FFI-rapport 2015/00923

Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

Odd Busmundrud, Maren Maal, Jo Hagness Kiran
og Monica Endregard

FFI Forsvarets forskningsinstitutt

Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger

Odd Busmundrud, Maren Maal, Jo Hagness Kiran og Monica Endregard

Forsvarets forskningsinstitutt (FFI)

8. juni 2015

FFI-rapport 2015/00923

398101

P: ISBN 978-82-464-2540-5
E: ISBN 978-82-464-2541-2

Emneord

Risikoanalyse

Risikovurdering

Verdivurdering

Trusselvurdering

Sårbarhetsvurdering

Trefaktormodell

Sannsynlighet

Godkjent av

Monica Endregard	Prosjektleder
Janet Martha Blatny	Avdelingssjef

Sammendrag

FFI har på oppdrag for Forsvarsbygg (FB) vurdert forskjellige tilnærminger til risikovurderinger for sikring mot tilsiktede uønskede handlinger (security), med spesiell vekt på FBs to tilnærminger. Den ene tilnærmingen er basert på Norsk Standard 5814:2008 der risiko defineres som et "uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse". Den andre er basert på den nye standarden NS 5832: 2014 der sikringsrisiko er definert som et "uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen" (ofte kalt trefaktormodellen), og en vurdering av sannsynligheten for at et scenario kan inntreffe er med hensikt utelatt.

FBs to tilnærminger har mange likhetstrekk. Forskjellen er at i tilnærmingen basert på NS 5814 foretas en separat vurdering av muligheten for at et angrep finner sted og er vellykket, og denne vurderingen er basert på en kunnskapsbasert sannsynlighetsvurdering. Videre ligger forskjellene i hvordan risiko kommuniseres, og her har begge modellene svakheter. Fordelen med risikomatrisen er at den er enkel å forstå. Faren er at den kan overforenkle og gi inntrykk av større sikkerhet enn det er grunnlag for. Den kommuniserer ikke usikkerhet. Trekanten eller de tre sirklene som er koblet sammen for å kommunisere resultatene fra trefaktormodellen, illustrerer bare hvilke faktorer som brukes. FBs endimensjonale visualisering av risiko er tilstrekkelig, men kommuniserer heller ikke usikkerhet.

Det er avgjørende i begge tilnærminger at resultatet dokumenteres og kommuniseres i en skriftlig rapport som gir et grunnlag for beslutninger. I begge tilnærmingene må usikkerheten knyttet til vurderingene klart kommuniseres. Dette er et forbedringspunkt. I tillegg kan FB vurdere om det bør utføres en følsomhetsanalyse. Videre anbefales FB å vurdere om tilnærmingene kan styrkes ved å benytte sløyfeanalyse og sløyfediagram (bow-tie) for å få frem spredningen i mulige årsaker som kan gi en uønsket hendelse, og spredningen i mulige konsekvenser. Her kan det også være nyttig å bruke hendelsestre- og feiltreanalyse.

Tilnærmingen basert på NS 5814 har en tydeligere og mye bredere vitenskapelig forankring enn NS 5832. En ulempe med NS 5832 er at en tilsynelatende ikke utfører en vurdering av sannsynlighet i analysen. FFI mener at en kunnskapsbasert sannsynlighetsvurdering er nødvendig og uunngåelig i en risikovurdering for tilsiktede uønskede handlinger, selv om dette kan være utfordrende, og selv om man skulle velge en tilnærming basert på NS 5832.

Det er ingen omforent beste fremgangsmåte internasjonalt eller nasjonalt for risikovurderinger for tilsiktede uønskede handlinger. Vitenskapelige artikler og intervjuer støtter opp om denne konklusjonen. Selv om det ikke eksisterer en beste fremgangsmåte, går følgende kjennetegn igjen i en god tilnærming: den (i) er strukturert, (ii) har en arbeidsgruppe med bred kompetanse, (iii) kartlegger kunnskapsstyrken, (iv) er basert på systemforståelse og er konkret, (v) har et helhetlig perspektiv, (vi) kommuniserer risiko og usikkerhet samt (vii) er gjennomsiktig, sporbar og etterprøvbar.

English summary

The Norwegian Defence Research Establishment (FFI) has assessed different approaches to security risk assessments for protection against intentional unwanted actions (security). The work was funded by the Norwegian Defence Estates Agency (FB). The objective was to compare FBs operationalization of two approaches. One approach is based on the Norwegian Standard (NS) 5814: 2008, in which risk is defined as an "expression for the combination of likelihood and consequences of an unwanted event". The second approach is based on the new standard NS 5832: 2014, where security risk is defined as "the relationship between threats towards a given asset and this asset's vulnerability to the specified threat". This approach is often called the three-factor model, and the assessment of the likelihood of a scenario is intentionally omitted.

FBs operationalization of the two approaches has many similarities, but also differences. The operationalization of NS 5814 has a separate assessment of the possibility of an attack, and to what extent the attack is successful, based on a knowledge-based likelihood assessment. Another difference is how risk is visualized and communicated to decision makers. In this case both approaches have weaknesses. A classic Boston Square risk matrix is easy to understand, but can simplify and give the impression of greater accuracy than is justified. The triangle, or the three circles of the three-factor model, illustrates only which factors that are used. It can be argued that FBs one-dimensional visualization of risk in this approach is sufficient, but does not communicate uncertainty.

It is essential in both approaches that the results must be documented and communicated in a report that provides the basis for decision making. In both approaches the uncertainty of the assessments must be clearly communicated. Here, improvements are suggested. FB should consider including sensitivity analyses. FB could also explore whether bow-tie analysis and bow-tie diagrams can be used to convey the variety of possible causes and consequences of a given undesirable event. Here, it may also be useful to use Event Tree Analysis and Fault Tree Analysis.

The NS 5814 approach has a clearer and broader scientific basis than NS 5832. A disadvantage of NS 5832 is that it apparently does not include an assessment of likelihood. FFI argues that a knowledge-based likelihood assessment is necessary and inevitable in a security risk assessment for intentional unwanted actions, even if this is challenging, and even when choosing an approach based on NS 5832.

There is no agreed best practice, internationally or nationally, for security risk assessment. Scientific articles and interviews support this conclusion. Although no best practice has been identified, the following characteristics may enhance and strengthen security risk assessments: One should (i) have a structured process, (ii) establish a working group with broad expertise, (iii) map the knowledge strength among the experts in the working group, (iv) base the assessment on knowledge of the system and be concrete, (v) have a holistic perspective, (vi) communicate risks and uncertainties, and (vii) be transparent, traceable and verifiable.

Innhold

Forord

Forfatterne retter en stor takk til Leif Riis og Margrethe Sørum Rønning i Forsvarsbygg som har bidratt med grunnlagsmateriale, og som dedikerte diskusjonspartnere gjennom hele prosessen i utarbeidelse av denne rapporten. Vi takker Dave Keir (Cloverdale) for hans bidrag, både med underlagsmateriale og vurderinger.

Vi takker også alle respondenter som velvillig har stilt opp og gitt oss viktig og klargjørende informasjon gjennom intervjuene. Det var også meget nyttig å diskutere risikovurderingsmetodikk med de sikkerhetsfaglige miljøene på Stortinget og i Norges Bank. Takk til Morten Bremer Mærli (Stortinget) og Anders Grønli (Norges Bank) som arrangerte disse møtene.

Til sist vil vi takke for alle innspill og tilbakemeldinger vi fikk da vi ba om kommentarer på et utkast av denne rapporten fra oppdragsgiver, respondentene og andre aktører innen sikkerhetsfaglige miljøer og myndighetsorganer.

Odd Busmundrud, Maren Maal, Jo Kiran Hagness og Monica Endregard

Kjeller, 29. mai 2015

1 Innledning

Forsvarsbygg (FB) har siden 2002 utarbeidet risikovurderinger for tilsiktede uønskede handlinger for en rekke forsvarsviktige og samfunnsviktige anlegg. Risikovurderingene har sett på trusler innenfor terrorisme, spionasje, sabotasje[1] og annen kriminalitet (for eksempel ran og tyveri) og vurdert risikoen for disse og foreslått sikringstiltak for å redusere risikoen til et akseptabelt nivå. FB benytter to ulike tilnærminger for denne type risikovurderinger. Den ene er en grovanalysemodell delvis basert på Norsk Standard (NS) 5814 "Krav til risikovurderinger". Den andre tilnærmingen er basert på NS 5832 "Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse".[2] Hensikten med denne rapporten er å vurdere FBs to tilnærminger[3] og hvilket vitenskapelig grunnlag de to tilnærmingene baserer seg på. Rapporten skal også gi en oversikt over metoder for risikovurdering brukt nasjonalt og internasjonalt, og gi anbefalinger til FB om mulige forbedringspunkter.

FBs førstnevnte tilnærming basert på NS 5814 er en kvalitativ analyse der sannsynlighet ikke er basert på frekvens eller hyppigheten til et scenario. I denne tilnærmingen vurderer analysegruppen muligheten for at det finnes aktører som har intensjon og kapasitet til å angripe virksomhetens verdier. I denne rapporten omtaler vi denne tilnærmingen som "sannsynlighet og konsekvens-tilnærmingen".

Nasjonal sikkerhetsmyndighet (NSM), Politiets sikkerhetstjeneste (PST) og Politidirektoratet (POD) ga i 2010 ut "En veiledning: Sikkerhets- og beredskapstiltak mot terrorhandlinger". I denne veilederen presenteres en tilnærming til risikovurdering basert på "total risiko som et utslag av forholdet mellom de tre variablene verdi, sårbarhet og trussel " (NSM m.fl. 2010:17). En arbeidsgruppe har utarbeidet en egen NS-serie for risikostyring for tilsiktede uønskede handlinger basert på denne tilnærmingen. I 2012 kom standarden NS 5830 "Samfunnssikkerhet. Beskyttelse mot tilsiktede uønskede handlinger. Terminologi", og i 2014 kom standardene NS 5831[4] om sikringsrisikostyring og NS 5832 om sikringsrisikoanalyse. FB har utført risikovurderinger basert på denne tilnærmingen for ulike departementsbygg og andre statlige etater de siste tre årene. I denne rapporten omtaler vi denne tilnærmingen som "trefaktormodellen".

Etter at NS 5831 og NS 5832 ble utgitt, har tilnærminger til risikovurderinger blitt diskutert i Dagens Næringsliv[5] og i andre fora. Diskusjonen går blant annet på: "kan man bruke begrepet

[1] Begrepene terrorisme, spionasje og sabotasje er definert i Sikkerhetsloven § 3 pkt. 3-5.
[2] NS (2008). *Krav til risikovurderinger*. NS 5814:2008 og NS (2014). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.* NS 5832:2014.
[3] Det er flere måter å operasjonalisere NS 5814 og NS 5832. Formålet med denne rapporten er å ta utgangspunkt i hvordan FB har valgt å operasjonalisere de to tilnærmingene.
[4] NS (2014). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring*. Norsk Standard NS 5831:2014.
[5] Debatt i *Dagens Næringsliv* fra 17. november- 7.desember 2014 med innlegg av Jan Helge Flesvik (*Aeger Group*), Carsten Rapp (*NSM*), Joakim Barane og Ronald Barø (*Falck Nutec*) og Morten Bremer Mærli (*Stortinget*). Se referanseliste for kilder.

sannsynlighet i en security-kontekst?", og "kan man bruke samme fremgangsmåte på safety og security-fagfeltet?". Denne rapporten bidrar også til å synliggjøre de ulike synspunktene som eksisterer i ulike fagmiljøer og begrunnelsen for disse synspunktene.

Hensikten med denne rapporten[6] er å:

- Vurdere de to tilnærmingene til risikovurdering som FB bruker i dag basert på henholdsvis NS 5814 og NS 5832: "sannsynlighet og konsekvens-tilnærmingen" og "trefaktormodellen" med hensyn til teoretisk og vitenskapelig forankring, kommunikasjon av risiko, bruksområde og styrker og svakheter.
- Gi en oversikt over ulike tilnærminger til risikovurdering for tilsiktede uønskede handlinger i større organisasjoner som Centre for theProtection of the National Infrastructure (CPNI) i Storbritannia, De forente nasjoner (FN), Den europeiske union (EU), Nato, Department of Homeland Security (DHS), ledende forskningsmiljøer og andre bransjer med stort sikringsbehov. Finnes det noen rådende "beste praksis" innenfor området?
- Gi en anbefaling til FB om det er tilnærminger for risikovurderinger for tilsiktede uønskede handlinger FB bør vurdere å bruke eller momenter som bør tas inn i de eksisterende modellene for å forbedre disse.

Rapporten er bygd opp på følgende måte:

Kapittel 2 presenterer rapportens metodiske tilnærming og hvordan rapportens informasjonsgrunnlag er samlet inn. **Kapittel 3** presenterer viktige begreper og definisjoner av disse. **Kapittel 4** beskriver FBs operasjonalisering og bruk av "sannsynlighet og konsekvens-tilnærmingen" og "trefaktormodellen" og gir en sammenligning av disse tilnærmingene. I dette kapitlet blir det også referert til diskusjonen rundt standardene med henvisninger til intervjuene som har blitt utført. I **kapittel 5** blir det vitenskapelige grunnlaget for disse ulike tilnærmingene presentert, samt andre relevante vitenskapelige artikler. I **kapittel 6** blir ulike internasjonale og norske tilnærminger til risikovurderinger presentert. **Kapittel 7** gir konklusjoner og anbefalinger.

Informasjonsgrunnlaget for rapporten er omfattende og inkluderer både transkriberinger av intervjuer, samt gjennomgang og beskrivelse av en rekke tilnærminger til risikovurderinger brukt nasjonalt og internasjonalt. Dette materialet kan ha nytteverdi utover bruken i denne rapporten. Derfor, og av hensyn til gjennomsiktighet og sporbarhet, er dette materialet lagt ved som vedlegg til rapporten.

2 Metode

FFI har brukt ulike typer datamateriale og kilder i denne rapporten. (i) Primærmateriale som for eksempel standarder utgitt nasjonalt og internasjonalt, veiledere for risikovurderinger fra ulike

[6] De tre problemstillingene er hentet direkte fra oppdragsavtalen inngått mellom FB og FFI.

intervjuer med noen relevante aktører. Dette har bidratt til ulike perspektiver på tilnærminger til risikovurderinger. Et utkast av rapporten ble distribuert til respondenter og ulike etater for kommentarer og innspill.

2.1 Dokumentanalyse

Én av metodene i denne rapporten er en kvalitativ dokumentanalyse, der rapporter og veiledninger fra nasjonale og internasjonale organisasjoner og Standard Norge fungerer som det empiriske hovedgrunnlaget. Rapportene er primærdokumenter i den forstand at de blir skrevet av aktørene selv og inkluderer dermed ikke 'et lag av fortolkning' (jfr. akademiske artikler som ofte fortolker og analyserer hva som blir presentert i primærmaterialet) (McCulloch 2004: 4). Det er flere utfordringer ved å basere seg på primærmateriale fra relevante myndigheter ettersom det kan være vanskelig å avdekke svakheter i for eksempel veiledere. Dette er fordi veiledere vanligvis ikke inkluderer informasjon om svakheter eller uoverensstemmelser blant de som har skrevet det. Dermed må en teste og prøve ut veilederne i praksis. Ettersom det ikke var rom for å teste veilederne konstruerte vi en sjekkliste med kriterier som omhandlet hva en god tilnærming til risikovurderinger bør inneholde, og generelle trekk ved tilnærmingen (se kapittel 7). På grunnlag av dette laget vi en sammenfattet tabell, mer detaljer om de ulike tilnærmingene finnes i vedlegg A.

FFI valgte ulike tilnærminger til risikovurderinger blant annet på grunnlag av rapporter som FB formidlet. Andre aktører foreslo også litteratur og forskjellige tilnærminger (se 2.3 for oversikt over FFIs deltakelse på ulike møter og seminarer). Forfatterne søkte også etter akademisk litteratur og veiledere, hovedsakelig anerkjente tilnærminger som var utbredt eller som store internasjonale organisasjoner bruker.

2.2 Semi-strukturerte telefonintervjuer

FFI har intervjuet personer fra ulike miljøer som representerer ulike syn i debatten om risikovurderinger for tilsiktede uønskede handlinger (se vedlegg B for en oversikt over respondenter). Intervjuene ble utført i perioden november 2014 til januar 2015. Hensikten var å kartlegge ulike oppfatninger, synspunkter og tilnærminger, samt sammenligne disse med funn fra dokumentanalysen. FB foreslo relevante personer vi kunne intervjue og vi valgte ut flere respondenter fra akademia, noen av etatene representert i NS 583X-arbeidsgruppen og komitéen, samt personer som har ledet arbeidet med disse standardene. Vi kunne med fordel ha intervjuet flere relevante aktører, men grunnet plass- og tidshensyn ble det valgt ut ni respondenter. Av hensyn til gjennomsiktighet og sporbarhet har vi valgt å inkludere intervjuobjektenes navn i rapporten, samt en oppsummering av hvert enkelt intervju (se vedlegg C).

Respondentene ble først kontaktet på telefon eller epost. Deretter ble et informasjonsbrev om formålet med studien samt noen generelle spørsmål oversendt. FFI foretok en skjønnsmessig vurdering av hvor mye informasjon som skulle gis i forkant av hvert intervju avhengig av hvor kjent intervjuobjektet var med FFIs studie på forhånd. Intervjuene ble foretatt over telefon slik at intervjusituasjonen ble mest mulig lik for respondentene. Det ble gjort opptak av samtalene med

intervjusituasjonen ble mest mulig lik for respondentene. Det ble gjort opptak av samtalene med respondentens samtykke. Intervjuene varte mellom 40-90 minutter. Respondentene svarte på grunnlag av sin fagbakgrunn, og dermed kunne intervjuet ta ulike retninger ettersom intervjuet var semi-strukturert. I forkant av intervjuene utarbeidet FFI en intervjuguide som bestod av generelle spørsmål om standardene NS 5814 og NS 583X-serien. Samtidig som intervjuene ble utført, var det en meningsutveksling på samme tematikk i Dagens Næringsliv. Dette bidro til at det var lettere å diskutere og få frem de ulike sidene i debatten i intervjusituasjonen. Det må bli presisert at respondentene ikke uttalte seg om FBs operasjonalisering av standardene, bortsett fra en respondent som kom fra FB. De andre respondentene uttalte seg om standardene NS 5814 og NS 5832 på bakgrunn av deres egen erfaring og kunnskap.

Intervjuene ble transkribert og sendt til respondentene for gjennomlesning og godkjenning. Alle respondentene fikk anledning til å spisse budskapet og fjerne detaljer slik at det ble en tekst de står inne for. En oppsummering av alle intervjuene er inkludert som vedlegg til rapporten. Alle sitater brukt i rapporten ble oversendt for sitatsjekk.

2.3 Studietur og deltakelse på fagseminarer

FFI og FB besøkte Centre for the Protection of the National Infrastructure (CPNI) i Storbritannia for et arbeidsmøte. CPNI presenterte sine tilnærminger til risikovurdering fra fem sektorer innen kritisk infrastruktur; (i) transport, (ii) finans, (iii) befolkede plasser, (iv) statlig sektor og (v) personell. CPNI ga også innspill på FBs tilnærminger til risikovurderinger basert NS 5814 og NS 5830 etter presentasjoner FB og FFI holdt. Erfaringer fra CPNI har vært viktig for denne rapporten og mange av deres vurderinger og beste praksis blir referert til.

FFI har hatt flere møter om ulike tilnærminger til risikovurderinger, herunder et seminar med FB som presenterte eksempler på bruk av FBs to tilnærminger[7], Stortingsadministrasjonen[8] og representanter fra Norges Bank[9]. Ellers deltok FFI også på fagseminarer i regi av polyteknisk forening[10] og Falck Nutec[11].

2.4 Avgrensninger

Studiens primære problemstilling er knyttet til tilsiktede uønskede handlinger (security) og FBs tilnærming til risikovurdering basert på de norske standardene NS 5814 og NS 5832. Tyngdepunktet har vært på den delen av risikovurdering som utgjør risikoanalyse i NS 5814, og som omtales som sikringsrisikovurdering i NS 5832. Vi har ikke berørt utfordringer knyttet til bruk av resultatene fra en risikoanalyse for å utføre en risikoevaluering opp mot risikoakseptkriterier.

[7] Møte i forsvarsbygg (28.02.2014).
[8] Møte med Stortingets administrasjon med Morten Bremer Mærli og andre i sikkerhetsavdelingen (04.06.2014).
[9] Møte med Norges Bank med Anders Grønli og flere representanter (28.08. 2014).
[10] Seminar i regi av Polyteknisk forening "Hvorledes skal vi tilnærme oss risikostyring av såkalt villede hendelser». (15.10.2014).
[11] Frokostseminar i regi av Falck Nutec vedrørende de nye standardene i NS 583x serien (18.11.2014).

Det er mange måter å operasjonalisere standarder på. FFI studerer FB sin operasjonalisering av NS 5814 og NS 5832 ettersom det var grunnlaget for studien og mandatet vårt fra FB. FBs operasjonalisering av standardene er ikke nødvendigvis "representativ" for alle andre virksomheter som utfører risikovurderinger. FB har mye praktisk erfaring med risikovurderinger basert på standardene.

Risikovurderinger for analyseobjekter mot tilsiktede uønskede handlinger inneholder nødvendigvis både en system- og verdibeskrivelse, en vurdering av sårbarheter og risiko spesifikt for virksomheten. Dette er sensitiv informasjon for virksomheten, og for offentlige etater ofte gradert etter Sikkerhetslovens bestemmelser. Vi har fått innsyn i kun få eksempler på faktisk bruk av tilnærmingene og dokumenterte risikovurderinger.

Omfanget av åpen litteratur på dette fagområdet er stort. Vi har så godt det har latt seg gjøre, innenfor rammen av prosjektet, forsøkt å dekke relevant litteratur i form av standarder, veiledninger og beskrivelser av ulike metodiske tilnærminger, akademiske lærebøker og vitenskapelig litteratur, men dette er på ingen måte komplett.

3 Bakgrunn, begreper og terminologi

Det er flere viktige begreper som inngår når en skal vurdere risiko, bl.a. sannsynlighet, risikostyring, risikovurdering og risikoanalyse. Ulike lærebøker, standarder, veiledninger og øvrig litteratur definerer og bruker disse og en rekke andre sentrale begreper, men definisjoner og begrepsbruk er ikke alltid enhetlig, noe som kan være forvirrende. Dette kapitlet presenterer ulike definisjoner og drøfter en del sentrale begreper blant annet risiko og sannsynlighet. I tillegg gis en kort presentasjon av metoder og trinn og aktiviteter i risikovurderinger.

3.1 Risiko

Gjennom tidene har begrepet "risiko" blitt brukt på mange måter. Aven (2012) har laget en oversikt over bruken av begrepet på forskjellige språk fra det 12. århundre til i dag.[12] Uansett språk og tid, har betydningen av risiko vært i retning av noe skadelig og ubehagelig. I vanlig språkbruk forstås risiko som muligheten for at noe negativt kan skje. Riktignok definerer SN-ISO guide 73:2009[13] risiko som "*virkningen av usikkerhet på oppnåelse av mål*", og som noe som kan være både positivt og negativt. Noe positivt kan være en "risiko for å tjene penger på en aktivitet". Dette har gjort det nødvendig å innføre et nytt begrep for å betegne en risiko som man bare kan tape på. Begrepet som er innført er "ren risiko" (hentet fra "pure risk"[14] på engelsk), som betyr en hendelse som ikke kan medføre gevinst, men bare tap eller ingen vinning.

[12] Aven T. (2012). The risk concept—historical and recent development trends. *Reliability Engineering and System Safety* **99** (2012) 33–44.
[13] SN-ISO (2009). SN-ISO Guide 73:2009. *Risikostyring. Terminologi*.
[14] "Pure Risk" er definert som "*A category of risk in which loss is the only possible outcome; there is no beneficial result […]*" (Investopedia 2014).

I sikkerhetsfagmiljøet er det imidlertid kommet kritiske røster mot definisjonen i SN-ISO guide 73:2009 (Aven, 2011 [15], Leitch, 2010[16]). Aven og Renn (2010:3)[17] foreslår en definisjon der "*Risk refers to uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value"* (*Usikkerheten om, og alvoret av følgen av en aktivitet på noe som mennesker verdsetter*). Definisjonen i SN-ISO guide 73:2009 fører også til at enkelte i fagmiljøet setter likhetstegn mellom risiko og usikkerhet, og begynner å snakke om "negativ usikkerhet", noe som ikke gir så mye mening.

SN-ISO guide 73:2009 ble etablert for å definere generelle termer for risikostyring "*for å stimulere til en felles og konsekvent forståelse av og en samordnet fremgangsmåte for beskrivelse av aktiviteter knyttet til risikostyring og til bruk av en enhetlig terminologi for prosesser og rammeverk som omhandler risikostyring"* på tvers av forskjellige bruksområder og – typer, på både norsk og engelsk. Diskusjonen om definisjonen av risiko som det er referert til ovenfor, er et eksempel på at dette er en utfordring. Imidlertid er det en rekke andre standarder fra den internasjonale standardiseringsorganisasjonen (International Standardization Organization, ISO) som forholder seg til og bruker de samme termene og definisjonene som SN-ISO guide 73:2009. Dette gjelder standarder i den såkalte 27000-serien[18] for IKT-sikkerhet og 31000-serien[19].

Denne rapporten tar for seg risikoen som følge av tilsiktede uønskede handlinger, og vi trenger ikke noen finurlig definisjon av risiko for å forstå at det som menes er muligheten for at noe ubehagelig skal kunne skje, og at det dreier seg om noe som er negativt for den som rammes. Dette samsvarer med definisjonen i NS 5814:2008[20], som sier at risiko er *"utrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse"*. Dette er altså en kombinasjon av to størrelser, sannsynlighet og konsekvens, og hendelsen er noe som er uønsket. I merknader til definisjonen av risiko i SN-ISO guide 73:2009 står at "*Risiko karakteriseres ofte ved å referere til potensielle hendelser og konsekvenser eller en kombinasjon av disse*", og videre at "*Risiko uttrykkes ofte som en kombinasjon av konsekvensene av en hendelse (…) og den tilhørende muligheten for at den skal forekomme*", som ikke skiller seg vesentlig fra definisjonen av risiko i NS 5814:2008. DHS Security Risk Lexicon (2010:27) definerer risiko som "*muligheten for et uønsket utfall som følge av en hendelse eller forekomst, som bestemmes av dens sannsynlighet og tilhørende konsekvense*r", som også er i samsvar med NS 5814:2008.

---

[15] Aven T. (2011). On the new ISO guide on risk management terminology, *Reliability Engineering and System Safety* **96** (2011) 719 – 226.
[16] Leitch M. (2010). ISO 31000:2009 - The New International Standard on Risk Management, *Risk Analysis*, Vol. **30**, No. 6 (2010) 887-892.
[17] Aven, T., Renn, O. (2010). *Risk Management and governance: Concepts, guidelines and applications.* Heidelberg: Springer Verlag.
[18] NS-ISO/IEC (2011). *Informasjonsteknologi. Sikringsteknikker. Risikostyring av informasjonssikkerhet.* Norsk Standard NS-ISO/IEC 27005:2011, ISO/IEC (2014). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO/IEC 27000:2014 og NS-ISO/IEC (2013). *Informasjonsteknologi. Sikringsteknikker. Styringssystemer for informasjonssikkerhet.* Krav. Norsk Standard NS-ISO/IEC 27001:2013.
[19] NS-ISO (2009a). *Risikostyring. Prinsipper og retningslinjer*. Norsk Standard NS/ISO 31000:2009. NS-ISO (2009b). *Risikostyring. Metoder for risikovurdering*. Norsk Standard NS-ISO/IEC 31010:2009.
[20] NS (2008). *Krav til risikovurderinger*. Norsk Standard NS 5814:2008.

NS 5830:2012 definerer risiko som "*forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifikke trusselen*". Her er altså sannsynligheten ikke spesifikt nevnt, og med hensikt utelatt i definisjonen og i de aktiviteter og prosesser som er beskrevet i de påfølgende standardene NS 5831:2014 og NS 5832:2014. Dette er kjernen i den foreliggende undersøkelsen. Fra et naturvitenskapelig/matematisk ståsted er det dessuten problematisk å snakke om "forholdet mellom". Forholdet mellom to størrelser er den første dividert med den andre, som når man ønsker å sammenligne literprisen på melk i forskjellige kartongstørrelser ved å regne ut forholdet mellom pris og innhold. Her vil "forholdet mellom trussel og sårbarhet" innebære at høy sårbarhet gir lav risiko. Her bør det vurderes om "forholdet mellom" skal byttes ut med andre ord som ikke kan bety en matematisk operasjon.

Hensikten med risikovurdering er å danne grunnlaget for risikoreduserende tiltak. For å vite om man lykkes, er det nødvendig å måle risiko. Risikovurderingen må derfor fremskaffe måltall for størrelsen av risiko. Utfordringene står i kø. Hvordan måle risiko? Hva er måle-enheten? Hvordan skal man gå fram for å utnytte tilgjengelig kunnskap for å finne fram til måltallene.

Fra et naturvitenskapelig ståsted ville det ideelle være å sette opp en formel som man setter tilgjengelige data inn i for å få et svar på hvor stor risikoen er. I forbindelse med ulykker eller skade forårsaket av naturkrefter kan man ha et erfaringsgrunnlag, og helt uventede ting skjer sjelden. Kommer det en storm har man data for hvilket vindpress en konstruksjon kan tåle, og man har data for vindstyrker og hyppigheter. Likeledes har man data for feilraten til mekaniske konstruksjoner. Man kan ha et erfaringsgrunnlag, ettersom skadeårsaken til en viss grad er forutsigbar. Men også i disse tilfellene har man usikkerheter. Været kan endre seg uventet, mennesker kan gjøre ting man ikke hadde regnet med, eller de kan unnlate å gjøre noe de skulle gjort. Imidlertid er usikkerheten i disse tilfellene av en annen karakter sammenlignet med usikkerheten når det gjelder tilsiktede uønskede handlinger. Der har man å gjøre med en trusselaktør som er strategisk og kalkulerende, som ønsker å volde mest mulig skade eller oppnå maksimal egen vinning, eller oppnå oppmerksomhet og spre frykt. En trusselaktør er også i stand til å tilpasse seg sikringstiltak og endrede rammebetingelser. De tilgjengelige data om truslene er i beste fall usikre. Ofte er det ikke mulig å beskrive trusselaktørenes intensjon og kapasitet på annen måte enn å beskrive dem med ord som "liten", "middels" eller "stor", og kanskje "svært stor". Det er klart at man kan tilordne tallstørrelser til disse begrepene og sette disse inn i en eller annen formel, og for analytikerens interne bruk kan dette være nyttig. Likevel må en være klar over at det resultatet som kommer ut er beheftet med usikkerheter. Derfor er risikovurderinger ekstra krevende når det gjelder tilsiktede uønskede handlinger. Ofte ender man opp med å måtte si noe sånt som at "det er 50 % sannsynlighet for at dette vil skje i løpet av de neste ti årene." Men hva betyr egentlig sannsynlighet?

3.2 Sannsynlighet

Sannsynlighet er et sentralt begrep i risikoanalyser og risikovurderinger, men ofte blir det brukt uten at det blir klart definert hva som menes med det. Willy Røed argumenterer at "*vi trenger å få en bedre fellesforståelse av sannsynlighetsbegrepet […] Det har over lang tid vært skarpe skiller*

mellom safety og security, og det kan ha ført til misforståelser" (vedlegg C.3). Her vil vi omtale definisjoner og tolkninger av sannsynlighet som er mest relevant for denne rapporten.

Et problem med sannsynlighet i forbindelse med risikovurdering av tilsiktede uønskede handlinger er at det er (i) vanskelig, (ii) beheftet med stor usikkerhet, og (iii) mange mener det ikke er mulig å vurdere og gradere sannsynligheten for hendelser som forekommer sjelden og der det i tillegg står en strategisk trusselaktør bak. Hadde en hendelse skjedd ofte, ville man uten videre satt sannsynligheten til 100 %, og da ville det ikke vært noe problem hvorvidt den skulle inngå i vurderingen eller ikke. Som vi skal se senere opererer Trefaktormodellen indirekte med en slik binær sannsynlighet ved at man i analysen enten må velge å ta med en hendelse eller utelukke den. Problemet oppstår når sannsynligheten for en hendelse vurderes som liten, samtidig som konsekvensene blir store. Dessuten kan sannsynlighet forstås på flere måter.

I dagens debatt på security-feltet er det uenighet om i hvilken grad sannsynlighet kan eller bør bli brukt når en studerer tilsiktede uønskede handlinger. Det er ofte sannsynlighetsbegrepet som blir trukket frem når en skal forklare hvorfor en trenger en ny standard som omhandler tilsiktede uønskede handlinger. I en artikkel i Teknisk Ukeblad skriver Barane om den nye 583X-standardserien: "*Standardenes tilnærming til risikoanalyse baserer seg på vurdering av tre faktorer; verdi, trussel og sårbarhet og samspillet mellom disse, i motsetning til den tradisjonelle vurderingen av sannsynlighet og konsekvens*"[21]. Standardserien 583X definerer ikke og bruker tilsynelatende ikke begrepet sannsynlighet.

NS 5814:2008 definerer sannsynlighet som "*i hvilken grad det er trolig at en hendelse kan inntreffe*". I merknader står at "*Sannsynlighet kan uttrykkes med ord eller som en tallverdi*", og at "*Frekvens kan brukes i stedet for sannsynlighet ved estimering av risiko*".

På engelsk brukes begrepene "probability" og "likelihood" om det som på norsk i risikostyringsterminlogi vanligvis oversettes med sannsynlighet. I SN-ISO Guide 73:2009 er "probability" definert som sannsynligheten for at noe skal skje, angitt som et tall mellom 0 og 1. Denne definisjonen er beholdt i den norske oversettelsen, hvor sannsynlighet er angitt som et tall, og altså er en matematisk sannsynlighet. Det engelske ordet "Likelihood" er i SN-ISO Guide 73:2009 definert som "*chance of something happening*", og oversatt til norsk med ordet "mulighet" definert som "*potensialet for at noe skal skje*".

T Aven (2010:623)[22] skriver at sannsynlighet kan forstås på to grunnleggende måter:

"(a) A probability is interpreted as a relative frequency P_f: the relative fraction of times the event occur if the situation analysed were hypothetically ''repeated'' an infinite number of times. The underlying probability is unknown, and is estimated in the risk analysis. We refer to this as the relative frequency interpretation."

[21] Barane, J.E. (2014). "Risikohåndtering krever analyser". *Teknisk Ukeblad*, oktober 2014.
[22] Aven, T. (2010). On How to define, understand and describe risk. *Reliability Engineering and System Safety* **95** (2010) 623 – 631.

(b) Probability P is a measure of uncertainty about future events and consequences, seen through the eyes of the assessor and based on some background information and knowledge. Probability is a subjective measure of uncertainty, conditional on the background knowledge (the Bayesian perspective).”

Sammenfattet kan altså sannsynlighet forstås på to måter:

(a) Sannsynlighet kan forstås som den relative hyppigheten en hendelse opptrer med i en hypotetisk situasjon som gjentas et uendelig antall ganger (matematisk sannsynlighet eller frekvensbasert sannsynlighet).
(b) Sannsynlighet er et mål for usikkerheten om fremtidige begivenheter og deres konsekvenser, sett gjennom øynene til den som vurderer, og basert på bakgrunnsinformasjon og kunnskap. Det er et subjektivt mål for usikkerhet basert på bakgrunnskunnskap (kunnskapsbasert sannsynlighet).

Disse to tilnærmingene vil bli nærmere kommentert i kapitlene 3.3.1 og 3.3.2. Rausand og Utne (2009:31) deler forståelsen av begrepet sannsynlighet inn i to grupper.[23] Frekventist-tilnærmingen er avgrenset til fenomener som kan tenkes gjentatt et stort antall ganger og beskrives matematisk. I en Bayesiansk tilnærming oppfattes sannsynlighet som et mål på vår tro om utfallet, det vil si en subjektiv sannsynlighet, men basert på den kunnskap den som vurderer dette besitter.

3.2.1 Eksempel på bruk av matematisk sannsynlighet

Med matematisk sannsynlighet menes et tall mellom null og én. Hvis sannsynligheten for en hendelse er én, vil den med sikkerhet skje. Er sannsynligheten null, vil den aldri skje. Hadde man kunnet tallfeste sannsynligheter, ville dette gitt en mulighet for å kunne regne ut risiko når konsekvensen av en hendelse var kjent. Det ideelle ville være at man hadde en oversikt over tilsvarende anslag mot tilsvarende virksomhet. Da kunne man si at sannsynligheten for at noe kommer til å skje er gjennomsnittlig antall hendelser per tidsenhet per virksomhet. Dersom det skjer mange hendelser kan dette la seg gjøre. Dette tilsvarer definisjon (a) i Avens definisjon ovenfor, men selv da kan usikkerheten være stor, slik følgende regneeksempler viser.

Tilsiktede uønskede handlinger i Norge

Siden terrorhandlinger i Norge er sjeldne, har vi, for å skaffe relevant tallmateriale, sett på forekomsten av bankran i Norge. Dette er også en tilsiktet uønsket handling, hvor det er steder det finnes verdier (penger), og det finnes aktører (bankranere) som gjerne vil tilegne seg disse verdiene. Opp til flere ganger hvert år er det personer som truer til seg penger i bankfilialer. Dette gjør det mulig å beregne i ettertid hvor stor sannsynligheten er for at en filial skal bli ranet i løpet av et år. Hadde alle bankranere hatt regelmessig arbeidstid ville dette tallet vært det samme hvert år, og man kunne forutsi nøyaktig hvor mange ran som ville skje det neste året. Dette ville gitt banksjefen nøyaktig informasjon som kunne brukes til å sette i verk sikringstiltak. Så enkelt er det ikke, også bankranere er uforutsigbare, slik *Tabell 3.1* viser.

[23] Rausund, M., Utne, I. B. (2009). *Risikoanalyse – teori og metoder*. Tapir akademisk forlag, Trondheim.

År	Antall ran	Antall bankfilialer	Ran pr. bankfilial pr. år
1999	32	1468	2,2 %
2000	25	1457	1,7 %
2001	15	1429	1,0 %
2002	16	1414	1,1 %
2003	9	1376	0,7 %
2004	8	1348	0,6 %
2005	8	1234	0,6 %
2006	1	1234	0,1 %
2007	3	1260	0,2 %
2008	3	1330	0,2 %
2009	5	1184	0,4 %
2010	10	1157	0,9 %
2011	10	1158	0,9 %
2012	9	1127	0,8 %
Gjennomsnitt			0,8 %
Standardavvik			0,6 %

Tabell 3.1 Antall bankran i Norge 1999 til 2012. (Tallene er hentet fra en artikkel i Stavanger Aftenblad 1. aug. 2013).

Her er det store variasjoner fra år til år i antall ran. Siden antall bankfilialer viser en systematisk nedgang i perioden, er ransraten gitt som antall ran pr. filial pr. år. Dette gjør det mulig å finne en gjennomsnittlig sannsynlighet og tilsvarende standardavvik. For at dette skal være meningsfullt må dataene følge en statistisk normalfordeling, og det gjør de faktisk. Da kan man kan beregne et konfidensintervall for sannsynligheten som kan brukes for å forutsi noe om fremtiden. Denne enkle utregningen fører imidlertid til at det blir en endelig sannsynlighet for et negativt antall bankran. 90% konfidensintervall blir [-0,184% ; 1,784%]. Man må derfor modifisere beregningen noe.

En grundigere statistisk analyse av tallene (se vedlegg D) anslår at 90 % konfidensintervallet for sannsynligheten for at en bankfilial skal bli utsatt for ran i løpet av et år er 0,15 % til 2,4 %. Det betyr at man med 90 % sannsynlighet kan si at det vil gå 42 til 667 år mellom hver gang en bestemt bankfilial blir ranet. Dette innebærer at selv der man har historiske data som kan brukes til å beregne en matematisk sannsynlighet, kan usikkerheten i sannsynligheten være så stor at et anslag basert på kunnskap, ville gjøre samme nytten. Om man anslo at det ville gå mellom 100 år og 1000 år mellom hver gang en bankfilial ble ranet ville nytten av denne kunnskapen være av samme størrelse som den matematisk beregnede sannsynligheten basert på historiske data.

I eksemplet ovenfor hadde man nok data til å komme fram til en matematisk sannsynlighet, ikke som et enkelt tall, men angitt ved en øvre og nedre grense. Samtidig kan det være nyttig å se hva dette betyr for en beslutningstager som skal vurdere om det er noen grunn til å sette i verk sikringstiltak mot ransforsøk.

Vår største bank har i dag ca. 140 filialer. Ut fra tallene ovenfor kan man si at det er mellom 0,15% og 2,4% sannsynlighet for at en av dem blir utsatt for et ran. For videre regning er det

enklere å se på sannsynligheten for at en filial ikke skal bli utsatt for ran. Man kan si at sannsynligheten for at en filial ikke skal bli ranet, p(ikke ran), er mellom 97, 6% og 99,85%. Sannsynligheten for at ingen av de 140 filialene skal bli ranet i løpet av neste år er da P(ingen ran) = p(ikke ran) ^{140}. Utregnet blir da dette P(ingen ran) = [3 % , 80 %], der tallene i hakeparentesen angir 90% konfidensintervall. Sannsynligheten for at minst én filial skal bli ranet er da 100 % minus P(ingen ran), eller matematisk uttrykt: P(minst ett ran) = 100 % - P(ingen ran) = [97 % , 20 %]. Det er altså mellom 20 % og 97 % sannsynlighet for at minst én filial skal bli forsøkt ranet kommende år. Dette er tallene bankens ledelse må forholde seg til når man skal avgjøre om det er nødvendig å sette inn sikringstiltak for å redusere risikoen for ran av filialer.

Terrorhandlinger i Europa

Når man ser på Europa under ett, er det utført eller planlagt tilstrekkelig antall terrorhandlinger til at det er mulig å gjøre meningsfylt statistikk. Det som er benyttet der er data fra en artikkel av FFI-forskerne Petter Nesser and Anne Stenersen[24]. Totalt har man der data over 122 planlagte jihadiske[25] terrorhandlinger i Europa i tidsrommet 1994 til 2013. Dette tallet inkluderer også mulige planlagte handlinger hvor dokumentasjonen er usikker. Av de 122 er 29 svakt dokumentert, og 93 er veldokument. 36 handlinger ble iverksatt. De to mest utsatte landene var Frankrike og UK, og disse er listet separat i *Tabell 3.2*.

90 % konfidensintervall angir det største og minste antall terrorhandlinger man med 90% sannsynlighet kan si vil forekomme i løpet at et år. Verdiene er rundet av til nærmeste hele tall. Dette kan oppfattes som en prediksjon av antall hendelser kommende år. Ved bruk av tradisjonell aritmetisk statistikk oppstår her det samme paradokset som i "bankraneksemplet" ovenfor, at det i noen tilfeller blir en endelig sannsynlighet for at det kan forekomme et negativt antall terrorhandlinger. Paradokset oppstår fordi man antar at dataene er normalfordelt. Dette kan løses ved å anta at dataene er log-normal fordelt, slik det også måtte gjøres for bankraneksemplet (Se vedlegg D). Det vil si at logaritmen til antallet er normalfordelt. Da må man riktignok se bort fra de årene det ikke forekommer noen terrorhandlinger (siden logaritmen til null er minus uendelig). Da blir 90% konfidensintervallene som angitt i den nederste raden.

[24] Nesser, P., Stenersen, A. (2014). "The Modus Operandi of Jihadi Terrorists in Europe", *Perspectives on Terrorism*, **8** (6) (2014) 2-24.
[25] "Jihadi" – "refers here to militant individuals, groups, networks and ideologies emanating from the Arab-based foreign fighter movement of the Afghan jihad in the 1980s."

År		Antall terrorhandlinger			
		Totalt (planlagt)	Iverksatt	Totalt Frankrike	Totalt UK
	1994	1	1	1	
	1995	9	8	9	
	1996	2	1	1	
	2000	1	0		
	2001	5	1	3	
	2002	7	0	1	2
	2003	11	1	0	4
	2004	12	2	1	2
	2005	6	2	1	2
	2006	7	1	0	1
	2007	7	1	0	3
	2008	8	2	2	3
	2009	6	4	1	1
	2010	12	4	1	3
	2011	7	1	0	2
	2012	9	3	2	3
	2013	12	4	3	4
Statistikk	Totalt	122	36	26	30
	Gjennomsnitt	7,2	2,1	1,6	2,3
	Standardavvik	3,5	1,9	2,1	1,1
	90% konfidensintervall	2 til 13	-1 til 5	-2 til 5	0 til 4
	90% konfidensintervall, lognormal fordeling	2 til 20	1 til 6	1 til 5	1 til 5

Tabell 3.2 Jihadistiske terrorhandlinger i Europa. I årene 1997 til 1999 forekom ingen handlinger av denne typen i Europa.

Disse eksemplene viser er at beslutningstagere må være klar over hva matematiske sannsynligheter betyr når de vurderer hvilke beslutninger som skal tas. Det er misvisende å oppgi sannsynligheten for en usikker hendelse som ett tall. Sannsynligheten må oppgis som et tallområde innenfor en nedre og øvre grense. Dette kan være en måte å kommunisere usikkerhet på. Som eksemplene viser, kan forventet øvre grense for antall terrorhandlinger pr år være 5- 10 ganger nedre grense. Dette viser samtidig at det ikke finnes noen "korrekt" sannsynlighet for hendelser av denne typen.

3.2.2 Kunnskapsbasert sannsynlighet

I praksis er det sjelden det lar seg gjøre å finne matematisk sannsynlighet for tilsiktede uønskede handlinger. Man mangler rett og slett nødvendige data når det gjelder hendelser som sjelden eller aldri har skjedd. Og, selv om man skulle ha forholdsvis god tilgang på historiske, data viser eksemplene ovenfor at usikkerheten er stor.

Når det gjelder virksomheter FB utfører oppdrag for, og den type handlinger som studeres, vil det være vanskelig å skaffe historiske data. Da må man ty til vurderinger og antagelser basert på tilgjengelig kunnskap. Det tilsvarer at Avens definisjon (b) av sannsynlighet basert på bakgrunnskunnskap bør brukes, og usikkerheten blir så stor at man bare kan angi sannsynligheten på en kvalitativ skala, av typen svært sannsynlig – sannsynlig – lite sannsynlig.

Aven argumenterer for at man må forlate tanken om at det finnes en korrekt (objektiv) sannsynlighet og dermed risiko (Aven, 2007:54)[26], og viser til litteraturen og vitenskapelige pionerer som betegner sannsynligheten som subjektiv. Aven foreslår å bruke begrepet "kunnskapsbasert sannsynlighet".

3.3 Risikostyring, risikovurdering og risikoanalyse

Risikostyring innebærer å "*identifisere, analysere og vurdere mulige risikoforhold i et system eller i en virksomhet, samt å finne frem til og iverksette tiltak som kan redusere mulige skadevirkninger*" (Rausand og Utne, 2009:77). SN-ISO Guide 73:2009 definerer risikostyring som "*Koordinere aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko*", og i Avens bok om Risikostyring er begrepet definert på følgende måte: "*Med risikostyring forstås alle tiltak og aktiviteter som gjøres for å styre risiko*" (Aven, 2007:13).

Lærebøker fra norske universiteter benytter de samme overordnede definisjonene av risikostyring, risikovurdering og risikoanalyse og sammenhengen mellom disse (Aven 2007, Aven m.fl., 2008, Rausand og Utne, 2009). Definisjonene og begrepsbruken i disse lærebøkene er også i tråd med NS 5814:2008, NS/ISO 31000:2009, NS-ISO/IEC 27005:2011 og SN-ISO Guide 73:2009. I både standarder og lærebøker er det brukt en enhetlig terminologi på norsk og engelsk.

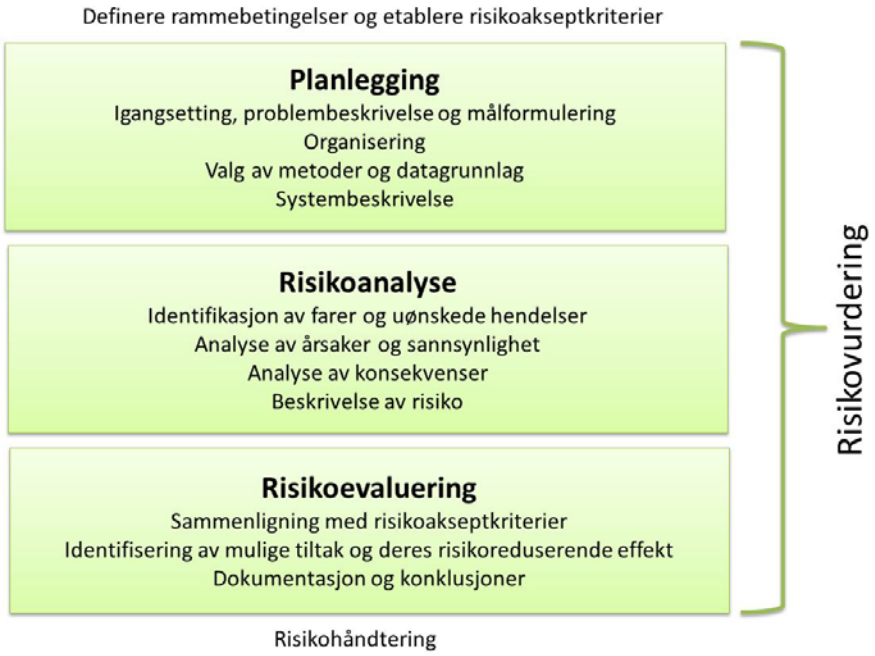
Både risikovurdering og risikoanalyse inngår som deler av en risikostyringsprosess. I henhold til NS 5814:2008 er **risikovurdering** en samlet prosess som består av de tre trinnene planlegging, **risikoanalyse** og risikoevaluering. **Risikoanalyse** defineres som en systematisk fremgangsmåte for å beskrive og/eller beregne risiko. Risikoanalysen utføres ved kartlegging av uønskede hendelser og årsaker til og konsekvenser av disse. Hva disse trinnene inneholder er illustrert i Figur 3.1.

NS 5832:2014 definerer **sikringsrisikoanalyse** som **sikringsrisikovurdering** samt vurdering av strategi og tiltak. Her har man altså valgt å snu om på bruken av "…*vurdering*" og "…*analyse*" sammenlignet med det som tidligere er gjort i lærebøker og andre standarder. **Sikringsrisikovurdering** er definert som en helhetsvurdering basert på verdivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering. Hva som inngår i disse trinnene er illustrert i Figur 3.2.

Når det gjelder definisjon av noen andre sentrale begreper, slik som **sårbarhet**, **konsekvens** og **fare** er NS 5814:2008 og NS 5830:2012 i samsvar, og den siste standarden viser til den første. NS

[26] Aven, T. (2007). *Risikostyring. Grunnleggende prinsipper og ideer*. Oslo. Universitetsforlaget.

5814:2008 definerer **sårbarhet** som "*manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin opprinnelige tilstand eller funksjon etter hendelsen*" og **konsekvens** som "*mulig følge av en hendelse*". **Fare** defineres som "*handling eller forhold som kan føre til en uønsket hendelse*". I merknaden står at dette kan skyldes både tilsiktede eller utilsiktede handlinger og forhold.



Figur 3.1 Sammenhengen mellom risikovurdering og risikoanalyse i henhold til NS 5814:2008.

Figur 3.2 Sammenhengen mellom sikringsrisikovurdering og sikringsrisikoanalyse i henhold til NS 5832:2014.

3.4 Scenarioer

I de fleste risikovurderinger brukes scenarioer for å hjelpe brukeren med å spille ut en uønsket hendelse som kan skje i fremtiden. Direktoratet for samfunnssikkerhet og beredskap (DSB) (DSB, 2012a:14) definerer scenario som: "*en detaljert og konkretisert beskrivelse av en uønsket hendelse; en beskrivelse av en framtidig tilstand og den serien av handlinger og/eller hendelser som leder dit*".

Oljedirektoratet (OD, 2011)[27] skriver at scenarioanalyser er ofte "*en kvalitativ og strukturert måte å beskrive mulige framtidige utfall*". Prinsipielt kan man si at et scenario består av (i) en beskrivelse av et system som er i en utgangstilstand, (ii) en tenkt starthendelse. Deretter analyserer man hva som kan komme til å skje ut fra dette utgangspunktet.

I sikringssammenheng må en velge scenarioer som passer med virksomheten en skal risikovurdere. Man har dermed noen rammebetingelser. Man har et system (virksomheten) som kan bli utsatt for en trussel. Systemet er gitt, og kan ikke velges. Det som kan velges er trusselen. Dette setter rammer for valg av scenarioer. Scenarioet må tilpasses rammebetingelsene. Dette innebærer at man ikke kan lage faste scenarioer som passer i alle situasjoner. Samtidig må man passe på at man får med alt som er tenkelig. Her kan det være en hjelp å ha en liste over tenkbare trusler, slik at man reduserer faren for å overse noe. Samtidig må ikke denne listen bli en sovepute som fritar de som skal foreta en risikovurdering fra å tenke selvstendig. Man må på eget initiativ kunne føye til nye punkter på listen.

