Sjur Hevrøy

Hvordan styre det som ikke kan måles?

Sikring mot tilsiktede ondsinnede handlinger

Masteroppgave i i organisasjon og ledelse, spesialisering i sikkerhet, pålitelighet og vedlikehold. PK6901
Veileder: Trond Kongsvik
Trondheim, august 2017

Norges teknisk-naturvitenskapelige universitet
Institutt for maskinteknikk og produksjon

NTNU
Kunnskap for en bedre verden

Et forord bestående av fire takk!

- Takk til gode kollegaer ved studiene på NTNU og UiS.
- Takk til Trond Kongsvik som gav presise og relevante råd.
- Takk til Reidar Mysen og Hanna Kåsin Vangen for metodiske og faglige innspill.
- Og takk til Bolla for inspirasjon til hurtig levering!

.

1 Bakgrunn og innledning

“Security is not established as a corporate function, recognised for its distinct characteristics and requirements. In most cases, security is a small part of broader health, safety and environment positions, and one for which few people in that role have particular experience and expertise” (The investigation team 2013, 6).

Etter Statoils granskning av In Amenas-angrepet, viste egenevalueringen at de ikke hadde et system for styring av security som ble fulgt opp på samme måte som styring av safety. I etterkant har mange andre virksomheter prøvd å gå i dybden på hva et slikt system kan innebære: For hva er egentlig forskjellen på å beskytte seg mot ulykker vs. trusler? I denne oppgaven ønsker jeg å drøfte hvordan det å beskytte seg mot intensjonelle handlinger skiller seg fra, men også har noe å lære fra, de sikkerhetssystemer som er innrettet mot å unngå ulykker. Formålet er å konstruere en god styringsmodell for kontroll og prioritering av aktiviteter innen trusselhåndtering.

Selv har jeg sikkerhetsutdanning fra UiS og NTNU, og begge steder har fokuset vært på sikkerhet i relasjon til ulykker. Men arbeidserfaringen min har primært vært innrettet mot å beskytte seg mot kriminelle, terrorister eller statlige aktører. De fleste av mine kollegaer har også hatt lignende oppgaver som meg selv. Leveson og Youngs oppsummering er treffende:

“Safety experts see their role as preventing losses due to unintentional actions by benevolent actors. Security experts see their role as preventing losses due to intentional actions by malevolent actors.” (Young and Leveson 2014)

Med ulik rolleforståelse, blir det ulikt fokus. Dette forsterkes av at det også er ulike utdanninger, typisk domineres security-feltet av politi eller eks-militære, mens safety er dominert av ingeniørutdannede.

Bakgrunnen for denne oppgaven er et opplevd “gap” mellom fag jeg har tatt på universitetet både innen sikkerhetsstyring og tidligere samfunnsvitenskapelige studier, og praksis som sikringsrådgiver. Gapet har flere elementer.

- Praktikere som jobber med sikring mot tilsiktede handlinger er ikke påkoblet akademisk litteratur om hva for eksempel terrorisme eller kriminalitet er, og hvordan

den best kan forstås og motvirkes. Snarere baserer man seg på standarder utviklet av kommersielle aktører. Slike standarder har en egeninteresse i å fremstilles som at de virker, men de er ikke *evidens*baserte. Man har ikke evaluert hvilke tiltak som har sikringseffekt, på samme måte som man har målt hvilke safety-kulturer som fører til færre ulykker/feilhandlinger, se for eksempel Ganatra og Johnsen om hvilke praksiser som fører til at man foretar færre feilhandlinger i medisinsk behandling (2016). Praktikere innen safety har derimot en forskningsbasert utdanning.

- Noe av dette kan skyldes sikringsfeltet selv, at effekten er vanskelig å måle. Akademiske diskusjoner tilknyttet hvordan man bør måle sikkerhet er eksempelvis knyttet til hva som bør måles og hvordan (Boehmer 2008; Wright 2006), men det er ikke knyttet til om tiltakene har effekt. Dette skiller seg fra safetyfeltet hvor man har etablerte metoder for å forske på oppnådd effekt (Kongsvik, Haavik, and Gjøsund 2014). Akademisk litteratur om kriminalitet og terrorisme besvarer spørsmål som: Hvem blir kriminell? Hva gjør terrorister? Og i noen grad også: hvordan kan vi forhindre at noen blir en trusselaktør? Men de besvarer sjelden spørsmålet som sikringsrådgivere som meg selv er opptatt av: Hvordan kan vi unngå at kriminalitet fører til tap? Den overordnede beskrivelsen for hvilke ferdigheter man tilegner seg etter endt bachelorstudie i kriminologi på universitetet i Oslo, har eksempelvis ingen henvisninger til at man lærer noe om hvordan man kan redusere kriminalitet (UIO 2014).
- Mens kollegaer innen safety-feltet har hatt *styring av risiko* som hovedfokus, har jeg sjelden sett gode systemer for å styre sikringsrisikoer. Det mest utviklede jeg har sett har vært innen informasjonssikkerhet, men jeg kjenner ikke til noen som sier de har et godt system for å veie sikringsrisikoer knyttet til liv/helse opp mot eksempelvis tap av konfidensiell informasjon og/eller leveransekapasitet. Sikringsfeltet har ikke en enhetlig forsknings- og metodediskurs. Faglitteratur fra sikringsfeltet har også vært svakt koblet på fag jeg har tatt i statsvitenskap, som omhandler eksempelvis terrorisme.

Dette gapet håper jeg å bidra til å lukke ved denne oppgaven. For å få det til har jeg foretatt en litteraturstudie, hvor jeg gjennomgår eksisterende litteratur, og prøver å syntetisere dette til styringsprinsipper for sikring.

Jeg prøver altså å tydeliggjøre hvordan akademisk litteratur og innsikter bør benyttes når man arbeider med sikring. Dette vil jeg knytte sammen med praksis i de virksomheter hvor jeg har arbeidet. Hovedmotivasjonen for å skrive oppgaven er et opplevd gap. Om du ønsker en oversikt over faget safety, og hvilke metoder som er tilgjengelig for å minske tap og skader på dine verdier, finnes det mange bøker og et stort akademisk fagfelt med noenlunde lik faglig basis. Skal man sikre virksomheten mot tilsiktede handlinger, finnes ikke det i samme grad.

1.1 Litt om begreper

Begrepsfestingen av skillet mellom safety og security ble i norsk sikkerhetsterminologi tydeliggjort med den norske offentlige utredningen «Når sikkerheten er viktigst» (Ullring et al. 2006). Enkelt sagt beskrives forskjellen som at det i security finnes en trusselaktør med ondsinnede intensjoner om å ønsker å skade eller stjele dine verdier, mens innen safetyfaget er det farer som ville dyr og naturkatastrofer, eller tekniske/menneskelige feil som fører til tap og skader.

I Norsk standard (NS 5830) skiller man mellom intenderte uønskede hendelser, til forskjell fra uønskede uintenderte hendelser. Dette for å få fram at det er forskjell på når mennesker gjør feil eller at teknologien svikter, og når mennesker ønsker å påføre skade. Konsekvensene kan bli det samme, men tiltakene for å forhindre det vil være ulike. I denne oppgaven betegne “tilsiktede” alltid ondsinnede handlinger. Et begrep fra samme standard som nok vil erstatte security er “sikring”. Jeg har valgt å benytte dette begrepet som dekkende for det som tidligere ofte ble kalt security. På samme måte har jeg prøvd å benytte ulykkesforebygging som betegnende for safety, da det gir mest mening i denne oppgavens kontekst. I de tilfeller hvor jeg henviser til annen originallitteratur har jeg brukt originalbegrepene (som samfunnsikkerhet).

Når jeg beskriver trusselaktørers ulike handlemåter benytter jeg begrepet modus (etter Modus Operandi) for å beskrive hvilke metoder som benyttes for å oppnå tilgang til verdien. De mulige metodene som kan brukes bestemmes av hvilke *kapabiliteter* trusselaktøren har, som kan beskrives som ferdigheter.

Barrierer kan beskrive både fysiske skiller mellom en skadekilde og en beskyttbar verdi, en aktivitet, en kunnskapsbasert fortolkning og mer immaterielle størrelser som normer, regler og lover (Kongsvik 2013, 73). I denne oppgaven har jeg et styringsperspektiv, og benytter derfor oftere begrepet *tiltak*, for å få fram at innføringen av noe som skal forhindre eller redusere konsekvensene av en hendelse er noe som må besluttes.

1.2 Problemstilling og forskningsspørsmål

Med bakgrunn i det over er min hovedproblemstilling: Hvordan bør et styringssystem for sikring være? Fra dette har jeg utledet tre forskningsspørsmål som jeg prøver å besvare i to separate underkapitler, som gir meg grunnlaget for å besvare det overordnede spørsmålet. Dette er:

- Hvilke modeller er mest relevante for et styringssystem for sikring?

I kapittel tre går jeg gjennom tre ulike sikkerhetsmodeller, nemlig Schiefloes samfunnssikkerhetsmodell (2011), Bjørgos generelle kriminalitetsforebyggende modell (2015), og Kjellens safety-modell (2002). Kapittelet er tenkt å vise til hva jeg ser på som mest relevant av tidligere forskning. Hvordan jeg har funnet disse modellene går jeg gjennom i kapittel 2 som kjennetegner dem tar jeg for meg i kapittel 3.

- Hva skiller sikring fra ulykkesforebygging?

I det relevante kapittelet gjennomgår jeg forskjeller i ulykkesforebygging og sikring, med eksempler fra relevant litteratur. Dette gjør jeg i hovedsak i kapittel fire, selv om jeg også i kapittel 3 kommenterer hva de spesifikke teoriene sier om forskjeller mellom ulykkesforebygging og sikring. Altså: jeg gjennomgår ulike *modeller* i kapittel 3, og mer modellspesifikke *forskjeller* i kapittel 4.

- Hva kjennetegner barrierer innen sikringsfaget?

I kapittel 3 gjennomgår jeg hva som regnes som barrierer i de ulike modellene. Som jeg nevnte i innledningen bruker jeg stort sett begrepet tiltak. Jeg vurderer også om modellenes skiller mellom beskyttelse mot trusler og farer. I kapittel 3.3.3 går jeg også gjennom kjennetegn ved typiske barrierer i safety, som jeg så benytter meg av i kapittel 5.

1.3 Avgrensninger

- Jeg har ikke hatt fokus på å etablere hva og hvordan sikringsarbeid foretas i sammenlignbare virksomheter. Det betyr at man kan bestride mine beskrivelser av hva som er “typisk”, “ofte” og “vanlig”. Min argumentasjon for hvorfor jeg har gjort det slik befinner seg i metodekapittelet, primært i 2.1, 2.4, og 2.5.
- Når jeg skriver om risikoreduserende tiltak beskriver jeg dette på et overordnet nivå. Det vil i de fleste tilfeller være langt flere aktuelle tiltak for å oppnå balansert sikring. Men dette er ikke en sikringsrisikoanalyse, jeg har bare prøvd å velge ut typiske eller interessante tiltak utfra erfaringer og litteraturstudien.
- I kapittel 5.2 beskriver jeg viktigheten av at de verdiene en sikrer, må ses opp mot hvor enkelt det er å få tilgang til disse verdiene for en trusselaktør hos andre sammenlignbare objekter. Dette er en tankegang som har etiske problemstillinger knyttet til et et “sikringskappløp” og verdien av et menneskeliv. Denne diskusjonen er viktig, men er ikke noe jeg har plass til å drøfte her.
- Jeg har litt for sent i prosessen forstått hvordan forskningen på storulykker har samme mangel på statistiske data som man ofte står overfor når man sikrer seg mot tilsiktede handlinger. Tilknyttet dette kunne det vært interessant å se på om Bayesiansk statistikk burde hatt større bruksområde innenfor sikring mot tilsiktede handlinger(Yu, Khan, and Veitch 2017). Neste gang!

2. Metode

Jeg har i innledningen forklart at bakgrunnen for oppgaven er et opplevd gap i kobling mellom akademisk litteratur tilknyttet forståelse av terrorisme og kriminelle handlinger og praksis blant kollegaer innenfor og utenfor egen virksomhet. Jeg har også snakket om at dette synes i mindre grad å være tilfelle når man jobber ulykkesforebygging. Det synes å mangle forskningsbaserte modeller som kan brukes for å styre all form for sikring mot tilsiktede handlinger på virksomhetsnivå. Dette er bakgrunnen for mine forskningsspørsmål. I dette kapittelet skal jeg beskrive hvordan jeg kom fram til mitt utvalg.

2.1 Om mine forskningsspørsmål

I en vitenskapsteoretisk ramme vil alle undersøkelser av "noe", enten det er vannets ulike egenskaper i ulike temperaturer, undersøkelser av sikkerhetskulturer i en bedrift eller effekten av et nytt legemiddel forholde seg et forskningsopplegg som vil inneholde fire elementer. Det er forskningsspørsmål, analytiske kategorier, erfaringsmateriale og svar (Engelstad et al. 2005, 110).

Forskningsspørsmål styrer retningen i undersøkelsene, og sier noe om hva vi undersøker og avgrenser samtidig feltet vi undersøker. Vi kan ikke forske på "alt". Vi må i stedet avgrense oss til forskbare spørsmål innenfor rammene av en masteroppgave.

Engelstad viser til at gode samfunnsvitenskapelige spørsmål grovt kan kategoriseres i dem som stilles fra forskersamfunnet, eller fra samfunnet til forskerne (2005, 127–128). Mine forskningsspørsmål er noe jeg selv har strevd med i samarbeid med kollegaer, og det synes derfor naturlig å plassere oppgaven i den siste kategorien. Videre kan forskningsspørsmålene kategoriseres som konstruktive og retningsgivende (2005, 136). Det er også betegnende for mine forskningsspørsmål, da jeg har formulert spørsmålene slik at svaret skal kunne bidra til å gjøre sikringsstyring bedre.

2.2 Erfaringsmateriale

For å besvare forskningsspørsmål, må man samle inn data. Dette vil da utgjøre basis for kunnskapen i oppgaven. Generelt kan man benytte seg av feltstudier, eksperimenter,

representative rundspørringer og kildestudier for å samle inn data. Hver av disse metodene har egne varianter av metodikker som skal sikre at dataene er reliable.

For min egen del er grunnen til at jeg har valgt litteraturstudie knyttet til hvilke spørsmål jeg stiller, og hva jeg ønsker svar på. For å forklare dette vil jeg vil jeg i det følgende forklare hvorfor jeg har valgt denne metoden, og ikke noen av de andre.

Forskningsdesign innebærer at man tar stilling til hva og hvem som undersøkes, og hvordan man gjennomfører dette (Johannessen, Tufte, and Christoffersen 2010, 69). Om forskningsspørsmålet hadde vært *Hvordan er styringssystemer for sikring i 5 norske bedrifter*, ville jeg valgt en annen metode. Jeg hadde da valgt ut 5 sammenlignbare virksomheter, for kunne beskrive deres styringssystemer tilknyttet ondsinnede handlinger. For å undersøke ville jeg kanskje benyttet meg av *empiribasert teori* og foretatt deltakende observasjon, dybdeintervju og benyttet fokusgrupper (Johannessen, Tufte, and Christoffersen 2010, 84). Svarene på spørsmålene mine ville ventelig vært knyttet til hvilke hendelser, strukturer, holdninger etc, hva som var beste praksis og indikatorer for styring som forekom i bedriften. Kanskje svaret mitt kunne blitt noe i retning av det Duus (2016) har funnet, nemlig at sikringsarbeid i norske virksomheter ikke er forankret/prioritert i virksomhetens målhierarki. Men med denne undersøkelsesmetoden (som ville vært svært egnet til å besvare dette alternative forskningsspørsmålet) ville man ikke kunne oppnådd den koblingen mellom sikring, ulykkesforebygging og akademia som jeg er interessert i. Dens normative kraft ville vært knyttet til eksempelets makt, og ikke forskningsbasert modellutvikling.

Helen Aveyard (2014, 1) definerer litteraturstudier som at de ofte har utgangspunkt i at det ønskes svar på spesifikke spørsmål ved å gjennomgå eksisterende litteratur. Litteraturstudier gjøres ofte som forarbeider til egne prosjekter. I Tyskland er det eksempelvis en obligatorisk del av doktorgrader at man henviser til tidligere forskning på området. Aveyard sier videre om (den typen litteraturstudie som ligner mest på min) at:

"...the purpose of the review will be to provide new insights into a research question by reviewing existing literature rather than provide a justification for a new study, although you

may well conclude that there is insufficient literature to answer your question and hence a new study is recommended." (2014, xiv)

En innvending både mot forskningsspørsmål og metodevalg kan være at jeg har gått ett trinn for langt. I stedet for å etablere min beskrivelse av gapet som sant, har jeg dermed søkt å løse et problem som man ikke kan vite at eksisterer. Jeg kan da kritiseres for at jeg er offer for den erkjennelsesteoretiske posisjonen *naiv realisme (Svendsen 2011)*.

Mitt tilsvar til dette må være at på en erfaringsbasert master bør det være rom for at erfaringen man har etter en viss mengde år i arbeidslivet må kunne tillegges noe vekt. Kunnskapen om hvordan andre virksomheter jobber med sikring kommer fra samarbeid med kollegaer fra ulike virksomheter, og egen erfaring fra ulike virksomheter. Litteraturstudiet mitt har heller ikke kommet opp med noen gode eksempler på at man tenker sikring mot tilsiktede handlinger helhetlig og påkoblet forskning. Når man skal forklare noe, er vanligvis problemet ikke at man har for lite informasjon, men for mye. Man trenger derfor syntetiserende forsøk for å skape meningsfulle og forståelige enheter (Weick 1995). Dette gjør at mitt utkast til styringsprinsipper kan være verdt å diskutere selv om min beskrivelse av gapet ikke er etablert.

2.3 Analytiske kategorier

Analytiske kategorier er de begrepet og typologier som man benytter når man skal ordne data. Først om begreper: Jeg har selvsagt prøvd å gjøre oppgaven så lesbar og gjennomsiktig som mulig. Imidlertid er denne teksten rettet mot noen, og ikke noen andre. Den viktigste målgruppen er andre som jobber med sikring og beredskap. Men videre er den rettet mot subgruppen "de som jobber med sikring og beredskap i en akademisk kontekst". Oppgaven er enklest å lese for dem, og så håper jeg at nok særbregreper er gitt en forklaring som gjør den lesbar også for andre interesserte. Mine typologier kommer fra benyttet litteratur og offentlige veiledninger. Jeg forklarer dem etterhvert som de introduseres i kapittel 3.

2.4 Hva er bakgrunnen for mine metodiske valg?

Selv har jeg ønsket å bøte på et opplevd gap mellom teori og praksis, og jeg mener at løsningen må være knyttet til å vise forskningens relevans for praksis. Påstanden min er jo

at dette fungerer innenfor safety, men ikke sikring. Jeg har ikke forsøkt å finne ut av hvordan andre løser oppgaver, siden det ikke ville besvart problemstillingen min. I stedet er utvalget av tekster basert på at de er av en *systematiserende* og *abstraherende* karakter. De er systematiske ved at de fra et stort antall kilder prøver å lage en modell, baserte på å abstrahere ut det vesentligste. Oppgaven min bearbeider derfor innhentet data/empiri men i samfunnsvitenskapelig forstand er den også innrettet mot å utvikle en metode.

