DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:
Risikostyring og sikkerhetsledelse

Vårsemesteret, 2021

Åpen

Forfatter: Richard Hansen

Fagansvarlig: Jon Tømmerås Selvik

Veileder(e): Jon Tømmerås Selvik

Tittel på masteroppgaven: Bruk av bayesianske nettverk for å vurdere risiko for innsideraktivitet.

Engelsk tittel: The application of bayesian network in risk assessment of insider activity.

Studiepoeng: 30

Emneord: bayesianske nettverk, personellsikkerhet, innsidere, modellering, risikovurdering, kvalitativ risikovurdering, kvantitative risikovurdering

Sidetall: .....88.....

+ vedlegg/annet: .....34.....

Asker

09.11.2021

Forord

Denne masteroppgaven er siste steget i en prosess som deltidsstudent som har strukket seg fra 2016. Etter en intensiv sluttspurt, hvor spesielt min kjære, lille familie har gitt meg mye tid til «oppgaven», sitter jeg tross alt igjen med et minne om en lærerik og spennende periode. Jeg er umåtelig glad for at dere begge har gitt meg tid til å fullføre tiden som deltidsstudent.

Jeg vil takke min veileder Jon Tømmerås Selvik, som gav meg uvurderlig input tidlig i oppgaven. Fjernstudier er likevel en utfordring, og en skulle gjerne høstet mer av din kunnskap.

Jeg vil også takke de som har tatt seg tid til være eksperter og lese korrektur på oppgaven min, og privatforelesere og sparringspartnere mens jeg har stått fast i løpet av studiet. Sondre, Stig-Erik, William, Bjarte, Stefan, Robert og Kristoffer (RIP) med flere har gitt meg uvurderlig forståelse og gode diskusjoner! Jeg vil også takke medelever som jeg har skrevet oppgaver med, og ikke minst foreleser som jeg har hatt gjennom studiene. Norsk narkotikapolitiforening og LO skal ha stor takk for å ha bidratt med økonomisk støtte gjennom stipender.

Nå er skippertaket over, og hverdagen uten «oppgaven» og skolearbeid tas imot med glede – både for meg og mine kjære.

Innholdsfortegnelse

1. Innledning 7

2.1 Bakgrunn 7

2.2 Innsidetrussel 8

2.3 Begrepsavklaringer og akronymer 8

2.3.1 Bayesiansk nettverk 8

Skjermet og gradert informasjon 8

3 Problemstilling 9

3.1 Motivasjon 9

3.2 Oppgavens utforming 9

Forskningsspørsmål 9

Avgrensninger og definisjoner 9

4 Teori 10

4.1 Myndigheter 10

4.2 Begreper 10

4.3 Sannsynlighet 11

4.4 Bayesiansk nettverk 12

Kunnskapsmodellering 15

4.5 Dagens virkemidler 16

Utfordringer og svakheter ved dagens system 16

4.6 Faglige teorier 17

5 Design og metode 18

5.1 Design science 18

5.2 Metoder for datainnsamling 19

5.2.1 Litteratur 19

5.2.2 Samtaler med eksperter 20

5.3 Verktøy 21

5.4 Plan og utførelse 21

6 Drøfting 22

5.1 Første iterasjon 22

5.1.1 Generelt 22

5.1.2 Bygging 24

5.1.3 Risikoen knyttet til innsidervirksomhet 27

5.1.4 Valg av perspektiv på risiko 30
5.1.5 Type informasjon 36
5.2 Andre iterasjon *36*
5.2.1 Sikkerhetskultur 37
5.2.2 Sikkerhetsstyring 39
5.2.3 Noder og modell andre iterasjon *41*
5.2.3 Evaluering av iterasjon 1 og 2 ..... *41*
5.2.4 Revidering iterasjon 1 og 2 42
5.3 Tredje iterasjon *43*
5.3.1 Bygging 44
5.3.2 Evaluering 76
5.3.4 Revidering 78
5.4 Den endelige modellen *79*
5.5 Problemer med kunnskapsmodelleringsprosessen *80*
6 Bruk av modellen – styrker og svakheter 80
6.1 Som visuelt hjelpemiddel *85*
6.2 Vekting og bruk av kvantitativ modell *87*
6.3 Visuelt og kvantitativ i kombinasjon *91*
Samsvar med tidligere forskning *94*
Behov for ytterligere forskning *94*
7. Konklusjon 94
8 Referanser 96
9 Vedlegg 98
9.1 Vedlegg 1: Tabell intensjon – iterasjon 1: *98*
9.2 Vedlegg 2: Tabell, kapasitet – iterasjon 1 ..... *99*
9.3 Vedlegg 3: Tabell, mulighet, iterasjon 2 ..... *100*
9.4 Vedlegg 4: Tabell intensjon, kapasitet og mulighet, iterasjon 3 ..... *102*
Terrorvirksomhet (*Terrorhandlinger og terrorrelaterte handlinger)* 102
9.4 Vedlegg: Resyme av intervju 1 med ekspert *118*
9.5 Vedlegg 5: Resyme av intervju 2 med ekspert *128*