Det kan her være fristende å innføre et nytt sannsynlighetsbegrep – "ubevisst sannsynlighet". Når man skal foreta en risikoanalyse er det uunngåelig at man må velge et begrenset antall scenarioer. Det innebærer at det er noen mulige scenarioer man velger bort. Som regel er det ut fra en bevisst tankeprosess, men det kan også være at det er noen scenarioer man ikke har fantasi til å tenke seg. En utenkelig hendelse som likevel inntreffer og har store konsekvenser, kalles gjerne sorte svaner (eng: "Black Swan"), et begrep som ble innført av Nassim N. Taleb i 2007. (Taleb, 2007)[28]

3.5 Metoder for risikovurdering

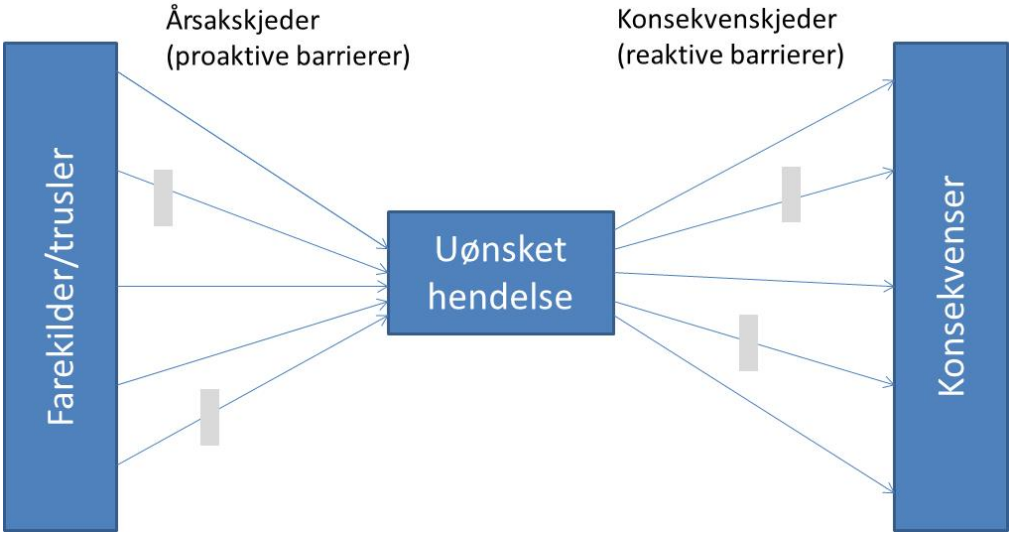
Et moment som trekkes frem er at valg av metodisk tilnærming og detaljeringsgrad i en risikovurdering er avhengig av formålet og rammene, både tidsmessig og ressursmessig (Aven m.fl., 2008; Rausand og Utne, 2009; NS 5814:2008; NS-ISO/IEC 31010:2009). Disse referansene gir til sammen en god forklaring og fremstilling av ulike metoder innen risikovurderinger. Ofte er det en fordel å kombinere flere metoder. Her omtaler vi meget kort noen aktuelle metoder.

En "**bow-tie-analyse**", eller oversatt til norsk som **sløyfeanalyse**, kan være et nyttig hjelpemiddel for rammeverk og for å illustrere hva som gjøres i en risikoanalyse. Det handler om å identifisere

[27] OD (2011). *Fra scenarioer til handling*. Sist besøkt 18.12.2014. http://www.npd.no/Publikasjoner/Rapporter/Fire-framtidsbilder/Fra-scenarioer-til-handling/

[28] Taleb, N. N. (2010). *The Black Swan: The Impact of the Highly Improbable*. Penguin Books, London, 2. utg., ISBN 978-0-1410-3459-1.

uønskede hendelser, farekilder/trusler som på ulik måte eller i kombinasjon kan føre til hendelsen (årsakskjeder), og til hvilke konsekvenser dette gir (konsekvenskjeder), gitt både systemets proaktive og reaktive barrierer. Dette kan illustreres i et **sløyfediagram** (se Figur 3.3).



Figur 3.3 Sløyfediagram (basert på Rausand og Utne, 2009:82).

En **grovanalyse**, eller også kalt en innledende fareanalyse, er en kvalitativ analysemetode, gjerne utført i arbeidsgrupper, med relativt kort tidshorisont, i den hensikt å etablere et overordnet risikobilde. En grovanalyse kan brukes til å prioritere hendelser som det er viktig å studere i mer detalj med en grundigere analyse og eventuelt andre metoder i tillegg.

Risiko- og sårbarhetsanalyse (ROS) er en mer detaljert grovanalyse som ble tatt i bruk i Norge utover 1990-tallet av kommuner, fylker, eiere av infrastrukturer. Rausand og Utne (2009:276) beskriver ROS-analysemetode for objekt- og informasjonssikkerhet (security) som ble utviklet gjennom et samarbeid mellom NSM og Norges teknisk-naturvitenskapelige universitet (NTNU).[29] DSB har nylig publisert oppdaterte veiledere både for kommunale ROS-analyser[30] og fylkeskommunale ROS-analyser[31]. Disse presenteres nærmere i Kapittel 7.2.

Feiltreanalyse brukes for å kartlegge sammenhengen mellom en uønsket hendelse, årsakene til hendelsen, sannsynligheter for hendelsen og hvor effektive barrierene er for å beskytte mot hendelsen eller minske konsekvensene. Både Aven m.fl. (2008:93) og Rausand og Utne (2009:171) beskriver metoden og gir eksempler på bruk av feiltrediagram.

Hendelsestreanalyse brukes for å analysere konsekvenser etter en gitt hendelse ved å analysere ulike hendelseskjeder og barrierer i systemet, dvs spesielt den høyre delen av sløyfediagrammet.

[29] NSM (2006) *Veiledning i risiko- og sårbarhetsanalyse*. Oslo, Nasjonal sikkerhetsmyndighet. Denne veilederen er trukket tilbake, og det kommer en ny veileder fra NSM i sikringsrisikoanalyse i 2015 basert på NS 5832:2014.
[30] DSB (2014a). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, Tønsberg, 2014.
[31] DSB (2014b). *Veileder for FylkesROS*, Tønsberg, 2014.

Dette vil bidra til å kartlegge mulighetsrommet for konsekvensene av en hendelse og om barrierene i tilstrekkelig grad bidrar til å minske konsekvensene.

3.6 Definisjoner

Når man skal beskrive noe med ord, er det viktig å vite hva ordene betyr. Ord kan forstås annerledes i dagligtale enn i en spesialisert sammenheng, og heller ikke blant spesialister er det alltid enighet om betydningen. Det kan også være slik at betydning kan forandres ved oversetting fra ett språk til et annet.

På engelsk brukes betegnelsene "security" og "safety". Begge blir gjerne oversatt til norsk med "sikkerhet", og det kan være forvirrende. Det som imidlertid menes her med security er beskyttelse mot tilsiktede uønskede handlinger, altså sabotasje, spionasje, terrorhandlinger, kriminelle handlinger som tyveri (også datatyveri), mens "safety" er sikkerhet mot utilsiktede uønskede hendelser som for eksempel naturkatastrofer, svikt og for eksempel pandemier[32]. NS 5830 foreslår å bruke "sikkerhet" om "security", og definerer ikke begrepet trygghet, siden den standarden bare omfatter tilsiktede uønskede handlinger. NOU (2006:6) "Når sikkerheten er viktigst" har en ganske omfattende drøfting av språkbruken på dette punktet, og har også konsultert språkprofessor Finn-Erik Vinje. NOU (2006:6) skriver at: "Enkelte store norske konserner har stipulert norske ord for safety og security til eget bruk. Safety er satt til "sikkerhet", mens security er satt til "sikring". Imidlertid foreslår Vinje at man bør bruke "trygghet" om "safety", og "sikring" om "security". Videre foreslår Vinje å bruke "sikkerhet" som et overordnet begrep (hypernym). FFI har observert at de engelske begrepene "security" og "safety" brukes i de relevante fagmiljøene for å unngå misforståelser, også når resten av diskusjonen er på norsk.

I denne rapporten velger vi å bruke et sett med norsk-engelske oversettelser som gitt i *Tabell 3.3*.

DHS Risk Lexicon (2010) er et dokument som gir detaljerte definisjoner av mange begreper, og er spesielt nyttig for å forstå betydningen av begreper på engelsk. Det fører for langt å skulle gå gjennom dette i detalj, men noen interessante begreper kan nevnes (se Tabell 3.4.). Det foreliggende dokumentet er andre utgave, og planen er at det jevnlig skal oppdateres.

[32] For mer informasjon om uønskede hendelser se Meyer S. (2008). *Typologi over uønskede hendelser*. FFI-rapport 2009 /00447. Sist besøkt 18.12.2014. http://www.ffi.no/no/Rapporter/09-00447.pdf

Norsk	Engelsk	Referanse
Evne	Capability	DHS Risk Lexicon (2010)
Fare	Hazard	SN-ISO Guide 73:2009
Feiltreanalyse	Fault Tree Analysis (FTA)	NS-ISO/ IEC 31010:2009
Grovanalyse	Preliminary Hazard Analysis (PHA)	NS-ISO/ IEC 31010:2009
Hendelsestreanalyse	Event Tree Analysis (ETA)	NS-ISO/ IEC 31010:2009
Konsekvens	Consequence	SN-ISO Guide 73:2009
Mulighet	Likelihood	SN-ISO Guide 73:2009
Risiko	Risk	SN-ISO Guide 73:2009
Risiko- og sårbarhetsanalyse (ROS)	Risk and vulnerability assessment (RVA)	Aven, 2007
Risikoakseptkriterier	Risk acceptance criteria	DHS Risk Lexicon (2010), NATO CSE ITSG-04
Risikoanalyse	Risk analysis	SN-ISO Guide 73:2009
Risikohåndtering	Risk treatment	SN-ISO Guide 73:2009
Risikokriterier	Risk criteria	SN-ISO Guide 73:2009
Risikonivå	Level of risk	SN-ISO Guide 73:2009
Risikostyring	Risk management	SN-ISO Guide 73:2009
Risikovurdering	Risk assessment	SN-ISO Guide 73:2009, Aven m.fl. (2008)
Sannsynlighet	Probability/Likelihood	SN-ISO Guide 73:2009, inkludert fotnote
Sløyfe-analyse	Bow-tie-analysis	Rausand og Utne 2009
Sårbarhet	Vulnerability	DHS Risk Lexicon (2010)
Trussel	Threat	DHS Risk Lexicon (2010)
Verdi	Asset	DHS Risk Lexicon (2010)

Tabell 3.3 Norsk-engelske oversettelser og definisjoner av sentrale begreper.

Norsk begrep	Engelsk begrep	Forklaring
Tilpasningsdyktig risiko	Adaptive risk	Dette er en risikokategori som inkluderer trusler forårsaket av personer som tilpasser seg sikringstiltak som settes inn.
Sosial forsterkning av risiko	Social amplification of risk	Offentlighetens forsterkning/forvrengning av alvorligheten av en risiko forårsaket av bekymringer for en trussel eller aktivitet som ellers er ubetydelig.
Subjektiv sannsynlighet (kunnskapsbasert sannsynlighet)	Subjective probability	En personlig vurdering av muligheten for at en bestemt begivenhet skal inntreffe, basert på kunnskap og tilgjengelige fakta.

Tabell 3.4 Noen nye begreper fra DHS Risk Lexicon (2010).

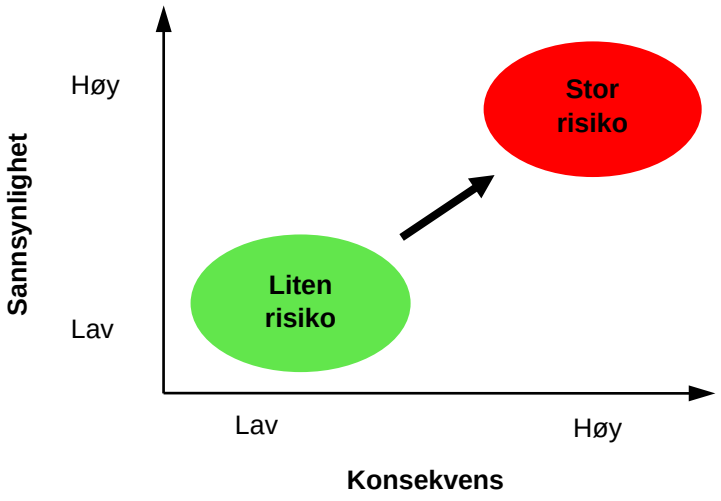
4 Forsvarsbyggs to tilnærminger til risikovurdering

Dette kapitlet går gjennom stegene i FBs operasjonalisering av NS 5814 og NS 5830/NS 5832 (kapittel 4.1 og 4.2). I kapittel 4.3 blir FBs operasjonalisering av standardene sammenlignet.

4.1 Sannsynlighet og konsekvens-tilnærmingen

ROS-analyser benyttes innenfor ulike områder i samfunnet. Tradisjonelt har slike analyser blitt brukt innen industri og normal samfunnsaktivitet i forbindelse med ulykker (safety), men benyttes nå i stor grad også for vurdering av tilsiktede uønskede handlinger (security). ROS-analysen skal normalt danne et beslutningsgrunnlag for å iverksette sikringstiltak for å redusere risikoen.

Begrepet risiko kan ha flere ulike betydninger (Kapittel 3.1). I dagligtale benyttes ofte risiko i betydningen sannsynlighet eller sjanse - "risikoen for å komme til skade", eller i betydningen konsekvens - "risikoen ved å bli truffet av lynet er at man kan omkomme". I NS 5814 defineres risiko som en funksjon av både sannsynlighet og konsekvens av en uønsket hendelse, slik det er indikert figur 4.1. Flere mener at NS 5814 ligger ganske nærme NS-ISO 31000[33], selv om begrepet risiko er definert forskjellig. NS-ISO 31000 ser på risikostyring i et mer overordnet perspektiv og i følge Røed er målet med NS-ISO 31000 "*å finne balansen med hva du ønsker å oppnå og hva du ønsker å unngå og som kan true din måloppnåelse […] dette gjelder både tilsiktede og utilsiktede hendelser*" (se vedlegg C.3).



Figur 4.1 Illustrasjon av sammenhengen mellom konsekvens, sannsynlighet og risiko.

Av definisjonen i NS 5814 følger det at hendelser som er svært lite sannsynlige og som får store konsekvenser kan vurderes å utgjøre samme risiko som en mindre alvorlig hendelse som opptrer med større forventet hyppighet. Sannsynligheten for at en hendelse skal opptre vil man forsøke å vurdere så godt det lar seg gjøre. For en rekke fysiske og teknologiske fenomener er bruken av statistiske data og frekvenser til å vurdere sannsynligheten for en hendelse mulig og meningsfullt.

[33] NS-ISO 31000 (2009). *Risk management – Principles and guidelines*.

Eksempler er radioaktivitet, lynnedslag, komponentsvikt og branntilfeller. Her finnes det tilfeldig variasjon, men lovmessighet i det lange løp.

Konsekvenser kan ofte tallfestes dersom man snakker om fysiske ødeleggelser (selv om det kan være vanskelig å gjøre det, siden det kan oppstå indirekte økonomiske tap som er vanskelige å beregne). Også for enkelte mer sammensatte fenomener som bunner i sosiale, økonomiske og teknologiske forhold vil statistikk og sannsynlighet kunne anvendes på en god måte. Eksempler kan være antall innbrudd og bilulykker i et bestemt område.

For tilsiktede uønskede handlinger vil årsakene være så sammensatte og omskiftelige at kvantitativ sannsynlighet vanligvis ikke kan benyttes. En innbyrdes rangering av ulike scenarier basert på faglige vurderinger vil likevel kunne gjøres.

Arbeidsmetoden som FB benytter i sin tilnærming kan grovt sett deles i fire ulike faser:

- Objektkartlegging/verdivurdering
- Trusselvurdering/scenariobeskrivelse
- Sårbarhetsvurdering
- Vurdering av risiko, sammenheng mellom konsekvenser (verdier) og sannsynlighet (trusler og sårbarheter) og presentasjon av risikobildet.

I tillegg utarbeides det en rekke sikringstiltak basert på risikovurderingen. Arbeidet organiseres som oftest gjennom en arbeidsgruppe bestående av tre til seks personer. Arbeidsgruppen kan trekke på ressurspersoner innenfor spesifikke områder. Vanligvis blir det opprettet brukergrupper. I større analyser er det naturlig at det opprettes en styringsgruppe med medlemmer fra virksomhetens ledergruppe som holdes orientert om arbeidet underveis. I tillegg kan det opprettes referansegrupper. I de følgende avsnittene beskriver vi kort fremgangsmåten for de ulike fasene. Tilnærmingen basert på NS 5814 som FB bruker, er et manuelt system og ikke et databasert program som sammenstiller variablene automatisk.

4.1.1 Objektkartlegging/verdivurdering (etablering av systembeskrivelse)

FB omtaler dette trinnet som objektkartlegging/verdivurdering. I NS 5814 omtales dette trinnet i prosessen “etablering av systembeskrivelse”. Hele objektet kartlegges; herunder oppdrag, organisasjon, beliggenhet, bygningsmasse, infrastruktur, fysisk og elektronisk sikring, samt tilhørende administrative rutiner. I denne fasen identifiseres også virksomhetens verdier som for eksempel skjermingsverdig informasjon eller kritiske objekter og hvor disse er lokalisert. Verdivurderingen må ikke forveksles med klassifisering av skjermingsverdige objekter iht. sikkerhetsloven.

4.1.2 Trusselvurdering/scenariobeskrivelse (identifikasjon av farer og uønskede hendelser)

FB kaller dette trinnet trusselvurdering/scenarioanalyse. I NS 5814 er dette trinnet “identifikasjon av farer og trusler. I en rekke sammenhenger vil det ikke være mulig å beskrive enhver tenkelig

situasjon som kan oppstå. Basert på gjeldende vurderinger fra en rekke kilder og ekspertmiljøer, slik som PST, Etterretningstjenesten, Forsvarets sikkerhetsavdeling, Næringslivets sikkerhetsråd, NSM osv, etablerer FB et helhetlig trusselbilde for analyseobjektet. Det utarbeides scenarioer som er eksempler på hva som kan skje. For tilsiktede uønskede handlinger deles scenarioene inn i fire hovedkategorier; terror, sabotasje, spionasje og annen kriminalitet. Det legges vekt på at scenarioene er *tenkelige* og *representative*. At de er representative betyr ikke at scenarioene nødvendigvis vurderes som de mest sannsynlige hendelsene, men snarere at beskrivelser, beslutninger og sikringstiltak som man kommer frem til basert på resultater fra disse eksemplene vil være relevante og dekkende for de fleste andre situasjoner som kan oppstå.

4.1.3 Sårbarhetsvurdering (analyse av årsaker og sannsynlighet)

FB omtaler dette trinnet som sårbarhetsvurdering, og dette tilsvarer "analyse av årsaker og sannsynlighet" i NS 5814. Sårbarhetsvurderingen er en beskrivelse og vurdering av i hvilken grad det er mulig for ulike trusselaktører å utføre en uønsket handling, uten å bli stanset eller påvirket. Et sentralt begrep i vurderingen er mulighet, det vil si i hvilken grad det er mulig for en trusselaktør å forsere virksomhetens sikringstiltak. Graden av mulighet varierer blant annet etter hvilken kapasitet trusselaktøren har, herunder blant annet hvilken kunnskap, ferdighet og verktøy som denne besitter eller kan få tilgang til. Effektiviteten av eksisterende sikringstiltak kan vurderes ved hjelp av et tidsregnskap.

4.1.4 Konsekvensvurdering

Konsekvensvurderingen tar for seg effekten av et angrep. Man tar her utgangspunkt i at de sikringstiltak som er til stede for å hindre at et angrep skal lykkes ikke er tilstrekkelig eller mangler. Konsekvensen av en gjennomført handling uttrykkes da som funksjon av bortfall av objektets tilknyttede verdi. Dette kan være i form av at materiell blir skadet eller ødelagt, at kritisk infrastruktur faller bort slik at andre objekter ikke kan operere som tiltenkt, eller at liv og helse rammes. For enkelte av scenarioene som behandles, vil en konsekvensvurdering være relativt enkel; f.eks. vil objektet kunne motstå en gitt bombelast, eller vil objektet bli skadet? For andre scenarioer er konsekvensen et mer flytende begrep, der kvantitative betraktninger må vike for mer kvalitative og skjønnsmessige vurderinger.

4.1.5 Vurdering av risiko

I vurderingen av risiko vurderes sammenhengen mellom identifiserte konsekvenser (verdier) og sannsynlighet (trusler og sårbarheter). Vurderingen er ikke en kvantitativ, men en kvalitativ vurdering, blant annet fordi det kan være vanskelig å anslå trusselaktørens intensjon og kapasitet.

Jo høyere verdi et objekt har, jo større konsekvens vil forringelse, ødeleggelse eller tyveri av verdien gi virksomheten. Det er altså avhengigheter mellom objektets verdier og konsekvensen som oppstår dersom de forringes, ødelegges eller tas bort. For de høyeste verdiene vil bortfall av disse kunne få relativt katastrofale konsekvenser for virksomheten. I andre tilfeller vil angrep ikke ha særlige konsekvenser, enten ved at de kan repareres relativt hurtig, eller ved at systemet er dimensjonert til å gjenopprette driften etter tilsvarende hendelser.

FB benytter et konsekvensskjema (driftsforstyrrelser /skade) som har fem nivåer rangert fra ufarlig til katastrofalt (se tabell 4.1). De ulike kriteriene for å vurdere konsekvensen beror på (a) nedetid i virksomhetens operative evne, (b) kompromittering av skjermingsverdig informasjon, (c) liv og helse og (d) økonomiske konsekvenser. Konsekvensskjemaet tilpasses den enkelte virksomhetens verdier.

For å vurdere sannsynligheten for at et scenario inntreffer, vil det derfor være nødvendig å benytte noen kriterier basert på de foregående vurderingene, spesielt de som omhandler trusselvurdering og sårbarhetsvurdering. Det er verdt å merke seg at sannsynligheten her ikke er en matematisk størrelse, men at det heller er en antagelse om en trusselaktørs mulighet til å ødelegge, ta bort eller forringe verdiene som virksomheten ønsker å beskytte. Risikoanalysen vil derfor innebære en viss grad av subjektivitet.

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

Tabell 4.1 FBs konsekvensskjema.

[1] Viktig funksjon: av betydning for drift av stasjon
[2] Vital funksjon: av betydning for samfunnet og/eller Forsvaret

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

Tabell 4.2 Tabell for kriterier og grad av sannsynlighet.

Resultatet presenteres av FB i form av en risikomatrise (på engelsk kjent som Boston square risk matrix) på formen vist i Figur 4.2. FB benytter en matrise per konsekvensklasse, og plasserer scenarioene inn i disse. Matrisens fargeinndeling er tilpasset hver virksomhet og deres risikoaksept. Matrisen kan også benyttes til å illustrere effekten av risikoreduserende tiltak. En slik matrise er én måte å visualisere resultatene på, men det finnes alternativer.

Metoden er systematisk og trinnvis. Metoden inneholder ikke noen beskrivelse av hvordan man skal utføre følsomhetsstudier eller hanskes med usikkerheter.

Sannsynlighet							
	Svært høy	5					
	Meget høy	4					
	Høy	3					
	Moderat	2					
	Lav	1					
Risiko Høy Moderat Lav			1	2	3	4	5
			Ufarlig	Farlig	Kritisk	Meget kritisk	Svært kritisk
			Konsekvens				

Figur 4.2 Risikomatrise for bestemmelse av risiko ut fra tallverdier for konsekvens og sannsynlighet.

4.2 Trefaktormodellen

FB har operasjonalisert trefaktormodellen basert på en veileder fra NSM, POD og PST (i det følgende kalt ”Veilederen”)[34] og NS 5832:2014. Trefaktormodellen inkluderer de tre parameterne verdi (V), trussel (T) og sårbarhet (S). Ut fra disse parametere finner man så et risikonivå. Sannsynlighet for at noe skal skje er altså ikke med som en eksplisitt parameter, men er implisitt med i trusselvurderingen. En vurdering av sannsynligheten for at et scenario kan inntreffe er med hensikt utelatt i denne modellen. Begrunnelsen for dette er at en fare for at scenarioer med lav sannsynlighet og stor konsekvens får for lav skåre i en risikomatrise og at sikringen mot typiske verstefallsscenarioer dermed nedprioriteres.

4.2.1 Verdivurdering

Dette er en kartlegging av virksomhetens verdier for å identifisere konsekvensene av uønskede handlinger. Veilederen gir ikke detaljerte indikasjoner på hvordan man skal sette disse verdiene. I det eksemplet på risikovurdering som FFI har benyttet i denne rapporten benytter FB konsekvenstabeller som har følgende overordnede konsekvensklasser: “liv og helse”, “informasjon”, “operativ evne” “omdømme” og “økonomi”. Spørsmålet man stiller seg er “hvor kritisk er bortfall av verdi X for de ulike konsekvensklassene?”. Slik rangeres eller kategoriseres verdiene ut ifra kritikalitet. Rangeringen skjer i henhold til en kvalitativ skala som vist i Figur 4.2.

Verdi:	*Beskrivelse:*
Svært høy	Tap eller reduksjon av verdi *har umiddelbare og svært alvorlige konsekvenser.*
Høy	Tap eller reduksjon av verdi *har store konsekvenser*
Moderat	Tap eller reduksjon av verdi *kan ha store konsekvenser*
Lav	Tap eller reduksjon av verdi *har små konsekvenser*

Figur 4.2 Skala for rangering av verdier etter kritikalitet.

4.2.2 Trusselvurdering

Truslene kan f. eks. være: terror, spionasje, sabotasje eller annen kriminalitet. Relevante faktorer å ta med her er som beskrevet i veilederen fra NSM, PST og POD (2010):

- Tilstedeværelse (Er det noen her som kan gjøre det?)
- Kapasitet (Er den som er til stede i stand til å gjøre det?)
- Intensjon (Har vedkommende vilje til å gjøre det?)
- Historie (Har det skjedd tidligere?)
- Målvalg (Er det noe som tyder på at det kan skje snart? “sannsynlighet”)

[34] NSM, PST og POD (2010). *En veiledning- Sikkerhets- og beredskapstiltak mot terrorhandlinger*. Sist besøkt 11.05.2015. https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/tiltak-mot-terrorhandlinger.pdf.
Det pågår et arbeid i NSM for å revidere denne veiledningen. En ny utgave kommer i løpet av 2015.

Veilederen skriver også at det kan være nyttig å identifisere scenarioene i et komplekst trusselbilde som ”mest sannsynlig” og ”verstefall”. I en slik identifisering ligger det faktisk en sannsynlighets- eller mulighetsvurdering.

Videre tar man hensyn til det nasjonale trusselnivået, og her benyttes det fire nivåer[35]. PST har i ettertid gått vekk fra disse trusselnivåene ettersom en trussel ofte er lokal og avgrenset i tid og rom. Dermed blir det misvisende å ha et nasjonalt trusselnivå[36].

Implisitt i det nasjonale trusselnivået ligger en vurdering av sannsynligheten for at noe skal skje. NS 5832:2014 sier at trusselvurderingene og verdivurderingene skal danne grunnlag for å utarbeide scenarioer som beskriver hvordan trusselaktører kan gå fram for å skade verdiene, og som er relevante for videre analyse.

4.2.3 Sårbarhetsvurdering

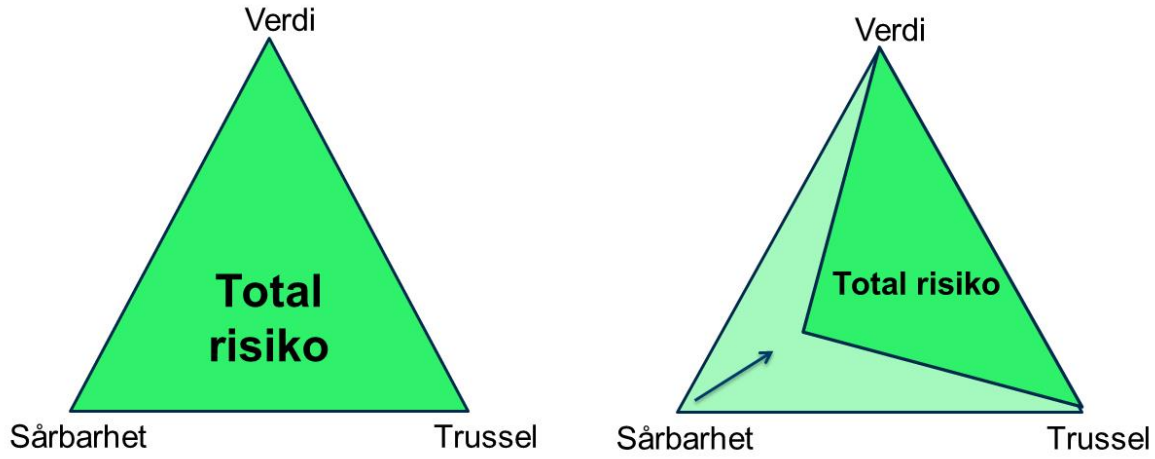
Dette er en vurdering av i hvilken grad en aktør kan utføre en uønsket handling uten å bli stanset. Det som spiller inn her er både hvilke ressurser en eventuell aktør har til rådighet, hvilke sikringstiltak som er iverksatt, eller kan iverksettes, og hvilken mulighet en trusselaktør har for å forsere virksomhetens sikringstiltak.

4.2.4 Sikringsrisikovurdering

I sikringsrisikovurderingen sammenstiller FB resultatene fra de tre foregående trinnene for hvert scenario, og basert på hvor kritisk verdiene som rammes er.

Veilederen opererer med en risikotrekant for å illustrere hvordan de tre parameterne S, V og T sammenstilles for å vise risiko. Veilederen understreker at det her dreier seg om en subjektiv og kvalitativ vurdering, og at det ofte er prosessen for å fremskaffe de nødvendige parametere som er viktigst. Dersom man kan tallfeste de enkelte parametere kunne det være mulig å lage en formel for beregning av en indeks for risiko, men det er ikke sikkert at dette vil være noe bedre enn en subjektiv kvalitativ vurdering.

[35] Nivåene som ble brukt av PST var (i) Lav, (ii) Moderat, (iii) Høy, (iv) Ekstrem.
[36] For flere begrunnelser se Fitje (2013). *Terrortrusselen og nasjonalt nivå*. Sist besøkt 18.12.2014. http://www.pst.no/blogg/trusselniva/



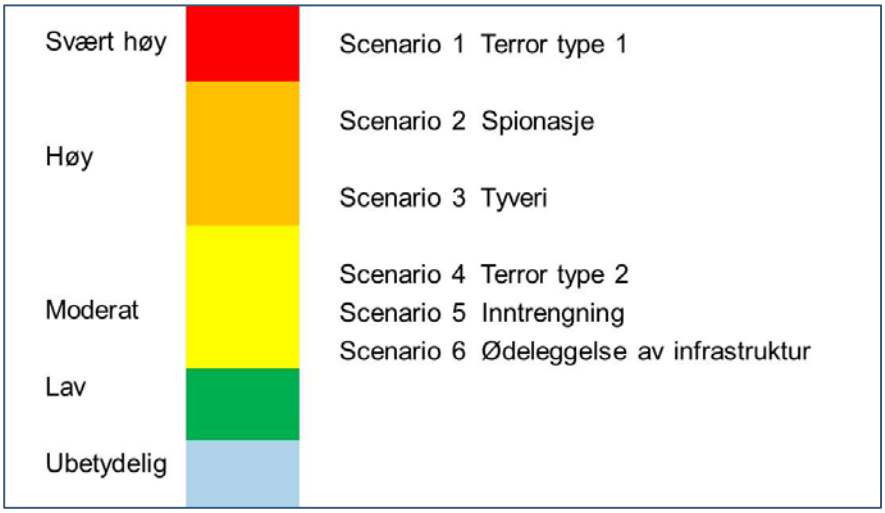
Figur 4.3 Risikotrekanten. Eksempel på visualisering av total risiko i henhold til trefaktormodellen, til venstre total risiko før tiltak er iverksatt for å redusere total risiko, til høyre total risiko etter at sårbarheten er redusert for en gitt verdi og trussel (NSM m.fl. 2010).

Et eksempel på risikovurdering basert på trefaktormodellen er FBs vurdering av et offentlig bygg. Kategorier og faktorer som er brukt i vurderingen er gjengitt i tabell 4.3.

FB har i sin tilnærming valgt å visualisere resultatet av analysen for beslutningstakerne, dvs risiko for de valgte scenarioene, i henhold til en én-dimensjonal kvalitativ skala med fargekoder. Figuren presenteres i risikoanalyserapporten sammen med en beskrivende og forklarende tekst. Figur 4.4viser et eksempel på en slik fremstilling. I NS 5832:2014 er det ikke gitt noe forslag til visualisering.

Verdier *(Fire kategorier)*	**Sårbarhet** *(Sikringstiltak)*	**Trusler** *(Scenarioer)*	**Sikringsrisiko** (*Sammenstilling av foranstående)*
Liv og helse Operativ evne Sensitiv informasjon Omdømme	Teknologisk *(sikring, "barrierer")* Organisatorisk *(Instrukser, prosessbeskrivelser, organisering, blir uønskede handlinger oppdaget)* Menneskelig *(opplæring, holdninger, forebygging)*	Inntrengning Avlytting Tyveri av informasjon Eksplosjoner (U/I) Væpnet angrep Infrastrukturødeleggelse *(kraftforsyning, vann og avløp, veiforbindelse)*	Denne beskrives kvalitativt som: Ubetydelig Lav Moderat Høy Svært høy
Vurdert etter: *Ubetydelig, Lav, Moderat, Høy, Svært høy*			

Tabell 4.3 Faktorer brukt ved vurdering av et bygg etter trefaktormodellen.



Figur 4.4 Eksempel på visualisering av resultatet av FBs risikoanalyse iht NS 5832 (Forsvarsbygg, 2013).

NS 5832 gir ingen beskrivelse av sammensetningen av arbeidsgruppen eller identifiserer konsekvensklasser. FB har valgt å gjøre dette i sin tilnærming. Den har ikke sannsynlighet som en eksplisitt parameter, og beskriver ikke usikkerhet. Resultatene blir uklart kommunisert.

4.3 Sammenligning av de to tilnærmingene

Ett av formålene med dette arbeidet er å sammenligne de to tilnærmingene til FB. FBs operasjonalisering av henholdsvis NS 5814 og NS 5832 er helt i tråd med de respektive anbefalingene i standardene. For bedre å få en oversikt er det nedenfor satt opp to tabeller som illustrerer dette. Arbeidsgangen i FBs prosess basert på NS 5814 er oppsummert i Tabell 4.4. Her blir risikoen gitt som en sammenstilling i en risikomatrise av konsekvensen av et vellykket angrep, og sannsynligheten/muligheten for at angrepet finner sted. Vurderingene som inngår i trefaktormodellen er oppsummert i tabell 4.5.

Begge tilnærmingene starter med en verdivurdering, trusselvurdering og sårbarhetsvurdering, som også inkluderer valg av et sett med relevante scenarioer. Så langt er det ingen forskjell. Forskjellen er at i tilnærmingen basert på NS 5814 foretas en separat vurdering av muligheten for at et angrep finner sted og er vellykket.

Arbeidsmetode	Første mellomtrinn	Annet mellomtrinn		Sluttresultat
Objektkartlegging/ verdivurdering	Oversikt over objektet og vurdering av verdiene	Beskrive et vellykket angrep	**Konsekvens** = mulig tap av verdi ved et vellykket angrep	Sammenstilling av konsekvens /mulighet og sannsynlighet **= risiko**
Trusselvurdering/ scenariobeskrivelse	Mulige scenarioer og angrepsmåter		**Sannsynlighet/ mulighet** for et vellykket angrep	
Sårbarhetsvurdering	Muligheten for at en angriper kan penetrere forsvarstiltakene			

Tabell 4.4 Samlet oversikt over tilnærmingen til risikoanalyse basert på FBs operasjonalisering av NS 5814:2008.

Arbeidsmetode	Delresultat	Samleresultat	Sluttresultat
Verdivurdering	Systematisk vurdering og rangering av de verdier entiteten eier eller forvalter	Verdi (V)	Sikringsrisiko som en sammenstilling av V, T og S.
Trusselvurdering	Identifisering av trusselaktører, deres intensjon og kapasitet og andre faktorer. Valg av scenarioer (trusler som kan true verdiene)	Trussel (T)	
Sårbarhetsvurdering	Vurdering av i hvilken grad eksisterende barrierer kan forhindre den uønskede handling	Sårbarhet (S)	

Tabell 4.5 Oversikt over FBs tilnærming til sikringsrisikovurdering basert på NS 5832.

I FBs operasjonalisering av trefaktormodellen foregår ikke noen separat vurdering av muligheten for at en tenkt trussel blir satt ut i livet og skal lykkes. Det er likevel ikke til å unngå at det foregår en mulighetsvurdering når aktuelle scenarioer velges og beskrives. Man vil ikke velge scenarioer som fremstår som helt usannsynlige, eller trusler som ikke er i stand til å penetrere sikringstiltakene, eller som er så vanskelige å sette ut i livet at det er usannsynlig at noen har kapasitet til å utføre angrepet. Her foregår en mulighetsvurdering både når det gjelder trussel og sårbarhet, selv om man ikke sier at man gjør det. Mulighetsvurderingen består i både hvilke scenarioer man velger å ta med og ikke, og hvilke handlingsmåter/strategier som beskrives i scenarioene. Her ligger en vurdering av sannsynlige/plausible handlemåter hos trusselaktører.

Det er derfor nærliggende å si at det egentlig ikke er noen stor forskjell på tilnærmingene. Utgangspunktet og datainnsamlingen er lik. Forskjellen ligger i måten å presentere vurderingene på. Når man presenterer risikoen i en konsekvens/sannsynlighetsmatrise, vil det være lettere å forstå. På den andre siden kan risikomatrisen gi inntrykk av mindre usikkerhet enn det er grunnlag for. I trefaktormodellen er det ikke like lett å kommunisere resultatet på en enkel måte ettersom man skal illustrere alle tre faktorer og hvordan de påvirker risikoen.

I NS 5814 er konsekvens (K) definert som følgen av en uønsket hendelse. Hvis vi bruker symbolet A for angrep (eller uønsket hendelse), kan dette uttrykkes som:

$$K = k(\text{Verdi}, \text{Sårbarhet}|A) = k(V, S|A)$$

der k er en funksjon av verdi og sårbarhet gitt at angrepet (A) finner sted. Risikoen kan uttrykkes som en funksjon av konsekvensen av et gitt angrep og muligheten for at angrepet finner sted. Symbolsk kan risikoen beskrives som sammenstilling av konsekvensen for et gitt angrep og muligheten for at angrepet finner sted:

$$R = r[k(V,S|A), p(A)]$$

Her er symbolet r en "risikofunksjon" som beskriver hvordan konsekvens og sannsynlighet for en hendelse tilsammen gir et uttrykk for risiko. Risikofunksjonen kan for eksempel være en risikomatrise. I og med at trusselen er utgangspunktet for den uønskede hendelsen (A), blir risikoen en funksjon av trussel, verdi og sårbarhet.

De samme størrelsene danner også utgangspunktet for trusselvurderingen i NS 5832. Man kunne symbolsk fremstille dette som:

$$R=f(V,T, S)$$

Også her blir (R) en funksjon av V, T og S. Men NS 5832 gir ingen anvisning på hvordan man skal komme fra disse tre størrelsene over til et utrykk for risiko, ut over å skrive at den innsamlede informasjon skal sammenstilles i en egen, selvstendig vurdering av ren risiko for hvert scenario. Her er det altså ikke noe krav om en egen konsekvensvurdering eller vurdering av muligheten for at en trussel blir satt ut i livet. Det er likevel vanskelig å tenke seg at valget av trusselscenarioer ikke inneholder en vurdering av muligheten for at en tenkt trussel skal bli satt ut i livet, og at man derfor foretar en vurdering av muligheten for at et angrep skal finne sted.

Forskjellen mellom sannsynlighet og konsekvens-tilnærmingen og trefaktormodellen blir da at i den første tilnærmingen foretas det en systematisk vurdering av konsekvensen av et angrep og muligheten for at det finner sted, som så settes sammen til en risiko, mens trefaktormodellen ikke inneholder noen anvisning på hvordan man kommer fra de tre faktorene over til risikoen. Satt opp i tabellform blir da sammenligningen som i tabell 4.6.

Sannsynlighet og konsekvens-tilnærmingen			Trefaktormodellen	
Inngangsparameter	**Delresultat**	**Resultat**	**Inngangsparameter**	**Resultat**
Verdi Trussel Sårbarhet	Konsekvens	Risiko	Verdi Trussel Sårbarhet	Sikringsrisiko
	Sannsynlighet			

Tabell 4.6 Sammenligning mellom de to tilnærmingene.

4.3.1 Utgivelse av NS 5832

NS 5832:2014 ble utgitt i november 2014 med en prøvetid på 1 år. FFI er klar over at NS 5832 er gjort så overordnet og generell som mulig i henhold til retningslinjer i Standard Norge. NS 583X-serien skal sette visse prinsipielle krav til gjennomføringen av en sikringsrisikoanalyse for å sikre en metodisk god gjennomføring. Meningen er at andre aktører skal bruke standardene som en ramme og deretter utvikle samt tilpasse tilnærmingen til sitt virksomhetsområde.[37]

I NS 5832 blir hele prosessen omtalt som sikringsrisikoanalyse, mens delen som omfatter verdivurderingen, trusselvurdering og sårbarhetsvurderingen heter sikringsrisikovurdering. Imidlertid er ikke dette gjennomført konsekvent. Begrepet "sikringsrisiko" ble ikke definert i de grunnleggende definisjonene i NS 5830, ettersom "sikring" er noe som ble lagt til begrepene senere i standardarbeidet som et kompromiss for å få ut standardene. Sikringsrisiko er definert som et "uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen", noe som fra et matematisk ståsted må bety at lav sårbarhet gir høy risiko[38].

Fra og med punkt 5.6 i NS 5832 skriver man om "ren risiko". "Sikringsrisiko" er ikke et begrep som benyttes før på slutten av NS 5832. Hvorfor man gjør det, er ikke klart. Ren risiko er et begrep for risiko som bare kan være negativ for den som utsettes for den, og er innført fordi risiko, slik den er definert i NS-ISO 73:2009, kan medføre positive konsekvenser for den som blir utsatt for en handling. Betyr bruken av "ren risiko" i stedet for "sikringsrisiko" at sikringsrisiko innebærer muligheten for handlinger som kan være positive for den som blir utsatt for dem? Her trengs en innstramming av språkbruken for å unngå unødvendige misforståelser.

[37] NSM har et pågående prosjekt "Sikkerhetstilstanden – årsaker, konsekvenser og virkemidler» (SÅKOV) for blant annet å fremskaffe et verktøy virksomheter kan bruke i anvendelse av NS 5831 og 5832. FFI bidrar inn i dette arbeidet.

[38] Forholdet mellom to størrelser er første størrelse dividert med den andre størrelsen. Se seksjon 3.1 for utfyllende kommentarer.

5 Diskusjon om standardene

"Det at modeller og standarder utvikles og endres viser at de ikke er "hugget i stein som evige sannheter", men som annet menneskeskapt også har svakheter som det over tid er behov for å utbedre eller utdype" (Rapp 2014, vedlegg C.8).

"Det som er viktigst er at vi har en felles og solid plattform for dette arbeidet slik at utviklingen går den riktige veien […] Hvis det som ligger i bunnen av konsepter og tankegods er vaklende så vil hele bygningen falle sammen." (Aven 2014, vedlegg C.1)

I dette kapitlet blir standardene NS 5832 og NS 5814 diskutert på generelt grunnlag med henvisning til sitater fra de semi-strukturerte intervjuene. Respondentene intervjuet i denne rapporten uttaler seg ikke om FBs operasjonalisering av standardene, men på bakgrunn av sin egen erfaring og kunnskap om standardene. Hovedtemaer i dette kapitlet er bruken av sannsynlighet (seksjon 5.1), endret språkdrakt i de nye standardene (seksjon 5.2), skillet mellom risikovurderinger for tilsiktede uønskede handlinger og utilsiktede uønskede hendelser (seksjon 5.3) og en gjennomgang av sannsynlighet og konsekvens-tilnærmingen og trefaktormodellen med henvisninger til de semi-strukturerte intervjuene (seksjon 5.4 og 5.5).

5.1 Sannsynlighetsvurderinger

"Sannsynlighet er ikke bare én ting. Det er i alle fall to fundamentale forskjellige ting – kunnskapsbaserte sannsynligheter som uttrykker usikkerhet og trolighet til den som gjør vurderingen – og frekvenssannsynligheter. For å kunne ha en ordentlig diskusjon må denne forståelsen være på plass." (Aven 2014, vedlegg C.1).

I NS 5814 står det at "årsaksanalysen kan ha en beskrivende (kvalitativ) del og/eller en beregningsmessig (kvantitativ) del".[39] I den kvantitative årsaksanalysen kommer en frem til frekvensen for uønskede hendelser (frekvenssannsynligheter), men hvis en bruker den kvalitative årsaksanalysen kan man bruke en skjønnsmessig vurdering av sannsynlighet. Dermed åpner NS 5814 for at sannsynlighet enten er frekvensbasert eller kunnskapsbasert.

Når FB baserer seg på NS 5814 så bruker de en kvalitativ årsaksanalyse med en kunnskapsbasert sannsynlighet. For FB er det derfor ikke en stor forskjell mellom NS 5814 eller NS 5832 når det gjelder forståelsen av sannsynlighet. Bakke-Hanssen (2014) sier at diskusjonen om bruken av sannsynlighet er en "*avsporing ettersom tilnærmingen man velger enten om det er NS 5814 eller NS 5832 består av kvalitative vurderinger hele veien og vurderinger av sannsynlighet*" (vedlegg C.6).

Selv om FB forstår sannsynlighet som kunnskapsbasert, er det andre som argumenterer med at personer som jobber med sikring oppfatter at begrepet sannsynlighet viser til en matematisk sannsynlighet, eller frekvens for forekomsten av en hendelse. *"Virkeligheten der ute er at man forstår sannsynlighet som frekvensbasert. I NS 5814 og i Sikringshåndboken står det at de tolker sannsynlighet som frekvensbasert. Det er dette folk leser, ikke artikler i vitenskapelige tidsskrifter"* (Stranden 2015, vedlegg C.9). Også Barane (2015) mener at "*NS 5814 setter*

[39] NS 5814 seksjon 4.2, fjerde avsnitt.

likhetstegn mellom sannsynlighet og frekvens (NS 5814:2008, 4.2, fjerde avsnitt)" (vedlegg C.7). Han argumenterer med at dette gjør tilnærmingen uegnet for sikring.

Jore (2014) forklarer dette med at "*Veldig mange henger fast i en naturvitenskapelig tankegang som vi i risikoanalysefaget har forlatt. Innen security-feltet har en begrenset med data og man kan ikke si noe med 100 % sannsynlighet om fremtiden. Jeg tror det er derfor vi misforstår hverandre. Jeg snakker ikke om matematisk eller statistisk sannsynlighet, jeg snakker om subjektive sannsynligheter*." (Jore 2014, vedlegg C.2).

Under intervjuene og i litteraturstudien ble det tydelig at de fleste som bruker sannsynlighet innen sikringsfaget forstår det som "muligheten for at noe skal skje", og denne oftest beskrives med ord som "liten", "middels" osv, altså en kunnskapsbasert (subjektiv) sannsynlighet. Aven (2014) hevder at " *[…] det er neppe noen som kjenner risikofaget som mener at man skal bruke frekvensbaserte sannsynligheter på security-området* […] *Det virker som mange security folk lager en stråmann for å skape et problem, men vi har aldri argumentert for frekvensbasert sannsynlighet."* (Aven 2014, vedlegg C.1).

Et annet aspekt som ble trukket frem er skillet mellom akademikere og de som arbeider med sikkerhet i praksis "*Folk flest oppfatter sannsynlighet som tall. Skal du begynne å differensiere mellom kunnskapsbasert sannsynlighet og frekvensbasert sannsynlighet så må dette igjen beskrives for folk flest, slik at de skjønner hva som ligger i det*" (Haneborg 2014, vedlegg C.4).

Det fremkom i intervjuer med medlemmer i NS 583X-arbeidsgruppen at de forstod sannsynlighet utelukkende som frekvenssannsynlighet, og at det dermed ikke kan brukes når det gjelder tilsiktede uønskede handlinger ettersom man har begrenset med data. Samtidig er det åpenhet om at en foretar en implisitt mulighetsvurdering når man velger ut sine tenkte scenarioer til bruk i analysen. "*F.eks. hvis man har en trusselaktør kan man si at den mest sannsynlige handlemåten er X, eller at i trusselvurderingen så er det mer sannsynlig at denne aktøren angriper deg enn en annen*" (Barane, vedlegg C.7). I dette ligger det en faktisk sannsynlighetsvurdering. Også når det gjelder den videre tenkte utviklingen av et scenario kan det være at man anser enkelte utviklinger som så usannsynlige at man velger å ikke følge dem videre. "*Man driver med en form for sannsynlighetsvurderinger om man vil eller ei, det kommer man ikke unna*." (Aven 2014, vedlegg C.1). Det kan derfor være grunnlag for å hevde at også de som sier at de ikke bruker sannsynlighet i sine vurderinger faktisk likevel gjør det.

Kujawski og Miller (2007) argumenterer for at man ikke skal vurdere sannsynlighet for at et angrep skal skje, men se på sannsynlighet for at et angrep kan være vellykket. Årsaken er at det er umulig å si noe om sannsynligheten for et angrep. Dette er den samme tankegangen som ligger til grunn for NS 5832 og samsvarer med Baranes perspektiv om at *"i NS 5830 så bruker man ikke sannsynlighet som en egen parameter når man vurderer risiko. Det er sannsynligheten for at du blir utsatt for en uønsket handling slik som det fremstilles i ROS-metodikk som vi er uenig i. Det er den sannsynlighetsvurderingen vi mener det er vanskelig for sikkerhetsfolk å forholde seg til, og til dels irrelevant"* (Barane 2015, vedlegg C.7).

Noe av misforståelsen kan skyldes at kunnskapsbasert sannsynlighet kan uttrykkes som "en gang hvert 10. år til hvert 100. år" (Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen). I listen over ord og uttrykk i samme veiledning er sannsynlighet definert som "Grad av tro på at en hendelse vil inntreffe". Hvis en ender opp med tall så er organisasjonene som utfører analysen " […] *bevisst over hva som ligger i tallene og hva slags usikkerhet og nyanser som er forbundet med dette, men do'erne trenger ikke nødvendigvis å fange opp dette*." (Haneborg 2014, vedlegg C.4).

Flere henviser til at det engelske språket er rikere enn vårt *" […] Sannsynlighet dekker både "probability" (matematisk sannsynlighet jfr. gambling) og "likelihood" (muligheten, troligheten og sjansen for). Hvis vi hadde hatt norske ord for disse to engelske begrepene så tror jeg mye kunne vært løst*" (Haneborg 2014, vedlegg C.4).

FFI foreslår at for å unngå misforståelser må man definere hva slags sannsynlighet man sikter til, om det er "kunnskapsbasert sannsynlighet/trolighet/mulighet" eller "frekvensbasert sannsynlighet". I de aller fleste veiledere og den vitenskapelige litteratur FFI har analysert anbefales det å bruke en kunnskapsbasert sannsynlighet heller enn en frekvensbasert sannsynlighet for å vurdere sannsynlighet for en tilsiktet uønsket handling.

5.1.1 Sannsynlighetsvurderinger steg-for-steg i NS 5832 og NS 5814

"Det er for øvrig mange likheter mellom 5830 og 5814 når man leser de. Begge ønsker å finne risikoen og usikkerhet rundt fremtidige hendelser. Organiseringen rundt utførelsen av en risikoanalyse er ganske sammenfallende. Det er likevel noen prinsipielle forskjeller som jeg mener blir bedre ivaretatt i NS 5830 når det gjelder tilsiktede uønskede handlinger […]" (Barane 2015, vedlegg C.7)

Ved nærmere analyse har vi funnet at trinnene i NS 5832 og NS 5814 er rimelig like. Begge starter med en systembeskrivelse for å identifisere hvilke verdier som kan trenge beskyttelse. Begge kartlegger trussel og sårbarhet. Men mens trefaktormodellen holder disse adskilt, blir de slått sammen til ett risikobilde i NS 5814. Så langt er standardene i praksis like.

Forskjellen ligger i risikobeskrivelsen. I NS 5814 skal man angi en separat "sannsynlighet for en uønsket hendelse" (punkt 2.5), eller "konsekvens og den tilhørende sannsynlighet" (punkt 4.4). Det er litt diskrepans mellom punkt 2.5 og punkt 4.4 i NS 5814. Det ene punktet sier "sannsynligheten for en uønsket hendelse", og det andre sier "sannsynligheten som hører til en konsekvens". Det kan oppfattes som en angivelse av sannsynligheten (eller muligheten) for at konsekvensen skal inntreffe. NS 5814 definerer sannsynlighet som grad av trolighet for at en hendelse vil kunne inntreffe, og at sannsynlighet kan uttrykkes med ord eller en tallverdi. Det er altså ikke noe krav om å bruke et numerisk uttrykk for sannsynlighet.

I NS 5814 angis risikoen med to dimensjoner, sannsynlighet og konsekvens, og det er lettfattelig for en bruker. Ofte visualiseres risiko i en risikomatrise. Men det kan altså være litt uklart hva det er sannsynligheten for. I trefaktormodellen etter NS 583X ender man opp med tre parametere, og det er vanskeligere å sammenfatte dem på en enkel og forståelig måte. Der inngår ikke

sannsynlighet som en separat parameter. Men det blir litt feil å si at sannsynligheten ikke inngår. Hvis man ser på arbeidsgangen ved risikovurderingen, slik FFI ville gjort det, blir den som følger:

1. Det er bare trusler man har fantasi til å tenke seg som blir tatt med. Det man ikke klarer å tenke seg er **usannsynlig.** Her ligger det en første sannsynlighetsvurdering.
2. Når man ser på de forskjellige scenarioene, sammenstillingen av trussel og verdi, vil man kanskje komme fram til at noen scenarioer er lite aktuelle. Noen hendelser er rett og slett **mindre sannsynlige,** og tas ikke med videre. Her er sannsynlighetsvurdering nr. 2.
3. Når konsekvensen utredes kan man kanskje finne at verdien likevel ikke er sårbar for det scenarioet som slapp gjennom siling nr. 2. Her får man sannsynlighetsvurdering nr. 3.

Dette innebærer at i trefaktormodellen er det faktisk en tretrinns vurdering som innebærer en kunnskapsbasert sannsynlighetvurdering, selv om den ikke eksplisitt kalles det. Dette betyr at trinnene fram til der man skal angi risikoen er nesten like, det er presentasjonen av risiko som er forskjellig.

I trusselvurderingen i trefaktormodellen inngikk tidligere også det nasjonale trusselnivået, men PST har nå gått bort fra dette. En annen sak er at sannsynligheten for at noe skal skje, er svært usikker når det gjelder noe som sjelden skjer. Og når da i tillegg PST, som er en hovedleverandør av slike sannsynligheter, sier at den er usikker er det kanskje like greit å se bort fra den. I tillegg er trusselbildet en dynamisk parameter, som stadig forandres. En mulighet er å bruke sannsynligheten for at noe skal skje som en binær parameter, og sette den til enten null eller én, og så forsøke å anslå sannsynligheten for at angrepet skal være vellykket, helt i tråd med NS 5832.