2.5 En metodisk utfordring knyttet til deling av sårbarheter

Et annet problem med å velge mer direkte innhenting av empiri fra praksisfeltet, er at at de fleste bedriftene ville vært svært tilbakeholdne med informasjon. Noe av kjernen i sikring er at tiltakene ikke er kjente for ondsinnede aktører - og det er derfor slik at hva som ligger bak ulike sikringsvalg ofte ikke er kjente for andre enn en liten gruppe mennesker i virksomheten. Utfra noen samtaler med bekjente innen feltet synes det ikke som om dette er noe som ville blitt delt, tross tillit til undertegnedes evner til å skjule relevante tiltak. Ved hjelp av litt snoking på min LinkedIn-profil kunne oppgaven da i verste fall ført til at utnyttbare sårbarheter ble eksponert.

Jeg foretrekker ellers å skrive om hva som er relevant for private virksomhet, siden det offentlige er mindre åpen for drøftinger om hva som utgjør god kvalitet, men i stedet er lovstyrt utfra hva som er juridisk riktig eller galt. Med dette menes at sikkerhetslovens føringer oftere gjør at man ikke selv kan prioritere innenfor ulike sikringstiltak, men i stedet må oppfylle de reguleringer som finnes. I verste fall betyr dette at sikringen innrettes mot å tilfredsstille en standard (oppfylle lover), fremfor å ha høyest mulig kvalitet. Siden sikringsfeltet er mindre regulert i privat virksomhet, er det flere interessante diskusjoner knyttet til hva som er god sikring, hva som er godt nok, og hva som er aller best. Jeg håper at oppgaven kan bidra til dette ordskiftet.

2.6 Hva har jeg sett etter for å finne relevant litteratur?

Gjennom kursene som er en del av masteroppgaven innen sikkerhet, pålitelighet og vedlikehold, har jeg blitt introdusert for mye relevant litteratur. En kjerne i perspektivene har vært risikostyring, og i undervisningen har dette ofte blitt eksemplifisert med eksempler fra industriell produksjon. Å styre risikoen er selvsagt et mål også innenfor sikringsfeltet,

men siden man mangler data på de mest alvorlige tilfellene (et typisk eksempel er terrorisme) er det vanskelige å fastsette målbare og aksepterte sikringsmål. Styringen må derfor være innrettet på et noe annet sett. Et generelt trekk ved litteratur innen security-feltet er at det drøfter enkeltstående fenomen. Både forelesere og kollegaer har i så måte anbefalt bøker/artikler om terrorisme eller cyberkriminalitet eller andre akademiske undersøkelser av kriminalitetsreduserende design. Men jeg har i svært liten grad sett dette satt inn i et rammeverk for hvordan man skal *styre og sikre bedre*. I stedet er det forklaringer og kanskje også mitigerende tiltak, men det er ikke rettet mot praktikere, det er heller rettet mot politikere og andre med en akademisk interesse for feltet. Dette i motsetning til safety-litteraturen jeg har fått presentert i fagene jeg har tatt. Denne er på en helt annen måte i kontakt med, og direkte innvirker i hvordan sikkerheten mot ulykker skal forbedres på virksomhetsnivå.

Fra kommersielle aktører som Norsk standard eller konsulentselskaper har man også sjekklister og rammeverk for sikringsstyring, men dette er i liten grad påkoblet forskning. Jeg har derfor spurt kollegaer for å få tips til hva jeg bør lese for å få mer informasjon om styring av sikringsfeltet. Jeg har ellers brukt søkeord som “evidence”, “tilsiktede handlinger”, “sikring”, security and safety”, “security and resilience”, “effectiveness of security measures” og via de artikler jeg har funnet, og deres referanser igjen kommet over de artiklene jeg siterer eller henviser til i denne teksten.

2.7 Hvilke modeller har jeg funnet, og hva har jeg sett bort fra?

Jeg er på utkikk etter en modell som kan hjelpe meg for å kunne svare på min problemstilling. Et moment å merke seg er at de bør kunne ha en effekt overfor villede handlinger. Eksempelvis er det vel få modeller som siteres (og brukes) like ofte i både ulykkesforebygging og sikring-kontekster som James Reason’s “Swiss-cheese model of defences” (Reason 1997, 9). Men samtidig er denne spesifikt innrettet mot å unngå ulykker. Feilhandlingene dekker ikke sabotasje. Han skiller mellom *aktive* feilhandlinger og *latente* betingelser. En aktiv feilhandling er eksempelvis det siste trykket på maskinen før noe går ned, eller den kodingen som fører til at noe ikke virker. Eksempler kan være produksjonsstansen på Mongstad i 2014 (Remen and Tomter 2016), eller problemer med nettbank hos DNB i 2017 (Sundberg and Framstad 2017). Men når man graver litt i hvorfor slike feil skjer, kommer man frem til at det er latente betingelser som gjør at disse tingene

skjer. Det er ingen som ønsker at at verdier skal tapes eller komme til skade. Siden "...fallibility is an inescapable part of the human condition, it is now recognized that people working in complex systems make errors or violate procedures for reasons that generally go beyond the scope of individual psychology." (Reason 1997, 10). Forklaringene på hvorfor den aktive feilhandlingen skjer, viser seg da oftest å være knyttet til latente betingelser som feil insentiver, dårlig produksjonsdesign, for lite og gal opplæring og trening, manglende ressurser og lignende. Når jeg senere skal konstruere en modell for helhetlig sikringsstyring, vil jeg benytte dette skillet, spesielt knyttet til insentiver, og støtte meg på Reason. Det er svært nyttig når man skal drøfte om organisasjoner har konflikter knyttet til for eksempel produksjonsmål og sikringsmål. Men jeg kan ikke bruke dette skillet til å forklare for eksempel sabotasje utført av ansatte. Da må jeg ta utgangspunkt i teorier som forutsetter at det finnes ondsinnede aktører.

Et annet utvalgskriterium er knyttet til at de som skal kunne si noe om hvordan man *bør* styre sikkerheten, må ha et normativt aspekt. Aven beskriver sikkerhetsstyring på følgende vis: "...alle systematiske tiltak som iverksettes for å oppnå og opprettholde de sikkerhetskrav en har satt seg." (Aven 1998, 151). Jeg har derfor sett etter litteratur som omhandler mål for sikkerhet, måling og oppfølging av sikkerhetsbildet, avvik fra styringsmål og organisering. For eksempel er risikoanalyser og granskingsmetodikk metoder som inngår i styringssystemer for sikring, men dette er ikke noe som utgjør en teori i seg selv.

Jeg tillater meg altså en viss eklektisisme i både i utvalget av modeller, hvilke momenter jeg finner nyttige, samt i hva jeg vektlegger. Dette fordi svaret på forskningsspørsmålene mine innebærer å foreslå en mer helhetlig modell for sikringsstyring. Men det viktigste er at de har et helhetlig og systematisk fokus.

2.7 Utfra kriteriene - hva er relevant litteratur?

Tore Bjørgos (2015) generelle kriminalitetsforebyggende modell er i så måte en av de få bøkene jeg kjenner til som

a) både er opptatt av hvordan noe bør styres,
b) som er rettet mot et bredt spekter av tilsiktede handlinger,
c) og som også er påkoblet akademisk forskning.

Om det ikke var for at den i liten grad er rettet mot mine kollegaer i sikringsbransjen, ville det vært vanskeligere å argumentere for mangelen jeg har identifisert i innledningen. Denne modellen ble presentert på et kurs jeg tok i Security på Universitetet i Stavanger. En tidligere variant av arbeidet til Bjørgo ble også anbefalt meg av Jan Hovden, tilknyttet en oppgave jeg skrev i et kurs om sikkerhet i organisasjoner på NTNU. På samme kurs var også Per Morten Schiefloes (2011) samfunnsikkerhetsmodell på pensum, og opplevdes umiddelbart relevant. Dette fordi den inkorporerte det brede spekteret av virkemidler som jeg da som offentlig ansatte kunne benytte og anbefale. Med det menes at man for eksempel ikke bare tenkte på vanlige fysiske sikringsbarrierer som pullerter og skuddsikre vester, men også at jeg i mitt daglige virke kunne skrive innspill til samfunnsikkerhetsmeldinger/høringer hvor forebygging av hendelser på samfunnsnivå var viktig. Schiefloes modell inkorporerer hele spekteret, noe som tidligere ikke var systematisert i vår styringsmodell. Fra før kjente jeg bare til enkeltstående studier av avgrensede fenomen, som for eksempel hvordan man beskyttet seg mot væpnede angrep. Siden dette var de meste relevante jeg kjente til på forhånd, opplevdes det naturlig å ta utgangspunkt i disse to. Et problem var selvsagt at ikke alle tiltakene var innrettet mot hva en virksomhet kunne gjøre selv, siden de var på et samfunnsikkerhetsnivå. Allikevel fant jeg de fleste momentene nyttige å vurdere, selv om vanlige virksomheter ikke besitter samme type virkemidler som myndigheter.

Av de varianter som finnes av helhetlige rammeverk for sikkerhet mot ulykker, hadde jeg på forhånd en oppfatning av at resilliencemodellen var den den som synes å ha størst overføringsverdi til sikring-feltet. Schiefloe refererer også til den, og tanken om å robustifisere en virksomhet. Med bakgrunn i Schiefloes referanser har jeg derfor benyttet meg av Erick Hollnagel (2011) når jeg skal beskrive resilliencemodellen.

Jeg ba mine veiledere om tips til litteratur som eksemplifiserte safety på en god og overordnet måte. Jeg ble da anbefalt Urban Kjellèns (2002) bok. Den er svært tydelig innrettet mot forskning på hva virksomheter kan gjøre/har gjort og hva som har effekt. Dette var en stor bonus når jeg skulle utvikle min egen modell. Dermed ble den også relevant for å utvikle styringssiden av prinsippene for styring av sikring mot tilsiktede handlinger.

I neste kapittel vil jeg altså gi et overblikk over de mest relevante modellene. Om man ser på problemstillingen min, og de tre avledede forskningsspørsmålene mine, er jeg selvsagt interessert i om modellene kan gi gode svar på forskningsspørsmålene mine. I gjengivelsen nedenfor er jeg derfor spesielt interessert i hvilken (om noen) forskjeller de ser på beskyttelse mot tilsiktede vs. utilsiktede handlinger, og hva som kjennetegner sikringsbarrierer.

3. Teoretisk utgangspunkt, og modeller brukt for å besvare forskningsspørsmål

Jeg har valgt å benytte meg av tre ulike modeller for å besvare forskningsspørsmålene mine knyttet til hva som skiller ulykkesforebygging og sikring. Jeg har prøvd å gjengi helheten i modellene, da jeg mener det har en større verdi når man skal trekke ut elementer jeg benytter meg av i kapittel fem. På denne måten vil man kunne se at elementene er i et system som allerede er forskningsmessig belagt, noe som igjen styrker min syntese i kapittel 5.

3.1 Schiefloes samfunnssikkerhetsmodell

På oppdrag for 22. julikommisjonen utarbeidet Per Morten Schiefloe et oversiktsnotat som plasserte samfunnssikkerhet, og sjeldne hendelser som terror inn i et sikkerhetsfaglig rammeverk (Per Morten Schiefloe 2011). I norsk sammenheng peker han tilbake til at et nøkkelverk i samfunnssikkerhetsdiskursen er NOU 2000:24 Et sårbart samfunn— Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet, oftest referert til som *Willochs' sårbarhetsutvalg*. Her gis den sivile beredskapen en retning som skiller den fra den militære. I tillegg introduseres bekymringer knyttet til informasjonssikkerhet, frafall av kritisk infrastruktur som strøm og transport, samt at terrorisme beskrives som et reelt problem også i Norge, ved at man henviser til tre foretatte flykapringer i Norge på nittitallet (Willoch and Politidepartementet 2000). Notatet er relevant da det viser til et eksempel på hvordan man med bakgrunn i sikkerhetsforskning (safety) lager en modell for hvordan hindre negative intensjonelle handlinger på samfunnssikkerhetsnivå.

Før vi går videre kan det være verdt å merke seg at modellen er utarbeidet på et nivå hvor den en tenkt å kunne si noe om styring av samfunnet, og sikring mot terror. Den er altså ikke spesifikk organisasjonsfaglig. Den oppfattes like fullt relevant for min oppgave, noe jeg håper gjennomgangen viser. Dette sporet kommer jeg tilbake til i oppsummeringen av dette underkapittelet.

Schiefloe åpner med å presentere forskningsfeltet, og henviser til at Hale og Hovden (1998) oppsummerer forskningen på hvordan forhindre at noe kan gå galt, som preget av tre historisk påfølgende perioder. I den første perioden var man mest opptatt av tekniske

tiltak, dvs. hvordan kan man ved å utbedre maskiner og annet utstyr fikse at noe ikke går galt. I den andre perioden var man mest opptatt av menneskene som gjorde feil - i hvilke settinger ville dette skje og hvorfor. I den tredje perioden var man opptatt av ledelse og den organisatoriske settingen som kunne virke forhindrende eller disponerende for ulykker (A. R. Hale and Hovden 1998).

Ifølge Schiefloe er praksis at de fleste arbeider ut fra en forståelse av at det er samspillet mellom *Menneske, Teknologi og Organisasjon* som avgjør om man arbeider sikkert eller ikke. Teknologien må reliabelt levere den tjenesten den er tenkt å gjøre - men den må også være tilpasset bruk av mennesker. Mennesker som feiler, som har en begrenset evne til å gjøre flere ting samtidig, og som responderer på ønsker om at oppgaver skal utføres raskere for å spare tid og penger. For å tilstrekkelig kunne analysere dette samvirket henviser Schiefloe til sin egen "pentagonmodell". Den har dette navnet med bakgrunn i fem faktorer som gir kontekst for de oppgavene en person skal løse. Faktorene er formell struktur, som viser til rammer og myndighet og regler som oppgavene utføres i, teknologi, som kan vise til maskiner og IT-utstyr, organisasjonskultur, med verdier og normer, hvordan interaksjonen foretas og sosiale relasjoner og nettverk. (P. M. Schiefloe 2014).

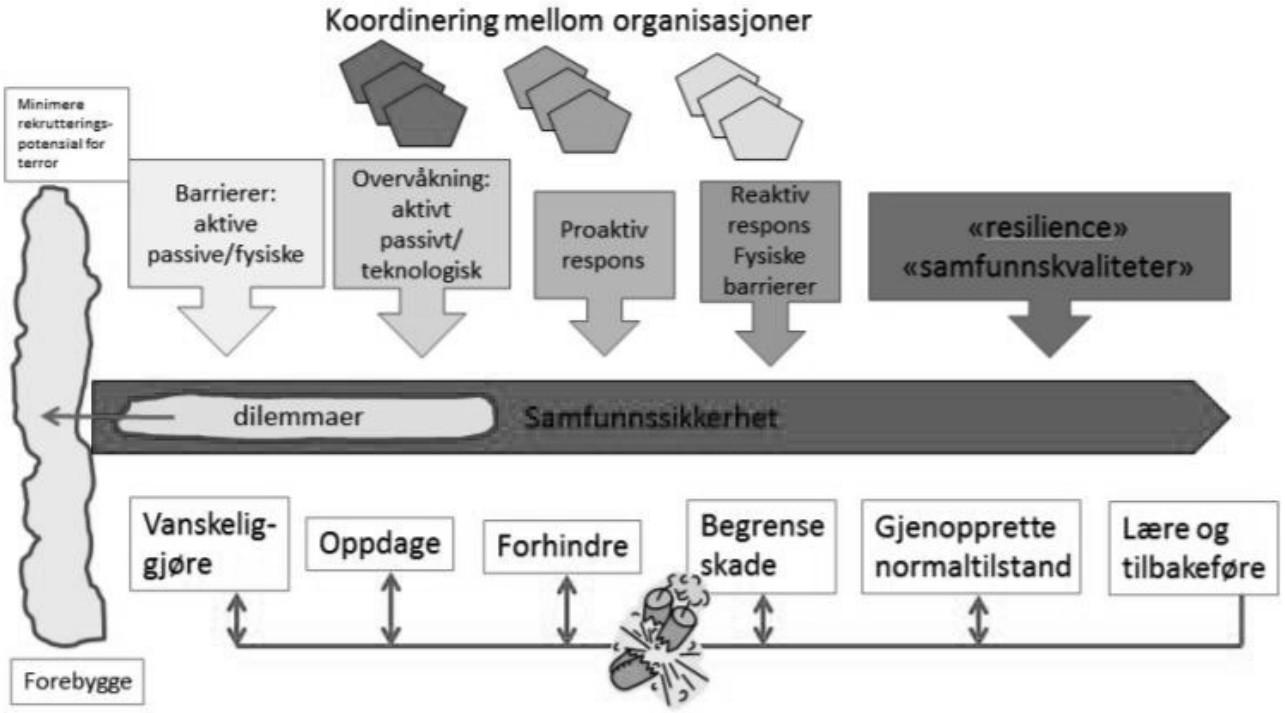
Essensen av å sikre samfunnet viser til evnen de kritiske funksjoner har til å stå imot påkjenninger. Det må være barrierer mellom det som skal sikres, og det som truer. Dersom en av barrierene svikter, skal helst en av de andre barrierene kunne forhindre at noe går galt. I Schiefloes modell er barrierer både noe som etableres for å unngå hendelsen, og noe som reduserer konsekvensene

Andre modeller som Schiefloe nevner, er Turners modell om Man-made Disasters. Det viktigste her er at det finnes en "inkubasjonsfase", hvor ulike feil får utvikle seg, mens de egentlig kunne blitt fanget opp (Engen et al. 2016). Man overser hendelser som har økende negative konsekvenser, fordi en kultur har utviklet seg hvor avvik blir sett på som normalt.

Schiefloe går også igjennom resilience engineering som kort gjengitt handler om å øke en organisasjons evne til å fortsette virksomheten tilnærmet upåvirket selv om det er skjedd

en hendelse som tilsier at det har vært et større avvik. Jeg vil gå nærmere inn på denne teoriretningen i kapittel 3.3, med henvisning til Urban Kjellens Safety, Health & Environment modell for hvordan unngå ulykker.

Etter å ha gjennomgått teorigrunnlaget, drøfter Schiefloe hvordan dette kan overføres til samfunnssikkerhet. Jeg har nå gjengitt de sikkerhetsfaglige modeller som er relevant for å forstå bakgrunnen for Schiefloes samfunnssikkerhetsmodell. Videre vil jeg vise hvordan dette kan tenkes å kunne beskytte samfunnet mot intensjonelle handlinger.



Figur 10: Modell for samfunnssikkerhet

(Per Morten Schiefloe 2011, 14)

Samfunnssikkerhet gjengis som den evnen samfunnet har til motstå negative hendelser, dvs et resilient samfunn. Schiefloe gjengir eksempelet utfra en terrorhandling, og jeg vil selv benytte samme eksempel i gjengivelsen. På den forebyggende siden vil man ha barrierer som kan redusere sjansen for at noen "får lyst" til å utøve terror. Avhengig av hva man ser som terrorens opphav, vil man da fokusere på å lage et samfunn som ikke

aksepterer vold, et samfunn hvor alle har muligheter, et samfunn hvor myndighetene avstår fra visse handlinger innenriks eller utenriks, etc. Mer konkrete barrierer handler om å vanskeliggjøre, og dermed redusere kapasitet. Eksempelvis gjøre tilgangen på våpen og ammunisjon restriktiv, eller kunnskapen om dette. Når det gjelder å oppdage, er dette noe som gjøres ved hjelp av overvåkning. Den kan tenkes å være passiv, i form av at man eksempelvis masseovervåker besøk av internettsider for å se etter "trender" korrelert med søkemønsteret til terrorister, eller aktiv, målrettet mot visse miljøer man venter/kjenner til har intensjoner.

