholde en normaltilstand. Sårbarhetsvurderingen vil beskrive hvordan virksomheten skal kunne klare å avverge eller redusere konsekvensene av de scenarioene som fremkom i scenariobeskrivelsen. Ved å redusere sårbarheten vil dette påvirke risikoen i virksomheten. Er det f.eks. et stort sprik mellom tilstedeværende trussel og de tiltak som er iverksatt, så vil det synliggjøre hvilke nye tiltak som bør innføres (NSM et al., 2015, s. 18).

Etter sårbarhetsvurderingen foretas det en totalvurdering av såkalt ren risiko. Det innebærer en kvalitativ sammenstilling av de vurderingene som er foretatt av verdi, trussel og sårbarhet. Subjektivitet og usikkerhet vil inngå i vurderingen av ren risiko, ettersom det som tidligere nevnt bl.a. kan være krevende å vurdere en trusselaktør sin intensjon og kapasitet.

Risikonivået blir vurdert og kan f.eks. bli satt til å være moderat (NSM, 2016, s. 22). Slik det fremgår av tabell 4 under kan skjemaet benyttes for å beskrive hver enkelt risiko, og der de tre trinnene verdi, trussel og sårbarhet sammenstilles til ett risikonivå.

K	Beskrivelse av en enkelt risiko					
Risikonavn :						
		Verdi	Trussel	Sårbarhet		Risikonivå
Risikobeskrivelse :						
Begrunnelse for risikonivå og vekting av vurderingene. Beskriv usikkerhet.						

Tabell 4: Skjema for vurdering av ren risiko (NSM, 2016, s. 22).

I tabellen over er det satt av egen plass for begrunnelse for det risikonivået som er valgt, samt beskrivelse av usikkerheten.

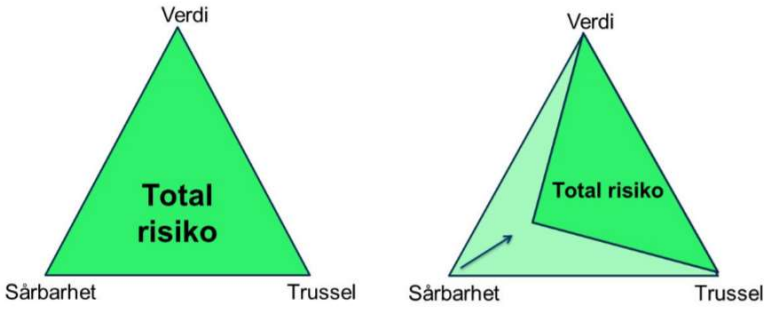
For å presentere risikobildet kan resultatene ved bruk av trefaktormodellen presenteres i en tabell, slik det fremgår av tabell 5 under. Risikoene er her rangert med bakgrunn i risikonivå og bruk av farger illustrerer de ulike nivåene.

L	Risiko rangering
	Risiko tittel og evt stikkord
Svært høy	Risiko 4 tittel …
Høy	Risiko 1 tittel
Høy	Risiko 3 tittel
Moderat	Risiko 6 tittel
Lav	Risiko 2 tittel
Lav	Risiko 5 tittel
Lav	Risiko 7 tittel

Tabell 5: Presentasjon av risiko ved bruk av tabell (NSM, 2016, s. 23).

Total risiko tilknyttet et gitt scenario kan også visualiseres ved bruk av en trekant som vist i figur 8. Forholdet mellom verdi, trussel og sårbarhet utgjør her den totale risikoen i trekanten til venstre i figuren. Trekanten til høyre illustrerer hvordan en reduksjon i sårbarheten vil

innebære at den totale risikoen også endres. En økning av f.eks. trusselen vil tilsvarende kunne illustreres på samme måte ved at den totale risikoen for scenarioet da vil øke.



Figur 8: visualisering av risiko for valgt scenario (Busmundrud et al., 2015, s. 34).

NSM har utviklet et forslag til mal for en rapport som kan dokumentere det som er fremkommet i risikovurderingen, samt hvilke vurderinger som er gjort. Dette for å sikre en systematisk dokumentasjon som gjør det enklere for en beslutningstaker å sette seg inn i de vurderingene som ligger til grunn i analysen (NSM, 2016, s. 23). På bakgrunn av presentert risiko skal beslutningstaker vurdere hvordan en skal håndtere risikoen og herunder velge egnet strategi. En rapport der de bakenforliggende vurderingene fremkommer vil med det være viktig (NSM et al., 2015, s. 19). Vurdering av strategi og videre håndtering av risiko vil ikke bli nærmere beskrevet.

3.5.4 Anbefalt metodikk

Som nevnt har studien til FFI tatt for seg de to metodikkene det her er redegjort for og sammenliknet disse. Deres vurdering av anbefalt metodikk vil her bli presentert.

Den kanskje største forskjellen mellom de to metodikkene er at det i tofaktormodellen og NS 5814 foretas en eksplisitt vurdering av sannsynligheten, altså muligheten for at et vellykket angrep finner sted (Busmundrud et al., 2015, s. 35). I trefaktormodellen og NS 5832 blir det derimot ikke gjort en like konkret sannsynlighetsvurdering. Selv om det ikke eksplisitt kommer til uttrykk må det like fullt ligge vurderinger av sannsynlighet til grunn når det bl.a. blir valgt ut scenarioer. Det må her foreligge en vurdering av hvilke trusler og sårbarheter som anses som sannsynlige (Busmundrud et al., 2015, s. 36). Måten risikoen blir presentert på utgjør også en vesentlig forskjell. Tofaktormodellen gjør på en systematisk måte en vurdering

av konsekvensen av en uønsket tilsiktet hendelse og tilhørende mulighet for at dette faktisk kan skje. Faktorene konsekvens og sannsynlighet sammenstilles så til en risiko, som kan fremstilles i en risikomatrise hvilket er enkel å forstå. Samtidig kommuniserer den i liten grad usikkerhet i de tallene som benyttes, og det kan medføre at det ved bruk av matrise kan fremstå som at det er mindre usikkerhet knyttet til resultatet enn det som faktisk er tilfelle. I trefaktormodellen gis det ingen fremstilling av hvordan de tre faktorene kan sammenstilles på samme måte (Busmundrud et al., 2015, s. 37). I denne modellen blir ikke risikoen kommunisert på en like lett forståelig måte ettersom det er tre faktorer og deres påvirkning på risikoen som skal visualiseres (Busmundrud et al., 2015, s. 37). FFI mener med det å finne at begge de to metodikkene har sine svakheter, særlig når det kommer til det å kommunisere risiko (Busmundrud et al., 2015, s. 64). FFI anbefaler at det i begge tilnærmingene kommuniseres tydelig hvilken usikkerhet de ulike vurderingene innebærer, og ser dette som mangelfullt ved begge metodikkene. Videre påpeker de at det er utfordrende å fremstille usikkerheten visuelt, slik at det gir et godt grunnlag for beslutningstaker å ta stilling til.

FFI viser i sin studie til at det ikke er etablert en bred enighet, hverken nasjonalt eller internasjonalt, om hvilken metodikk for risikovurderinger av tilsiktede uønskede hendelser som vil være å anbefale. FFI finner at flere vitenskapelige artikler og intervjuer underbygger dette (Busmundrud et al., 2015, s. 70). Like fullt forklarer FFI at følgende kjennetegnes ved en god tilnærming: *«den er strukturert, etablerer en arbeidsgruppe med bred kompetanse, kartlegger kunnskapsstyrken, er basert på systemforståelse og er konkret, har et helthetlig perspektiv, kommuniserer risiko og usikkerhet, er gjennomsiktig, sporbar og etterprøvbar»* (Busmundrud et al., 2015, s. 71). Instituttet er også tydelig på at det uavhengig av valgt metodikk så anbefales det at prosessen dokumenteres på en god måte. *«Det er avgjørende i begge tilnærmingene at resultatet må dokumenteres og kommuniseres i en skriftlig rapport som grunnlag for beslutninger»* (Busmundrud et al., 2015, s. 65). Videre anbefaler FFI at *«beslutningstaker må settes seg inn i hele risikovurderingen inkludert forutsetninger, antakelser, vurderinger og usikkerheter, og ikke bare nøye seg med å se på risikomatrisen eller en annen type fargekart*» (Busmundrud et al., 2015). For UH-sektoren kan det være relevant å se til de kjennetegnene FFI vektlegger ved en god tilnærming, ettersom riksrevisjonen nylig har påpekt svakheter knyttet til risikoanalyseprosessen ved universiteter og høyskoler i Norge. De funn som ble gjort i revisjonen er i stor grad knyttet til manglende

dokumentasjon av risikoanalyser og handlingsplaner, samt revidering og plan for alvorlige tilsiktede hendelser (Riksrevisjonen, 2020).

NS 5814 er for tiden under revisjon og status er nå at den har vært ute på høring, og komitéen er i ferd med å implementere høringsinnspillene. Bakgrunnen for revisjonen er at standarden i større grad skal tilpasses utviklingen som har vært innen risikoanalyser og de behovene som brukerne har. De største endringene som er foretatt er bl.a. at det er tatt inn flere aspekter ved risiko, som f.eks. usikkerhet og sårbarhet. Videre er målet å sikre en felles standard for risikovurdering av tilsiktede og utilsiktede hendelser, og standarden skal også oppfylle kravene til sikkerhetsloven. Revisjonen har til hensikt å synliggjøre sammenhengene og forme en helhet ved de tre standardene NS 5814, NS 5832 og NS-ISO 31000 (Standard Norge, 2020). En vil slik det ble påpekt i innledningen ikke gå nærmere inn i denne revisjonen ettersom dette er en pågående prosess. Det kan like fullt bli trukket fram at dette kan resultere i en metodikk som også UH-sektoren kan vurdere å benytte seg av i fremtiden, nettopp for å sikre en enhetlig tilnærming til feltet.

3.6 Oppsummering av teori

Det teoretiske rammeverket i studien består med det av forskjellene og likhetene mellom safety og security, der safety er en mer etablert vitenskap. Security består i større grad av hendelser der noen har et ønske om å ramme noen negativt, men slik det er redegjort for finner en viljestyrte handlinger med negativ konsekvens også innen safety. For å risikovurdere security hendelser er det redegjort for de to metodikkene tofaktor- og trefaktormodellen. Tofaktor har sitt opphav fra safety, mens trefaktor er mer skreddersydd med tanke på security. De to metodikkene har hver sine styrker og svakheter, men som felles svakhet er særlig det at de begge i liten grad kommuniserer usikkerhet uheldig. Den største forskjellen er at tofaktormodellen benytter sannsynlighet eksplisitt, noe som kun kan sies å være implisitt tilstede innen trefaktormodellen. Trefaktor er en mer systematisk prosess der de bakenforliggende årsakene fremkommer, men det er i forlengelsen av denne metodikken krevende å fremstille det totale risikobildet visuelt og forståelig. På samme måte er tofaktormetodikken enkelt bestående av sannsynlighet og konsekvens, men får i svært begrenset grad fram de bakenforliggende vurderingene. Risikobildet fremstilles lett forståelig ved bruk av en matrise, men dette kan medføre en feilaktig vurdering av risikoen. Målet og

hensikten med risikoanalysene er at de skal bidra som grunnlag for å ta beslutninger. Det finnes en rekke ulike perspektiver på risiko, og det er av betydning hvilken definisjon som legges til grunn. Usikkerhet og bakgrunnskunnskap er her begreper som har fått større betydning, og som foretrekkes av mange fremfor sannsynlighetsbegrepet.

Det er i det teoretiske bidraget gitt eksempler på hvordan dette kan ha betydning for UH-sektoren. Ved å se til teorien er det trukket fram at det er viktig å vurdere hva som er formålet med analysene, og at målet er at disse skal bidra til at det blir tatt beslutninger om tiltak som kan redusere risikoen. Det teoretiske rammeverket vil gi sektoren mulighet til å vurdere egen risikoanalyseprosess i sin helhet opp mot det som er anbefalt.

4.0 Design og metode

En vil i dette kapittelet redegjøre for hvilket forskningsdesign og metodebruk som ligger til grunn for oppgaven. Videre vil kapittel 4.5 om studiens troverdighet innebære at forskeren reflekterer over de styrker og svakheter valgene innebærer, samt i hvilken grad kvalitet er ivaretatt.

4.1 Forskningsdesign

Temaet for oppgaven som er risikoanalyser av tilsiktede uønskede hendelser er gjenstand for pågående debatt. Riksrevisjonen kommer som nevnt tidligere med kritikk av UH-sektoren for mangelfull gjennomføring og bruk av risikoanalyser i arbeidet med samfunnssikkerhet og beredskap, der kun 6 av 21 virksomheter oppfyller kravene for risikoanalyser satt av KD (Riksrevisjonen, 2020). Undersøkelse av problemstillingen vil med det være et viktig bidrag til hvordan de ulike studiestedene kan fremme egen sikkerhet og beredskap ved bruk av risikoanalyser som beslutningsstøtte.

Teorien som er valgt ut er nøye vurdert for at den skal kunne bidra til å besvare problemstillingen. Problemstillingen innebærer at det må redegjøres for hva risiko er, samt hva hensikten er med å gjennomføre risikoanalyser. Det er som tidligere nevnt en debatt rundt valg av metodikk opp mot safety og security hendelser, og derfor er det viktig at det også blir redegjort for forskjeller og likheter ved metodikkene. En redegjørelse av de to

risikoanalysemetodikkene er et viktig teoretisk bidrag for å kunne vurdere de opp mot de valg som det fremkommer i empiridelen at praktiseres i sektoren. Det er stor usikkerhet knyttet til security hendelser i forhold til hva som kan bli det neste angrepet, og derfor er det også valgt å redegjøre for usikkerhet som begrep.