Figurliste

Figur 1: Bayes formell....12
Figur 2: Enkelt bayesiansk nettverk....14
Figur 3: Forholdet mellom noder i bayesianske nettverk....15
Figur 4: Sikringsrisiko....28
Figur 5: Intensjon, iterasjon1....33
Figur 6: Kapasitet, iterasjon 1....35
Figur 7: Iterasjon 1....35
Figur 8: Iterasjon 2....41
Figur 9: Rus og innsidere....64
Figur 10: Endelig modell....79
Figur 11: Eksempel bruk av nettverk – fullstendig....82
Figur 12: Eksempel bruk av nettverk – Intensjon....83
Figur 13: Eksempel bruk av nettverk – Mulighet....84
Figur 14: Eksempel bruk av nettverk – Kapasitet....84
Figur 15: Visualisering ved diagram – individ....91
Figur 16: Visualisering ved diagram – virksomhet....92

TABELLISTE

Tabell 1: Definisjon innsider – 1....23

Tabell 2: Definisjon innsider – 2....24

Tabell 3: Definisjon innsider – 3....25

Tabell 4: Definisjon innsider - oppgave....25

Tabell 5: Kapasitet, konsekvens og slutthendelser 45

Oppsummering

Formål. Formålet med masteroppgaven har vært å studere fenomenet innsidervirksomhet, og forsøke å se hvordan bayesianske nettverk kan benyttes i personellsikkerhetsarbeid som en kvalitativ og kvantitativ metode.

Teoretisk forankring. Oppgaven tar utgangspunkt i det som kan beskrives som «best practice» på personellsikkerhetsfaget gjennom norske og amerikanske offentlige publikasjoner, samt noe av det som finnes av akademisk litteratur på feltet. Innsidervirksomhet er videre vurdert og modellert i lys av ulike tilnærminger til risikobegrepet, samt kriminologisk teori. Oppgaven bygger på en tilnærming hvor ulike individ- og virksomhetsspesifikke sårbarhetsindikatorer kan brukes til å risikovurdere innsidervirksomhet.

Metode: Metoden som er brukt i oppgaven er design science, hvor en kombinasjon av «best practice» gjennom offentlige veileder og akademisk litteratur er forsøkt kombinert med ekspertvurderinger fra en ekspert innen domenet. På denne måten har jeg forsøkt å forankre oppgaven i litteratur- og dokumentstudier, så vel som semi-strukturerte intervjuer.

Resultater: 1) Innsider-risiko basert på sårbarhetsindikatorer lar seg modellere, men gir mange og komplekse sammenhenger. Det vil dog kreve gode software-løsninger og trenet personell for at et slikt system skal fungere. Ikke minst vil det kreve et særdeles godt datagrunnlag for å tallfeste sannsynligheter og risikoaksept-verdier for innsiderrisiko. 2) En visuell fremstilling av innsider-risikoen på individ- og avdelingsnivå kan modellers og visualiseres, og nyttes i forbindelse med kommunikasjon av risikoen, opplæringsøyemed og for å skape oversikt for egen del.

Konklusjon: Det er behov for bedre datagrunnlag for at modellen skal fungere som et kvantitativt hjelpemiddel, men modellen slik den foreligger kan med enkel programvare brukes i praktisk personellsikkerhetsarbeid. Dette er i samsvar med ekspertenes vurdering, og fagfeltet sammenlignet med lignende fagfelt.

Abstract

Purpose. The purpose of the thesis has been to study insider activity as a phenomenon and to see how bayesian networks can be utilized in the field of personnel security as a qualitative and quantitative method.

Theoretical grounding. The thesis is based in what can be described as "best practice" in personnel security through Norwegian and American official national publications, as well as academic literature on the subject. Insider activity will also be further examined and modeled in light of different approaches to risk assessment as well as criminological theory. The text is built on an approach where vulnerability indicators specific to the individuals or businesses in question can predict insider activity.

Method: The method used in this thesis is based on Design science, where the combination of

best practices provided by a public counselor and academic literature is combined with expert opinions from an expert on the subject. In this way I've tried to anchor the text in literature and document studies, as well as semi structured interviews.

Results:
1) Insider activity risks based on vulnerability indicators is applicable to models but results in many and complex relationships between different factors. It will require excellent software solutions and trained personnel for such a system to function. It will also require a solid foundation of data to quantify probability acceptable risk values for insider activity.
2) A visual model of insider risk on a personnel and department level can be produced, and used in conjunction with communicating the risk, training purposes and to create an overview for internal use.