Som man ser på modellen, er den innrettet mot hvordan samfunnet skal styres for å håndtere terror bedre. Men om man ser på momentene i modellen, vil noen av delene også kunne overføres til hvordan man skal styre en virksomhet, som jeg nevner i kapittel 5.

Dersom man oppdager at noen planlegger noe, vil man søke å forhindre at noe skjer, før det skjer. Man kan da jobbe indirekte eller direkte mot trusselaktørers kapabilitet som ved å forby visse typer våpen for alle, eller pågripe og arrestere spesifikke aktører.

Om noen har foretatt seg noe, må man søke å begrense skadene. Rask og kompetent reaksjon er da sentralt, eksempelvis fra Delta eller andre politistyrker. De mest kompetente må løse oppgavene, og det er derfor viktig å avklare ansvarslinjer på forhånd. Eksempelvis har regjeringen besluttet at reaksjonsstyrken i Nordsjøen ved terrorangrep skal være Forsvarets spesialkommando, og ikke Delta.

Å gjenopprette normal tilstand er det som skjer når hendelsen er "over". Hermetegnene gjengir at selv om en terroroperasjon er avsluttet, at gjerningsmennene eksempelvis er drept og/eller arrestert, og det ikke lenger eksisterer et forhøyet trusselnivå med bakgrunn i denne gruppen, er det fremdeles mange oppgaver som gjenstår. Man må reparere de fysiske skadene, gjenskape tillit i samfunnet, skadde må få oppfølging ol. "Vi kan også omtale dette som resilience på samfunnsnivå" (Per Morten Schiefloe 2011, 13).

Jeg har over gjengitt hvordan Schiefloes samfunssikkerhetsmodell henter inspirasjon fra ulike deler av sikkerhetsfaget, for å kunne lage en modell for hvordan man skal lage et

resilient samfunn. På forskningspørsmålet mitt om hva som skiller sikring fra ulykkesforebygging synes Schiefloes svar å være at det er svært lite. Schiefloes modell er snarer ulykkesforebygging applisert på terrorforebygging på samfunnsnivå. Begrepene som benyttes kommer fra safety-faget som helhet og det er lite henvisninger til eksempelvis statsvitenskapelige drøftinger om terrorisme, eller politifaglige om kriminalitet.

På forskningspørsmålet mitt om hva som kjennetegner barrierer innen sikringsfaget er Schiefloes syn basert på en bow-tie modell der man har sannsynlighetsreduserende tiltak på venstre side av modellen, og konsekvensreduserende på høyre.

Som nevnt ovenfor, ser Schiefloe barrierer som både sannsynlighets- og konsekvensreduserende. Siden hans samfunnssikkerhetsmodell er på et såpass deskriptivt nivå, er det heller ikke slik at han på den ene siden kan sies å vektlegge noen av barrierene sterkere enn andre. Alle må være på plass. På den annen side er det høyeste nivået samfunnets funksjon, og det er derfor lett å tenke seg at selve gjenopprettelsen, eller de av samfunnets kvaliteter som fremmer rask normalisering er det aller viktigste. Essensen av samfunnssikkerheten er robustheten overfor de uønskede handlingene. Siden Schiefloe henter begrepene fra safety-feltet, er det altså ikke noe vesentlige skiller mellom tilsiktede handlinger og ulykker.

3.2 Bjørgos kriminalitetsforebyggende modell

Bjørgos kriminalitetsforebyggende modell kommer fra politifaglig hold, og når man kikker på litteraturlisten er det slående hvor lite overlapp den har med for eksempel Schiefloes modell. Like fullt er Bjørgos overordnede modell svært lik Schiefloes, noe som er et indirekte tegn på at mitt forsøk på å forbinde politifaget med risikostyring i kapittel 5 kan gi gevinster.

Bjørgos tekst er også et sjeldent eksempel på at man behandler sikring mot alle former for tilsiktede handlinger innenfor samme kontekst, spesielt siden den er evidensbasert. Terror blir behandlet som en form for kriminalitet, og de virkemidler som benyttes for annen kriminalitetsreduksjon blir også benyttet for denne.

Bjørgo plasserer sin modell som et forsøk på å integrere fire modeller for kriminalitetsbekjemping: "...både den tradisjonelle sosiale og personrettede kriminalitetsforebyggingen, den situasjonelle forebyggingsstrategien som handler om å gjøre det vanskeligere å begå kriminalitet, den strafferettslige kriminalitetsbekjempelsen og perspektiver på samfunnsikkerhet og krisehåndtering" (Bjørgo 2015, 13).

Ved å kombinere disse fire retningene innen kriminalitetsforebygging er tanken at modellen skal kunne brukes til å motvirke alle former for kriminalitet, fra boliginnbrudd til terrorisme. Verdien som skal beskyttes er ikke så eksplisitt som hos Schiefloe, men trusselen er altså "kriminelle handlinger". Modellen er sammensatt av ni kriminalitetsforebyggende mekanismer. En mekanisme er i denne sammenhengen noe som kan igangsettes av ulike aktører på ulike måter, ut fra hvilken type kriminalitet det er snakk om (Bjørgo 2015, 14). Vitenskapsteoretisk er det en forklaringsmodell for årsakssammenhenger. (Bjørgo 2015, 18). Mens jeg gjengir de mest relevante trekkene vil jeg benytte Bjørgos begreper som for eksempel mekanismer og virkemidler, men jeg vil i kapittel 5 benytte mekanismene som risikoreduserende tiltak. Jeg vil først beskrive de ni mekanismene før jeg går i detalj på hver enkelt av dem. Det er:

- bygge og vedlikeholde normative barrierer mot å begå kriminelle handlinger
- redusere rekruttering til kriminelle miljøer og aktiviteter gjennom å fjerne eller reduserer samfunnsmessige og individuelle årsaker og prosesser som fører til kriminalitet
- avskrekking: få potensielle gjerningspersoner til å avstå fra kriminelle handlinger gjennom trussel om straff eller andre negative konsekvenser
- avverging av kriminelle handlinger ved å stanse dem før de gjennomføres
- inkapasitering (eller uskadeliggjøring) ved å frata gjerningspersoner evnen (kapasiteten) til å gjennomføre nye kriminelle handlinger
- vanskeliggjøre gjennomføring av kriminelle handlinger og beskytte sårbare mål
- redusere skadevirkninger av kriminelle handlinger
- redusere gevinster av kriminelle handlinger
- rehabilitering: hjelpe person som har vært involvert i eller straffet for kriminalitet til å slutte, og komme tilbake til et liv uten involvering i kriminalitet.

(Bjørgo 2015, 1)

I likhet med Schiefloes modell ser man av de ulike mekanismene hvordan også disse er innrettet mot samfunnet som helhet, og ikke innrettet mot en virksomhet. Gitt formålet i oppgaven må dette tas hensyn til når jeg senere skal utlede hvordan man skal innrette et styringssystem på virksomhetsnivå. For eksempel er de handlinger man kan foreta seg overfor "voldelige ungdomsgjenger" i mindre grad noe som har overføringsverdi til en virksomhets sikringsstyring.

Bjørgo bruker fem "ideelle" kriminalitetstyper for å vise at det er allmenne og effektive mekanismer. Gitt oppgavens fokus har jeg funnet det mest fornuftig å benytte eksemplene hans knyttet til terrorisme og organisert kriminalitet. Bjørgo deler mekanismene inn i de som forhindrer at lovbrudd skjer, de som benyttes når lovbrudd har skjedd, og de som skal forhindre at lovbrudd skjer igjen (Bjørgo 2015, 26). Den første er selve tanken, eller ideen om at man ikke skal bryte loven.

Bygge og vedlikeholde normative barrierer mot å begå kriminelle handlinger.

Dersom det eksisterer en normativ barriere mot å begå lovbrudd, som etterleves av borgerne, er dette en måte å forhindre at lovbrudd foretas. Bjørgo henviser til kriminologisk forskning som finner at: "Positiv sosialisering gjennom oppvekst, samhandling i sosiale fellesskap og integrering av moralsystemer i vår personlighet bidrar til å bygge og internalisere disse normative barrierene mot å begå kriminalitet" (Bjørgo 2015, 27). Med en henvisning til Wikstrøm (2014) sies det at menneskets handlingsmønstre er regelstyrte innenfor den sosiale kontekst man operer i. Om de reglene som man internaliserer tilsier at å bryte loven er en opsjon vil det være lettere å gjøre det. Eksempel: For noen vil det aldri være en opsjon å true eller slå ved en uenighet om et økonomisk oppgjør, for andre er dette et taktisk valg.

Normative barrierer mot å begå kriminelle handlinger er også noe som utvikles gjennom de relasjoner borgerne har til representanter for statsmakten. Eksempelvis når man samvirker med NAV eller politiet: Dersom man opplever at slike representanter behandler deg rettferdig og forutsigbart vil man i større grad oppleve at det er riktig å følge loven. Motsatt: om disse er korrupte og dermed ikke er til å stole på, men noe som kan

manipuleres utfra pengegaver eller annet press, er loven i mindre grad en rettferdig dommer og i stedet noe som bare står i veien for egen vinning. I slike tilfeller vil borgerne bare følge loven i den grad de har frykt for at lovbrudd skal oppdages.

Et annet poeng er at man har ulikt forhold til de strukturer som skal bidra til å opprettholde eksisterende skiller mellom rett og galt. Empati kan normalfordeles utfra en Gausskurve - og Baron-Cohen (2011) viser at dette er et "normalt" trekk ved alle samfunn. Bjørgo henviser også til Milgram (1974) som viste hvordan man i visse situasjoner kunne utføre handlinger man egentlig var imot, som å påføre andre smerte, dersom autoriteter sa det var riktig. På bakgrunn av dette må vi slutte at: Det finnes noen som rett ut sagt ikke bryr seg om lov og rett, og om det de gjør er galt eller påfører skade, og i tillegg at "de fleste" kan påvirkes til å gjøre noe de mener er galt. En meta-studie viser at prosentandelen som med vilje foretar seg kriminelle handlinger varierer mellom 28 og 91 (Blass 1999).

Redusere rekruttering til kriminelle miljøer og aktiviteter

Forebyggingsmekanismen er her innrettet mot å forhindre at man begynner med kriminalitet, og deretter fortsetter. For Bjørgo er det viktig at man kan arbeide både på makro, meso og mikronivå, gitt hans generelle fokus på forebygging av all kriminalitet (Bjørgo 2015, 48). Boken hans gjennomgår derfor fem ulike former for kriminalitet. Med bakgrunn i oppgavens fokus på det klassiske sikring-feltet, kan det være interessant å se på dette om man tenker på å redusere trusselen fra organisert kriminalitet. Bjørgos eksempel er knyttet til organisert kriminalitet med utgangspunkt i 1% MC-klubber. Prosentbegrepet angir andelen av motorsykkelinteresserte som er kriminelle (POD 2012, 9). Organisert kriminalitet er ekstra interessant, siden det i de fleste bransjer er dette som medfører den største tapskonsekvensen om angrep lykkes. Til kontrast vil opportunistiske kriminelle oftere ta med seg verdier som ikke medfører særlige tap.

Bjørgo vektlegger her noe som kan kalles en omdømmerettet taktikk. Dette fordi den er innrettet mot å knytte medlemskap i 1% klubbene opp mot kriminalitet, gjerne ved å bruke media, skole, lokalt næringsliv som arenaer hvor det markeres ikke-aksept. Man må ikke gi dem legitimitet, for eksempel ved å delta på åpne familiedager eller andre aktiviteter. Dette også fordi man da senere kan bli satt i situasjoner som kan bli kompromitterende, og brukes til å presse deltakerne til å bistå i kriminell aktivitet (Bjørgo 2015, 137).

Avskrekking: få potensielle gjerningspersoner til å avstå fra kriminelle handlinger gjennom trussel om straff eller andre negative konsekvenser

For å gjøre kostnadene ved å delta i kriminelle MC-gjenger større, kan man bruke både "tradisjonelle strafferettslige reaksjoner, rettighetstap og mer uformelle sosiale sanksjoner" (Bjørgo 2015, 139). De strafferettslige er basert på at deltakerne i klubbene blir anmeldt hyppigere, og slik får mer fengselsstraff. Dette kan utøves av politi og justismyndigheter. Andre tiltak er uro-strategier, basert på å forhindre treff, gjennomføre visitasjoner, beslag og kontroller og annet som forstyrrer det sosiale i klubbvirksomheten, som reduserer utbyttet ved å delta. Å få frem hvor lite attraktivt det kan være å delta i slike miljøer for eksempel for kvinner, (og ved redusert deltagelse av kvinner, kan det også bli færre menn) er en annen måte å sosialt ekskludere gruppen (Bjørgo 2015, 148). I den grad man da jobber med å ekskludere og øke kostnaden utenom det strafferettslige systemet er også sivilsamfunnet bredt her en aktør. For eksempel ved ikke å benytte innkrevingsfirmaer opprettet av klubbene, og slik skape en gråsone mellom legal og illegal aktivitet. Synlige sikkerhetstiltak vil også høyne kost-vurderingen til de kriminelle, slik at det kan tenkes at de velger andre mål. For eksempel gikk Østfold politidistrikt ut og oppfordret til å la lys og radio stå på for å unngå innbrudd (Nordli and Bjørnstad 2016). Dersom noen faktisk prøver å bryte seg inn vil det ikke ha effekt, men dersom noen tror at det er noen hjemme vil man unngå akkurat det huset. Denne formen for sikkerhetsteater (Schneier 2007) har effekt.

Avverging av kriminelle handlinger ved å stanse dem før de gjennomføres

Kanskje den mest kjente strategien for å forhindre kriminalitet, er å forsøke å stanse den før den gjennomføres. Det vil si å reagere på forberedelser eller forsøk på å gjennomføre kriminalitet. Dette kan være ved at reaksjonsstyrker (Politiet i Bjørgos eksempel) får tak i informasjon om hva som skjer, og deretter intervenerer før selve handlingen utføres. Informasjonen kan tilkomme ved spaning, avlytting, bruk av informanter eller tips.

Inkapasitering (eller uskadeliggjøring) ved å frata gjerningspersoner evnen (kapasiteten) til å gjennomføre nye kriminelle handlinge

Forebyggingsmekanismen er rettet mot å frata kriminelle aktører kapasiteten til å begå kriminelle handlinger (Bjørgo 2015, 153). Eksempler på dette kan være å frata dem

innsatsmidler som skytevåpen, bilder og førerkort, som de organiserte kriminelle trenger for å være i stand til å true, eller utføre ran eller drap med. Et annet eksempel Bjørgo trekker fram er når ledere for terrororganisasjoner blir drept. Spesielt i hierarkiske organisasjoner kan dette vise seg å ha mye effekt (Bjørgo 2015, 233). Eksemplene ovenfor er på gruppe- og individnivå, men eksempelvis er det vanskelig å skaffe seg våpen i Norge, sammenlignet med for eksempel USA. Lovene er innrettet slik at denne kapasiteten er vanskelig tilgjengelig. På samme vis er det regler for hvem og hvordan man kan kjøpe sprengstoff, begrensninger på kjøp av spesifikke kjemiske midler og forbud mot salg av annet. Dette er en form for inkapasitering på samfunnsnivå.

Vanskeliggjøre gjennomføring av kriminelle handlinger og beskytte sårbare mål

Grunntanken er at man skal identifisere og fjerne muligheter for å begå spesifikke kriminelle handlinger. Dette kan innebære å øke kostnaden ved å gjennomføre angrep, som å ha mer og bedre overvåking, beskytte mulige ofre eller å gjøre det mer krevende å gjennomføre. (Bjørgo 2015, 157). Skal man vanskeliggjøre terrorisme kan man for eksempel sette opp kjøretøysperrer i gågater, om trusselen man ønsker å redusere er angrep med samme modusen som det som skjedde i Nice 14. juli 2016. Bjørgo trekker fram at det er mange aktører som kan bidra, for eksempel ved å forhindre at viktig infrastruktur blir slått ut, at man opprettholder god adgangskontroll, at flyreisende blir forhindret i å ta med seg våpen etc. (2015, 237).

Der man kjenner til Modus operandi for forbrytelsene man ønsker å forhindre, kan dette lykkes 100 %, om tiltakene er effektive nok. Eksempelet mitt fra innledningen om væske på fly kan illustrere:

a) Mulighet: det er mulig å sprenge fly ved bruk av en viss mengde væske i riktig blandingsforhold,
b) Tiltak: Å ta med nok væske til å oppnå en effekt

Så lenge tiltaket a opprettholdes er det ikke mulig å gjennomføre b). Nå er det vel sjelden at man er istand til å kontrollere de ulike faktorene så godt som i dette eksempelet, men målet er å redusere muligheten så godt som det lar seg gjøre.

Redusere skadevirkninger av kriminelle handlinger

Så langt har alle mekanismene vært på "venstre side" av bow-tie (Per Morten Schiefloe 2011, 6). Ved å redusere skadevirkningen er således den formen for reaksjon noe som iverksettes idet noe har skjedd. Hos Bjørgo er dette noe som i første rekke utøves av statlige intervensjonsstyrker som politiet, helsevesenet og brann og redning. På det mer forebyggende området har andre etater som Direktoratet for samfunnssikkerhet og beredskap en viktig rolle, spesielt med tanke på det nasjonale risikobilder eller som arrangerer av fullskala nasjonale øvelser. Formålet med de handlinger man foretar seg etter at noe er skjedd, er å redde liv og redusere materielle skader (Bjørgo 2015, 240, 162–163).

Redusere gevinster av kriminelle handlinger

Å redusere gevinstene av kriminelle handlinger henger tett sammen med forrige mekanisme, og kan når det gjelder for eksempel terrorisme være nesten overlappende. Mens når det gjelder organisert kriminalitet er de tiltak som redusere ngevinsten for de kriminelle av vellykkede angrep. Det kan eksempelvis være å sørge for at stjålne penger blir farget, slik at det blir vanskelig å benytte de uten å bli oppdaget. I dette eksempelet vil samfunnets (banken, verditransportørens) tap være det samme, men tiltaket reduserer nytten av foreta seg kriminalitet. En årsak til å ha en begrepsmessig distinksjon også innenfor terrorismefeltet, kan illustreres ved å se på mediedekningen av det. Mens politistyrkens *avbrytelse/forhindring* av aksjoner (mekanismen: å redusere skadevirkning) kan redusere tap av liv, kan *gjenfortellingen* av den samme terroraksjonen føre til at de har mer eller mindre effekt. Bjørgo viser til hvordan gisseltakere i Irak 2004-2005 produserte videoer hvor man skar av hodet på gisler. Når man sluttet å vise disse videoene, opphørte også denne handlingen (2015, 244)

Rehabilitering: hjelpe person som har vært involvert i eller straffet for kriminalitet til å slutte, og komme tilbake til et liv uten involvering i kriminalitet.

Å få noen til å slutte med å bryte loven, forhindrer at de begår ny kriminalitet. Så med dette tiltaket er ringen sluttet: det er om å gjøre å installere de hindringene mot å begå kriminalitet som vi kjenner igjen fra den første mekanismen. Forskjellen ligger i at tiltaket er spesifikt (det er ikke allment i samfunnet) og at det er innrettet mot dem som allerede er

straffet for å bryte loven fra før. Når det gjelder terrorister så har den mest effektive "pasifiseringen" forekommet når gruppene har lagt ned våpnene. Dette har skjedd i bytte mot politiske gevinster, i gjensidige samarbeidsavtaler mellom gerilja/terrorgrupper eller selvbestemt som for eksempel når Rote Armee Fraktion erklærte at deres væpna kamp var over.