Ved bruk av kvalitativ metode blir det foretatt semistrukturerte intervjuer av ti informanter. Informantene ble plukket ut på bakgrunn av nettverk som forskeren har tilgang til, bl.a. gjennom egen deltakelse i beredskapsrådet for sektoren. Funnene i disse intervjuene blir drøftet sammen med teorien som er valgt ut. Det er her viktig å påpeke at det som blir studert er det informantene sier at de gjør opp mot problemstillingen, det er altså ingen fysisk observasjon av hvordan arbeidet blir gjort i sektoren. I slutten av studien presenteres det en konklusjon der forslag til videre forskning utgjør en del av denne.

Forskningsdesign er med det tilpasset problemstilling og forskningsspørsmål.

4.2 Metodevalg

Det blir benyttet kvalitativ metode og foretatt semistrukturerte intervjuer. Relevant teori er valgt ut og brukt som grunnlag i både datainnsamling og den påfølgende analysen. Bruk av risikoanalyser som beslutningsstøtte opp mot security er et relativt komplekst tema. For å få fram fyldige beskrivelser og subjektive oppfatninger er det her valgt en kvalitativ metode med semistrukturerte intervjuer av ti informanter. Gjennom intervjuet kan man stille oppfølgingsspørsmål som vil gjøre at man kan gå dypere, samt oppklare eventuelle misforståelser. Kvalitativ metode er her egnet for å få mer detaljert og nyansert informasjon (Johannessen et al., 2016, s. 28).

Valget av informanter er gjort ut ifra en bevisst utvalgsstrategi da de er relevante og interessante ut fra formålet med studien. Samtlige av informantene har stillinger som innebærer ansvar eller oppgaver knyttet til sikkerhet og beredskap ved eget studiested. De har ulik og relevant bakgrunn, og utvalget av informanter har således god variasjon da de besitter ulike kunnskaper og forutsetninger (Johannessen et al., 2016, s. 113). Det er valgt ut studiesteder bestående av både høyskoler og universiteter, og disse er også av ulik størrelse og fordeler seg utover hele landet. Størrelse på institusjonen er her definert ut fra antall studenter der liten har inntil 10 000 studenter, mellomstor inntil 15 000 studenter og stor over 15 000

studenter. Tabell 6 under er tatt med for å gi en oversikt over utvalget av informanter og herunder deres erfaring, stilling og bakgrunn. Det vurderes her at utvalget og funnene er generaliserbare til andre institusjoner. Opplysningene i tabellen er anonymisert.

Informant	Størrelse institusjon	Tittel, Erfaring fra virksomheten, stilling og bakgrunn	Kjønn	Dato
1	Stor	Fagleder beredskap, 3 år, sykepleier, org. utvikling og pedagogikk	Mann	30.04.20
2	Mellomstor	Assisterende direktør, 4 år, bedriftsadministrasjon og ledelse	Kvinne	12.05.20
3	Stor	Seniorrådgiver HMS og beredskap, 4 år, samfunnssikkerhet	Mann	15.04.20
4	Liten	Sikkerhets- og beredskapsrådgiver, 3 år, IT og ledelse	Mann	06.05.20
5	Stor	Seniorrådgiver sikkerhet og beredskap, 3 år, politi	Kvinne	28.04.20
6	Mellomstor	Seniorrådgiver samfunnssikkerhet og beredskap, 1 år, ambulanse og HMS	Mann	22.04.20
7	Stor	Drifts- og sikkerhetssjef, 5 år, forsvaret	Mann	08.04.20
8	Mellomstor	Seniorrådgiver samfunnssikkerhet og beredskap, 3 år, samfunnssikkerhet	Kvinne	13.05.20
9	Liten	Sikkerhetssjef, 10 år, økonomi og forsvaret	Mann	04.06.20
10	Stor	Seniorrådgiver sikkerhet og beredskap, 1 år, politi	Mann	06.05.20

Tabell 6: Anonymisert oversikt over informantene.

Det er det teoretiske rammeverket i kapittel 3 som ligger til grunn for intervjuguiden, denne følger som vedlegg til studien. Teorien er førende for de temaer og spørsmål som er valgt ut i intervjuguiden. Det er her lagt vekk på temaene tilsiktede uønskede hendelser, safety vs security, risikoanalysemetodikk og beslutningsstøtte. Det skal med det være en rød tråd fra teorien til metoden.

4.3 Datainnsamling

Intervjuene har foregått digitalt til avtalt tid med forsker og informant til stede. Digitale intervjuer ble valgt ettersom det på grunn av koronakrisen ikke var mulig å møtes fysisk. Det vil som regel være en fordel for kommunikasjonen at man i intervjuer kan møtes ansikt til ansikt. Like fullt har det fungert godt med digital gjennomføring i denne studien, i det forskeren har kunnet ta opp samtalen i tillegg til at informanten har kunnet presentere relevante dokumenter m.m. fortløpende. Forskeren kjente ikke informantene fra tidligere og startet alle intervjuene med en uformell prat, for å sikre en felles forståelse for intervjusituasjonen og legge forholdene til rette for en god kommunikasjon. I forkant av intervjuene fikk informantene tilsendt informasjon om prosjektet. Informantene ble gjort kjent

med at intervjuet er anonymt, samt at konfidensielle data ikke skulle videreformidles. Det skal i studien ikke fremkomme informasjon som kan bidra til at noen av informantene kan identifiseres. Intervjuet ble tatt opp på lyd for å gjøre det lettere for forskeren i etterkant å kvalitetssikre hva som ble sagt. Samtlige informanter ble spurt om de samtykket til dette. De ble gjort kjent med at opptaket vil bli slettet i etterkant. Intervjuene ble transkribert i sin helhet.

Ut ifra oppgavens omfang har forskeren samlet inn de data som er mest mulig relevante og pålitelige for å kunne svare på problemstillingen innenfor tidsrammen.

4.4. Datainnsamlingens utfordringer

Ettersom forskeren selv er ansatt som ansvarlig for sikkerhet og beredskap ved Handelshøyskolen BI kan dette by på noen utfordringer knyttet til dataanalysen, men samtidig adresseres noen fordeler. Av fordeler kan man her nevne at forskeren har engasjement og endringslyst knyttet til UH-sektoren, og problemstillingen som studien omfatter. Bakgrunnen for valg av problemstilling var som nevnt i innledningen et kurs i sikringsrisikoanalyser i regi av DSB, og forskeren sitter her med ønske om å bedre arbeidet knyttet til dette i sektoren.

Sett fra den andre siden kan engasjementet medføre en mulig feilkilde ved at det fungerer styrende for den konklusjonen man kommer fram til, samt at forskeren kan påvirkes av forutfattede meninger og fordommer. En annen utfordring kan i dette tilfellet være å gjengi en usminket sannhet. Det er avdekket forbedringspotensial, og ettersom forskeren selv jobber i sektoren kan det stilles spørsmål ved om man klarer å fremstille data på en korrekt måte, eller om man blir påvirket til å begrense det man kan kalle negative funn (Jacobsen & Repstad, 2004). I dette tilfellet blir ikke forskerens egen arbeidsplass omfattet av studien, og utfordringer knyttet til dette sees ikke som relevant.

I studien er alle informantene ansatt i stillinger med ansvar for sikkerhet og beredskap ved et gitt studiested. Man kan således stille spørsmål ved om informantene i intervjuene svarer det de oppriktig mener, eller om de forsøker å glatte over eventuelt forbedringspotensiale. Informantene kan tenke at det innebærer ulemper å oppgi svakheter knyttet til problemstillingen. Informantene virket i dette prosjektet å være åpne og ærlige. Flere av informantene har bl.a. sagt en del ting som «*for å være ærlig*» og «*jeg må nok erkjenne at*»,

noe som bekrefter at de ikke legger skjul på eget forbedringspotensial. Ved en kvalitativ tilnærming er det rom for feiltolkning ettersom det blant annet er subjektive oppfatninger som blir kommunisert. Det avgjørende er at det folk forteller må vurderes i forhold til konteksten (Jacobsen & Repstad, 2004, s. 239). For å minimere risikoen for feiltolkning har forskeren her tatt hensyn til dette ved blant annet å oppsummere det informantene har sagt, for å kontrollere at informasjonen er forstått riktig.

Det kan dessuten være en fordel ved intervju av informanter at forskeren selv jobber i sektoren, da det nettopp vil være vanskelig å glatte over sannheten, og det vil være lettere å få fram et eventuelt skille mellom ord og handling (Jacobsen & Repstad, 2004, s. 240). Det vil også være lettere å stille utdypende spørsmål, da forskeren selv kjenner hverdagsspråket i sektoren (Jacobsen & Repstad, 2004, s. 240). Dette har her vært en fordel opp mot samtlige informanter i denne studien. Problemstillingen er av en slik art at det vil være en stor fordel at forskeren selv er ansatt i sektoren, samt medlem av beredskapsrådet. Arbeidet med å velge ut informanter blir både praktisk enklere, samtidig som strategien opp mot utvalget er lettere å kvalitetssikre. Forskeren har riktignok bare vært ansatt i sektoren i et halvt år og medlemskapet i rådet har hatt enda kortere varighet, noe som kan styrke evnen til å være objektiv.

4.5 Studiens troverdighet

En vil i dette kapittelet gjøre refleksjoner over de valg som er foretatt av forskningsdesign og metode. Det vil her stå sentralt å vurdere troverdigheten til det som blir presentert som empiri, i tillegg til å vurdere fordeler og ulemper ved metoden som ligger til grunn i studien. Å reflektere over og evaluere kvaliteten av en studie er av stor betydning, og avhenger ikke av hvilke metoder som er benyttet. Særlig innen kvantitativ forskning benyttes gjerne begreper som reliabilitet og validitet som kriterier for å vurdere kvaliteten i studien (Johannessen et al., 2016, s. 231). En vil her legge Lincoln og Guba sine kvalitetsbegreper til grunn, da det vil gi et bedre grunnlag for å vurdere kvalitative undersøkelser som er anvendt i denne studien. Begrepet trustworthiness står her sentral med de fire kvalitetsbegrepene troverdighet, overførbarhet, pålitelighet og bekreftelse (Lincoln & Guba, 1985). En vil videre gå gjennom hver av de fire kvalitetsbegrepene og reflektere over hvorvidt de er ivaretatt tilfredsstillende.

Troverdighet innebærer i hvilken grad det man skulle undersøke faktisk har blitt undersøkt, og herunder at leseren etablerer tillit til at de resultatene som blir presentert samsvarer med virkeligheten. Å fremme troverdighet kan gjøres på flere måter og Johannessen et.al trekker her fram det å sette seg godt inn i feltet som skal studeres, involvere flere forskere til å vurdere prosjektet, samt benytte seg av flere metoder ved innhenting av data (2016). I denne studien har målet vært å undersøke hvordan universiteter og høyskoler benytter risikoanalyser som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser. Problemstillingen og forskningsspørsmålene har her vært sentral, og på bakgrunn av denne ble det laget en intervjuguide som var inndelt i temaer. Temaer og spørsmål ble utviklet og avgrenset direkte mot problemstillingen og tilhørende forskningsspørsmål, nettopp for å bidra til at intervjuene faktisk ga svar på dette. Informantene fikk tilsendt intervjuguiden i forkant slik at de kunne stille forberedt og foreta eventuelle undersøkelser eller forberedelser, og på denne måten kunne gi mest mulig utfyllende svar. Det har trolig hindret informantene i å gi improviserte svar fordi de føler at de må komme opp med noe. Studien har kun benyttet kvalitative intervjuer som metode for å skaffe viktige data, og dette har vært nødvendig for å kunne dokumentere hvordan jobben faktisk gjøres der ute. Spørreundersøkelser ville eksempelvis ikke gitt den samme kvaliteten eller grunnlaget for å kunne besvare problemstillingen. Intervjuene har gjort at informantene har kunnet gi en grundig forklaring, og der forskeren har kunnet stille oppfølgingsspørsmål dersom noe har vært uklart. Temaet for oppgaven kan sies å være et krevende fagfelt og det å stille oppfølgingsspørsmål har vært avgjørende for å sikre kvalitet i studien. Det at ti informanter er intervjuet utgjør et godt grunnlag for å kunne svare på problemstillingen, og troverdigheten blir med det ivaretatt. I etterkant av samtlige intervjuer har forskeren gitt en oppsummering av hvordan svarene er forstått og tolket. Dette for å kvalitetssikre at forskeren har oppfattet innhentet materiale riktig. Intervjuene ble tatt opp på lyd slik at de kunne gjennomgås for nøye analyse i etterkant. Det har sikret at det er mulig å høre det som ble sagt flere ganger, i motsetning til en mer stressende metode ved å ta notater underveis i samtalen der det ikke blir gjort lydopptak. De innhentede dataene viser noe ulik praksis og kunnskap mellom studiestedene, noe som viser at forskeren gjennom intervjuene har fått fram flere sider enn det man på forhånd kunne anta. Dette styrker troverdigheten til studien etter forskerens mening.

Ettersom forskeren selv er student er det ikke naturlig å involvere flere forskere i prosjektet. Det har heller ikke vært mulig eller hensiktsmessig å benytte seg av flere metoder. Det har

vært god dialog med veileder, som på denne måten også har fungert som en kontroll av kvaliteten i prosjektet fortløpende. Blant annet har veileder vurdert intervjuguiden før intervjuene ble gjennomført. Dialog med veileder har medført justeringer underveis.

Forskeren er som tidligere nevnt selv en del av beredskapsrådet for sektoren. En kan med det stille spørsmål ved om det svekker troverdigheten. Slik forskeren har vurdert det har deltakelsen her kun vært kortvarig, og dette har ikke påvirket studien i negativ retning. Tvert imot har det bidratt til tilgang på informanter og andre kontaktpersoner av betydning. Det har også gjort at forskeren har hatt god kjennskap til sektoren og dets arbeid med sikkerhet og beredskap, og herunder kunnet sette seg godt inn i feltet som skulle studeres.