Flere hevder at sannsynlighetsbegrepet (kunnskapsbasert sannsynlighet) er nødvendig "*For å kunne få et risikobilde som kan sammenlignes med de andre risikobildene […]"* (Røed 2014, vedlegg C.3). Ett annet poeng er at "*Uten bruk av sannsynlighet som en tidsangivelse, blir risikovurderingen et øyeblikksbilde*" (Midtgaard 2014, vedlegg C.5). Andre mener at sannsynlighet er ett av redskapene for å kunne si noe om usikkerhet; "*De tre dimensjonene verdi, trussel og sårbarhet er helt konsistent med tankemåten vår – der usikkerhet beskrives med redskaper som kapasitet, intensjon, sannsynlighet og kunnskapsstyrke, uten at vi da snakker om frekvenssannsynligheter*." (Aven 2014, vedlegg C.1).

FFI mener at en kunnskapsbasert sannsynlighetsvurdering er nødvendig og uunngåelig i risikovurderinger for tilsiktede uønskede handlinger. I tillegg må usikkerheten klart kommuniseres.

5.2 Språkdrakt: Helhetlig risikostyring

Innen fagmiljøene i Norge later det til å herske en viss uenighet med tanke på forskjeller mellom trygghet og sikring. Spesielt ser det ut til å være store utfordringer i NS 5832 med tanke på definisjoner og prosess-steg som er forskjellig fra NS 5814 og som kan skape forvirring for praktikerne. *"I NS 583X-serien har man villet være tro mot ordbokdefinisjonene av de to*

begrepene [analyse og vurdering], og det ble også hentet inn en vurdering fra Språkrådet. Analyse er brukt der hvor det er snakk om en prosess der man "bryter informasjon ned til sine enkelte bestanddeler og setter dem sammen igjen for å avdekke en mening", mens vurdering er brukt der man beskriver "hva dette egentlig betyr for oss". Språkrådet støttet denne bruken" (Barane 2015, vedlegg C.7).

Aven argumenterer for at "*Det er høyst unødvendig at en skal skape en språkdrakt som er inkonsistent med allmenn terminologi i Europa om hva som er en risikoanalyse og en risikovurdering*." (Aven 2014, vedlegg C.1).

FFI støtter Aven sitt syn. Det trengs en avklaring når det gjelder språkbruk og ordforståelse. FFI mener at NS 583X-serien burde definert "analyse" og "vurdering" i henhold til ISO 31000 og SN-ISO Guide 73:2009. Forskjellig ordbruk kan skape forvirring for brukerne, samt at det blir en utfordring å etablere enhetlige norsk-engelske oversettelser til bruk i ulike standarder, internasjonalt samarbeid og i vitenskapelig litteratur (se *Tabell 3.3*).

5.3 Skillet mellom risikovurderinger for tilsiktede og utilsiktede hendelser

Det er ingen tvil om at den store forskjellen mellom utilsiktede hendelser (naturhendelser og ulykker) og tilsiktede uønskede handlinger ligger i forutsigbarheten av den utløsende hendelsen. Når den utløsende hendelsen først har inntruffet, vil verktøyet for å finne konsekvensene i hovedsak være det samme. For ulykker kan det ofte være mulig å finne data for hvor ofte en utløsende hendelse forekommer, som f. eks. når det gjelder hendelser relatert til været. Dette kan til en viss grad gjøre det mulig å beregne risiko. Samtidig har vi sett at usikkerhetene også her kan være store, f. eks. når det kommer en 100-års flom med to års mellomrom. Det er derfor risikabelt å stole for mye på statistikk. Den folkelige forståelsen av statistikken ville her være at når det har vært én 100-års flom vil det gå 100 år til den neste.

Når det gjelder tilsiktede uønskede handlinger blir usikkerheten enda større. Her står det et beregnende individ med onde hensikter bak, en hjerne som kan skaffe seg informasjon om sikringstiltak og kan planlegge hvordan gjøre størst mulig skade. Historiske data er derfor mangelvare, og trenger heller ikke være så veldig relevante. Selv om de finnes, er usikkerheten svært stor, slik regneeksemplene i kapittel 3.2.1 viser. Dette samsvarer med synet til Aven og Renn (2009) som maner til forsiktighet når det gjelder å stole på tall fra kvantitative analyser når dataene er mangelfulle. I forbindelse med tilsiktede handlinger kan det derfor ikke bare være feil å bruke matematisk sannsynlighet, det kan være direkte skadelig ved å introdusere falsk trygghet.

Statistikkeksemplene i seksjon 3.2.1 viser at selv der man tilsynelatende har en datamengde som er stor nok til at det går an å beregne sannsynligheter, kan det være at den sannsynligheten man kommer fram til er så usikker at man like gjerne kunne foretatt en kvalitativ vurdering basert på den kunnskap og de data som er tilgjengelig.

5.4 Vurdering av "sannsynlighet og konsekvens-tilnærmingen"

Sannsynlighet og konsekvens-tilnærmingen (NS 5814) er i all hovedsak en enkel metode å bruke. Den er oversiktlig bygget opp og beskriver stegene i analysen i detalj. Denne styrken kan riktignok også sees på som en svakhet ved metoden. Ved å forenkle stegene i for stor grad står man i fare for å miste kritiske elementer i analysen, eller at disse elementene nedtones. Det er derfor svært viktig at brukere av metoden er godt kjent med bakgrunnen for metoden, og ikke kun benytter den som en enkel mal for risikovurderinger.

I likhet med at metoden er enkel å bruke, er presentasjonen av resultatet, risikoen, enkel. Bruken av en to-dimensjonal risikomatrise, gjerne fargelagt, med sannsynlighet langs den ene aksen og konsekvens langs den andre, gir et visuelt enkelt uttrykk for resultatene av vurderingen. Matrisen gjør det enkelt å kommunisere den overordnede risikoen, og kan på en enkel måte også illustrere effekten av risikoreduserende sikringstiltak. Jore (2014) trekker frem at NS 5814 er "*(i) enkel å forstå og (ii) den kommuniserer klart prioriteringer som gjør det enklere for lederen å ta beslutninger*" (Jore 2014, vedlegg C.2). På den andre siden kan en argumentere at plotting av scenarioer inn i risikomatrisen gjør at risikoanalytikeren tar avgjørelsene gjennom fargekoding og ikke lederen.

Andre ulemper ved risikomatrisen er at (i) det gir et inntrykk av at vurderingene er mer presise enn de egentlig er, (ii) noen kan oppfatte matrisen som den egentlige risikovurderingen, (iii) usikkerheten kommuniseres ikke tydelig, og da usikkerhet er et sentralt begrep er dette uheldig, og (iv) risikomatrisen forenkler virkeligheten. Med usikkerheten menes usikkerheten i fastsettelsen av sannsynlighet og til en viss grad konsekvens (en hendelse kan ha flere forskjellige konsekvenser). Uansett hvilken definisjon av sannsynlighet som legges til grunn, vil det være store usikkerheter knyttet til nivåfastsettelsen. Ved å tillegge risikoen en fast verdi eller nivå for å plassere den i matrisen overses det faktum at risiko kan være høyst flytende.

Grunnlaget for matrisen skal være en grundig og metodisk gjennomgang av verdier, sårbarheter, konsekvenser og sannsynligheter som kan stå i fare for å komme i bakgrunnen. Matrisen blir i altfor mange sammenhenger oppfattet som det avgjørende resultatet av analysen, mens den egentlig kun er oppsummering av langt viktigere resultater som sårbarhetsvurderingen og konsekvensvurderingen.

Forenklingen som risikomatrisen representerer kan skyldes bruken av sannsynlighet i risikomatrisen. Som det har blitt påpekt tidligere, eksisterer det flere sannsynlighetsbegreper. I mange tilfeller oppfattes sannsynlighet som en matematisk sannsynlighet, altså noe som kan tallfestes. En slik sannsynlighet har liten verdi innenfor sikring. Når det så presenteres nivåer for sannsynlighet i risikomatrisen, kan det oppfattes som om man likevel kan tallfeste denne sannsynligheten, mens det i virkeligheten er snakk om en kvalitativ kunnskapsbasert vurdering. Dersom dette tydeliggjøres i vurderingen, og risikomatrisen forklares og kun brukes som et visualiseringsverktøy, burde ikke dette utgjøre noe stort problem.

Ett annet aspekt som Jore (2014) trekker frem er: "*Siden sannsynlighet er en viktig dimensjon i risikomatrisen, kan man komme til å nedprioritere security-risikoer i forhold til andre risikoer*." (Jore 2014, vedlegg C.2). Dette fordi en hendelse som antas å inntreffe sjelden lett oppfattes å representere en ubetydelig risiko, selv om konsekvensene skulle være store dersom den inntreffer.

Jore (2014) hevder at NS 5814 " *[…] 'tvinger' folk til å sette risikoen i ulike kategorier og den utrykker heller ikke usikkerhetsmomentet*" (Jore 2014, vedlegg C.2).

Videre er det viktig at risikoanalytikeren presenterer risikomatrisen som et verktøy og ikke en løsning. Hensikten med analysen er å gi et beslutningsgrunnlag for gjennomføring av sikringstiltak. Risikomatrisen er ett, av flere, verktøy i vurderingen av sikringstiltak.

FFI anbefaler at beslutningstaker må sette seg inn i hele risikovurderingen inkludert forutsetninger, antakelser, vurderinger og usikkerheter, og ikke bare nøye seg med å se på risikomatrisen. FFI anbefaler at FB legger mer vekt på å kommunisere usikkerhet i de ulike vurderingene.

5.5 Vurdering av "trefaktormodellen"

> *"Jeg opplever at det har blitt harde fronter, nesten som en religionskamp, og jeg opplever at mange har tatt et standpunkt uten egentlig å forstå forskjellen"* (Stranden 2015, vedlegg C.9)

Rapp (2014) argumenterer at "*Det er enkelte som hevder at trefaktormodellen er ny og ukjent, men det kommer an på hvor du har vært de siste 20 årene. Der jeg har vært (security-miljøet i ulike deler av forsvarssektoren) har trefaktormodellen vært 'best practice' og det har heller ikke vært særlig omstridt i de miljøene*" (Rapp 2014, vedlegg C.8). FFI har fått tilgang til metodedokumenter fra bl.a. FSA og FB der sannsynlighet og konsekvens blir brukt. Dermed er trefaktormodellen nødvendigvis ikke så utbredt i forsvarssektoren som det kan virke basert på sitatet til Rapp.

Mye av kritikken mot NS 5832 er at resultatet ikke kan presenteres sammen med resultater innen safety for å gi et helhetlig risikobilde for beslutningstakerne. Barane mener at det er en oppkonstruert problemstilling at en ikke kan sette ulike typer risiko sammen til et helhetlig risikobilde selv om det er brukt forskjellig metodikk: *"Det er litt som analogien om at hvis en skal bygge et hus trenger en flere typer verktøy. Det er enklere å gjøre alt med samme tilnærming, men hvis én type metodikk ikke passer alle typer risiko, da mister man flere viktige nyanser og helheten, eller huset om du vil, blir deretter"* (Barane 2015, vedlegg C.7).

Jore (2014) mener at "*Trefaktormodellen er i seg selv ikke 'revolusjonerende'; det er de samme stegene, med ulike begrep som overlapper med NS 5814*" (Jore 2014, vedlegg C.2). Samtidig er det flere positive trekk med trefaktormodellen som at den *"(i) får bedrifter til å prioritere hva er det de vil beskytte, (ii) fanger opp at verdien er sårbar overfor en strategisk trusselaktør. Dette er gode kvalitative dimensjoner som det er nyttig at bedrifter tar innover seg i sine risikoanalyser" (ibid).* Haneborg (2014) eksemplifiserer dette ved å si at hvis en gjør en grundig verdivurdering

"*så er det kanskje ikke hele butikken du må beskytte, det er kanskje bare deler av butikken. Da er det enklere som objekteier å prioritere hva du skal investere i av sikringstiltak slik at man kan bedre styre risikoen*" (Haneborg 2014, vedlegg C.4). Andre trekker frem det økte fokuset på sårbarhet som en styrke "*[…] jeg er vant til å tenke at sårbarhetsvurderinger er en del av risikovurderinger. Men mange i safety ser likevel på risiko uten å se på sårbarhet.*" (Røed 2014, vedlegg C.3).

De fleste vi intervjuet mente at stegene i trefaktormodellen med de tre dimensjonene er "*logisk og forståelig, men jeg skjønner ikke at dette betyr at en ikke kan si noe om sannsynlighet […] Disse tre dimensjonene blir et slags underlag for å vurdere sannsynlighet.*" (Røed 2014, vedlegg C.3).

Stranden (2015) trekker frem at *"Det som gjør 5830-serien unik er fokuset på verdivurderingen. Dette er grunnlaget for en enhver fornuftig bruk av ressurser for å sikre noe. Det må komme først! Hvis man begynner å identifisere trusler eller risikoer så ser man for bredt og en tenker ikke på relevans! Dette var grunnen til at jeg mener at vi måtte få en ny retning, vi må tenke hvilke trusler er mest relevant ovenfor mine verdier og min virksomhet."* (Stranden 2015, vedlegg C.9). *"Et annet aspekt som andre tilnærminger ikke ivaretar er etterretning som prosess og produkt for å si noe om trusselen."* (Stranden 2015, vedlegg C.9).

En svakhet er at "*det vitenskapelige grunnlaget for trefaktormodellen er mangelfullt, og denne tilnærmingen har ikke tatt innover seg forskningen innen risikoanalysefaget de siste årene."* (Jore 2014, vedlegg C.2). Samtidig som trefaktormodellen har en "*manglende begrepsdybde, hva er det egentlig som ligger i begrepene?" og at "tilnærmingen sier ingenting om usikkerhet. Det finnes mange typer usikkerhet; usikkerhet om faktagrunnlag og kunnskap eller om hvordan trusselbildet utvikler seg osv. Når en bare viser til en "trekant", så kommer ikke usikkerhetsdimensjonen frem*". Hensikten ved trefaktormodellen er at den skal bli brukt i beslutningssammenheng, men i følge Jore (2014) sier "*modellen ingenting om prioritering"*. Dette er problematisk ettersom "*hele poenget er at risikoanalysen skal gi beslutningsstøtte slik at man kan prioritere de mest hensiktsmessige tiltakene. I trefaktormodellen er det ingen sannsynlighetsgradering og det blir vanskeligere for beslutningstakere å prioritere hva en skal beskytte osv*." (Jore 2014, vedlegg C.2).

FFI mener at trefaktormodellen er vanskeligere å kommunisere på en like lettfattelig måte som NS 5814. Den tradisjonelle bruken av en trekant som illustrasjon er god til å kommunisere hvilke faktorer som inngår i vurderingene, men er uegnet til å kommunisere resultatet. Det er avgjørende at resultatet må dokumenteres og kommuniseres i en skriftlig rapport som grunnlag for beslutninger.

6 Vitenskapelig grunnlag

Det sier seg selv at det blir krevende å skulle studere tilnærminger til risikovurderinger vitenskapelig. Å prøve ut de forskjellige tilnærmingene til risikovurderinger eksperimentelt er vanskelig, annet enn ved å sette opp øvelser som simulerer en virkelig situasjon. Samtidig er den

virkelige situasjonen noe man enten må tenke seg, eller i beste fall bygge på allerede inntrufne hendelser. Derfor vil man i stor utstrekning bli nødt til å beskrive de forskjellige elementene med ord, og den første utfordringen blir da å definere språkbruken. Det samme ordet betyr ikke nødvendigvis det samme for forskjellige mennesker eller innen forskjellige fagmiljøer. Dette indikerer behovet for bruk av samfunnsvitenskapelige metoder sammen med metoder som brukes innen naturvitenskap.

6.1 Forskningsmetodiske utfordringer med risikovurderinger

"Social Science at its best is a creative process of insight and discovery taking place within a well-established structure of scientific inquiry" (King, Keohane and Verba 1994:12)

I samfunnsvitenskapelige fag er en godt kjent med utfordringene knyttet til vitenskapelig samfunnsforskning. På noen temaer kan en bruke eksisterende data og plotte statistikk over trender, men på tilsiktede hendelser (jfr. angrepet 22. juli 2011) har en sjelden nok informasjon eller datapunkter til å lage meningsfull statistikk. I samfunnsvitenskapelig forskning og samfunnssikkerhet er det derfor flere vitenskapelige forskningsprinsipper det er vanskelig å følge. Allikevel, forskere har tilpasset disse prinsippene til at vi på en vitenskapelig måte kan håndtere komplekse strukturer og hendelser i samfunnet. Gjennomsiktighet, sporbarhet og etterprøvbarhet er målet i følge statsviterne og metodeekspertene King, Keohane og Verba (1994)[40]. Etterprøvbarhet blir ofte omtalt som *reliabilitet* i samfunnsfaglig litteratur og dreier seg for eksempel om hvor nøyaktig en beskriver risikoanalyseprosessen i en arbeidsgruppe og i hvilken i grad prosessen kan gjentas/replikeres. Altså, hvorvidt det er mulig for andre å gjennomføre det samme forskningsopplegget og få mer eller mindre samme resultater. Dette kan for eksempel inkludere utvalgsmetoden for arbeidsgruppen og fremgangsmåten for å innhente informasjon i arbeidsgruppen. En forutsetning for god reliabilitet er åpenhet om hvordan man har kommet frem til de slutningene som har blitt trukket i en undersøkelse, det vil si hvilke data som ligger til grunn, og hvordan man har gått frem metodisk (Hellevik 2002:183)[41]. Det er viktig at en rapporterer usikkerhet ved slutninger som er tatt og datagrunnlaget for slutningene. Dette er prinsipper som burde følges i risikoanalyseprosessen.

I denne rapporten kommer det tydelig frem at forskjellige grupperinger innad i land og mellom land bruker forskjellige begreper som kan ha lik betydning, og like begreper som kan ha forskjellig betydning. Mangelen på konsistent språkbruk innen risikoanalyser er tydelig og det er derfor viktig å tenke på *begrepsvaliditet*. Lund argumenterer at god begrepsvaliditet beror på om måten en stiller spørsmål på "måler" eller "fanger opp" de relevante begrepene på en god måte (Lund 2002[42]). For eksempel, hvis en bruker et feil begrep i en risikoanalyseworkshop som gjør at ekspertene får ulike assosiasjoner så kan ekspertene ende opp med å gi oss mye informasjon om noe vi ikke nødvendigvis er interessert i. Det er viktig å stille spørsmålet "måler vi det vi tror vi måler?". Begrepsavklaringer er derfor viktig.

[40] King, G., Keohane, R. O., Verba, S. (1994). *Designing Social Inquiry*. Princeton: Princeton University Press.
[41] Hellevik, O. (2002). *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.
[42] Lund, T. (ed.) (2002). *Innføring i forskningsmetodologi*. Oslo: Unipub.

6.2 Vitenskapelige publikasjoner

Det er utfordrende å gjennomføre et litteratursøk på temaet risikovurderinger. Det er svært mange publikasjoner og dermed er det vanskelig å få en oversikt på det vitenskapelige arbeidet som er gjort innenfor feltet. Standardene (både Norsk Standard og ISO) refererer ikke til vitenskapelige artikler. Dermed er det vanskelig å identifisere hvilke artikler som er det vitenskapelige grunnlaget for standardene. Flere av de vitenskapelige publikasjonene FFI har funnet omhandler hvordan tilnærminger til risikovurderinger har blitt tilpasset en gitt kontekst eller et system.

6.2.1 Utfordringer ved risikovurderinger for tilsiktede uønskede handlinger

Dillon m.fl.[43] (2009:322) argumenterer at etter terrorangrepene i USA 11. september 2001 så har utviklingen og forskningen på risikovurderinger på tilsiktede uønskede handlinger (med fokus på terror) vært omfattende. Allikevel er det flere utfordringer som gjenstår, blant annet (i) risiko knyttet til tilsiktede uønskede handlinger er dynamisk ved at trusselaktører kan lett endre intensjon og målvalg og at virksomhetseiere kan iverksette sikkerhetstiltak. Det kan være vanskelig å fange oppe hvordan endringer kan påvirke risikoen. Enda vanskeligere blir det å kvantifisere, regne ut kost/nytte for tiltak som er iverksatt (Dillon m.fl.2009:322). (ii) Det er ikke nok ressurser for å kunne eliminere alle typer risiko eller for å møte kravene som blir stilt av myndighetene i dag. Forfatterne henviser til situasjonen i USA, men det samme kan sies å være tilfellet i Norge. (iii) Det er et stort antall mulige angrepsscenarioer og nivåer av sikring av verdier som gjør det vanskelig å beregne effekten av sikringstiltak og sikringsbarrierer. (iv) Som nevnt tidligere er dataomfanget på tilsiktede uønskede handlinger begrenset og det er enorme usikkerheter knyttet til vurdering av trusler, sårbarheter og konsekvenser. (v) Risiko er til slutt en subjektiv vurdering ettersom en må ta stilling til "hva er akseptabel risiko? Hva slags risikoreduserende tiltak er godt nok?" Dillon poengterer at selv om de fleste forskere er enig om at terrorismerisiko er en funksjon av trussel, sårbarhet og konsekvens, er det en rekke konkurrerende teorier for hvordan disse komponentene skal vurderes (Dillon m.fl. 2009:322).

I tillegg påpeker Jore og Moen (2015) flere utfordringer for virksomheter som skal utføre risikovurderinger som ledd i en risikostyringsprosess.[44] En viktig utfordring for virksomheter er å inkludere et relevant utvalg av scenarioer for mulige tilsiktede uønskede handlinger. Valg av scenarioer baseres ofte på "siste hendelser" og det gjeldende sikkerhetslandskapet. Denne utfordringen gjenstår også etter at den nye standardserien er utgitt. Videre, er det utfordrende å vurdere hva som er et passelig sikringsnivå, referansepunkter eksisterer ikke og er vanskelig å etablere fordi informasjon om begrunnelse og valg av sikringsnivåer i ulike virksomheter er som regel sensitiv og sikkerhetsgradert informasjon.

[43] Dillon, R.L., Liebe, R.M., Bestafka, T. (2009). "Risk-Based Decision Making for Terrorism Applications", *Risk Analysis* **29**(3) (2009) 321 – 335.

[44] Jore, S., Moen, A. (2015). "A discussion of the risk-management and the rule-compliance regulation regimes in a security context", in *Safety and Reliability: Methodology and Applications*, Nowakowski m.fl. (Eds), Tayler & Francis Group, London, ISBN 978-1-138-02681-0, 677 – 684.

6.2.2 Betydningen av bakgrunnskunnskap og rollen til usikkerhet

Aven og Renn [45]drøfter bruken av kvantitativ risikoanalyse (Eng: Quantitative Risk Analysis (QRA)) i forbindelse med terrorhandlinger. QRA er en mye brukt tilnærming for å vurdere risiko i industriell sammenheng. Forfatterne mener at QRA også har en rolle å spille i forbindelse med risikovurderinger, men maner samtidig til forsiktighet når det gjelder å stole for mye på tallene som kommer fram, og huske på at i denne forbindelsen er dataene mangelfulle. Dette kan i noen grad støtte bruken av NS 5814, men drøftingen i artikkelen understreker den rolle usikkerheten spiller, og betydningen av bakgrunnskunnskap. Viktigheten av å beskrive bakgrunnskunnskapen blir understreket, og usikkerhet betegnes som hovedkomponenten i risikoen. De skriver videre at dersom man prøver å (be)vise at det er rasjonelt å basere risikoaksept på forventningsverdier vil man få en for innskrenket forståelse av problemstillingen.

6.2.3 Betinget sannsynlighet – sannsynligheten for et vellykket angrep

Kujawski og Miller [46] skriver at mens ulykker og naturkatastrofer opptrer som stokastiske hendelser og kan bli evaluert med statistiske metoder og eksisterende databaser, er tilsiktede uønskede handlinger begått av aktører som er både "ondsinnede" (malicious) og "kalkulerende" (subtle), og nye skademetoder blir stadig utviklet. Statistiske metoder er derfor lite anvendelige. I stedet må man prøve å tenke som en trusselaktør. Dette er viktig å huske når man skal evaluere metoder for risikoanalyser i sikringsøyemed. Kujawski og Miller foreslår en alternativ sannsynlighetsberegning, basert på en betinget sannsynlighet for at et terrorangrep skal være vellykket, gitt at det settes i gang. Man lager altså et scenario som man antar vil skje, og ser på sannsynligheten for at det skal være vellykket, sett fra angriperens side. Dette støtter bruken av NS 5830, hvor man ser bort fra sannsynligheten for at et angrep skal finne sted, og i stedet ser på følgene av et angrep.

6.2.4 Vitenskapelig grunnlag for sannsynlighet og konsekvens-tilnærmingen

To fremtredende norske sikkerhetsfaglige akademiske miljøer er Universitet i Stavanger (UiS) og NTNU. Begge institusjoner har i en rekke år forsket og undervist i sikkerhetsfag og bidratt til å bringe fagfeltet videre både i Norge og internasjonalt.

Avens monografi om risikostyring (Aven, 2007) og monografien om risikoanalyse av Aven, Røed og Wiencke (Aven m.fl., 2008) er vitenskapelige og forskningsbasert. Det er gitt omfattende henvisninger til vitenskapelig litteratur. Det samme gjelder boken av Rausand og Utne (2009)[47]. Utgivelsen av denne boken er direkte inspirert av utgivelsen av den nye versjonen av standarden NS 5814 i 2008. Forløperen til denne boken het "Riskoanalyse – En veiledning til NS 5814" og ble utgitt i 1991 (Rausand, 1991)[48]. Standarden NS 5814 er i tråd med metoder, tilnærminger,

[45] Aven T., Renn, O. (2010). "The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk". *Risk Analysis*, **29** (4) (2009) .
[46] Kujawski, E., Miller G. A. (2007). "Quantitative Risk-Based Analysis for Military Counterterrorism Systems". *Systems Engineering*, **10** (4) (2007) 273 – 289.
[47] Rausund, M., Utne, I. B. (2009). *Risikoanalyse – teori og metoder*. Trondheim. Tapir Akademisk Forlag,
[48] Rausand, M. (1991). *Risikoanalyse; Veiledning til NS 5814*. Trondheim, Tapir Akademisk Forlag.

begrepsdefinisjoner i disse monografiene. FBs operasjonalisering av standarden er i tråd med det som beskrives som en grovanalyse og en ROS-analyse i disse bøkene (se Kapittel 3.5 som kort beskriver disse metodene).

Forskningsprosjektet Risk and Decisions Systems for Critical Infrastructures (DECRIS) er et eksempel på en forskningsbasert utvikling og testing av et metodisk verktøy for risikovurdering for kritisk infrastruktur (Line m.fl., 2009[49]; Utne m.fl., 2008).[50] Det tar utgangspunkt i metodiske verktøy for grovanalyse, ROS og bruk av andre mer detaljerte metoder ved behov (hendelsestrær og feiltrær). Metoden er helt i tråd med NS 5814.

6.2.5 Vitenskapelig grunnlag for trefaktormodellen

I følge medlemmer av arbeidsgruppen for NS 583X-serien (se Barane, 2014), er noe av grunnlaget for trefaktormodellen en artikkel av Giovanni Manunta[51] i tidsskriftet Security Journal. I denne vitenskapelige artikkelen innen fagfeltet kriminologi fra 1999 postulerer Manunta at sikkerhet (security (S)) kan beskrives som en funksjon av verdi (asset (A)), beskytter (protector (P)) og trussel (T), symbolisert ved S=f(A,P,T|Si) gitt en situasjon Si. For Manunta er dette en definisjon av sikkerhet som erstatter de språklige definisjonene man finner i ordbøker.

Manuntas artikkel tar også for seg bruken av sikring i forbindelse med risikostyring, men her blir det noe uklart hvordan dette skulle foregå. Det synes som Manunta mener at risikostyring utelukkende dreier seg om bruk av (numerisk) sannsynlighetsregning, mens sikkerhet i Manuntas definisjon er mer helhetlig. Manunta hevder at risikostyring er basert på et mekanistisk og deterministisk syn. Men hans artikkel omhandler altså sikring, og definerer ikke sammenhengen mellom sikring og risiko. Det kan virke som Manuntas forståelse av risikostyring er noe utdatert sammenlignet med dagens forståelse.

I en senere artikkel med tittelen "Risk and Security: Are they Compatible Concepts?" i samme tidsskrift[52] behandler Manunta risikobegrepet. For det meste handler det om risiko i forbindelse med trygghet, altså ulykker. Men han har også et avsnitt om risiko og sikkerhet (Risk and Security). Her argumenterer han for at probabilistisk behandling av sikringsrisiko ikke kan brukes på grunn av manglende data. Dette samsvarer med det rådende synet i norske fagmiljøer, selv om enkelte aktører i miljøet hevder at andre aktører bruker frekvensbasert sannsynlighet.

[49] Line, M.B., Bertelsen, D., Fridheim, H., Hokstad, P., Kjølle, G., Røstum, J., Utne, I.B., Vatn, G.Å., Vatn, J. (2009). *Metode og verktøy for samlet risikovurdering av kritiske infrastrukturer. Sluttrapport for DECRIS: Risk and Decision Systems for Critical Infrastructures*. SINTEF Rapport A11636, Trondheim, ISBN 9778-82-14-04814-8. Sist besøkt 24.11.2014.
http://www.sintef.no/globalassets/project/samrisk/decris/documents/decris-rapport.pdf

[50] Utne, I.B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I.A., Bertelsen, D., Fridheim, H., Røstum, J. (2008), *Risk and Vulnerability Analysis of Critical Infrastructures – The DECRIS Approach*.

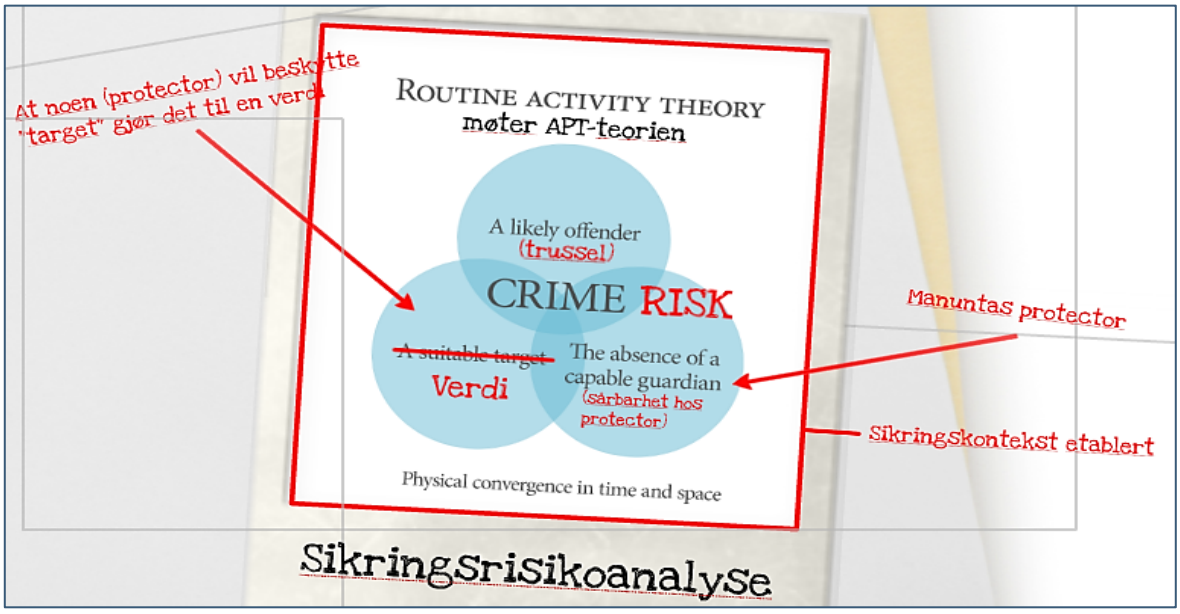
[51] Manunta G. (1999). "What is Security", *Security Journal*, **12** (2) (1999) 57-66.

[52] Manunta G. (2002). "Risk and Security: Are they Compatible Concepts?" *Security Journal* **15** (2), 43-55

Når det gjelder sammenhengen mellom risikobegrepet og Manuntas definisjon av sikring finner man et svar i følgende setning, der Manunta skriver:*"However, there is a very good reason for considering the concept of risk incompatible with that of security"*.

Dette bør besvare spørsmålet om hvordan Manunta mener at risiko henger sammen med sikkerhet slik han har definert sikkerhet. Risiko og sikkerhet henger etter hans syn ikke sammen i det hele tatt. Her blir det litt underlig at enkelte norske fagmiljøer tar Manuntas definisjon av sikkerhet til inntekt for at risiko kan beskrives som en funksjon av trussel, verdi og sårbarhet R=f(T,V,S).

I tillegg henviser de norske fagmiljøene til "Routine activity theory[53]" og "Rational choice theory[54]" som en del av det vitenskapelige teorigrunnlaget for trefaktormodellen. I "Routine activity theory" blir tre faktorer fremhevet når en studerer tilsiktede uønskede handlinger. Man trenger (i) en motivert trusselaktør med hensikt til å begå en forbrytelse, (ii) et egnet mål for trusselaktøren og (iii) fraværet av noe(n) som beskytter målet (verdien). Når disse forholdene samsvarer i tid og rom, er kriminalitet eller en tilsiktet uønsket hendelse sannsynlig. Figur 6.1 visualiserer hvordan "Routine activity theory" møter Manuntas APT-teori (figuren er hentet fra Falck Nutec-foredrag av Joakim Barane 2014).



Figur 6.1 Routine activity theory møter APT-teorien (Barane 2014)[55].

Det som blir trukket frem som det mest interessante med Manuntas teorier er at han etablerer betegnelsen *sikringskontekst*. For at man skal ha en slik kontekst er man avhengig av en verdi som både noen er ute etter å "ta" og som noen er interessert i å beskytte. Et eksempel kan være en

[53] Felson L. E, Cohen, M. (1979). "Social change and crime rate trends: A routine activity approach", *American Sociological Review*, Vol. 44, No. 4 (Aug., 1979), pp. 588-608
[54] Caplan, B. (2006). "Terrorism: The relevance of the rational choice model". *Public Choice* (2006) 128, 91-107
[55] FFI så figuren første gang under et frokostseminar i regi av Falck Nutec vedrørende de nye standardene i NS 583X- serien (18.11.2014).

rusbruker med abstinenser og et desperat behov for å skaffe penger til en ny dose (motivert trusselaktør), som treffer på en beruset person har akkurat vært i minibanken og tatt ut penger (et egnet mål for trusselaktøren) som forviller seg inn en mørk bakgate og øde sted (fravær av noe(n) som beskytter personen). Dette kan det lett resultere i et ran.

"Rational choice theory" tar utgangspunkt i at samfunnsaktører tar rasjonelle valg av midler for å oppnå ønskede mål. For en terrorist kan dette innebære valg som for andre kan synes irrasjonelle, som f. eks. å sprenge seg selv for å oppnå et mål. Men for terroristen er dette et rasjonelt valg, og det er aktøren som har definisjonsmakt her. Det gjør terrorhandlinger ekstra vanskelig å forutse.

FFI mener at trefaktormodellen bærer preg av at risikotrekanten ble funnet først og at en deretter har funnet og tilpasset ulike teorier for å skape et teoretisk grunnlag (se vedlegg C.9. for intervjuet med Roy Stranden under tittelen "Bakgrunnen til NS 583X-serien og standardarbeidet"). Jore (2014) hevder at "*det vitenskapelige grunnlaget for trefaktormodellen er mangelfullt, og denne tilnærmingen har ikke tatt innover seg forskningen innen risikoanalysefaget de siste årene."* (Jore 2014, vedlegg C.2).

6.2.6 Sannsynlighetsvurderinger i trussel- og sårbarhetsvurderingen

I artikkelen "Guiding Resource Allocation based on Terrorism Risk [56] foreslås det å bruke en modell som kan ligne på trefaktormodellen, ved at risiko angis som en funksjon av trussel, sårbarhet og konsekvens (Willis 2007). Imidlertid benyttes det her en dobbelt sannsynlighet, i det trusselen er definert som sannsynligheten av at et angrep finner sted og sårbarheten er sannsynligheten for at angrepet resulterer i skade.

Faktorene som inngår er:
Threat= p(attack occurs)
Vulnerability = p(attack results in damage|attack occurs)
Concequences= E(damage|attack occurs and results in damage) (E=expected value, forventningsverdi).

Risiko fremstilles da som en sammenstilling av disse tre faktorene
Risk = p(attack occurs) p(attack results in damage|attack occurs)* E(damage|attack occurs and results in damage*), eller forkortet:
Risiko = trussel*sårbarhet*konsekvens.

Dette kan oppfattes som et produkt av de tre størrelsene, og dermed støtter en sannsynlighets-konsekvens-modell. Imidlertid påpeker også Wills at risiko oppstår når de tre faktorene faller sammen, og dermed kan dette også oppfattes som en støtte for en trefaktormodell. Her er det også en uklarhet.

[56] Willis, H. (2007)."Guiding Resource Allocation based on Terrorism Risk", *Risk Analysis*, **27**, (2007) 597 – 606.

6.2.7 Kommunikasjon av risiko og usikkerhet

I en artikkel publisert i tidsskriftet Reliability Engineering and System Safety beskrives prosessen ved risikoanalysen av gassterminalen i Risavika (Vinnem, 2010)[57]. Her ble risikoen opprinnelig beskrevet ved en konvensjonell risikomatrise med sannsynlighet og konsekvens. Artikkelforfatteren er noe kritisk til hvordan dette ble kommunisert til befolkningen i nabolaget til anlegget. I artikkelen er risikoen også beskrevet ved hjelp av F-N-kurver, hvor frekvensen (F) av hendelser er plottet som funksjon av antall dødsfall (N), og artikkelforfatteren mener risikomatrisen burde vært erstattet med slike kurver i den informasjonen som ble gitt før det ble holdt en offentlig høring om anlegget, men erkjenner at slike kurver kan være vanskelige å forstå.

Risikoanalyser har en lang historie i oljeindustrien. Samtidig har man mye statistiske data å bygge på, også når det gjelder trygghet. Dette kan lede til at man tror at risiko er noe som kan beregnes eksakt. I en artikkel fra 2004[58] understreker Aven og Kristensen at det er viktig å kommunisere usikkerhet ved risikoanalyser (Aven og Kristiansen, 2004). De understreker at selv om det finnes vitenskapelig grunnlag for å ta beslutninger, må man erkjenne at prosessen med å vurdere usikkerheter og ta beslutninger ligger utenfor det tradisjonelle naturvitenskapelige området hvor man kan gjøre kontrollerte eksperimenter.

6.3 Gir vitenskapen et svar?

Det hadde vært ønskelig om forskningen og vitenskapen kunne fortelle hvordan man skulle foreta risikoanalyser og -vurderinger på best mulig måte. Men her, som på andre områder, finner ikke vitenskapen absolutte sannheter. Forskning er å produsere kunnskap, ikke gi et svar med to streker under. Ut fra det lille utvalget av publikasjoner som er beskrevet ovenfor, samt gjennomlesning av et større utvalg relevante publikasjoner, er det klart at en enhetlig arbeidsmetodikk ikke finnes. Men det man oppnår med gjentatte drøftinger av problemstillinger er møysommelig å utvide kunnskapen, og finne et mønster. I dette tilfellet, når det gjelder risikovurderinger i forbindelse med tilsiktede uønskede handlinger, kan man skimte et mønster:

1. Det er bare unntaksvis fruktbart å basere seg på historiske data for å beregne tallverdier for risiko. Dertil er datagrunnlaget for spinkelt, og aktørene tilpasser seg eventuelle forsvarstiltak som iverksettes på grunnlag av vurderingene[59].
2. Det er nødvendig å basere seg på kunnskap, både faktisk kunnskap om det systemet som skal vurderes, og kunnskap om trusselaktører. Dette kan også inkludere kunnskap som er basert på trusselvurderinger. Hvis en har relevant statistikk og datamaterialet om f.eks. en

[57] Vinnem, J.E. (2010). "Risk analysis and risk acceptance criteria in the planning process of hazardous facilities – A case of an LNG plant in an urban area", *Reliability Engineering and System Safety* **95** (2010) 662-670.
[58] Aven, T., Kristensen, V. (2005). "Perspectives on risk; review and discussion of the basis for establishing a unified and holistic approach" in *Reliability Engineering and Systems Safety* **90** (2005) 1-14.
[59] Det må presiseres at det ofte finnes lite historiske data på ekstreme naturhendelser. Manglende tallmaterialet og lite empiri er dermed også en metodisk utfordring for ekstreme utilsiktede, uønskede hendelser.

trusselaktørs modus operandi eller målhistorikk kan en bruke dette som bakgrunnsinformasjon i trusselvurderingen og i scenarioutviklingen.

3. Dette er et dynamisk område. Aktørene tilpasser seg forsvarstiltak, og tar samtidig i bruk ny teknologi.
4. Risikovurderinger er ikke statisk, men må stadig revurderes og oppdateres.

7 Ulike tilnærminger til risikovurderinger

Dette kapitlet beskriver kort ulike internasjonale og nasjonale tilnærminger til risikovurderinger. For å kunne sammenligne de ulike tilnærmingene laget vi en sjekkliste med kriterier som omhandlet hva en god tilnærming bør inneholde, og generelle trekk ved tilnærmingen[60]. Kriteriene var (i) i hvilken grad arbeidsgruppens sammensetning blir nevnt i tilnærmingen, om tilnærmingen gjaldt (ii) alle typer verdier og (iii) identifisering av relevante trusler. Inkluderer tilnærmingen (iv) konsekvensklasser, (v) sikringsbarrierer, (vi) sensitivitetsstudier, og (vii) risikoaksept. Andre kriterier var om tilnærmingen var (viii) systematisk, (ix) brukervennlig, (x) brukt av mange aktører, (xi) kvantitativ eller kvalitativ, og om (xii) usikkerhet ble beskrevet. (xiii) Er tilnærmingen manuell eller databasert, (xiv) er sannsynlighet en eksplisitt parameter, (xv) blir resultatet kommunisert klart og (xvi) er det lagt opp til at vurderingsprosessen blir dokumentert på en god måte. Det var flere utfordringer knyttet til sjekklisten ettersom det for eksempel var vanskelig å bedømme i hvilken grad sannsynlighet var en eksplisitt parameter. Sannsynlighet var ikke i risikoformelen, men det ble gjort sannsynlighetsvurderinger underveis. Dette gjorde at vi i denne rapporten la mindre vekt på disse kriteriene.

Det er mange ulike tilnærminger og metoder for risikovurderinger som f.eks. (i) Grovanalyse (innledende fareanalyse), (ii) Bow-tie-analyse, (iii) Ulike kvantitative metoder, (iv) Risiko- og sårbarhetsanalyser (ROS), (v) Norsk standard 5814:2008 “Krav til risikovurderinger” og Veiledning i risiko- og sårbarhetsanalyse fra NSM (2006) og (vi) NS 5830:2012, NS 5831:2014, NS 5832:2014 og veileder fra POD, NSM, PST (2010).

Etter å ha studert flere tilnærminger til risikovurdering er det tydelig at mange av de samme elementene går igjen. De fleste anbefaler å starte med en idédugnad og en såkalt grovanalyse, og deretter supplere med andre tilgjengelige metoder etter analysens behov. Det kan være hensiktsmessig å gå mer i detalj både med hensyn til årsaker og konsekvenser for enkelte av de mulige hendelsene som er kartlagt som aktuelle (scenarioer). Her kan andre etablerte risikoanalysemetoder egne seg.

Dette kapitlet beskriver kort noen ulike tilnærminger utviklet i andre land (kapittel 7.1) og noen norske tilnærminger (Kapittel 7.2).

[60] Her fikk vi innspill fra en britisk konsulent Dave Keir som har over 20 års erfaring innen risikoanalyser innen kjernekraft, militære anlegg, bioteknologi og støtte til britiske sivile myndigheter.

7.1 Ulike tilnærminger til risikovurderinger brukt i andre land

En oversikt over utvalgte tilnærminger til risikovurderinger som er brukt i forskjellige land utenom Norge er beskrevet i mer detalj med kilder i vedlegg A. Nedenfor følger sammendrag av beskrivelsene.

Canada: Harmonized Threat and Risk Assessment

Harmonized Threat and Risk Assessment **(**HTRA)-tilnærmingen inkluderer både tilsiktede og utilsiktede handlinger.[61] Dette er en sammensmelting av forskjellige tilnærminger. Dette har resultert i en meget omfattende veileder, som består av flere forskjellige moduler som er ment å dekke alt. Men brukeren kan velge detaljeringsnivået. Metoden kan minne om NS 5830, i det den beskriver risiko som en funksjon av *kritiske verdier* (A), *trusselhendelser* (T), *sikringstiltak* (safeguards) (S) og *sårbarheter* (V). R = *f* (A, T, S, V). Den beskriver ikke risiko som en funksjon av sannsynlighet og konsekvens, men det blir beskrevet at det blir gjort sannsynlighetsvurderinger spesielt i trusselvurderingen. Det vil si at selv om sannsynlighet ikke er en eksplisitt parameter i risikoformelen, så blir det allikevel gjort sannsynlighetsvurderinger. Metoden beskrives imidlertid som vanskelig å bruke for ikke-eksperter, og har en meget omfattende brukerdokumentasjon (se vedlegg A for en mer grundig gjennomgang).

Storbritannia: Centre for the Protection of National Infrastructure

CPNI gir råd til offentlig og privat sektor innen (i) Fysisk sikring, (ii) Sikring av informasjon (cyber) og (iii) personellsikkerhet[62]. CPNI tilpasser tilnærmingene til risikovurderinger til sektorene som skal analyseres. FFI besøkte CPNI sammen med representanter for FB 3. september 2014, og fikk en orientering om de forskjellige arbeidsområdene. Tilnærmingen til risikovurderingene kan minne om NS 5814, siden alle sektorene benytter seg av risikomatriser som hjelpemiddel for å visualisere og sammenstille risiko basert på sannsynlighet og konsekvens. CPNI poengterte at tilnærmingen til risikovurdering i seg selv ikke er så avgjørende, så lenge man har (i) ressurspersoner med riktig fagkompetanse samlet i arbeidsgruppen (bl.a. fra ulike deler av virksomheten), (ii) at ressurspersonene har samme forståelse av trusselbildet, og (iii) tilnærmingen blir brukt på en gjennomtenkt og systematisk måte.

USA: Department of Homeland Security

US Department of Homeland Security (DHS) ble etablert i 2002. DHS har ansvar for å sikre USA best mulig mot tilsiktede handlinger som terror, sabotasje og illegal innreise til landet, men også forebygging og krisehåndtering ved alvorlige ulykker og naturkatastrofer. DHS utvikler og benytter et risiko-basert rammeverk for å bidra til et godt beslutningsgrunnlag. DHS benytter flere ulike modeller i sine analyser. Noen av dem er kort beskrevet her.

[61] Dziadyk, W. (2011). Harmonized TRA (HTRA) Methodology – Limitations. BD Pro Inc. Sist besøkt 06.10.2014. http://www.bdpro.ca/wp-content/uploads/2012/05/Harmonized_TRA_Limitations_13Sep2011.pdf

[62] CPNI (2013). Personnel Security Risk Assessment - A Guide. 4th Edition, June 2013.

Partnering for Critical Infrastructure Security and Resilience

I dokumentet "National Infrastructure Protection Plan, NIPP 2013", skriver DHS at risiko kan bli vurdert i form av trussel, sårbarhet og konsekvens, uten å angi mer detaljert hvordan dette kan gjøres.[63] Dette kan minne om NS 5830, men samtidig henvises til en definisjon av risiko som et uønsket resultat angitt ved sannsynlighet (likelihood) og konsekvens. Det er ikke klart angitt hvordan sannsynlighet kommer inn i vurderingen.

Risk Management Fundamentals

I *Risk Management Fundamentals* fra DHS står det at også trusler med lav sannsynlighet men alvorlig konsekvens må tas hensyn til, slik at en eventuell sannsynlighets- og konsekvensmodell må anvendes med forsiktighet.[64] Og det er interessant at de skriver at usikkerhet om risiko kan i seg selv være en risiko. Her brukes en trefaktormodell med trussel, sårbarhet og konsekvens. Men det advares mot å bruke dette rammeverket på feil måte, og særlig mot å beregne risiko ved å multiplisere de tre faktorene, siden de ikke er uavhengige av hverandre.

FedRAMP

FedRAMP er en mal for sikkerhetsvurderingsrapporter (Security Assessment Report, (SAR) Template), og gjelder IT-systemer.[65] Metoden er basert på kvalitativ risikoanalyse. Resultat gis som en kombinasjon av muligheten for at en trusselaktør kan utnytte et sikkerhetshull og følgen av at trusselaktøren utnytter hullet. For å kommunisere risikoen benyttes en (todimensjonal) risikomatrise med tre trinn, både for muligheten, for konsekvensen og for risikoen.

Gjennomgang av risikoanalysemetoder i DHS

National Research Council (NRC) fikk i 2008 i oppdrag å gå gjennom og evaluere aktiviteter i DHS knyttet til risikoanalyser.[66] DHS dekomponerer risiko til tre variabler; trussel, sårbarhet og konsekvens (Risiko = f(T, S, K)), som minner om trefaktormodellen. Det går imidlertid frem av rapporten at sannsynlighetsvurdering er en del av analysen, som ledd i vurdering av både trussel og sårbarhet. NRC konkluderer med at rammeverket som DHS benytter er bra og i tråd med akseptert praksis i risikoanalysefeltet. Imidlertid sier komiteen at operasjonaliseringen av rammeverket er svært mangelfull og må legges om. Dette gjelder vurderinger av de ulike komponentene og kombinasjonen av dem. Særlig for terrortrusler advares det om at komponentene er gjensidig avhengig av hverandre, og at dette må tas hensyn til i analysen. NRC påpeker at DHS bør støtte videre forskning på dette. Videre påpeker NRC at DHS må vurdere og kommunisere usikkerheter og forutsetningene omkring analysene, spesielt for risikoanalyse for terrorisme.

---

[63] DHS (2013). *National Infrastructure Protection Plan*, NIPP. Sist besøkt 11.05.2015. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[64] DHS (2011). *Risk Management Fundamentals.*Sist besøkt 11.05.2015. https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

[65] DHS (2012). *Security Assessment Report Template Version 0.1, May 2012*. Sist besøkt 21.01.2015. http://www.gsa.gov/graphics/staffoffices/SAR_Template_050212_508.doc

[66] National Research Council (2010). *Review of the Department of Homeland Security's approach to risk analysis*, The National Academies Press, Washington DC, 2010, ISBN-13: 978-0-309-15924-1.

Sandia: National Labs Security Risk Assessment Methodologies

Sandia har blant annet utgitt en PowerPoint-presentasjon som beskriver den generelle fremgangsmåten som benyttes.[67] De benytter et dataverktøy basert på en tradisjonell risikoligning: Risiko = P_A * (1 - P_E) * C, der P_A er muligheten for et angrep, P_E er effektivitet til forsvarssystemene og C er følgene av tap av verdier. Med sannsynlighet menes "likelihood", mulighet, med P_A, altså ikke matematisk sannsynlighet.

Thales: Et eksempel fra industrien

Firmaet Thales har utgitt veileder/brosjyre som beskriver deres fremgangsmåte ved vurdering av sikkerhetsrisiko og risikostyring.[68] I den beskrives risiko som kombinasjonen av sannsynligheten for en trussel, og den mulige virkningen på en kritisk verdi. Imidlertid illustreres dette med en trekantfigur, og gangen i vurderingen beskrives som en identifisering av trusselen, identifisering av kritiske verdier og identifisering av sårbarhet. Dette ender da opp i en risiko. Det kan virke som dette på den ene siden er en slags trefaktormodell, men risiko kommuniseres med en tradisjonell risikomatrise.

FN: Security Management System

De forente nasjoner (FN) har utgitt veiledere for sikring av personell i tjeneste.[69] For å kommunisere risiko benyttes en risikomatrise med fem nivåer både for sannsynlighet, konsekvens og risiko. Dette betyr at det er fem nivåer for hver av størrelsene. Mulighet og konsekvens settes av langs aksene i et todimensjonalt risikodiagram. Risiko leses av fra fargen til rutene inne i diagrammet, hvor det er fem forskjellige farger. Samme fremgangsmåte benyttes av USAID, som er det amerikanske organet for internasjonal utviklingshjelp. I veilederen brukes en ferdig fargelagt risikomatrise hvor mulighet og konsekvens settes inn på aksene, og risikonivået finnes ut fra fargen på det feltet man havner i.

EU

Risikovurderinger i offentlig transport

EU-prosjektet Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities (COUNTERACT) gir retningslinjer for risikovurderinger i forbindelse med tilsiktede uønskede handlinger rettet mot offentlige transportsystemer.[70] Her benyttes sannsynlighet for at

---

[67] Sandia (2006). *Sandia National Labs' Security Risk Assessment Methodologies*. Sandia corporations works for the United States Department of Energy's National Nuclear Security. A Risk Assessment Methodology (RAM) for Physical Security. Sist besøkt 06.10.2014. http://www.sandia.gov/ram/RAM%20Overview%20%20Presentation%20Aug%2006.pdf
Sandia (ND). *A Risk Assessment Methodology (RAM) for Physical Security*. Sandia corporations works for the United States Department of Energy's National Nuclear Security. Sist besøkt 06.10.2014. http://www.sandia.gov/ram/RAM%20White%20Paper.pdf

[68] Thales (ingen dato). *Oil & Gas Industry Towards Global Security- A Holistic Security Risk Management Approach*. Sist besøkt 06.10.2014. http://tinyurl.com/lkluwm8

[69] UN (no date). Policy and conceptual overview of the security risk management Process. Sist besøkt 21.01.2015. http://documents.wfp.org/stellent/groups/ercb_content/documents/manual_guide_proced/wfp203399.pdf

[70] EU COUNTERACT (2009).*Generic Guidelines For Conducting Risk Assessment In Public Transport Networks*. EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891. Sist besøkt 21.01.2015.

noe skal skje ("Probability of Occurence"), (5 nivåer), og konsekvens ("Impact/severity") (4 nivåer). Sannsynlighet er bl. a. basert på historiske data, men dette er en vurdering, ikke matematisk sannsynlighet. Både sannsynlighet og konsekvens angis som kategorier. Men for å kommunisere dette angis hver kategori med et heltall (1, 2, 3, 4) som så multipliseres med hverandre. Risikonivået regnes ut som produktet av tallverdiene for konsekvens og sannsynlig forekomst.