Enkeltmedlemmer slutter ofte ved at de blir desillusjonerte. Virkemidlene varierer, men de fleste er preget av man må gi medlemmene et alternativ. Når det gjelder organisert kriminalitet, viser forskning fra Pyroos & Decker (2011) at yngre gjengmedlemmer i større grad gjør det etter påvirkning fra sivilsamfunnet som for eksempel venner og familie, enn ut fra statlig intervensjon.

Oppsummering

Jeg har nå gjennomgått Bjørgos generelle kriminalitetsforebyggende modell fordi jeg anser den som en relevant teori for oppgavens tema. Den kan ved første øyekast virke mer omfattende enn det man kunne forvente er relevant for noen som er primært opptatt av hvordan virksomheter kan begrense tap ved å ha bedre styringssystemer for sikring. Samtidig gir den en god ramme å diskutere ut fra, nettopp ved at den har et såpass bredt perspektiv. Jeg syns også det er relevant å ta den med siden den kommer fra et politifaglig/kriminologisk hold.

Et av forskningsspørsmålene mine er knyttet til barrierer. I likhet med Schiefloe (2011) ser Bjørgo (2015) barrierer både som sannsynlighet- og konsekvensreduserende. Utfra sin forskningstradisjon benytter Bjørgo "mekanismer" som begrep for å betegne det som både hos Kjellen og Schiefloe regnes som barrierer. Sammenlignet med de to andre modellene jeg gjennomgår, er Bjørgos modell preget av et svært bredt sett med virkemidler. "Alle" får en oppgave i å bistå til barrierebygging mot kriminalitet. I safety-sammenheng kan dette synes noe fremmed, kanskje primært fordi litteraturen oftest er rettet mot virksomheter og organisasjoner, og ikke mot samfunnet som helhet. Knyttet til forskningspørsmålet mitt om forskjeller mellom sikring og ulykkesforebygging er kanskje Rasmussen (1997), som fokuserer på målkonflikter, et perspektiv som kanskje ligner mer på Bjørgos, spesielt med tanke på hans fokus på koordinering.

Om man ser på mine innledende betraktninger knyttet til hvem denne oppgaven skal kunne leses av, og brukes til, må jeg nå gå videre til et virksomhetsperspektiv. Jeg har nemlig gått igjennom to helhetlige modeller for sikring mot tilsiktede handlinger, men mangler enda en del på organisatoriske metoder for å oppnå bedre sikring på virksomhetsnivå.

3.3 Kjellens modell for å forhindre ulykker

Jeg har nå gjennomgått to modeller som er innrettet mot å sikre mot villede handlinger. Begge har et bredt samfunnssikkerhetsperspektiv, og inkluderer derfor virkemidler som for mange virksomheter ikke er relevante siden man ikke har myndighet til å utføre dem. Jeg vil vektlegge det interessante i at selv om de har grunnlag i ulike faglige perspektiv, ender de opp med modeller som er svært like. Konvergensen kan tolkes som et uttrykk for modellenes validitet.

Oppgavens formål er knyttet til hvordan man bedre kan styre sikring på virksomhetsnivå, og jeg trenger jeg derfor flere teorikilder. Samfunnsikkerhetsnivået kan blir for “stort” da virksomheter mangler de relevante virkemidlene.

Innen safety-feltet, som utvilsomt har et større akademisk corpus, finnes det mye forskning omkring hva man gjøre på virksomhetsnivå. Kjellens bok Preventions of accidents thorugh experience feedback er (Kjellen 2002) er foreslått av mine veiledere, som eksempel på bok som tar for seg faget ulykkesforebygging og sikkerhetsstyring i bred forstand. At den brukes som lærebok på NTNU er i så måte et tegn på dens viktighet. Men det som gjør den spesielt egnet er at den gjennomgår mange metoder og praktiske aktiviteter for å oppnå bedre sikkerhet. Fremfor å foreslå en one-size-fits-all modell anerkjenner den forskjellene mellom industrier, og har i mente at forskjeller i størrelse betyr noe for hva som kan oppnås, og hvordan tiltak bør utformes. For meg som er ute etter å ta det mest effektfulle fra ulykkesforebygging med meg inn i sikring, er den ekstra nyttig siden den fremstår som en katalog over mulige tiltak og aktiviteter for å oppnå bedre sikkerhet.

Ulykkesforhindring gjennom styringsinformasjon. (Prevention of accidents through experience feedback)

En forutsetning for at noe skal styres, er at det finnes informasjon om det man skal styre, ellers kan man ikke endre retning eller innsatsfaktorer i produksjonsmiljøet. Urban Kjellens modell for å unngå ulykker, er derfor basert på et "Safety, Health and environment information system" (2002, 4). Et slikt system kan gi beslutningsstøtte (styringsinformasjon) til flere viktige områder innenfor sikkerhet, helse og miljø. Kjellens fokus er på hvordan man kan forhindre ulykker som fører til skader på personell, utslipp som forurenser, eller skader på produksjonsmidler. Videre velger jeg å kalle dette for et Helse-, Miljø- og Sikkerhetssystem, (HMS) og understreker at informasjonshåndteringen er en del av dette.

Grunnen til at man ønsker å styre HMS-feltet er selvsagt for unngå tap eller skader. Men det hadde det ikke vært et poeng å gjøre, om man ikke kunne vise til at innsatsen - tiltakene som styringssystemet iverksetter har effekt. Kjellen gjengir forskningsresultater fra 70-tallet og frem til 90-tallet som viser til at virksomheter med lav ulykkesrate kjennetegnes ved:

- godt regime for skade/avviksmeldinger
- velutviklede rutiner for å undersøke arbeidsplassen og rutineoppfølging
- tydeligere tendens til å utrede og undersøke nestenulykker

(2002, 8)

Han viser også til annen forskning som tyder på at ikke bare skade/tapsraten blir lavere, men også at produksjonsraten blir høyere pga færre avbrudd. Så med både høyere produksjonsrate og mindre tap, er viktigheten av å ha et velfungerende HMS-system etablert. Men hva er essensen for å få dette til?

Kjellen åpner med å gjennomgå begrepet "grensebetingelser" (boundary conditions), som omfatter faktorer som ligger utenfor kontrollområdet for den som søker å styre. Poenget er: om du ønsker å lager et bedre HMS-system for å unngå tap og skader, er disse faktorene noe du ikke kan endre. Oppmerksomhet omkring grensebetingelsene er avgjørende for å

få HMS-systemet til å fungere. Jeg vil kort gjennomgå disse før vi går inn på selve systemet og hvilke virkemidler det innebærer.

Størrelse, teknologi og ressurser

Virksomhetens størrelse har betydning, da man i små virksomheter lett vil få vite om skader/tap/avvik, mens i større må man ha en systematikk og formelle kanaler for at dette skal oppnås. En svakhet er eksempelvis når man er mellom 50 og 500 ansatte. Når man er innenfor denne skalaen vil man være for liten til å iverksette et effektivt rapporteringsregime (uten at det koster alt for mye) og for store til at uformell "prat" fører til forbedring.

Det er også slik at noen industrier bruker materialer eller produksjonsutstyr som i seg selv medfører høyere risiko enn andre. Produksjon av kunstgjødsel medfører større eksplosjons- og brannfare enn produksjon av melk eller apper. Kompleksiteten i hvordan noe produseres spiller også en rolle. Er det eksempelvis software som overvåker produksjonen, og endrer produksjonsfaktorer om noe beveger seg mot en ulykke? Isåfall betyr det at algoritemene er viktigere enn menneskeligt skjønn. Og hva skjer om man mottar alarmer fra software: Dersom man selv ikke vet hvordan og hvorfor noe varsles, er det lettere å ta feil valg, eller i mindre grad være i stand til å redusere konsekvensene når noe først har skjedd.

Før et produkt foreligger, har en organisasjon foretatt en beslutning som hva som skal produseres, og iverksatt dette ved hjelp av teknisk utstyr og mennesker med riktig kompetanse (Thorsvik and Jacobsen 2013). Kjellens setting er produksjonselementene stort sett sentrale for leveransene, og de kan koste hundrevis av millioner. Ulykker kan medføre utgifter i milliardklassen. I andre bedrifter, slik som i en bank hvor jeg jobber nå, er alle produksjonselementene billige og utskiftbare. For å oppnå leveransen "salg av fond" trenger man en pc med riktig programvare og nettilkobling og noen som er i stand til å betjene systemet og selge fondet. For slike leveranser vil tap av hovedkvarteret som operasjonssentral medføre mindre driftsutfordringer. Dette fordi man gjerne har backup av alle dataprosesser andre steder. Kompetansen hos de ansatte er kanskje dyr, men heller

ikke denne er unik. Slike grensebetingelser er også viktig når man skal vurdere konsekvenser av tap.

Ressurser handler i denne sammenheng først og fremst om økonomi, og den gjennomføringsevnen til å innføre og forbedre et HMS-system som både mottar og behandler det eksisterende informasjonstilfanget på en tilstrekkelig måte. Tiltakene er vanskeligere å få gjennomført om man har lav omsetning og knappe marginer, i motsetning til om inntjeningen er høy og pilene peker oppover (Kjellen 2002, 12–13).

Organisasjonen

Organisasjonens beslutningsstruktur har betydning for hvordan HMS-systemet skal implementeres. Man kan ha hierarkiske organisasjoner, organisasjoner med ulike kulturer, det kan være ulike former for maktkamp og ulike insentiver. Dette er relevant når man skal innføre tiltak, siden disse må være tilpasset bedriftskultur og struktur.

Arbeidsgivers ansvar og krav fra myndighetene

Virksomheter forholder seg til et samfunn hvor det er lovkrav til hva arbeidsgiver skal gjøre og hvordan for å unngå skader og tap. Dette kan for eksempel henvise til at man skal ha oversikter over de største risikoene, og kunne vise til aktiviteter for å unngå skader, slik som det står i den norske arbeidsmiljølovens kapittel 4 eller internkontrollforskriften se Kongsvik (2013, 27).

Beste praksis

Når ulike bedrifter kjøper tjenester av hverandre, eller ønsker å forsikre seg om at leveransene holder en kvalitetsmessig og/eller etisk standard, kan man velge å benytte seg av nasjonale eller internasjonale standarder. Eksempelvis kan man velge å bare kjøpe hos leverandører som er sertifiserte av uavhengige selskaper, eller på annen måte be om bevis på at leveransene holder tilstrekkelig kvalitet. I Norge reguleres dette av Norsk standard, som er tilknyttet International Organization for Standardization (ISO).

Jeg har da gjennomgått noen eksterne/interne faktorer som man må ta hensyn til når man skal innføre et HMS-system. Jeg vil nå gå inn i selve modellen, både for å fremvise

eksempler på typiske kjennetegn ved safety-regimer, men også for å hente virkemidler til egen konstruksjon av et styringssystem for sikring i kapittel 6.

Data, monitorering og risikoanalyse.

Alle HMS-systemer må inneholde elementene data (innhenting og bearbeiding av informasjon), monitorering (at systemets elementer produserer og leverer som planlagt) og risikoanalyser. Jeg vil i det følgende beskrive hvordan dette er tenkt gjennomført.

3.3.1 Innhenting og bearbeiding av informasjon om avvik og ulykker

De fleste land har lover og regler som sette rammer for hvordan arbeidsoppgaver skal utføres, samt hvordan man skal rapportere og forbedre dersom noe har gått galt, eller nesten har gått galt (Kjellen 2002, 16). Det betyr at en virksomhet må ha et eller annet system for å håndtere risiko.

I den grad man registrerer avvik eller nesten-ulykker, representerer dette også en mulighet til å lære. Dersom noe nesten gikk galt en dag, kan det godt være at noe kan gjøres med dette for å unngå at det går galt neste gang. Om dette rapporteres videre til industrielle organer eller myndighetene, kan det brukes til å fortelle andre om farer, og kanskje også disse virksomhetene kan unngå å bli utsatt for noe, ved å lære av andres feiltrinn. (Kjellen 2002, 146).

Det viktigste elementet er at systemet må innrettes slik at det er designet for å lære av den informasjonen man samler inn; det gjøres ikke for å finne en syndebukk enten i den konkrete arbeidsoperasjonen, eller i juridisk forstand. Da skaper man ikke insentiver for å rapportere nestenulykker, og man kan risikere å gå glipp av vital informasjon.

Kjellen anbefaler at ulykker granskes på tre nivåer:

1) Førstelinje, eller dem som utfører gransker umiddelbart når noe har skjedd, eller holdt på å skje. Dette må gjøres av de involverte, lokal HMS-koordinator og nærmeste leder.
2) Et utvalg av alvorlige hendelser, eller hendelser som har potensiale til å bli det ut fra konsekvensvurderinger, granskes av en dedikert problemløsningsgruppe.

3) I noen tilfeller kan man også sette ned egne utvalg, gjerne uavhengige og med et fritt mandat til å påpeke forbedringer (Kjellen 2002, 147).

Man kan forvente ulike funn fra de ulike nivåene. Førstelinje vil kunne påpeke avvik fra rutiner og prosedyrer, eller forbedringer i eksisterende. Andrelinje vil i større grad se på faktorene rundt - er det for eksempel slik at lignende hendelser kan skje andre steder. Mens tredjelinje også vil se på rotårsaker som: Er det over tid satt av for lite ressurser i HMS-arbeidet, er organisasjonsmessige problemer knyttet til implementering etc. Et eksempel på det siste kan være Statoil sin granskning av In Amenas-rapporten, som viste til rotårsaker som at safety-problemer ble fulgt opp og var del av et system, mens trusler fra villede handlinger ikke ble behandlet systematisk.

Jeg har nå gjennomgått organiseringen. For å gå i dybden er det nødvendig å si mer om hvordan man gransker, og hva man ser etter.

3.3.2 Ulykkesmodeller

Ulykkesmodeller trekkes fram som meget viktige, siden de gir basis for hvilke rotårsaker man kan finne, og dermed hvilke problemer man løser. Men dette er ikke uproblematisk. En modell gir en ramme eller en kikkert som former det man finner - *what you look for is what you find* (Lundberg, Rollenhagen, and Hollnagel 2009) og så fikser man det. I verste fall kan det hende at valget av modell, gjør at de vesentligste årsakene ikke avdekkes. Det dette forteller oss, er at vi må være nøye med å forstå og skjønne begrensningene i hvilken modell vi velger, siden modellen vil være konstituerende for kunnskapen som utvinnes. Kjellens oppsummerer hva en ulykkesmodell kan/bør hjelpe oss med slik:

- å lage et mentalt bilde av den kausale kjeden ulykken står i
- Hjelpe oss i å stille de riktige spørsmålene, og vite hvilke data vi faktisk trenger
- etablere regler for hvor langt i en ulykkessekvens man skal lete etter årsaker, for å unngå en uendelig regress
- på en oversiktlig måte avdekke om alle relevante data er innsamlet
- vurdere, strukturere og oppsummere innsamlet informasjon
- vurdere og analysere tilknytninger mellom data, og koble disse

- identifisere og vurdere tiltak for å redusere risikoen for at den samme ulykken skal skje igjen
- Ulykkesmodellen letter kommunikasjon ved at man sikrer at interessenter diskuterer det samme når tiltak skal besluttes senere. Man får felles forståelse for problemet

(Kjellen 2002, 31)

Feltet ulykkesgransking har vært forsket på lenge, og med henvisning til bl.a Herbert W. Heinrich (Heinrich 1941) viser Kjellen hvordan tidligere viten om emnet baserte seg på ideer som i korthet gikk ut på at enten gjorde folk feil, eller så var det noen uheldige mennesker som ble utsatt for ulykker. Dagens forskningsresultater har andre perspektiv på hva som er årsaker til hvorfor noe går galt. Det som trekkes fram er systematiske undersøkelser som ser etter hvor i sikkerhetsstyringen det sviktet. Dette i motsetning til at man ser etter en syndebukk. Var det satt av for lite ressurser fra ledelsen til å sørge for et godt sikkerhetsarbeid? Fantes det urealistiske/farlige krav knyttet til produksjonshastighet? Hadde personen som ble skadd eller utløste ulykken tilstrekkelig opplæring i arbeidsoppgavene? Var planen for hvordan arbeidsoppgavene skulle utføres optimalisert for å unngå ulykker?

Det finnes mange ulike modeller for ulykkesgransking som har ulike akronymer, og i denne sammenhengen er det ikke viktig å gjennomgå de ulike modellene. Kjellens modell er basert på et arbeid han har gjort sammen med Jan Hovden (Kjellén and Hovden 1993). Når han oppsummerer dette, sier han at essensen for å kunne analysere ulykken er:

1. Forståelsen av tid: ulykken må forstås som ledd av en kjede av hendelser. En utviklingsprosess der ulike forutsetninger for at noe kunne gå galt starter. I oppstarten er det manglende kontroll, som leder til tap av kontroll over energier som utveksles i systemet, som igjen leder til tap/skade.
2. Oppstarten ses på som avvik fra hvordan man normalt skulle produsere/arbeide
3. Skaden eller tapet er resultatet av at ukontrollert energi møter en person, materiell eller miljø som skades.
4. Skaden eller ulykken fører til tap.

(Kjellen 2002, 55)

Alt dette kan systematiseres på ulikt vis. Mange varianter av ulykkesgranskning finnes, og granskeren må beslutte hvilken som benyttes. Ulykkens kompleksitet og omfang må selvsagt tas i betraktning, og man må også huske på at ulike innsamling- og bearbeidingsmodeller for data, som nevnt tidligere kan produsere ulike resultat. Innen sikringsfeltet opplever jeg ikke noen konsensus om hvordan det bør gjøres. Eksempelvis kan det argumenteres for at 22.juli rapporten ikke har noen metode (NOU 2012:14). Det er snarere en gransking av handlingsforløpet med kvalitative vurderinger av ulike trinn. Jeg kjenner ikke til noen forskning som har gjennomgått hvilke metoder som oppnår mest effekt, det vil si at flest forbedringer gjennomføres i etterkant. Dette skyldes nok det relativt enkle faktum at de fleste ulykker/hendelser bare granskes med én metodisk bakgrunn, og man kan derfor ikke sammenligne to virksomheters foretatte endringer, siden det bare en en virksomhet som vanligvis granskes.

Min opplevelser er at om man bruker kompliserte årsak-virkningskjeder med mange faktorer som for eksempel Rasmussen (1997), gjør dette at man oppnå mindre enn om man benytter modeller med mer pedagogisk slagkraft. Som for eksempel den intuitive menneske, teknologi, organisasjon (Sintef 2004). Med oppnå mindre, mener jeg at man får gjennomført færre relevante tiltak. For det er jo også viktig at tiltakene er gode og adresserer rotårsaker. Ellers kunne man bare gjennomført mange lite ressurskrevende tiltak som ikke har effekt. En fordel med å tenke på det pedagogiske når man velger ulykkesmodell, er mulighetene til å kommunisere resultatet. Om resultatene blir forstått, kan det gi mer eierskap hos de som skal gjennomføre tiltakene. Og dette er ikke en kritikk av forannevnte Rasmussen. Eksempelvis er jeg overbevist om at 22. julirapporten både hadde vært mye bedre faglig, og kunne hatt større innflytelse om den hadde basert seg på Rasmussens modell. Den kunne da vist hvordan “alt henger sammen med alt” på en bedre måte enn en rapport som i de fleste gjengivelser konkluderer med at “Hovedkonklusjonen var bedre ledelse og endring av kultur.”(Lerø 2016). Det er ganske nært å si at det som gikk galt var enkeltlederes mangel på prioritering. Rasmussen ville fått fram at de ikke prioriterte i et vakuum.