Med overførbarhet menes i hvilken grad de funn som fremkommer i studien er overførbare til andre sammenhenger (Lincoln & Guba, 1985). Med det kan vi forstå at det vurderes hvorvidt resultatene og metoden altså er gyldig i en annen setting. Ettersom studien består av kvalitativ metode og herunder semistrukturerte intervjuer vil antallet informanter være mer begrenset, enn dersom det ble benyttet kvantitative metoder i form av spørreundersøkelser m.m. Det er like fullt her gjort et nøye utvalg av informanter, og disse er godt egnet til å bidra med data til å besvare problemstillingen. Det er beskrevet hvilke kriterier informantene er valgt ut på, hvilket vil gjøre at leseren selv kan ta stilling til overførbarhet basert på resultater i studien og den øvrige litteraturen. Informantene har alle stillinger der de på noe ulikt nivå har ansvar for sikkerhet og beredskap i sin virksomhet. Sett ut fra antall virksomheter i UH-sektoren er antallet som her er intervjuet høyt, og informantene representerer et bredt spekter av utdanningssteder både i form av størrelse, geografisk plassering m.m. Forskeren kan ikke selv trekke konklusjonen, men leseren bør kunne vurdere at resultatene er overførbare til hele sektoren det her gjelder.

Det vil her være forskerens tolkninger av resultatene som er av betydning for å vurdere grad av overføring. Som nevnt tidligere har bl.a. 22. juli hendelensene medført økt fokus på sikkerhet og beredskap, og herunder bruk av risikoanalyser i dette arbeidet. Dette er altså ikke unikt for UH-sektoren. Ved å gi en utvidet beskrivelse av prosessen i studien vil leseren kunne vurdere overførbarheten til andre sammenhenger. Forskeren vurderer at de resultatene

som er presentert vil være relevant i arbeidet med sikkerhet og beredskap, her med fokus på security hendelser, også i andre sektorer. Det antas at tilsvarende resultater vil kunne fremkomme også ved å benytte et annet utvalg av informanter. Forskeren mener med det at de vurderinger og valg som er gjort fremkommer tydelig i metodekapittelet, og at det dermed vil være egnet og mulig dersom andre ønsker å gjenta prosjektet i samme målestokk eller større omfang.

I hvilken utstrekning en annen forsker vil kunne gjenta prosjektet påvirker grad av pålitelighet til studien. Lincoln og Guba forklarer at måten spørsmålene blir stilt i intervjuet vil påvirke grad av påliteligheten til studien, og de trekker frem åpne eller lukkede spørsmål som eksempel (1985). For å reflektere over påliteligheten av egen studie vil dermed intervjuguiden og de spørsmål som er stilt i intervjuene stå sentralt. Intervjuguiden er nøye vurdert i forhold til hvordan de spørsmålene som blir stilt kan bidra til å besvare problemstillingen på en objektiv måte, og slik at det unngås lukkede spørsmål som begrenser muligheten til å fortolke dataene. Forskeren har for øvrig bakgrunn fra politiet og er kjent med viktigheten av at de som blir intervjuet får presentert åpne spørsmål, samt at de har mulighet til å forklare seg fritt uten avbrytelser. Forskerens egen erfaring og bakgrunn har med andre ord bidratt til å styrke påliteligheten av studien. Den samme intervjuguiden er benyttet i alle intervjuene og spørsmålene har i størst mulig grad blitt stilt på samme måte. Det vil gjøre at andre i stor grad vil kunne gjennomføre intervjuene på samme måte. Intervjuene er for øvrig transkribert i sin helhet og tilgjengelig. I forkant av intervjuene ble alle informantene informert om at dersom de var usikre på om de forstod spørsmålet som ble stilt så måtte dette fremkomme. Det ble oppfattet slik at det ble gjort i de tilfellene det var behov for oppklaringer. Selv om intervjuguiden og spørsmålene er tilgjengelig vil det like fullt måtte erkjennes at en annen forsker vil kunne komme frem til noe annet resultat, ettersom det ikke vil være mulig å legge til rette for at spørsmålene blir stilt på akkurat samme måte. Det er benyttet sitater fra intervjuene i både resultat og drøftingsdelen, dette for at leseren skal forstå hvordan resultatet er fortolket og hva som ligger til grunn for de ulike konklusjoner.

Med pålitelighet kan det forstås slik at det etableres en tillit til studien som er gjennomført. For å styrke påliteligheten og tilliten er det slik det tidligere er nevnt av betydning at det gis en fyldig beskrivelse av prosjektets rasjonale og fremgangsmåte. Andre vil da kunne ha

muligheten til å kunne spore forskerens dokumentasjon av data, metoder og avgjørelser gjennom prosjektet (Johannessen et al., 2016). Med argumentasjonen ovenfor legges det til grunn at tilliten er ivaretatt i denne studien.

I bekreftbarhet ligger at de presenterte funn er reelle og samsvarer med virkeligheten, forskerens egne synspunkter bør ikke utelukkende legges til grunn. For at bekreftbarheten skal fremmes bør prosessen og fremgangsmåten i studien beskrives nøye og i sin helhet. På denne måten kan leseren som tidligere nevnt selv bli satt inn i de beslutninger og valg som er gjort. Forskeren må her selv reflektere over de forhold som kan påvirke subjektive tolkninger og tilnærminger i studien (Johannessen et al., 2016). Som forsker bør en reflektere over subjektive meninger, og kanskje særlig innen kvalitative studier som det er snakk om her. For å fremme bekfreftbarheten og for å redusere muligheten for at resultatene utelukkende baseres på forskerens subjektive forståelse, har en i denne studien tydelig beskrevet de forhold som er forskerens egen oppfattelse eller vurdering. Samtidig må en erkjenne at en som forsker, og kanskje særlig i en sektor og et fagområde man har god kjennskap og kunnskap om, vil være krevende å fristille seg på en helt objektiv måte. Bekreftbarheten må her ivaretas ved at forskeren er kritisk til sin egen objektivitet og kommuniserer tydelig de forhold som er subjektive forståelser, hvilket er gjort i størst mulig grad i denne studien. Lincoln og Guba påpeker at for at en studie skal være bekfreftbar bør den inneha gjennomsiktighet i form av en rød tråd gjennom prosessen i sin helhet (1985). Med rød tråd kan vi her forstå at forskeren må reflektere og kommunisere de valg som blir gjort gjennom hele prosjektet, fra problemstilling, metodiske valg og til resultat. I denne studien er dette ivaretatt ved at fremgangsmåten skal være gjennomsiktig ved disse forholdene.

Vi kan se likheter mellom kriteriet for pålitelighet og bekreftbarhet, der sistnevnte skiller seg fra førstnevnte ved at det essensielle er at resultatet utelukkende er basert på fremskaffet data, og ikke forskerens subjektive oppfattelser (Anney, 2014). I denne studien er flere av funnene i samsvar med det som tidligere har fremkommet om temaet på både virksomhets og samfunnsnivå, i tillegg til at tidligere forskning og teori blir diskutert opp mot de funnene som er gjort. Rapporten fra riksrevisjonen, der det som tidligere nevnt fremkommer at det er mangler knyttet til gjennomføring og oppfølging av risikoanalyser i sektoren, må for øvrig kunne sies å styrke kvaliteten i denne studien i det resultatene er samsvarende.

En har i dette kapitelet reflektert og argumentert over de fire kvalitetskriteriene, og en vil med bakgrunn i dette konkludere med at disse kriteriene er ivaretatt på en god måte i studien.

4.6 Etiske hensyn

I forbindelse med gjennomføring av de semistrukturerte intervjuene ble disse tatt opp på lyd. Slik det ble argumentert for tidligere i studien ble dette gjort for å kunne høre på opptaket etter intervjuene, og på denne måten forsikre seg om at innholdet ble tolket mest mulig korrekt. Det medførte også at de direkte sitatene som ble fremlagt ble gjengitt slik det ble sagt. Norsk senter for forskningsdata regner stemme på lydopptak som en behandling av personopplysninger. På bakgrunn av dette ble prosjektet meldt til senteret og etter råd fra dem er opptakene lagret slik at ingen kan identifiseres, samt at opptakene ble slettet på det tidspunktet det ikke lenger var behov for å benytte seg av disse.

Ettersom det er et strengt regelverk knyttet til det å behandle personopplysninger er samtlige informanter informert om sine rettigheter i forkant av intervjuene, både på e-post og muntlig like før oppstart. Informantene har alle samtykket til at intervjuene ble tatt opp på lyd. Forskeren har med det ivaretatt etiske utfordringer knyttet til dette, og kan ikke se at det foreligger andre uheldig forhold opp mot de generelle forskningsetiske retningslinjer utarbeidet av de nasjonale forskningsetiske komiteene. Prinsippene om respekt, gode konsekvenser, rettferdighet og integritet står her sentralt og disse anses ivaretatt i denne studien.

5.0 Empiri

I dette kapittelet blir de funn som har fremkommet i intervjuene presentert. Empirien blir her inndelt i temaer med utgangspunkt i forskningsspørsmålene og intervjuguiden.

5.1 Tilsiktede uønskede hendelser

Alle informantene forklarer at de har fokus på tilsiktede uønskede hendelser i arbeidet med sikkerhet og beredskap ved deres virksomhet, men at fokuset særlig har økt de siste årene. Graden av fokus varierer mellom de ulike virksomhetene. Nesten samtlige benytter risikoanalyser i dette arbeidet, men omfanget av bruken varierer. Der en av informantene forklarer at dette benyttes aktivt også i forkant av kommende arrangementer som fadderuke m.m., forklarer en annen at de ikke har gjennomført egne analyser opp mot tilsiktede uønskede hendelser de siste årene. Sistnevnte forklarer at tilsiktede uønskede hendelser ikke inngår som en del av risikoanalysene, men at vold og trusler generelt er med i den overordnede risikoanalysen. *«Dette er veldig perifert og er ikke delt opp i ulike scenarioer eller knyttet til egne tiltakskort»* (Informant 9). Samme informant forklarer også at de har gitt opplæring/informasjon om muligheten for skoleskyting, men dette er på bakgrunn av pålegg gitt av kunnskapsdepartementet og ikke som et resultat av oppfølging av risikoanalysene.

Samtlige av informantene oppgir at de benytter risikoanalysene til å opprette beredskapsplaner for de scenarioene som fremkommer i de mer overordnede analysene.

5.2 Safety vs security

Ingen av informantene i studien oppgir at de har noe organisatorisk skille mellom safety og security. Noen skiller dette ved valg av metodikk i risikoanalysene, og empirien rundt dette fremkommer i kapittel 5.3.2. De fleste har organisert arbeidet slik at en HMS eller HR avdeling håndterer oppgaver knyttet til både safety og security, men at ansvar og tilnærming er fordelt. Det er ingen som har egne avdelinger eller stillinger som kun er øremerket for å jobbe med security hendelser. Det eneste unntaket er her enkelte stillinger som jobber med informasjonsteknologisk (IT) sikkerhet, som også innebærer forebyggende og reaktiv innsats mot dataangrep. Flere av informantene forklarer at de ønsker en egen stilling for en person

som er ansvarlig for sikkerhet og beredskap eller liknende. Argumentene er her at for at arbeidet skal kunne prioriteres og ivaretas på en optimal måte, så må det være egne ansatte som er øremerket og dedikert til dette. Det er flere som ønsker et skille der det opprettes en egen sikkerhets- og beredskapsavdeling, ettersom det er mange som har oppgaver knyttet til sikkerhet og beredskap der disse kommer i tillegg til opprinnelige primæroppgaver i virksomheten. Argumentene er videre at det å jobbe med sikkerhet og beredskap er blitt et stadig mer omfattende og krevende felt, slik at det er en stor fordel at dette ivaretas av noen som utelukkende har dette som fokus. Men det ønskes altså ikke et organisatorisk skille, slik den ene informantene understreker ved å si at *«tiltak opp mot security får også betydning for safety, så man må se dette i sammenheng»* (Informant 3). Dette fordi de to områdene henger sammen og tiltak innen det ene vil kunne påvirke det andre. Flere trekker fram at det er safety som er gjenstand for hovedfokuset, og at det å tenke security er nyere og har fått økt oppmerksomhet først de senere årene.

Informantene er positive til at arbeidet organiseres slik at oppgaver knyttet til både safety og security er samlet under samme avdeling eller område. Det blir forklart at for å sikre den optimale totale kompetansen i virksomheten, er det mest hensiktsmessig at det i arbeidet med sikkerhet og beredskap ikke gjøres organisatoriske skiller mellom safety og security. Det blir fremhevet at HMS og øvrig beredskap må henge tett sammen, og at dette ikke bør fragmenteres. Eksempel på dette er det en av informantene forklarer: *«vi opplever at det er fornuftig å ha flere fagpersoner å spille på. Dette handler om mye av det samme, nemlig trygghet og sikkerhet for brukerne våre. Så dette går i hverandre»* (Informant 1). En annen informant støtter dette ved å si at *«vi har en bevisst tilnærming til safety vs security, og fletter HMS og øvrig beredskap inn i ett»* (Informant 3).

5.3 Risikoanalyser

Alle informantene benytter risikoanalyser i arbeidet med sikkerhet og beredskap. Det fremkommer noen ulikheter hva gjelder metodikk, kompetanse og beslutningsstøtte.