Oversikt over risikovurderingsmetoder for kritisk infrastruktur i EU
Giannopoulos m.fl. (2012) ved EUs Joint Research Centre (JRC) har laget en oversikt over forskjellige tilnærminger for risikoanalyse for beskyttelse av kritisk infrastruktur, og som er i bruk i forskjellige land.[71] Mange av de tilnærmingene som er omtalt ser på vekselvirkning mellom forskjellige deler av nasjonens infrastruktur, og er kanskje mindre relevante i forbindelse med risiko knyttet til tilsiktede uønskede handlinger. De som er relevante i forbindelse med tilsiktede uønskede handlinger er også omtalt andre steder i vår rapporten. Dette gjelder COUNTERACT, Sandia RAM og NIPP som er omtalt lenger opp i denne seksjonen, og DECRIS som er omtalt i kapittel 7.2.

RAND Corporation: Reducing Terrorism Risk at shopping Centers
RAND bruker i sin tilnærming historiske data for å forutsi risiko for terrorhandlinger mot kjøpesentre.[72] Dette er et eksempel på hva man kan gjøre når det dreier seg både om et stort antall objekter som skal beskyttes, og der hvor det har forekommet relativt hyppige angrep. Dette er mer et eksempel på en utført risikoanalyse enn en metode.

Frankrike: Franske myndigheters system for risikovurderinger
Franske myndigheters system for risikovurderinger (EBIOS) er et databasert verktøy utviklet i Frankrike for å samle kvalitativ kunnskap fra brukeren og brukerens fageksperter. Verktøyet er menybasert, og man trenger ikke være ekspert for å bruke det. EBIOS blir brukt i Frankrike og i utlandet, samt offentlig og privat sektor. Brukeren fyller inn informasjon om verdier og konteksten, krav til sikring og relevante trusselaktører. Ved å se sikkerhetsbehovene opp mot trusselaktørene så gir EBIOS til slutt ut en risikodiagnose. Det er vanskelig for brukeren å få innsikt i de forhåndsdefinerte innstillingene, dette gjør at metoden er lite gjennomsiktig (se en mer grundig gjennomgang i vedlegg E).

Nato
I dag har Nato flere tilnærminger innenfor ulike tema. Etter et litteratursøk i Natos databaser fant vi bl.a. "Manual on Explosives Safety Risk Analysis" og "NATO Risk Management Guide for

---

http://www.transport-research.info/Upload/Documents/201207/20120719_145438_7577_COUNTERACTGuidelines_lr.pdf
[71] Giannopoulos, G., Filippini, R., Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. Technical notes for the European Commission Joint Research Centre. Sist besøkt 26.11.2014. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf
[72] RAND (2006). *Reducing Terrorism Risk at Shopping Centers- An Analysis of Potential Security Options*. http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR401.pdf

Acquisition Programmes". Begge metodene er kvantitative og bruker sannsynlighet og konsekvens i sammenstilling og fremstilling av risiko (jfr. NS 5814). En Nato arbeidsgruppe arbeider med å komme fram til felles metoder for Nato (se vedlegg A).

7.2 Norske tilnærminger til risikovurderinger

I tillegg til de to tilnærmingene som FB bruker, har vi sett på noen andre tilnærminger til risikovurderinger som benyttes i Norge.

DSB: Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen
DSBs veileder for kommunale ROS-analyser gir en grundig innføring og veiledning og inkluderer også et analyseskjema for helhetlig ROS (DSB 2014a)[73]. Veilederen tar for seg hvordan dette arbeidet skal utføres fra planleggingsstadiet til kommunikasjon av resultatet og oppfølging etterpå. Veilederen er detaljert, inneholder eksempler, og tar for seg fremgangsmåten trinn for trinn, med skjemaer for dokumentasjon av arbeidet. Det gis anbefalinger for hvordan en prosjektgruppe bør settes sammen, og hvordan arbeidet bør organiseres. Veilederen inneholder en liste med eksempler på mulige uønskede hendelser, delt i følgende tre kategorier: naturhendelser, store ulykker og tilsiktede hendelser.

Veilederen beskriver hvordan risikobildet kan kommuniseres, både som detaljerte skjemaer, og som en forenklet fremstilling i en risikomatrise med konsekvens og sannsynlighet. Det understrekes at sannsynlighet ikke er frekvensbasert, men er en kunnskapsbasert mulighetsvurdering, basert på lokalkunnskap og ekspertvurderinger. I risikomatrisen angis sannsynlighet som et sannsynlighetsområde, som f. eks. "en gang per 100 til 1000 år". Usikkerhet vektlegges i kommunikasjonen. Veilederen omtaler også hva statistiske sannsynligheter faktisk betyr, og nevner som et eksempel at dersom man anslår sannsynligheten for en hendelse i en kommune til å være 0,1 % per år, vil dette bety at dersom man antar at alle Norges 400 kommuner er like, så ville det være 40% sannsynlighet for at en slik hendelse ville inntreffe i en av landets kommuner i løpet av ett år. Dette er et eksempel det kan være nyttig å ta med seg for å forstå hva sannsynligheter betyr.

DSB: Veileder for FylkesROS
Dette er en tilsvarende veileder som veilederen for ROS-analyse i kommunen, tilpasset forholdet i en større enhet som fylket (DSB, 2014b)[74]. Veilederen henviser også til veilederen for kommunal ROS-analyse for mer detaljert beskrivelse av fremgangsmåten. Veilederen henviser til NS-ISO 31000 når det gjelder gjennomføringen av risikovurderingen. Presentasjonen av fylkesROS kan være både i form av tall og beskrivende med ord, og kan oppsummeres i en risikomatrise med aksene sannsynlighet og konsekvens, hvor hendelsenes plassering i matrisen bygger på en vurdering av sannsynlighet og konsekvens, altså ikke en frekvensbasert sannsynlighet, med mindre tilgjengelig tallmateriale skulle gjøre det naturlig. Det understrekes i veilederen at det er

[73] DSB (2014a). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, Tønsberg, 2014.
[74] DSB (2014b). *Veileder for FylkesROS*, Tønsberg, 2014.

viktig å kommunisere at en risikomatrise eller annen sluttpresentasjon er en forenklet måte å vise resultatet av analysen.

DSB: Nasjonalt risikobilde

I DSBs nasjonale risikobilde (NRB) blir det etablert forskjellige verstefallsscenarioer for bruk innen samfunnssikkerhetsarbeidet (DSB, 2014c[75]; DSB 2014d[76]). Scenarioer innen tilsiktede uønskede handlinger (f.eks. terrorangrep i by) og innen utilsiktede uønskede hendelser (naturhendelser som kvikkleirskred i by eller storulykker som gassutslipp på industrianlegg) blir presentert i en felles risikomatrise med sannsynlighet og konsekvens på hver sin akse[77] (DSB 2014c:9). Det kan sies at DSB bruker en blanding av kunnskapsbasert sannsynlighet og frekvensbasert sannsynlighet "siden det er svært sjeldne hendelser som analyseres i NRB, er angivelsene for sannsynlighet ikke bare basert på statistikk, men også på systemforståelse, faglige vurderinger og lokalkunnskap". Når sannsynlighet blir omtalt for tilsiktede uønskede handlinger blir det beskrevet med ord som intensjon og kapasitet (se DSB 2014c:185). For utilsiktede uønskede hendelser blir sannsynligheten angitt "som det tidsrommet den uønskede hendelsen antas å ville inntreffe innenfor og regnes om til prosentvis sannsynlighet for at hendelsen vil inntreffe i løpet av ett år" (DSB 2014d:22).

DSB opererer med ulike konsekvenstyper. Fastsettelsen av samlet konsekvensskåre for et scenario skjer ved at "hver av konsekvenstypene gis en skåre på en skala fra A–E, som tilsvarer en tallverdi" (DSB 2014d:11).[78] Det gjøres også en "usikkerhetsvurdering knyttet til alle angivelsene for sannsynlighet og konsekvenser […] gjennom en vurdering av *kunnskapsgrunnlaget* for analysen og *resultatenes sensitivitet* for endringer i forutsetningene" (DSB 2014d:11).

NVE: Veiledning i risiko- og sårbarhetsanalyse for kraftforsyningen

Norges vassdrags og – energidirektorat (NVE) ga i 2010 ut en veileder for ROS-analyser for kraftforsyningen.[79] Den gjelder for både tilsiktede og utilsiktede hendelser. Innledningsvis står det: "*I denne sammenhengen handler det om å forebygge og håndtere hendelser som truer forsyningssikkerheten [for elektrisk kraft]. Dette er gjerne hendelser som kan medføre alvorlige konsekvenser, ofte med lav sannsynlighet. Det er viktig å presisere at det er et*

[75] DSB (2014c). *Nasjonalt risikobilde 2014*. Sist besøkt 12.03.2015 http://www.dsb.no/Global/Publikasjoner/2014/Tema/NRB_2014.pdf

[76] DSB (2014d). Fremgangsmåte for utarbeidelse av Nasjonalt risikobilde (NRB). Sist besøkt 12.03.2015. http://www.dsb.no/Global/Publikasjoner/2014/Tema/Fremgangsmaate_for_utarbeidelse_av_NRB.pdf

[77] Selv om sluttproduktet kan minne om en visualisering av sluttproduktet i NS 5814 så blir det understreket i NRB'en at det blir brukt ulike tilnærminger for utilsiktede hendelser og tilsiktede uønskede handlinger. DSB (2014d:15) henviser til NS 5830:2012 og skriver "Risikovurderinger knyttet til tilsiktede uønskede handlinger tar utgangspunkt i risiko definert som 'uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen'».

[78] DSB (2014d). *Fremgangsmåte for utarbeidelse av Nasjonalt risikobilde (NRB)*. Sist besøkt 12.03.2015. http://www.dsb.no/Global/Publikasjoner/2014/Tema/Fremgangsmaate_for_utarbeidelse_av_NRB.pdf

[79] Norges vassdrags- og energidirektorat (2010). *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen*. Veileder nr: 2-2010. Sist besøkt 20.12.2015. http://www.nve.no/Global/Publikasjoner/Publikasjoner%202010/Veileder%202010/veileder%202-10.pdf

forskriftskrav at ROS-analysene skal være oppdatert og dokumentert. Det legges vekt på uønskede hendelser, og det benyttes begreper som konsekvens og sannsynlighet" (NVE 2010: 5).

Konsekvenser beskrives på fem nivåer. Resultatet av analysen kommuniseres ved hjelp av en risikomatrise som en funksjon av konsekvens og sannsynlighet.

Veilederen gir en detaljert gjennomgang av arbeidsprosessen, og kommuniserer altså risiko med en risikomatrise med konsekvens og sannsynlighet. Men med sannsynlighet menes vanligvis ikke statistisk sannsynlighet, men en sannsynlighetsvurdering. Det understrekes i veilederen også viktigheten av å kommunisere usikkerhet der dette er relevant. NVEs tilnærming er konsistent med NS 5814.

Kystverket: Vurdering av sårbarhet for havner og havneterminaler

Kystverket utga i 2012 en veiledning [80] for vurdering av sårbarhet for havner og havneterminaler, og i 2014 en mal [81] for utarbeidelse av sårbarhetsvurderinger for havneanlegg (Kystverket, 2012; Kystverket 2014). Disse tar spesifikt for seg trusselen fra tilsiktede uønskede handlinger, og har derfor stor relevans for dette prosjektet. Selv om malen spesifikt tar for seg havneanlegg, er den et godt eksempel på hvordan en metodisk vurdering kan bygges opp. Metoden bygger på NS 5832, og ser på verdi, trussel og sårbarhet, og skriver at risiko er et samspill mellom disse, men det gis ingen beskrivelse eller anbefaling om hvordan risikoen skal bestemmes eller kommuniseres.

Fremgangsmåten er at etter en kartlegging av operasjoner og objekter foretas først en verdivurdering, så en trusselanalyse og til slutt en sårbarhetsanalyse. Dette danner så grunnlag for tiltak for å redusere sårbarheten. Det kan virke som denne sårbarheten er et mål for risikoen. Her er begrepene litt uklare. Tilnærmingen baserer seg på kvalitative vurderinger. Sannsynligheter inngår ikke eksplisitt i risikovurderingen, men ligger implisitt i trusselvurderingen. Trusselvurderingen bygger på vurderinger fra PST, Etterretningstjenesten, NSM, DSB, og Europol, og her kommer sannsynligheter for hendelser inn.

Analysen baserer seg på NS 5832 og er meget detaljert og gjennomarbeidet for denne typen objekter. Sammen med Kystverkets mal for sårbarhetsvurderinger gir den en meget god beskrivelse av fremgangsmåten trinn for trinn, og inneholder også skjemaer for dokumentasjon av prosessen og hvordan en skal kommunisere resultatene.

DECRIS

"Risk and Decision Systems for Critical Infrastructures" (DECRIS) var et prosjekt under forskningsprogrammet SAMRISK, ledet av SINTEF, og med deltakere fra NTNU og FFI[82]. Hensikten var å bygge på sektorvise ROS-analysemetoder og koble disse for å utføre

[80] Kystverket (2012). *Vurdering av sårbarhet for havner og havneterminaler. Veiledning.* Versjon 1.9 (21. februar 2012)

[81] Kystverket (2014): *Kystverkets mal for utarbeidelse av sårbarhetsvurderinger for havneanlegg*. Versjon 1.0, 05.06.2014

[82] DECRIS (2009). *Metode og verktøy for en samlet risikovurdering av kritiske infrastrukturer*. Sist besøkt 24.11.2014 http://www.sintef.no/globalassets/project/samrisk/decris/documents/decris-rapport.pdf

tverrsektorielle analyser der det ble tatt hensyn til avhengigheter mellom f. eks. kraft og IKT. Prosjektet så på konsekvensene av forskjellige hendelser, som også kunne være viljeshandlinger, men studerte ikke spesifikt på risikoen for tilsiktede uønskede handlinger. Tilnærmingen som er utviklet er viktig for å se på *konsekvensene* av en tilsiktet uønsket handling enten det er sabotasje, terror eller vanlig kriminalitet, dersom man har utviklet et scenario. Analysen angir en detaljert og trinnvis tilnærming, og benytter analyseverktøyet InfraRisk. Resultatet angis i en sannsynlighets- og konsekvens-matrise. Tilnærmingen ble testet for utvalgte infrastrukturer i Oslo kommune.

7.3 Oppsummering av tilnærminger

På bakgrunn av denne gjennomgangen kan en skissere noen fellestrekk. Alle tilnærmingene til risikoanalyse vi har gjennomgått har *samme formål* om å "finne risikoen knyttet til at noe skal kunne skje". I alle tilnærmingene blir *sannsynlighet (mulighet)* inkludert, enten på en eksplisitt måte (NS 5814) eller implisitt (NS 5830). *Safeguards/ sikringsbarrierer* er også et viktig innslag som blir inkludert enten som et eget trinn i metoden, eller som en del av sårbarhetsanalysen. Som oftest ser en sikringsbarrierer i sårbarhetsanalysen. Alle tilnærmingene vi har studert har i stor grad de samme hovedprosessdelene (trusselvurdering, sårbarhetsvurdering, systembeskrivelse/ verdivurdering (beskrivelse av hva man skal beskytte)). De ulike tilnærmingene bruker ulike metoder for datainnsamling (hendelsestrær, scenarioer, feiltreanalyse osv), men de fleste datainnsamlingsmetodene skjer innenfor rammen av ekspertgrupper.

Alle tilnærmingene har en systematisk fremgangsmåte. De fleste kan karakteriseres som brukervennlige. Nesten alle identifiserer (i) konsekvensklasser, (ii) trusler og (iii) sikringstiltak. Nesten alle inkluderer risikoakseptnivåer og stiller krav til dokumentasjon.

Derimot er det nesten ingen som beskriver hvordan følsomhetsstudier kan gjennomføres selv om dette vil være en naturlig del av en konkret trusselvurdering. Det er ulikt hvordan man skal beskrive usikkerhet, i hvilken grad vurderingene er til å stole på, underveis i prosessen. Noen veiledere nevner ikke problematikken, mens andre veiledere har egne metoder for å undersøke usikkerhet og hvor mye påvirkning det har på risikoen. Dette er generelt et svakt punkt hvor ingen av metodene gir en god framgangsmåte for å kommunisere dette. Noen metoder blander sammen sannsynlighet og usikkerhet. Dette kommuniserer ikke at sannsynligheten i seg selv kan være usikker.

Noen forskjeller er at tilnærmingene bruker ulike begreper og konsepter. Selv om hovedprosessdelene ofte er de samme, så kan de være i forskjellige rekkefølge. Detaljeringsnivået er forskjellig. Her er det et skille mellom de manuelle og databaserte tilnærmingene. I de fleste manuelle tilnærmingene bruker en ekspertgrupper, mens det ofte vil være én person som plotter inn analysen i den databaserte tilnærmingen. De fleste tilnærminger er manuelle, bl.a. CPNI-Pers. security, FN, Counteract, RAND (butikksenter), kommunale ROS, kraftforsynings-ROS, Kystverkets veileder, FBs tilnærminger basert på NS 5814 og NS 583X-serien og HTRA er kvalitative. De som er databaserte er Sandia, EBIOS og DECRIS. Thales og DHS er både manuelle og databaserte.

Det er omtrent like mange metoder som legger vekt på sammensetningen av arbeidsgruppen som de som ikke gjør det. Å si noe om hvordan arbeidsgruppen bør settes sammen, anses av FFI som et kvalitetstegn, ettersom det har store konsekvenser for analysen. Den canadiske HTRA-tilnærmingen, CPNI og Thales er de internasjonale tilnærmingene som presiserer dette. Av de norske tilnærmingene nevner KraftforsyningsROS, Kommunale ROS og NS 5814 noe om sammensetning av arbeidsgruppen. Det er flere tilnærminger som eksplisitt ikke nevner dette: Sandia, UN, EU (Counteract), RAND (Butikk-senter), EBIOS, Kystverkets veileder, DECRIS og NS 583X-serien.

Noen tilnærminger har flere bruksområder, men en del er utviklet for spesifikke systemer.

De fleste tilnærminger angir hvordan resultatet skal kommuniseres (f. eks. med en risikomatrise) og de fleste tilnærminger har sannsynlighet som en eksplisitt parameter. Disse er CPNI- Pers. security, Sandia, Thales, UN, EU (Counteract), kommunale ROS, DECRIS, NS 5814 og KraftforsyningsROS. De som ikke bruker sannsynlighet som en eksplisitt parameter er: HTRA, RAND (butikksenter), Kystverkets veileder og NS 583X-serien. EBIOS er vanskelig å klassifisere.

De fleste tilnærminger er kvalitative, noen er både kvalitative og kvantitative, mens bare to tilnærminger er rent kvantitative. De tilnærmingene som kan beskrives som kvalitative er: FN, Counteract, Kystverkets veileder, NS 583X-serien og CPNI- Pers. security. De tilnærmingene som kan beskrives som kvantitative er: Sandia, Thales og RAND. Mens HTRA, DHS, Kommunale ROS, KraftforsyningsROS, DECRIS og NS 5814 kan beskrives som begge deler. EBIOS er vanskelig å klassifisere.

8 Konklusjoner og anbefalinger

Utgangspunktet for denne rapporten er følgende tre konkrete oppdrag til FFI fra FB:

(1)Vurdere de to modellene for risikovurdering som FB bruker i dag, med hensyn til teoretisk og vitenskapelig forankring, kommunikasjon av risiko, bruksområde og styrker og svakheter.

(2) *Gi en oversikt over ulike tilnærminger til risikovurdering for security-området i større organisasjoner som FN, EU, Nato, Department of Homeland Defence, CPNI, ledende forskningsmiljøer og andre bransjer med stort sikringsbehov (security). Finnes det noen rådende "best practice" innenfor området?*

(3) *Gi en anbefaling til FB om det er tilnærminger for security risikovurderinger FB bør vurdere å bruke, eller momenter som bør tas inn i de eksisterende modellene for å forbedre disse.*

8.1 Vurdering av FBs to tilnærminger til risikovurdering

Dette kapitlet tar for seg FBs første og tredje spørsmål:
(1)Vurdere de to modellene for risikovurdering som FB bruker i dag, med hensyn til teoretisk og vitenskapelig forankring, kommunikasjon av risiko, bruksområde og styrker og svakheter.

(3) *Gi en anbefaling til FB om det er tilnærminger for security risikovurderinger FB bør vurdere å bruke, eller momenter som bør tas inn i de eksisterende modellene for å forbedre disse.*
Etter omfattende dokumentanalyser kan vi konkludere at FBs operasjonalisering av NS 5832 og NS 5814 er rimelig like ettersom mange av trinnene er de samme og standardene er så overordnede og generelle. De fleste gjennomfører risikoanalyser "basert på" en standard og ikke i "henhold til". Dermed er det rom for justeringer og tilpasninger som gjør at tilnærmingene ikke nødvendigvis blir så forskjellige i praksis. Dette samsvarer med funn fra CPNI studiebesøket.

FBs to tilnærminger har mange likhetstrekk. Begge starter med en verdivurdering, trusselvurdering og sårbarhetsvurdering, som også inkluderer valg av et sett med relevante og plausible scenarioer. Så langt er det ingen forskjell. Forskjellen er at i tilnærmingen basert på NS 5814 foretas en separat vurdering av muligheten for at et angrep finner sted og er vellykket basert på en kunnskapsbasert sannsynlighetsvurdering. Primært ligger forskjellene i hvordan risiko kommuniseres utad, og her har begge modellene svakheter. Risikomatrisen kan forlede beslutningstagerne til å tro at risikoanalysen er mer presis enn den er, og den symbolske trekanten i trefaktormodellen forteller bare hvilke faktorer som inngår i vurderingene.

Tilnærmingen basert på NS 5814 har en tydeligere og mye bredere vitenskapelig forankring enn NS 5832. Imidlertid ble NS 5814 etablert for safety-feltet, og anvendelser på security-området kom etter hvert. For NS 5832 ble tilnærmingen etablert først, og deretter kom en teoretisk vitenskapelig forankring, som ikke er særlig omfattende. Imidlertid har man den samme sentrale utfordringen i begge tilnærmingene: Hvilken trussel skal man ta høyde for i analysen gjennom valget av scenarioer?

En ulempe med NS 5832 er at den tilsynelatende ikke bruker begrepet sannsynlighet. Det kan gjøre at en generell bruker ikke fanger opp at en nødvendigvis må utføre en vurdering av sannsynlighet i analysen, og i tillegg gjøres det ingen relativ vektlegging av hvilke scenarioer som er de viktigste eller mest aktuelle overfor virksomhetens verdier. Vurderingen er binær; enten inkluderer man et scenario eller ikke, og de scenarioene man inkluderer, tillegges like mye vekt. Som grunnlag for beslutninger om risikoreduserende tiltak vil dette kunne bli problematisk for beslutningstakerne. I oppdaterte veiledninger til NS 5832 anbefaler FFI at dette klargjøres.

FFI anbefaler at for å unngå misforståelser må man definere hva slags sannsynlighet man sikter til, om det er "kunnskapsbasert sannsynlighet/trolighet/mulighet" eller "frekvensbasert sannsynlighet". I de aller fleste veiledere og den litteratur FFI har analysert anbefales det å bruke en kunnskapsbasert sannsynlighet heller enn en frekvensbasert sannsynlighet for å vurdere muligheten for tilsiktede uønskede handlinger. I den vitenskapelige litteraturen har FFI ikke funnet argumenter for at man IKKE skal vurdere sannsynlighet/mulighet for mulige fremtidige

handlinger i risikovurderinger, slik NS 5832 legger opp til. Vi har funnet flere argumenter for at dette et den mest utfordrende og vanskelige delen av en risikovurdering for security, og som forskere og analytikere fortsatt sliter med å finne gode løsninger på.

FFI mener at en kunnskapsbasert sannsynlighetsvurdering er nødvendig og uunngåelig i en risikovurdering for tilsiktede uønskede handlinger, selv om dette er vanskelig, og selv om man skulle velge en tilnærming basert på NS 5832. Dette bør synliggjøres.
En fordel med NS 5832 er at den fokuserer på hvilke verdier en virksomhet har og identifiserer hvilke av disse det er viktigst å beskytte. En slik verdisentrisk tilnærming kan bidra til en god grunnsikring i et omskiftelig trusselbilde. En virksomhet har kontroll både med egne verdier og sikringstiltak, mens trusselen er høyst usikker og varierende, dette fordi den eies av en trusselaktør utenfor virksomhetens kontroll.

Kommunikasjon av risiko er en utfordring i begge tilnærminger. For å kommunisere resultatene til brukerne har risikomatrisen den fordelen at den er enkel å forstå. Faren er at den kan overforenkle og gi inntrykk av større sikkerhet enn det er grunnlag for. Den kommuniserer ikke usikkerhet. Trekanten eller de tre sirklene som er koblet sammen for å kommunisere resultatene ut fra trekantmodellen illustrerer bare hvilke faktorer som brukes. FFI mener at risikobildet basert på trefaktormodellen er vanskeligere å kommunisere på en like lettfattelig måte som en risikomatrise. Den tradisjonelle bruken av en trekant som illustrasjon er god til å kommunisere hvilke faktorer som inngår i vurderingene, men er mindre egnet til å kommunisere resultatet. Trefaktormodellen har ingen god løsning på dette, og FBs valg av en éndimensjonal fargeskala er muligens tilstrekkelig. Den grafiske fremstillingen kan imidlertid ikke presenteres alene.

I begge tilnærmingene må usikkerheten knyttet til vurderingene klart kommuniseres. Dette er et forbedringspunkt. Dette er vanskelig i en grafisk fremstilling. I tillegg kan FB vurdere om det bør utføres en følsomhetsanalyse, det vil si å systematisk variere inngangsparametere og antakelser og vurderinger beheftet med særlig usikkerhet, for å se hvordan dette påvirker konklusjonene i risikovurderingen. Dette er en nyttig måte å synliggjøre variasjon som følge av usikkerhet på overfor beslutningstakere.

Det er avgjørende i begge tilnærminger at resultatet må dokumenteres og kommuniseres i en skriftlig rapport som grunnlag for beslutninger. FFI anbefaler at beslutningstaker må sette seg inn i hele risikovurderingen inkludert forutsetninger, antakelser, vurderinger og usikkerheter, og ikke bare nøye seg med å se på risikomatrisen eller en annen type fargekart.

En utfordring med NS 5814 er at risikoreduserende tiltak for scenarioer med lav sannsynlighet men høy konsekvens kan bli nedprioritert. I en vurdering basert på NS 5832 som har en verdisentrisk tilnærming, kan man risikere å prioritere for omfattende sikringstiltak fordi man vektlegger konsekvensene for verdiene, og i mindre grad sannsynlighetsaspektet. Her hadde det vært en klar fordel med veiledning, retningslinjer og deling av informasjon om sikringsnivå i ulike virksomheter, dette for å unngå store skjevheter og variasjoner mellom rimelig like virksomheter.

En viktig utfordring i valg av scenarioer, årsaker og konsekvenser, er om man skal velge verstefallshendelser, mest "trolige eller sannsynlige" hendelser eller en variasjon av ulike muligheter. Dette gjelder både årsaksanalysen (angrepsmåter) og konsekvensanalysen. FFI anbefaler FB å vurdere om tilnærmingene kan styrkes ved å benytte sløyfeanalyse og sløyfediagram for å få frem spredningen i mulige årsaker som kan gi en uønsket hendelse, og spredningen i mulige konsekvenser. Her kan det også være nyttig å bruke hendelsestre- og feiltreanalyse.

FFIs oppdrag var også å vurdere teoretisk og vitenskapelig forankring for FBs metodevalg og tilnærming. NS 5814 er forankret i lærebøker og forskning fra sikkerhetsfaglige akademiske miljøer ved UiS og NTNU, samt internasjonal forskning. NS 583X-serien har ikke et like omfattende vitenskapelig grunnlag som NS 5814.

Det ble identifisert utfordringer i NS 583X-serien knyttet til definisjoner, begreper og prosess-steg som er forskjellig fra NS 5814 /NS-ISO 31000, og som kan skape forvirring for praktikerne. FFI mener at det trengs en avklaring når det gjelder språkbruk og ordforståelse i NS 5832. FFI mener at NS 583X-serien burde definert "analyse" og "vurdering" i henhold til NS-ISO 31000 og SN-ISO Guide 73:2009.

Selv om vi ikke kan peke på én av FBs tilnærminger som foretrukket, kan vi likevel gi noen anbefalinger.

(i) Kunnskap og metodeforståelse er viktigere enn valg av metode og tilnærming.
(ii) Man bør unngå en homogen ekspertgruppe. I gruppen må en ha folk med ulike perspektiver, kompetanse og bakgrunn. Det trengs kritiske røster for å få belyst alle sider av en sak. Det øker kunnskapsstyrken.
(iii) Det er viktig å kommunisere på en forståelig måte og beskrive usikkerhet. Bruk av tall og enkle diagrammer kan gi inntrykk av at man er sikrere enn man er. Grafiske fremstillinger kan være et hjelpemiddel, men det er viktig å gi et godt bilde av hele sammenhengen.
(iv) Man bør være varsom med bruk av tall i kommunikasjon av resultater til beslutningstakere. Tall kan være hensiktsmessig for å strukturere tanker internt, og som et hjelpemiddel i analysen, men kan kommunisere større nøyaktighet i resultatene enn det er grunnlag for.
(v) Man må dokumentere arbeidsgangen, valg og bruk av metode og tilnærming, og hvilken brukerveiledning man har tatt i bruk.

8.2 Ulike tilnærminger og beste fremgangsmåte

"Internasjonalt finnes det ikke en rådende "best practice" i metodologien på security-området. Det å sikre seg mot ondsinnede villede handlinger er vanskelige problemstillinger, det er ikke noen som har funnet svaret." (Jore 2014, vedlegg C.2)

Dette kapitlet tar for seg FBs andre spørsmål:

(2) *Gi en oversikt over ulike tilnærminger til risikovurdering for security-området i større organisasjoner som FN, EU, Nato, Department of Homeland Security, CPNI, ledende forskningsmiljøer og andre bransjer med stort sikringsbehov (security). Finnes det noen rådende "best practice" innenfor området?*

Rapporten har undersøkt tilnærminger til risikovurderinger i utlandet og store organisasjoner, bl.a. den canadiske HTRA-tilnærmingen, CPNI i Storbritannia, med referanse til ulike tilnærminger fra US DHS, Sandia National Laboratory Security, FN-systemet, EU, RAND og Nato. Det er ingen omforent beste fremgangsmåte internasjonalt. Vitenskapelige artikler og intervjuer støtter opp om denne konklusjonen. Dette samsvarer med Communications Security Establishment som skrev "*Despite a wealth of informed discussion and documented research, no single approach has emerged as a clear choice for security professionals*" (Communications Security Establishment 2007:51). Imidlertid kan vi oppsummere med noen viktige suksesskriterier for å utføre gode risikovurderinger. I tillegg viser vi til vedlegg F og G.

Strukturert tilnærming med fokus på prosessen

CPNI argumenterer at man må ha en strukturert tilnærming med klare trinnvise steg som det er enkelt å gjennomføre, men at det finnes ulike tilnærminger som er egnet. Ifølge Aven m.fl. (2008:189-198) er det avgjørende at tilnærmingen man bruker er tilpasset analysens formål og det man skal studere. Hensikten med risikovurderinger er "å gi beslutningstøtte vedrørende valg av løsning og tiltak" (ibid). For risikoanalytikeren er det viktig å "reflektere over betydningen av valg av metode, tilnærming, modeller". Dette må også formidles til beslutningstakerne ettersom ulike metoder, tilnærminger og modeller har sterke og svake sider.

Viktigheten av arbeidsgruppen og kartlegging av kunnskapsstyrke

CPNI argumenterer at standarden eller tilnærmingen er mindre viktig, det viktigste er å ha de rette personene i arbeidsgruppen (bl.a. fra ulike deler av virksomheten). Ifølge CPNI er det viktig at det er en kompetent person som har erfaring med risikovurderingsmetoden som leder risikovurderingsarbeidet og som tvinger frem gode vurderinger og begrunnelser for disse vurderingene (sporbarhet, dokumentasjon og grunnlag for vurdering).

Sikringsfeltet er som sagt preget av lite erfaringsdata, dermed er det et større behov for å benytte seg av eksperters subjektive vurderinger. Som nevnt i intervjuene med Jore (2014) og Røed (2014) må man sikre god bakgrunnskunnskap ved å ha riktig ekspertise representert i arbeidsgruppen. Det er viktig å ha eksperter som (i) kan noe om systemet en undersøker og konteksten rundt det gitte systemet, (ii) har kjennskap til risikovurderingsmetoden, og (iii) har risikoforståelse og kjenner til trusselbildet. En bør benytte seg av flere eksperter innenfor ulike fagfelt for å få helhetlige vurderinger. Det er viktig at ekspertene er tydelige på hva de legger i begreper slik at de ikke "snakker forbi" hverandre eller at det oppstår misforståelser. Noen begreper det er nyttig å ha klarhet i er sannsynlighet, risikometoder, usikkerhet etc. Risikoanalytikeren må introdusere temaene de skal gjennomgå til ekspertene. Man må fortelle om

begrensninger og antakelser gjort, hva som er formålet med analysen, hvor komplekst eller omfattende analysen skal være. Njå, m.fl. (1998) (sitert i Egeli 2014:32) hevder at en må "konkretisere problemet og bestemme informasjonsbehovet: Ekspertene bør evaluere hvorvidt modellene og verktøyene som brukes i analysen bør bli utvidet, revidert eller avvist".

Risikoanalytikeren burde undersøke bakgrunnskunnskapen til ekspertene ettersom en må vite hva eksperten baserer sine vurderinger på. Ekspertuttalelser vil ofte være basert på subjektive meninger. Njå, m.fl. (1998) (sitert i Egeli 2014:32) har beskrevet flere faktorer som kan prege ekspertuttalelser som (i) Hendelser som eksperten er godt kjent med eller som ofte er blitt omtalt i lignende situasjoner, (ii) Eksperten justerer vurderinger fra funn og informasjon fra et spesielt utgangspunkt, som for eksempel tidligere erfaring. (iii) Eksperten vurderer "sannsynlighet ved å sammenligne sin kunnskap om et fenomen med den stereotypiske oppfatningen av dette fenomenet. Jo mer samsvar, desto mer sikker blir eksperten i sin vurdering" (Njå m.fl. sitert i Egeli 2014:32).

Viktige ting underveis i risikovurderingsprosessen

Det er viktig å være konkret i analysen. Midtgaard (2014) hevder at "*det ikke er tilstrekkelig å si at togtrafikken er avhengig av ekom. Avhengigheten må forklares og synliggjøres. For eksempel at lokomotivførere er avhengig av mobiltelefon for å kommunisere med togledelsen. Ved bortfall av ekomtjenester faller mobilnettene ut og alle tog må stanse uten kommunikasjon mellom lokfører og togledelse*". Når man er konkret er det enklere for leseren å følge resonnementene i risikoanalysen. Jo mer konkret og tydelig analysen blir, dess enklere er det for lederen å fatte beslutninger og sikringstiltak. "*Presentasjonen av en risikoanalyse bør invitere leseren til selv å trekke konklusjoner ved å lese resonnementene*." (Midtgaard 2014, vedlegg C.5).

Flere respondenter understreker behovet for et helhetlig perspektiv når en presenterer risiko for beslutningstakeren. Beslutningstakere ønsker ofte å vite hva risikoen er på ulike områder og hvor den er størst for å kunne prioritere sikringstiltak. "*Det er viktig at man ikke låser seg til bare én tilnærming og én type trusler. Beslutningstakere må ofte forholde seg til et helhetlig risikobilde. Og da vite bare risikoen for brann, eller bare risikoen for industrispionasje, er ikke tilstrekkelig*" (Rapp 2014, vedlegg C.8).

Rapp (2014) uttrykker at det er viktig å fokusere på de tingene vi faktisk har noe informasjon om, nemlig verdiene og sårbarhetene. "*Virksomheter må prøve å innhente informasjon om trusselen og vurdere dens relevans for egne verdier. Vi må imidlertid sette strek på et punkt og si at uavhengig av hvem de er og hvorfor de gjør det de gjør, så medfører det skade hvis de lykkes i sine forsøk, derfor må vi sikre oss. Som virksomhet må vi fokusere på hva som er viktig for oss å sikre og hvordan. Vi bør ikke bruke mye tid på hvem trusselaktøren er, som det kan være vanskelig å finne informasjon om og som den enkelte virksomhet i liten grad kan påvirke*". (Rapp 2014, vedlegg C.8).

Systemforståelse
Det er ikke fruktbart å sitte en hel dag inne i et rom og risikovurdere en virksomhet. Man må bli kjent med systemene, se hvordan de fungerer i praksis og se systemene i et holistisk perspektiv. "*Du må bli møkkete på henda og gjøre et dypdykk i fagområdet du studerer ettersom du er nødt til å få en systemforståelse. Du må skjønne hvordan ting henger sammen for å finne kjernen i problemet*" (Midtgaard 2014, vedlegg C.5).

Kommunisere risiko og usikkerhet
Hensikten med en risikovurdering er å fremskaffe en beskrivelse av risiko som beslutningstagere kan bruke for å vurdere om risikoen er akseptabel, og eventuelt vurdere hvilke sikringstiltak som må settes inn for å bringe risikoen ned på et akseptabelt nivå. Denne beskrivelsen må kommuniseres på en slik måte at det er forståelig for beslutningstagerne.

Det er risikoanalytikerne som har ansvaret for å kommunisere resultatet på en måte som oppfattes riktig av beslutningstagere. Her må både risiko og usikkerhet kommuniseres på en klar måte uten å forenkle så mye at mottageren trekker feilaktige konklusjoner. Her må hovedpunktene i vurderingene sammenfattes på en måte som ikke kan misforstås. "*Hvis ledere skal ta gode beslutninger så må de forstå usikkerheten og datagrunnlaget som analysen er bygget på. En enkel modell eller et tall er mangelfull. Derfor må ledere sette seg inn i analysene. Dette er spesielt viktig i security- fagfeltet ettersom en ofte mangler relevante data."* (Jore 2014, vedlegg C.2).

Samtidig må man huske at de som skal fatte beslutninger basert på rapporten ofte er personer som er vant til å fatte avgjørelser på usikkert grunnlag, og derfor også forstår hva usikkerhet er. Dette samsvarer med Aven (2007:153-162) som sier "det er en myte at ledere ikke kan forholde seg til usikkerhet. Analytikerne har sviktet". En kan undersøke usikkerheten ved "usikkerhetsanalyser" (sensitivitets- og robusthetsanalyser) ved å se betydningen av å endre en parameter. Dette må gjøres på en systematisk måte.

Noe av det vanskeligste kan være å kommunisere at usikkerheten i seg selv er usikker. Selv om det i noen tilfeller kan la seg gjøre å fremskaffe et tall for hva sannsynligheten for en hendelse kan være, kan denne sannsynligheten i seg selv være usikker. Som eksemplet med bankran (kapittel 3.3.1) viser, kan det bli stor usikkerhet selv med et ganske godt underlagsmateriale. I de tilfellene man finner det formålstjenlig å angi risiko med tall, kan det derfor være aktuelt å angi dette som et intervall, slik som i eksemplet ovenfor. Ett enkelt tall kan bli oppfattet som en sikker verdi, og usikkerheten kommuniseres ikke.

Gjennomsiktighet, sporbarhet og etterprøvbarhet
Helt sentrale prinsipper i enhver analyse er "gjennomsiktighet, sporbarhet og etterprøvbarhet" og i tillegg må man rapportere usikkerhet ved slutninger som er tatt og datagrunnlaget for slutningene. Begrepsvaliditet er viktig, man må definere og avklare begreper og definisjoner.

Samfunnssikkerhetsfeltet som er et relativt nytt fagfelt har mye å hente av forskningsmetodiske prinsipper fra mer etablerte fagfelt innen samfunnsvitenskap. Felles utfordringer er at det kan

være vanskelig å kvantifisere komplekse samfunnsfenomener, dermed er en avhengig av kvalitative forskningsmetoder. Da blir prinsippene gjennomsiktighet, sporbarhet og etterprøvbarhet viktig.

Flere respondenter hevdet at det vitenskapelige grunnlaget for NS 583X-serien ikke er grundig nok. Det er et behov for at akademia samarbeider med praktikerne for å teste, utvikle og validere denne tilnærmingen. En konklusjon her må være at de forskjellige miljøene kommer sammen og harmoniserer de aktuelle standardene, både med tanke på faktisk innhold, men også at man kommer fram til felles definisjoner og begreper.

8.3 Oppsummering

FBs to tilnærminger har mange likhetstrekk. Forskjellen er at i tilnærmingen basert på NS 5814 foretas en separat vurdering av muligheten for at et angrep finner sted og er vellykket basert på en kunnskapsbasert sannsynlighetsvurdering. Videre ligger forskjellene i hvordan risiko kommuniseres, og her har begge modellene svakheter. Fordelen med risikomatrisen er at den er enkel å forstå. Faren er at den kan overforenkle og gi inntrykk av større sikkerhet enn det er grunnlag for. Den kommuniserer ikke usikkerhet. Trekanten eller de tre sirklene som er koblet sammen for å kommunisere resultatene ut fra trekantmodellen illustrerer bare hvilke faktorer som brukes. FBs én-dimensjonale visualisering av risiko er tilstrekkelig, men kommuniserer heller ikke usikkerhet.

Det er avgjørende i begge tilnærminger at resultatet må dokumenteres og kommuniseres i en skriftlig rapport som gir et grunnlag for beslutninger. I begge tilnærmingene må usikkerheten knyttet til vurderingene klart kommuniseres. Dette er et forbedringspunkt. I tillegg kan FB vurdere om det bør utføres en følsomhetsanalyse.

Tilnærmingen basert på NS 5814 har en tydeligere og mye bredere vitenskapelig forankring enn NS 5832. En ulempe med NS 5832 er at en tilsynelatende ikke utfører en vurdering av sannsynlighet i analysen. FFI mener at en kunnskapsbasert sannsynlighetsvurdering er nødvendig og uunngåelig i en risikovurdering for tilsiktede uønskede handlinger, selv om dette er vanskelig, og selv om man skulle velge en tilnærming basert på NS 5832.

FFI anbefaler FB å vurdere om tilnærmingene kan styrkes ved å benytte sløyfeanalyse og sløyfediagram for få frem spredningen i mulige årsaker som kan gi en uønsket hendelse og spredningen i mulige konsekvenser. Her kan det også være nyttig å bruke hendelsestre- og feiltreanalyse.

Det er ingen omforent beste fremgangsmåte internasjonalt eller nasjonalt for risikovurderinger for tilsiktede uønskede handlinger. Vitenskapelige artikler og intervjuer støtter opp om denne konklusjonen.

Selv om det ikke eksisterer en beste fremgangsmåte går følgende kjennetegn igjen i en god tilnærming, at den

(i) er strukturert,
(ii) etablerer en arbeidsgruppe med bred kompetanse,
(iii) kartlegger kunnskapsstyrken,
(iv) er basert på systemforståelse og er konkret,
(v) har et helhetlig perspektiv,
(vi) kommuniserer risiko og usikkerhet,
(vii) er gjennomsiktig, sporbar og etterprøvbar.

Referanser

Aven, T (2010): On How to define, understand and describe risk. *Reliability Engineering and System Safety* **95** (2010) 623 – 631.

Aven, T. (2007). *Risikostyring. Grunnleggende prinsipper og ideer*. Oslo. Universitetsforlaget.

Aven, T. (2011). "On the new ISO guide on risk management terminology", *Reliability Engineering and System Safety* **96** (2011) 719 – 226.

Aven, T. (2012). "The risk concept—historical and recent development trends", *Reliability Engineering and System Safety* **99** (2012) 33–44.

Aven, T. (2013). "Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts", *Reliability Engineering and System Safety* **119**, (2013) 229-234.

Aven, T., Kristensen, V. (2005). "Perspectives on risk; review and discussion of the basis for establishing a unified and holistic approach" in *Reliability Engineering and Systems Safety* **90** (2005) 1-14.

Aven, T., Renn, O (2010). *Risk Management and governance: Concepts, guidelines and applications.* Heidelberg: Springer Verlag.

Aven, T., Røed, W., Wiencke, H. (2008). *Risikoanalyse*. Oslo: Universitetsforlaget.

Barane, J.E. (2014). "Risikohåndtering krever analyser". Teknisk Ukeblad, oktober 2014.

Barane, J.E., Barø, R. (2014). "Terror og metodikk", *Dagens Næringsliv* 7. desember 2014. Sist besøkt 12.12.2014.
http://www.dn.no/meninger/debatt/2014/12/07/2053/Politikk/terror-og-metodikk

Caplan, B. (2006). *Terrorism: The relevance of the rational choice model.* Public Choice (2006) 128:91-107

Communications Security Establishment (2007). *Harmonized TRA (HTRA).* TRA-1 Date: October 23, 2007. Sist besøkt 03.10.2014
https://www.cse-cst.gc.ca/en/system/files/pdf_documents/tra-emr-1-e.pdf

CPNI (2013). *Personnel Security Risk Assessment - A Guide*. 4th Edition. June 2013.

DECRIS (2009). *Metode og verktøy for en samlet risikovurdering av kritiske infrastrukturer*. Sist besøkt 24.11.2014.
http://www.sintef.no/globalassets/project/samrisk/decris/documents/decris-rapport.pdf

DHS (2010). *DHS Risk Lexicon 2010 Edition*. Sist besøkt 21.01.2015.
https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

DHS (2011). *Risk Management Fundamentals.*
https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

DHS (2012). *Security Assessment Report Template Version 0.1, May 2012*. Sist besøkt 21.01.2015.
http://www.gsa.gov/graphics/staffoffices/SAR_Template_050212_508.doc

DHS (2013). *National Infrastructure Protection Plan, NIPP*. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Dillon, R.L., Liebe, R.M., Bestafka, T. (2009) Risk-Based Decision Making for Terrorism Applications, *Risk Analysis* **29**(3) (2009) 321 – 335.

DSB (2012a) *Nasjonalt risikobilde 2012*. Sist besøkt 24.11.2014 http://www.dsb.no/Global/Publikasjoner/2012/Tema/NRB_2012.pdf

DSB (2012b). *Sikkerhet i kritisk infrastruktur og kritiske samfunnsfunksjoner – modell for overordnet risikostyring*. Sist besøkt 21.01.2015. http://www.dsb.no/Global/Publikasjoner/2011/Rapport/KIKS.pdf

DSB (2014a). *Veileder til helhetlig risiko- og sårbarhetsanalyse i kommunen*, Tønsberg, 2014.

DSB (2014b). *Veileder for FylkesROS*, Tønsberg, 2014.

DSB (2014c). *Nasjonalt risikobilde 2014.* Sist besøkt 12.03.2015 http://www.dsb.no/Global/Publikasjoner/2014/Tema/NRB_2014.pdf

DSB (2014d). *Fremgangsmåte for utarbeidelse av Nasjonalt risikobilde (NRB)*. Sist besøkt 12.03.2015. http://www.dsb.no/Global/Publikasjoner/2014/Tema/Fremgangsmaate_for_utarbeidelse_av_NRB.pdf

Dziadyk, W. (2011). *Harmonized TRA (HTRA) Methodology – Limitations*. BD Pro Inc. Sist besøkt 06.10.2014. http://www.bdpro.ca/wp-content/uploads/2012/05/Harmonized_TRA_Limitations_13Sep2011.pdf

Egeli, A. (2014). *Analysemetodikk i forbindelse med terrorisme - Bruk eller ikke bruk av sannsynlighet.* Masteroppgave i Samfunnssikkerhet, Institutt for medie-, kultur- og samfunnsfag, Universitetet i Stavanger.

EU COUNTERACT (2009).*Generic Guidelines For Conducting Risk Assessment In Public Transport Networks*. EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891. Sist besøkt 21.01.2015. http://www.transport-research.info/Upload/Documents/201207/20120719_145438_7577_COUNTERACTGuidelines_lr.pdf

FEDRAMP US (2012). *Security Assessment Report (SAR) Template*. Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Report (SAR).

Felson, L.E., Cohen, M. (1979). "Social change and crime rate trends: A routine activity approach", *American Sociological Review* **44**(4) (1979) 588-608

Fitje, J. (2013). *Terrortrusselen og nasjonalt nivå*. Sist besøkt 18.12.2014. http://www.pst.no/blogg/trusselniva/

Flesvik, J. H. (2014). "Om sannsynlighet for terror" i *Dagens Næringsliv*, 1. desember 2014. Sist besøkt 12.12.2014. http://www.dn.no/meninger/debatt/2014/12/01/2158/Terror/om-sannsynlighet-for-terror

Flesvik, J. H. (2014). “PST må ut med terrorinfo” i *Dagens Næringsliv* 17. november 2014. Sist besøkt 12.12.2014.http://www.dn.no/meninger/debatt/2014/11/17/2159/Terror/pst-m-ut-med-terrorinfo

Forsvarsbygg (2013). “Risikovurdering”, Rapportnummer 486/2013, Forsvarsbygg Futura, Nasjonalt kompetansesenter for sikring av bygg. (Konfidensielt)
Garrick, B. J, Hall, J.E, Kilger, M, McDonald, J. C, O’Toole, T, Probst, P.S, Parker, E.R, Rosenthal, R, Trivelpiece, A.W, Arsdale L.V,, Zebroski, E.L (2004). “Confronting the risks of terrorism: making the right decisions”, *Reliability, Engineering and System Safety* 86 (2004) 129–176.

Giannopoulos, G., Filippini, R., Schimmer, M. (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. Technical notes for the European Commission Joint Research Centre. Sist besøkt 26.11.2014. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

Hellevik, O. (2002). *Forskningsmetode i sosiologi og statsvitenskap*. Oslo: Universitetsforlaget.

Investopedia (2014). Definition of pure risk. Sist besøkt 18.12.2014 http://www.investopedia.com/terms/p/purerisk.asp

ISO/IEC (2014). *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. ISO/IEC 27000:2014.

Jore, S., Moen, A. (2015). A discussion of the risk-management and the rule-compliance regulation regimes in a security context, in *Safety and Reliability: Methodology and Applications*, Nowakowski m.fl. (Eds), Tayler & Francis Group, London, ISBN 978-1-138-02681-0, 677 – 684.

King, G., Keohane, R.O., Verba, S. (1994). *Designing Social Inquiry*. Princeton: Princeton University Press.

Kujawski, E., Miller G.A. (2007). *Quantitative Risk-Based Analysis for Military Counterterrorism Systems*. Systems Engineering, Vol. 10, No. 4, (273 – 289) (2007)

Kystverket (2012). *Vurdering av sårbarhet for havner og havneterminaler*. Sist besøkt 06.10.2014 http://www.kystverket.no/Maritim-infrastruktur/Havnesikring/Veiledning-/

Leitch, M. (2010). ISO 31000:2009 - The New International Standard on Risk Management, *Risk Analysis*, **30(**6) (2010) 887-892.

Line, M.B., Bertelsen, D., Fridheim, H., Hokstad, P., Kjølle, G., Røstum, J., Utne, I.B., Vatn, G.Å., Vatn, J. (2009). Metode og verktøy for samlet risikovurdering av kritiske infrastrukturer. Sluttrapport for DECRIS: Risk and Decision Systems for Critical Infrastructures. SINTEF Rapport A11636, Trondheim, ISBN 9778-82-14-04814-8.

Lund, T. (ed.) (2002). *Innføring i forskningsmetodologi*. Oslo: Unipub.

Mærli, M. B. (2014). “Usannsynlig sannsynlig”, *Dagens Næringsliv* 23. november 2014. Sist besøkt 12.12.2014.
http://www.dn.no/meninger/debatt/2014/11/23/2058/Terror/usannsynlig-sannsynlig

Manunta, G. (1997). “What is security?”, *International Security*. Perpetuity Press Ltd.

Manunta, G. (2002). “Risk and Security: Are they Compatible Concepts?” *Security Journal* **15** (2) (2002) 43-55.

Marsden, E. (2015). Risk metrics. Sist besøkt 11.05.2015. http://www.slideshare.net/EricMarsden1/risk-metrics

Meyer, S. (2008). *Typologi over uønskede hendelser*. FFI-rapport 2009/00447. Forsvarets forskningsinstitutt. Sist besøkt 18.12.2014. http://www.ffi.no/no/Rapporter/09-00447.pdf http://www.ffi.no/no/Rapporter/09-00447.pdf

National Research Council (2010). “Review of the Department of Homeland Security’s approach to risk analysis”, The National Academies Press, Washington DC, 2010, ISBN-13: 978-0-309-15924-1.

NATO (2008). *Improving Common Security Risk Analysis*. Final Report of Task Group IST-049. RTO Technical Report. Sist besøkt 06.10.2014. http://ftp.rta.nato.int/public/PubFullText/RTO/TR/RTO-TR-IST-049/TR-IST-049-02.pdf

NATO (2008). Manual on Explosives Safety Risk Analysis. NATO International Staff – Defence Investment Division. AASTP-4 (Edition 1).

NATO (2012). NATO Risk Management Guide for Acquisition Programmes. NATO STANDARD ARAMP-1. Published by the NATO Standardization Agency (Nsa).

Njå, O., Aven, T., Rettedal, W.K. (1998). “Subjective probability assignment in QRAs for offshore construction and cessation projects”. Sørco.

Norges vassdrags- og energidirektorat (2010). *Veiledning i risiko- og sårbarhetsanalyser for kraftforsyningen*. Veileder nr: 2-2010. Sist besøkt 20.12.2015. http://www.nve.no/Global/Publikasjoner/Publikasjoner%202010/Veileder%202010/veileder%202-10.pdf

NOU (2006:6). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Departementenes servicesenter, Oslo, 2006.

NS (2008). *Krav til risikovurderinger*. Norsk Standard NS 5814:2008.

NS (2012). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi.* Norsk Standard NS 5830:2012.

NS (2014). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikostyring.* Norsk Standard NS 5831:2014.

NS (2014). *Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.* Norsk Standard NS 5832:2014.