Vi har nå gjengitt noen måter å se på hvordan ulykkesgransking kan foretas. I en styringsmodell må man ha en måte å behandle avvik. Jeg har tilkjennegitt min preferanse for MTO-modellen, på bakgrunn av dens pedagogiske kraft. Jeg ser det også som en stor

fordel at Nasjonal Sikkerhetsmyndighet nylig har gått bort fra administrative, fysiske og logiske tiltak, og i stedet benytter MTO, for å forklare sårbarheter og tiltak (NSM 2016). Felles språkbruk letter felles måloppnåelse, og gir også større tyngde når praktikere skal få støtte til tiltak hos beslutningstagere. Når vi går over til barriere-begrepet, er dette også noe hvor man ofte grupperer utfra om de er menneskelige, teknologiske eller organisatoriske.

3.3.3 Barrierer og risikoanalyse

Jeg har nå gjennomgått hvordan man i informasjonsinnhentingssystemet samler inn data som skal brukes til å innføre tiltak som er barrierer mot at "energi skal komme på avveie". Jeg vil nå gå nærmere inn på hva barrierer er, og hvordan man finner dem. Slik besvarer jeg også underspørsmålet mitt om hva som kjennetegner safety-barrierer.

Man kan starte med det åpenbare: Det er en klar fordel å kunne innføre barrierer før ulykken oppstår, og ikke bare i etterpåklokskapens lys. Jeg vil derfor åpne med å gjennomgå strategier for å unngå ulykker, før jeg gjennomgår risikoanalyse som er en måte å være etterpåklok på forhånd. Jeg går så over til respons på hendelser, som er knyttet til hvordan redusere konsekvensene når noe er gått galt.

William Haddon (1980) har lansert en matrise som er ment å kunne forhindre at ulykker oppstår. Kjellen har adaptert denne til eget behov, dette er:

Strategier knyttet til kilden

- Unngå at den farlige energien produseres (kinetisk, termisk, elektrisk)
- Endre mengden av energi
- Unngå ukontrollert utløsning av energi
- Endre mengden av energi som kan utløses

Strategier knyttet til barrierer

- Skille det som kan skades fra det som skades
- Skille det som kan skades fra det som skades ved hjelp av fysiske barrierer
- Endre kvaliteter ved energien som utløses, for å gjøre den mindre skadelig.
- Endre kvaliteter ved det som skal beskyttes slik at det har større motstandskraft

Strategier knyttet til det sårbare objektet

- Gjøre det sårbare målet mer motstandsdyktig mot energien
- Begrense skaden
- Rehabilitere det sårbare målet

(Kjellen 2002, 40)

Å tenke barrierer på denne måten er en måte å kunne behandle både rotårsaker og konsekvenser av energi på avveie. For å benytte strategiene er det vanlig å ta utgangspunkt i en risikoanalyse. Navnet er felles for flere ulike metoder. Fellestrekkene er:

1. Definere analyseobjeektet og beslutte scope
2. Identifisere farer og situasjoner hvor mennenesker eller andre verdier kan eksponeres for faren
3. Estimere sannsynlighet for eksponering, og konsekvenser dersom dette skjer.

(Kjellen 2002, 265)

Når risikoanalysen er foretatt, vurderes resultatet av analysen med risikoakseptkriterier fastsatt i risikostyringsprosessen. Kjellen gjengir en tabell hvor det fremkommer at de ulike metodene har ulike parametre for måling av risiko. Eksempelvis vil en *feiltreanalyse* måle risikoen i frekvensen av topphendelsen sett opp mot kjente konsekvenser, en *Sikker jobbanalyse* vil plassere risikoen i en tredelt lav-medium-høy risikomatrise, og *Crisis Intervention in Offshore Production* vil måle risiko i hvilke konsekvenser menneskelige feilhandlinger får. Poenget med å beskrive dette er å få fram at også her ser vi at i likhet med ulykkesgransking vil metoden man benytter for å avdekke, estimere og visualisere risiko, gi innvirkninger på hvordan man agerer. Dermed kan altså to ulike risikoanalysemetoder ende opp med å anbefale ulike tiltak på samme prosess.

Et annet moment som vektlegges blant annet av Aven, er usikkerhet knyttet til risikovurderingen (Aven et al. 2013). Hvor sikker er konsekvensvurderingen? Hvilke av vurderingene har vi godt informasjonsgrunnlag til: verdivurderingen, konsekvensvurderingen, effekten av tiltak osv. Poenget er at vi skal uttrykke det når

risikoanalysen foretas, slik at beslutningsgrunnlaget for å akseptere, håndtere eller å unnlate å ta risiko fremkommer.

Innen sikringsfaget benyttes barriere oftest som betegnelse på sikringstiltak innen fysisk sikring. Mens tiltak er det mer overordnede begrepet. Jeg går utfra at det skyldes at når man skal beskytte seg mot en bevegelig trusselaktør vil assosiasjoner knyttet til barrierers passivitet ikke være dekkende for den årvåkne tilpasningen av det risikoreduserende tiltaket som sikring mot en tenkede aktør krever. I denne oppgaven benytter jeg begge begrepene, avhengig av om jeg beskriver ulykkesforebygging eller sikring, men både tiltak og barrierer er risikoreduserende.

3.3.4 Respons

Det siste elementet når energien er på avveie, er å begrense skade. Det vil si at man må respondere, og minimere skade så effektivt som mulig. Responsen kan være knyttet til automatiske systemer som f.eks at sprinkleranlegg slår seg på når grenseverdier for varme eller røyk nås. Eller det kan være at et kriseteam samles for på et systematisk vis sette inn alle ressurser for å raskest mulig begrense skaden. Ofte vil man ha forhåndsplanlagte og øvde responser, som en kontinuitets- og responsplan for å håndtere DDOS-angrep, eller nedetid på strømtilførsel.

Jeg har overfor behandlet barrierer som skal forhindre at energi kommer på avveie, sammen med en grov gjengivning av essensen av risikoanalyser. Dette fordi man vanskelig kan tenke seg gode barrierer uten at det er basert på informasjon om hva som har gått galt, eller hva som kan gå galt.

Gitt oppgavens scope ser jeg det som mindre hensiktsmessig å gå mer i dybden her på forskjeller mellom industrier, som vil kreve ulike typer analyser. Jeg vil gjennomgå hvordan man kan måle sikkerhet, siden dette er noe som man kan gjøre etter at man har innført barrierer som skal beskytte mot ulykker. Jeg anser også dette som et felt hvor sikring kan kompletteres fra safety.

3.3.5 Sikkerhetsindikatorer og måling av sikkerhetstilstanden

Har man innført et regime, vil man gjerne vite hvor godt det fungerer. I utgangspunktet kan man tenke seg at om ulykker ikke skjer, så er alt sikkert. Men om man tenker noe mer proaktivt vil man jo helst finne ut av om ulykker holder på å skje, før det skjer, og da må man se etter indikatorer på at noe er galt.

Kjellen sorterer sikkerhetsindikatorer ut fra tre overordnede kategorier:

1) Man kan måle sikkerhet i hvor mange arbeidstimer som går tapt på bakgrunn av skader (*Lost- time injury frequence ratio*).
2) Man kan måle prosess-sikkerhet. Dette kan gjøre på flere måter, men et eksempel er å ta utgangspunkt i avviksrapportering, og se om det er en systematikk i hvor avvikene forekommer. Dette er spesielt relevant dersom produksjonsmåte er relativt likt over lang tid. En tilknyttet måte er å ta utgangspunkt i adferd, for å etablere standarder for sikker oppgaveløsning, og følge opp dem som avviker fra dette. (Kjellen 2002, 242–244)
3) En tredje variant er knyttet til kausale faktorer og rotårsaker. Her er ledelsen sentral og den fokuserer på å evaluere organisasjonen ut fra en standard. Et eksempel kan være Veritas-utviklede International Safety Rating System (ISRS), som på bakgrunn av sin utbredelse kan si noe om hvordan virksomheten måles mot tilsvarende virksomheter. Spørsmålene er bredt innrettet mot alt fra utdanning av ledere og personell, kommunikasjonsformer, hvor god kontroll man har på logistiske elementer og mer(Kongsvik 2013, 57). Svarene graderes ut fra en "modenhets"-skala, hvor toppresultat betinger at man kontinuerlig på alle nivåer jobber med å avdekke feil og mangler ved eget sikkerhetssystem (Kjellen 2002, 248–252).

Kvaliteten på sikkerhetsindikatorer kan vurderes utfra følgende kriterier:

- observerbare og kvantifiserbare
- relevante indikatorer knyttet til risiko for tap
- mulig å endre dersom faktorer i produksjonsprosessen endres
- kompatible med andre ledelsesverktøy og beslutningsprosesser
- forståelig og transparent i hvordan de lages og brukes

- resultatene må ha integritet, noe som oppnås når insentivene er riktige

(Kjellen 2002, 136)

3.3.6 Fra ulykkesforhindring til robusthet - oppsummering om safety

På et overordnet nivå har jeg nå gjennomgått metoder som benyttes for å oppnå god sikkerhet mot ulykker i en virksomhet. Jeg åpnet med å ta for meg hvorfor og hvordan informasjonsinnhenting og bearbeiding er basis for styring. Jeg gjennomgikk deretter ulike metoder denne kan innhentes på, risikoanalyser, ulykkesmodeller og sikkerhetsindikatorer. For min oppgave er det nyttigste fra Kjellens bok hvordan den direkte er knyttet til styring på virksomhetsnivå. Dette har ikke har vært tilfelle for de to andre modellene som har behandlet sikring mot tilsiktede handlinger.

Et nøkkelbegrep i sikkerhetsforskning i nyere tid er resilience, som oftest oversettes til robusthet. Essensen er at man fremdeles kan levere/produsere selv om uventede problemer eller hendelser forekommer. Wreathall (2006) har forsket på hva som kjennetegner robuste organisasjoner, og resultatene gjengis slik i Kongsvik (2013, 18):

- Engasjement og forpliktelse fra toppledelsen: Toppledelsen anerkjenner betydningen menneskelige prestasjoner har for sikkerheten, og følger dette opp gjennom handling.
- Rettferdig kultur: rapportering av uønskede hendelser oppmuntres og belønnes, selv om straffbare forhold ikke tolereres.
- Læringskultur: uønskede hendelser medfører tiltak og endringer og bortforklares eller benektes ikke.
- oppmerksomhet: Organisasjonen er i forkant av mulige problemer knyttet til menneskelige prestasjoner og er forberedt på at de kan oppstå
- Fleksibilitet: Fleksibilitet er evnen organisasjonen har til å møte nye eller komplekse problemer på en slik måte at virksomheten ikke blir påvirket. Dette krever at beslutningsmyndigheten er delegert til de som er nær problemet, som førstelinjeledere.
- Grensebevissthet: Organisasjonen er klar over egne sikkerhetsmarginer og hvor nær grensene man opererer.

Det kan være verdt å nevne at ingenting av dette bryter med de metoder som er gjennomgått hos Kjellen. Men det kan argumenteres for at man med robusthet kan oppnå et bredere fokus, og dermed en litt annen innretning på tiltak. For eksempel sier Hollnagel at kjernen av robusthet er "The key feature of a resilient system is its ability to adjust how it functions" (Hollnagel 2011). Han skiller da mellom noe han kaller safety 1, og safety 2. Rammene for informasjonsinnhenting knyttet til safety 1 sies da å være å se på hva som har gått galt, eller hva som kan gå galt. Informasjonsinnhentingen er således enten proaktiv eller reaktiv. Men Hollnagel utvider safety 2 begrepet, og sier at robusthet kommer når man fokuserer på organisasjonens evne til å forbedres og utvikles når noe ikke går som planlagt. Å styrke leveransen er det avgjørende kriteriet for om noe er robust eller ikke. Han definerer safety 1 som det å redusere frekvens og konsekvens av hendelser, mens safety 2 handler om å forbedre et systems leveranser satt opp mot ulike negative hendelser eller betingelser. Begrepet safety 2 dekker derfor noe bredere enn bare å unngå/minimere tap; det er knyttet til forbedring eller robustifisering. Det har ikke en ontologisk kjerne, og gis derfor en funksjonell beskrivelse knyttet til *betingelser for endring*. Han summerer opp de fire betingelsene som:

- evnen til å respondere på informasjon eller endringer i faktorer
- evnen til å monitorere relevante hendelser eller produksjonsfaktorer internt eller eksternt
- evnen til å lære og implementere endring
- evnen til å forutse mulige hendelser eller produksjonsfaktorer som kan komme til å hindre leveranser.

(Hollnagel 2011)

Målet med safety 2 er ha fokus på hvordan man gjør leveransen mer sannsynlig uavhengig av ulike faktorer.

Kjellen behandler ikke direkte sikring mot tilsiktede handlinger, så forskningsspørsmålene om barrierer innen sikring eller forskjeller mellom fagfeltene har han få svar på. Men som det fremgår i kapittel 5 er det likefullt svært mange elementer å benytte, og jeg har da også strukturert modellen utfra et informasjonsstyringssystem slik det fremgår i kapittel 3.3.1. Det som da gjenstår av forskningsspørsmål er å grundigere gjennomgå forskjeller mellom ulykkesforhindring og sikring.

4. Forskjeller mellom ulykkesforebygging og sikring

Jeg har overfor gått igjennom tre perspektiver som skal hjelpe meg med å besvare hovedproblemstillingen min. Men et av forskningsspørsmålene mine er knyttet til forskjeller på ulykkesforebygging og sikring For å besvare dette vil jeg ta for meg måling av sikkerhet, deretter statistikk og risikostyring. I dette kapittelet ønsker jeg altså å besvare forskningsspørsmålet: Hva skiller sikring fra ulykkesforebygging?

4.1 Å måle et fravær

“Vi som arbeider med sikkerhet får sjelden oppleve at vi vinner. En seier for oss er når ting ikke skjer, og det er alltid vanskelig å ta æren for det som ikke skjer.” (Thon 2013).

På overordnet nivå synes dette sitatet å være beskrivende både for dem som arbeider med sikring og ulykkesforebygging. Målet er å unngå tap av verdier, og når man har laget et styringssystem som unngår dette - enten ved at ingen utøver/lykkes i å begå et angrep, eller at ingen ulykker forekommer - har man lykkes. Men dykker man litt inn i det, ser man at det er forskjeller.

For å unngå en gasseksplosjon, kan man eksempelvis merke en gasstank med fareskilt for å gjøre de som arbeider ekstra observant på at de ikke skal foreta seg noe risikofylt i nærheten av den. For en trusselaktør er gasstanken en sårbarhet som kan utnyttes og dette fareskiltet vil fortelle trusselaktøren hvor målet er.

For å unngå ulykker må man unngå og eliminere sjanser for tap. Et ofte benyttet begrepstrekløver for å gruppere og optimalisere produksjonsforhold er menneskelige, teknologiske og organisatoriske faktorer. La meg illustrere ved å beskrive en ideell situasjon. Tanken er å få frem forskjellen på iverksetting av tiltak innenfor ulykkesforebygging og sikring. Man kan for eksempel tenke seg at man i en produksjonsprosess benytter seg av kokende vann for å drepe bakterier. Dette gir fordeler knyttet til produktets sterilisering. Men samtidig øker dette risikoen for at vannet skal koke over, og at kokekaret skal eksplodere. Man kan videre tenke seg at man er ansvarlig for å forhindre ulykker på denne arbeidsplassen. Man foretar da kanskje en risikoanalyse i tråd med kap 3.3.3, og det viser seg at Haddons første strategi kan benyttes: Dersom man i

produksjonsprosessen i stedet benytter et kjemisk stoff, kan man på tilfredsstillende vis sterilisere produktet. Dersom dette ikke gir andre ulemper vil risikoen for at vannet skal koke over og karet eksplodere være borte.

Innen sikring er det slik at hver gang en modus "lukkes" vil aktøren se etter andre utnyttbare sårbarheter. Modus henviser her til at en spesifikk angrepsmåte umuliggjøres. Sikrer man et spesifikt arrangement mot terror, vil terroristen benytte seg av et annet arrangement med mindre sikring. Finner man en måte å beskytte seg mot alle typer angrep med et visst modus, påvirker dette kost-nytte vurderingen til terroristen. Eksempelvis: helt siden 1980-tallet har man i London gjort det vanskeligere å plassere koffertbomber uoppdaget i søppelspann ved å minske dimensjonen på åpningen, produsere mindre spann med gjennomsiktige poser eller ved å fjerne dem. I Bjørgos terminologi har man vanskeliggjort gjennomføring av kriminelle handlinger (kap. 3.2.). Byrommet er designet slik at man i større grad vil oppdage uidentifiserte objekter, og se hvem som har plassert dem der. Bakgrunnen for dette var IRAs bombeangrep, som hadde nettopp denne modusen. Dette gjør det mer trolig at terrorister i London vil forsøke andre moduser, hvor måloppnåelsen er lettere. Man kan jo måle at IRA har foretatt færre bombeangrep i London siden disse tiltakene ble innført. Men det er vanskelig å vise til at det er fordi tiltaket hadde effekt.

I eksempelet mitt med kokende væske derimot, vil man vite om tiltaket var effektivt. Fraværet av hendelser skyldes tiltaket. Sikringstiltaket *kan* ha virket avskrekkende for aktøren, men det vil man vanligvis ikke vite. Hvorfor man ikke ble angrepet kan være knyttet til faktorer helt utenfor egne handlinger. Om man har beskrevet prosedyrer for anmeldelser på hjemmesiden kan ha vært avskrekkende, men det kan også være at trusselaktør aldri har vært på hjemmesiden.

Mer konkret dreier dette seg om tallmateriale, noe som viser seg på ulike styringsområder. Jeg vil derfor si noe om statistikk.

4.2 Statistikk

Et kjernespørsmål i forskjeller mellom ulykkesforebygging og sikring er bruken av frekvens og sannsynlighet. Skal man gjøre en pålitelighetsanalyse (Ett rør pleier å tåle ti millioner liter vann før det ryker, ergo bytter vi det etter at 3 millioner vann har passert, etc.) er sannsynlighetsvurderinger avgjørende for å si noe om hva som er akseptabel risiko. Dette benyttes sjelden når man eksempelvis skal gjøre analyser av sikring mot terror. I stedet har trusselvurderinger og tiltak innen sikring ofte vært innrettet mot ting som aldri har skjedd, eller reaktivt ved usannsynlige ting som bare har skjedd bare en gang. En stor forskjell mellom Bjørgos mekanismer og Kjellens strategier er dermed at Bjørgo har mye mindre data på hvor effektive tiltakene er overfor faren/trusselen. Å forhindre at et menneske ikke skal foreta seg noe spesifikt et år fram i tid, er mye mer komplekst enn å forhindre varme på feil sted.

Et eksempel på en modus som ble forhindret uten statistiske data, kan være forbudet mot å ta mer enn 100 ml. væske på fly. Det var fordi konkrete planer om å ta med flytende eksplosiver på fly var avdekket (Nic Robertson og Lister 2012). Dermed ble tiltaket mot denne mulige, og statistisk usannsynlige angrepsmodusen innført. De mest konkrete drøftingene av bruken av sannsynlighet i risikovurderinger innen sikringsfeltet finnes i en masteroppgave (Egeli 2014), samt en forskningsrapport fra FFI (Busmundrud et al. 2015). Her fremkommer det imidlertid at varianter av sannsynlighet benyttes i utvalgsfasen av trusselaktører samt modus, så fra FFI oppfordres man til å tydeliggjøre hvilken form for sannsynlighet man benytter.