5.3.1 Metodikk

Informantene bruker ulik metodikk når det gjelder risikoanalyser av tilsiktede uønskede hendelser. Det er et skille der omtrent halvparten benytter tofaktormodellen og den andre halvparten trefaktormodellen. Noen benytter tofaktor til å analysere både safety og security hendelser. Andre benytter tofaktor kun til safety, men trefaktor opp mot security. Flertallet av informantene benytter riktignok samme metodikk for å analysere safety hendelser som for security. Det er kun en av informantene som benytter trefaktormetodikken til begge. En av informantene forklarer at de bruker tofaktor med sannsynlighet og konsekvens for både safety og security, men at flere av begrepene fra trefaktormetodikken blir implementert inn i tofaktormetodikken. *«Begrepene sårbarhet, verdi og trussel blir bragt inn i den tradisjonelle ROS-analysen. Vi spør da hvilke verdier har vi, hvem er trusselen og hva er sårbarheten»* (Informant 4). Informanten forklarer at de gjør dette fordi man i forhold til bl.a. terror og skoleskyting har lite tallgrunnlag for Norge sin del. *«Konsekvensene vil jo være store, men det er vanskelig å sette eller diskutere sannsynligheten for disse hendelsene. Men hvis man får inn verdi, trussel og sårbarhet så blir det kanskje lettere»* (Informant 4). Informanten som forklarer at de ikke har gjennomført systematiske analyser opp mot tilsiktede uønskede hendelser, forklarer at de ville benyttet trefaktormetodikken dersom de skulle gjort dette. En av informantene forklarte at det var noe uklart hvilken metodikk som ble benyttet.

Det fremkommer noen ulikheter i forhold til i hvor stor grad valg av metodikk er et bevisst valg. En av informantene forklarer at de er bevisst på valg av metodikk ved å si at «*vi har tatt et valg på at det fungerer bra å benytte tofaktor knyttet til både safety og security»* (Informant 1). En annen informant forklarer at krisehåndteringsverktøyet CIM benyttes og at denne legger noen føringer. Modulen for risikoanalyser der tofaktormetodikken ligger til grunn skiller ikke mellom safety og security, både safety og security sammenstilles i en oversikt. Det er flere som påpeker at tofaktor er en enklere og mer gjennomførbar metodikk, og dermed velger å benytte seg av denne for begge feltene. Informanten som sier at det er uklart hvilken metodikk de benytter forklarer at det ikke er noe bevisst valg knyttet til dette.

5.3.2. Egen metodikk for security

I synet på om det trengs egen metodikk for risikoanalyser av security hendelser, svarer flertallet at de ikke ser behovet for en egen tilnærming til dette. Det blir påpekt at dette kan

avhenge av møtedeltakerne og hvilken kultur det er for å fokusere på gjennomføring av risikoanalyser opp mot security. En av informantene forklarer at det trolig er lettere å benytte det vedkommende kaller en mer korrekt metodikk dersom et konsulentfirma bistår med gjennomføringen og holder i det, enn dersom de skal stå for dette selv. Informanten ser ikke behov for en egen metodikk opp mot security ved å si at «*for vår del vil nok det komplisere analysearbeidsmøtet i så stor grad at vi mister fokus på det som er viktig. Da burde man nok dele møtene inn i egne for tilsiktede og egne for ikke tilsiktede. Da vil man møte utfordringer mtp. tidsbruk og spørsmål om man ikke kan gjennomføre safety og security analyser i de samme møtene»* (Informant 4).

En annen informant støtter dette ved å argumentere for at valgt metodikk bør være lett gjenkjennbar når man går inn i et dokument, både for den som skal gjennomføre og den som skal bruke analysen som beslutningsstøtte. *«Det burde være en standard på ting så det er gjenkjennbart på tvers, og en bør med det ikke gå for en egen metodikk opp mot security»* (Informant 7).

Flere argumenterer for at det vil være fordeler og ulemper ved å bruke egen metodikk for security, og at dette kan variere mellom de ulike virksomhetene som også må være fleksible. Det blir trukket fram at det er lite gunstig å tvinge noen til å måtte lære seg en ny metodikk når de er godt innarbeidet i en annen. Det er også flere av informantene som påpeker at det her bare er snakk om metodikk, og at det ikke er det i seg selv som må vektlegges tyngst. En av informantene forklarer dette ved å si at «*dette dreier seg bare om metodikk og det viktigste er å ha et bevisst forhold til risiko. Man må benytte terminologi som er kjent for de som skal bruke dette»* (Informant 5). Vedkommende har brukt bow-tie modellen med stort hell for å vise sannsynlighets og konsekvensreduserende tiltak. *«Dette medfører at folk tenker at jammen jeg kan jo dette her, og bruker det»* (Informant 5).

En informant som forklarer at de ikke ser behov for egen metodikk for security sier at de får best resultater ved at de kun benytter en metode. Det blir også dratt parallell opp mot det at man ikke ønsker et skille mellom safety og security generelt. *«Skal vi ha forskjellige metoder så blir ingen gode. Vi finner nok ikke noe som er helt perfekt på alle mulige måter, men det nytter ikke å sitte å jobbe med samme utfordringer, men med forskjellig tilnærming»* (Informant 6). Et annet argument for det samme er at de i organisasjonen ikke skiller mellom

safety og security, men er kjent med at det av enkelte hevdes at det er gunstig med egen metodikk opp mot tilsiktede uønskede hendelser, og at trefaktormodellen da er egnet. «*Det er nok enklere å få fram verdier m.m. ved bruk av trefaktormodellen, men vi har ikke sett behovet for å gjøre en slik systematisk vurdering opp mot security»* (Informant 9).

5.4 Kompetanse

Det er ulikheter i forhold til kompetanse om metodikk og valg av dette blant informantene og i virksomhetene generelt. To av informantene oppgir at de har egne ansatte som er spesialister på risikoanalyser, i tillegg til konsulenter fra CIM som sikrer høy kvalitet i deres prosesser. Scenarioene tilpasses her de ulike avdelingene ved studiestedet, og hver enkelt avdeling er tungt inne og vurderer dette. Det er de største studiestedene som her besitter mest kompetanse og ressurser på feltet.

Flere av informantene erkjenner at de og virksomheten har mangelfull kunnskap om gjennomføring av risikoanalyser, og at det særlig opp mot security er manglende kunnskap og erfaring rundt hvordan man skal benytte risikoanalyser inn i arbeidet med å redusere risikoen. En av informantene sier følgende: *«jeg må være ærlig på at min kompetanse er for lav ift. valg av metodikk, og jeg har ikke gjort vurderinger på om det ene metodevalget er bedre enn det andre. Jeg bruker stort sett erfaring og ting jeg har lest om, og det er min metode. Det er et metodeverk som ligger bak, men du finner nok ikke dette igjen i noen lærerbok»* (Informant 7).

En av informantene forklarer at det internt i virksomheten er et sprik i kompetansen til de som gjennomfører analysene, samt i hvilken grad dette faktisk gjennomføres. *«De har ulik metodikk, innhold og fokus». De ulike fakultetene har for dårlig kompetanse til å gjennomføre analyser, og det er ikke mange av fakultetene som har vurdert tilsiktede uønskede hendelser»* (Informant 5).

5.5 Trusselvurderinger og scenarioer

Informantene forklarer at de benytter flere ulike kilder for å vurdere trussel og aktuelle scenarioer for tilsiktede uønskede hendelser. De fleste benytter her offentlig tilgjengelige trusselvurderinger fra ulike instanser som PST og NSM. Tidligere gjennomførte risikoanalyser, interne hendelser og erfaringer blir også benyttet. Det er flere som baserer scenarioene på det som fremkommer i styringsdokumentet fra KD, og som igjen er basert på risikovurderingen fra DSB. Noen få bruker også hendelser i utlandet som blir kjent gjennom mediene og da særlig Norden, som en del av grunnlaget for egne vurderinger av relevante scenarioer og trussel mot egen virksomhet.

5.7 Risikoanalyse som beslutningsstøtte

De fleste informantene forklarer at analysene særlig er brukt som beslutningsstøtte for å opprette eller oppdatere beredskapsplaner. De færreste oppgir at de benytter risikoanalysene som beslutningsstøtte for konkrete tiltak eller handlingsplaner for de aktuelle security scenariene. Flere argumenterer for at analysene blir brukt som grunnlag mer i underbevisstheten ettersom de med det er klar over risikoen, og overordnede tiltak blir gjennomført for å redusere denne. En av informantene forklarer dette ved å si at de bruker risikoanalysene mest for å lage beredskapsplaner, og lite i forbindelse med konkrete forebyggende tiltak i hverdagen. *«Man må nok legge godviljen til for å se noen bevisst sammenheng mellom de risikoanalysene som er gjennomført og de beslutningene vi tar»* (Informant 2).

En annen forklarer at de snart har et nytt bygg som står ferdig og i forbindelse med prosjektet er det ikke gjennomført risikoanalyser opp mot security hendelser, kun opp mot safety. En annen informant forklarer at de har gjennomført risikoanalyser som har identifisert hendelser, men at dette ikke har blitt fulgt opp videre. *«Analysene har f.eks. identifisert pågående livstruende vold (PLIVO), men det blir ikke operasjonalisert med tiltak eller handlingsplan». «Jeg prøver å sammenfatte det så det blir lettere for beslutningstaker å sette seg inn i dette, slik at det i fremtiden vil komme flere tiltak og handlingsplaner som følge av dette. Analysene blir i for liten grad benyttet som beslutningsstøtte»* (Informant 6). Det er også en av informantene som trekker fram styringsdokumentet fra KD og sier at «*det er gitt i oppdrag fra*

KD at vi skal gjennomføre dette og at vi skal rapportere på det, så derfor gjør jeg det. Analysene brukes i liten grad som beslutningsstøtte» (Informant 7). Det er flere som argumenterer for at en del trolig gjør dette fordi det er et krav fra KD. Den ene informantene forklarer dette ved å si at «*det er nok en del i sektoren som gjør dette for å krysse av at man har vært flinke og utført analyser»* (Informant 4).

Det er flere av informantene som trekker frem at det er viktig at ikke risikoanalysene blir stående ubrukt i fine permer, men at de faktisk benyttes som støtte for beslutninger av tiltak og handlingsplaner. Det er en erkjennelse fra flere om at risikoanalysene fort blir stående uten oppfølging og tiltak. Flere av informantene forklarer at det trolig er ulikheter i sektoren i forhold til i hvilken grad risikoanalysene benyttes som beslutningsstøtte, men at disse uansett øker risikobevisstheten i organisasjonen.

At det er ulik praksis i sektoren fremkommer bl.a. ved at en informant sier at de bevisst bruker risikoanalysene som beslutningsstøtte for tiltak. «*De besluttede security tiltakene er basert på risikoanalyser. Tiltakene blir ikke gjennomført fordi det er kjekt å gjøre det, men fordi det er gjennomført analyse som har påpekt at disse tiltakene vil være med å redusere risikoen»* (Informant 4). Det er kun et fåtall av informantene som oppgir at analysene benyttes som beslutningsstøtte også opp mot mindre arrangementer eller planlagte hendelser. En av informantene forklarer her at «*vi gjennomfører analyser opp mot tilsiktede uønskede hendelser i forbindelse med arrangementer der det er mange studenter til stede, som bl.a. fadderuke og studiestart*» (Informant 4). Vedkommende forklarer at de i forkant av slike arrangementer har gruppemøter hvor de vurderer relevante scenarioer og tilhørende risikoer. Risikoanalysene benyttes da som beslutningsstøtte for egnede tiltak. Samme informant forklarer at de opplever å ha størst utbytte av analysene som foretas opp mot arrangementer som nevnt. De mer overordnede prosessene der mange er involvert medfører ifølge informanten gjerne at en bruker uforholdsmessig mye tid, og at en primært sitter igjen med topphendelser og tilhørende beredskapsplaner. *«Topphendelsene er som regel kjent fra før* og *beredskapsplanene foreligger allerede. Det fremkommer sjelden tiltak eller handlingsplaner som følge av de overordnede ROS-analysene*. *Vi burde heller bruke mer tid på tiltakene, og man merker det på de ansatte at det blir en plage dersom man bruker for mye tid på prosessen før dette*» (Informant 4).

5.8 Ledelsens involvering

De fleste av informantene som benytter analysene som beslutningsstøtte forklarer at de i gjennomføringen av disse har en prosess som involverer større eller deler av organisasjonen, men praksisen varierer også her. En av informantene forklarer at prosessen starter med møter der en rekke ulike hendelser blir presentert, og der det velges ut og sorteres på bakgrunn av diskusjoner. På bakgrunn av dette gjøres en prioritering av anbefalte tiltak, og deretter beslutningsmøte hvor disse tiltakene sendes ut til aktuelle personer i gjeldende del av organisasjonen. Større deler av organisasjonen involveres og det blir laget en tiltaksplan for beslutning, og den igjen blir sendt til oppfølging til ansvarlige personer. En annen av informanten forklarer også at de i prosessen benytter større deler av organisasjonen til å få innspill på type hendelser, og forklarer at dette gir både forankrings- og involveringsprosess. I etterkant av dette har de et større ledermøte hvor man går gjennom risikobildet og vurderer hvordan man skal jobbe videre med dette.

Det varierer i hvilken grad ledelsen er aktive og involvert i risikoanalyseprosessen. En av informantene forklarer at i prosessen så deltar hele den administrative ledelsen, slik at disse er aktivt med. «*Ledelsen har vært med i selve risikoanalyseprosessen, samt bearbeidingen etterpå. Ved røde og gule hendelser går man gjennom for å vurdere hvilke tiltak man bør iverksette»* (Informant 4). Andre informanter forklarer at ledelsen er lite involvert i dette arbeidet. En informant sier følgende: *«Ledelsen involverer seg i liten grad i prosessen rundt analysene». «Jeg får ingen bestilling på hva de ønsker jeg skal komme med av analyser eller hva som er formålet. Foreløpig så er det jeg som tar initiativ og analysene brukes lite som beslutningsstøtte. Det er kommet noen tiltak, men det er ikke godt nok. Det har stoppet litt opp. Jeg skal skissere analysene, de skal ta beslutningene. En god risikoanalyse er rett og slett bare beslutningsstøtte. Forståelse og forankring i ledelsen er helt essensielt, hvis ikke så er arbeidet bortkastet. De må bli vant til at når de skal ta beslutninger så må de ha et beslutningsgrunnlag»* (Informant 6). En annen av informantene forklarer også at involveringen fra ledelsen er begrenset: *«jeg informerer ledergruppen en gang i året, men jeg opplever at interessen er litt fraværende»* (Informant 7).