NS-ISO (2009a). *Risikostyring. Prinsipper og retningslinjer.* Norsk Standard NS/ISO 31000:2009.

NS-ISO (2009b). *Risikostyring. Metoder for risikovurdering*. Norsk Standard NS-ISO/IEC 31010:2009.

NS-ISO/IEC (2011). *Informasjonsteknologi. Sikringsteknikker. Risikostyring av informasjonssikkerhet*. Norsk Standard NS-ISO/IEC 27005:2011.

NS-ISO/IEC (2013). *Informasjonsteknologi. Sikringsteknikker. Styringssystemer for informasjonssikkerhet.* Krav. Norsk Standard NS-ISO/IEC 27001:2013.

NSM, POD, PST (2010). *En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger*. Sist besøkt 20.12.2015.
https://www.politi.no/vedlegg/rapport/Vedlegg_882.pdf

OD (2011). *Fra scenarioer til handling*. Sist besøkt 24.11.2014.
http://www.npd.no/Publikasjoner/Rapporter/Fire-framtidsbilder/Fra-scenarioer-til-handling/

RAND (2005). *Estimating Terrorism Risk.* Sist besøkt 06.10.2014.
http://www.rand.org/pubs/monographs/MG388.html

RAND (2006). *Reducing Terrorism Risk at Shopping Centers- An Analysis of Potential Security Options*. http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR401.pdf

Rapp, C. (2014). "Terror vanskelig å forutse" i *Dagens Næringsliv* 24. november 2014. Sist besøkt 12.12.2014.
http://www.dn.no/meninger/debatt/2014/11/24/2159/Terror/terror-vanskelig--forutse

Rausand, M. (1991). *Risikoanalyse; Veiledning til NS 5814.* Trondheim, Tapir Akademisk Forlag.

Rausund, M., Utne, I. B. (2009). *Risikoanalyse – teori og metoder*. Trondheim. Tapir Akademisk Forlag.

Sandia (2006). *Sandia National Labs' Security Risk Assessment Methodologies*. Sandia corporations works for the United States Department of Energy's National Nuclear Security. A Risk Assessment Methodology (RAM) for Physical Security. Sist besøkt 06.10.2014.
http://www.sandia.gov/ram/RAM%20Overview%20%20Presentation%20Aug%2006.pdf

Sandia (2008). *Security Risk Assessment Methodology*.
http://www.edams.upv.es/docs/English_Course/_7b%20Mattalucci_Security.pdf

Sandia (ND). *A Risk Assessment Methodology (RAM) for Physical Security*. Sandia corporations works for the United States Department of Energy's National Nuclear Security. Sist besøkt 06.10.2014.
http://www.sandia.gov/ram/RAM%20White%20Paper.pdf

SN-ISO (2009). *Risikostyring. Terminologi. Risk Management Terminology*. SN-ISO Guide 73:2009

Stavanger Aftenblad (2013). Bankran. Utgave datert den 1. august 2013

Taleb, N.N. (2010). *The Black Swan: The Impact of the Highly Improbable*. Penguin Books, 2. utg., London, ISBN 978-0-1410-3459-1.

Thales (ingen dato). *Oil & Gas Industry Towards Global Security- A Holistic Security Risk Management Approach.* Sist besøkt 06.10.2014. http://tinyurl.com/lkluwm8

United Nations (ingen dato). *Policy And Conceptual Overview Of The Security Risk Management Process*. Sist besøkt 06.10.2014.
http://documents.wfp.org/stellent/groups/ercb_content/documents/manual_guide_proced/wfp203399.pdf

USAid (ingen dato). *Security risk management ngo approach*. Sist besøkt 03.10.2014 http://tinyurl.com/l8y3mfx

Utne, I.B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I.A., Bertelsen, D., Fridheim, H., Røstum, J. (2008), Risk and Vulnerability Analysis of Critical Infrastructures – The DECRIS Approach.

Vinnem, J.E. (2010). "Risk analysis and risk acceptance criteria in the planning process of hazardous facilities – A case of an LNG plant in an urban area", *Reliability Engineering and System Safety* **95** (2010) 662-670.

Willis, H.H. (2007). "Guiding Resource Allocation based on Terrorism Risk", *Risk Analysis*, **27**(3) (2007) 597 – 606.

Forkortelser

COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities
CPNI	Centre for the Protection of National Infrastructure
CSEC	Communications Security Establishment Canada
DECRIS	Risk and Decisions Systems for Critical Infrastructures
DHS	Department of Homeland Security
DSB	Direktoratet for samfunnssikkerhet og beredskap
EU	European Union
FB	Forsvarsbygg
FFI	Forsvarets forskningsinstitutt
HTRA	Harmonized Threat and Risk Assessment
ISO	International Standardization Organization
JRC	Joint Research Centre
NATO	North Atlantic Treaty Organization
NOU	Norges offentlige utredninger
NRB	Nasjonalt risikobilde
NS	Norsk standard
NSM	Nasjonal sikkerhetsmyndighet
NTNU	Norges teknisk-naturvitenskapelige universitet
NVE	Norges vassdrags og – energidirektorat
OD	Oljedirektoratet
POD	Politidirektoratet
PST	Politiets sikkerhetstjeneste
RCMP	Royal Canadian Mounted Police
ROS	Risiko- og sårbarhetsanalyse
SN	Standard Norge
UiS	Universitetet i Stavanger
UN	United Nations
US	United States

Vedlegg A Tilnærminger til risikovurderinger

I denne seksjonen blir det henvist til flere tilnærminger til risikovurderinger som er brukt internasjonalt. Tabell B.1 gir en samlet oversikt over alle tilnærminger rapporten har sett på.

Metodeutviklingen innen risikovurderinger i Canada blir beskrevet nøye ettersom de har kommet langt på dette feltet. Det blir også fokus på tilnærmingene som er utviklet av Centre for the Protection of the National Infrastructure (CPNI) i Storbritannia. Representanter fra FFI og FB var på studiebesøk og fikk dermed en mer detaljert innsikt i tilnærmingene. Det blir kortfattede beskrivelser av tilnærminger fra blant annet Sandia, RAND og EU.

Harmonized Threat and Risk Assessment (HTRA) fra Canada

Canada har i løpet av de siste tjue årene investert betydelig med tid og krefter på å utvikle ulike TRA tilnærminger med tilhørende retningslinjer og opplæringspakker. Denne kunnskapen og erfaringen har blitt brukt til å utvikle en trinnvis forbedring i stedet for et radikalt avvik fra etablert praksis.

Tilnærmingen er generell nok til å gjelde fysiske objekter, informasjon og IT-ressurser, samt vern av ansatte og tjenesteleveranser. Den inkluderer både tilsiktede og utilsiktede hendelser. HTRA er fleksibel og en kan selv finne et passende detaljnivå for å tilfredsstille sikkerhetsmål i organisasjonen. Svakheten er at det har blitt en omfattende tilnærming som gjør at det er vanskelig å få oversikt. Før 2007 hadde Canada flere tilnærminger innenfor fysisk sikring og IT-sikkerhet. Selv om tilnærmingene lignet hverandre var det forskjeller i opplæringen, retningslinjene og tilnærmingsmåten. Dette forårsaket forvirring hos statlige institusjoner i Canada som var brukerne. I Canada har en gått fra (i) flere tilnærminger på ulike felt, (ii) til kombinasjonstilnærmingen, (iii) én harmonisert tilnærming. Utviklingen blir skissert her med fokus på Canadas nåværende tilnærming "Harmonized Threat and Risk Assessment" (HTRA).

Royal Canadian Mounted Police (RCMP)

RCMP sin tilnærming blir beskrevet som en enklere prosess som består av fire steg (1) *Forberedelser* (hva skal man beskytte?), (2) *Trusselvurdering* (hva skal vi beskytte oss mot og hva er konsekvensene av en trussel?) (3) *Analysér risikoen* (fungerer sikringstiltakene godt nok?), (4) *Håndtering av risiko* (hva skal man gjøre for å redusere risikoen?) (NATO RTO 2008: 3-11[83]). Denne tilnærmingen ble brukt bredt fordi den var (i) enkel å bruke, (ii) analysen er presentert i en tabell slik at leseren kan se resultatene fra ulike scenarioer fra trussel og sårbarhet til risiko, (iii) tilnærmingen inkluderer kvalitative og kvantitative rangeringer (ibid)[84].

[83] NATO (2008). Improving Common Security Risk Analysis. Final Report of Task Group IST-049. NATO RTO Technical Report. Sist besøkt 06.10.2014.
http://ftp.rta.nato.int/public/PubFullText/RTO/TR/RTO-TR-IST-049/TR-IST-049-02.pdf

[84] Her blir det spesielt henvist til RCMP "The Guide to Threat and Risk Assessment for Information Technology" publisert i 1994 ettersom NATO RTO så på IT-sikkerhet.

Svakhetene ved tilnærmingen er at (i) sårbarhetsanalysen mangler dybde og er inkonsistent i måten man regner ut restrisikoen (residual risk), (ii) tilnærmingen bruker en kvalitativ rangering "høy - middels – lav", men det er ingen forklaring på hva de ulike nivåene betyr. Disse nivåene svekker granulariteten i analysen ettersom kategoriene ikke er definert. (iii) Blandingen av kvalitative rangeringer med numerisk verdi gjør det vanskelig for toppledelsen å tolke resultatene, (iv) det blir ikke skissert en oppfølgingsplan.

Communications Security Establishment Canada (SCEC) publiserte en veileder i 1999 som ble en populær tilnærming brukt av konsulenter og statlig personell. Tilnærmingen henviser til flere eksempler på verdier, trusler og sårbarheter og har ni steg som blir presentert i tabellform med et skille mellom hovedaktivitetene og hva slags dokumenter som skal bli publisert for hvert trinn. Svakhetene er at det er lang og omfattende prosess. Tilnærmingen tillater mer granularitet/ mer detaljer, men bruken av numeriske verdier og ulike skalaer gjør det vanskelig for objekteieren å forstå resultatene. Det er heller ingen oppfølgingsplan om hvordan man kan ta anbefalingene videre (Nato, 2008).

Kombinasjonstilnærmingen - RCMP og SCSEC
På ett tidspunkt tok de statlige institusjonene og blandet de ulike tilnærmingene fra RCMP[85] og SCSEC[86]. Slik kunne en kombinere styrker fra begge metodene. Terminologien er den samme for begge tilnærmingene, dermed er det mulig å bruke ulike moduler fra hver tilnærming. I kombinasjonstilnærmingen ble risikoen fastsatt på en subjektiv måte. Risikoen ble en funksjon av *kritiske verdier* (A), *trusselhendelser* (T), *sikringstiltak* (safeguards) (S) og *sårbarheter* (V). Motivasjonen og sannsynligheten for at en trusselaktør skulle angripe ble indirekte tatt med i beregningen av risiko (Dziadyk 2011:7[87]).

$R = f\ (A, T, S, V)$

Dette minner om NS 5830/NS 5832 ettersom den ikke fokuserer på sannsynlighet og konsekvens. Man har i tillegg "sikringstiltak" som en egen parameter.

Kombinasjonstilnærmingen vil som oftest bruke kvalitative vurderinger med en beskrivelse av nivåene "lav - moderat – høy". En kan velge om sårbarhetsvurderingen skal bli håndtert på et mer overordnet nivå eller om en skal ha en grundig analyse. I følge NATO RTO (2008) har kombinasjonstilnærmingen vist seg å få mer konsistente resultater på tvers av ulike deler av analyser. Allikevel blir det understreket at dybden og kvaliteten på analysen beror på personene som utfører analysen og deres erfaring fra dette feltet.

[85] Henvisning til RCMP dokumentene SIP-58 og R1-0019.
[86] Henvisning til CSEC dokumentene ITSG-0410, MG-211, MG-312, og MG-413.
[87] Dziadyk, W (2011). Harmonized TRA (HTRA) Methodology – Limitations. BD Pro Inc. Sist besøkt 06.10.2014. http://www.bdpro.ca/wp-content/uploads/2012/05/Harmonized_TRA_Limitations_13Sep2011.pdf

Harmonized Threat and Risk Assessment (HTRA)
SCSEC og RCMP initierte i 2004 et fellesprosjekt for å utvikle ett harmonisert rammeverk for risikovurderingsmetode. I 2007 ble det harmoniserte rammeverket innført (HTRA). HTRA-tilnærmingen sikter på å være enkel å bruke samtidig som den er fleksibel. HTRA består av flere moduler der brukeren selv kan bestemme hva slags detaljeringsnivå de vil legge seg på. I HTRA dokumentet er det 6 vedlegg som gir en detaljert gjennomgang av de ulike stegene.

Figur A.1 viser hvordan de ulike aspektene er knyttet sammen. HTRA veilederen understreker at det er i hovedsak 5 faser med flere prosesser under hver.

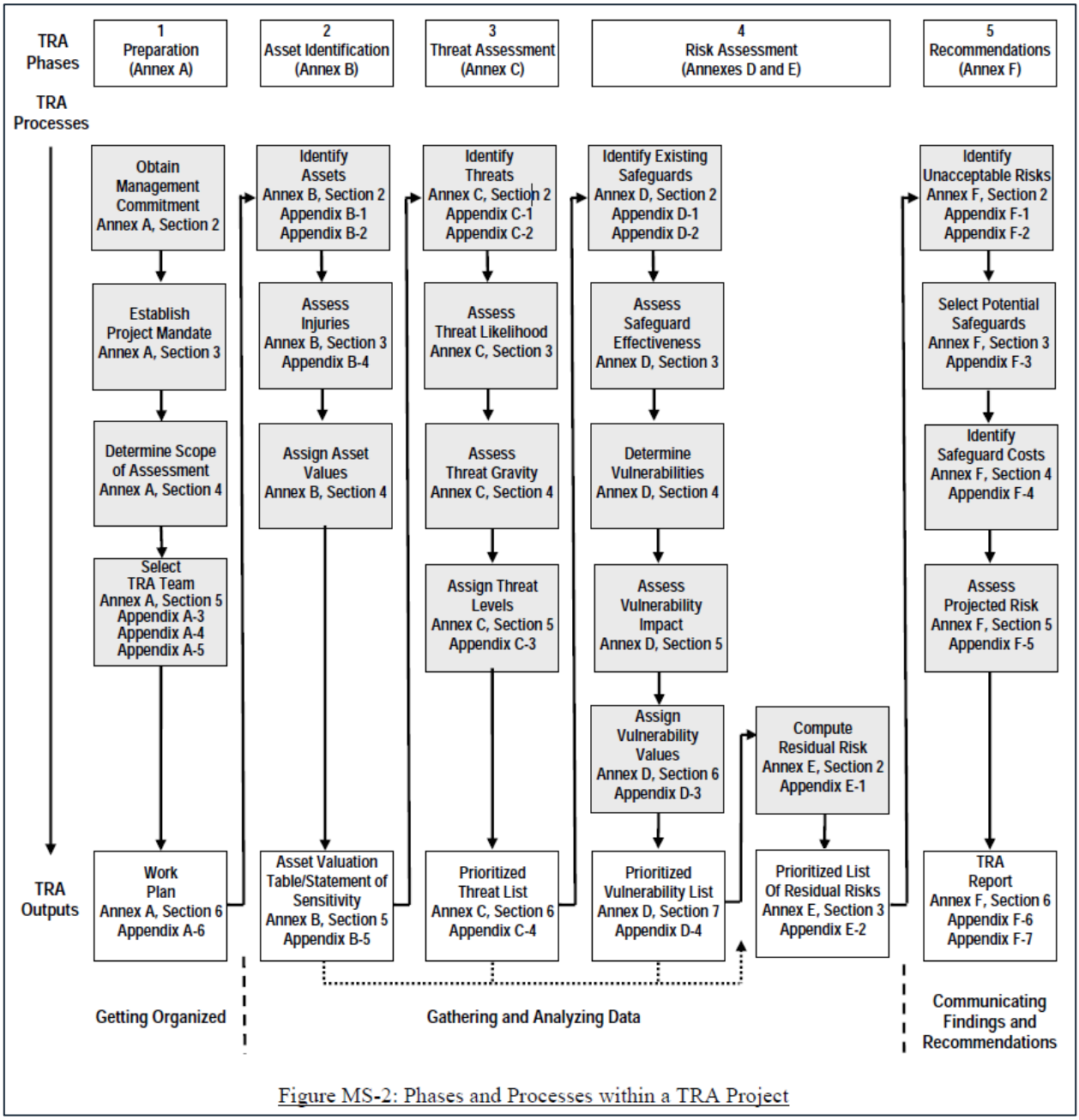


Figure MS-2: Phases and Processes within a TRA Project

Figur A.1 Harmonized Threat and Risk Assessment (HTRA) veileder.

Det er hovedsakelig anneks B-E som er relevant og som ser på (i) verdier, (ii) trusler, (iii) sårbarheter og (iv) kalkulering av risiko og restrisiko. Således minner modellen om NS 5832. Interessant nok gjelder tilnærmingen både naturkatastrofer (safety) og tilsiktede sikkerhetstruende hendelser (security).

Dziadyk (2011:2) argumenterer for at det er flere svakheter ved HTRA:

(i) *HTRA veilederen er vanskelig å bruke*. Dokumentet har 290 sider (inkludert 38 separate vedlegg). I motsetning til CSEC og RCMP veilederne, er HTRA ikke et dokument som man kan forvente seg at objekteierne kan lese og forstå. Mange risikoanalytikere har uttrykt at det er en altfor komplisert og lang guide.

(ii) *Overordnet beskrivelse av analytiske elementer som verdier, trusselaktører og sikringstiltak gjør at den påfølgende analysen blir mer generell.* I HTRA skal en først ha en overordnet beskrivelse av de ulike elementene som inngår i analysen. Konsekvensen er at i den påfølgende analysen gjennomfører man ofte overordnende analyser, istedenfor mer detaljerte analyser av sikringstiltak og brister. Dziadyk (2011:3) argumenterer "*the high level generalization or simplification of the analytical elements advocated by the HTRA Methodology tends to require the Risk Analyst to provide more of a high-level health check for an enterprise or system rather than focused lower-level recommended technical and operational security controls (i.e. safeguards) for implementation within security requirements baselines for individual security critical systems*".

(iii) *Dokumentasjon og formidling av resultater*. HTRA er prosessorientert med flere analysetabeller med små rubrikker. I rubrikkene er det gjennomsnittlig plass til 12-15 tegn, dette formatet gjør det vanskelig med en detaljert analyse/eller dokumentasjon på detaljert analyse. Dette minker sporbarhet.

(iv) *Beregning av restrisiko*. HTRA vurderer ikke eksplisitt styrken av eksisterende sikringstiltak (safeguards) eller sannsynligheten og motivasjon til trusselaktører i beregningen av risiko. Hvis risikoformelen ikke tar innover seg styrken på sikringstiltak så fører det til en forhøyet restrisiko.
(v) *Sertifisering av sikkerhetssystem og akkreditering*. HTRA burde identifisere anbefalte sikringstiltak som er påkrevd/pålagt. Ifølge Dziadyk (2011:7) "*the HTRA output provides high level generalized controls and does not generally provide the level of detail to allow mapping to control standards*".

Centre for the Protection of the National Infrastructure

Centre for the Protection of the National Infrastructure (CPNI) gir råd til offentlig og privat sektor innen (i) fysisk sikring, (ii) sikring av informasjon (cyber) og (iii) personellsikkerhet. CPNI har ikke én enhetlig tilnærming til risikovurderinger. De benytter en kritikalitetsskala (CAT-Criticality scale) fra 0 til 5 (0: minor, 1: moderate, 2: significant, 3: substantial, 4: severe og 5: catastrophic). CPNI definerer kritikalitet med at bortfall av en gitt funksjon/infrastruktur har (i) innvirkning på statens mulighet til å levere essensielle/viktige tjenester til befolkningen, (ii) store

økonomiske konsekvenser (som følge av tap av viktig tjeneste) og (iii) innvirkning på liv og helse som følge av tap av viktig tjeneste.

CPNI har forskjellige tilnærminger til risikoanalyse for ulike felt. I denne seksjonen undersøker vi (i) Transport, (ii) Finans, (iii) Befolkede plasser (crowded places), (iv) Statlig sektor (Government sector) og (v) Personellsikkerhet. Tilnærmingen brukt ligner NS 5814 og er beskrevet kort under. CPNI argumenterte at tilnærmingen i seg selv ikke er så avgjørende, men at man har (i) de riktige folkene samlet i arbeidsgruppe (bl.a. fra ulike deler av virksomheten), (ii) at folkene i arbeidsgruppen har samme forståelse av trusselbildet, og (iii) tilnærmingen blir brukt på en intelligent måte.

I *transportsektoren* bruker CPNI en kvantitativ risikoanalyse som har en statistisk analyse der numeriske skår er avgjørende for sluttproduktet og hvilke tiltak en må implementere. Tilnærmingen er knyttet opp til regjeringens årlige Nasjonale risikovurdering (NRA) som består av scenarioer som er konfidensielle. Det er etablert en "risk-advisory sub-commitee" som inviterer representanter fra statlig sektor, etterretning, politi, militæret og flyindustrien (flyselskaper og flyplasser). Forumet diskuterer de nasjonale scenarioene og minner således om DSB sitt nasjonale risikobilde som baserer seg på "*sannsynlighet og konsekvens*" (NS 5814). Dette brede forumet med de viktigste aktørene gjør at vurderingene av scenarioene blir nøyaktige og gode.

Risikovurderingen som dekker statlig sektor består av et skjema med følgende titler/felter (i) trusseltype, (ii) lokasjon, (iii) sannsynlighet, (iv) sårbarhet, (v) konsekvens, deretter blir det regnet ut en (vi) risikoverdi (risk factor), og til slutt har man et felt på (vii) tiltak (mitigation). Dette er en kvantitativ tilnærming med "*sannsynlighet og konsekvens*" og dermed minner om NS 5814. Numerisk skår blir brukt internt på CPNI i analysen, men til statlig sektor bruker CPNI en kvalitativ skala med nivåene lav, medium og høy risiko. Dette er fordi tall kan bli misbrukt politisk og tatt ut av kontekst.

Befolkede plasser (*Crowded places*) har en egen risikoanalyse der prosessen består av tre ledd ("*What needs to be done", "Why" and "How"*). Objekteierne, med veiledning fra CPNI, gjennomfører en vurdering av sin virksomhet og identifiserer sårbarheter i møte med seks angrepsmåter (*attack types*). Det er spesielt fem tiltaksfelt en ser på (i) "policy", (ii) "process", (iii) "physical security", (iv) "training and education" og (v) "partnership". Prosessen og aksjonsplanen med tiltak er det objekteier som har ansvar for. CPNI har overblikket og veileder prosessen. "Målattraktivitet" er et veiledende prinsipp slik at en kan bruke ressursene best mulig.

I finanssektoren ser risikoanalysen på konsekvens av bortfall av en verdi og tiden det tar for å gjenopprette denne funksjonen/verdien. 'Sannsynlighet for angrep' og 'sannsynlighet for suksess' er en del av et risikoanalysehjul. Hjulet består av fem momenter: (1) threat, (2) probability of attack, (3) vulnerability, (4) probability of success, (5) impact. CPNI har en statistikk over kritiske verdier i de 9 sektorene (critical assessts by sector). I finanssektoren er det relativt få CA, men mange av de skårer fem på CAT-skalaen.

Risikoanalyse knyttet til personell (personnel risk assessment) baserer seg på en sannsynlighetsskala (1-5) og konsekvensskala (1-5) og en kvalitativ beskrivelse (ikke multiplisering). Det er en enkel fremgangsmåte med ulik prioritering av risikomatriser. I analysen lages en oversikt over personell med mulighet til å være utro tjener. Dette er en kategorisering av hva personell med ulik type funksjon kan utføre. Det er få som har nok kunnskap om "utro tjener" problematikk.

US Department of Homeland Security

Partnering for Critical Infrastructure Security and Resilience

US Department of Homeland Security (DHS) har utgitt en oppdatert utgave av dokumentet National Infrastructure Protection Plan, NIPP 2013[88], som erstatter utgaven fra 2009. Av spesiell interesse er at de i avsnittet om risikovurdering og risikoanalyse skriver at risiko kan bli vurdert i form av trussel, sårbarhet og konsekvens, uten å angi mer detaljert hvordan dette kan gjøres. For definisjon av risiko henviser de imidlertid til DHS Risk Lexicon[89] fra 2010, der risiko er definert som et uønsket resultat angitt ved sannsynlighet (likelihood) og konsekvens. Det er ikke klart angitt hvordan sannsynlighet kommer inn i vurderingen.

Risk Management Fundamentals fra DHS

Dette dokumentet[90] henviser til samme definisjon av risiko, men har et eget avsnitt om uvanlige, usannsynlige og framvoksende risikoer, og skriver at:

"Prior to conducting a risk assessment, it is valuable to make a concerted effort to identify risks beyond those usually considered. For example, risks that are newly developing, even if they are poorly understood, are useful to identify. Risks that are highly unlikely but have high consequences should also be identified and incorporated into the assessment, if possible. This can even include identifying the risk of the unknown as a possible risk."(Homeland Security 2011:18)

Dette må forstås som støtte for det synet at også trusler med lav sannsynlighet men alvorlig konsekvens må tas hensyn til, slik at en eventuell sannsynlighets/konsekvensmodell må anvendes med forsiktighet. Og det er interessant at de skriver at usikkerhet om risiko kan i seg selv være en risiko. Og her kommer de med noen konkrete råd om hvordan slike risikoer kan håndteres:

"Brainstorming is a common technique to identify these unusual, emerging, and rare risks. So, too, is involving a wide range of perspectives and strategic thinkers to avoid the trap of conventional wisdom and groupthink. Even when a risk is difficult to assess, it may still be important to try to understand and should be noted. It should also be acknowledged that no identification of risks is likely to capture every potential unwanted outcome — there will always be things that happen that are unanticipated." (Homeland Security 2011:18)

---

[88] DHS (2013). *National Infrastructure Protection Plan, NIPP*. http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

[89] DHS (2010). *DHS Risk Lexicon 2010 Edition.* https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf

[90] DHS (2011). *Risk Management Fundamentals.* https://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf.

Her brukes en trefaktormodell med trussel, sårbarhet og konsekvens. Men det advares mot å bruke dette rammeverket på feil måte, og særlig mot å beregne risiko ved å multiplisere de tre faktorene med, siden de ikke er uavhengige av hverandre.

FedRAMP (US Department of Homeland Security)
Dette er en mal for sikkerhetsvurderingsrapporter (Security Assessment Report, (SAR) Template), og gjelder IT-systemer [91]. Her inngår (i) identifikasjon av sårbarhet og (ii) trusselvurdering. Dette er en kvalitativ risikoanalyse og resultat gis som en kombinasjon av muligheten for at en trussel kan utnytte et sikkerhetshull og følgen av at en trussel utnytter hullet. For å kommunisere risikoen benyttes en (todimensjonal) risikomatrise med tre trinn, både for muligheten, for konsekvensen og for risikoen.

Sandia National Labs Security Risk Assessment Methodologies
Sandia har blant annet utgitt en Powerpoint-presentasjon [92] som beskriver den generelle fremgangsmåten som benyttes, benytter et dataverktøy. det er basert på en tradisjonell risikoligning:

$Risk = P_A * (1 - P_E) * C$,
P_A is the likelihood of adversary attack,
P_E is security system effectiveness,
$1 - P_E$ is adversary success, and C is consequence of loss of the asset

Risiko beregnes ut fra sannsynligheten for et angrep, sannsynligheten for at en angriper kan penetrere beskyttelsen og følgen av et vellykket angrep. Med sannsynlighet menes ”likelihood”, mulighet, altså ikke matematisk sannsynlighet.

Fremgangsmåten er:

- Bestemme hva som er viktig
- Hvilke ressurser er tilgjengelig (økonomi)
- Hvilke følger av et angrep kan aksepteres
- Baserer seg på trussel og risiko

Et eksempel fra industrien
Thales utga i 2007 en veileder/brosjyre [93]som beskriver deres fremgangsmåte ved vurdering av sikkerhetsrisiko. I den beskrives risiko som kombinasjonen av sannsynligheten for en trussel, og

[91] US Department of Homeland Security (2012). *Security Assessment Report Template Version 0.1, May 2012*.
http://www.gsa.gov/graphics/staffoffices/SAR_Template_050212_508.doc
[92] Sandia (2008). *Security Risk Assessment Methodology*.
http://www.edams.upv.es/docs/English_Course/_7b%20Mattalucci_Security.pdf
[93] Thales (ingen dato). *Oil & Gas Industry Towards Global Security- A Holistic Security Risk Management Approach.* http://tinyurl.com/lkluwm8

den mulige virkningen på en kritisk verdi. Imidlertid illustreres dette med en trekantfigur, og gangen i vurderingen beskrives som en identifisering av trusselen, identifisering av kritiske verdier og identifisering av sårbarhet. Dette ender da opp i en risiko. Det kan virke som dette på den ene siden er en slags trefaktormodell, og det er uklart hvilken rolle sannsynligheten spiller. På dette trinnet er den ikke en eksplisitt parameter, men inngår i identifiseringen av trusselen. Senere i prosessen, når man skal vurdere nødvendigheten av å sette i verk tiltak for å møte en gitt trussel, illustreres dette i et diagram hvor man langs den ene aksen har sannsynlighet, og langs den andre aksen har virkning. Altså en tradisjonell sannsynlighets/konsekvens-matrise.

United Nations Security Management System, Chapter IV, Annex A (2012)
FN[94] har utgitt veiledere for sikring av personell i tjeneste. Definisjonene som benyttes ved risikovurdering er:

- Trussel: enhver faktor som kan volde skade
- Risiko: kombinasjon av påvirkning og muligheten (likelihood) for skade, tap eller ødeleggelse som følge av å bli utsatt for trusler.
- Benytter risikomatrisen med fem nivåer både for mulighet og ”Impact (konsekvens). Fem nivåer også for risiko: Very Low, Low, Medium, High, Very High, og Unaceptable. Mulighet (likelihood) er en eksplisitt parameter som beskrives med ord.

USAID har publisert en veileder[95] som bruker de samme begrepene og tilnærmingene som FN Security Management System i sin veileder INTERACT. Her benyttes mulighet (likelihood) og konsekvens (impact), begge på fem nivåer. Det blir gitt noen retningslinjer for hvordan man skal anslå nivåene, og de blir så satt inn i en ferdig fargelagt risikomatrise, og risikonivået finnes ut fra fargen på det feltet man havner i.

EU – offentlig transport (COUNTERACT)
Dette er retningslinjer for risikovurderinger i forbindelse med tilsiktede uønskede handlinger rettet mot offentlige transportsystemer [96]. Tilnærmingen inkluderer sannsynlighet for at noe skal skje (Probability of Occurence), (5 nivåer), og konsekvens (Impact/severity) (4 nivåer). Sannsynlighet er bl. a. basert på historiske data. Da ser en på om trusselen er blitt utført tidligere, og hvor ofte. Tilnærmingen spesifiserer at sannsynlighet er en parameter, og deler sannsynlighet inn i kategorier, på samme måte som konsekvensen av det som kan skje. En risikomatrise (Impact/severity vs. Probability of Occurrence) blir laget for å kommunisere risiko. Det benyttes fire risikonivåer som regnes ut som er produkt av tallverdiene for konsekvens og sannsynlig forekomst.

---

[94] UN (no date). *Policy and conceptual overview of the security risk management Process.* Sist besøkt 21.01.2015. http://documents.wfp.org/stellent/groups/ercb_content/documents/manual_guide_proced/wfp203399.pdf
[95] USAid (ingen dato). *SECURITY RISK MANAGEMENT NGO APPROACH*. http://tinyurl.com/l8y3mfx
[96] EU counteract (2009). *PT4: GENERIC GUIDELINES FOR CONDUCTING RISK ASSESSMENT IN PUBLIC TRANSPORT NETWORKS.* Final report 4 (october 2009). http://www.transport-research.info/Upload/Documents/201207/20120719_145438_7577_COUNTERACTGuidelines_lr.pdf

EU - JRC Technical Notes

Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art [97] Dette er en oversikt over forskjellige tilnærminger for risikoanalyse for beskyttelse av kritisk infrastruktur, og som er i bruk i forskjellige land. Tilnærmingene som er omtalt er for det meste tilnærminger som tar for seg følgene av uønskede hendelser på infrastruktur, men er lite relevant for sikkerhet, annet enn for å vurdere verdi og sårbarhet. De som er relevante i forbindelse med sikkerhet er omtalt andre steder i denne rapporten.

RAND Corporation: Reducing Terrorism Risk at Shopping Centers [98]

Denne tilnærmingen bruker historiske data for å forutsi risiko og konsekvens for terrorhandlinger, og setter tallverdier for "likelihood" ved å normalisere til den typen angrep som har forekommet oftest, nemlig bombe plassert på utsiden av kjøpesentre. Tilnærmingen sier samtidig at det er vanskelig å forutsi hvordan fremtidige terrorhandlinger vil utvikle seg. Imidlertid er dette en type angrep som på verdensbasis har forekommet så ofte at det gir en viss mening å tallfeste sannsynligheter. Tilnærmingen har en liste over scenarioer og deres relative sannsynlighet (Likelihood), og konsekvens i form av antall døde og nedetid. Dette er brukt til å beregne kostnadseffektiviteten ved sikringstiltak. Dette er et eksempel på hva man kan gjøre når det dreier seg både om et stort antall objekter som skal beskyttes, og der hvor det har forekommet relativt hyppige angrep. RAND tilnærmingen er mer en utført risikoanalyse enn en metode, men gir et godt eksempel på en metodikk tilpasset et gitt scenario.

Franske myndigheters risikovurderingssystem - EBIOS

EBIOS er et databasert verktøy for å samle kvalitativ kunnskap fra brukeren og brukerens fageksperter. Verktøyet kategoriserer den gitte informasjonen gjennom fem steg. Verktøyet ber om informasjon om verdier og verdiens kritikalitet, sikkerhetsbarrierer og trusler. Slik greier verktøyet å vurdere risiko og nødvendige sikringstiltak. Verktøyet produserer delrapporter om hva som er besluttet av brukeren på hvert trinn. Dette tydeliggjør hva slags beslutninger som blir tatt underveis.

For å fullføre en EBIOS vurdering må brukeren gjennom 5 trinn:

Trinn 1: Brukeren må svare på spørsmål der en først identifiserer verdien, ser på viktigheten av verdien og hvor avhengig virksomheten er av verdien.
Trinn 2: Brukeren må svare på hva slags beskyttelsesbehov verdien har.
Trinn 3: Trusselanalyse - En undersøkelse av potensielle trusler
Trinn 4. En studie av samspillet mellom sikkerhetsbehov og troverdige trusler er ferdig. Systemet hevder å gi brukeren en objektiv vurdering av risikoen.

---

[97] Giannopoulos, G, Filippini, R and Schimmer, M (2012). *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A.* EU- JRC technical notes.
state of the art. Sist besøkt 26.11.2014. http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf

[98] Rand (2006). *Reducing Terrorism Risk at Shopping Centers- An Analysis of Potential Security Options*. http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR401.pdf

Trinn 5: De eksisterende sikringsmålene for å møte de identifiserte risikoene (og ytterligere sikkerhetssystemer kreves) blir deretter identifisert, og nivået av dekningen er igjen hevdes å være "vurdert, og restrisiko gjort eksplisitt."

Styrker ved EBIOS systemet er at (i) du trenger ikke å være en ekspert for å bruke verktøyet. (ii) Det er menybasert og brukeren blir instruert steg for steg hva de skal gjøre og hvordan de skal fylle ut feltene i malen. (iii) I noen trinn er det anbefalt at brukeren konsulterer med fageksperter. (iv) Det er relativt lett å fullføre EBIOS vurdering, den er rask og den er kvalitativ (flere styrker ved systemet er beskrevet i vedlegg E).

Noen av svakhetene ved systemet er (i) brukeren kan ikke gjennomføre "sensitivitetsstudier" og andre kvantitative vurderinger av resultatene. (ii) Det er uklart hvordan usikkerhet blir håndtert. (iii) Det er flere steg som for eksempel 'vurdering av "rest risiko"' og 'sikringstiltak tilpasset risikoen' som brukeren ikke får innsyn i. Dette gjør det vanskeligere for bruken å forstå hva som ligger i risikovurderingen.

Natos arbeid med å skape en felles tilnærming til risikoanalyse for Nato-landene

Etter 11. september 2001 satte Natos "Information Systems Technology Panel" (IST) ned en arbeidsgruppe kalt "Forbedring av felles risikoanalyser"[99] (Nato 2008: 2-1). Funnene fra arbeidsgruppen som ble publisert i 2008 understreker Natos behov for å skape en felles tilnærming til risikoanalyse som Nato-landene kan bruke. I dag bruker Nato-landene ulike tilnærminger til risikoanalyser, definisjoner og kategorier for sårbarheter og trusler. Dette gjør at det blir vanskelig for Nato-land å sammenligne resultater fra sine risikoanalyser.

I dag har Nato flere tilnærminger innenfor ulike tema. Etter et litteratursøk i Natos sine databaser fant vi bl.a. "Manual on Explosives Safety Risk Analysis" og "NATO Risk Management Guide for Acquisition Programmes". Begge metodene er kvantitative og bruker en tilnærming som minner om sannsynlighet og konsekvens-modellen (jfr. NS 5814).

Fra et analysedokument NATO RTO (Research and Technology Organization) ble ulike metoder som ble brukt av flere Nato-land analysert. "Improving Common Security Risk Analysis" inkluderer også en sammenstilling av de viktigste trinnene en fremtidig Nato metode burde ha. Arbeidsgruppen skisserte fire faser/steg som de fleste risikoanalysene har og bør ha:

1. **Bli enig om rammen for risikoanalysen**. Lag tydelige avgrensinger om hva man skal fokusere på. En må lage en utfyllende liste om systemet en skal analysere. For en mer detaljert liste med eksempler se Nato (2008).

2. **Identifiser risiko**. Lag en liste der du beskriver risikoer som systemet ditt er eksponert for (beskrevet i fase 1). Se på sårbarhetene ved de ulike komponentene i systemet. En sårbarhet er "iboende egenskaper hos noe som gir følsomhet for en risikokilde" (SN-ISO guide 73:2009). En risikokilde er et "element som alene eller i kombinasjon har et iboende potensial til

[99] "Improving common security risk analysis"

å forårsake risiko" (SN-ISO guide 73:2009). Trusselaktører med kapasitet og intensjon om å utnytte en sårbarhet blir listet opp. Trusselaktørene og sårbarhetene blir sett opp mot kontrollmekanismene som er tilstede. Ut ifra dette kan en danne seg et bilde av sannsynligheten av reell risiko verdien/systemet ditt er utsatt for. Denne informasjonen vil be behandlet og vurdert i påfølgende trinnene.

3. **Analyser risikoen**. Risikoene identifisert i fase 2 blir analysert i mer detalj. Her skiller man mellom lave og akseptable risikoer, og høy risiko som må bli eliminert eller redusert. Ofte inneholder denne fasen en rangering av risiko som indikerer sannsynligheten for at en sårbarhet blir utnyttet av en trusselaktør og potensielle konsekvenser av dette. Potensielle konsekvenser kan være tap eller degradering av informasjonens integritet, tilgjengelighet og konfidensialitet. Dette blir ofte illustrert i form av 'sannsynlighet og konsekvens' matrise.

4. **Håndtering av risiko**. Her blir det skissert flere tilnærminger (i) risikounngåelse, (ii) risikoredusering[100] der du endrer muligheten av å utnytte en sårbarhet eller endrer konsekvensene av at sårbarhet har blitt utnyttet, (iii) Risikodeling[101] der man fordeler risk med andre parter, (iv) ta risiko for egen regning som innebærer at en aksepterer "den potensielle fordelen ved gevinst eller byrden ved et tap fra en bestemt risiko" (SN-ISO guide 73:2009).

Oppsummering av andre tilnærminger til risikoanalyser

Det ser ikke ut til å være noen fundamental forskjell mellom hva de forskjellige aktørene innen risikoanalyse benytter seg av. Men i alle tilfeller inngår sannsynlighet mer eller mindre eksplisitt i større grad enn i trefaktormodellen. Samtidig ser det ut til at sannsynligheten det dreier seg om er mer en vurdering enn et eksakt tall, og den beskrives mer med ord enn med tall. Ofte brukes "likelihood" i stedet for probability, og på norsk kan "mulighet" brukes i stedet for sannsynlighet. Sannsynlighet kan oppfattes som en statistisk parameter som angis med tall, mens mulighet kan bedre oppfattes som en beskrivelse. Dette er derfor et bedre ord når det er snakk om hendelser som ikke så lett lar seg beskrive statistisk.

Samlet oppsummering av faktorer i forskjellige tilnærminger

Vi har identifisert noen faktorer som bør være til stede i en god tilnærming til risikoanalyser. Tabell B.1 gir en sammenstilling av disse for noen av metodene som er beskrevet her.

[100] "Risk reduction» har blitt beskrevet under risikohåndtering (risk treatment) i SN-ISO guide 73:2009

[101] Nato bruker begrepet "risk transfer», men definisjonen samsvarer med "risikodeling»/"risk sharing» i SN-ISO guide 73:2009.

Method	Is the composition of WG described?	Are all relevant assets identified	Are consequence classes identified?	Are threats identified?	Are safeguards identified?	Are sensitivity studies included?	Is risk acceptance included?	Is the process systematic	Is the process user-friendly	Is the method widely used?	Is the method quantitative or qualitative	Is uncertainty described	Is the method computer based or manual?	Is probability an explicit parameter	Are the results communicated clearly?	Is the assessment process clearly documented
HTRA	Y	Y	Y	Y	Y	Y	Y	Y	N	?	Both	Y	Manual	N	-	Y
CPNI-Pers. Security	Y	Y	Y	Y	Y	N	Y	Y	Y	?	Qualit	?	M	Y	Y	Y
US DHS	?	Y	Y	Y	Y	?	Y	Y	Y	Y	Both	N	Both	N	?	Y
Sandia	N	?	Y	Y	Y	N	Y	Y	?	?	Quant	N	Comp.	Y	?	
Thales (Risk management)	Y	Y	Y	Y	Y	N	Y	Y	?	Y	Quant	N	Both	Y	?	Y
UN	N	Y	Y	Y	Y	N	Y	Y	Y	Y	Qual	N	M	Y	Y	N
EU (Counteract)	N	Y	Y	Y	Y	?	?	Y	Y	?	Qual	N	M	Y	Y	Y
RAND (Butikksenter)	N	Y	Y	Y	Y	Y	Y	Y	N	N	Quant	Y	M	N	Y	Y
EBIOS	N	Y*	Y*	Y*	Y*	N	Y	Y	Y	Y	?	N	Comp.	?	Y	Y

Method	Is the composi-tion of WG described?	Are all relevant assets identified	Are conce-quence classes identified?	Are threats identified ?	Are safe-guards identified ?	Are sensi-tivity studies included?	Is risk accep-tance included?	Is the process systematic	Is the process user-friendly	Is the method widely used?	Is the method quantita-tive or qualitativ e	Is uncertainty described	Is the method computer based or manual?	Is proba-bility an explicit para-meter	Are the results communi -cated clearly?	Is the assessment process clearly documented
Kommu-nale ROS	Y	Y	Y	Y	Y	N	Y	Y	?	Y	Both	N	M	Y	Y	Y
Kraft-for-syning ROS	Y	Y	Y	Y	Y	Y	Y	Y	Y	Spesific for the system	Both	Y	M	Y	Y	Y
Kyst-verkets veileder	N	Y	N	Y	Y	N	Y	Y	Y	Spesific for the system	Qual	N	M	N	Y	Y
DECRIS	N	Y	Y	Y	Y	N	Y	Y	?	?	Both	N	Comp.	Y	Y	Y
NS 5814**	y	Y	Y	?	?	N	Y	Y	Y	Y	Both	N	M	Y	Y	Y
NS 583X-serien**	N	Y	N	Y	Y	N	Y	Y	?	?	Qual	N	M	N	?	Y

Tabell A.2 Oppsummering av metoder og tilnærminger denne rapporten har sett på.

*) If the user answers all questions

**) NS 5814 og NS 5830 er omtalt i kapittel 4.

Vedlegg B Oversikt over intervjuer

Tidspunkt	Hvem ble intervjuet	Bakgrunn
04.11.2014	Sissel Haugdal Jore	Førsteamanuensis og leder av SEROS -Center For Risk Management and Societal Safety, Universitetet i Stavanger (UiS).
05.11.2014	Willy Røed	Konsulent i Proactima, har bakgrunn fra Safety-miljøet og har en PhD fra Universitetet i Stavanger (UiS).
26.11.2014	Terje Aven	Professor fra Universitetet i Stavanger (UiS) og har skrevet mange av de akademiske artiklene brukt i denne rapporten.
12.12.2014	Carsten Rapp	Avdelingsdirektør for Avdeling for sikkerhetsstyring i Nasjonal sikkerhetsmyndighet (NSM).
16.12.2014	Thomas Haneborg	Seniorrådgiver i PST, satt i arbeidsgruppen for NS 5831 og NS 5831.
15.12.2014	Ann Karin Midtgaard	Seniorrådgiver i DSB. Satt i NS 5830-komiteen.
19.12.2014	Stein Ove Bakke-Hanssen	Seniorrådgiver i Nasjonalt kompetansesenter for sikring av bygg, Forsvarsbygg. Har deltatt i Krim 296 gruppen fra starten og vært med i arbeidsgruppene for NS 5830, 5831 og 5832.
06.01.2015	Joakim Barane	Seniorrådgiver og seksjonsleder security risk management i Falck Nutec. Leder av arbeidsgruppen for NS 5830 og sekretær i arbeidsgruppen for NS 5831 og NS 5832. Medlem av Standard Norge Komité SN/K 296. Deltok i arbeidsgruppen for PST under arbeidet med “En veiledning – sikkerhets- og beredskapstiltak med terrorhandlinger”.
30.01.2015	Roy Stranden	Direktør for sikkerhet for medieselskapet Schibsted. Ledet arbeidsgruppen for NS 5831 og NS 5832.

Vedlegg C Intervjuer

C.1 Intervju med Terje Aven

Navn: Terje Aven
Bakgrunn: Professor fra Universitetet i Stavanger (UiS).
Tid og sted: 26. november 2014, telefonintervju

Jeg og flere fra UiS har snakket om kunnskapsbaserte sannsynligheter i mange år, men det er flere fra security-miljøet som ikke skjønner hva dette innebærer eller hva det betyr. De vil ofte forstå sannsynligheter som frekvensbasert der sannsynlighet er "*den relative hyppigheten en hendelse opptrer i en hypotetisk situasjon som gjentas et uendelig antall ganger*". Dette er en total skivebom, det er neppe noen som kjenner risikofaget som mener at man skal bruke frekvensbaserte sannsynligheter på security-området. Dette avslører en manglende kunnskap om risikofaget.

Kunnskapsbasert sannsynlighet, "judgemental probability" eller subjektiv sannsynlighet kan bli brukt, men vi unngår ordet 'subjektiv' ettersom det er så negativt ladet. Så det er den kunnskapsbaserte sannsynligheten vi sikter til når vi snakker om sannsynlighet i denne sammenheng. Sannsynlighet er ikke bare er én ting. Det er i alle fall to fundamentale forskjellige ting – kunnskapsbaserte sannsynligheter som uttrykker usikkerhet og trolighet til den som gjør vurderingen – og frekvenssannsynligheter. For å kunne ha en ordentlig diskusjon må denne forståelsen være på plass. Når noen er negativ til sannsynlighetsbegrepet er det ofte den frekvensbaserte de sikter til. Vi er jo også kritiske til denne forståelsen. Det virker som mange security folk lager en stråmann for å skape et problem, men vi har aldri argumentert for frekvensbasert sannsynlighet.

NS 583X-serien
Det at man har gått vekk ifra sannsynlighetsbegrepet i NS 583X-serien er veldig uheldig. Dette er en stor svakhet. Arbeidsgruppen som jobbet med standardene kunne ha diskutert dette med noen som har innsyn i fagområdet og fått dette belyst i forkant.

Man driver med en form for sannsynlighetsvurderinger om man vil eller ei, det kommer man ikke unna. For eksempel når PST går ut og sier noe om "sannsynlighet for et angrep i Norge", hva betyr egentlig det? Da er en jo inne på betraktninger om sannsynligheter og det er denne type ting vi må få frem. Da må vi ha en plattform på et faglig nivå som holder en viss standard. Kapasitet og intensjon er viktig, det kan forenes med sannsynlighet og kunnskapsstyrke[102]. Dette er viktig poeng, når en kommer med sannsynlighetsbetraktninger må en også snakke om kunnskapen disse bygger på og styrken av denne. Er sannsynlighetsvurderingene basert på sterk eller svak bakgrunnskunnskap? Det er ikke nok å bare se på sannsynlighet. Allikevel kan en komme med en sannsynlighetsvurdering, men da må en si om dette er basert på sterk eller svak

[102] Se Aven, T (2013). "Probabilities and background knowledge as a tool to reflect Uncertainties in relation to intentional acts" in *Reliability Engineering and System Safety* 119 (2013) 229-234.

bakgrunnskunnskap. Hvis det er basert på sterk bakgrunnskunnskap så har sannsynlighetene mer tyngde og da har vi mer interesse av å høre på denne betraktningen. Så det å forstå sannsynlighetsbegrepet og sette det inn i en større kontekst er viktig. Det virker ikke som dette er kjent i sikringsmiljøet. Det er litt pussig - en burde ha gjort en vurdering av relevant litteratur og snakket med fagfolk innen området.

NS 5814 har sine begrensninger, det er viktig å se utover denne tenkningen om at risiko er sannsynlighet og konsekvens. Vi vil ha med usikkerhetsdimensjonen og viktigheten av bakgrunnskunnskapen en baserer seg på. NS 5814 har mange steg og prosessbeskrivelser som er greie og helt standard, men den er ikke helt oppdatert i forhold til fagets utvikling.

Den nye linjen med verdier, trussel og sårbarhet er helt mulig å inkorporere i forhold til vår tenkning og den risikoforståelse som vi argumenterer for og som har en solid vitenskapelig plattform med mange publikasjoner i internasjonale vitenskapelige tidsskrifter på det høyeste nivået. Det er ingen prosessuelle problemer i forhold til dette og ville vært helt naturlig.

Vår tilnærming er at vi ser på en aktivitet (i vid forstand), vi ser på konsekvensene av denne i forhold til de verdiene som er aktuelle. Verdier er helt essensielt. Konsekvenser er hele bildet med trusler, men en må inkludere usikkerhetsdimensjon ved trusler. Dette er jo trusler som er fremover i tid. Tanken om at det er en relevant trussel har jo et risikoaspekt. Sårbarheten er jo gitt at noe har skjedd. De tre dimensjonene verdi, trussel og sårbarhet er helt konsistent med tankemåten vår – der usikkerhet beskrives med redskaper som kapasitet, intensjon, sannsynlighet og kunnskapsstyrke, uten at vi da snakker om frekvenssannsynligheter.
Det trenger ikke være et motsetningsforhold mellom trefaktormodellen og det å sette den inn i en risikokontekst som dekker både safety og security, hvis en bare får frem usikkerhetsdimensjonen i tilstrekkelig grad. Da kan en bruke samme tenkesett, samme strukturer i en bedrift i forhold til all type risikostyring. Men man kan bruke samme fundamentale språkdrakt og prinsipper. Man trenger ikke å snu opp ned på verden her bare fordi en har ulike typer risiko. Spesifikke metoder er selvfølgelig for å analysere risikoene, men det er noe annet.

I NS 5830 definerer man risiko som et "*uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen*", dette må jo være en skrivefeil. Man ser ikke på *forholdet*. Forholdet betyr at en skal dele en trussel på en gitt verdi og denne verdiens sårbarhet;

$$Risiko = \frac{\text{Trussel mot en gitt verdi}}{\text{Verdiens sårbarhet overfor den spesifiserte trusselen}}$$

Dette er ikke gjennomtenkt og det kan umulig være riktig. Jeg synes språkdrakten i NS 5830 er veldig spesiell. Sikkerhet blir definert som "*Reell eller oppfattet tilstand av sikkerhet som innebærer fraværet av uønskede hendelser, frykt eller fare*". Så det er dermed ikke mulig å prate om *grad av sikkerhet* fordi enten har du fravær uønskede hendelser eller så har du tilstedeværelse av uønskede hendelser. Dermed kan man ikke si noe mer enn at man har sikkerhet eller ikke, og ser en framover så er jo dette en ukjent størrelse og begrepet fungerer ikke. Hvis ikke sentrale

begreper er på plass, så blir det bare rot. Det er egentlig tragisk at disse standardene har kommet gjennom.

Hvis en tenker at NS 5814 med sannsynlighet og konsekvens skal gjelde tilsiktede uønskede hendelser så sliter en. Dette er ikke nok og da får en problemer innen security. Men det er ikke den forståelsen av risiko vi snakker om, for oss er denne 'sannsynlighet og konsekvens' forståelsen foreldet, vi ser utover dette. Hvis man bruker den tilnærmingen vi anbefaler så er den konsistent med ISO 31000, og med usikkerhetsdimensjonen så kan man få et rammeverk som kan dekke både security og safety. Men man får ikke til dette basert på den gamle tankegangen om at risiko er sannsynlighet og konsekvens, og sannsynlighet er frekvenssannsynligheter.

Det er flere trekk ved prosessgangen i NS 5814 som er greit og standardisert og på linje med ISO 31000. Men så kommer NS 5830 og roter det til og sier at risikoanalyse er noe mer en risikovurdering. Det er høyst unødvendig at en skal skape en språkdrakt som er inkonsistent med allmenn terminologi i Europa om hva som er en risikoanalyse og en risikovurdering. Konseptuelt er ISO 31000 på et annet nivå enn NS 5814 med tanke på risikoforståelse. En må ha en risikoforståelse som er mer usikkerhetsfokusert skal man lykkes å omforene security og safety, eller så går det ikke.

Det er forskjeller mellom safety og security, men det handler allikevel om risiko i forhold til et eller annet.