Utfordringene for en praktiker vil på dette området være knyttet til et dilemma som oppstår i vurderingen av sårbarheter, opp mot sannsynlige angrepsmodus. La meg spissformulere det slik: dersom det viser seg noen kan penetrere din fysiske grunnsikring på en ny og ukjent måte (for eksempel ved bruk av jetscooter) er dette en sårbarhet. På den annen side: det har aldri vært noen som har brukt en jetscooter for å penetrere fysisk grunnsikring noensinne. Så da er spørsmålet: Skal man bruke ressurser på å sikre seg mot jetscooter-baserte angrep - eller skal man la det være? NSM er tydelige: “NSM anbefaler heller å lage beskyttelsen mer generell og dermed robust i forhold til både kjente og mer ukjente trusler” (Jullum 2016). Mot dette vil eksempelvis Terje Aven hevde at man

da baserer seg på et antikvarisk syn på hva sannsynlighet er, nemlig som frekvens, og at man ikke bruker usikkerhet i vurderingen som belysende faktor (Aven 2011).

Skulle man kritisere oppfatningen om at statistikk ikke er viktig innenfor sikring, er det lett å peke på at når det gjelder kriminalitet er situasjonen en annen. Der har man god statistikk både på hva som virker forebyggende og hvordan forhindre konkrete angrepsmodus i å lykkes. Dette er sjelden er henvist til i risikostyringslitteratur om tilsiktede handlinger, men snarere noe vi må til det politifaglige som eksempel Tore Bjørgo (2015) for å finne. Men politiet har andre virkemidler enn det sikringsansvarlige i virksomheter har, og det må gjøres en del tilpasninger for at tiltak fra dette fagområdet er nyttig.

Tilknyttet mangelen på tallmateriale, er det innen sikring en svak tradisjon for å fremstille akseptert risikonivå. For hvordan kan man akseptere en risiko som er vag og mindre spesifikk? Roy Stranden sier det slik i tidligere nevnte FFI-rapport:

“I NS 5814/ISO 31000 så skal en bestemme risikoakseptkriteriene på et tidlig tidspunkt og de har ikke inkludert akseptkriteriene i selve analysen. For meg er dette bakvendt, det er det samme som å si hva du aksepterer før du egentlig vet hva problemstillingen er. Jeg har ennå ikke kommet over en beslutningstaker som er villig til å si det “ (Busmundrud et al. 2015, 135).

Et talende eksempel fra politikken (som i stort nok har vært mottakere av de fleste analyser som Stranden har utført), kan hentes fra Stortingsmelding 15 (OED 2012). Tittelen på stortingsmeldingen er : *Hvordan leve med farene.* Tiittelen gir forventninger om en gjengivelse av hvilken risikoaksept regjeringen mener vi kan leve med. Rapporten er generelt basert på på beste kunnskap, og henviser til forskning som inkluderer sannsynlighetsberegning for neste skred og flom. Men om du slår opp på kapittel 5.1 om *Risiko og risikoaksept* er kapittelet et gjennomgang av modellen bak risikoanalyser og risikomatriser. Det sies eksempelvis ikke noen sted at “Regjeringen forventer at over en 50 års periode, vil det i snitt dø 50 personer av flom eller skred, og de økonomiske konsekvensene er ventet å være mellom 2 til 10 milliarder i 2011 kroner.”. Stortingsmeldingen om “å leve med farene” sier faktisk ikke hvilke farer vi bør godta å leve med.

Det interessante med eksempelet er at regjeringens risikoaksept ikke spesifiseres. Mens risikoen for *produksjonstap* innen safety ofte er estimert og kommunisert, er det

vanskeligere å få beslutningstagere til å uttrykke aksept for tap av menneskeliv ved terrorhandlinger. Jeg kommer tilbake til dette i avslutningen av oppgaven min da jeg mener dette er et nyttig tiltak på samfunnssikkerhetsnivå.

Jeg har da gjennomgått en typisk forskjell mellom ulykkesforebygging og sikring, som er knyttet til bruken av tall og knyttet dette til generelle forskjeller samt utvalgte problemstillinger hos Kjellen og Bjørgo.

4.3 Helhetlig ulykkesforebygging, stykkevis og delt sikring

I kapittel 3 gjennomgikk jeg modeller for sikring, og refererte til offentlige veiledere og enkeltstudier som dekket sikring på samfunnsnivå mot terror, og sikring mot kriminalitet på virksomhetsnivå. Påstanden min er at at det innen sikringsfaget finnes styringssystem eksempelvis for informasjonssikkerhet (Landoll 2017), mye god forskning om terrorisme (Lia 2007; Hegghammer 2017), og evidensbasert gjennomgang av hvordan man kan forhindre kriminalitet (Bjørgo 2015). Men ikke noe av dette er helhetlig og gir et overordnet rammeverk for hvordan man som sikkerhetsleder i en virksomhet skal tenke og vurdere når man skal sikre seg mot *ulike* trusselaktører i en sikringskontekst. Motsatt er det et akademisk korpus og utdanninger som behandler ulykkesforebygging på helhetlig vis, og det synes også å være langt mer bruk av felles virksomhetsovergripende metoder. Jeg har altså satt meg fore å foreslå en modelle for å bøte på dette problemet, og vil nå gå over til konstruksjonen av denne.

5. Et utkast til styringsmodell for beskyttelse mot tilsiktede handlinger

Hittil i oppgaven har jeg gjennomgått mine tre avledede forskningsspørsmål. Jeg har besvart to av dem ved hente teoretiske perspektiver fra henholdsvis samfunnsikkerhet, kriminologi og ingeniørfaget. Det mer overordnede spørsmålet om forskjeller mellom ulykkesforebygging og sikring har jeg prøvd å besvare ved å henvise til et mer mangefasettert kildemateriale, samtidig som jeg har prøvd å komme med praktiske eksempler fra eget arbeidsliv, samt modellene i kapittel 3. Med dette som bakgrunn vil jeg da prøve å besvare hovedspørsmålet mitt: "Hvordan bør et styringssystem for sikringsfeltet innrettes?". Jeg vil primært støtte meg på de tre "hovedteoriene" fra kapittel 3. Jeg vil også komme med eksempler for å vise modellen i bruk, stort sett hentet fra oppgaven en fiktiv sikkerhetsleder i en IT-bedrift har.

5.1 Sikring mot tilsiktede handlinger

Modellen har 6 kronologiske elementer, hvor boksen "risikoreduksjon" på toppen viser hvor den faktiske risikoreduksjonen finner sted, mens boksen "Sikringstyring" viser til hvor styringinformasjon går inn, og beslutninger ut (se kap. 3-3.3.). De bokser som er satt sammen betegner at det ikke er separarate prosesser.

1. Verdi/operasjon
2. Trusselvurdering/tiltak/sårbarhet
3. Monitorering/revisjon
4. Håndtering/øvelser
5. Evaluering
6. Risikoreduksjon

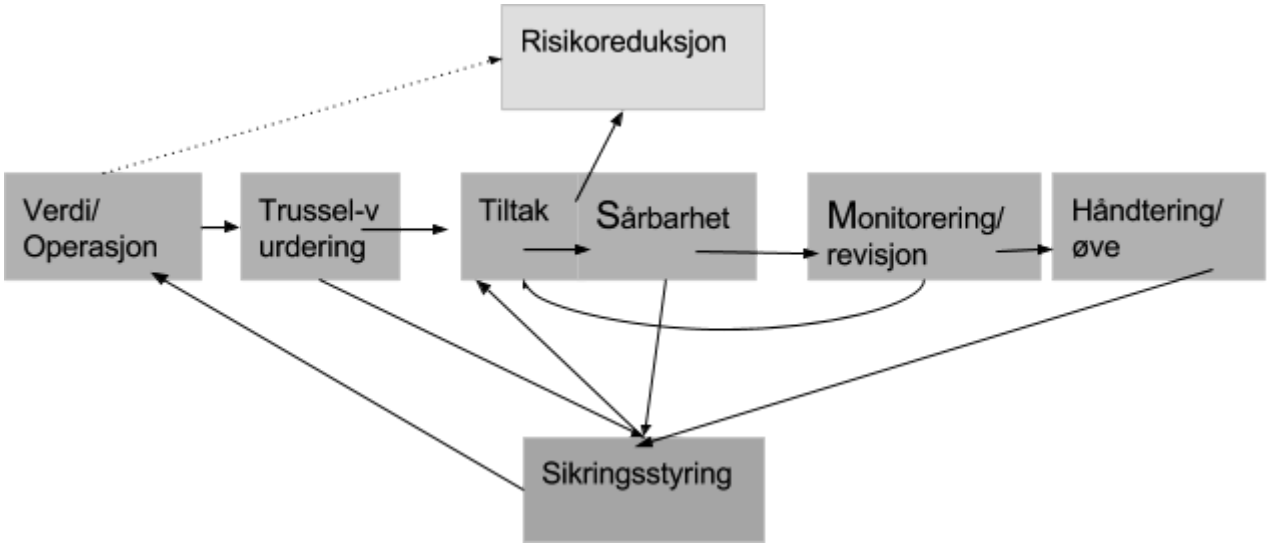


Fig. 1.

5.1. Verdi/operasjon

I sikringsarbeid er det essensielt å starte med å definere hva du faktisk ønsker å beskytte. Er det informasjon, er det produksjon eller leveranser, eller er det mennesker? Noen ganger er dette en statisk størrelse, for eksempel “kundens penger” eller “koden til spesifikk programvar”. I slike tilfeller er verdivurderingen enkel, og ikke verdt å bruke mye tid på i seg selv. Verdt å huske på i slike tilfeller er: kan man redusere verdien? Kan man for eksempel gjøre noe mindre verdt, ved å dele informasjonen opp, slik at selv om man foretar et vellykket innbrudd, vil man bare tilegne seg en femtedel av koden? Om det som skal gjennomføres eksempelvis er en operasjon av noe slag, for eksempel en reise til et sted med ugunstige sikringsforhold, blir verdivurderingen mer kompleks. Skal man kanskje beskytte en spesifikk leveranse, eller er det eget personell? Som eksempel kan vi bruke en reise til Somalia, lett omskrevet fra en arbeidsoppgave jeg hadde i en tidligere jobb.

Når man reiser til Somalia kan formålet med reisen være at man eksempelvis skal skal kontrollere midler brukt til en pikeskole. Det kan defineres som operasjonen som skal gjennomføres på en mest mulig risikofri måte. Man vil da se på stedlige trusler, deres modus operandi, hvilke sårbarheter som finnes og hvilke tiltak man kan iverksette for å redusere sannsynligheten for å bli rammet av noe. Typisk sannsynlighetsreduserende tiltak vil for eksempel være å forkorte oppholdet, holde reiseruten hemmelig og minimere transport. Men man vil også kunne søke å øke resiliensen til å motstå angrep, ved å ha

væpnet eskorte og tilgjengelig legehjelp. Det er også denne oppgaven med å planlegge denne reisen som de fleste som jobber med sikring da vil ta på seg. Men om man går litt nøyere til verks, og ser på hva som faktisk er hensikten med det som skal utføre - altså gjøre verdivurderingen litt grundigere, kan andre tiltak komme opp. For selv om oppdraget nok kan gjennomføres på en tilfredsstillende måte bør man samtidig se på: er det andre måter å få kontrollert at denne pikeskolen oppfyller kravene? Eller videre: dersom den ble bygget for å understøtte norsk politikk knyttet til likestilling - kan man kanskje oppnå den egentlige hensikten på annet vis? Som ikke innebærer eksponering for farene i det hele tatt, altså at reisen ikke blir gjennomført?

Poenget er at verdivurderingen må knyttes sammen med de strategiske mål og visjoner virksomheten har. Det er dette som angir bakgrunnen for at operasjonen faktisk foretas.

Kanskje man kan oppnå hensikten ved å møte de samme personene man planla å møte uten å reise til Somalia? Eller om man går enda lengre tilbake: Kanskje man kan fremme likestilling på annet vis? (I mitt arbeidsliv, viste det seg at de avtalte møtene kunne avholdes på en annen arena en måned senere, hvor personene som skulle møtes uansett hadde tenkt å delta).

Denne formen for verdivurdering hvor man også ser det opp mot “den vanlige” betydningen av ordet verdier, mener jeg vil kunne styrke sikringsarbeidet. Den er per i dag ikke en del av for eksempel offentlige veiledninger (NSM 2016). For den som styrer sikringen spesielt, fordrer det evnen til å tenke strategisk, og i tråd med virksomhetens egentlige mål. Det vil også gi et større ansvar når man tenker sikring: ikke bare at sikringsarbeidet må være forankret for å ha effekt, men også at sikringsarbeidet må forankres i den overordnede målstyringen i virksomheten.

Et annet problem med Norsk standards definisjon av verdivurdering, er eksempelvis at den tar utgangspunkt i at det finnes “umistelige” verdier. Det er kanskje tilfelle for de virksomheter som er underlagt sikkerhetsloven, og til dels også for industrier i høy-risiko virksomheter som olje og industri, men dette er ikke særlig relevant for eksempel for industrier som bank og finans, varehandel etc. Ofte er det teknologiske produksjonsutstyret hyllevare, og personalets kompetanse ikke vanskelige å erstatte. Det

vil da være bedre å ta utgangspunkt i leveransen, for eksempel “tilgjengelige data for å foreta skatteavregning”. Da vil verdien kunne skaleres med reell viktighet framfor komponent-viktighet.

Det kan være verdt å nevne at en av forskjellene mellom Schiefloe og Bjørgo fremkommer tydeligst når man ser på hvilke verdier som skal beskyttes. I Schiefloes modell er det nemlig slik at man skal sikre samfunnets leveranser. Samfunnssikkerheten oppstår når samfunnet er robust nok til at samfunnskritiske funksjoner leveres også under press. Hos Bjørgo har ikke verdivurdering noen eksplisitt plass, siden verdiene er definert av loven. Hva som utgjør kriminalitet vedtas av den lovgivende forsamling (Stortinget). Man trenger derfor ikke “på nytt” definere hva som skal beskyttes, siden det er den lovgivendes forsamlings oppgave. Dette er en utfordring for dem som skal adaptere strategier for å redusere kriminalitet og tap for egen virksomhet.

Fra Kjellens innledende betraktninger vil jeg knytte opp til at den som ønsker å bedre sikring i egen virksomhet, må ta hensyn til det han kaller grensebetingelser. Dette innebærer at virksomhetens størrelse, hvilken type teknologi og ressurser som benyttes og er tilgjengelig både i produksjonen, men også på tiltaksdelen, må inkorporeres når man skal sette rammene både for verdivurdering og analyse. Ved at målsettinger blir en del av verdivurderingen vil virksomhetsstyring og sikringsstyring være samkjørt.

Oppsummert har jeg altså argumentert for at verdivurderingen i større grad enn det som ekspliseres i Norsk standard og NSMs veiledninger skal

- ta hensyn til virksomhetens strategiske mål
- Se på grensebetingelsene for virksomhetens praksis
- vurdere å benytte leveransens viktighet som graderingsnivå

5.2 Trusselvurdering/tiltak/sårbarhet

Man beskytter seg mot ulike trusselaktører på ulike måter, utfra hvilken modus de benytter for å få tilgang til verdien. Når jeg skriver inn ordtrekløveret trusselvurdering/tiltak/sårbarhet, er det for å få fram at det vil være kontinuerlige sårbarheter som kan utnyttes, også etter at tiltak er iverksatt. Man må akseptere at det er noen trusler man er sårbare overfor. Ikke alle virksomheter skal være robuste nok til å

håndtere et væpnet angrep uten produksjonsstopp, derfor må vi innse at det vil være noen hendelser som faktisk vil medføre ekstreme skader.

Om man går grundigere inn på trusselvurderingen, bør man se dette utfra hvilke trusselaktører som finnes og som kan ha en intensjon og kapabilitet til å ramme eller få tak i verdier som virksomheten beskytter (Engen et al. 2016, 87). Vi kan illustrere dette med å tenke oss to generiske trusselaktører, og tenke oss at den virksomheten vi beskytter er en innovativ IT-bedrift.

I de fleste trusselvurderinger figurerer trusselaktører kategorien "terrorister" og "organiserte kriminelle". Først ser vi på terroristers utgangspunkt: målutvelgelsen har bakgrunn i politiske intensjoner, målet er ikke-stridende og handlingen kommuniserer noe til befolkningen og/eller de herskende i et land (Böwering, Crone, and Mirza 2013). De har ikke evne til å gjøre opprør eller å beholde geografiske områder: Aksjoner foretas for å oppnå politisk handling og/eller stemningsskifte i deres favør. Ulike terrorister har derfor ulike former for mål: Tar man USA som eksempel vil høyreekstremister og konspirasjonsteoretikere stort sett fokusere på ordensmakten og statlige mål, mens islamister søker å drepe flest mulig av folk flest. Dette betyr at en standard høyreekstremist vil ha færre mål enn en islamist. For terroristen vil oppdagede sårbarheter være viktig ved målutvelgelse.

«Terrorists shape themselves to our vulnerabilities, to the seams in our defenses; the threat they pose depends on us. The 9/11 hijackers, for instance, did not come to their plan of attack because they were aviation buffs. They came to it because they had identified gaps in our aviation defenses" (Treverton 2007).

Dette betyr at om du jobber med sikring i en IT-bedrift, vil virksomheten ikke være et mål for terrorister. Det finnes mange mål med de samme attributter som deg, og du er ikke den mest attraktive. Dette betyr ikke at du ikke kan rammes. Eksempelvis ved at arbeidsstedet ditt er like ved typiske mål som transportknutepunkt eller kjøpesentre eller symboltunge åpne plasser. Men det betyr at det du bør sikre deg mot er resultatet av angrep på målet i nærheten av deg, (det kan være splintglass på vinduer, trening på hurtig rømming til sikkert rom, at perimetersikringen har hurtiglukkende ståldører etc) og ikke at noen

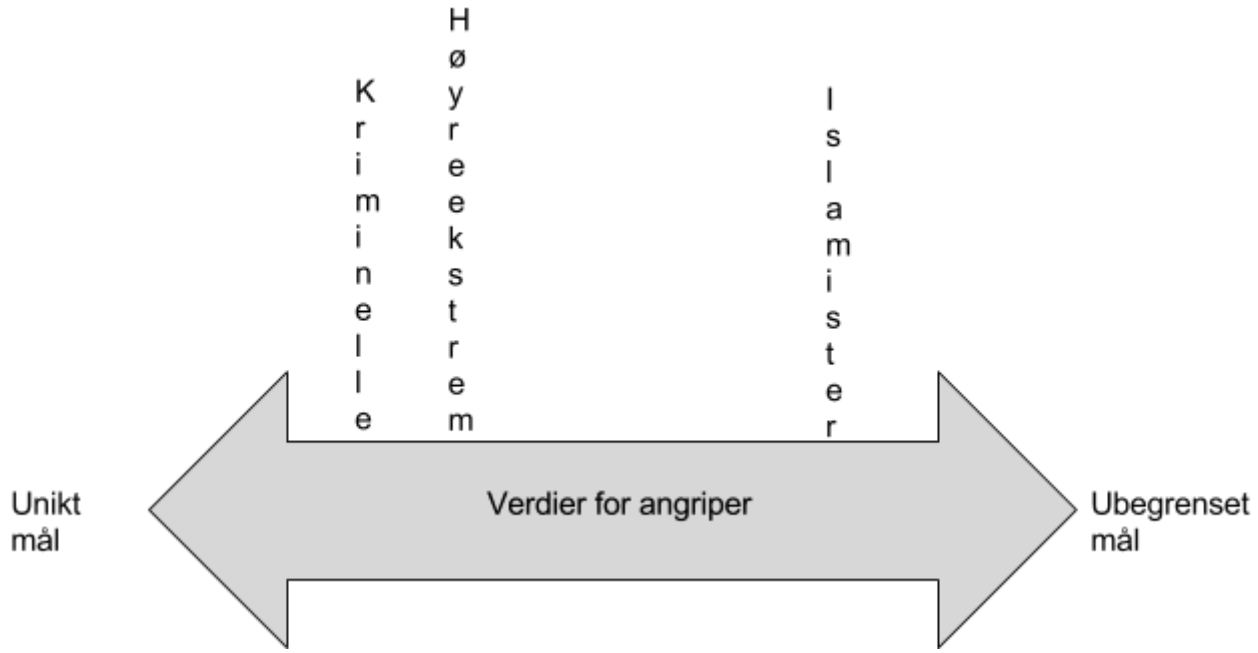
terrorister har deg som mål. I Usa er trusselbildet knyttet til “workplace-shootings” et helt annet, men det regnes der som mord, og ikke terror.