5.9 Fremstilling og visualisering av risiko

Som det har fremkommet tidligere benytter litt over halvparten av informantene tofaktormodellen. For å fremstille og visualisere resultatene fra risikoanalysene til ett risikobilde benytter de fleste i forlengelsen av denne metodikken en matrise. Flere av informantene forklarer at det er risikomatrisen som legges fram som beslutningsstøtte, i tillegg til at enkelte legger ved en rapport som forklarer de bakenforliggende vurderingene. Informanten som forklarte at de benytter tofaktormodellen når det gjelder safety hendelser og trefaktormodellen opp mot security, forklarer at de fremstiller resultatene i ett risikobilde ved å sammenstille alt i et felles excel dokument. I dokumentet skilles fortsatt safety og security. Risikoene blir visualisert ved trafikklys grønt, gult og rødt. Informanten forklarer at det er dette dokumentet lederne forholder seg til som beslutningsstøtte.

Flere uttrykker at det er utfordringer knyttet til det å visualisere/kommunisere risikobildet og det er ulike synspunkter på hva som er egnet. Flere av de som benytter matrisene hevder at disse ikke kommuniserer risiko godt nok. En av informantene forklarer at det særlig er vanskelig å tilpasse dette til større organisasjoner, og forklarer at hendelser her vil få ulik grad av konsekvens i ulike deler av organisasjonen. *«En påsatt brann vil f.eks. kunne ha enorme konsekvenser for en spesiell avdeling, mens det for andre ikke ville være i nærheten av like alvorlig. Vi har ikke landet på noen god løsning for hvordan kommunisere det helhetlige risikobildet». Det er også vanskelig å kommunisere og skape forståelse for at selv om vi har gått fra rødt til grønt så er ikke risikoen eliminert»* (Informant 3).

Informanten som benytter trefaktormodellen for både safety og security hendelser, svarer følgende på spørsmål om hvordan risikobildet visualiseres eller kommuniseres: *«dette er jo kjernen i det som er vanskelig. Da jeg begynte i stillingen var de andre veldig opptatt av fargekoder og matriser, men det som er viktig er jo begrunnelsene bak disse tallene. Farger er skummelt fordi hjernen din blir så opphengt i dette. Jeg har mer fokus på det skriftlige grunnlaget som beskriver verdier, trussel og sårbarhet. Matrise er enkelt å forstå, men samtidig så kommer ikke vurderingen som ligger til grunn fram og blir synliggjort. Dette fremkommer ved bruk av trefaktormodellen, men denne er igjen vanskeligere å legge fram for ledelsen slik at de forstår det og kan benytte det som beslutningsstøtte»* (Informant 6).

En av informantene forklarer at de benytter matrise til å visualisere risikobildet for både tilsiktede og ikke tilsiktede uønskede hendelser. *«Jeg har tro på grafiske fremstillinger som beslutningsstøtte. «Den grafiske fremstilling viser også effekten av tiltak og deres påvirkning på risikoen»* (Informant 5).

Det er ulik praksis knyttet til om det i tillegg til matriser eller annen visualisering av risikobildet blir skrevet rapporter, som beskriver de bakenforliggende vurderingene i risikoanalysene. En av informantene forklarer at de skriver rapport for å dokumentere disse vurderingene, og forklarer at matrisen bare utgjør en del av rapporten og som en overordnet fremstilling av resultatene fra analysene. Den skriftlige rapporten forklarer også bakgrunn, formål, avgrensning og alt det som er omfattet av analysearbeidet. Det er flere som ikke skriver rapport for å begrunne vurderingene. En av informantene forklarer at de ikke gjør noe skriftlig rundt dette i dag, men «*dette kommer nok framover og vi burde dokumentere med mer beskrivende tekst i fremtiden*» (Informant 4). En annen informant forklarer at trefaktormodellen her er godt egnet fordi du der må skrive ned de vurderingene som er gjort. «*Skriftliggjøring er nødvendig for å vise hvilke vurderinger som ligger til grunn. Det blir mer skrivearbeid, men når noen må sette seg ned å sette ord på ting så blir det så mye lettere å håndtere enn om noen bare setter opp et tall basert på synsing. Når du skriver må du faktisk begrunne det med ord. Her handler det mer om at man må bli gode til å trekke ut det vesentlige og sammenfatte dette til en kort rapport»* (Informant 6).

5.10 Usikkerhet

Som det fremkommer i kapittel 5.9 finner informantene det krevende å visualisere risiko, og det er ulikt syn på hvordan dette bør gjøres. Det er kun en av informantene som eksplisitt nevner at de i rapportene beskriver de bakenforliggende vurderingene som ligger til grunn, i tillegg til at de beskriver usikkerheten som foreligger. Ingen av de øvrige informantene trekker fram usikkerhet som et relevant tema å vektlegge.

5.10 Oppsummering av funn

Alle informantene forklarer at de har fokus på tilsiktede uønskede hendelser i arbeidet med sikkerhet og beredskap ved deres virksomhet, men fokuset har særlig økt de siste årene. Flere

trekker fram at det fortsatt er safety som er gjenstand for hovedfokuset. Ingen av informantene oppgir at det er noe organisatorisk skille mellom safety og security. Det er heller ingen som har egen avdeling eller stillinger som kun er øremerket for å jobbe med security hendelser.

Nesten samtlige benytter risikoanalyser i arbeidet med tilsiktede uønskede hendelser, men det fremkommer noen ulikheter hva gjelder metodikk, kompetanse og beslutningsstøtte. Det varierer i hvilken grad ledelsen er aktive og involvert i risikoanalyseprosessen. Informantene benytter flere kilder for å vurdere trusler og aktuelle scenarioer for tilsiktede uønskede hendelser, og de fleste ser her til offentlig tilgjengelige trusselvurderinger fra ulike instanser. Det foreligger videre et skille der omtrent halvparten benytter tofaktormodellen og den andre halvparten trefaktormodellen. I synet på om det trengs egen metodikk for risikoanalyser av security hendelser svarer flertallet at de ikke ser behovet for en egen tilnærming til dette, og det fremkommer ulikheter i forhold til kompetanse om valg av metodikk blant informantene. De fleste informantene forklarer at analysene særlig er brukt som beslutningsstøtte for å opprette eller oppdatere beredskapsplaner, og det er få som oppgir at de benytter risikoanalysene som støtte for konkrete sannsynlighets- eller konsekvensreduserende tiltak for de aktuelle scenarioene.

De fleste av informantene som benytter tofaktormodellen som metodikk bruker en matrise for å fremstille og visualisere resultatene fra risikoanalysene til ett risikobilde. Det er kun en av informantene som eksplisitt nevner at de i rapportene beskriver de bakenforliggende vurderingene som ligger til grunn, i tillegg til at de beskriver usikkerheten som foreligger. Ingen av de øvrige informantene trekker fram usikkerhet som et relevant tema å vektlegge.

6.0 Diskusjon

En vil i denne delen av studien diskutere teori og empiri opp mot problemstillingen som er valgt for studien. Problemstillingen blir her gjengitt:

Hvordan benytter universiteter og høyskoler i Norge risikoanalyser som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser?

For videre å drøfte teori og empiri opp mot denne tas det utgangspunkt i de tre forskningsspørsmålene.

6.1 Hvordan samsvarer valg av risikoanalysemetodikk i sektoren med anbefalinger i teoretiske bidrag?

Det kan med bakgrunn i resultatene sies at et lite flertall av informantene i sektoren benytter tofaktormodellen, mens den resterende benytter trefaktormodellen når det kommer til risikoanalyser opp mot tilsiktede uønskede hendelser. Den tradisjonelle tofaktormodellen der risiko er produktet av sannsynlighet og konsekvens er en mye brukt forståelse som legges til grunn (Engen et al., 2016, s. 78). Tofaktormodellen har generelt lang tradisjon opp mot ulykker og safety, men bruken øker opp mot også security (Busmundrud et al., 2015, s. 27). Samtidig kan det sies at det i sektoren varierer hvorvidt valgt metodikk og herunder definisjon av risiko er et bevisst valg. Resultatene kan tyde på at informantene i studien i liten grad tar en bevisst vurdering når de velger metodikk opp mot tilsiktede uønskede hendelser, men at mange velger en metodikk med opphav i safety fordi de er godt kjent med denne fra tidligere. Slik Aven hevder er kvaliteten i risikovurderingen i stor grad avhengig av at en er bevisst på hvilken definisjon av risiko som benyttes (2008, s. kapittel 1 og 2). En felles forståelse for risiko er også avgjørende når det skal tas beslutninger (Aven, 2008, Kapitler 1 og 2).

Selv om omtrent halvparten av informantene benytter trefaktormodellen er det flere av dem som tar til orde for at denne er noe mer utfordrende å benytte. Det blir påpekt at den krever en viss grad av modenhet og kunnskap. Flere ser det som en fordel at denne metodikken grundig identifiserer både verdi, trussel og sårbarhet, hvilket gjør den egnet til å identifisere tilsiktede uønskede hendelser. FFI forklarer at fasen for objektkartlegging og verdivurdering er av vesentlig betydning, ettersom den bidrar til å kartlegge sensitiv informasjon eller andre verdier som er særlig viktig å beskytte (Busmundrud et al., 2015, s. 28). Disse elementene

kommer ifølge flere av informantene ikke like eksplisitt til uttrykk i tofaktormodellen. Det er samtidig flere som påpeker at trefaktormodellen er vanskeligere å benytte i den daglige driften.

For å ivareta elementene verdi, trussel og sårbarhet er det en av informantene som forklarer at de implementerer dette inn i tofaktormodellen. Hensikten med det er at de bevisst ikke ønsker å ta i bruk en metodikk som er ukjent for mange, men at de opp mot tilsiktede uønskede hendelser ser det som vesentlig at disse begrepene blir vurdert i analysene. Samme informant vektlegger at det er prosessen som er av betydning, og ikke valg av metodikk i seg selv. Det kan argumenteres for at dette er en fornuftig tilnærming, og det er viktigere at prosessen tilpasses den enkelte virksomhet fremfor at noen blir påtvunget å benytte en gitt metodikk. Forsvarsbygg argumenterer i sin forskning for at det er godt dokumentert at det ikke foreligger noen omforent anbefalt metodikk, og at ikke valg av metodikk i seg selv bør være det som har størst betydning (Busmundrud et al., 2015, s. 70).

Selv om det ikke foreligger en omforent praksis i forhold til valg av metodikk i sektoren, kan en altså argumentere for at det er prosessen og valg av en god tilnærming som er av størst betydning. Det er som nevnt en pågående revisjon av NS 5814 standarden og denne utformes slik at både tilsiktede og utilsiktede hendelser kan vurderes etter denne (Norge, 2020). Revisjonen er ikke endelig, men det er grunn til å argumentere for at denne vil kunne være et viktig bidrag til at sektoren kan vurdere en mer enhetlig tilnærming til risikovurderinger av både safety og security hendelser.

Studien tyder på at det er store skiller hva gjelder kompetanse om risikoanalyser, og særlig av tilsiktede uønskede hendelser. Enkelte virksomheter har egne ansatte som er eksperter på risikoanalyser, mens andre sitter mer alene med gjennomføringen og erkjenner at de har for lite kompetanse på dette feltet. Det er svært få av informantene som trekker fram begrepet usikkerhet som et viktig moment i risikovurdering av tilsiktede uønskede hendelser. Det kan tyde på at det er manglende kunnskap i sektoren knyttet til dette. Det kan i forlengelsen av det argumenteres for at manglende fokus på usikkerhet gjør at sektoren ikke er nok fremover lent. De vil med det vanskelig kunne klare å ta inn over seg nye og ukjente trusler. Slik Jore

forklarer vil risikovurderinger alltid omfattes av usikkerhet, men denne er særlig tilstede innenfor security (Jore, 2019, s. 8). Det er ikke kjent hvordan det neste angrepet vil være, og usikkerheten knyttet til hvem, hva, hvor, hvordan og når bør beskrives. Sannsynlighet kan benyttes som verktøy, men bakgrunnskunnskapen og usikkerhet bør kommuniseres (Aven, 2008, kapittel 2). For å unngå at en overser uforutsette og potensielle overraskelser er det viktig at en har et bredere perspektiv enn det å basere seg på sannsynligheter. Vektlegging av usikkerhet og bakgrunnskunnskap er her et viktig bidrag (Aven & Krohn, 2014, s. 2). Å inkludere vurderinger knyttet til usikkerhet inn i risikovurderinger av security hendelser, herunder planlegging, vil være av vesentlig betydning (Askeland et al., 2017, s. 202).

Det kan også argumenteres for at det er manglende kunnskap om prosessen rundt gjennomføring av risikoanalyser av tilsiktede uønskede hendelser. Der noen involverer større deler av organisasjonen, er det andre som mer eller mindre gjennomfører analyser på egenhånd. FFI hevder at en god tilnærming til risikoanalyseprosessen kjennetegnes ved at *«den er strukturert, etablerer en arbeidsgruppe med bred kompetanse, kartlegger kunnskapsstyrken, er basert på systemforståelse og er konkret, har et helthetlig perspektiv, kommuniserer risiko og usikkerhet, er gjennomsiktig, sporbar og etterprøvbar»* (Busmundrud et al., 2015, s. 71).