Veien videre
Vi trenger et felles rammeverk, en konseptuell forståelse og et apparat som er hensiktsmessig og så må man ha metoder som møter denne utfordringen. For eksempel hvis man snakker om sannsynlighet så må man nevne kunnskapsstyrke og det gjør man ikke i dag, heller ikke innenfor safety. Metodeutviklingen er en kontinuerlig prosess og det kommer hele tiden nye metoder. Vi har en lang vei å gå, men vi utvikler oss videre. Det som er viktigst er at vi har en felles og solid plattform for dette arbeidet slik at utviklingen går den riktige veien. Dette er viktig slik at når noe nytt kommer så kan vi plassere det på en grundig plattform. Hvis det som ligger i bunnen av konsepter og tankegods er vaklende så vil hele bygningen falle sammen. Det føler jeg skjer i vårt fagfelt ettersom man kan sitte i en hjemmesnekret gruppe å skrive ting som ikke er faglig fundert og ikke ta kontakt med de som jobber vitenskapelig med dette.

C.2 Intervju med Sissel Haugdal Jore

Navn: Sissel Haugdal Jore
Bakgrunn: Førsteamanuensis og leder av SEROS -Center For Risk Management and Societal Safety, Universitetet i Stavanger (UiS)
Tid og sted: 4. november 2014, telefonintervju

Debatten på security-området har i Norge intensivert etter 22. juli og In Amenas angrepet. I dag er det flere diskusjoner som pågår innen security-fagfeltet; (i) hva risiko betyr i en security-kontekst, (ii) hvilken risikoanlysemetode man burde bruke, (iii) i hvilken grad en kan bruke

samme fremgangsmåte på safety og security-fagfeltet, (iv) hvordan en skal forstå og bruke begrepet sannsynlighet, (v) hvordan en skal ta høyde for usikkerhet, og (vi) hvordan kommunisere usikkerhet til beslutningstakere.

Safety vs. Security

I Norge i dag er det en tendens til at det er et skille i security-debatten mellom aktører som kun jobber innen security-fagfeltet, og de som også jobber med safety-området. Norsk Standard, PST, NSM og POD har laget standardene og veiledere som bedrifter må forholde seg til, og det kan synes som at de som jobber både innen fagfeltet safety og security er mer kritisk til trefaktormodellen enn de som kun jobber med security. Aktørene innen sikringsmiljøet (security) er ofte fraværende på arenaer i akademia. Jeg skulle ønsket at vi hadde en dialog mellom ulike fagmiljøer. Jeg tror at vi ikke er så uenig som mange innen security-fagfeltet tror vi er. Istedenfor å se på debatten om NS 583X-serien vs. NS 5814 som motpoler hadde vi kommet mye lengre ved å samarbeide og lære av hverandres fagfelt.

"Best practices" og suksesskriterier

Internasjonalt finnes det ikke en rådende "best practice" i metodologien på security-området. Det å sikre seg mot ondsinnede villede handlinger er vanskelige problemstillinger, det er ikke noen som har funnet svaret. I USA har dette temaet vært en del av den akademiske debatten lenger sammenlignet med Norge og resten av Europa.

Utfordringen er at risikoanalysefaget ikke er enkelt. Ledere/brukere/beslutningstakere må ta dette innover seg. Hvis ledere skal ta gode beslutninger så må de forstå usikkerheten og datagrunnlaget som analysen er bygget på. En enkel modell eller et tall er mangelfull. Derfor må ledere sette seg inn i analysene. Dette er spesielt viktig i security- fagfeltet ettersom en ofte mangler relevante data. Et annet aspekt ved den norske diskusjonen rundt security-risikoanalyser er at man i dag tillegger risikoanalysemetoden stor vekt. Det som skjer i etterkant av analyseprosessen, for eksempel hvordan risikoanalysene blir brukt for å fatte beslutninger, er like viktig. Et helhetlig perspektiv er nødvendig. Risikoanalysen må forståes som en del av en risikostyrings- og beslutningsprosess.

Uansett hva slags tilnærming en velger så har man noen generelle suksesskriterier det er viktig å huske på i risikoanalyseprosessen (i) bred ekspertise, målet er å fange opp mest mulig synspunkter, (ii) ha fruktbare diskusjoner, (iii) at bedriften selv skal ha eierskap til prosessen og resultatene i ettertid, (iv) analysene må oppdateres, de skal ikke lages og deretter bli lagt i en skuff, (v) beslutninger må tas på grunnlag av analysen. Ofte er disse momentene undervurdert i risikostyringsprosessen innen security-fagfeltet.

Som nevnt tidligere er det er viktig å innhente forskjellige type kompetanse når en skal gjennomføre en risikoanalyse innenfor security. Det er viktig å kartlegge bakgrunnskunnskapen til personene som skal utføre analysen. Kompetansekravet bør være at man har personer som må kunne noe om security/trusselbildet, og om selve bedriften (sårbarhetene). Dette er viktig for å få til en god analyse.

NS 583X-serien og NS 5814

Det vitenskapelige grunnlaget for trefaktormodellen er mangelfullt, og denne tilnærmingene har ikke tatt innover seg forskningen innen risikoanalysefaget de siste årene.
Det er vanskelig å tenke seg at "one model fits all" innen security-fagfeltet. Man har ikke bare én metode innen safety-faget heller, ettersom det kommer an på hva man skal analysere og hva slags datagrunnlag man har osv. I så måte vil jeg si at det er ikke er mulig å ha "one model fits all". En må bruke ulike modeller og metoder i ulike sammenhenger, og en del av safety-risikoanalysene kan også brukes på security.

Jeg mener at en må tilpasse tilnærmingene/metodene til hva en analyserer, folk må reflektere over hva en risikoanalyse er og hva den skal brukes til, man trenger mer diskusjon og dialog mellom de ulike miljøene. Veldig mange henger fast i en naturvitenskapelig tankegang som vi i risikoanalysefaget har forlatt. Innen security-feltet har en begrenset med data og man kan ikke si noe som er 100% sannsynlighet om fremtiden. Jeg tror det er derfor vi misforstår hverandre. Jeg snakker ikke om matematisk eller statistisk sannsynlighet, jeg snakker om subjektive sannsynligheter. Risiko er en vurdering av fremtiden, ikke et objektivt fakta. Man kan gjøre risikoanalyser selv om man har et begrenset datagrunnlag. Dette blir gjort i dag, f.eks i forhold til storulykker offshore.

NS 5814

Det positive med NS 5814 er at den er (i) enkel å forstå og (ii) den kommuniserer klart prioriteringer som gjør det enklere for lederen å ta beslutninger. Negative trekk ved NS 5814 er at det er en forenkling av virkeligheten. Den "tvinger" folk til å sette risikoen i ulike kategorier og den utrykker heller ikke usikkerhetsmomentet. I tillegg kan en uønsket hendelse ha flere ulike konsekvenser, og i risikomatrisen blir man tvunget til å velge en konsekvens. Det blir dermed forenklet. Siden sannsynlighet er en viktig dimensjon i risikomatrisen, kan man komme til å nedprioritere security-risikoer i forhold til andre risikoer.

NS 583X-serien

De nye standardene har ikke tatt innover seg eksisterende kunnskap fra akademia. UiS har ikke en avklart holdning utad om NS 5830 vs. NS 5814. Personlig er jeg skeptisk til at noen av standardene i NS 583X-serien avviker fra ISO 31000 både i forhold til risikoterminologien og risikoanalysen som en del av den helhetlige virksomhetsstyringen.

NS 5830 bygger på det etablerte synet myndighetene har hatt i noen år. Den fanger opp viktige dimensjoner når en skal gjennomføre risikoanalyser. Positive trekk med trefaktormodellen er at den (i) får bedrifter til å prioritere hva det er de vil beskytte, (ii) fanger opp at verdien er sårbar overfor en strategisk trusselaktør. Dette er gode kvalitative dimensjoner som det er nyttig at bedrifter tar innover seg i sine risikoanalyser. Trefaktormodellen er i seg selv er ikke 'revolusjonerende'; det er de samme stegene, med ulike begrep som overlapper med NS 5814. Jeg savner en debatt om det vitenskapelige grunnlaget NS 583X-serien bygger på, og om hvor vidt de som benytter seg av denne metodikken mener den er mer hensiktsmessig.

Noen svakheter ved trefaktormodellen er:

(i) manglende begrepsdybde, hva er det egentlig som ligger i begrepene? Dette må komme tydelig frem i utfyllende kvalitative beskrivelser for å fange opp hva en verdi er og hvordan den er koblet til trusselaktøren og sårbarhet. Beskrivelse av hvilken intensjon og kapasitet en angriper har overfor en verdi er nødvendig for å fange opp sårbarheten.
(ii) tilnærmingen sier ingenting om usikkerhet. Det finnes mange typer usikkerhet; usikkerhet om faktagrunnlag og kunnskap eller om hvordan trusselbildet utvikler seg osv. Når en bare viser til en "trekant", så kommer ikke usikkerhetsdimensjonen frem.
(iii) hensikten ved trefaktormodellen er at den skal bli brukt i beslutningssammenheng, men modellen sier ingenting om prioritering. En kan bruke sannsynlighet med tall, eller kategorier som "lav, middels og høy" for å gradere risikoen. Hele poenget er at risikoanalysen skal gi beslutningsstøtte slik at man kan prioritere de mest hensiktsmessige tiltakene. I trefaktormodellen er det ingen sannsynlighetsgradering og det blir vanskeligere for beslutningstakere å prioritere hva en skal beskytte osv.

Usikkerhet
Det finnes mange typer usikkerhet for eksempel statistisk usikkerhet. Innen security så blir usikkerhet tolket annerledes ettersom man ikke har et godt nok tallmateriale. Vi må håndtere usikkerhet rundt (i) datagrunnlaget (er det representativt?) (ii) vi skal si noe om fremtiden og usikkerhet rundt vurderingen av hva man tror skal skje (iii) hvor bredt skal vi ta analysene/hva er relevante scenarioer?

Sårbarhetsvurdering vs. risikovurdering
Sårbarhetsbegrepet dekker det som skjer når en krise inntreffer, og hva som skjer etterpå i form av konsekvenser (hvor hardt en verdi blir rammet). Risikoanalyser ser på hele risikoen; altså sannsynlighet for at noe skal skje og konsekvensen. Her bruker en verktøy som grovanalyse, HAZOP, feiltreanalyse osv. Når en snakker med folk som kun jobber innen security-fagfeltet, kan man få inntrykk av noen tror at risikoanalyser er det samme som risikomatrisen - det er det ikke!

C.3 Intervju med Willy Røed

Navn: Willy Røed
Bakgrunn: Konsulent i Proactima, har bakgrunn fra Safety-miljøet og har en PhD fra Universitetet i Stavanger (UiS).
Tid og sted: 5. november 2014, telefonintervju

Safety og security
Jeg har troen på at det er mulig å ha en mer enhetlig fremgangsmåte som kan dekke både safety, security og andre områder på en god måte. Jeg mener at innfallsvinkelen burde være at man har (i) en virksomhet som skal fatte beslutninger, (ii) noen av beslutningene har noe med security å gjøre. Man må ha denne innstillingen istedenfor å begynne med at man har security-problemstillinger som skal løses internt i security-avdelingen. Det er nødvendig å se ting på tvers, å ha begreper som fungerer på tvers i organisasjonen, kunne presentere et risikobilde som kan

sammenlignes med resten av risikobildet en virksomhet står overfor. Ved at ledelsen får et oversiktlig og helthetlig perspektiv på risiko så kan de ta gode beslutninger. Det er dette som er den overordnede hensikten med risikoanalyser - at man skal fatte beslutninger. Derfor kan man ha en fellesprosess for risiko, men det er behov for ulike metoder for selve risikoanalysen. Innen safety bruker en ulike metoder som HAZOP, feiltreanalyse, hendelsestreanalyse, grovanalyse osv. Jeg ser ikke bort ifra at det er behov for ulike, eller andre typer, metoder i security.

ISO 31000 og NS 5814

Det finnes flere standarder som ser på risikostyring i et mer overordnet perspektiv, men ISO 31000 har ofte blitt henvist til de siste årene. Målet er å finne balansen med hva du ønsker å oppnå og hva du ønsker å unngå og som kan true din måloppnåelse. Dette gjelder både tilsiktede og utilsiktede hendelser. NS 5814 ligger ganske nærme ISO 31000. Den er ikke er identisk, noen ting er forskjellig. F.eks. er risikoakseptkriterier tydeligere løftet frem 5814. Definisjonen på "risiko" i ISO 31000 er forskjellig fra NS 5814. Dette er uheldig og det er et tegn på risikofaget er relativt ungt. Jeg vet at når de skrev ISO 31000 endret de definisjonen på risiko helt på slutten. Det er jo nokså drastisk og oppsiktsvekkende når hele standarden omhandler risikostyring. Alt i alt, ISO 31000 og NS 5814 overlapper i stor grad, det handler mest om antall bokser i figurer, men det er i stor grad de samme trinnene.

NS 583X-serien

Jeg synes trefaktormodellen med de tre dimensjonene er logisk og forståelig, men jeg skjønner ikke at dette betyr at en ikke kan si noe om sannsynlighet. Disse faktorene påvirker sannsynlighet. Disse tre dimensjonene blir et slags underlag for å vurdere sannsynlighet. Det er noen ting ved de nye standardene jeg har stusset ved. De snudde på begrepene risikoanalyse og risikovurdering og inkluderte nye begreper som 'ren risiko'. Det er vanskelig for en virksomhet å ha ett risikobegrep i en avdeling og et annet i annen avdeling osv. Dermed blir denne endringen vanskelig i praksis. De har også en annen prosess, det gjør at selve trinnene en skal gjennom når en gjør en risikovurdering er forskjellig. Dette er også en kompliserende faktor. Hvis standardene blir gitt ut som dette så fremstår security som noe forskjellig/annerledes fra resten av risikostyringen. Dette er ikke den rette veien å gå, man burde i så stor grad som mulig se på risikostyring på tvers mellom avdelinger og kompetanseområder i virksomheten. Stikkordet er helhetlig risikostyring.

De positive trekkene med NS 583X-serien er fokus på sårbarhet. Jeg er vant til å tenke at sårbarhetsvurderinger er en del av risikovurderinger. Men mange i safety ser likevel på risiko uten å se på sårbarhet. Alle gode risikovurderinger burde se på og reflektere over sårbarhet. Dette gjelder både for safety og security.

Hvis jeg måtte ha valgt én av prosessene så hadde det vært 5814 ettersom det ligger tettere opp mot ISO 31000. Jeg tror at en kan bruke ISO 31000/NS 5814 både innen safety og security. Det kan hende at selve risikoanalysen trenger forskjellige metoder/verktøy i security enn i safety. Men jeg kan tenke meg at ideen om "verdi, trussel og sårbarhet" kan kombineres med risikoanalyseprosessen i NS 5814 eller ISO 31000. Det trenger ikke å være enten/eller. Jeg kan se for meg at trefaktormodellen kunne bli brukt som risikoanalysemetoden inne i NS 5814

tilnærmingen som et underlag for å vurdere om et angrep kan tenkes å finne sted, det vil si at det kan hjelpe oss å belyse usikkerhets- /sannsynlighetsdimensjonen. Jeg ønsker imidlertid at man bruker sannsynlighetsbegrepet. Man har en verdi, aktør som ønsker å angripe deg og han har kapasitet til å angripe deg, da må det jo være høyere sannsynlighet for at denne verdien blir angrepet. Det er det PST har sagt i dag og mtp. trusselvurdering.

Sannsynlighetsbegrepet
For å kunne få et risikobilde som kan sammenlignes med de andre risikobildene så er det en forutsetning at du kan bruke sannsynlighetsbegrepet. Jeg har forstått at i security er det skepsis mot bruken av sannsynlighetsbegrepet. Men jeg merker meg jo at det er et begrep de bruker også, senest i dag hadde PST pressekonferanse der de brukte begrepet sannsynlighet i ingressen. Det er fordi vi trenger begrepet sannsynlighet for å få frem noen poeng.

Vi trenger å få en bedre fellesforståelse i sannsynlighetsbegrepet. Det har over lang tid vært skarpe skiller mellom safety og security, og det kan ha ført til misforståelser. Hvis vi hadde jobbet litt sammen og sett på begrepet sannsynlighet og fortolkningene så tror jeg man vil se at det er mulig å bruke sannsynlighetsbegrepet i security også. Her tror jeg arbeidet til Terje Aven om subjektive/kunnskapsbaserte sannsynligheter er viktig. Det er veldig sentralt og han har gjort veldig mye forskning med fokus på usikkerhet og sannsynlighet og forståelsen av risiko. Jeg mener at man skal tenke på sannsynlighet som en subjektiv vurdering, og da trenger man ikke statistikk. Jeg jobber med risikoanalyser innen safety, men det er sjelden en bruker tall. Jeg tror vi trenger sannsynlighetsbegrepet og at det er en stor fordel at vi får opp et risikobilde som inneholder sannsynlighet. Men det er ikke nok å bare bruke sannsynlighetsbegrepet. Aven har arbeidet mye med hva som er et godt risikobilde og god forståelse av risiko. Styrke på bakgrunnskunnskap er en viktig faktor. En kan gi en vurdering av sannsynlighet, men så må man si om den er basert på god eller dårlig kunnskap. Jeg tror at flere har sett situasjoner der en har kommet med en sannsynlighet som har vært basert på dårlig bakgrunnskunnskap (dette er ofte tilfellet for sjeldne hendelser) og at en derfor ser på det som vanskelig å uttrykke sannsynlighet.

Hva er de viktigste faktorene for å få til en god risikoanalyseprosess?
Det viktigste er planleggingsfasen, det er suksesskriteriet for å få til en god risikovurdering. Jeg har sett flere ganger at dette er glemt. Som konsulent spør jeg kunden “hva skal du bruke risikovurderingen til?”. Da blir det ofte stille, de har ikke tenkt gjennom hva de skal bruke den til, bare at det er noe som må bli gjort. Nøkkelen er jo at risikovurderingen skal bli brukt som et underlag for å fatte beslutninger, for eksempel å velge blant risikoreduserende tiltak. Dette må en fokusere mer på under planleggingen, dette er kjempeviktig.

Det finnes flere måter å presentere et risikobilde og dermed kommunisere risiko til brukere/ledere. F.eks. risikomatrisen er veldig populær, men den er også skummel fordi den overkommuniserer budskapet ditt. Det kan gi inntrykk av at en kan sette to streker under svaret. Ettersom risiko er en vurdering så er det viktig å få frem (i) forutsetningene og antakelsene som ligger grunn, (ii) metodevalg og hvordan dette kan påvirke, og (iii) styrke på bakgrunnskunnskap, når en presenterer risikobildet. På den måten er man ærlig mot lederen ved å si “Dette er det vi

vet, dette er det vi tror, og dette er det vi antar". Ved å ha en ydmyk presentasjon av risikoen så forstår lederen usikkerheten og dermed oppnås et mer ærlig beslutningsgrunnlag. Ledere er vant til å ta vanskelige beslutninger under usikkerhet. Derfor er jeg skeptisk til voldsom fokus på risikoakseptkriterier der en i praksis flytter beslutningene til analytikeren istedenfor lederen.

Når man skal gjennomføre en risikoanalyse er det viktig at man har noen kompetansekrav til folkene som skal delta. Det er viktig å ha noen i gruppen som er (i) gode i risikoanalysemetoden, (ii) forstår systemet som blir undersøkt. I en gruppe trenger man både metodekompetanse og systemforståelse, ellers blir det dårlig. En person uten risikoanalysekompetanse kan bruke verktøy feil, og dermed komme frem til et beslutningsgrunnlag som er basert på metodiske bommerter. Mens en person uten systemforståelse ikke greier å fange opp viktige elementer som påvirker risikoen. For eksempel når vi gjør kvalitative analyser så har vi to som har gode risikoanalysekompetanse, 7-8 personer som har systemforståelse innen ulike områder.

Fokuserer vi i dag kanskje for mye på metode/metodikk og for lite det som skal være resultatet av en analyseprosess?
Det er selve beslutningen som viktig. Dette er mer enn risikoreduserende tiltak, det kan være å overføre risikoen til andre, akseptere risikoen etc. Du må starte med (i) planlegging, deretter tenke (ii) hva skal analysen brukes til, (iii) hvordan skal vi gå frem og (iv) hva slags risikoanalysemetode/tilnærming skal vi velge for å få et godt beslutningsgrunnlag. Hvis man bruker denne tilnærmingen finner man en god metodisk tilnærming. Hvis man begynner i feil ende og alltid ender med å bruke en lik metode og alltid gjør det likt så kommer du lett i en situasjon der du putter informasjon i en metode som du ikke helt hva skal brukes til.

Hva med risikoaksept/toleranse?
Jeg er prinsipielt forsiktig med å ha slike kriterier, fordi du flytter beslutningen fra den som faktisk har ansvaret og ned på risikoanalytikeren. Man burde ha en metode som tvinger lederen til å sette seg inn beslutningsgrunnlaget og ta en beslutning. Det finnes andre gode metoder som et alternativ til risikoakseptkriterier, for eksempel ALARP-prinsippet.

Om risikoanalyseprosessen i praksis
Når vi har kvalitative analyser med eksperter så bruker vi analyseskjema. Da samler vi en gruppe 5-15 personer, vi har to personer. En leder prosessen, mens den andre noterer og fyller inn analyseskjemaet.

Man kan i mange tilfeller ikke samle folk med ekspertkompetanse mer enn en gang, det er ofte noen praktiske begrensninger. Da må vi tenke hvordan kan vi best benytte denne gruppen. Alle avklaringer om hva som burde være innholdet, formatet, formålet med analysen det gjør vi på forhånd og gjennom kontaktpersonen vår. Analysemøtet tar ofte én dag. Noen ganger bruker vi begynnelsen av dagen på å bli enig om uønskede hendelser. Hvis vi ser at vi kommer til å få det travelt sender vi ekspertene et spørreskjema "questback" på forhånd slik at vi kan få ekspertene til å identifisere hendelser før risikoanalysemøtet. . Dermed bruker vi ikke mye tid på å avklare ting, fokuset er alltid i møte på selve risikovurderingen. Vi har alltid med noen fra kunden, ulike

kompetanser på forskjellige områder basert på hva du ser på. Det er viktig å utfordre ekspertene. Ofte har man med en prosjektleder med eierskap til prosjektet, de ønsker å forsvare sine valg. Da kan det være fornuftig å ta med en annen prosjektleder som kan hans/hennes språk og utfordre hans/hennes standpunkt.

Hvordan ta høyde for usikkerhet?
Det er viktig å være tydelig på hva man mener med begrepet usikkerhet. Det er ikke noe som heter sann risiko. Fra UiS-miljøet er man vant til å tenke at risiko er en subjektiv vurdering. Når en vurderer risiko, sitter man jo egentlig og vurderer usikkerhet. Usikkerhet er veldig sentralt i alle risikovurderinger, det er vanskelig å ta hensyn til dette i praksis. Men man kommer ganske langt ved å kategorisere bakgrunnskunnskap, og si at i dette tilfellet har vi god eller dårlig bakgrunnskunnskap. Du kommer også langt ved å se på utfallsrommet, hva er 'worst case', og hva er 'best case'? Hvis 'worst case' er veldig alvorlig sammenlignet med 'best case', så er det et stort spenn i utfallsrommet og det indikerer stor usikkerhet i hva konsekvensene på verdiene våre kan bli.

C.4 Intervju med Thomas Haneborg

Navn: Thomas Haneborg
Bakgrunn: Seniorrådgiver i PST
Tid og sted: 12. desember 2014, telefonintervju

Debatten innen Security-området
Det er åpenbart at hoveddiskusjonen innen temaet risikoanalyser handler om sannsynlighet, dette har en sammenheng med hva slags metode eller tilnærming man velger til risiko.

Jeg har vært med i arbeidsgruppen til NS 5831 "krav til sikringsrisikostyring" og NS 5832 "krav til sikringsrisikoanalyse". I disse arbeidsgruppene satt representanter fra PST, NSM, Næringslivets Sikkerhetsråd (NSR), Statoil, Standard Norge og Forsvarsbygg. De som startet dette prosjektet i PST videreførte dette arbeidet nesten som privatpersoner ettersom de senere arbeidet i andre virksomheter som Norges Bank, Falck Nutec og Ernst & Young, sånn som Roy Stranden og Joakim Barane.

Gjennom arbeidet med en ny standard er det tydelig at PST har vært en av de største pådriverne for en ny type metodikk. Det har hele tiden vært uttalt at den beste måten å få frem denne metodikken i lyset er å gjøre det til en standard. PST var tidlig ute sammen med POD og NSM med å utvikle veilederen for "sikrings og beredskapstiltak". Veilederen har lagt metoden til grunn for denne standarden. PST er en av hovedaktørene sammen NSM og NSR.

Frontene er mellom den tradisjonelle safety-tankegangen og en security-tankegang som egner seg i større grad for tilsiktede uønskede handlinger. DSB eier på mange måter den siden samfunnsrisikoen, og på mange måter er det de som holder om den tradisjonelle risikotankemetodikken. Da tenker jeg på "Sannsynlighet og konsekvens", altså NS 5814. Vi

hadde ganske stor motstand fra Difi og Finanstilsynet, det var de som møtte opp på høringer og som sendte skriv.

Et "UK-utdannet miljø"

Jeg har forstått at det er flere som har omtalt ledende personer i dette arbeidet som et "UK-utdannet miljø". Dette er sant, jeg er stolt over å si at jeg passer inn i det. Jeg vil påstå at England har den beste tilnærming i dette faget kontra andre land. På universitetet i UK er ikke trefaktormodellen sett på som en sannhet. Dette er i mine øyne en metode som passer best når man snakker om tilsiktede handlinger. Ved å ha brukt 5814 i mange år som "do'er", og før jeg var i England, så har jeg alltid sett at denne tilnærmingen er feil. Regnestykket går ikke opp. Så i mine øyne har ikke nødvendigvis den utdanningen jeg har tatt hatt noe betydning for mine synspunkter, dette er tanker jeg har hatt i mangfoldige år før dette. UK har kommet langt innen kriminologi, jeg vil ikke si at de som brukere av risikometoder har kommet så veldig mye lengre enn oss, men de har kommet mye lenger i å danne et grunnlag for mye metoder. På vårt felt så er engelskmennenes analyser vesentlig enklere, de tar vekk store deler av trusselvurderingsbiten og sier "vi erkjenner at terrorister bruker denne type modus operandi gjennomført med visse kapasiteter" og så ligger dette til grunn for en scenariobasert tilnærming bare for å beskytte verdiene. De har nesten en enda mer forenklet prosess enn vår tilnærming. I NS 5830 legger vi mer fokus på trusselvurderingen og en fremtidig utvikling av moduset til en trusselaktør, vi prøver å se litt mer inn i fremtiden og velge en retning vi antar at trusselaktøren kan gå.

NS 583X-serien vs. NS 5814

Jeg vil si at de mest grunnleggende prinsippene ved NS 5814 er at en baserer seg på historie og empiri. Jeg er ikke negativ til NS 5814, jeg synes det er en fantastisk metode for utilsiktede hendelser der du ikke har mennesker som ønsker å skade deg. Du kan også bruke NS 5814 for tilsiktede handlinger hvis du har et godt nok empirisk grunnlag. For eksempel, på Karl Johan har man kanskje 50 antall ruteknusinger som medfører tyveri av varer fra butikker. Dette kan danne et godt sannsynlighetsgrunnlag for å si når det kommer til å skje med for eksempel din butikk. Da er det flott man bruker denne metoden, men når man kommer til lavfrekvente hendelser så er metoden i mine øyne ubrukelig.

Sannsynlighet er den fundamentale forskjellen. Hvis man har et godt sett med talldata så kan man også benytte 5830-serien. Det vil bare gjøre vurderingene bedre. Dette blir kvalitativt beskrevet og ikke kvantitativt, da er det lettere å forstå den risikoen du tar eller ønsker å unnvike.

NS 5832 gjør at du har et større fokus på verdiene og at du bedre ser hva det er du må beskytte, du vil få frem risikoen på en helt annet måte. Gjør du en grundig verdivurdering så er det kanskje ikke hele butikken du må beskytte, det er kanskje bare deler av butikken. Da er det enklere som objekteier å prioritere hva du skal investere i av sikringstiltak slik at man kan bedre styre risikoen. NS 583X-serien har et vesentlig bedre fokus på verdiene enn NS 5814.

Ved lavfrekvente hendelser der man ikke har talldata så må man inn i NS 5814 metodikken og ta et standpunkt på hvordan man skal sette det inn i regnestykket. Da bruker man mest sannsynlig en

konstant. Altså setter du en sannsynlighet som 0 eller 1 for at noe skal skje. Gjør man det vil man falle ned på et lavere risikotall enn det som kan være virkeligheten. En beslutningstaker vil dermed få et feil grunnlag. I 2012 så ble det regnet ut at sannsynligheten for et terroranslag i Oslo var 0,01% pr. år over 10 000 år. Hvis du setter dette tallet inn i "sannsynlighet X konsekvens" så vil en få et så lavt risikotall i Boston Square matrisen at du nesten alltid ender på grønt eller gult når du legger frem dette for en beslutningstaker. Hvis du sitter som en administrerende direktør eller departementsråd så vil du si at sannsynligheten er så liten at når jeg går av om 5 år så er det en annen persons problem. Hvorfor skal jeg gå ut av historien som den som har brukt 50 millioner kroner på ingenting. Det er til slutt tallene som rår. Hvis du ikke får et godt beslutningsgrunnlag så vil du gå på en smell.

Arbeidet med NS 5830 begynte lenge før terror i Norge, dette har ingenting med 22. juli å gjøre. Dette er en tankegang som har vært lenge i internasjonal kriminologi.

Utfordringene ved å tallfeste sannsynligheter i tilsiktede hendelser

Akademisk så skjønner jeg at DSB prøver å vise til prosenter når de snakker om tilsiktede hendelser ettersom det er vanskelig å presentere det på en annen måte eller at man har valgt en metode så må man gå for det. Men så kommer det store spørsmålet; "hvem er det som skal benytte seg av denne informasjonen?", det er do'erne ute i Norge fra kommunene, stat og i næringslivet. Når DSB gjennom sine kurs i Heggedal sier at "sånn skal det gjøres på bakgrunn av våre tall", så er det disse tallene som brukes på bakken av do'erne. Da får du de skumle valgene basert på dette. DSB kan være bevisst over hva som ligger i tallene og hva slags usikkerhet og nyanser som er forbundet med dette, men do'erne trenger ikke nødvendigvis å fange opp dette.

Utfordringene er at hvis noen setter et stempel på oss som et "UK-utdannet miljø" så må en spørre hvem er Norge-miljøet? Det finnes ikke for vi har få utdanningsretninger innen dette faget per i dag i Norge. Vi har ingen utdannede personer på høyt akademisk nivå innen dette faget fordi vi har ingen retning. Det er en utfordring. Da blir det slik at do'erne der ute, som gjør en god jobb, bare baserer seg på det DSB, PST og andre fagmyndigheter sier. Det er vanskelig å gå mot myndighetene hva myndighetene sier for det finnes ikke nok kunnskap der ute til å motsi det.

Vil du si at det er forskjellige bruksområder for metodene?

Jeg er tilhenger av at man skal ha flere metoder. Det som overrasker meg og den "UK-utdannede gruppen" er at man er så negativ til et nytt verktøy. Istedenfor å si at "det er bra at vi har fått en ny skrutrekker som kan skru inn de nye skruene våre og at verktøykassen blir bedre rustet". Man trenger ikke å bruke den nye skrutrekkeren, men så greit at man har muligheten til det. Her merker jeg at jeg blir irritert når man er så negativ til en ny metode. Det er ingen som sier at dette er et "must" eller et krav, men at dette er det beste verktøy for tilsiktede, lavfrekvente hendelser. Jeg tror at folk er tilbakeholdne fordi de har et kraftig eierskap til en tilnærming eller metode og at det er en redsel for at det synet skal bli borte. Mangel på kunnskap skaper frykt. Det er ingen som har lært at det er flere veier til et mål. På noen mål må en kanskje ta en annen retning for å oppnå det beste resultatet.

Når det gjelder lavfrekvente hendelser og tilsiktede uønskede hendelser så er trefaktormodellen bedre enn en tofaktormodell. Man kan jo si at man har jo overlevd på en tofaktormodell. Er det flaks, eller ikke? Jeg vil påstå at det er flaks. Uansett hvilken analysemodell brukt på regjeringskvartalet før 22. juli så hadde man ikke kunnet avverget hendelsen, men man ville kanskje ha sett utfordringene i annet lys hadde man brukt en trefaktormodell.

Jeg mener at trefaktormodellen kunne vært en "one model fits all" både på safety og security, men ikke omvendt. Når jeg svarer nå så svarer jeg som (i) akademiker, (ii) ansatt i PST som er en av pådriverne og (iii) jeg jobber med spesifikke ting som er lavfrekvente med høy konsekvens. Gjelder det vinningskriminalitet der en har gode tall så kan man bruke 5814, men jeg ville anbefalt å bruke en trefaktormodell.

Sannsynlighet, trolighet, probability og likelihood

Det engelske språket er rikere enn vårt. Sannsynlighet dekker både *"probability"* (matematisk sannsynlighet jfr. gambling) og *"likelihood"* (muligheten, troligheten og sjansen for). Hvis vi hadde hatt norske ord for disse to engelske begrepene så tror jeg mye kunne vært løst. For eksempel, det er helt naturlig å si at i et gitt scenario, basert på historiske hendelser og en antatt retning denne vil trusselen vil gå i fremtiden, så er det mulighet for dette scenarioet vil skje sammenlignet med andre scenarier. Dette er en beskrivelse av "likelihood".

Det er mange i dag som bruker en frekvensbasert sannsynlighet, sånn som DSB. I NRB 2014 referer DSB til at trusselnivået indikerer en form for sannsynlighet. Her står det i NRB (DSB 2014:23) "En trussel kan kategoriseres ut fra stigende sannsynlighet eller trusselnivå"[103]. Dette er interessant for her referer de til en ny metode. Hvor kom dette fra? En stigende sannsynlighet eller trusselnivå, det kan ikke settes i samme bolk mener jeg.

Selv om DSB sier at de ikke bruker frekvens, men kommer med tall og prosenter på sannsynlighet så er det problematisk når du setter ned på do'er nivå. Som do'er leser du det du er opplært til og det er at "sannsynlighet er et tall som du setter i en ligning som du skal presentere i en Boston square". Hadde alle vært akademikere og alle hadde sett på dette her, så hadde vi kanskje skjønt det. Da er vi på et høyere nivå enn do'erne på bakken, der ingen har fått denne input'en i en form for utdannelse på dette feltet. Og hvis du har den input'en da er du antageligvis ikke sikkerhetsfaglig dyktig.

Å kommunisere risiko

Boston square matrisen er veldig enkel å forstå med farger som viser hva som er trygt, usikkert og farlig. Det er lett for ledelsen å ta en avgjørelse, og si at "vi har 10 scenarioer på grønt, og én på rød, og hvor mye koster det å håndtere scenarioet på rødt - jo 10 millioner, fint, fiks det nå". Da har du gjort unna de 5 minuttene du har fått hos direktøren. Denne metoden er brukt og vist så mange ganger at man skjønner den intuitivt.

[103]DSB (2014). Nasjonalt risikobilde 2014. sist besøkt 17.12.2014
http://www.dsb.no/Global/Publikasjoner/2014/Tema/NRB_2014.pdf

En beslutningstaker må nå sette seg ned og ta en avgjørelse basert på noe han må lese, f.eks. en rapport på 50 sider for å forstå "hva er det jeg tar en avgjørelse på". Det er en de tingene jeg synes er bra med 5830-tilnærmingen er at man ansvarliggjør den ansvarlige ettersom han må sette seg inn i dette. Dette handler om risikoaksept og hvis de ikke vet noe om det hvordan kan de ha en klar risikoaksept? Det legger metodikken opp til å gi.

Hva er etter deres vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?

Standardene er et krav til hva du skal følge og hvilke momenter som skal være med. Det er fortsatt ikke laget en veileder på 5830-serien ettersom det er så nytt.

(i) Det absolutt viktigste er å gjennomføre en *god verdivurdering*, dette må gjennomføres av verdieieren selv gjerne med bistand og veiledning. Det er viktig for oss å være med i vurderingen men mer som en sparringpartner. Man kan ha en prosess sammen der en ser verdiene fra et litt annet perspektiv enn verdieieren selv. Prosessforståelse er viktig. Jeg har et eksempel på en kraftstasjon eller vannkraftanlegg. "Er verdien dammen som holder vannet inne? Eller er det røret som leder vannet ned? Er det skovlhjulene som gjør at stangen går rundt til børstene som produserer strøm?". Vi gjorde en analyse der man i alle år hadde trodd at det var dammen som var verdien. Så viste det seg at den kunne jo repareres på to dager, men så fant vi at det var en stålstang som går fra skovlen til børstene som var den viktigste verdien. Hvis denne stålstangen hadde blitt ødelagt så hadde det tatt 9 måneder å produsere en ny ettersom de ikke hadde reserver. De hadde aldri tenkt på dette som en verdi.

Man må ha en prosess der en bruker f.eks. en feiltre-analyse med verdieier, så er det til stor hjelp. Systemforståelsen for du aldri som utenforstående, men du kan få hjelp av verdieieren ved å spørre "hvordan funker dine verdier?".

(ii) Usikkerhet er jo noe man får i etterkant av analyse, usikkerhet er på mange måter en del av produktet av en analyse. En må tenke på de konkrete bolkene en skal gjennom.

(iii) Det å *fastsette sikringsmål* er viktig. På bakgrunn av den verdivurderingen som er gjort av verdieieren så kan man si noe om hva en aksepterer av tap eller ikke. Da er dette et utgangspunkt for den videre analysen.

(iv) På trusselvurderingen er det viktig å si "jeg bryr meg ikke om hvem som utfører handlingen eller hva som er motivasjonen deres", det vi må se på er "hvordan operer de? Hva slags kapasiteter har de? Og hvordan går de på målet?".

Kan helhetsperspektivet på risiko forsvinne når vi har to typer terminologi i NS 5814 og NS 583X-serien?

Vi har hørt dette perspektivet før. De som mener dette går i sin egen felle. En redsel for silotankegang og ikke kunne kommunisere den totale risikoen, det er i mine øyne feil. Går man til næringslivet i dag har man helt klare siloer når det gjelder å gjennomføre arbeidet. Det er på toppen av dette man setter sammen produktet av de ulike delene og ser hva selskapets totale risiko er. Det er utrolig viktig med helhetstankegangen, men man jo kunne åpne for at et fagfelt er et fagfelt og hvordan ser en best på et fagfelt? Det er i hvert fall ikke å generalisere det. Man må

ha spesifikke rammer. Angående terminologien er det viktig å definere begrepene. Jeg tror dette innspillet er frykten for at noe skal overta min skrutrekker (jfr. den tidligere metaforen).

Sannsynlighet i PST

Angående kommentaren til Flesvik om at PST bruker sannsynlighet så er dette basert på et gradert dokument som ble lekket. Når det gjelder sannsynlighet presentert så er det to forskjellige prosesser som skjer. I en utarbeidelse av et etteretningsgrunnlag så bruker man ofte sannsynlighet. Det som ikke kommer frem i innleggene er hva er det man henviser til når man snakker om sannsynlighet. Da bruker man tabeller som er laget på forhånd som sier noe om hva betyr denne sannsynligheten. Vi snakker egentlig om en "likelihood". I en etterretningsprosess som er beskrevet som en Nato-prosess, så er det stort sett bare én vei til Rom og den har blitt gått opp over mange år og de fleste som bruker etterretning bruker den samme metoden. Hadde man sett denne tabellen hadde man sett at det er snakk om "likelihood". Det er bare for å kunne beskrive det sånn at folk skjønner det på et do'er nivå. Når man har gjort denne etterretningsprosessen har man fått et produkt, det er det som legger grunnlaget for en risikoanalyse. Hvis noen, nå snakker jeg ikke om PST, sier at det er 60-90 % sannsynlig med et terroranslag de neste 24 månedene så er det ingen som sier noe om "hvor, når, eller hvordan".

I en risikoanalyseprosess som vi snakker om her, så vil ikke disse tallene bety noe for hvordan man skal legge til grunn for at f.eks. min dørfabrikk på Mysen blir et mål for terror, det jo helt latterlig. Det at terror kan skje i en nasjon kan man kanskje si noe om. Påstandene som kommer frem i DN-innleggene faller sammen fordi man kan ikke bruke disse tallene i en sikringskontekst. Hadde man visst at nå er det 60-90 % sannsynlig med et terroranslag for at oljebransjen blir angrepet innen 12 måneder da hadde det vært noe annet, men det vet man ikke.

Folk flest oppfatter sannsynlighet som tall. Skal du begynne å differensiere mellom kunnskapsbasert sannsynlighet og frekvensbasert sannsynlighet så må dette igjen beskrives for folk flest, slik at de skjønner hva som ligger i det. Vi er igjen tilbake på det fattige norske språket. Jeg bruker "mulighet for" eller "sjansen for". Ser man på historiske terrormål er det større sjanse for at større menneskemengder blir angrepet enn en enslig person på Hardangervidda. Hvis man hadde sagt at det er en større sannsynlighet for det hadde folk spurt "hva er sannsynligheten? Gi meg en prosent". Beslutningstakeren vil basere seg på tallet som man forventer å få når man bruker begrepet sannsynlighet, slik at han kan putte dette tallet opp i mot bunnlinja på sitt eget regnskap. I en sikringssammenheng så er det det kommer an på. I bunn av 5830 er spørsmålet "ønsker du at dette skal skje med dine verdier, eller ønsker du det ikke". Dette kan skje i morgen eller om 10 000 år, men det kan skje. Dette skaper en bedre type sikring.

Avsluttende refleksjoner

Vi kan synes hva vi vil om metodikk og ulike tilnærminger. Det som mangler er at man har nok mennesker til å forstå hvorfor det er som det er. Man må ha en viss type grunnutdannelse slik at man har muligheten til ikke å tenke som "UK-gutta", men da må man også kunne argumentere for det på en god måte. I Norge mangler vi en høyere akademisk utdannelse på security risk management.

C.5 Intervju med Ann Karin Midtgaard

Navn: Ann Karin Midtgaard
Bakgrunn: Seniorrådgiver i Enhet for analyse i Direktoratet for Samfunnssikkerhet og Beredskap (DSB) og satt i komiteen som utarbeidet NS 583X-serien.
Tid og sted: 15. desember 2014, telefonintervju

Debatten innen Security-området
Sånn som jeg leser det handler debatten om den ulike forståelsen av begrepet sannsynlighet. Det kom fram i diskusjoner i NS 5830-komiteen og i debatten som har vært i Dagens Næringsliv etter at standarden kom ut. Det er tydelig at ulike aktører legger forskjellige ting i begrepet sannsynlighet. Det som låser diskusjonen er imidlertid når man tillegger alle andre samme forståelse av sannsynlighet som man selv har - uten å sjekke om dette stemmer.

Det kom tydelig fram i komiteen, både skriftlig og muntlig, at de som argumenterte for den nye risiko-definisjonen i 5830-standarden (som ikke inneholder sannsynlighet) oppfattet sannsynlighet som frekvens (gjentakende hendelser) og tilla alle andre samme oppfatning. Det ble hevdet at bruk av sannsynlighet forutsetter statistikk og at historien gjentar seg. Dette er etter mitt syn en gammeldags forståelse av sannsynlighetsbegrepet som stammer fra før årtusenskiftet og som baserer seg på gamle lærebøker der "risiko = sannsynlighet X konsekvens" - et enkelt tall. Det er lenge siden de mest fremtredende risikomiljøene gikk vekk ifra denne enkle sannsynlighetsforståelsen. Det ble også hevdet at DSB bruker en frekvensbasert sannsynlighet. Det er en oppfatning noen har fått en gang i tiden, og så har man ikke sjekket ut med virkeligheten om dette stemmer.

DSB sin forståelse av sannsynlighet
I DSBs Nasjonalt risikobilde (NRB) definerer vi sannsynlighet som hvor trolig det er at en hendelse skal inntreffe (likelihood) og så bruker vi et tidsintervall som mål på det. Vi bruker ikke returperioder eller frekvenser ettersom vi ser på svært alvorlige engangshendelser i NRB. Da er vi veldig nærme den betydningen man legger i en trusselvurdering; "hvor trolig det er at en hendelse skal inntreffe". Jeg har hørt at DSB selv glipper på definisjonen av begrepet, men nå er vi veldig nøye på dette i NRB: vi sier ikke én gang hvert 300. år, vi sier bare én gang i løpet av 300 år. Dette er nyanser vi er ekstremt bevisst på, men som andre kanskje ikke er. Grunnen til at vi bruker et tidsintervall er for å tallfeste/konkretisere sannsynligheten for hendelsen; for eksempel hendelse X kan skje i løpet av en 100-årsperiode, mens en hendelse Y kan skje i løpet av en 1000-årsperiode. Da er hendelse X mer sannsynlig enn hendelse Y. Vi er nødt til å bruke en tidshorisont.

Når man vurderer sannsynlighet og konsekvenser så er det som å legge et puslespill med brikker av kunnskap hentet fra ulike hold. Det kan være tilsvarende hendelser som har skjedd andre steder, modeller for jordskjelv og andre naturhendelser eller ny forskningsbasert kunnskap. Du setter sammen de bitene av kunnskap som finnes og så gjør man seg opp en mening som sannsynlighet. Vi sier konsekvent at vi *angir* en sannsynlighet fremfor *å anslå* en sannsynlighet. Det uttrykker tydeligere at det er *noen* som angir den. I NRB 2014 angir vi sannsynlighet også

for tilsiktede uønskede hendelser [104]. Det gjorde vi ikke i 2013 fordi vi følte at motforestillingene var sterke, særlig fra PST. I år har vi valgt å angi sannsynlighet også for disse hendelsene, slik at de kan presenteres i samlet risikomatrise sammen med de utilsiktede hendelsene. Hovedbegrunnelsen vår er at både en sannsynlighetsvurdering og en trusselvurdering sier noe om hvor trolig det er at en hendelse vil inntreffe. Det er ikke nødvendigvis enklere å angi sannsynlighet for en utilsiktet hendelse enn en tilsiktet.

I NRB 2013 innførte vi usikkerhetsbetraktninger ved vurderingene basert på kunnskapsgrunnlaget de bygger på (inspirert av Terje Aven ved UiS). Nå er DSB mer eksplisitte på usikkerhet også i veiledere til f.eks. FylkesROS og Helhetlig ROS i kommunene.

Sannsynlighetsbegrepet og ulike forståelser av begrepet

Det er utfordrende at visse miljøer forstår og definerer sannsynlighet som en historisk frekvens – og tror at alle andre gjør det samme. Det er imidlertid ikke vanlig forståelse på samfunnssikkerhetsområdet. Selv i sektorer med mye tilgjengelig data, som veisektoren, legger man mer enn bare historiske frekvenser i sannsynlighetsbegrepet. Man har flere faktorer og indikatorer på risiko enn bare tidligere hendelser. På slutten av arbeidet med NS 5831 og 5832 opplevde jeg også en større forståelse for at sannsynlighet kan angis på et bredt, kvalitativt kunnskapsgrunnlag.

PST var ikke representert i komiteen som utarbeidet NS 583X-serien, men det var to-tre personer med felles utdanning fra UK og bakgrunn fra PST. Jeg er ikke sikker på i hvilken grad denne gruppen representerer PST i dag. PST har nok sin metode som de bruker uavhengig av de nye standardene. Det som er litt rart er at PST ved flere anledninger det siste året muntlig har brukt begrepet sannsynlighet, men ikke vil gjøre det i sine trusselvurderinger. Jeg har vanskeligheter med å forstå hvordan man kan unngå å vurdere sannsynlighet i risikovurderinger eller trusselvurderinger.

NS 583X-serien og NS 5814

En grunnleggende forskjell mellom de to tilnærmingene er bruken av sannsynlighet. Det gir i mine øyne risikovurderinger iht. NS 5814 og NS 5832 ulik tidshorisont. Uten bruk av sannsynlighet som en tidsangivelse, blir risikovurderingen et øyeblikksbilde. Risikoen er slik i dag, men i morgen kan den være annerledes. Med en svært kort tidshorisont (uker eller måneder) er det selvsagt veldig krevende å si noe om sannsynligheten for at en hendelse skal inntreffe. Det er lettere hvis man utvider tidshorisonten til noen år eller ti-år. Er det ikke slik at en trusselvurdering kan endre seg raskere enn en sikringsrisikovurdering, siden verdier og sårbarhet er mer stabile faktorer enn trusselen? Da kan man kanskje ha en lengre tidshorisont for risikovurderingen enn for trusselvurderingen.

[104] DSB (2014). Nasjonalt risikobilde 2014. Sist besøkt 16.12.2014

Er det noen klare positive/negative trekk ved NS 5814? Er det noen klare positive/negative trekk ved NS 5830?

Her har jeg ingen sterke oppfatninger ettersom jeg tror jeg kunne brukt begge modellene og fått samme type analyseresultat fordi jeg legger tilnærmet samme betydning i begrepene som brukes. En ting jeg mener ikke skiller tilnærmingene er antall "faktorer" eller dimensjoner som inngår i risikobegrepene. Riktignok blir "sannsynlighet og konsekvens"-tilnærmingen av enkelte kalt en "tofaktormodell", mens NS 5830-modellen kalles "trefaktormodell". Den skal dermed omfatte mer enn "tofaktormodellen" og være mer generell og anvendelig. Risikobegrepet de fleste bruker – inklusive DSB - har fire dimensjoner (i) sannsynlighet, (ii) konsekvens, (iii) sårbarhet, og (iv) usikkerhet.

Jeg synes NS 5814 er romslig nok til å kunne brukes. Du er nødt til å finne din måte å gjennomføre analysene på innenfor det beskrevne rammeverket og handlingsrommet som ligger der. I forordet til NS 5814 står det at den kan brukes både for tilsiktede og utilsiktede hendelser. Vi bruker også figuren i ISO 31 000 for å vise hvordan de ulike vurderingene og analysen henger sammen. Det er fullt mulig med en felles tilnærming til risikoanalyse både på safety- og security-området, og så kan man ha ulike veiledere som er tilpasset ulike sektorer og problemstillinger. I arbeidet med NS 583X-serien var DSB mest skeptisk til at arbeidsgruppen ga etablerte og definerte begreper i andre standarder et nytt innhold. Det var grunnen til at vi gikk imot utgivelse av standardene i første omgang ettersom det ville vanskeliggjøre all kommunikasjon om risiko og risikoanalyser. Derfor ble løsningen til slutt i NS 5831 og NS 5832 at en konsekvent bruker "sikringsrisiko" istedenfor "risiko". Det er et helt nytt begrep som ikke er definert i andre standarder tidligere. Dermed kunne de definere begrepet.

I NS 583X-serien hadde man opprinnelig byttet om på (i) risikoanalyse og risikovurdering, og (ii) risikostyring og risikohåndtering, i forhold til hvordan disse begrepene brukes andre steder. Dette er delvis endret på i de utgitte standardene. Jeg har imidlertid fått spørsmål om "hvordan skal vi forholde oss til alternative standarder for risikoanalyse?" og "hva i all verden er sikringsrisiko?". Vi har også fått henvendelse fra konsulenter som ser de faglige utfordringene i å skulle bruke to metoder for risikovurdering innenfor samme virksomhet. Hva da med den helhetlige risikostyringen?

Hvordan kommunisere risiko til brukere/ledere

Det jeg har sans for er en viss standardisering av presentasjonen av analyseresultatene innenfor samme område og nivå. Det synes jeg langt på vei at vi har klart i NRB. Der har vi standardiserte tabeller, forhåndsdefinerte intervaller for sannsynlighet, konsekvenstyper osv. Det må være mulig å sammenlikne risikoen knyttet til ulike hendelser. I utarbeidelsen av veileder for ROS-analyse i kommunene har vi brukt tid på å utvikle et skjema som angir fremgangsmåten i analysene, rekkefølge på stegene og et konsistent presisjonsnivå. De som skal gjennomføre analysene blir ved å bruke skjemaet veiledet til å (i) konkretisere, (ii) kvantifisere, (iii) si noe om forutsetningene for anslag og (iv) hele tiden begrunne, (v) kartlegge usikkerhet basert på kunnskapsgrunnlaget, (vi) vurdere sårbarhet og hvilke kritiske samfunnsfunksjoner som berøres av hendelsen osv.

Hva er etter deres vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?
(i) *Strukturen er viktig* med klare trinnvise steg som det er enkelt å gjennomføre. Dessuten er det visse vurderinger som må med for å kunne kalle det en risikoanalyse.

(ii) Kommunikasjonsmessig er det viktig å *presentere resultatene relativt likt* slik at man kan få et oversiktlig helhetsbilde.

(iii) I analysene må man grave *dypt* nok i problemstillingene. Det blir ikke gode risikoanalyser av å surfe på overflaten av et fagfelt. Man kan ikke bare lese seg opp på gamle risikovurderinger. *Du må bli møkkete på henda* og gjøre et dypdykk i fagområdet du studerer ettersom du er nødt til å få en *systemforståelse*. Du må skjønne hvordan ting henger sammen for å finne kjernen i problemet. Derfor bruker vi bortimot ett år på hver risikoanalyse i Nasjonalt risikobilde nå. Det er mange vi må snakke med og mye som skal sjekkes og kvalitetssikres for at vi skal tørre å trekke egne konklusjoner og ikke bare basere oss på hva andre sier. Jeg mener at dette er avgjørende for troverdigheten og nytten av analysen.

(iv) *Konkretisering* er en suksessfaktor. Det er f.eks. ikke tilstrekkelig å si at togtrafikken er avhengig av ekom. Avhengigheten må forklares og synliggjøres. For eksempel at lokomotivførere er avhengig av mobiltelefon for å kommunisere med togledelsen. Ved bortfall av ekomtjenester faller mobilnettene ut og alle tog må stanse uten kommunikasjon mellom lokfører og togledelse.

(v) Et kvalitetstegn ved risikoanalyser er *tydelige resonnementer*. Disse må med i presentasjonen av analyseresultatene for at de skal være etterprøvbare. Presentasjonen av en risikoanalyse bør invitere leseren til selv å trekke konklusjoner ved å lese resonnementene.

Disse suksesskriteriene er metodeuavhengig, de gjelder uansett hvilken standard du forholder deg til. Det er dette som er det viktige. Standardene er ikke noen metodebeskrivelse, det gir bare noen knagger og referanser. Du er nødt til å gjøre mange valg innenfor en standard.
Jeg synes noen har en overdreven tro på at bestemte metoder og standarder kan sikre kvaliteten på en analyse. Jeg mener at analysekompetanse er noe langt mer enn dette.