Fra min egen hverdag som sikringsmedarbeider i en bank, er den største trusselen en ny fremvekst av venstreekstremister som har finansvesen og kapitalisme som fiender. Da er plutselig arbeidsstedet mitt og ansatte i bank og finans kan blitt et mål, slik det var på 70 og 80-tallet. Det er derfor avgjørende at trusselvurderingen ser på trusselaktørens intensjon, for å se om det innebærer at det man skal sikre kan bli et mål.

Bjørgo (2015) fremhever at for kriminelle er kost/nytte vurderinger sentralt. For deg som sikringsmedarbeider ønsker du derfor å maksimere kost, og minimere nytte. Kriminelle vil alltid gå etter verdier som er lettest mulig å nå. Ved å vanskeliggjøre gjennomføring av kriminelle handlinger øker du kost.

Å utnytte sårbarheter og å velge mål er begge en del av trusselaktørens kost/nytte vurdering. For den som skal utføre sikringstiltak, er det også med i vurderingen å se på egen virksomhet opp mot andre virksomheter med lignende eller samme verdier. Dette vil innebære å bruke tid på grensebetingelsene (kap. 3.3). Ved å gå i dybden når man vurderer intensjon, vil man kunne avlede om man selv er et mål. Man må plassere seg selv på en skala over mulige mål. For IS-terrorister er de fleste forsamlinger av mennesker potensielle mål. De mest attraktive målene er de som gir mest kommunikativ effekt. På den andre siden av skalaen kan man tenke seg informasjon om spesifikke kontrakter og planer innen olje, som er mål bare kriminelle aksjespekulanter er ute etter. I de tilfeller hvor det finnes kjente og definerte trusselaktører med vilje til å angripe, vil tilhørigheten til en målgruppe hvor det er mye “tilbud” redusere sjansen for å rammes.

Jeg har illustrert dette poenget under, siden jeg finner det underkommunisert i for eksempel NS 5830:



(fig. 2)

Om man befinner seg på høyre side av denne skalaen, er det viktig å fremstå som bedre sikret enn *sammenlignbare virksomheter* med verdi av samme type. Desto lengre ut på venstre side operasjonen/verdien som skal beskyttes befinner seg, desto mindre viktig blir dette, og i større og større grad vil viljen til å gjennomføre hos trusselaktør være avgjørende.

Jeg har i dette kapittelet drøftet hvordan analysen av verdi og trusselaktører gir innspill til hvordan oppnå risikoreduksjon. Jeg skal nå gå videre til tiltakene, som er der den faktiske risikoreduksjonen skjer.

5.2.1 Tiltak og implementering

Jeg bruker i dette avsnittet begrepet tiltak som likelydende med barriere. Tiltak mot tilsiktede handlinger er i en ideell verden kapabilitetsforhindrende. Eksempelvis må man bare oppdatere programvaren for å være immun mot de fleste varianter av dataangrep. Dette vil vanskeliggjøre gjennomføring av kriminelle handlinger og beskytte sårbare mål, i Bjørgos terminologi (2015). Et slikt rent teknisk, 100% kapabilitetsforhindrende tiltak er sjelden tilgjengelig utenfor cyberdomenet, selv om “væske-på-fly” nærmer seg innenfor det fysiske domenet. Forskjellen ligger i den menneskelige faktoren. For at tiltaket mot væske på fly skal ha effekt må det være mennesker som er trent i å avdekke for høye

væskemengder, disse må ha ressurser til å utføre jobben sin, og de må ha mandat til å agere tilstrekkelig effektivt til å forhindre alle tilfeller når noe oppdages. Alt dette innebærer en helt annen ressursbruk enn den som bare er basert på at pcen må oppdateres med siste patch.

I Bjørgos variant er avskrekking, og trusler om straff (2015, 139) knyttet til typiske politifaglige tiltak som uro-aksjoner og rettighetstap. Men for vår sikkerhetsleder vil også denne typen tiltak være aktuelle. Å ha synlige kameraer, eller å kommunisere tydelig at man straffeforfølger all kriminalitet; at man sier på hjemmesiden at man aldri betaler løsepenger: Alt dette er tiltak som kan redusere sjansen for å bli utsatt for noe. Det øker kost (man kan bli sett), og reduserer nytte (man betaler ikke løsepenger for data av prinsipp).

Det er forskjeller på systemer hvor det er høy grad av menneskelige innsatsfaktorer vs. dem hvor det er tekniske komponenter som er avgjørende for sikkerheten. Som sikkerhetsleder i en IT-bedrift vil man ofte lettere kunne få midler til tekniske tiltak enn tidkrevende menneskelige tiltak. Dette selv om samlet ressursbruk (tid x penger) ofte vil være høyere når det tekniske tiltaket skal kjøpes inn, tilpasses og driftes. Pr. d.d. henger dette sammen med at mangelen på IT-ingeniører er prekær. Et tiltak som fører til at ansatte må bruke mer tid på å tilegne og vedlikeholde informasjonssikkerhetskompetanse fører til mindre utvikling og drift, og man kan ikke ansette flere for å kompensere for dette.

Som resultat av trusselvurderingen vil man han en oversikt over de viktigste trusselaktørenes modus for å angripe, noe som forteller en hvilke tiltak som vil være effektive for å avverge. I de tilfeller hvor man ikke kan avverge må man forberede en respons. I scenariobeskrivelsen er det viktig å fullt beskrive konsekvensene av trusselaktørens angrep på dine verdier, både med dagens og evt. planlagte sikringstiltak. Når man jobber med sikring vil dette utgjøre risikoanalysen.

Sikringstiltak inndeles vanligvis i hvordan man kan deter (avskrekke), detect (oppdage), delay (forsinke) and deny (respondere) på trusselaktøren. Avskrekking er alltid å foretrekke, siden det fører til at angrep ikke gjennomføres. Det du håper på, er at trusselaktøren gjør en ny kost/nytte vurdering som tilsier at dette angrepet ikke er verdt

det. Eksempler på avskrekkende tiltak kan være mindre dramatiske, som for eksempel god belysning koblet med synlige kameraer, alarmer med lyd, klistremerker som sier noe om respons o.l. Poenget er at for at avskrekking skal virke, må det kommuniseres. Sikkerhetsteater kan her ha en effekt. Men kommunikasjonen av tiltaket lager et dilemmma for sikringslederen: La oss si at en tidligere sårbarhet knyttet til verditransport kan lukkes ved å innføre tiltaket *væpnet vakt*. Risikovurderingen viser at dersom man har væpnet vakt, vil man respondere på angrep på måter som gjør at de ikke er vellykket, og man innfører dette tiltaket. En væpnet vakt vil i de fleste tilfeller gjøre at trusselaktøren velger andre mål. Men en gitt aktør med tilstrekkelig vilje, vil da endre sine planer til å inkludere inkapasitering av den væpnede vakten. Plutselig vil man da stå overfor angrep som vil ha helt andre konsekvenser (tap av liv) enn det opprinnelige scenarioet. Innføringen av tiltaket kan derfor øke konsekvensene av et angrep.

Generelt vil tiltak være basert på at sårbarheter fjernes eller elimineres, men man må også huske på at reduksjon av verdier er en mulighet. For sikkerhetslederen i IT-bedriften kan man eksempelvis lage rutiner som partisjonerer verdien “utnyttbar børsinformasjon” slik at den er lagret ulike steder. Eller mer IT-teknisk : krypteringen for å oppnå tilgang til dokumentet er basert på to-faktor autentisering eller asymmetrisk kryptering hvor privat nøkkel ikke kan gjenfinnes ved digitale angrepsvektorer. Om sårbarheten er at det finnes en “knapp” for å stoppe alle operasjoner, vil man robustifisere ved å gjøre systemet mindre strømlinjeformet.

Til sist kan det være verdt å minne om at også virksomheter er deltagere i et samfunn. Mange av de forebyggende tiltakene som Schiefloe og Bjørgo viser til, er det myndigheter som utfører, men mange virksomheter arbeider også opp mot myndigheter og/eller har satsinger knyttet til veldedig arbeid. Dersom man avdekker miljøer som har uønskede kapabiliteter, eller dersom man er enig i at dårlige sosiale forhold produserer kriminalitet, kan man ta initiativ overfor dette. Dette kan vanskelig tilordnes som del av virksomhetens sikringsstyring, men kan være verdt å vurdere dersom man skal gå etter rotårsaker. Spesielt Bjørgo med sitt brede fokus på virkemidler hvor alle har en rolle, kan her gi inspirasjon.

Jeg har nå gått gjennom hvordan man kan redusere sårbarheter, men det er ikke alle man kan bli kvitt, som i terror-eksempelet mitt. Noen sårbarheter må aksepteres.

5.2.2 Å akseptere sårbarheter

Traavik-utvalget sier om PST at en av utfordringene de har er å arbeide innenfor rettsstaten, og samtidig beskytte samfunnet (JD 2012). De støtter 22.juli kommisjonens utsagn om at man ikke kan forvente at PST skal forhindre alt: «Denne stilltiende aksepten av risiko er ofte underkommunisert fra myndighetenes side» (NOU 2012:14, 365). Det samme er tilfelle når man jobber med tilsiktede handlinger. Om man er sikkerhetsleder i en IT-bedrift skal man ikke sikre seg for at den typen militære stridskrefter som terrorister benytter kan angripe uten at leveransene blir påvirket. Men man bør kanskje ha en kontinuitetsplan som sier noe om hvordan konsekvensene kan reduseres.

Ofte når man gjør risikovurderinger vil scenarioer som inkluderer terrorister ha så alvorlige konsekvenser at nær uavhengig av sannsynligheten for at noe skjer, så vil slike scenarioer være “røde”. Det trenger ikke bety at noe skal gjøres. Også på virksomhetsnivå må man akseptere at terror kan skje. Visselig bør man (dersom verdi og trusselvurderingen tilsier det) ha beredskapsplaner som kan iverksettes, men at skader/tap av liv/helse kan oppstå når man utsettes for noe ekstremt er å forvente. Schiefloe henviser til dette som robusthet på samfunnsnivå (se 3.1). Som sikkerhetsleder må scenarioer av denne typen skrives ut i risikoanalysen og konsekvensene være kjent. Det engasjementet og forpliktelsen som virksomhetens toppledelse har (se 3.3.6) må også knyttes til til å godta konsekvenser av at scenarioer med liv/helse konsekvenser skjer. Dette er styringsinformasjon, men det er også kunnskap som som når den er spredd senker terrorristers måloppnåelse/gevinst ved å utføre angrep, da det spres mindre frykt.

5.3. Monitorering/revisjon

Schiefloe (2011) trekker fram at man må ha overvåkning av trusselaktører for å se om det planlegges noe. Avhengig av grensebetingelser som størrelse m.m. er det et minstekrav at man må bokstavelig talt lese trusselbildet slik det finnes for eksempel i offentlige trusselvurderinger som dem fra NSM (NSM 2017) eller Kripos (2015) eller fra hyppigere oppdaterte kommersielle aktører. Det aller viktigste når man leser disse er å vurdere: Er det samsvar mellom intensjonen hos trusselaktørene og de verdiene du skal beskytte? Og

om dette er tilfelle: Benytter de seg av modus som man ikke er beskyttet mot? I mange tilfeller vil det vise seg at trusselaktørenes modus er lite varierende. Men kanskje det er slik at en spesiell form for svindel, eller ransomware nå har økt i hyppighet. Da kan det bety at sikringsressurser som man tidligere har benyttet på annet hold, må innrettes tydeligere mot disse.

Det kan også tenkes at nye moduser oppstår som man ikke er beskyttet mot. Det tidligere eksempelet mitt med vannscooter kan benyttes: Dersom det er noen som har intensjoner som sammenfaller med dine verdier som benytter en vannscooter: Hvordan er dette gjort? Hvordan er det eventuelt tenkt gjort? I møte med dine sikringstiltak: hvordan vil angrepet utspille seg? Hva vil konsekvensene være for den verdien angrepet søker? Vil andre verdier bli berørt? Mitt neste trinn i prosessen handler om evaluering av hendelser, men i monitoreringsfunksjonen må man evaluere andres hendelser. Et nettverk hvor man deler informasjon om angrepsmoduser og effektive mottiltak (som finansCERT) gir uvurderlig informasjon om hva man må være forberedt på.

En annen form for styringsinformasjon kan man få ved å overvåke prosessikkerhet: Håndteres digitale informasjonsmedium utenfor bedriftens områder slik prosedyrene tilsier? Logger man seg på med VPN, kan man spore om informasjon merket konfidensielt er sendt til eksterne e-poster o.l. Digitalt finnes det ofte verktøy for å spore om organisatoriske prosedyrer følges.

I kapittel 3.3.5 gjennomgikk jeg sikkerhetsindikatorer. De fleste av disse vil være relevante når man jobber med risikoreduksjon, men punktet om at resultater må ha integritet, bør utdypes noe. Typisk vil detaljerte prosedyrer når man står overfor en trusselaktør ikke være tilstrekkelige, da man kan forvente at de mest vanlige sikringsmetodene vil være kjente for trusselaktør. Det er derfor viktig at man oppnår en kultur hvor det å se etter, og å prøve å oppdage sikkerhetsbrister blir belønnet. Dette dekket jeg i 3.3.1: Det er svært viktig å skape insentiver som gir styringsinformasjon, og ikke insentiver som belønner at rutiner fravikes. På byggeplasser er ofte daglige Sikker jobbanalyser rutine. Når dette er i ryggmargen blir resultatene mye bedre enn om det “kobles på” i etterkant. Det engelske slagordet built-in security vs. bolt-on security kan illustrere: Når man forestiller seg at noen ønsker verdiene, er det lettere å designe noe sikkert, enn å sikre i etterkant.

Det å skape en god sikringskultur vil være knyttet til at man belønnes for å robustifisere leveransen. Å sørge for at hele verdikjeder er sikret mot sabotasje kan synes dyrere på kort sikt, men kan gi langsiktige fordeler som må premieres.

5.4 Håndtering og øvelser

Som IT-sikkerhetsleder får man testet sikkerheten hver dag. Det er ikke fordi en trusselaktør vil ha informasjonen din, men fordi det eksisterer mange angrepsvåpen som sirkulerer skjult i e-poster, på websider og ulike sikkerhetshull i ulik software. Heldigvis blir denne formen for angrep rutinemessig unngått ved hjelp av oppdatert software, men allikevel vil det være noen som slipper igjennom og kan gjøre skade.

Det som er spesielt omgripende, uvanlig eller på andre måter krever en respons som ikke dekkes av driftsapparatet krever spesielle prosedyrer. Hvor man trenger å ha en forhåndsplanlagt respons, vil vises gjennom scenariobeskrivelsen i risikoanalysen slik det er beskrevet i 5.2.1. En responsplan vil sette godhetskrav til hva som er akseptabel håndtering av hendelser, og hvilken dimensjonering (utstyr, personell, kompetanse) som er nødvendig for å oppnå disse. Det kan være opplærings-, trenings- og øvelsesaktiviteter, nytt utstyr eller software, andre lokaliteter, ekstra personell eller oppgradert eget personell, endringer i organisering for å oppnå tilstrekkelig hurtige beslutninger og lignende. Om det viser seg at man eksempelvis trenger forhandlingskompetanse for å håndtere et ransomware-angrep, må man enten trene eget personell i dette, eller gjøre avtaler som sikrer at denne kompetansen er tilgjengelige i løpet av en viss tid.

Det man gjør hver dag blir man dyktig til. Det man gjør sjelden trenger man å øve på. Når man skal øve, er det viktig at man øver på ferdigheter som man forventer å benytte seg av en sjelden gang, men som man må være i stand til å utføre. Eksempler på dette kan være:

- Å prioritere bort driftsoppgaver
- Å forholde seg til eksterne interessenter som media, toppledelse, eiere, myndigheter
- Å samarbeide med avdelinger og personer som man vanligvis ikke samarbeider med

Både for daglig drift og sjeldne hendelser ønsker man å generere styringsinformasjon, men avviksrapportering er noe mindre omfattende enn evaluering av en større hendelse eller øvelse.

Øvelser kan gjøres mer eller mindre komplisert. Man må ikke glemme hvorfor man øver, som er å forbedre egen organisasjons evne til å håndtere en hendelse. Forbedringen kan bestå i enkle, avledede ferdigheter fra de tre eksemplene mine: Om for eksempel noen som ikke pleier det har fått medietrening, vil samlet konsekvens av et angrep ha gått ned. Det betyr at det er foretatt en forbedring.

Om en mer effektiv form for drift av staben, eller "problemløserne" kan etableres, er det selvsagt en fordel å gjøre dette. Om det skulle vise seg å ha effekt på håndteringen av en krise, kan det tilogmed hende at noe kan benyttes til til daglig drift.

En variant av øvelser er red teaming (Zenko 2015). Erfaringsmessig kan dette gjøres veldig bra - og veldig dårlig! Om ikke formålet er å lære og forbedre organisasjonen kan man lett ende opp i helt urealistiske angrepsmoduser, så dette må gjøres skikkelig om det skal fungere. Trusselaktørenes modus må være utgangspunkt for øvelsen.

Evaleuringer må ha gjenkjennbare metoder som gjør det mulig å avlese "hvor noe gikk galt på systemnivå. Om en barriere sviktet - er det kanskje andre som kunne vært tilstede, og fanget opp angrepet, eller redusert konsekvensene?

5.5 Sikkerhetsstyring

Som man kan se er modellen for styring innrettet etter Kjellens modell. Informasjonen som tilflyter sikringsleder må være *reliabel*, *nøyaktig* og være *relevant* (2002, 136). Reliabilitet oppnås i en sikringskontekst ved at verdi, trusselvurderinger og revisjoner foretas etter samme mal. Nøyaktighet betyr i en sikringskontekst at informasjonen må ha integritet. Den viktigste forskjellen mellom ulykkesforebygging og sikring ligger her i hvordan oppnå relevant informasjonstilfang. Trusselen endrer karakter etter hvilke tiltak du har iverksatt. Idet en modus er lukket er det de andre du må beskytte deg mot. Balansert sikring oppnås

først når samspillet mellom menneskelige, teknologisk og organisatoriske faktorer fungerer. Om ikke hele dette bildet rapporteres vil ikke informasjonen være relevant.

Derfor blir analyse og monitoreringsfunksjonen essensiell når man beskytter seg mot farer. Trusselaktører lærer av hverandre, og når NSAs metoder for å få tilgang til din informasjon er offentlig tilgjengelig, krever det umiddelbar sikring mot den modusen NSA tidligere kunne benytte. Man må derfor investere mer tid i overvåkning. Når det er sagt: her finnes det mange profesjonelle aktører som leverer 90% av det du trenger. Men til de siste 10% trenger du en aktiv vurdering av om trusselaktørene kan ventes å være interessert i nye verdier (dine), eller har tilegnet seg nye kapabiliteter.