Det er ingen av informantene som eksplisitt trekker fram at det i risikoanalyseprosessen er vesentlig å avklare hva som er formålet med analysen. Risikoanalyseprosessen består av de tre fasene planlegging, risikovurdering (gjennomføring) og risikohåndtering (bruk), og det er i planleggingsfasen at formålet med analysen må avklares. Ettersom dette er mangelfullt i sektoren kan en slik Aven forklarer hevde at analysene sin funksjon som beslutningsstøtte blir svekket (Aven, 2008, s. 43). «*Hvordan analysen og dens resultater skal brukes i beslutningsprosessen må være tydelig»* (Aven, 2008, s. 45). Slik en av informantene forklarte kan bow-tie modellen kunne sies å være et egnet hjelpemiddel for ledelsen, til å tydeliggjøre hva analysen skal belyse og hva det ønskes beslutningsstøtte til. I modellen tas det utgangspunkt i de initierende hendelsene, samt tilhørende årsaker og konsekvenser. Bow-tie kan således sies å være en enkel fremstilling som kan brukes også for å illustrere hvilken del av denne som er formålet med analysen. I risikoanalyseprosessen vil dessuten det å

identifisere initierende hendelser ha stor betydning, og Aven hevder at *«det du ikke har identifisert, kan du ikke håndtere» (2008, s. 55).*

Aven forklarer at avklaring av formålet med analysen har betydning for både valg av metodikk, organisering av arbeidet og ressursbruk (Aven, 2008, s. 44). Flere av informantene i studien trekker frem at det ofte brukes for mye tid på å diskutere det som omtales som korrekt nivåsetting av konsekvens og sannsynlighet. I følge Aven brukes det ofte mest tid på selve gjennomføringen av risikovurderingen (2008, s. 44). Funn i studien tyder på at sektoren kan fokusere mer på hvordan de fordeler tid og ressurser i risikoanalyseprosessen, og med det bruke mer tid på planlegging og risikohåndteringen. Aven forklarer at en fordeling der tidsbruken mellom de tre fasene planlegging, risikovurdering og risikohåndtering fordeles ved 1/3 i hver, vil gi en mer balansert prosess (2008, s. 44).

6.2 Skilles det mellom safety- og security hendelser i forhold til valg av metodikk?

Det er ingen av informantene som ser behovet for å skille de to områdene rent organisatorisk, og det blir trukket fram at det er viktig å være bevisst på at tiltak opp mot security også vil kunne få betydning for safety. Det at tiltak opp mot de to feltene påvirker hverandre, er i tråd med det Jore bl.a. forklarer at man skal være oppmerksom på (2019, s. 11). Flere av informantene påpeker riktignok at det er et viktig skille mellom safety og security, ettersom det er mindre tilgjengelig datagrunnlag for tilsiktede uønskede hendelser. Slik en av informantene forklarte det så brukes det mye tid på å diskutere korrekt grad av sannsynlighet og konsekvens opp mot security hendelser, selv om man ofte har et relativt tynt grunnlag med data tilgjengelig å vurdere dette på. Kvantitative metoder har generelt blitt mer benyttet opp mot safety enn security, og Aven et.al. forklarer at et godt grunnlag for å risikovurdere security hendelser bør bestå av kvalitative metoder i kombinasjon med vurderinger fra eksperter (Aven & Renn, 2009). Data som kan være egnet er ofte ikke tilpasset den enkelte virksomheten, slik en finner innen safety, og består i stor grad av mer overordnede trusselvurderinger på et generelt nivå i samfunnet (Jore, 2019, s. 8). Kvalitative vurderinger bør inngå ettersom det er vanskelig å beregne en trusselaktørs intensjon og kapasitet (Busmundrud et al., 2015, s. 29). En kan derfor med bakgrunn i noe ulikt behov og tilgang på data, argumentere for at det er hensiktsmessig å skille mellom safety og security i forhold til valg av metodikk.

De fleste informantene bruker samme metodikk for både safety og security hendelser, og svært få benytter med det egen metodikk opp mot tilsiktede uønskede hendelser. Flere vektlegger at det er ønskelig at metodikken som benyttes er gjenkjennbar både for de som gjennomfører og de som skal benytte analysen som beslutningsstøtte. Man ønsker derfor å benytte samme metodikk for begge hendelsestypene. Det kan også argumenteres for at det å benytte ulik metodikk vil medføre økt bruk av ressurser i gjennomføringen ettersom dette kan kompliserer arbeidet. Slik vi har sett forklarer Aven at det er i selve gjennomføringen av risikovurderingen det ofte brukes uforholdsmessig mye ressurser (2008, s. 44). Det kan med det påstås at en felles metodikk vil kunne sikre en mer effektiv prosess og herunder ressursbruk. Som nevnt er NS 5814 standarden under revisjon og ettersom denne har som mål å være egnet til å risikovurdere både safety og security hendelser, vil en ha grunn til å tro at denne kan vurderes av sektoren som felles metodikk. Forskjellig metodikk kan sies å medføre en risikostyring som ikke gir en enhetlig tilnærming (Jore & Egeli, 2015, s. 810). Det kan dessuten argumenteres for at en enhetlig tilnærming i UH-sektoren vil kunne styrke den totale kompetansen på området.

Funnene i studien kan riktignok tyde på at informantene ikke er så opptatt av metodikk i seg selv, men at dette må tilpasses den enkelte virksomhet. Informantene kan med det sies å ikke være av den oppfatning at security på grunn av sin særegenhet trenger egen tilnærming, slik flere forskere har argumentert for i debatten rundt dette (Amundrud et al., 2017). Selv om det kan argumenteres for at det ikke er behov for egen metodikk kan det sies at det her er viktig å være fleksibel. Slik informantene forklarer er fokuset på tilsiktede uønskede hendelser i sektoren av relativt nyere dato, og kom særlig med nye føringer fra KD etter 22. juli. Trefaktormodellen vokste fram nettopp i etterkant av disse hendelsene, ettersom det medførte økt fokus på å beskytte seg mot tilsiktede uønskede hendelser (Jore & Egeli, 2015, s. 808). Det kan med det hevdes at sektoren bør være mer åpne for å vurdere en egen metodikk rettet mot security hendelser, nettopp på grunn av sin særegenhet. Om valg av metodikk forklarte en av informantene at de har en bevisst metodikk, *«men båten blir til mens vi ror»* (Informant 3). Det kan sies å være en fornuftig tilnærming og det kan være at man i for stor grad er tro mot en metodikk fordi den har sterkere forankring og bakgrunn. Security og beskyttelse mot tilsiktede uønskede handlinger er et område som er gjenstand for økt fokus og herunder forskning, men fortsatt er safety i større grad en etablert vitenskap (Jore, 2019, s. 2). Legger en til grunn security som særegent kan en her argumentere for at en bør skille safety og

security metodikk etter hvert som man ror båten videre. Flere forskere ser behovet for å gjøre et skille her når det gjelder risiko og krisehåndtering (Boholm et al., 2016).

Videre er vurdering av sannsynlighet og relevante scenarioer momenter som informantene trekker frem som krevende i forhold til valg av metodikk opp mot security. Dette kan nok sies å være kjernen i det som er vanskelig. Slik det tidligere er nevnt forklarer Jore at det i risikoanalyser av security hendelser vil være stor usikkerhet (2019, s. 8). Jore og Egeli forklarer at trefaktormodellen skiller seg ut ved at den ikke eksplisitt uttrykker sannsynligheten for en hendelse (2015, s. 808). I denne studien tyder det på at de fleste av informantene uttrykker at bruk av sannsynlighet forenkler fremstillingen, og noen få hevder at det ikke er egnet å snakke om sannsynlighet innenfor security. Til sammenlikning viser studier fra petroleumssektoren hvor man har god erfaring innen safety, at de også er positive til å benytte sannsynlighetsbegrepet opp mot security, gitt at denne er basert på subjektive vurderinger og tilgjengelig bakgrunnskunnskap (Jore & Egeli, 2015, s. 810). Det kan like fullt argumenteres for at vurderingene knyttet til sannsynlighet og usikkerhet opp mot safety og security innebærer så ulikt utgangspunkt, at det for å ivareta dette bør skilles mellom de to områdene når det kommer til valg av metodikk.

Samtidig kan en reflektere over hvorvidt informantene har en klar forståelse av hva security hendelser omfatter. Det ble stilt spørsmål om dette innledningsvis i intervjuene, og svarene kan tyde på at informantene ser på security hendelser som primært skoleskyting og terror. Slik Jore forklarer kan security trusler forekomme på mange måter og nivåer, og det gjelder ikke bare terrorisme. Security omfatter også mer tradisjonell kriminalitet som innbrudd, tyveri og skadeverk (2019, s. 7). Det kan med det argumenters for at det er mangelfull kunnskap og forståelse for hva security er i sektoren. Et bredere security perspektiv taler for at det kan være behov for en mer spisset metodikk for å analysere hendelser der trusselaktøren har en ondsinnet vilje. For UH-sektoren vil kanskje bruk av trefaktormodellen med en prosess der en tar utgangspunkt i verdiene kunne gi et større spekter av identifiserte security hendelser. Ingen av informantene har f.eks. trukket fram forskning som en verdi. Det fremkommer tydelig av PST sin trusselvurdering av 2020 at en må forvente at utenlandske etterretningstjenester retter sin spionasje bl.a. mot forskning og utvikling.

En kan med bakgrunn i diskusjonen i dette kapittelet hevde at det i sektoren ikke klart skilles mellom safety og security i forhold til valg av metodikk.

6.3 Fungerer metodikk opp mot safety og security forskjellig i forhold til det å støtte beslutninger?

Det mest sentrale i studien er hva risikoanalysene faktisk brukes til. Målet med en risikoanalyse er at denne skal kartlegge og beskrive risiko, og med det utgjøre beslutningsstøtte. I det ligger det at den skal presentere et risikobilde (Aven, 2008, s. 13). Resultatene tyder på at dette praktiseres noe ulikt i sektoren. I forhold til valg av metodikk foreligger det som nevnt en deling, der flesteparten av informantene benytter tofaktormodellen og presenterer/visualiserer risikoen ved bruk av en risikomatrise. Slik flere av informantene også gjør, kan en argumentere for at dette er en lite komplisert metodikk. Fremstilling av risiko gjøres på en enkel måte, som er lett forståelig og kjent for de fleste parter involvert i risikoanalyseprosessen. En kan med det hevde at tofaktormodellen, som har sitt opphav fra safety metodikk (Busmundrud et al., 2015, s. 27), i større grad fungerer og blir brukt som beslutningsstøtte opp mot security hendelser i UH-sektoren. På denne måten kan det altså tyde på at de to metodikkene fungerer forskjellig i forhold til det å støtte beslutninger.

En av grunnene til at matrisen blir foretrukket kan være at denne blir benyttet som eksempel for fremstilling av risiko i styringsdokumentet for samfunnssikkerhet og beredskap i UH-sektoren (KD, 2019, s. 35). Samtidig er ikke UH-sektoren alene om å benytte matrisen, og studien til FFI viser at denne blir brukt av mange. Den kan sies å være en enkel fremstilling av risiko ut fra tallverdier for konsekvens og sannsynlighet (Busmundrud et al., 2015, s. 31). En vil ved å bruke en matrise kunne nivåsette risikoen ut i fra disse to faktorene, og på denne måten visualisere resultatene fra risikoanalysen. Fargeinndelingen er enkel å forstå og kan tilpasses virksomheten ut fra hvilke risikoakseptkriterier de har satt (Busmundrud et al., 2015, s. 31). Slik den ene informanten som bruker matrise for fremstilling av både utilsiktede og tilsiktede hendelser sier, kan en argumentere for at grafiske fremstillinger er oversiktlig og i tillegg viser effekten av tiltak og deres påvirkning på risikoen. En kan med det hevde at tofaktormodellen og tilhørende bruk av matrise legger til rette for et lett forståelig risikobilde, hvilket gjør at denne metodikken i stor grad fungerer som beslutningsstøtte.

Like fullt kan en argumentere for at matrisene, slik en annen av informantene forklarte, ikke kommuniserer godt nok. En rekke avdelinger i en virksomhet kan være svært ulike, slik at scenarioer som kommer høyt ut for noen avdelinger, er lite relevant for andre i virksomheten. Dette kan gjøre det vanskelig å kommunisere det helhetlige risikobildet ved bruk av matrise. En kan også argumentere for at vi mennesker blir lett påvirket av farger, og risikoer som kommer ut i fargen rødt kan gjerne få for ensidig fokus og for høy prioritet. Nettopp dette med å fremstille og kommunisere risikoen visuelt kan sies å være kjernen i det som er krevende. Funn i studien tyder på at informantene finner det krevende å kommunisere risiko. FFI hevder at de to metodikkene har særlig og felles svakhet når det kommer til dette punktet (Busmundrud et al., 2015, s. 64). Informantene er delt i hvilken metodikk som er best egnet, men uttrykker i begrenset grad at de har noe særlig sterke preferanser. Der noen er tilhenger av matrisen for å kommunisere risiko er andre tilhenger av trekanten.

Som en del av kommunikasjon av risiko er det ingen av informantene som eksplisitt uttrykker viktigheten av usikkerhet, og dette kan argumenteres for som empiri i seg selv. Vurderinger av usikkerhet bør fremkomme i risikovurderinger av security hendelser (Askeland et al., 2017, s. 202). Dette er krevende ettersom security hendelser skjer sjelden, og beslutninger blir gjerne tatt på bakgrunn av ekspertuttalelser (Askeland et al., 2017, s. 198). Slik Aven forklarer er det viktig at forutsetninger og bakgrunnskunnskap som ligger til grunn fremkommer i analysene. Det er av betydning ettersom det kan forekomme feil, eller analysen rett og slett er basert på svært begrenset grad av kunnskap (Aven, 2015, s. 43). En kan med det argumentere for at trefaktormodellen slik den gjennomgås i kapittel 3.5.3, foretar en mer systematisk gjennomgang av de bakenforliggende faktorene og vurderingene som ligger til grunn, enn det tofaktormodellen gjør. Det kan altså sies at trefaktormodellen i større grad ivaretar og fungerer som beslutningsstøtte når det gjelder usikkerhet i security hendelser. Samtidig fremkommer det heller ikke i denne tilnærmingen en eksplisitt vurdering av bakgrunnskunnskapen. En fremstilling av dette ville gitt muligheten til å gjøre gode vurderinger av risikoer der f.eks. høy bakgrunnskunnskap innebærer lav usikkerhet, og der lav bakgrunnskunnskap medfører høy usikkerhet (Askeland et al., 2017, s. 197).