C.6 Intervju med Stein Ove Bakke-Hanssen

Navn: Stein Ove Bakke-Hanssen
Bakgrunn: Seniorrådgiver i Nasjonalt kompetansesenter for sikring av bygg, Forsvarsbygg. Har deltatt i Krim 296 gruppen fra starten og vært med i arbeidsgruppene for NS 5830, 5831 og 5832.
Tid og sted: 19. desember 2014, telefonintervju

Debatten innen Security-området og bruken av sannsynlighet
Jeg synes det er mye kunstige fronter og mye uenigheter over småting. Debatten går veldig på bruken av sannsynlighet, men dette synes jeg er en avsporing ettersom tilnærmingen man velger enten om det er NS 5814 eller NS 5832 består av kvalitative vurderinger hele veien og vurderinger av sannsynlighet.

Alle disse standardene er et overordnet hjelpemiddel. FB har brukt en kvalitativ, kunnskapsbasert sannsynlighet (*likelihood*) i mange år, også i den gamle metodikken. Mye av kritikken på sannsynlighet har gått på tallfestingen. I Forsvarsbygg har sannsynlighet hovedsakelig vært en kvalitativ gruppering og ikke noen tallfesting eller frekvenser.

Deltakelse i NS 583X-arbeidsgruppene

Når jeg satt i 5832-arbeidsgruppen har flere aktører kommet med angrep uten at det er noe faglig innhold. Kritikken går kun på at vi har feil definisjon på risiko. Det finnes bøtter og spann av metodikk og ulike tilnærminger til risiko, det er helt frivillig i hvilken grad man skal velge å bruke de forskjellige standardene og modellene. I tidligere analyser sier vi at "vi baserer oss på" NS 5814 og andre relevante tilnærminger fra f.eks. NSM. Vi kunne med den gamle tilnærmingen med tilpasninger sagt at "vi baserer oss på" NS 5832 uten at det ville være direkte feil. Man må alltid tilpasse tilnærmingen til hva en vurderer.

Kampen om NS 5830-serien skulle stått for to år siden når Standard Norge (i NS 5830) definerte risiko annerledes enn i NS 5814, men da ble ikke endringen fanget opp.

Det er Roy Stranden som i stor grad har drevet frem den nye standarden, uten han som pådriver er det tvilsomt om standarden hadde hatt den formen som den har i dag. PST og NSM tok tidlig stilling til trefaktormodellen. I "Veileder. Sikkerhets- og beredskapstiltak mot terrorhandlinger" som ble utgitt av Nasjonal sikkerhetsmyndighet, Politidirektoratet og Politiets sikkerhetstjeneste i 2010. Det er enkeltpersoner som har frontet denne saken i media. Jeg har merket meg at de som har mest bastante meninger, både positive eller negative, ofte er folk som ikke nødvendigvis har jobbet tett med risikoanalyser. Det er de som lager disse frontene i debatten.

I møter jeg har vært i der det har vært høy temperatur drar kritikerne frem definisjonen på risiko. Der de mener at risiko er sannsynlighet og konsekvens og alle som mener noe annet har feil. Jeg føler at kritikerne ikke har vært konstruktive ettersom vi har spurt hva som er feil med tilnærmingen og så har de holdt på sitt om at "risiko er sannsynlighet og konsekvens". Det har ikke vært kritikk av selve metodikken bare at vi har en "feil forståelse av risiko". Da har vi sagt at frekvens ikke er riktig å bruke i security analyser, hvert fall ikke på terrorscenarioer. Jeg bruker og snakker om sannsynlighet som frekvens, men vi har ikke hatt en ordentlig diskusjon om dette internt i gruppen.

Vi prøvde å si til kritikerne at dette er bare en tilnærming blant flere tilnærminger til risikoanalyse. Det er valgfritt å bruke og det er tenkt at dette bare skal bli brukt på tilsiktede uønskede handlinger. Faggruppen og sikkerhetsfolk som jobber med tilsiktede uønskede handlinger har behov for en annen tilnærming enn vi har i dag. Mye av prosessen ble preget av diskusjoner på personnivå, dette gjelder begge sider.

Hvor står du i denne debatten?

Jeg er mer pragmatisk i denne debatten, jeg synes det er kunstige fronter. Jeg har jo tidligere jobbet mye med NS 5814. Jeg har vært uenig med PST, som i alle fall i en periode har ment at

sannsynlighetsbegrepet var bannlyst eller et "fyord", jeg tror PST sine sterke meninger på dette påvirket deltakerne i arbeidet. Det er ikke mulig å velge ut scenarioer uten en implisitt sannsynlighetsvurdering. Selv om man ikke bruker "sannsynlighetsbegrepet på papiret" så gjør man det hele tiden underveis. Den nye tilnærmingen består jo bare av kvalitative vurderinger og du vurderer jo ut ifra sannsynlighet i stor grad. I tidligere utgaver av standarder stod det tydelig at sannsynlighet ikke må brukes, men nå har den blitt rundere i formen. Hvis du har tall og statistikk, så kan du bruke det.

NS 5832 er jo bare overordnete bokser og sier ikke noe om hvordan man skal gjennomføre risikoanalysen i praksis. Min store utfordring er boksene med vurdering av risiko og presentasjon av risikobildet. Disse sier bare at verdi, trussel og sårbarhet skal vurderes og bli kommunisert klart. For meg er allikevel sannsynlighet og konsekvens sentrale begreper i en risikoanalyse modell. Jeg ser for meg en modell som i en viss grad benytter sannsynlighetsbegrepet og allikevel si at den er basert på NS 5832. Når jeg snakker om sannsynligheten tenker jeg på den mer kvalitative forståelsen av sannsynlighet (likelihood) og ikke den frekvensbaserte sannsynligheten. Vi bruker en skjønnsmessig sannsynlighet for å kunne prioritere tiltak. Sannsynlighet for meg er ofte en tallverdi fra 1-5. Her bruker vi kunnskapsbasert sannsynlighet der vi trekker på teori, empiri og statistikk hvis det er tilgjengelig.

Våre tidligere risikovurderinger/-analyser basert på NS 5814 er ikke så sporbar eller etterprøvbar i forhold til vurderingene som er gjort. NS 5832 har en mer rød tråd gjennom analysen. I den tidligere tilnærmingen var sårbarhet kamuflert. Sårbarheten kom ikke godt nok frem. I NS 5814 kom risikoakseptkriteriene før analysen startet, mens i NS 5832 skal sikringsmål vurderes både i startfasen og mot slutten av analysen. Som praktikker ser jeg problemer i at analysen ikke avsluttes med anbefaling av tiltak, men at analysen omfatter også både revurdering av sikringsmål og beslutning av akseptabel risiko og valg av tiltak som skal implementeres. Dette representerer en idealverden, men det er generelt ekstremt vanskelig å få beslutningstakerne til å si noe om risikoaksept. Den nye tilnærmingen legger mer opp til at lederne må si noe om risikoaksepten. Man kan si at NS 5814 er ren safety, eller hendelsesbasert, men igjen må det bli sagt at NS 5814 og NS 5830-serien er overordnede bokser der en gjør tilpasninger. En typisk formulering er ofte at en "baserer seg på" standarder, ikke at det er i "henhold til" ettersom det ofte er tilpasninger og justeringer jevnt over. I praksis vil antagelig de fleste 5832 analysene være delt i to. Analysen "avsluttes" etter tiltak og akseptabel risiko og valg av tiltak gjennomføres adskilt.

Med den nye tilnærmingen vet man ikke hvordan man skal presentere risiko. Fordelen med NS 5814 og Boston square med sannsynlighet og konsekvens er at enhver leder er vant til dette og brukt det i flere sammenhenger. Det er en utfordring at man ikke har presentert en modell på dette, dette har blitt diskutert mye. Skal risikoen bli beskrevet skriftlig, eller skal man ha en enkel figur med røde firkanter osv. Jeg foretrekker tabeller og tall, uten for lange utredninger. Det skal selvfølgelig være en rød tråd i analysen, men det folk flest leser er konklusjonen og tiltak. Sånn sett er 5814 å foretrekke der du får en "rød-effekt" der folk skjønner uten forklaring at rødt ikke er bra. I hvilken grad en får til dette i 5832 vet jeg ikke, men det er ikke noen klare fine løsninger per dags dato. Jeg synes vi skulle hatt noen alternative løsninger på hvordan en skulle presentert

risikoen før en gikk ut med standardene. Det er egentlig ingen som er uenig i de andre boksene der en skal identifisere verdier, trusler og sårbarheter. Kampen står egentlig om hvordan en skal presentere risikobildet. Det at vi at sier at en må presentere det på en helt annet måte i den nye standarden, uten å si hvordan en skal gjøre dette er problematisk. Hadde vi hatt en fin visialisering av risikobildet klar hadde vi antagelig sluppet mye av kritikken som har blitt rettet mot NS 5830-serien.

Utgangspunktet for den nye standarden var at man ikke skulle bruke den frekvensbaserte sannsynligheten. Jeg har argumentert for at vi skulle bruke sannsynlighetsbegrepet i tilnærmingen, med den forståelsen at det er kunnskapsbasert sannsynlighet, men det fungerte ikke. Det er en av utfordringene med utviklingen av standarder at alle må bli enige. Internasjonale standarder blir ofte dårlige fordi de blir utvannet. Sånn sett har 5830-arbeidsgruppen vært bra ettersom det har vært få deltakere med faglig konsistente meninger. Så derfor har det ikke blitt så utvannet som mange internasjonale standarder. Vi sendte standardene på internhøring før den ble offentliggjort, jeg mener at flere miljøer var på listen med bl.a. Terje Aven fra UiS, men jeg kan ikke huske at vi fikk noen innspill. Aven var i alle fall nevnt som en viktig aktør som vi burde sparret med underveis i prosessen.

Avslutningen på NS 5831/5832 har vært en litt rar prosess ettersom godkjenningen ble stoppet og Standard Norge tok med seg halvparten av arbeidsgruppen videre. Jeg ble misfornøyd når jeg så alle de nye begrepene som ble tatt inn; sikringsrisikoanalyse! At sikring hadde blitt lagt til diverse begrep bryter med prinsippet vi hadde når vi lagde definisjonene i 5830 for et par år siden. Jeg er overrasket over at det ble gjort såpass store endringer, men skjønner at de nye begrepene var et kompromiss for å få ut standardene.

Vi har diskutert begrepene mye i arbeidsgruppen. Vi har følt at problemene ofte er dårlige engelske oversettelser i tidligere standarder. Mye av det som har kommet i ISO-standarder har blitt oversatt av en som er veldig flink i engelsk, men som ikke nødvendigvis spesial kompetanse innen fagfeltet. En del av problemene kunne vært løst om begrepene hadde vært godt nok oversatt tidligere. Spørsmålet var om vi skulle ta kampen nå? På møte med Standard Norge har jeg også informert at det var mye utfordringer innen security-feltet fordi standarder som har kommet internasjonalt blir ordrett oversatt til norsk. Det er en del nyanser som har forsvunnet.

Den gamle metodikken baserte vi på 5814. Hvis jeg skulle basert meg på den nye standarden ville jeg ha inkludert et nytt kapittel om sårbarhet og inkludert deler fra objektbeskrivelsen og trusselvurderingen. Sånn sett blir det mer ryddig og en bedre tråd gjennom analysen. Ellers er ikke noen nye bokser for oss. Det som er den store utfordringen er hvordan vi skal presentere risikoen.

Vil du si at det er forskjellige bruksområder for metodene?
Jeg mener at begge disse standardene er så overordnede at de kan brukes til både safety og security. Når jeg har brukt 5814 har jeg ikke brukt en frekvensbasert sannsynlighet. NS 5814 sier ikke at det må være frekvensbasert sannsynlighet man viser til. Den store forskjellen er hvordan

en vurderer risikoen mtp. risikoaksept. I 5814 kommer en med risikoaksept før analysen og det fungerer som et fasitsvar gjennom analysen. Mens i 5832 så skal den vurderes underveis og revurderes. Det høres mer riktig ut fra mitt ståsted.

De som jobber med security brukte nok ofte allerede før 5832 en kunnskapsbasert sannsynlighet og ikke frekvenssannsynlighet. Utfordringen for oss som arbeider med risikoanalyser og spesielt de som gjør dette en sjelden gang uten noe særlig erfaring er ikke de overordnede standardene. Å sette seg ned å gjennomføre en analyse kun basert på standardene er vanskelig. Man har behov for en modell som beskriver hvordan analysen i praksis skal gjennomføres. Antagelig er de fleste helt uinteressert i standardene. Det de trenger er nivået under, en modell/veileder som leder de gjennom trinnene i analysen uten at de nødvendigvis må ha spesialkompetanse. Det er veilederen som har stor innvirkning og den gruppen du setter sammen som skal gjennomføre risikoanalysen er helt avgjørende.

Finnes det noen rådende ”best practice” i metodologien på security-området? Er det noen land eller organisasjoner som har kommet spesielt langt?
Vi forholder oss mye til britene på vårt fagfelt. De har mange bra sjekklister, men på risikoanalyser er jeg mer usikker. Jeg har akkurat tatt et masterstudie på BI og var imponert over it-konsulentfirmaene og hvor strukturert metodikken deres var spesielt på trusselscenarioer. IT-risiko har et veldig bra utgangspunkt. Men analysen blir ikke bedre enn de som utformer analysene. Det så i alle fall bra ut på papiret. På IT-risikohåndtering føler jeg at de har kommet lenger.

Hvordan burde en kommunisere risiko til brukere/ledere som ikke er eksperter?
Risikostyring er komplekst. Det er ett av de store problemene å presentere risiko til lederne. Security er et sært, lite fagområde, det passer ikke inn i resten. For at det skulle bli bra måtte security inn i firmaets mål sånn at ledelsen ble målt på dette. Sånn som det er nå er enhver risikoanalyse enkelttilfeller som må vurderes når det dukker opp, det gjør det vanskelig å sammenligne. Kommunikasjon er derfor en stor utfordring ettersom sikkerhet blir mer ‘ad hoc’ og ikke en del av det fortløpende arbeidet. Dermed faller det utenfor, det er ofte enkeltanalyser som blir bestilt som man gjerne har blitt pålagt til å gjøre. En utfordring for meg er at jeg mister kontakten med analysen når den ferdigstilles, med beskrivelse av anbefalte risikoreduserende tiltak.

Ofte kan det se ut som det ikke skjer noe etter at en analyse er gjennomført. Jeg håper da at arbeidet pågår men tar tid eller at noen bevist har akseptert risikoen. Det viktigste er at ansvarlige ledere informeres om risikoen og tar beslutninger i forhold til denne. Sikkerhetsloven åpner for at man i stor grad kan akseptere risiko så lenge man har vurdert den. Lederforankring gjennom analysearbeidet er imidlertid avgjørende for at analysen følges opp i etterkant.

Hva er etter din vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?
Sammensetningen av arbeidsgruppen er viktig for om det blir en bra analyse eller ikke. Det er involveringen av beslutningstakerne som er det avgjørende punktet om det skal skje noe eller ikke. I FB kan dette være utfordrende siden vi til dels er på utsiden og prøver å involvere de vi lager analyser for. Vi vil at de skal gjøre mer enn bare å lese sammendraget. Sånn sett er det forskjell på 5814 og 5832 ettersom 5814 krever beslutninger før arbeidet, mens i 5832 kreves det at beslutningstakerne er med underveis, og at risikoaksepten revurderes. Dermed løftes det opp til ledelsesnivået. NS 5832 prøver å legge til rette for mer involvering av beslutningstakerne. Det er viktig.

Det er mange fallgruver underveis i prosessen. Det er viktig at man har med noen som har erfaringer med risikoanalyser. Det er et vanskelig felt med mange kvalitative vurderinger. Praktisk erfaring er viktig hvis det skal bli en bra analyse.

Man er helt avhengig av å snakke med de som opplever problemene. Med min lange erfaring med risikoanalyser kan jeg lage en relativt bra analyse bare med nødvendig skriftlig dokumentasjon og tegninger/bilder uten å besøke objektet. Sannsynligheten er imidlertid meget stor for at man da ikke får med vesentlige sårbarheter/forhold. Jeg ser at mange analyser gjennomføres uten at de som faktisk opplever problemene på nært hold involveres og dette er uheldig. Under samtaler med "gutta på gulvet" (vaktmester, resepsjonist, vakt, etc.) dukker det bestandig opp overraskelser som er viktig for analysen og som man ofte ikke får tak i hvis man kun snakker med "overordnede".

Utfordringer med standardarbeid- nasjonalt og internasjonalt
Når en utvikler standarder er det viktig at de ulike meningene blir ordentlig forankret. I alt standardarbeid står man ovenfor utfordringer ettersom alle skal bli enig og at ting må bli avklart innad i organisasjon, mellom land osv. Ettersom standardene er basert på å få konsensus så kan innholdet lett bli utvannet. Det har vi sett i flere internasjonale standarder. Fordelene med å lage norske standarder er at de blir mer spisset og dermed blir de bedre enn internasjonale standarder. Arbeidsgruppen til NS 583X-serien har vært en mindre gruppe som ikke nødvendigvis har søkt forankring utover sine security-fagmiljøer. Det var en hurtig arbeidende gruppe, dermed er ikke denne standarden så utvannet som andre standarder. Allikevel er denne standarden overordnet. Det er en utfordring å få forankret standardarbeid i egen organisasjon. I en stor organisasjon vil det være forskjellige meninger og hvem skal det forankres med? I arbeidsgruppen ble jeg nedstemt på f.eks. bruken av sannsynlighet, skal man da trekke seg ut og ikke bidra videre i arbeidet? Gjør alle det, faller standardarbeidet sammen. Det er masse kompromiss og justeringer underveis så det er vanskelig å få det forankret i egen organisasjon.

Kommentar fra Stein Ove Bakke-Hanssen: Etter å ha lest gjennom intervjuet er det viktig å presisere at når jeg uttaler meg om metoder og sannsynlighet så er det ut fra mine erfaringer med bruk av modeller innen security området. Når jeg kritiserer organisasjoner er det på bakgrunn av hvordan jeg opplever at de har fremstått under arbeidet med standardene.

C.7 Intervju med Joakim Barane

Navn: Joakim Barane
Bakgrunn: Seniorrådgiver og seksjonsleder security risk management i Falck Nutec. Leder av arbeidsgruppen for NS 5830 og sekretær i arbeidsgruppen for NS 5831 og NS 5832. Medlem av Standard Norge Komité SN/K 296. Deltok i arbeidsgruppen for PST under arbeidet med "En veiledning – sikkerhets- og beredskapstiltak med terrorhandlinger".
Tid og sted: 19. desember 2014, telefonintervju

Debatten innen Security-området
Debatten har gått på bruken av sannsynlighet eller ikke, og hva man eventuelt legger i begrepet sannsynlighet, samt hvorvidt en kan bruke safety risikoanalysemetodikk på security-området. Er det "one-size-fits- all" eller skal man bruke flere tilnærminger.

Mitt inntrykk i debatten er at det er en del grupperinger som vil ha det slik "det alltid har vært", eller slik at det samsvarer med standarder på andre områder. De har andre agendaer og ansvarsområder og er gjerne motstandere av å gjøre ting på en ny måte. Det er gjerne de som er mest negative til en annen tilnærming på security. Kritikerne henviser til at "sånn er det ikke i andre standarder, vi ser ikke behovet for en ny standard", de ønsker at alt skal gjøres likt fordi det er praktisk. Jeg føler at det er enkeltpersoner som driver frem de ulike sidene, jeg tror ikke hele organisasjoner har felles oppfatninger om slike ting, dermed koker det ned til enkeltpersoner som har ansvar og interesse. Derimot oppfatter jeg at alle miljøer som har en akademisk tilnærming på hva som ligger bak standardene og hvordan man kan forbedre ting drives mer av nysgjerrighet og er mer åpne for debatt. Samtidig er det et klart skille mellom den teknisk-naturvitenskapelige skolen med sin tilnærming til risiko, og den samfunnsvitenskapelige/kriminologiske skolen som NS 5830-serien er basert på.

I arbeidet med NS 5830-serien har jeg ikke en eneste gang blitt møtt med faglig argumentasjon for at trefaktormodellen ikke er egnet for security. All motstand har gått på andre ting som at *(i)* det ikke er i samsvar med ISO 31000, hvilket jeg mener er helt feil. ISO 31000 presiserer ikke at man må bruke en tofaktortilnærming med sannsynlighet og konsekvens, de stiller seg relativt åpen til hvilken tilnærming en velger å bruke. *(ii)* Det blir ofte trukket frem at dette ikke er likt som NS 5814 som har en mer tradisjonell teknisk og naturvitenskapelig tilnærming. *(iii)* En annen innvending er at hvis man vil vurdere mange typer risiko som man vil presentere i et helhetlig risikobilde, så blir det vanskelig å bruke forskjellige tilnærminger og at en da må bare bruke én tilnærming. Jeg synes dette er dårlig argumentasjon ettersom ulike typer risiko trenger ulike tilnærminger. Det er oppkonstruert at en ikke kan sette ulike typer risiko sammen til et helhetlig risikobilde selv om det er brukt forskjellig metodikk. Det er litt som analogien om at hvis en skal bygge et hus trenger en flere typer verktøy. Det er enklere å gjøre alt med samme tilnærming, men hvis én type metodikk ikke passer alle typer risiko, da mister man flere viktige nyanser og helheten, eller huset om du vil, blir deretter.

Hvor står du i denne debatten?
Jeg mener at risiko knyttet til uønskede handlinger krever en annen tilnærming enn andre typer risiko. Tilnærmingen i 5830-serien er den beste for dette området. Det er viktig å få frem at i andre sammenhenger er det annen metodikk og tilnærminger som er relevant. Jeg er opptatt av at man ikke skal utkonkurrere andre tilnærminger, det betyr bare at man har flere verktøy i verktøykassen som blir tilgjengelig for brukerne.

NS 5830-serien og NS 5814
Den mest grunnleggende forskjellen er at de to standardene kommer fra to ulike skoler; *(i)* samfunnsvitenskapelig tilnærming som ligger bak 5830-serien, *(ii)* 5814 har et mer teknisk/ naturvitenskapelig utspring. Det er i utgangspunktet stor forskjell på disse tilnærmingene.

I tillegg er oppbygningen av analysen i NS 5830-serien annerledes, som går på *(a)* identifisering av verdier, *(b)* ut ifra dette identifiserer man hvem som kan være ute etter verdiene (trusler) og ulike handlemåter trusselaktørene kan bruke og *(c)* hvor sårbare man er mot dette. Sammen med usikkerhet knyttet til de ulike vurderingene utgjør dette sikringsrisiko. Det blir en rød tråd gjennom hele analysen[105]. Dette er en samfunnsvitenskapelig tilnærming som man ikke finner i 5814 og som jeg mener er viktig for å gjøre denne type security-risiko helt relevant. Dette er også konsistent med den relativt vide risikodefinisjonen som finnes i ISO 31000 som er "usikkerhet om måloppnåelse".

Det er for øvrig mange likheter mellom 5830 og 5814 når man leser de. Begge ønsker å finne risikoen og usikkerhet rundt fremtidige hendelser. Organiseringen rundt utførelsen av en risikoanalyse er ganske sammenfallende. Det er likevel noen prinsipielle forskjeller som jeg mener blir bedre ivaretatt i NS 5830 når det gjelder tilsiktede uønskede handlinger, hovedsakelig på grunn av at NS 5830 er tuftet på samfunnsvitenskapelig metode, atferdsteori og kriminologisk teori.

Er det noen klare positive/negative trekk ved NS 5814 eller NS 5830-serien?
NS 5814 setter likhetstegn mellom sannsynlighet og frekvens (NS 5814:2008, 4.2, fjerde avsnitt). Dette gjør den etter min mening uegnet for security, men kan være god hvis man arbeider med et fagområde med frekvensbaserte fenomener der dette er mer relevant. Hvis du har frekvensbaserte fenomener så kan 5814 være en egnet tilnærming, men med security der man skal håndtere tenkende, rasjonelle aktører så er 5830 den mest egnede tilnærmingen sett ut ifra mitt ståsted. Den ivaretar usikkerhetsdimensjonen og kunnskapsdimensjonen på en bedre måte.

Security er et fagområde i rask utvikling. NS 5832 representerer dette fagområdet der det står nå i 2015, NS 5814:2008 er en eldre standard fra en tid da security i større grad lente seg på metodikk og teori fra andre disipliner. NS 5814 er i utgangspunktet ikke en standard som er tiltenkt å håndtere security-problematikk. Jeg tror en må slutte å strebe etter "one model fits all". Det finnes ikke. Dette er forskjellige fagområder og det går ikke an å tilnærme seg de på samme måte.

[105] For mer informasjon se Barane (2014). *Et rasjonelt valg – om trefaktortilnærmingen til sikringsrisiko*. Sist besøkt 07.01.2015. http://www.proakt.no/et-rasjonelt-valg-om-trefaktortilnaermingen-til-sikringsrisiko/

Jeg synes også at sannsynlighetsbegrepet slik det brukes i NS 5814 er misvisende og uegnet for problemstillinger knyttet til uønskede tilsiktede handlinger. Det er nok bred enighet i de akademiske miljøene om at en frekvensbasert sannsynlighetstenkning er uegnet for security. Problemet er at det store flertallet som gjør risikoanalyser innen security ikke forholder seg til akademia, men til standarder som NS 5814. NS 5814 oppfordrer til bruk av slik frekvensbasert sannsynlighet og bruk av en Boston square matrise, og da er det slik risikoanalysene blir. Det er også verdt å nevne at de aller fleste risikoanalyser ikke gjøres på samfunnssikkerhetsnivå, men for mindre områder og virksomheter. Etter mitt inntrykk tar mye av akademia i Norge utgangspunkt i risikohåndtering på et høyere nivå, og er mindre relevant for "do'erne".

Når det gjelder sannsynlighet synes jeg det er et dårlig begrep uansett om du sier frekvensbasert eller kunnskapsbasert sannsynlighet, ref engelske "likelihood" og "probability" gitt at det refereres til sannsynligheten for at en bestemt handling inntreffer på et bestemt objekt.
I NS 5830-serien er det ikke slik at man ikke kan bruke begrepet sannsynlighet. F.eks. hvis man har en trusselaktør kan man si at den mest sannsynlige handlemåten er X, eller at i trusselvurderingen så er det mer sannsynlig at denne aktøren angriper deg enn en annen. Sårbarhetsvurderingen vil si noe om dersom man blir utsatt for et angrep, så er det sannsynlig for at de lykkes eller ikke. *I NS 5830 så bruker man ikke sannsynlighet som en egen parameter når man vurderer risiko. Det er sannsynligheten for at du blir utsatt for en uønsket handling slik som det fremstilles i ROS-metodikk, som vi er uenig i. Det er den sannsynlighetsvurderingen vi mener det er vanskelig for sikkerhetsfolk å forholde seg til, og til dels irrelevant.*

Jeg synes ikke den kunnskapsbaserte sannsynligheten fungerer som et godt substitutt på virksomhetsnivå, og det er tross alt der 99 % av alle risikoanalyser gjøres. Jeg som virksomhet ønsker å vite om risikoen for *min* virksomhet. Det helt greit å si at det er stor sannsynlighet for at det skjer et terrorangrep i Norge de neste 5 årene, men det hjelper ikke den personen som skal drive hensiktsmessig risikostyring for egen virksomhet. PST gikk ut og sa at de anser det som sannsynlig at det vil skje ett terrorangrep de neste 12 månedene. Men hva betyr det for meg? Det er vanskelig å si noe velbegrunnet hva sannsynligheten er for at *min virksomhet* blir angrepet, og det er tross alt det som er det interessante for meg. I NS 5830 tar man utgangspunkt i at dersom jeg har verdier som denne trusselaktøren er ute etter, og vi vet at denne trusselaktøren er reell, så kan min virksomhet like gjerne være et mål som noen andre. Dersom virksomheten også er sårbar overfor et slikt angrep, har man en stor grad av risiko: det er med andre ord stor grad av usikkerhet knyttet til denne mulige fremtidige hendelsen. Hvis man ikke kan leve med dette, bør man iverksette tiltak for å ta kontroll over fremtiden og redusere risikoen.

Vanskeligheten med å inkludere ulike fagmiljøer i standardutvikling
Generelt ser jeg at det er lite broer mellom akademia og praksis innenfor dette området i Norge. Dette er synd, og definitivt en utfordring vi alle burde ta tak i. Flere akademiske miljøer i Norge har blitt invitert til å delta i arbeidet med NS 5830-serien, men arbeidsgruppen har ikke fått noen respons. Ingenting ville glede meg mer enn god, saklig debatt rundt dette med relevante forskningsmiljøer.

Jeg sendte for eksempel personlig e-post til Terje Aven og Tore Bjørgo med høringsutkastet til NS 5830, uten å få noen respons. Vi viste også veilederen som ble utgitt av PST, POD og NSM i 2010 til Aven på en konferanse vi var på. Han var interessert, men kom ikke med noen videre innspill. Ulike miljøer på UiS og andre personer har vært i en utvidet referansegruppe, andre har vært spesielt tipset når den lå til offentlig høring. Mitt inntrykk er at flere fra de akademiske miljøene ikke er interessert i operasjonaliseringen og de praktiske aspektene. Dette er synd fordi akademikerne som sitter med mye av forskningen og kompetansen kunne ha hjulpet "do'erne" på bakken som skal gjøre dette i praksis. Det er viktig at man skal nyttiggjøre seg av kunnskapen fra akademia, men det synes jeg ikke skjer i dag. I prosessen med NS 5830 har det vært lite interesse å spore fra for eksempel UiS eller NTNU. Vi kan ikke tvinge dem til å være med, men vi har prøvd å få dem med ettersom det hadde vært positivt å få innspill fra ulike fagmiljøer.

Nå er det også viktig å understreke hva en norsk standard egentlig er. I utformingen av en standard er alle interessenter like velkomne til å delta, og standardarbeid er tuftet på konsensus. Det er med andre ord potensielt svært mange aktører med forskjellige ståsteder, agendaer, erfaring og kompetanse som skal bli enige om et slags "minste felles multiplum". Dette er standardens velsignelse og forbannelse, og står i sterk kontrast til for eksempel et forskningsprosjekt, en bok eller en artikkel der forfatteren selv kan forfekte egne meninger og konklusjoner. Det er i all hovedsak miljøer som jobber praktisk med sikring og sikringsrisikohåndtering som har drevet frem arbeidet med NS 5830-serien.

Finnes det noen rådende "best practice" i metodologien på security-området? Er det noen land eller organisasjoner som har kommet spesielt langt?

Jeg vil si at Norge har kommet langt; med at vi har en nasjonal standard på security som har en "asset, threat, vulnerability" tilnærming som jeg føler er den veien det går innen security-feltet og har gjort ganske lenge. Jeg vet ikke om det er noen anerkjent beste praksis, det er vel derfor det er så mye debatt rundt de nye standardene. Med utgivelsen av den nye standardserien i Norge tror jeg dette er i ferd med å bli beste praksis i Norge ettersom NSM, PST med fler forfekter denne tilnærmingen. FEMA, USA og britene har tilnærminger som ligner. ISO 31000 er såpass åpen at de favner forskjellige type tilnærminger for risikoanalyse.

Begrunnelse for språkdrakten i NS 5830-serien

Definisjonen på sikkerhet i NS 5830-serien er hentet fra samfunnsvitenskapelig akademia, og bygger på den originale latinske betydningen som er noe sånt som "freedom from worry, fear, anxiety, danger…". Det vil si at sikkerhet er en tilstand der man enten er, eller føler at man er, trygg, og det er denne tilstanden vi vil strebe etter å oppnå, helst begge deler. Man har forskjellige oppfatninger av når man er sikker, altså risikoaksept, og det ivaretar denne definisjonen godt. Samtidig ivaretar den konseptet om at man kan være sikker, men ikke føle seg det; og føle seg sikker, men ikke være det. Alle disse dimensjonene er relevante for god sikringsrisikohåndtering.

Risiko er i NS 5830-serien definert som forholdet mellom verdi, trussel og sårbarhet. Dette er på ingen måte en matematisk formel, men sier at form og farge på disse tre faktorene samt hvordan man tolker samspillet dem imellom vil avgjøre grad av risiko. Definisjonen passer til security og

henger sammen med det teoretiske fundamentet for standardene, og er godt innenfor definisjonen av risiko i ISO 31000.

Det har også vært en del diskusjon på at NS 5830-serien bruker begrepene "analyse" og "vurdering" litt annerledes enn for eksempel NS 5814. I NS 5830-serien har man villet være tro mot ordbokdefinisjonene av de to begrepene, og det ble også hentet inn en vurdering fra Språkrådet. *Analyse* er brukt der hvor det er snakk om en prosess der man "bryter informasjon ned til sine enkelte bestanddeler og setter dem sammen igjen for å avdekke en mening", mens *vurdering* er brukt der man beskriver "hva dette egentlig betyr for oss". Språkrådet støttet denne bruken. Når det er sagt; ingen "eier" begrepene analyse eller vurdering, det er generelle termer som må settes inn i en kontekst slik at det kommer frem hva man legger i begrepene. Jeg synes derfor ikke det er problematisk at de brukes litt ulikt. Min erfaring er uansett at i praksis brukes disse begrepene om hverandre uten at det skaper stor forvirring.

Hvordan burde en kommunisere risiko til brukere/ledere som ikke er eksperter?
Det viktigste er at risikobildet skal si noe om "hva betyr dette for deg og din virksomhet". Det må være relevant for lederen og det må komme sammen med øvrig risiko. En må presentere det sammen i et helhetlig risikobilde. Da er vi tilbake på verdier. De verdiene er de samme uansett om man snakker om security eller safety. Sikringsrisiko må være relevant og må kunne sammenlignes med andre typer risiko, ellers så klarer ikke security å gjøre seg relevant i "den store sammenhengen".

Det jeg har møtt på tidligere er at når en presenterer risikobildet til ledere føler sikkerhetsfolk at de "*må*" presentere risiko i en Boston square matrise ettersom det er det lederne er vant til. Derfor må det omgjøres til sannsynlighet og konsekvens. Ledergruppen trenger å vite om risikoen er høy, moderat eller lav. Hvis de ønsker å vite noe mer om en spesiell risiko så må man gå inn og se på hvordan vi har kommet frem til dette. Alle er så vant til og glad i denne Boston square matrisen. I praksis er det ikke noe problem og bare henvise direkte til risikoen som lav, moderat og høy, det venner lederne seg til veldig raskt. Da kan man bruke den metoden som passer best så lenge man har en del parametere som gjør at en kan sammenligne dette, nettopp gjennom identifisering av verdier. Jeg mener at konsekvensmatrisen er god og at på øverste hold i virksomheten må man si noe om verdier, som miljø, økonomi, liv og helse. Alle som vurderer risiko (både safety og security) kan forholde seg til disse konsekvensparameterne.
Da kan en sammenligne hendelser som brann og terrorrisiko som konsekvenser på verdier.

Hvis noen kunne komme opp med en måte en kan fremstille trefaktor-risiko på en pedagogisk måte så ville jeg vært veldig interessert i å se det, for det er vrient. Jeg mener at man bare kan fremstille risiko alene. Det blir opp til hver enkelt å bestemme hvordan en best kan presentere dette. Man må uansett alltid gå inn og se på analysen og hvordan man kommer frem til risikoen, dersom man ønsker å gjøre noe med den.

Hva er etter din vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?

(i) *Etterprøvbarhet er viktig*. Alt må være begrunnet. Du må kunne dokumentere hva slags faktagrunnlag du har og hva slags vurderinger du gjør på grunnlag av dette. Da er det mulig for andre i ettertid å sjekke vurderingene dine og i hvilken grad det var riktig. Eller hvis noe har endret seg siden sist, så vet man hvor en kan gå inn og legge inn mer fakta om f.eks. trusselbildet.

(ii) Det kreves en *god analytiker med inngående forståelse for metodene* og hvorfor tilnærmingen er som den er. En trenger også en god systemforståelse av hva man analyserer.

(iii) I NS 5830 må man forholde seg tre faktorer. Hvis disse faktorene er f.eks. moderat, høy og lav så er analytikeren nødt til gjøre en skjønnsmessig vurdering. Da ser man på usikkerhet ved bakgrunnsmaterialet etc. Sånn sett *tvinger den nye tilnærmingen analytikeren til å komme med egne vurderinger*. Det kan være mer krevende. Det vi dessverre alt for ofte ser, uavhengig hvilken tilnærming man bruker, er at det er slepphendt arbeid uten begrunnelser for vurderinger.

(iv) *Hvis en hendelse faktisk inntreffer så er tilnærmingen/metoden en brukte viktig*. Da kan man gå tilbake og si "vi implementerte disse tiltakene, det viste seg ikke å holde. Basert på den informasjonen vi hadde på dette tidspunktet så gjorde vi disse vurderingene. Det kan vise seg at dette var feil, men på dette tidspunktet mente vi det var riktig osv". Tenk deg f.eks. regjeringskvartalet før 22. juli. Hvis en hadde gjort en slik øvelse og kunne vise hvilken informasjon en la til grunn, så kunne det vært nyttig i etterkant for å identifisere gap eller svakheter. Metode leder opp til et resultat. Man skal ikke sikre seg for lite, men skal heller ikke sikre seg for mye, og fremfor alt sikre seg på en hensiktsmessig måte basert på relevante scenarioer. Man må ha sikringstiltak som er praktiske og hensiktsmessige (kost og nytte). Da blir denne metodeprosessen riktig. Avgrensingene i 5830-tilnærmingen gjennom identifisering av kritiske verdier; deretter relevante trusselaktører knyttet til disse verdiene; deretter relevante handlemåter knyttet til hvordan trusselaktørene kan skade verdiene osv, er viktig. I NS 5814 så starter med å identifisere alt som kan skje, og da havner man fort "utpå viddene", spesielt hvis kompetansenivået er lavt. NS 5830 er mer fokusert.

Avsluttende tanker

Det er viktig å velge riktig verktøy til riktig jobb. NS 5830-serien er ikke "sannheten" eller "lyset". F.eks. da sikringshåndboken kom så fylte den et vakuum og ble raskt en "bibel" innen fysisk sikring i Norge, men den trenger nå sårt en oppdatering. NS 5830-serien er nå ute og som jeg mener per i dag er den beste måten å håndtere tilsiktede uønskede hendelser. Jeg håper dette faget vil fortsette å utvikle seg og at NS 5830-serien kan revideres om noen år. Jeg kjøper ikke argumentet om at "vi må gjøre slik som vi alltid har gjort". NS 5830-serien er et skritt i riktig retning. All den debatten vi har nå er veldig bra for metodeutviklingen og faget uansett om man er kritisk eller positiv til de nye standardene.

C.8 Intervju med Carsten Rapp

Navn: Carsten Rapp
Bakgrunn: Avdelingsdirektør for *Avdeling for sikkerhetsstyring i Nasjonal sikkerhetsmyndighet (NSM)*
Tid og sted: 12. desember 2014, telefonintervju

Debatten innen Security-området
Jeg har oppfattet det slik at det har vært en bevegelse i debatten på security-området, spesielt de siste månedene. Mitt inntrykk er at PST og NSM lenge har vært samlet om at trefaktortilnærmingen er den riktige tilnærmingen innenfor security-området.

I tillegg er det et fagmiljø bestående av personer med mastergrad i sikkerhet og risikostyring fra ulike universiteter i Storbritannia (det "UK-utdannede miljøet"). Disse har jobbet i ulike virksomheter og flere har vært sentrale i å utvikle NS 583x-serien. De har hovedæren for innholdet i standardene som er utgitt til nå og at trefaktormodellen har blitt såpass sentral i standardserien. Det betyr ikke at jeg alltid er enige med disse om terminologi, prosess og måten risiko bør kommuniseres til beslutningstakere, men jeg støtter de faglige hovedtrekkene.

PST har lenge støttet opp om trefaktormodellen, det har 'satt seg' og blitt institusjonalisert. Den samme institusjonaliseringen har skjedd i NSM. Med unntak av PST, NSM og det "UK-utdannede miljøet", så vil jeg ikke si at det er en samlet bransje som står bak trefaktormodellen. Jeg tror sikringsmiljøene som denne "UK-utdannede" gruppen er en del av, samlet sett er for små til å kunne få til dette alene. Men det denne gruppen har vært flinke til er å arbeide fram en standard som mange er enig i, det skal de ha veldig skryt for.

Jeg har også merket meg at DSB har tilsluttet seg trefaktormodellen. Det jeg har fått forklart er at DSB har vært mest opptatt av at terminologien og måten å jobbe på ikke skal være i strid med de metodene de bruker allerede (bl.a. tofaktormodellen). DSB jobber primært med sikring mot naturkatastrofer og storulykker. Det gjør at de har et nærmere forhold til sannsynlighetskomponenten, noe som er mulig ettersom truslene på DSBs fagområde i stor grad inntrer som stokastiske sannsynligheter (hendelser som skjer med jevne mellomrom). Man har ofte et statistisk grunnlag og historiske hendelser man kan vise til, derfor har man et helt annet tallmaterialet og omfang av data som muliggjør at man kan analysere sannsynlighet. Det er f. eks. ikke slik at meteorologien forandrer seg dramatisk fra år-til-år (selv om en har klimaendringer), dermed er det mulig å predikere sannsynligheten. Det forstår jeg at DSB har fortsatt lyst til å gjøre, så slik jeg har oppfattet DSB er at så lenge 5830-serien bruker terminologi som ikke er i strid med terminologien i ISO 31000, og at man kan velge hvilken av standardene en har lyst til å bruke, så går det greit. Jeg henviser mht. tofaktormodellen mest til ISO 31000 og ikke NS 5814, ettersom jeg oppfatter at NS 5814 har med et mindre nedslagsfelt enn ISO 31000.

Så nå har DSB også tilsluttet seg NS 583X-serien som gjorde at vi kunne gi ut standarden. Man har noen medlemmer i komiteen for 583X-serien som står i bakgrunnen og er med, men som ikke

har noen sterke oppfatninger og så har du andre som er mer avventende. Det er PST, NSM og det "UK-utdannede miljøet" som har vært mye av drivkraften bak standardutviklingen.

Trefaktormodellen – ikke ny og ukjent

Første gang jeg hørte om trefaktormodellen var da jeg begynte å jobbe med sikkerhet i 1997. Da underviste vi i trefaktormodellen i Forsvarets overkommando/Sikkerhetsstaben (FO/S). Jeg var litt usikker på hvor dette kom fra, dette var noe jeg fikk overlevert fra "sikkerhetsideologene" i FO/S. Da fikk jeg vite at dette var tilnærmingen vi skulle bruke, og etter å ha brukt det så fant jeg ut at modellen fungerte veldig bra. Spesielt da jeg senere brukte modellen i andre mer operative stillinger hos andre arbeidsgivere.

Det er enkelte som hevder at trefaktormodellen er ny og ukjent, men det kommer an på hvor du har vært de siste 20 årene. Der jeg har vært (security-miljøet i ulike deler av forsvarssektoren) har trefaktormodellen vært 'best practice' og det har heller ikke vært særlig omstridt i de miljøene. Grunnen til at dette nå har kommet på agendaen, er spesielt på grunn av utarbeidelsen av standardene. Tidligere var security-miljøet i Norge veldig delt; (i) de som var under sikkerhetsloven og det FO/S'erne jobbet med, var en verden for seg. Informasjon med sikkerhetsgradering var (og er) strengt regulert, og man hadde (og har) en sterk myndighetsrolle, som gjorde det mulig å gi tydeligere føringer om metodevalg. Så hadde man et annet miljø; (ii) de med en mer tradisjonell bakgrunn innen risikostyring og kvalitetsstyring, hvor ISO 31000 og 9000-seriene var sentrale. Dette har så gradvis utviklet seg. Det var en 'British Standard' på 1990-tallet som ble ansett som den beste standarden på 'information security management', etterpå kom ISO 2700x-serien, som i hovedsak baserte seg på denne britiske standarden. Disse standardene fulgte 'sannsynlighet og konsekvens'-sporet lenge, men de senere årene har det skjedd endringer der også. ISO 27005 om 'information risk management' bruker uttrykk som 'likelihood' og ikke 'probability'. Den bruker begreper som 'assets', 'threats' og 'vulnerability' og i kurs om standarden med anbefalte metoder vises det til trefaktormodellen som en av metodene/tilnærmingene en kan bruke under ISO 27005.

Jeg har merket meg at sikkerhetsmiljøet i Difi har vært veldig imot trefaktormodellen. Ettersom Difi er så ISO/IEC 27001-orientert, var jeg overrasket over dette, siden ISO/IEC 27005 også bruker uttrykkene "assets", "threats" og "vulnerability", som jo er de engelske kjerneuttrykkene i trefaktormodellen. Det er mulig at Difi ikke er så avvisende lenger til trefaktormodellen, men det får Difi uttale seg om.

Jahn Helge Flesvik skrev en artikkel om risikovurdering i DN[106]. Vi i NSM syntes han hadde en for ensidig og i overkant tradisjonell tilnærming. Vi skrev derfor et tilsvar i DN[107].

[106] Flesvik, Jan Helge (2014). "PST må ut med terrorinfo» i Dagens Næringsliv 17. november 2014. Sist besøkt 12.12.2014. http://www.dn.no/meninger/debatt/2014/11/17/2159/Terror/pst-m-ut-med-terrorinfo

[107] Rapp, Carsten. (2014). "Terror vanskelig å forutse" i Dagens Næringsliv 24. november 2014. Sist besøkt 12.12.2014. http://www.dn.no/meninger/debatt/2014/11/24/2159/Terror/terror-vanskelig--forutse

Akademia i Norge og den vitenskapelige bakgrunnen til ISO 31000/ NS 5814

Jeg har et inntrykk av at UiS har vært relativt moderne og modne på dette området med Terje Aven i spissen. Vi har jo en person i NSM som har tatt en UiS-master som sier at der har man en tilnærming med mer kvalitative vurderinger også innen verdi- og trusseldelen av risikobegrepet, og at den sannsynlighetstilnærmingen NTNU tradisjonelt har forfektet er mer ingeniørrettet/matematisk. Risikoteori oppstod i forbindelse med gambling, altså spillteori, der en med matematisk presisjon kan predikere risiko og sannsynlighet. Innenfor safety er det ofte riktig å bruke en lignende modell pga. god empiri, utfordringen er at en har prøvd å overføre dette til security. Innenfor security har vi trusselaktører som kan skifte mål og strategi. Hvis det for eksempel publiseres en karikaturtegning i morgen kan det gjøre at terrortrusselen er radikalt endret to dager etterpå. Så har man trusselaktører som skjuler det de gjør, slik som fremmed etterretning der en vellykket operasjon er en operasjon som ikke blir oppdaget. Det å tro at man som virksomhet kan anslå sannsynligheten i statistiske vendinger for å bli rammet av trusselaktører som forsøker å skjule sine hensikter og handlinger, mener jeg er ganske naivt.

Sannsynlighetsbegrepet

Innenfor ISO 31000 og andre tradisjonelle standarder så kan man bruke alt fra "frekvensbasert sannsynlighet" til mer kvalitativ beskrivelse av sannsynlighet. Det er ikke slik at alt er overlatt til matematisk presisjon. Poenget mitt er at for å forstå hvor dette stammer fra så er det viktig å huske på at det er spillteorien med matematikere/statistikere og dernest ingeniørene som i stor grad har drevet frem tofaktormodellen. Så har man etterhvert tatt i bruk andre modeller, og sett avskallinger av den matematiske tilnærmingen og tatt inn kvalitative vurderinger. Kvalitative vurderinger har fått et så kraftig innslag at det blir subjektive analyser. Da kan man ikke bruke sannsynlighet ettersom dette overkommuniserer det vitenskapelige aspektet. En gir skinn av at man kan predikere noe som ikke kan predikeres. Derfor må vi kalle det noe annet og ta inn andre faktorer, og så har man kommet frem til trefaktormodellen.

Man kan jo si at man gjør sannsynlighetsvurderinger i trefaktormodellen mtp. valg av scenarioer, men man bruker ikke begrepet 'sannsynlighet'. Vi sier heller at 'det er en muligheten for' og hvor stor denne muligheten er. Det er noen innen security-miljøet som skiller mellom trusselsentriske tiltak (tenke hvor en trusselaktør kan angripe og beskytte skallet sitt) og verdisentriske tiltak (der fokuset er på å identifisere nærmere og sikre de viktigste verdiene på innsiden). Det er flere områder innen security der en har et verdisentrisk fokus. Det er der "mulighetsbegrepet" og "muligheten for", og "hvor sårbare vi er" blir viktig. Det er viktigere å se på sårbarhetene enn på hvem som er trusselaktøren og hvor stor og sterk trusselaktøren er. Vi har erfart over tid at veldig mange vil vite mye om trusselen; hvem er trusselaktørene, hva gjør de og hvorfor gjør de det? Vi i NSM jobber primært med den forebyggende delen av sikkerhet, vi er ikke en etterretningstjeneste og det skal vi heller ikke bli. Virksomheter må prøve å innhente informasjon om trusselen og vurdere dens relevans for egne verdier. Vi må imidlertid sette strek på et punkt og si at uavhengig av hvem de er og hvorfor de gjør det de gjør, så medfører det skade hvis de lykkes i sine forsøk, derfor må vi sikre oss. Som virksomhet må vi fokusere på hva som er viktig for oss å sikre og hvordan. Vi bør ikke bruke mye tid på hvem trusselaktøren er, som det kan være vanskelig å finne informasjon om og som den enkelte virksomhet i liten grad kan påvirke.

Forskjellen på sårbarhetsvurderinger og risikovurderinger

Vi kan ikke alltid vite så mye om trusselen og vi kan heller ikke i så stor grad påvirke den, i hvert fall ikke for den enkelte virksomhet. Det er makthaverne; politiet og Forsvaret som i ytterste konsekvens kan gjøre noe med selve trusselen. Det vi må konsentrere oss om, er det vi kan gjøre noe med, og det er å jobbe med sårbarheten. Vi må likevel ikke gå for fort på sårbarheten ettersom virksomheter må bli mye flinkere til å aller først identifisere de viktigste verdiene sine. Dette er noe vi i NSM har vært opptatt av veldig lenge. Hvis du går til en gjennomsnittlig norsk virksomhet i dag og spør styret "hva er det viktigste du har for å kunne levere det som er viktigst for dere å levere?" så vil du ofte få flakkende blikk og spørrende uttrykk. Dette er fordi de egentlig ikke har gjort denne jobben. Før du begynner å se på sårbarhet må du identifisere hva som er dine viktigste verdier, virksomheter *må* starte med verdivurderingen. Derfor kan man ikke si trefaktormodellen minner om en sårbarhetsvurdering alene ettersom også verdivurderingen er en grunnleggende del av risikovurderingen. Når du har gjort en god verdivurdering først, så er du klar for å vurdere om verdiene dine er sårbare mot trusler. Det betyr ikke at trusselvurderingen ikke er relevant, men i mine øyne bør den i et *langsiktig* sikkerhetsarbeid vektes mindre enn verdivurderingen og sårbarhetsvurderingen. På *kort sikt* derimot kan konkrete og umiddelbare trusler måtte tillegges større vekt, men da er det mer beredskapstiltak og krisehåndtering det er snakk om, og ikke langsiktige tiltak med store investeringer.

Hvordan bruke trefaktormodellen i praksis og hvordan kommunisere risiko til beslutningstakeren?

Når jeg har brukt trefaktormodellen har jeg vært opptatt av enkelhet og gjennomførbart, i hvert fall hvis du skal gjøre det selv i en virksomhet med begrensede ressurser. Alternativet er ofte at det blir så omfattende at man ender med å ikke gjøre det i det hele tatt, og det er jo enda verre enn å forenkle. Så det jeg har gjort er å lage scenariobeskrivelser på bakgrunn av verdi- og trusselvurderingen, og så har jeg vurdert i hvilken grad man er sårbar mot det scenariet. Når man får resultatet har vi svaret på hva som er risikoen. Det du bør legge vekt på når du skal kommunisere dette videre er (i) hvilke av scenarioene som det er viktigst å beskytte seg mot, og (ii) gapet mellom nåværende og ønsket sikkerhetsnivå i et gitt scenario. Risikovurderingen er summen av disse faktorene, da har man sammenfattet alle delvurderingene og kommer til slutt til hva som egentlig er risikoen.

Når man skal kommunisere denne risikoen videre så har jeg to tilnærminger: (i) man kan *bruke mottakerens språk og terminologi og operasjonelle risikostyringssystem*. Mange virksomheter har allerede et system for risikovurdering av egen måloppnåelse, der sikkerhet bør være en integrert del av det store risikobildet i virksomheten. Hvis virksomheten har faste rapporteringssykluser og grafer/modeller for dette, bør man som sikkerhetsleder bruke det. Mange bruker fargekoder og to-dimensjonale grafer med plotting for å illustrere risiko for beslutningstakere. I noen av de risikovurderingene jeg har utført har jeg presentert risiko på den måten for at beslutningstakeren ikke skal oppfatte at security er "noe annet skummelt eller fremmed", men at security er en del av den totale risikostyringen. Da har jeg t.o.m. gått så langt at jeg har brukt ordet sannsynlighet. Man må være pragmatisk og tenke at dette må til for å kunne få gjennomslag. Da har jeg brukt

trefaktormodellen internt i utredningsarbeidet, og så har jeg for ledergruppen oversatt konklusjonene til et format de forstår.

(ii) Den andre måten er å *formulere scenarioene i prosatekst*. Jeg trekker frem de scenarioene det er viktigst å fokusere på; de som har en kombinasjon av høy risiko og gap mellom ønsket og nåværende sikkerhetstilstand. Med andre ord, de risikoene som jeg anbefaler at man må jobbe mest med for å redusere. Det kan bli formulert som "*risikoen for at trusselaktør A skal ramme verdi B ved å utnytte sårbarhet C anses som uakseptabelt høy, altså bør man iverksette tiltak D*". Dette er mer pedagogisk ettersom det blir så konkret, da er det lettere for lederen å forstå og også lettere å få gjennomslag for tiltak.