Styringsmodellen er induktivt utledet av mange ulike eksempler og kilder, og skal ideellt sett være tilpasset alle verdier og trusler. Forskningsmessig skulle det være mulig å teste deler av den, men det får være en annen oppgave.

5.6 Risikoreduksjon

I denne modellen er risikoreduksjon tegnet inn for å forklare hvor risiko faktisk reduseres, og betegner ikke noe eget trinn i prosessen. Jeg har stiplet linjen fra verdi, for å få fram at man må ikke glemme å redusere samlet risiko ved å redusere verdi der det er mulig, slik jeg har tatt for meg i kapittel 5.1

6. Konklusjon

Mitt innledende spørsmål var *Hvordan bør et styringssystem for sikring være?* Jeg forklarte så at grunnen til at jeg hadde valgt dette spørsmålet var at jeg opplevde at sikringsfaget var lite påkoblet forskning, både innenfor ulykkesforebygging og forskning på kriminelle og terrorister. For å besvare dette satte jeg opp tre forskningsspørsmål som måtte besvares. Jeg beskrev så hvordan jeg kom frem til bakgrunnslitteratur som kunne hjelpe meg å besvare forskningsspørsmålene i kapittel 2 om metode, og hva denne inneholdt i kapittel 3. Jeg hadde ikke besvart forskningsspørsmålet om forskjellen på å sikre seg mot ulykker og å sikre seg mot tilsiktede handlinger på tilstrekkelig vis i dette tredje kapittelet, og jeg viet derfor kapittel fire til å gå gjennom svaret på spørsmålet.

Kapittel fem var et forsøk på å besvare hovedspørsmålet mitt, om hvordan et styringssystem for beskyttelse mot tilsiktede handlinger burde være innrettet. Jeg fokuserte på at det måtte være basert på informasjonsflyt og påfølgende. For hvert av elementene i prosessen skrev jeg noe om hva gjennomgangen i kapittel 3 kunne gi av råd, og prøvde å krydre dette med erfaringsbaserte eksempler som viste modellen i funksjon.

Dersom jeg skulle implementert en god styringsmodell for kontroll og prioritering av aktiviteter innen trusselhåndtering, ville jeg gjort det slik jeg har beskrevet i kapittel 5.

6.1 Kritikk, og utkast til videre forskning

Jeg sa at jeg var interessert i at det måtte være et system bak det sikringsfaglige, slik at sikringen kan styres. Men det kan rettes en kritikk mot selve utgangspunktet, eksempelvis kan det være at jeg har falt for en illusjon om at det som kan styres er kontrollerbart. Jeg kan dermed sies å ha en kontrollingeniørs innstilling til fagfeltet.

“It works well for stable and mature technologies, where one right, safe way of working can be defined, based on long experience. However, in other situations where risks are incompletely known and technology and work methods are rapidly or constantly changing, there is no “ideal state” which can be usefully defined” (A. Hale 2003, 5)

Tilknyttet dette kan det argumenteres for at at jeg har begått en kategorifeil i utgangspunktet: nemlig å se for seg at materie og mennesker er like forutsigbare. Argumentet vil være noe sånn som: Når man skal beskytte seg mot ulykker behandler man bare energi. Energi og annen materie følger naturlover. Ved å behandle alle faktorer kan man dermed beregne hvor risikoen er størst, og dermed redusere frekvens og konsekvens av hendelser. Ontologisk sett er alt bare varianter av at årsak A (varme), fører til årsak B (koking).

Men mennesker er ikke forutsigbare. Det har aldri vært en psykolog som ved å studere alt et menneske har gjort fram til nå i livet, som på noe fornuftig vis kan forutsi hva denne personen gjør på samme dag om et år fra nå (som er den type spådommer som ligger til grunn for risikoanalyser). Det eksisterer heller ingen som forsker på grupper av mennesker, enten det er sosiologer eller andre som kan forutsi hvordan en gruppe vil agere om et år fra nå. For mennesker er det ikke slik at årsak A (dysleksi) alltid fører til utkomme B (fattigdom). Ingen historiske eller samfunnsmessige lover med denne form for naturvitenskapelig nødvendighet er noensinne avdekket.

Argumentet for at dette er noe man bør tilstrebe, ligger først og fremst i oppgaven selv.. Jeg har tilstrebet metodologisk koherens og empirisk anvendbarhet. Men jeg har ikke kunne testet at modellen er empirisk valid. I en ideell verden hadde mitt forslag blitt implementert i flere lignende virksomheter, og så hadde en kontrollgruppe benyttet sine vanlige systemer. Man kunne da uten altfor store vanskeligheter målt hvem som hadde færrest tap. Dette eksperimentet er det nok ikke mulig å gjennomføre. Istedet er modellen basert på min beste kunnskap fra akademia og erfaring fra arbeidslivet.

En annen ting jeg nok burde sagt mer om, er hvordan man kan robustifisere innenfor alle elementer av sikringsfaget. Modellen min og eksemplene mine er mer likt det som kalles safety 1, enn det som kalles safety 2 (Eurocontrol 2013).

Men en masteroppgave kan bare gi svar på de spørsmål man stiller selv - og mitt svar er altså :

- Et styringssystem for sikkerhet bør fokusere på at verdier må knyttes opp mot bedriftens målsetninger.

- Det bør modelleres utfra et informasjonsflytsystem, da dette er en forutsetning for å kunne styre noe som helst.
- Truslene må vurderes utfra om verdiene er lettere tilgjengelig hos deg enn hos andre virksomheter.
- Sikringstiltakene generelt må være innrettet mot å avskrekke. Jeg forsvarte med den bakgrunn sikkerhetsteater som effektfullt.
- Monitoreringsfunksjonen knyttet til tilsiktede handlinger må være innrettet mot å avdekke nye moduser, spesielt om man skal sikre seg mot kriminelle. Om nye moduser finnes, må deretter vurdere om aktuelle trusselaktører har vilje til å benytte seg av dem.
- Egne øvelser må baseres på realistiske moduser, og hendelser må evalueres etter samme mal

Litteraturliste

Aven, Terje. 1998. *Pålitelighets-Og Risikoanalyse*. Universitetsforlaget.

———. 2011. *Misconceptions of Risk*. John Wiley & Sons.

Aven, Terje, Enrico Zio, Piero Baraldi, and Roger Flage. 2013. *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods*. John Wiley & Sons.

Aveyard, Helen. 2014. *Doing a Literature Review in Health and Social Care: A Practical Guide*. McGraw-Hill Education (UK).

Baron-Cohen, Simon. 2011. *Science of Evil : On Empathy and the Origins of Cruelty*. New York: Basic Books.

Bjørgo, Tore. 2015. *Forebygging Av Kriminalitet*. Universitetsforlaget.

Blass, Thomas. 1999. "The Milgram Paradigm After 35 Years: Some Things We Now Know About Obedience to Authority 1." *Journal of Applied Social Psychology* 29 (5). Oxford, UK: Blackwell Publishing Ltd: 955–78.

Boehmer, W. 2008. "Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001." In *2008 Second International Conference on Emerging Security Information, Systems and Technologies*, 224–31. ieeexplore.ieee.org.

Böwering, Gerhard, Patricia Crone, and Mahan Mirza. 2013. *The Princeton Encyclopedia of Islamic Political Thought*. Princeton University Press.

Busmundrud, Odd, Maren Maal, Jo Hagness Kiran, and Monica Endregard. 2015. "Tilnærminger Til Risikovurderinger for Tilsiktede Uønskede Handlinger." 2015/00923. Forsvarets forskningsinstitutt.

Duus, Aksel Hødnebø. 2016. "Sikring Av Virksomheter Mot Tilsiktede Uønskede Handlinger." UiT Norges arktiske universitet. http://munin.uit.no/handle/10037/9677.

Egeli, Anne. 2014. "Analysemetodikk I Forbindelse Med Terrorisme-Bruk Eller Ikke Bruk Av Sannsynlighet." University of Stavanger, Norway. https://brage.bibsys.no/xmlui/handle/11250/221328.

Energidepartementet, Olje- og. 2012. "Meld. St. 15 (2011–2012) Hvordan Leve Med Farene – Om Flom Og Skred." *Regjeringen.no*. https://www.regjeringen.no/contentassets/65e3e88d0be24461b40364dd61111f21/no/pdfs/stm201120120015000dddpdfs.pdf.

Engelstad, Fredrik, Carl Erik Grennes, Ragnvald Kalleberg, and Raino Malnes. 2005. "Introduksjon Til Samfunnsfag." *Gyldendal Norsk Forlag A/S*.

Engen, Ole Andreas, Bjørn Ivar Kruke, Preben Lindøe, Kjell Harald Olsen, Odd Einar Olsen, and Kenneth Arne Pettersen. 2016. *Perspektiver På Samfunnssikkerhet*. Oslo: Cappelen Damm akademisk.

Eurocontrol. 2013. "From Safety-I to Safety-II: A White Paper - SKYbrary." September. http://www.skybrary.aero/bookshelf/books/2437.pdf.

Ganatra, B., and B. R. Johnson. 2016. "Evidence-Based Practices Can Improve Safety and Timeliness of Care for Women Needing Safe Termination of Pregnancy." *BJOG: An International Journal of Obstetrics and Gynaecology* 123 (10). Wiley Online Library: 1692–1692.

Haddon, W., Jr. 1980. "Advances in the Epidemiology of Injuries as a Basis for Public Policy." *Public Health Reports* 95 (5): 411–21.

Hale, A. 2003. "Management of Industrial Safety." *Delft University of Technology, Draft*.

Hale, Andrew R., and J. Hovden. 1998. "Management and Culture: The Third Age of Safety. A Review of Approaches to Organizational Aspects of Safety, Health and Environment." *Occupational Injury: Risk, Prevention and Intervention*. Taylor & Francis, London, 129–65.

Hegghammer, Thomas. 2017. *Jihadi Culture: The Art and Social Practices of Militant Islamists*. Cambridge University Press.

Heinrich, Herbert William, and Others. 1941. "Industrial Accident Prevention. A Scientific Approach." *Industrial Accident Prevention. A Scientific Approach.*, no. Second Edition. New

York & London: McGraw-Hill Book Company, Inc. https://www.cabdirect.org/cabdirect/abstract/19432701767.
Hollnagel, Erik. 2011. “RAG-The Resilience Analysis Grid.” *Resilience Engineering in Practice: A Guidebook. Ashgate Publishing Limited, Farnham, Surrey*. erikhollnagel.com, 275–96.
JD. 2012. *Ekstern Gjennomgang Av Politiets Sikkerhetstjeneste - Rapport Fra Traavikutvalget*. Beredskapsdepartementet, Justis- og.
Johannessen, Asbjørn, Per Arne Tufte, and Line Christoffersen. 2010. “Introduksjon Til Samfunnsvitenskapelig Metode.” Abstrakt Oslo.
Jullum, Rolf. 2016. “God Grunnsikring Gjør Terrorhandlinger Vanskeligere.” *Nsm.no*. https://nsm.stat.no/blogg/god-grunnsikring-gjor-terrorhandlinger-vanskeligere/.
Kjellen, Urban. 2002. *Prevention of Accidents Through Experience Feedback*. CRC Press.
Kjellén, Urban, and Jan Hovden. 1993. “Reducing Risks by Deviation Control—a Retrospection into a Research Strategy.” *Safety Science* 16 (3): 417–38.
Kongsvik, Trond. 2013. *Sikkerhet I Organisasjoner*. Akademika forlag.
Kongsvik, Trond, Torgeir Haavik, and Gudveig Gjøsund. 2014. “Participatory Safety Barrier Analysis: A Case from the Offshore Maritime Industry.” *Journal of Risk Research* 17 (2). Routledge: 161–75.
Kripos. 2015. “TRENDRAPPORT 2016 ORGANISERT OG ANNEN ALVORLIG KRIMINALITET I NORGE.” *Politi.no*. October 11. https://www.politi.no/globalassets/dokumenter/01-rapporter-statistikk-og-analyse/organisert-kriminalitet/trendrapport-2016.pdf.
Landoll, Douglas J. 2017. *Information Security Policies, Procedures, and Standards: A Practitioner’s Reference*. CRC Press.
Lerø, Magne. 2016. “Ledelse Og Etterpåklokskap.” *Dagens Perspektiv*. May 24. http://www.dagensperspektiv.no/2016/ledelse-og-etterpaklokskap.
Lia, Brynjar. 2007. *Globalisation and the Future of Terrorism: Patterns and Predictions*. Routledge.
Lundberg, Jonas, Carl Rollenhagen, and Erik Hollnagel. 2009. “What-You-Look-For-Is-What-You-Find – The Consequences of Underlying Accident Models in Eight Accident Investigation Manuals.” *Safety Science* 47 (10): 1297–1311.
Nic Robertson, Paul Cruickshank, and Tim Lister. 2012. “Document Shows Origins of 2006 Plot for Liquid Bombs on Planes - CNN.com.” *CNN*. April 30. http://edition.cnn.com/2012/04/30/world/al-qaeda-documents/.
Nordli, Tobias, and Geir Bjørnstad. 2016. “Politiets Beste Råd for å Unngå Innbrudd.” *Www.smaalenene.no*. November 1. https://www.smaalenene.no/politiet/tyveri-og-innbrudd/sarpsborg/politiets-beste-rad-for-a-unnga-innbrudd/s/5-38-258448.
NOU 2012:14. n.d. “Rapport Fra 22. Juli-Kommisjonen - Regjeringen.no.” https://www.regjeringen.no/contentassets/bb3dc76229c64735b4f6eb4dbfcdbfe8/no/pdfs/nou201220120014000dddpdfs.pdf.
NSM. 2016. “Risikovurdering for Sikring - Nasjonal Sikkerhetsmyndighet.” https://www.nsm.stat.no/globalassets/dokumenter/handboker/risikovurdering_nsm_handbok_mars2016.pdf.
———. 2017. “Risiko Og Sårbarheter I En Ny Tid.” March 29. https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf.
POD. 2012. “Hvor Kommer 1% Begrepet Fra.” *Norsk Politi*, no. 2: 9.
Pyrooz, David C., and Scott H. Decker. 2011/9. “Motives and Methods for Leaving the Gang: Understanding the Process of Gang Desistance.” *Journal of Criminal Justice* 39 (5): 417–25.
Rasmussen, Jens. 1997. “Risk Management in a Dynamic Society: A Modelling Problem.” *Safety Science* 27 (2): 183–213.
Reason, James. 1997. *Managing the Risks of Organizational Accidents*. Routledge.
Remen, Anne Cecilie, and Line Tomter. 2016. “Tastefeilen Som Stoppet Statoil.” *NRK*. October 28. https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013.

Riecken, Henry W. 1974. “Obedience to Authority. An Experimental View. Stanley Milgram. Harper and Row, New York, 1974. Xx, 224 Pp., Illus. $10.” *Science* 184 (4137). American Association for the Advancement of Science: 667–69.
Schiefloe, Per Morten. 2011. “En Modell for Samfunnssikkerhet.” *NOTAT: 10/12* 10/12 (November). https://www.regjeringen.no/html/smk/22julikommisjonen/22JULIKOMMISJONEN_NO/CONTENT/DOWNLOAD/308/2358/VERSION/6/FILE/NOTAT_10_12_SCHIEFLOE.PDF.
Schiefloe, P. M. 2014. “Analyzing and and Developing Organizations: The Pentagon Approach.” *Trondheim: NTNU Social Research*.
Schneier, Bruce. 2007. “In Praise of Security Theater.” *Schneier on Security* 25.
Sintef. 2004. “Granskingsmetodikk: Menneske – Teknologi – Organisasjon.” STF38 A04422 . 384648. http://www.ptil.no/getfile.php/13698/z%20Konvertert/Helse%2C%20milj%C3%B8%20og%20sikkerhet/Sikkerhet%20og%20arbeidsmilj%C3%B8/Dokumenter/ulykkesgranskingstf38a04422.pdf.
Sundberg, Johann D., and Anders Park Framstad. 2017. “DNB: Menneskelig Feil Skapte Banktrøbbel.” *E24*. June 19. http://e24.no/boers-og-finans/nettbank/dnb-menneskelig-feil-skapte-banktroebbel/24076680.
Svendsen, Lars Fredrik. 2011. “Store Norske Leksikon.” *Naiv Realisme – Filosofi – Store Norske Leksikon*. Store norske leksikon. https://snl.no/naiv_realisme_-_filosofi.
The investigation team. 2013. “The In Amenas Attack. Report of the Investigation of the Terrorist Attack on In Amenas. Prepared for Statoil ASA’s Board of Directors.” Statoil.
Thon, Roar. 2013. “Sikkerhetstilstanden Er Ikke Tilfredsstillende | Sikkerhetsbloggen.” February 19. http://blogg.nsm.stat.no/index.html%3Fp=3092.html.
Thorsvik, Jan, and Dag Ingvar Jacobsen. 2013. *Hvordan Organisasjoner Fungerer*. Vol. 4. fagbokforlaget.
Treverton, Gregory F. 2007. “Risks and Riddles.” *Smithsonian*. http://www.smithsonianmag.com/people-places/risks-and-riddles-154744750/?no-ist.
UIO. 2014. “Hva Lærer Du?” *Kriminologi (bachelor)*. May 21. http://www.uio.no/studier/program/kriminologi/hva-lerer-du/.
Ullring, Svein, J. Lea, T. Hofshagen, G. Høiland, B. Tørmo, G. Bjørhovde, A. Reinsnes, W. Jensen, K. P. Hagen, and E. Ellingsen. 2006. “Når Sikkerheten Er Viktigst.”
Weick, Karl E. 1995. *Sensemaking in Organizations*. Vol. 3. Sage.
Wikström, Per-Olof H. 2014. “Why Crime Happens: A Situational Action Theory.” In *Analytical Sociology*, 71–94. John Wiley & Sons, Ltd.
Willoch, Kåre, and Norge Justis- og Politidepartementet. 2000. *Et Sårbart Samfunn : Utfordringer for Sikkerhets- Og Beredskapsarbeidet I Samfunnet : Innstilling Fra Utvalg Oppnevnt Ved Kongelig Resolusjo N 3. September 1999 : Avgitt Til Justis- Og Politidepartementet 4. Juli 2000*. Vol. 2000: 24. Norges Offentlige Utredninger (tidsskrift : Online). Oslo: Statens forvaltningstjeneste, Informasjonsforvaltning.
Wreathall, John. 2006. “Properties of Resilient Organizations: An Initial View.” *Resilience Engineering: Concepts and Precepts*. Ashgate, Aldershot, UK, 275–85.
Wright, Steve. 2006. “Measuring the Effectiveness of Security Using ISO 27001.” *White Paper Published in*. wwww.iwar.org.uk. http://wwww.iwar.org.uk/comsec/resources/iso-27001/measuring-effectiveness.pdf.
Young, William, and Nancy G. Leveson. 2014. “An Integrated Approach to Safety and Security Based on Systems Theory.” *Communications of the ACM* 57 (2). ACM: 31–35.
Yu, Hongyang, Faisal Khan, and Brian Veitch. 2017. “A Flexible Hierarchical Bayesian Modeling Technique for Risk Analysis of Major Accidents.” *Risk Analysis: An Official Publication of the Society for Risk Analysis*, February. Wiley Online Library. doi:10.1111/risa.12736.
Zenko, Micah. 2015. *Red Team: How to Succeed by Thinking like the Enemy*. Basic Books.