Det er dessuten grunnlag for å hevde at det som ligger bak vurderingene faktisk er viktigere å få fram, enn akkurat hvordan risikoen blir fremstilt rent visuelt. Slik den ene informanten

forklarte «*så er jo begrunnelsene bak disse tallene og vurderingene det som er viktig».* Matrisen kan sies å være enkel å forstå, men like fullt så kan det fort være at vurderingene som ligger til grunn blir gjenstand for lite fokus. Slik Aven hevder er det i presentasjonen av risikobildet vesentlig at også usikkerheten og bakgrunnskunnskapen som ligger til grunn blir dokumentert og kommunisert (Aven, 2008, s. 61–65). Det at en del matriser i liten grad kommuniserer usikkerhet kan gjøre at beslutningstaker tror det er mindre usikkerhet knyttet til resultatet enn det som er virkeligheten (Busmundrud et al., 2015, s. 37).

Flere av informantene benytter trefaktormodellen, men har ikke funnet noen god måte å presentere risikobildet på. FFI finner at det er særlig når risikobildet skal presenteres at de to metodikkene har sine svakheter (Busmundrud et al., 2015, s. 64). En kan slik det er nevnt argumentere for at trefaktormodellen i større grad får fram de bakenforliggende vurderingene som ligger til grunn, men at dette igjen kan være vanskeligere å fremstille grafisk i et risikobilde. Et grafisk fremstilt risikobilde vil kunne gjøre det lett forståelig for beslutningstaker og dermed egnet som beslutningsstøtte. Trekanten som ofte blir brukt illustrerer bare de faktorer som er benyttet og kommuniserer ikke usikkerhet (Busmundrud et al., 2015, s. 37). FFI anbefaler at usikkerheten knyttet til de ulike vurderingene blir kommunisert, men at det å fremstille usikkerheten visuelt slik at det gir god beslutningsstøtte er kjernen i det som er krevende i denne sammenheng (Busmundrud et al., 2015, s. 45). En kan med det hevde at den største forskjellen mellom metodikkene er hvordan de kommuniserer og presenterer risikobildet, og slik informantene i studien forklarer er det ulike oppfatninger om hva som her er best egnet. Dette tyder på at safety og security metodikk fungerer forskjellig i forhold til det å støtte beslutninger, men dette avhenger slik det fremgår bl.a. av informantenes preferanser og kompetanse.

Så det store spørsmålet blir hvordan en skal fremstille og kommunisere risiko slik at det er egnet og forståelig som beslutningsgrunnlag. NSM forklarer at *«Presentasjon av risiko bør bestå av en visuell fremstilling som gir oversikt, supplert av en rapport som viser forutsetninger og detaljerte vurderinger av hver enkelt risiko»* (2016, s. 23). En kan forklare flere måter å gjøre dette på, både ved bruk av diagrammer, figurer m.m. For UH-sektoren kan en argumentere for at målet ikke trenger å være at alle presenterer risiko på samme måte, ettersom dette bør tilpasses den enkelte virksomheten eller den enkelte avdeling. NSM trekker

her fram at det også bør tilpasses beslutningstakeren og den måten den eller de ellers er vant til å få presentert risikobildet på (NSM, 2016, s. 23). Sett fra dette perspektivet kan en derfor hevde at de to metodikkene ikke har særlig ulik funksjon i forhold beslutningsstøtte, men at de kan ha størst effekt dersom metodikken som benyttes opp mot security hendelser er kjent fra tidligere.

En kan like fullt argumentere for at trefaktormodellen er mer egnet opp mot security hendelser, hvilket ofte innebærer usikkerhet, ettersom metodikken i større grad får fram de bakenforliggende vurderingene som er gjort. Det fordrer at de som utfører analysene skriver gode rapporter, samt at ledelsen setter seg grundig inn i det som blir fremstilt. Utfordringen for sektoren kan imidlertid være at trefaktormodellen er noe mer ukjent for ledelsen og generelt mindre illustrativ. Det kan argumenteres for at det er gjeldende også for UH-sektoren. En må kanskje her i større grad fristille seg fra enkle matriser med fine farger, og heller fokusere på rapportene i sin helhet. FFI anbefaler at beslutningstaker setter seg inn i den totale risikovurderingen, som også innebærer forutsetninger, antakelser, vurderinger og usikkerheter, og ikke bare nøye seg med å se på risikomatrisen eller en annen type fargekart (Busmundrud et al., 2015).

Det er få av informantene som forklarer at det utarbeides en mer utfyllende rapport, som dokumenterer de vurderingene som blir gjort for å komme fram til risikobildet. NSM forklarer at slike rapporter er viktig for at en bl.a. skal ha mulighet til å etterprøve de vurderingene som er gjort (NSM, 2016, s. 23). Selv om få av informantene dokumenterer i rapport form, så erkjenner de fleste at dette vil være en god tilnærming for å synliggjøre vurderingene som ligger til grunn for presentert risikobilde. En kan også hevde at risikobildet bør presenteres slik NSM anbefaler, ettersom det er dette som danner grunnlaget for beslutningsstøtte og risikohåndteringen. Det er på bakgrunn av presentert risiko at beslutningstaker kan vurdere hvordan en skal håndtere risikoen og med det velge egnet strategi (NSM et al., 2015, s. 23). Slik Aven forklarer det er hensikten med risikoanalyser at de skal resultere i et presentert risikobilde, og herunder fungere som beslutningsstøtte (Aven, 2008, s. 15). FFI understreker også dette ved å si at *«det er avgjørende i begge tilnærmingene at resultatet må dokumenteres og kommuniseres i en skriftlig rapport som grunnlag for beslutninger»* (Busmundrud et al., 2015, s. 65). En kan med det si at en har gode argumenter for at risikovurderingen bør

tydeliggjøres i en mer utfyllende rapport, som går lenger enn å bare sette opp en matrise. Det kan argumenteres for at dette er avdekket som et forbedringspotensial i sektoren, og at således trefaktormetodikken i større grad ivaretar dette momentet.

Når det videre gjelder om risikoanalysene benyttes som beslutningsstøtte, kan det tyde på at de primært blir brukt til å utarbeide beredskapsplaner for ulike scenarioer. En av informantene forklarer bl.a. at det i forbindelse med et prosjekt der det er oppført et nytt bygg, så er det kun gjennomført risikoanalyser opp mot safety og ikke security hendelser. Enkelte av informantene erkjenner også at analysene i stor grad blir gjennomført fordi det er et krav fra KD om å gjøre dette. Aven forklarer at mange gjennomfører risikoanalyser for å oppfylle krav fra myndighetene, og hevder at det er lite gunstig dersom det er dette som er motivasjonen for å gjennomføre slike. Det medfører at potensialet i resultatene ikke blir utnyttet til det fulle (Aven, 2008, s. 16). «*Poenget med en risikoanalyse er å gi et underlag for å kunne ta gode beslutninger»* (Aven, 2008, s. 16). Funn i studien kan tyde på at resultatene i mindre grad blir brukt i forhold til å vurdere tiltak som kan redusere risikoen. Resultater fra risikoanalyser vil kunne sies å være egnet for å sammenlikne ulike tiltak og herunder hvilken effekt de får på risikoen (Aven, 2008, s. 15). Riktignok er variasjonen stor blant en del av informantene, der en erkjenner at det kun blir gjort fordi det er et pålagt krav, mens en annen forklarer at de i tillegg til å utarbeide beredskapsplaner også bruker dette til å vurdere tiltak opp mot kommende arrangementer m.m.

Samtidig kan en si at en ikke burde se på en risikoanalyse som noen form for fasit, da det er en rekke ulike vurderinger som ligger til grunn. Aven understreker dette ved å si at analysene ikke gir beslutningene i seg selv, men gir et grunnlag for at beslutninger kan tas (2008, s. 70). Å vurdere tiltak knyttet til tilsiktede uønskede hendelser vil ofte innebære krevende avveininger mellom bl.a. sikkerhet, økonomi, etikk m.m. Det er her risikoanalysene er tiltenkt å komme til sin rett, ved å komme fram til beslutninger som ivaretar denne balansen, i tillegg til at virksomhetens øvrige mål oppnås på best mulig måte (Aven, 2008, s. 16).

En kan argumentere for at det å gjennomføre risikoanalyser av mulige tilsiktede uønskede hendelser kan gi god beslutningsstøtte, opp mot bl.a. planlagte arrangementer der det samles

mange mennesker. I mangel av å gjøre dette vil en ikke få identifisert initierende hendelser eller vurdert sannsynlighets- eller konsekvensreduserende tiltak, som kan ha betydning for sikkerheten ved arrangementet. Den ene informanten forklarte at de gjør dette ved å gjennomføre møter i forkant hvor de diskuterer risikoen og vurderer tiltak. Aven forklarer at det er risikoanalysen og diskusjonen knyttet til resultatene av disse, som skal gjøre at det kan etableres et risikobilde med påfølgende risikohåndtering og tiltak for enten å redusere, optimalisere, overføre eller beholde risiko (Aven, 2008, s. 20). Her vil altså ikke nødvendigvis valg av metodikk være avgjørende for i hvilken grad dette arbeidet fungerer som beslutningsstøtte.

Dessuten kan en som tidligere nevnt argumentere for at det brukes for mye tid på selve risikovurderingen, i stedet for håndteringen der tiltakene inngår. Den ene informanten var tydelig på dette ved å forklare at ofte brukes det mye tid der hele organisasjonen involveres i risikoanalyser, men der en gjerne ikke sitter igjen med annet enn såkalte topphendelser som man kjente til fra før. Som eksempel kan man si at det er en viss sannsynlighet for at PLIVO kan ramme UH-sektoren. Men det viktige er kanskje heller å få på plass tiltakene for å redusere risikoen, enn å bruke mye tid å presentere et korrekt risikobilde der analyser krever mye ressurser. Aven forklarer at erfaring tilsier at det er risikovurderingen som er fasen hvor det normalt brukes mest tid, og for lite går til planlegging i forkant og selve håndteringen av risikoen i etterkant. Det er fasen for risikohåndtering der analysene faktisk blir brukt som beslutningsstøtte (2008, s. 44). Som en har sett i teorikapittelet er trefaktormodellen en relativt omfattende prosess som vil kreve en del tid og ressurser, samt høyere grad av kompetanse og opplæring. En kan med det argumentere for at tofaktormodellen vil være mer effektiv til bruk i sektoren, og på denne måten i større grad fungere som beslutningsstøtte. Her vil som nevnt revisjonen av standarden NS 5814 kunne være et viktig bidrag.

Med bakgrunn i argumentasjonen ovenfor kan en hevde at safety og security metodikk har hver sine styrker og svakheter, og at totalt sett fungerer de relativt likt i forhold til det å støtte beslutninger. Safety metodikk og matrise er enkelt og kjent, men får i mindre grad frem de bakenforliggende vurderingene. Security metodikk ved trefaktormodellen blir på en måte motsatt, der metodikken i større grad dokumenterer disse vurderingene. Samtidig er den mer ukjent for noen og på den måten i mindre grad egnet som beslutningsstøtte for ledelsen.

Informantene har ulik kunnskap og erfaringer, og med det ulike preferanser hva gjelder metodikk. Det viktigste er ikke valg av metodikk, men at dette tilpasses den enkelte sektor eller virksomheten. Det er prosessen som legger grunnlag for god beslutningsstøtte.

7.0 Konklusjon

Studien viser at UH-sektoren i løpet av de siste årene har økt sitt fokus på å forebygge uønskede tilsiktede hendelser. Dette har medført at en i større grad erkjenner risikoen og gjennomfører risikoanalyser som et ledd i dette arbeidet. Slik det er redegjort for i studien er det et krav at virksomhetene som er underlagt kunnskapsdepartementet gjennomfører slike.

Hensikten med studien har vært å belyse hvordan universiteter og høyskoler benytter risikoanalyser for å beskytte seg mot tilsiktede uønskede hendelser.

Før en konkluderer rundt problemstillingen i sin helhet vil konklusjoner opp mot forskningsspørsmålene bli presentert.

1. Hvordan samsvarer valg av risikoanalysemetodikk i sektoren med anbefalinger i teoretiske bidrag?

Studien viser at omtrent halvparten av informantene benytter tofaktormodellen og andre halvparten trefaktormodellen opp mot tilsiktede uønskede hendelser. Det varierer noe i hvilken grad valg av metodikk er et bevisst valg. Det er her av stor betydning for kvaliteten i risikovurderingen at en har klart for seg hvilken definisjon som legges til grunn. Risikoen skal uttrykkes og presenteres for både beslutningstakere og ulike interessenter, og det er av betydning at en har felles forståelse av begrepet risiko for å kunne ta gode beslutninger (Aven, 2008, Kapitler 1 og 2). Studien viser at det er store skiller blant informantene hva gjelder hvilken kompetanse og ressurser de mener å ha i forhold til både vurdering og bruk av metodikk, særlig opp mot security hendelser. Det bekrefter det inntrykket KD har av at det foreligger noe usikkerhet mht. hvordan den enkelte virksomhet kan lage en god og hensiktsmessig risikovurdering.