Jeg har også gjennomført risikovurderinger der jeg så på alle typer trusler (både tilsiktede og utilsiktede hendelser). Da brukte vi ISO 31000-tilnærmingen, vi hadde ett dokument for alt og i trusselvurderingen hadde vi to hovedkapitler; (i) tilsiktede/ viljestyrte handlinger der vi brukte trefaktormodellen og (ii) utilsiktede hendelser der vi brukte en sannsynlighetstilnærming basert bl.a. på empiri innen jordskjelvfare, brannfare etc. (vi kontaktet da en del fageksperter på respektive områder). Der det var mulig kunne vi bruke en frekvensbasert tilnærming, men det er jo ikke alle naturkatastrofer og ulykker der det er mulig. Så da kombinerte vi begge tilnærmingene og resultatet ble veldig bra ettersom det ble veldig helhetlig. Det er viktig at man ikke låser seg til bare én tilnærming og én type trusler. Beslutningstakere må ofte forholde seg til et helhetlig risikobilde. Og da vite bare risikoen for brann, eller bare risikoen for industrispionasje, er ikke tilstrekkelig. De ønsker ofte å vite hva risikoen er generelt sett og hvor den er størst for å kunne prioritere tiltak med ofte knappe ressurser. Da må man som en sikkerhetsseksjon i en virksomhet ha evne til å tenke helhetlig.

Er det noen land eller organisasjoner som har kommet spesielt langt i metodologien på security-området?

Jeg mener at Storbritannia har kommet spesielt langt. De har jo selv opplevd mange former for høy-risiko virksomhet og trusler. De har måttet forholde seg til et høyt trusselnivå fra både fremmedstatlig etterretning, terrortrusler og høykompetente ransmiljøer. Dette har gjort at de har måttet forholde seg til sikkerhet på en mer profesjonell måte enn for eksempel det vi i Norge har måttet gjøre. Det gjør videre at det akademiske miljøet i større grad har utviklet seg og blitt større enn i Norge og andre land, og dermed mer modent på dette området. Jeg synes fortsatt det akademiske tilbudet av relevante studier på dette området i Norge er umodent, lite og veldig fragmentert. Der det er sikkerhetsfag er det ofte i høyden som et vedheng til annen type studier, og ikke som et hovedstudium i seg selv.

Kan to forskjellige tilnærminger til risiko basert på safety og security redusere den helhetlige risikoforståelsen?

Her er det to ting man må ta i betraktning: (i) Dette er et nytt område, trefaktormodellen som en standard er nytt. Jeg tror at dette er et spørsmål om modenhet. Jeg tror vi må få brukt disse tilnærmingene parallelt, vi må få mer erfaring med det, og så tror jeg i fremtiden at vi klarer å utvikle standarder som ser disse mer i sammenheng. Hvor man kan bruke dette lettere og koble de

i det praktiske arbeidet. Enten det er på standard- nivå eller på verktøy-nivå, det kan hende at dette er mulig, men ett sted må vi jo starte. Det har lenge vært et behov for trefaktormodellen i standardform, det sier litt når Standard Norge sier at NS 5831 og 5832 har vært de mest etterspurte standardene de siste årene. Så vi må leve med at de ulike standardene for risiko ikke er helt samkjørte, hvert fall for en periode.

(ii) Hvis man bruker NS 583x-serien riktig, så kan man bruke sannsynlighet og statistikk hvis man ønsker det. NS 5831 og NS 5832 er prosessbeskrivelser, men ikke beskrivelser av metodene som sådan. Innenfor hver aktivitet i disse prosessbeskrivelsene så kan bruke ulike metoder for å løse aktiviteten. En kan dermed tilpasse metoden til det man analyser. Dette har ikke blitt prøvd ennå fordi det er helt nytt, det blir interessant å se fremover om noen greier å kombinere ulike typer metoder med hell. Jeg tror at hvis man er kompetent på å lage risikovurderinger, så er dette mulig.

Terminologien i NS 583X-serien og ISO 31000

Uenighet om terminologien i NS 583x-serien opp i mot bl.a. ISO 31000 var en av grunnene til at det tok tid å gi ut standarden. Veldig mye ble avklart frem til 2012 eller 2013, men da gjensto det uenighet om enkelte sentrale begreper som gjorde at arbeidet stoppet helt opp i lang tid. NSM foreslo derfor i 2014 noen endringer i terminologien slik at den skulle være mer tro mot ISO 31000. Selv om det "UK-utdannede miljøet" mente at NSM hadde "latt dem i stikken" og gitt etter for "motparten", var det NSMs forslag som førte til at dialogen kunne fortsette i en mer konstruktiv retning. Forslaget var også ment som et kompromiss i den uenigheten som da var mellom på den ene siden det "UK-utdannede miljøet" og PST og på den annen side Difi og DSB. I komiteen for standardene kom det enkelte motforslag til NSMs forslag, og det endte til slutt med justeringer som alle representantene i komiteen kunne akseptere (mulig at Difi tok dissens, det husker jeg ikke). Kompromisset var at man kom med helt nye begreper som sikringsrisikovurdering som ikke var i strid med ISO 31000.

Hva er etter deres vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?

(1) *Det er viktig å kommunisere med det språket og den risikomodellen beslutningstakerne allerede har*. Her vet jeg at enkelte i "det UK-utdannede miljøet" er mer kompromissløs og har uttalt at vi må "tvinge" lederne til å forstå trefaktormodellen. Jeg er mer pragmatisk. For meg er det viktigere å få resultater enn å ha akademiske diskusjoner i organisasjonen. Det er viktig å ha en anerkjent risikovurderingsmodell. Som tidligere praktiker synes jeg det blir for mye diskusjon om valg av modell og ikke det at en bruker modellen godt. *Det viktigste er at du har en strukturert og grundig nok gjennomgang av faktorene og den erkjennelsen du får av denne prosessen. Disse standardene endrer seg i rykk og napp, dels i takt med annen utvikling. Det finnes neppe en endelig og perfekt standard på noe område, men det betyr jo ikke at arbeidet som ble gjort i samsvar med en tidligere utgave eller annen standard var bortkastet. Det er prosessen som er gullet ved det.*

(2) *Modellen tilpasses etter behov og må samsvare med det en studerer*. Det er viktig at vi vektlegger faktorene som vi har god kunnskap om enn faktorer vi er usikre på. Usikkerhet og kunnskapsgrunnlaget må tas hensyn til. Det betyr i praksis at en virksomhet vil vite for lite om trusselen til at de kan legge mye vekt på hva trusselaktører kan gjøre på kort og lang sikt. Verdiene sitter du på selv og sårbarhetene kan du finne mye informasjonen om. Egne verdier og sårbarheter må tillegges mer vekt enn trusselkomponenten ettersom det kortsiktige trusselbildet fort kan gå ut på dato.

(3) *Virksomheter må ha en verdisentrisk tilnærming, tildele nok ressurser og ha god lederforankring*. Det er også viktig at tilnærmingen kan skaleres basert på hvor mye ressurser du har. Tilnærmingen må være anvendbar i praksis. Hvis man i f. eks. en krisesituasjon bare har noen timer på å lage en risikovurdering, må en kunne ha en tilnærming som kan skaleres slik at en kan få inn komponentene verdi, trussel og sårbarhet på en 1-2 siders memo til lederen.

Avsluttende kommentar
Man må ikke bli for "religiøs" rundt de ulike tilnærmingene til risikoanalyser. Man må være litt mer åpne for andres synspunkter. En må erkjenne at disse modellene kan leve side om side, og kanskje bli koblet sammen. Det er ikke slik at én modell er svaret på alt alltid. Det at modeller og standarder utvikles og endres viser at de ikke er "hugget i stein som evige sannheter", men som annet menneskeskapt også har svakheter som det over tid er behov for å utbedre eller utdype. Jo mer man låser seg til ett syn og én metode, dess mer lukker man for utvikling og endring på området.

C.9 Intervju med Roy Stranden

Navn: Roy Stranden
Bakgrunn: Ledet arbeidsgruppen som utviklet standarden.
Tid og sted: 30. januar 2015, telefonintervju

Debatten innen Security-området
Det er flere diskusjoner som pågår samtidig; (i) *Bruken av ordene tofaktor- eller trefaktormodell.* Jeg vet at det er mange som har talt imot denne grovdelingen ettersom begge modellene i praksis inkluderer flere faktorer enn dette. Begrepene tofaktor og trefaktor er hovedsakelig knyttet til hvordan sluttresultatet blir presentert.

(ii) *Bruken av sannsynlighetsbegrepet*. Dette er preget av at folk har ulike ståsted. Mitt synspunkt er at sannsynlighetsbegrepet er vanskelig eller umulig å forstå for folk flest. Det kan godt være at det finnes en matematisk formel for alt, det kan godt være at noen har funnet denne, men min oppfatning er at de som jobber praktisk med security har lite eller ingen erfaring med matematiske formler og sannsynlighetsberegninger. Jeg tok derfor tidlig et prinsipielt standpunkt mot å bruke sannsynlighet. Jeg så i praksis at det var fullt mulig å få et godt resultat uten at en bruker sannsynlighetsbegrepet. Jeg mener det er umulig å si noe fornuftig om sannsynligheten for at man blir rammet eller ikke, men du kan si noe om at hvis du blir rammet er det mer sannsynlig

at du blir rammet på denne måten fremfor en annen måte. Her har man kanskje statistikk om *modus operandi* som kan bli brukt. Den type informasjon kan opplyse vurderingene.

Min erfaring med virksomheter som har lite kompetanse innen dette feltet er at de ikke skjønner de forskjellige tolkningene av sannsynlighetsbegrepet. Da ender de opp med en tabell med hendelser rangert som usannsynlig til svært sannsynlig basert på frekvenser. Alle skjønner forskjellen når man forklarer dem "likelihood" og "probability", men jeg har aldri opplevd at dette er noe de forstår før jeg nøye forklarer problemstillingen. Virkeligheten der ute er at man forstår sannsynlighet som frekvensbasert. I NS 5814 og i Sikringshåndboken[108] står det at de tolker sannsynlighet som frekvensbasert. Det er dette folk leser, ikke artikler i vitenskapelige tidsskrifter. Det er folk som har tatt et standpunkt om at de bruker en kunnskapsbasert sannsynlighet, men dette er gjerne de litt mer viderekomne enn majoriteten.

(iii) *Majoriteten av de som jobber med security har ingen akademisk utdannelse innenfor dette feltet.* Dette er en utfordring. Jeg prøvde å finne en tilnærming der en kunne helt fjerne bruken av sannsynlighet, og heller inkludere andre faktorer som gir like god eller bedre informasjon. For det handler om å opplyse grunnlaget for en beslutning om en mulig fremtid. Hvis du klarer å gjøre dette uten å binde deg til sannsynlighet og konsekvens så er målet oppnådd.

(iv) *Ny og gammel tilnærming.* Jeg opplever at det har blitt harde fronter, nesten som en religionskamp, og jeg opplever at mange har tatt et standpunkt uten egentlig å forstå forskjellen. Det opplever jeg som frustrerende. Det mangler en grunnleggende forståelse for at en risikobasert tilnærming til sikkerhet bare er én av flere tilnærminger til å oppnå sikkerhet. Det er også flere som argumenterer at risiko og sikkerhet er to forskjellig ting som ikke kan sammenstilles. Hvis man velger en risikobasert tilnærming som har blitt veldig populært, så må man ha med seg at man må gjøre noen kompromisser. Hvis man skal prøve å rangere i hvilken grad det er sikkerhet som styrer risiko, eller om det er risiko som styrer sikkerhet i forhold til strategier, så vil de fleste tro at sikkerhet er en måte å håndtere eller styre risiko på. Min forståelse fra studier og praksis er at sikkerhet er kun én strategi av flere for å kunne håndtere risiko. Rekkefølgen er ikke ubetydelig. Man kan enten unngå handlingen som skaper risiko, overføre risiko, bruke sikkerhets- og beredskapstiltak til å redusere eller fjerne risiko, eller så kan akseptere risikoen. Da ser du den hierarkiske ordningen og at sikkerhets- og beredskapstiltak er bare én av flere strategier.

(v) *Mangel på reell kommunikasjon*. En annen ting jeg har opplevd er at man i denne diskusjonen prater til hverandre, ikke med hverandre. Dette er fordi vi har kommet så langt ned i skyttergravene. Vi blir nesten mer belærende ovenfor hverandre enn å gå i dialog, det synes jeg er synd.

(vi) *Andre motiver har preget diskusjonen om standardene*. Kan andre motiver enn rent faglige motiver være med på å bestemme hvilke retninger et standardarbeid kan ta? Vi opplevde dette tydelig i standardutviklingsprosessen. DSB jobbet for eksempel mot at standarden skulle bli gitt

[108] Sikringshåndboken ble utgitt i 2005 av FB. Den oppdateres nå og det kommer en ny omarbeidet versjon som er offentlig tilgjengelig.

ut. En representant fra DSB sa til meg at noe av årsaken til dette var at de var redd for at kommunene skulle bruke en annen metode enn det DSB anbefaler og at dette kunne skape forvirring. Selv om dette er forståelig, er det en helt feil tilnærming og et forsøk på å kvele nytenkning innenfor et område de ikke nødvendigvis forstår like godt som safety.

Det var også aktører som var i mot at en introduserte flere måter å gjennomføre risikoanalyser på. De mente av prinsipp at flere tilnærminger ville gjøre det mer komplisert for sluttbrukerne. Uansett hva vi argumenterte med faglig var de ikke interessert i en faglig diskusjon. De konkluderte bare med at det ikke var likt andre standarder som er publisert, og derfor var de i mot. Det vakte engasjement hos meg. Jeg er prinsipielt imot å lage vurderinger som selv bestemor kan gjennomføre fordi det ofte gir ingen mening. Min forståelse er at en enten gjør en risikoanalyse godt, eller så lar du være å gjennomføre den. En av årsakene til det er at risikoanalysen skal være et beslutningsgrunnlag for tiltak. Hvis du baserer beslutningen din på et dårlig grunnlag kan det få konsekvenser som du ikke ønsker. Man ønsker at virksomheter skal tenke rundt problemstillinger. Er problemstillingen derimot enkel og du vet mye om problemet og hva den potensielle løsningen kan bli, ikke gå veien om en risikoanalyse. Det tar tid og vil ikke gjøre beslutningene noe bedre.

NS 583X-serien

Standarden NS 5832 er ikke ment å brukes som en rettledning når en virksomhet skal gjennomføre en risikoanalyse. I standardutviklingsprosessen ble det tydelig at Standard Norge satte som krav at teksten skulle være kort og presis uten store utdypninger. Vi visste at dette ville skape et behov for mer kunnskap. Vi kom frem til at det da må tilbys kurs og noen må skrive bøker og veiledere etc. Dette måtte også komme i etterkant av utgivelsen av standarden.

Det har også vært personer fra steder som f.eks. Kystverket som har operasjonalisert NS 5832. Det er akkurat det som har vært hensikten. Når vi lagde standarden, visste vi at vi ikke kunne lage noe som dekker alle behov. Det vi ønsket var en dreining vekk fra gammel tenkning om risiko. Standarden skal legge noen premisser som en må forholde seg til, deretter er det opp til den enkelte næring og virksomhet å optimalisere tilnærmingen til deres behov. En risikoanalyse skal opplyse en beslutning, hvis problemstillingen er kompleks da vil ikke en enkel metode klare å gjøre jobben.

Bakgrunnen til NS 583X-serien og standardarbeidet

Jeg har sett på dette som en kontinuerlig utvikling. Gjennom studiene så lærte jeg at diskusjonen rundt risikoanalyser og metodikk er egentlig veldig gammel. Jeg husker at Royal Society i UK lagde to rapporter, én på 1980-tallet og én på 1990-tallet der de prøvde å finne en felles definisjon for risiko. De konkluderte med at det ikke var mulig. For meg var dette en inspirasjon til å se på temaet med nye øyne. For meg startet derfor tankene rundt trefaktortilnærmingen rundt 2004 da jeg jobbet i Etterretningstjenesten. Da ble jeg blant annet kjent med hvordan andre land utviklet sine metoder for risikoanalyser. Siden 2006 har trefaktortilnærmingen vært mer eller mindre den

samme. Det første publiserte utkastet ble skrevet av meg og ble skrevet inn i fellesveilederen som ble utviklet av PST, NSM og POD i 2010[109].

Selv om det tok kort tid å skrive utkastet til denne veilederen, når jeg kom inn i prosessen i 2008, tok det totalt fire år å utvikle denne veilederen. Mye av tiden gikk med på å diskutere (i) hvem er det som skal ha makt til å mene noe om hvordan veilederen skulle se ut, og (ii) diskutere ord og uttrykk.

NSM var også tidlig ute på 2000-tallet og pratet om risikotrekanten. Da jeg spurte NSM hvor risikotrekanten kom fra så var det ingen som kunne fortelle meg det. Jeg prøvde derfor å finne en akademisk knytning som kunne være basis for denne tankegangen. Når jeg gikk tilbake til det jeg hadde studert, var det ganske enkelt å finne en slik forankring. Vi har innen kriminologien rutineaktivitetsteorien[110] og Manunta[111] sin APT-teori hvor han skrev en doktoravhandling for å finne en enhetlig forståelse og definisjon av sikkerhet. Her hadde jeg det akademiske fundamentet som jeg mente man trengte for å ha en plattform å stå på.

Det er for øvrig mange som ikke vet at veilederen fra 2010 var forløperen til NS 5832. Da vi jobbet med å utvikle veilederen i 2010 ledet jeg seksjonen for sikkerhetsrådgivning i PST, det vil si at vi bistod private og offentlige virksomheter med råd og veiledning når det gjaldt bl.a. risikovurderinger. Vi fant ut at det ikke fantes et felles språk og ikke noe felles metode. Det var komplett kaos og alle brukte 'sannsynlighet og konsekvens'. I tillegg til utarbeidelse av veilederen lagde vi internt i PST en definisjonsliste. Arbeidet med veilederne og definisjonslisten sammenfalt i tid med et arbeid som pågikk i Standard Norge hvor man ønsket å kartlegge hva som fantes av standarder innenfor Security i Norge. Standard Norge utarbeidet en rapport som konkluderte med at det fantes ikke noen gode standarder innenfor dette området i Norge. Da forstod jeg at dette var et riktig tidspunkt å pensle inn det vi gjorde i PST inn i et standardarbeid, nettopp for at vi kan få en større flate å jobbe på.

NS 583X-serien har sitt utgangspunkt fra arbeidet vi gjorde i PST. Istedenfor at jeg og Barane satt i PST og lagde utkast til en veileder alene, så åpnet vi opp for at flere skulle involvere seg og være med på å skape forankringen. En arbeidsgruppe ble valgt av en komite i Standard Norge. Det vi raskt satte som prinsipp var at vi i denne arbeidsgruppen skulle samle en riktig gruppe mennesker som var handlingsdyktige og at vi skulle være rundt 7 deltakere. Vi sørget for å ha med (i) *sentrale myndigheter* som PST, NSM, (ii) *næringslivet* var representert gjennom Statoil og NSR, og (iii) *kompetansebærere* gjennom FB, Joakim Barane og meg. Mandatet var at vi var en hurtigarbeidende arbeidsgruppe som skulle utvikle utkastene til standarden og så skulle vi ha en stor høringsgruppe der alle skulle bli involvert. Det vi opplevde var at ingen meldte seg på. Vi

[109] NSM, POD, PST (2010) "En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger». Sist besøkt 20.12.2015.
https://www.politi.no/vedlegg/rapport/Vedlegg_882.pdf
[110] Felson og Cohen (1979). "Social change and crime rate trends: A routine activity approach" in *American Sociological Review*, Vol.
44, No. 4 (Aug., 1979), pp. 588-608
[111] Giovanni Manunta (1999). "What is Security" I *Security Journal*, 12, 57-66 (1999)

måtte løpe etter folk for at de skulle uttale seg. Vi hadde også en håndplukket selektiv høringsgruppe av virksomheter og personer vi absolutt ville skulle uttale seg (DSB, POD, UiS), i tillegg til den åpne høringsgruppen.

I standardarbeidet møtte vi på utfordringer knyttet til at representanter ikke hadde forankret arbeidet i virksomheten de representerte. Når medlemmer i arbeidsgruppen og den utvalgte høringsgruppen ble byttet underveis i prosessen så ville den nye personen plutselig representere en ny mening/standpunkt på vegne av virksomheten. Dette hadde store konsekvenser for diskusjonen rundt standarden og språkdrakten.

NS 583X-serien og NS 5814

NS 583X-serien er en helt annen prosess enn det NS 5814 og ISO 31000 legger opp til. Bl.a. har NS 5832 en annen måte å fremstille sluttresultatet på. Man sier ikke at resultatet skal presenteres f.eks. gjennom en Boston Square matrise. Sluttresultatet i NS 5832 trengs egentlig ikke å vises i et diagram, man kan bare si at "*risikoen er høy, lav eller moderat*". NS 583X-serien har også et fokus på noen sentrale områder som andre tilnærminger ikke dekker. Eksempler på dette er stort fokus på verdivurderingen, fravær av bruken av sannsynlighet og bruken av etterretning.

Noe av det som gjør NS 583X-serien unik er fokuset på verdivurderingen. Dette er grunnlaget for en enhver fornuftig bruk av ressurser for å sikre noe. Det må komme først! Hvis man begynner å identifisere trusler eller "risikoer" så ser man for bredt og en tenker ikke på relevans! Dette er en av grunnene til at jeg mener at vi må få en ny retning. Vi må tenke hvilke trusler er mest relevant ovenfor mine på forhånd definerte verdier og min virksomhet.

Et annet aspekt som andre tilnærminger ikke ivaretar er *etterretning som prosess og produkt for å si noe om trusselen*. Dette er litt trøblete ettersom vi introduserer et begrep som er betent og som den store majoriteten som jobber med sikkerhet ikke vet hva innebærer. Etterretning er et ladet ord, eller et fyord, for mange. Det er beklagelig fordi det er egentlig ikke annet enn å innhente informasjon og bearbeide denne. Etterretningshjulet er ikke noe annet enn samfunnsvitenskapelig metode. Jeg prøver å avmystifisere dette. Du har et informasjonsbehov, du avdekker hvordan du skal innhente informasjon, analyserer informasjonen du har hentet inn og deretter lager du et produkt og sprer dette til ulike mottakere.

Når det gjelder trusselvurderingen går man først til de åpne kildene man har. F.eks. PST sin åpne trusselvurdering. Utfordringen er at denne er veldig overordnet. Det er ofte ikke konkret nok for en virksomhet til å ta dette direkte i bruk. Jeg bruker også å gå til lokalt politi, men her varierer det veldig hvilken virksomhet du representerer og hvor mye informasjon de gir deg. Man har også mye informasjon internt i virksomheten som kan være relevant. Jeg går bredt ut og ser også hva som skrives akademisk og i media. Hvis usikkerhetsfaktoren knyttet til denne vurdering er stor så kan man ta et standpunkt. Forklar at du har manglende kildegrunnlag og at du velger en dimensjonert trusselaktør. Det er viktig at du beskriver hvorfor du kom frem til nivået du gjorde. Det er ofte i trusselvurderingen usikkerheten er størst og hvor man har minst mulighet til å avdekke relevant informasjon på en god måte. Hvis du ikke har kilder og kompetanse, eller kan

trekke på folk som har det, så blir resultatet dertil dårlig om man ikke velger en dimensjonerende trussel.

Jeg har fått inntrykk at ingen egentlig er i mot de tre faktorene verdi, trussel og sårbarhet som brukes i NS 5832, men flere mener at en kan bake inn disse aspektene i NS 5814 eller ISO 31000. Utfordringen er at majoriteten av sikkerhetsfolkene som jobber med dette ikke har kompetanse nok til å gjøre dette. Jeg kan selvfølgelig bruke NS 5814 og 'tweeke' analysen til at den blir bra, men da må du ha nok kompetanse til dette. Styrken til NS 5832 er at den på en god måte leder deg gjennom prosessen steg-for-steg. Du slipper å måtte tolke eller omgjøre noe for å få et godt resultat.

Finnes det noen rådende "best practice" i metodologien på security-området? Er det noen land eller organisasjoner som har kommet spesielt langt?
Jeg har plukket en del ideer fra USA og UK, men jeg opplever at Norge er langt fremme. Ikke det at vi bruker de tre faktorene, mange andre gjør også dette. Det at vi frigjør oss fra behovet for å bruke sannsynlighet, det tror jeg vi er alene om. Her ser jeg evolusjonen innen sikkerhetsfaget hvor en begynte med at "risiko=sannsynlighet X konsekvens". Så kommer vi til at en har lyst til å bruke tre faktorer istedenfor bare sannsynlighet og konsekvens. Da blir det matematiske regnestykket at risiko er "konsekvens X (trussel, sårbarhet)". Altså at en baker sårbarhet og trussel inn i samme faktor som er sannsynlighet. Min forståelse er at dette er problematisk. En mister mye av nyansene ved å tvinge disse to faktorene inn i én. Trusselen og sårbarheten kan nemlig bytte nivå hvor først trusselen var lav og sårbarheten høy til det motsatte. Det kan være at dette ikke gir nevneverdig utslag på den beregnede sannsynligheten. Situasjonen vil imidlertid være helt forskjellig, men denne endringen forsvinner kanskje når disse faktorene blir puttet sammen. For meg er dette en dramatisk endring som kanskje ikke kommer frem. En av årsakene til dette er at intensjon og evne er kanskje den viktigste faktoren når man vurderer trusselen. Hvis en har en aktør med høy motivasjon er det ofte bare snakk om tid før en skaffer seg kapasitet til å omgå sikringstiltak. Intensjon er dessuten ufattelig vanskelig å si noe om og det kan endre seg på et sekund. Dette kompliserer trusselvurderingen.

Et annet aspekt er tilgjengelig litteratur på norsk. Sikringshåndboken kom i 2005 og den statusen den har fått hos mange sikringsmiljøet har vært svært ødeleggende for den risikobaserte tenkningen innen sikringsfaget. Både mtp. spredning av boken og at den vil eksistere i lang tid. Per dags dato har vi i Norge ikke et godt alternativ. Sikringshåndboken er veldig tydelig på at en skal bruke frekvensbaserte sannsynligheter og tar ikke tilstrekkelig hensyn til verdi, trussel og sårbarhet. Den fremmer enkelhet både i prosess og sluttresultat. Dette har blitt et autoritativt dokument som majoriteten forholder seg til og det svekker nytenkning på dette området.

Hvordan burde en kommunisere risiko til brukere/ledere som ikke er eksperter?
Jeg opplever at forenkling ofte skaper forvirring. Et eksempel på dette er bruken av ordet risikoer eller risiki. For meg handler det om at en identifiserer risiko knyttet til ulike aktiviteter. Da kan trusler som terrorisme og kriminalitet være relevant. Men "terrorisme" og "kriminalitet" er ikke risikoer slik mange uttrykker det. Det er kanskje enklere å snakke om risikoer, enn risiko knyttet

til en handling. Hvis ting og begreper er for enkelt blir det imidlertid ikke tydelig og skaper forvirring.

Det er ikke alltid slik at en risikoanalyse er det riktige å gjennomføre. En risikoanalyse er kun relevant når problemstillingen er stor og/eller kompleks. Hvis ikke er ikke risikoanalysen veien å gå. Dette budskapet synes jeg er veldig viktig; Du må ikke gjennom en risikoanalyse hvis ikke det er hensiktsmessig. Det at virksomheter er pålagt å gjøre risikoanalyser i alle sammenhenger er ofte basert på dårlig råd og veiledning til beslutningstakere (politisk ledelse) som har gjort at dette blir et politisk krav. Dette har jeg blant annet opplevd i PST. Det er veldig enkelt at krav om risikoanalyser blir populistisk. Risikoanalysen blir dessuten brukt politisk ikke bare til å opplyse en sak, men kanskje til å drenere en prosess. Her vet jeg om flere eksempler fra blant annet helsesektoren. Hvis noe kontroversielt blir besluttet så ropes det på at man må gjennomføre en risikoanalyse. Det stopper hele prosessen og blir brukt som virkemiddel til å få debatten inn på et annet spor osv. Dette er en stor frustrasjon for oss som faglig bruker dette for å opplyse beslutninger på en objektiv måte.

Hvis det er "Compliance" eller etterlevelse av et krav om at risikoanalyser skal gjennomføres som er hensikten for å kunne krysse det av på en sjekkliste, så kan "dummy-tilnærmingen" være egnet. Spesielt i standardverden er dette utbredt. For mange som følger ISO standarden er det nesten viktigere at du har krysset av på at du har gjort en analyse enn at kvaliteten på selve analysen er god. Det er flere etater med tilsynsroller som også faller i denne fellen.

Det er en stor forskjell mellom NS 5832 og NS 5814 eller ISO 31000 med tanke på forankring hos beslutningstakeren. 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. I NS 5832 legger en opp til at beslutningstaker skal si noe om sikringsmålene etter verdivurderingen, eller ambisjonen ved sikringstiltakene. Dette sier beslutningstaker bare for at vi som gjennomfører analysen skal ha riktig sett med briller når vi ser på trussel og sårbarhet. F.eks. har du en nullvisjon ser vi på problemstillingen på en helt annen måte enn hvis man har en lavere ambisjon. Helt avslutningsvis så skal man revidere sikringsmålene. Det er her du ser om du råd til å gjennomføre sikringstiltakene i henhold til ambisjonen eller om du kanskje må akseptere mer risiko. Risikoaksept kan også endre seg underveis i prosessen. Et eksempel er 22. juli 2011. Det kan argumenteres for at risikoaksepten endret seg kraftig før og etter denne hendelsen.

Hva er etter din vurdering de viktigste faktorene for å lykkes med en risikoanalyse, og hvorfor?

(i) Mange prøver å samle alt i ett risikobilde. Jeg har stilt spørsmålet om dette er mulig? Her snakker vi egentlig om å sammenligne epler og pærer. Dette må man egentlig avklare før man gjennomfører en risikoanalyse. For å lykkes i å presentere hva man skal avdekke så må du beskrive risiko knyttet til ulike typer aktiviteter. F.eks. i min hverdag jobber jeg med problemstillingen om man skal publisere karikaturtegninger eller ikke, da risikovurderer man en

gitt aktivitet - ikke terrorisme eller en virksomhet i sin helhet. Ved å være konkret i å fokusere på risiko knyttet til aktiviteter blir det enklere å formidle.

(ii) Man må være konsis og komme med konklusjonen på en enkel og kortfattet måte tidlig i dokumentet. Alt annet er vedlegg.

(iii) Skriv prosa og ikke stikkord. Kom med drøftingen når du gir konklusjonen. Innen security-feltet er det altfor vanlig å konkludere uten å forklare analysens begrensinger og avgrensinger etc. Du må forklare hva slags informasjonstilfang du har og usikkerhet knyttet til tolkninger. Har vi avdekket alle relevante faktorer og har vi tolket dem riktig. Her støtter jeg Aven sine tanker om det å legge trykk på usikkerhet og hvordan man kan redusere usikkerheten. Det er noe av de viktigste i hele analysen. For eksempel hvis jeg har fått liten tid til å utføre en risikoanalyse og ikke har mye informasjon så må jeg skrive dette i analysen og at det dermed er stor usikkerhet knyttet til konklusjonene.

Avslutningsvis

Kompetansekrav til analytikere er viktig. Jeg ønsker at dette faget skal utvikle seg i en retning der en aksepterer at dette faget ikke er for “hvem som helst”. Det er ikke noe som alle skal gjøre. Erkjennelsen for at dette er tilstanden i dag er interessant. Jeg holder kurs i regi av NSR og et av de viktigste poengene jeg prøver å få frem er at dette er et eget fagområde. Hvis du ikke har kompetansen selv så må du kanskje kjøpe kompetansen. Å pålegge at alle skal gjennomføre risikoanalyser i alle sammenhenger fremmer heller ikke det vi egentlig ønsker å fremme, nemlig at risikoanalysene på en god måte skal opplyse beslutningene. Om ikke beslutningsgrunnlaget er godt vil man kanskje innføre tiltak som ikke fungerer etter hensikten, eller er unødig kostbart.

Vedlegg D Statistikk-eksempel

I Kapittel 3.2.1 er matematisk sannsynlighet behandlet ut fra et numerisk eksempel med statistikk over bankran i Norge i tiden 1999 til 2012. Det er der regnet ut antall bankran pr bankfilial, og tallene er som vist i tabell D.1.

År	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
Ran pr. filial	2,2 %	1,7 %	1,0 %	1,1 %	0,7 %	0,6 %	0,6 %	0,1 %	0,2 %	0,2 %	0,4 %	0,9 %	0,9 %	0,8 %

Tabell D.1 Bankran i Norge

Her er det av interesse å se på gjennomsnittsverdi og spredning. En vanlig måte å gjøre det på er å beregne aritmetisk gjennomsnitt og standardavvik. Da finner man et gjennomsnitt på 0,8% og et standardavvik på 0,6%, og man antar implisitt at tallene følger en normalfordeling (og det gjør de faktisk). Her støter man imidlertid på det problemet at det blir en endelig sannsynlighet for et negativt antall ran. (Gjennomsnitt – 2*standardavvik = -0,4%)

Dette problemet kan løses ved å transformere tallene i tabell A.1. En transformasjon som ofte fungerer er å ta logaritmen til tallene, og så beregne gjennomsnittsverdi og standardavvik av de nye tallene. Man antar at tallene er log-normalt fordelt. I dette tilfellet viser en sjekk at de transformerte tallene er bedre normalfordelt enn utgangstallene. Da kan man bruke vanlig statistikk på dem, beregne gjennomsnitt og standardavvik, og beregne konfidensintervaller, og så transformere resultatene tilbake. Da finner man et 90% konfidensintervall på 0,15% til 2,4%, og en gjennomsnittsverdi på 0,6%, som altså er litt forskjellig fra det aritmetiske gjennomsnittet på 0,8%.
Også ved å bearbeide tilgjengelig statistikk over andre typer anmeldte lovbrudd viser det seg at en statistisk beskrivelse basert på antagelsen av en log-normal sannsynlighetsfordeling gir et mer realistisk bilde når det gjelder hendelser som forekommer sjelden.

Det finnes et teoretisk grunnlag for å anta at frekvensen av denne typen handlinger følger en log-normal fordeling. Som et utgangspunkt, enten det gjelder vanlige lovbrudd eller terrorhandlinger kan man anta følgende:

1. Det finnes en gjerningsperson, som har et motiv for å foreta handlingen
2. Gjerningspersonen har vilje til å utføre handlingen.
3. Gjerningspersonen foretar faktisk handlingen
4. Gjerningspersonen lykkes

For alle punktene kan det defineres en sannsynlighet P_n.(n=1 til4)Sannsynligheten for at handlingen skal fullføres blir da:

P(handling)= $P_1 \cdot P_2 \cdot P_3 \cdot P_4$, altså produktet av alle sannsynlighetene. De enkelte sannsynlighetene er i utgangspunktet ikke kjent, men man vet at de alle er mellom 0 og 1.

Hvis man tar logaritmen til P, vil denne bestå av summen av logaritmene til de enkelte faktorene. Videre sier sentralgrenseteoremet i matematisk statistikk at en sum av uavhengige og identisk fordelte tilfeldige variabler går mot en normalfordeling når antallet går mot uendelig. Derfor vil ln(P) være log-normalt fordelt, siden alle P-ene er identisk og uavhengig fordelt mellom 0 og 1, dersom det er tilstrekkelig mange P-er. Og simuleringer viser at det er tilstrekkelig med 3 P-er for at dette skal være oppfylt i rimelig grad.

Vedlegg E Gjennomgang av franske myndigheters risikovurderingssystem

Review of the French Government Risk Assessment System (EBIOS)
Utarbeidet av Dave Keir for FFI og FB

EBIOS is essentially a software tool for eliciting qualitative knowledge from the user and his/her subject matter experts, marshaling this knowledge into an identification of main risks and then allocating appropriate security measures to those risks from a predetermined set (mirroring the recommendations in s set of named standards). The system generated reports of what is decided by the user at every step, making the decisions transparent to all who are interested.

There are five steps to completing an EBIOS assessment, all using expert-system user interface pages, which track responses and produce a report. The steps are:

Step 1: A question and answer on the context (essentially asset identification and value of assets) deals with context analysis in terms of total business process dependency on the assets. This step asks the user to identify the main assets (items, material, information) to decide which are essential and which are supporting– and then to identify the essential attribute of value in the essential items material and functions. The example given is an identity card. It is not the **card** which is of value and potentially at risk, but the name and other attributes which allow the individual to identify him/herself which are the assets requiring protection.

Step 2: A question and answer on security requirements for the identified types of assets (effectively a security needs analysis).
Step 3: Threat analysis - A survey of the potential menaces, and filtering out of any irrelevant or insignificant ones
Step 4. A study of the interplay between security needs and the credible threats is completed (it is claimed "systematically"), to attempt to yield an objective diagnostic on risks.
Step 5: The existing security objectives to meet the identified risks (and any further security systems required) are then identified, and the level of coverage is again claimed to be "*assessed, and residual risks made explicit."*

On the subject of the knowledge bases provided with EBIOS software, which help the user to fill in the electronic forms represented by the pages, there is also a user capability for extending these. To quote the ENISA review again: *"Local standard bases (e.g.: German IT Grundschutz) are easily added on to its internal knowledge bases (attack methods, entities, vulnerabilities) and catalogues of best practices (EBIOS best practices, ISO/IEC IS 17799)."*

Good Features of EBIOS:

- EBIOS is designed for the non-expert. It is menu-based and the user is instructed step by step in what to do and how to fill in the blanks in the template statements at each of five Steps.

- At some stages the user is advised to consult subject matter experts to decide on their responses to questions.

- It is relatively easy to complete the EBIOS assessment. It is quick and resource-light, not requiring the involvement of risk assessment experts or those familiar with Boolean methods, or probabilistic assessment in general. In fact it is apparently non-numerical. This may be an attractive feature to many users.

- As the system is aimed at information financial services and other more intangible assets, some time is spent in identifying the **services** being provided by the organization, the main responsibilities for delivering those and the types of harm that could be done to the services and also the reputation of the organization. These are interesting features of an asset identification exercises.

- Completing an EBIOS assessment results in the identification of the key features and value to the organization of assets, the menaces to these assets, the essential security measures already in place and any extra ones required to meet Standards. Choosing of required security measures, is by selection from the EBIOS knowledge base (and compatible with Standards for given types of security risk) appropriate to the risks identified.

- Textual reports are automatically generated at the end of each Step, making the process transparent and easily communicable to all stakeholders, managers and colleagues.

- EBIOS is apparently widely used, both in France and overseas, and in public and private sector organisations. It is also claimed to be compliant with a set of quoted Standards (ISO 17799, ISO 15408). I have not checked this compatibility myself as part of this review.

Shortfalls:

- It is (as far as I as a surrogate user can see) non-numerical and does not explicitly use probabilities. This means that sensitivity studies and other quantitative assessments of the results of changes to defence systems can not easily be done. Whether uncertainties can be handled in any way is not clear.

- The EBIOS process seems philosophically different to the standard probabilistic risk assessment approach, in that although the user is guided through the process of identifying assets, impacts of loss or damage to them, based on identifying threats, and vulnerabilities. The end result is that the list of justified included risks is apparently simply allocated a selection of security measures already predetermined as appropriate to those kinds of risk, based on Standards and selected by the user from an on-board knowledge base. Who did this

predetermination, where and when, is not immediately clear. The user simply follows instructions.

- It is claimed that the ‘risk matrix’ employed in EBIOS allows the user to be informed as to whether the risks have been fully covered, under-covered or over-covered by the set of chosen Security Measures. ‘Residual Risk’ is apparently also identified. How the risk matrix does these things in terms of the mechanism used, is unclear at the present level of review.

Vedlegg F Optimal prosess for risikovurdering for tilsiktede uønskede handlinger

The optimal process for conducting a Security Risk Assessment

Utarbeidet av Dave Keir for FFI og FB.

	Steps	Description
1	**Initiation**	A successful exercise requires a contract (even if only a verbal one) to be in place between the Requirer and the Deliverer.
2	**Appointment of Delivery Manager**	This individual should agree to take overall responsibility for delivery of the risk assessment.
3	**Statement of Need from the Requirer**	This should state concisely what is required and what the scope and boundary conditions are. Can be prepared by the Delivery Manager and submitted to Requirer for agreement.
4	**Plan, with proposed deliverables and timeline**	The Delivery Manager should prepare a work plan, with a timeline, deliverables and delivery date for the finished assessment document.
5	**Risk Assessment team appointments and responsibilities**	At the same time as preparing the Plan, the Delivery Manager should assemble a team of appropriate size, skills and experience to complete the exercise to time, cost and quality.
6	**Access to facilities**	Access to the entity and to facility managers, deputies and operating staff.
7	**Formal description of the facility**	A description of the facility or entity, including its structure, function, inputs and outputs, and how it fits into the larger entity. All security features should be identified and described.
8	**Contingency and Emergency procedures**	Similarly, contingency procedures and emergency procedures - including facilty or contingency-wide emergency response plans – should be fully identified and documented.
9	**Standards of structures and equipment**	If some of the security safeguards and mitigators claimed as already existing are structures, equipment and other technology items, the risk assessor team should ideally establish that they are to suitable modern standards of design and build.
10	**Standards of procedural safeguards**	If some of the security safeguards and mitigators claimed as already existing are procedural ones, contained within operating manuals, work instructions, process instructions or SOPs, then these should ideally be reviewed by the risk assessor team.
11	**Descriptive Chapter for facility review**	All this should ideally form an early chapter of the final risk assessment document. And the whole chapter should be submitted in draft to the facility manager or a deputy, to check for accuracy and completeness.
12	**Security Risk (or threat) Identification**	The risk assessment team should, on the basis of the above information, carry out an identification of all the security risks to the entity, facility and the identified assets. For a limited security analysis the study could end at this point of the process and the results could be presented to the Requirer.
13	**Risk Assessment**	This would ideally be carried out using some quantitative method, and ideally would be done consequence type-by-consequence type, invoking all the relevant security systems, to produce residual risk values. Thus a complete picture for each consequence type of all credible events, both low probability and high; and both low consequence and high would be produced.
14	**Risk tolerability comparison**	Where possible, the final picture of the risks for the facility or entity in question should be compared with risks which are tolerated in other facilities, entities, and other industries or walks of life.
15	**Communication of the results**	This overall picture has sometimes been referred to as the Risk Envelope of a facility or entity.
16	**Risk Assessment Review**	Ideally, the whole risk assessment should be reviewed by one or more independent (and security-cleared if necessary) reviewers.

The document is a distillation of best practices in risk assessment as observed and experienced by the author in both safety and security studies in the UK in the last 20 years[112]. It must be emphasized that the field of risk assessment for attacks on locally and nationally important assets is an emerging field, and so little historical data exists for comparison purposes. Nevertheless, the methodologies are scientifically based, proven to work and shown acceptable to national and industry authorities in various applications.

By their nature, these recommendations are detailed and comprehensive and in reality might need to be modified and streamlined in non-optimal circumstances.

1) Initiation:
A successful exercise requires a contract (even if only a verbal one) to be in place between the Requirer (That is, the principal person or body who is requiring the security risk assessment to be delivered to them. This may be the entity owner, the facility manager, or may be a local or national authority) and the Deliverer (that is, the organization who will themselves deliver the risk assessment to the Requirer (perhaps with the aid of sub-contractor organisations or individuals). A clear indication of the resources (funding and human resources) available, as well as the time window for completion, should be established at this stage.

2) Appointment of Delivery Manager (or Project Manager)
This individual should agree to take overall responsibility for delivery of the risk assessment. If it is clear that access to classified information or sites and facilities will be required in order to carry out the job of security risk assessment delivery , then a Delivery Manager with an appropriate level security-clearance should be appointed, along with an approved secure system of information handling, document control and communications with non-security cleared colleagues.

3) Statement of Need from the Requirer
This should state concisely what is required and what the scope and boundary conditions are. This statement should be in written form from the Requirer (or may be prepared by the Delivery Manager and then submitted to the Requirer for written agreement as to its contents).

4) Plan, with proposed deliverables and timeline
The Delivery Manager should prepare a work plan, with a timeline, deliverables and delivery date for the finished assessment document. This should ideally be communicated to the Requirer as well as the management of the Deliverer organisation.

5) Risk Assessment team appointments and responsibilities
At the same time as preparing the Plan, the Delivery Manager should assemble a team of appropriate size, skills and experience to complete the exercise to time, cost and quality. Their responsibilities and reporting structure and timescales should be clearly communicated to each

individual, ideally in writing. A contingency plan should be in place for quickly replacing team members who may be lost due to illness or other causes.

If it is clear that access to classified information or sites and facilities will be required in order to carry out the security risk assessment, then a team with an appropriate number of security-cleared individuals should be assembled, along with an approved secure system of information handling, document control and communications.

The particular individuals appointed must depend upon the realistic availability of appropriately-skilled and experienced individuals and the resources available. Obviously, the more experienced in the most relevant areas the better. If it is deemed appropriate to apply techniques such as event-tree analysis, fault tree analysis, HAZOP committee, or other specialized methods then team members with experience of these should be included.

6) Access to the entity and to facility managers, deputies and operating staff

In modern Japanese industry there is a principle: 'Go to Gemba". This means that anyone tasked with managing or assessing any process should first and foremost physically go to the workplace. This is a good principle.

There they should see and understand the structures, functions and systems which make up the entity. They also require access to the facility manager or deputies and possibly also to workplace operatives, and permission to interview them. These should all be made available to the Delivery manger and his risk assessment team, via agreement with the entity owner, manager, and operator.

7) Formal description of the facility or entity to be risk-assessed

A description of the facility or entity, including its structure, function, inputs and outputs, and how it fits into the larger entity and (if appropriate the local or national infrastructure, should be prepared by appointed member(s) of the risk assessment team. A clear identification of the assets therein, the consequence class these assets fall into, and if appropriate a vulnerability assessment[113] should be included. Most importantly any security systems should be identified and documented as part of this facility description.

Any entity-wide security systems which apply to the facility in question should also be identified and documented. Safety systems should also be identified, as they may have impact on the development of security situations in case of attack.

8) Contingency and Emergency procedures

Similarly, contingency procedures and emergency procedures - including facilty or contingency-wide emergency response plans – should be fully identified and documented. This is because it is possible to envisage attack scenarios which will first trigger emergency alarms and other

responses, and so these interactions need to be factored in to scenario development during the risk assessment process.

9) Standards of structures and equipment

If some of the safeguards and mitigators claimed as already existing are structures, equipment and other technology items, the risk assessor team should ideally establish that they are to suitable modern standards of design and build (and certification, where appropriate) and are also subject to appropriate maintenance regimes.

10) Standards of procedural safeguards

If some of the safeguards and mitigators claimed as already existing are procedural ones, contained within operating manuals, work instructions, process instructions or SOPs, then these should ideally be reviewed by the risk assessor team.

11) Descriptive Chapter for facility review

All this should ideally form an early chapter of the final risk assessment document. And the whole chapter should be submitted in draft to the facility manager or a deputy, to check for accuracy and completeness. The importance of this cannot be over-stated, as this is the foundation information for the whole subsequent assessment.

12) Risk (or hazard) Identification

The risk assessment team should, on the basis of the above information, carry out an identification of all the security risks to the entity, facility and the identified assets. This may be according to a Requirer-provided list of possible attacks or insults, or may require the Delivery Manager to initiate and deliver a risk (or hazard) identification. This may be simply by interview, expert elicitation and other informal methods, or may be done more formally using a HAZOP-type committee procedure – involving facility manager, designer, operator and security risk and asset experts[114].

13) Limited risk exercise

In some instances, where resources, or timescales are very limited, this may be the end of the risk assessors' job, and the Requirer may want to take risk reduction and management action solely on the basis of the identified hazards, irrespective of their (as yet unrevealed) relative probabilities and consequence magnitudes.

14) Risk Assessment

This would ideally be carried out using some quantitative method, and ideally would be done consequence type-by-consequence type. Thus a complete picture for each consequence type of all credible events, both low probability and high; and both low consequence and high would be produced. Ideally this would be done by producing a transparent analysis of the possible series of events following each kind of identified attack or insult – a scenario development – which takes

fully into account all the existing security, safety and emergency response systems. Ideally this should be done for all the main asset/consequence groups.

The advantage of a quantitative approach is that uncertainties can be investigated by sensitivity studies using only the risk assessment model on a theoretical basis. And, of course, the effect of new or extra safeguards can be investigated in the same theoretical manner.

15) Risk tolerability comparison
Where possible, the final picture of the risks for the facility or entity in question should be compared with risks which are tolerated in other facilities, entities, and other industries or walks of life.

This comparison should include high probability-low consequence risks, low probability-high consequence risks; and others in between. This overall picture has sometimes been referred to as the Risk Envelope of a facility or entity. Realistically this will only be possible where data exists for similar consequence types (e.g. risk of immediate death of members of the public from knife and gun street crime). Historical data for risk tolerability concerning other types of consequence, like theft of information, may be more difficult to locate.

16) Communication of the results
The results should be communicated in a formal report – a document which is as transparent and readable as possible. Where necessary, 'drill-down' information, for instance about the technicalities of the methods used, should be provided in Appendices, under the same cover. Internal review by the risk assessment Delivery Manager and appointed internal reviewers should be carried out, but most importantly, the best test of communicability and transparency will come from the independent external reviewer(s).

17) Risk Assessment Review
Ideally, the whole risk assessment should be reviewed by one or more independent (and security-cleared if necessary) reviewers. Their review results should ideally be communicated in writing to the Delivery Manager. This exercise should be completed in good time to amend the document(s) or re-work parts of the risk assessment if deemed necessary, before final submission as a deliverable to the Requirer. A presentation of the final document may be appropriate, depending upon the needs of the Requirer.

Merknad
Dave Keir har over 20 års erfaring innen kjernekraft, militære anlegg, bioteknologi og støtte til britiske sivile aktører. Basert på sin erfaring har Keir utarbeidet en prosessbeskrivelse på 16 steg en burde gå gjennom for å få til en optimal risikovurderingsprosess.

Vedlegg G Sårbarhetsvurdering – likheter og forskjeller fra risikovurdering[115]

According to the Oxford English Dictionary, the definition of vulnerable in English is: 'an adjective, meaning exposed to the possibility of being attacked or harmed, either physically or emotionally. Examples sentences therein are: We were in a vulnerable position. Small fish are vulnerable to predators.' [116] So, vulnerability is, by extension to our case, a property of an entity and/or its assets.

According to various US government and associated agencies, as quoted on Wikipedia 'vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to, information technology systems, energy supply systems, water supply systems, transportation systems, and communication systems.'

In this author's view, a vulnerability assessment is a correct and complete listing or cataloguing (ideally in a communicable way) of all the individual vulnerabilities of an entity and its assets.

Risk is the likelihood of a situation occurring – specifically an undesirable situation occurring, in which threats come to fruition or, to put it another way, in which attack hazards are realized. A risk assessment starts with the identification of the threats or hazards which apply to the entity and its assets – that is, an understanding of the risk environment (in our case the likely actors and the methods they might use to attack our assets.

Similarities and differences
Both risk assessment and vulnerability assessment have similar broad aims – to reduce the chances of bad things happening – by design, by equipping with security and safety features, by having a recovery plan and ideally by identifying what aspects to improve to give the maximum gain in security.

But they are different. The difference seems to be of focus or emphasis. A vulnerability assessment consists in large part of identifying assets, identifying their attractiveness to attack or insult and identifying the systems, (structures equipment, personnel and procedures) in place, which will work against those attacks or insults – and the strength or quality of those resisting systems.

So it is really a systematic listing of weaknesses and strengths, bearing in mind the threats. This will of course raise awareness of the characteristics of the entity, of its assets and of the possible weaknesses which one might wish to consider addressing.

[115] The meaning of Vulnerability Assessment – similarities and differences to Risk Assessment Utarbeidet av Dave Keir for FFI og FB.

Risk assessment traditionally also requires identification of these same factors, but it proceeds quickly to identifying the characteristics of the relevant environment – the attacks and security breaches which might happen; how likely each one is, and how effective it will be, given the existing security and other defence systems in place. Often this means assessing likelihoods of attack types, propagating the probabilities of event pathways from the point of the attack and assessing both the likelihood of the endpoints and the size of the resulting consequences – to produce an array of theoretical possibilities, with large consequences and small.

Illustrative analogy

It is quite difficult to discuss these issues in a generic and abstract way, so an analogy can be proposed here, albeit a mainly safety-based one. Let us consider an asset, which is a sea-going yacht and the immediate working environment, which is a planned voyage to a specific geographic location.

The vulnerability assessment might be done by a marine architect or engineer, or a boat safety certifier, who is asked to carry it out. He/she would be given access to the yacht itself and to the build plans, the equipment inventory and the outline plan of the voyage. On the basis of his knowledge of yacht design, typical weak points and needs on a sea voyage, plus his knowledge that the assets are the crew's lives and well-being and also the yacht itself, he can come up with a list of vulnerabilities which are common to such vessels (such as old and weak sail fabric or ropes, inadequately-maintained auxiliary engine, lose or corroded fittings) and also any particular to the vessel, that he has observed as being below-standard during his inspection.

The risk assessment would be carried out by someone who would carry out the same sort of inspection and generic risk identification on the vessel and its fittings but, if properly done, he/she will examine the route to be taken and other characteristics of the environment, such as weather forecasts, political situations in sea areas to be traversed (and which storms may drive the vessel into) – essentially looking for credible threats. He/she might also consider depths or anchorage and the possibility of anchor-dragging (requiring a safeguard of a longer anchor chain), other special dangers on or near the planned route such as icebergs, dangerous rocks, known piracy etc. and might therefore recommend, as part of his assessment, extra mitigators of a newer and larger life-raft, extra distress flares, more powerful distress beacon, extra food stores and water and defence equipment to be carried. To ensure completeness, this would ideally be carried out in structured, documented and transparent way and would include an element of tolerability (that is comparing the likely risks with those which are routinely tolerated and managed in other walks of life).

Conclusion

Although both approaches have similar aims, the author recognizes that in practice a vulnerability assessment may not be as thorough as a risk assessment and may not go as far as to identify the most important and least important vulnerabilities, nor what the most effective way to combat them is. On the plus side, it focuses attention on the assets themselves, and may be quicker and less resource intensive to complete than a comprehensive risk assessment.

A comprehensive risk assessment would be likely to actually contain a vulnerability assessment as part of its methodology. The focus on the assets and the consequences to those assets of attack or insult may not be as thorough in this approach, simply because that aspect will only be part of the whole risk assessment job, and, with resource limitations, this may mean the effort on any one aspect will be spread thinly. On the plus side, the decision-makers will have an authoritative justification for any spending of extra resource on risk reduction; as they will be able to point to the maximum benefit per unit spend as discovered during the risk assessment.