Det er svært få av informantene som har fokus på usikkerhet i risikoanalysene og det er mangelfullt i hvilken grad vurderinger rundt dette blir dokumentert. Det er særlig usikkerhet

knyttet til risikovurderinger innenfor security (Jore, 2019, s. 8), og usikkerhet er et vesentlig moment som må beskrives i risikoanalyser (Aven, 2008, s. kapittel 2).

2. Skilles det mellom safety- og security hendelser i forhold til valg av metodikk?

Studien viser at det ikke er organisatoriske skiller mellom safety og security i UH-sektoren, og det benyttes i stor grad samme metodikk opp mot disse hendelsene. Fordelene ved en felles metodikk er at det blir gjenkjennbart for alle som er involvert, herunder beslutningstaker. Det vil kunne være ressursbesparende at safety og security vurderes i samme prosess, og det vil bli krevende for mange å implementere en ny metodikk blant ansatte som er godt innarbeidet i en opprinnelig valgt metodikk. De to feltene henger også tett sammen ved at ulike tiltak medfører konsekvenser som gjensidig påvirker hverandre. Forskjellig metodikk vil kunne medføre en risikostyring som ikke gir en enhetlig tilnærming (S. H. Jore & Egeli, 2015, s. 810).

3. Fungerer metodikk opp mot safety og security forskjellig i forhold til det å støtte beslutninger?

Studien viser at risikoanalysene i liten grad blir benyttet som beslutningsstøtte opp mot tiltak eller handlingsplaner, men primært til å utvikle og oppdatere beredskapsplaner. Analysene er med det lite brukt som underlag for konkrete sannsynlighets eller konsekvensreduserende tiltak. Noen få av informantene erkjenner at analysene blir gjennomført fordi dette er et krav fra KD.

I forbindelse med presentasjon og kommunikasjon av risiko er det å fremstille usikkerhet og risikobilde visuelt en av utfordringene for sektoren. Formidling av risikobildet er vurdert som svakhet ved begge metodikkene. De fleste som benytter tofaktormodellen tar i bruk matrisen, men denne kan medføre at de bakenforliggende vurderingene ikke fremkommer tilstrekkelig, samt at matrisen ikke kommuniserer usikkerhet. Det kan resultere i at beslutningstaker får en oppfatning av at det er lavere usikkerhet knyttet til resultatet enn det som er realiteten. De som benytter trefaktormodellen har ikke funnet en egnet måte å presentere risikobildet på.

Safety og security metodikk har hver sine styrker og svakheter, og totalt sett fungerer de relativt likt i forhold til det å støtte beslutninger. Safety metodikk og matrise er enkel og mer kjent, men får i mindre grad frem de bakenforliggende vurderingene. Security metodikk ved trefaktormodellen blir på en måte motsatt, der metodikken i større grad dokumenterer disse vurderingene. Samtidig er den mer ukjent og på den måten i mindre grad egnet som beslutningsstøtte for ledelsen. Informantene har ulik kunnskap og erfaring, og med det ulike preferanser hva gjelder metodikk. Det viktigste er ikke valg av metodikk, det er prosessen som legger grunnlag for god beslutningsstøtte.

Hvordan benytter universiteter og høyskoler i Norge risikoanalyser for å sikre seg mot tilsiktede uønskede hendelser?

Dette er oppgavens problemstilling og konklusjonen blir her at risikoanalysene primært blir brukt for å opprette og vedlikeholde beredskapsplaner, og i mindre grad som beslutningsstøtte opp mot tiltak eller handlingsplaner direkte rettet mot tilsiktede uønskede hendelser. De blir også i liten grad benyttet til dette formålet opp mot kommende og planlagte hendelser som arrangementer m.m. Det er varierende kompetanse i sektoren knyttet til metodikk, gjennomføring og bruk av risikoanalyser for å beskytte seg mot tilsiktede uønskede hendelser. Den nylig reviderte versjonen av NS 5814 er utformet slik at både tilsiktede og utilsiktede hendelser kan vurderes, og det antas at denne vil være et viktig bidrag til at sektoren kan vurdere en enhetlig og effektiv metodikk.

I risikoanalyseprosessen mangler en avklaring av hva som er formålet med analysene. For at analysen skal utgjøre god beslutningsstøtte er det av stor betydning at det er avklart hvilke svar en ønsker at analysen skal gi (Aven, 2008, s. 43). Formålet bør avklares i planleggingsfasen og det kan heller benyttes noe mindre tid i fasen for risikovurdering. En jevnere fordeling av tidsbruken i risikoanalyseprosessen vil gi en mer balansert prosess i UH-sektoren.

7.1 Anbefaling

De ulike virksomhetene i sektoren bør ha større fokus på hva som er formålet med risikoanalysene som blir gjennomført. Dette vil sikre et bedre samspill og forståelse mellom

beslutningstaker og de som gjennomfører analysene. For at tidsbruken i risikoanalyseprosessen skal gi en mer balansert prosess bør avklaringen av formålet som en del av planleggingen således tillegges mer tidsbruk.

Det bør i større grad fokuseres på at usikkerheten som foreligger opp mot de ulike security hendelsene blir kommunisert. Risikoanalysene bør fremstilles i en helhetlig rapport der også fremgangsmåte, bakgrunnskunnskap og metodikk beskrives. I forlengelse av analysene bør disse i større grad benyttes som beslutningsstøtte for sannsynlighets- og konsekvensreduserende tiltak, opp mot de uønskede tilsiktede hendelsene som blir identifisert. Her bør det ikke bare fokuseres på de hendelsene som vurderes til middels eller høy, slik KD ønsker (Kunnskapsdepartementet, 2019, s. 19). Det kan med fordel også etableres en praksis der det gjennomføres analyser i forkant av arrangementer eller andre tilstelninger der mange mennesker samles.

7.2 Videre forskning

Det ville vært interessant å undersøke gode måter å kommunisere risikobildet på. Slik KD forklarer er målet med analysene at de uønskede hendelsene som kan inntreffe blir identifisert og at tilhørende risiko vurderes for disse, samt at både sannsynlighets- og konsekvensreduserende tiltak fremkommer (2019, s. 18). Men hvordan skal dette kommuniseres og presenteres slik at det er egnet som beslutningsstøtte, samtidig som det heller ikke gjøres for enkelt slik at viktig informasjon glipper. En matrise kan sies å være for enkel? Men det er heller ingen som leser store permer med risikoanalyser? Dette kan danne grunnlag for en meget interessant studie, som også andre sektorer vil kunne ha stor nytte av.

8.0 Referanser

Amundrud, Ø., Aven, T., & Flage, R. (2017). How the definition of security risk can be made compatible with safety definitions. *Proceedings of the Institution of Mechanical Engineers. Part O, Journal of Risk and Reliability*, *231*(3), 286–294.

Anney, V. N. (2014). *Ensuring the Quality of the Findings of Qualitative Research: Looking at Trustworthiness Criteria*.

Askeland, T., Flage, R., & Aven, T. (2017). Moving beyond probabilities – Strength of knowledge characterisations applied to security. *Reliability Engineering & System Safety*, *159*, 196–205.

Aven, T. (2008). *Risikoanalyse: Prinsipper og metoder, med anvendelser.* Universitetsforlaget.

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

Aven, T., & Krohn, B. S. (2014). A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering & System Safety*, *121*, 1–10.

Aven, T., & Renn, O. (2009). The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Risk Analysis*, *29*(4), 587–600.

Boholm, M., Möller, N., & Hansson, S. O. (2016). The Concepts of Risk, Safety, and Security: Applications in Everyday Language. *Risk Analysis*, *36*(2), 320–338.

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*. (FFI-rapport 2015/00923) https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

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

Hegghammer, T. (2016). The Future of Jihadism in Europe: A Pessimistic View. *Perspectives on Terrorism (Lowell)*, *10*(6), 156–170.

Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)—Lovdata. (2017).

Jacobsen, D. I., & Repstad, P. (2004). *Dugnadsånd og forsvarsverker: Tverretatlig samarbeid i teori og praksis* (2. utg. Universitetsforlaget.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg.) Abstrakt forlag.

Jore, S. (2019). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174.

Jore, S. H., & Egeli, A. (2015). Risk management methodology for protecting against malicious acts: Are probabilities adequate means for describing terrorism and other security risks. *Safety and reliability of complex engineered systems.* 807–815.

Jore, Sissel, Utland, I.-L. F., & Vatnamo, V. H. (2018). *T*he contribution of foresight to improve long-term security planning. *Foresight*. *20*(1), 68–83.

Kriaa, S., Pietre-Cambacedes, L., Bouissou, M., & Halgand, Y. (2015). A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, *139*, 156–178.

Kunnskapsdepartementet. (2014, desember 10). *Kunnskapsdepartementets etater og virksomheter* https://www.regjeringen.no/no/dep/kd/org/etater-og-virksomheter/id2344548/

Kunnskapsdepartementet. (2019, juni 17). *Styringsdokument for arbeidet med samfunnssikkerhet i Kunnskapsdepartementets sektor*. https://www.regjeringen.no/no/dokumenter/styringsdokument-for-arbeidet-med-samfunns-sikkerhet-og-beredskap-i-kunnskapssektoren/id2512037/

Kunnskapsdepartementet. (2020, januar 2). *Samfunnssikkerhet og beredskap i Kunnskapsdepartementets sektor* https://www.regjeringen.no/no/dep/kd/samfunnssikkerhet-og-beredskap-i-kunnskapssektoren/id2550118/

Maal, M., Busmundrud, O., & Endregard, M. (u.å.) Methodology for security risk assessments – Is there a best practice? *Forsvarets forskningsinstitutt*. https://www.researchgate.net/publication/313807145_Methodology_for_security_risk_assessments-is_there_a_best_practice

NOU 2012:14. (2012) Rapport fra 22. juli-kommisjonen. https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf

Nasjonal sikkerhetsmyndighet. (2016). *Risikovurdering for sikring*: *Håndbok*. Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet, Politidirektoratet, & Politiets sikkerhetstjeneste. (2015). *Terrorsikring: En veileder i sikrings- og beredskapstiltak mot tilsiktede og uønskede handlinger. Oslo: NSM, POD og PST.*

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

Piètre-Cambacédès, L., & Bouissou, M. (2013). Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, *110*, 110–126.

Reason, J. T. (1990). *Human error*. Cambridge University Press.

Riksrevisjonen. (2020). *Revisjonsrapport for 2019 om samfunnssikkerhet og beredskap ved statlige universiteter og høyskoler*. Dokument 1 (2020-2021) https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/samfunnssikkerhet-og-beredskap-ved-statlige-universiteter-og-hoyskoler.pdf

Smith, C. L., & Brooks, D. J. (2012). *Security Science: The Theory and Practice of Security*. Butterworth Heinemann.

Standard Norge. (2008). *Krav til risikovurderinger.* NS 5814:2008. *S*tandard.no.

Standard Norge. (2012). *Beskyttelse mot tilsiktede uønskede hendelser, Terminologi.* NS 5830:2012. Standard.no.

Standard Norge. (2020). *Høringsnotat krav til risikovurderinger*.

Yvonna S. Lincoln. (1985). *Naturalistic inquiry*. Sage

Vedlegg 1

Intervjuguide - Semistrukturert, individuelt intervju

Tema:

Risikoanalyser i universitets- og høyskolesektoren.

Problemstilling:

Hvordan benytter universiteter og høyskoler risikoanalyser som beslutningsstøtte for å sikre seg mot tilsiktede uønskede hendelser?

Forskningsspørsmål:

1. Hvordan samsvarer valg av risikoanalysemetodikk i sektoren med anbefalinger i teoretiske bidrag?
2. Skilles det mellom safety- og security hendelser i forhold til valg av metodikk?
3. Fungerer metodikk opp mot safety og security forskjellig i forhold til det å støtte beslutninger?

Form: forsker intervjuer respondenten på enerom. Intervjuet tas opp på lyd etter samtykke, mens forskeren tar notater. Intervjuet blir transkribert i sin helhet.

Rammesetting	1. Uformell prat 2. Informasjon. Forklarer om temaet og bakgrunnen for intervjuet. Forklarer at respondenten er anonym og at konfidensielle data ikke skal videreformidles. 3. Informerer om at samtalen tas opp på lyd. Forutsatt at respondenten samtykker til dette.
Presentasjon av respondenten	4. Hvilken stilling har du? Hvor lenge har du hatt denne? 5. Hvilken utdanning/bakgrunn har du?
Tilsiktede uønskede hendelser	6. Hvordan jobber virksomheten opp mot tilsiktede uønskede hendelser?
Safety vs security	7. Skilles det mellom safety og security i institusjonen? Hvordan og hvorfor? 8. Kan du se noen fordeler/ulemper ved et større samarbeid mellom disse områdene?
Risikoanalysemetodikk	9. Hvilken risikoanalysemetodikk benyttes opp mot tilsiktede uønskede hendelser? Brukes det samme metode

	for safety og security hendelser? Bevissthet rundt dette? 10. Trengs det egen metodikk knyttet til security hendelser? 11. Hvordan er oppsettet og kompetansen til den eller de som utfører analysene? 12. Hva baseres trusselvurderinger og scenarioer på? Hvordan kommer en frem til initierende hendelser? 13. Hva er det som eventuelt vanskeliggjør en felles metodikk? 14. Ser du fordeler ved en felles metodikk for safety og security hendelser? 15. Involverer ledelsen seg i risikoanalyseprosessen? 16. Hvordan benyttes analysene som beslutningsstøtte? 17. Hvordan setter beslutningstaker seg inn i risikovurderingen? Forutsetninger, antakelser, vurderinger og usikkerheter? 18. Hvordan fremstilles/visualiseres resultatene av en risikoanalyse? 19. Hvordan kommuniseres resultatet til beslutningstaker? 20. Skrives det rapport og i tilfelle hvordan?
Tilbakeblikk	1. Oppsummering 2. Har jeg forstått deg riktig? 3. Er det noe du vil legge til?