Conclusion: It will require more data for the model to function as a quantitative aid, but the model as it is can be used with basic software for the purpose of practical personnel security. This conclusion aligns with evaluation of experts as well as the professional field compared to related fields.

Universitetet i Stavanger, Det teknisk- naturvitenskapelige fakultet
Institutt for sikkerhet, økonomi og planlegging, 2021.

1. Innledning

Utgangspunktet for oppgaven er «utro tjenere», eller innsidervirksomhet, som har flere og kompliserte årsakssammenhenger. Ved vurdering av personers skikkethet til å behandle en virksomhets verdier må man skape et totalbilde. I kjente innsidersaker så er det sjelden en enkelt ting man kan peke på som har ledet frem til slik atferd. I etterforsknings- og granskningsarbeid fremstår konklusjonen ofte som at «dette kunne vi forutsett, hvis vi bare hadde tatt tegnene alvorlig». Man har kunnskapen om hva som fører til innsidervirksomhet, men feiler i forsøket på å bruke den i praksis, og det er mange grunner til at man går glipp av tegnene.

Hensikten med denne oppgaven er å finne ut mer rundt hvorvidt kunnskapsmodellering er en mulig metode å bruke innen personellsikkerhetsarbeid. Dette vil jeg gjøre ved å kartlegge sårbarhetsfaktorer innen personellsikkerhet og litteratur om innsidere, etablere sammenhenger mellom disse og sette de inn i en modell ved hjelp av bayesianske nettverk.

Denne oppgaven vil først ta for seg bakgrunnskunnskap, og deretter presentere en detaljert beskrivelse av problemstillingen og presentere en plan. Deretter vil det følge en drøfting av hvordan oppgaven ble utført og en presentasjon av den ferdige modellen. Til slutt vil det være en diskusjon av resultatene av oppgaven etterfølgt av en konklusjon.

Innsidervirksomhet må kunne sies å være et marginalt fenomen, men kan plasseres i kategorien «lav sannsynlighet, høy konsekvens». En innsider kan ha stor kunnskap om forhold som en virksomhet vil holde skjult, tilganger som gir store muligheter og et terrorangrep utført ved hjelp av en innsider vil kunne medføre både store konsekvenser og gi symboleffekt. Når en person først har fått innsyn i informasjon som virksomheten ønsker å beskytte, er det kun tilliten til vedkommende som står mellom at denne fremdeles er skjermet og at den er kjent for andre. Aristoteles sa allerede for over 2000 år siden følgende: "Det er sannsynlig at noe usannsynlig vil skje"

Spørsmålet er bare når og hvor!

2.1 Bakgrunn

Jeg vil nå gå gjennom noe av bakgrunnsmateriale i oppgavens tematikk. Dette har jeg brukt for å utarbeide en målrettet problemstilling, samt planlegge for hvordan jeg skal nå målene som problemstillingen stiller.

2.2 Innsidetrussel

Innsidetrusselen mot norske virksomheter er reell og beskrives i flere offentlige publikasjoner. I PSTs årlige trusselvurderinger trekkes det frem at etterretningspersonell fra fremmede stater vil forsøke å benytte seg av forledelse og press for å tilnærme seg personell innen statlig og privat sektor i den hensikt å skaffe tilgang til informasjon om temaer som for eksempel teknologi og beslutningsprosesser.

Historien viser eksempler på personer som har tilegnet seg informasjon gjennom stilling og posisjon, for deretter å gi denne informasjonen til en tredjepart eller lekket til media. Den kanskje mest kjente saken fra nyere tid i Norge er Arne Treholt, som er dømt for å ha gitt gradert informasjon til sovjetiske og irakiske myndigheter. Så seint som 17.august 2020 meldte TV2 at en norsk mann med ansettelse i DNV GL har innrømmet å gi informasjon til en russisk etterretningsoffiser i bytte mot penger.

2.3 Begrepsavklaringer og akronymer

2.3.1 Bayesiansk nettverk

Bayesianske nett er et rammeverk som brukes for å modellere variabler og de kausale forholdene som finnes mellom disse. Disse nettene bruker sannsynlighetsteori for å beregne hvilken påvirkning de forskjellige variablene i modellen har på hverandre. (Aven, 2008).

Skjermet og gradert informasjon

Det er to regelverk som er gjeldende når det kommer til skjermet og gradert informasjon. Sikkerhetsloven § 5-1 sier at informasjon er skjermingsverdig om det kan skade nasjonale sikkerhetsinteresser at den gjort kjent for uvedkommende, endret eller gjort utilgjengelig. Etter lovens § 5-3 er graderingsnivåene i begrenset, konfidensielt, hemmelig og strengt hemmelig – etter hvor store skadefølger det kan få dersom den gjøres tilgjengelig for andre.

I beskyttelsesinstruksen gjelder informasjon som trenger beskyttelse av andre grunner enn det som nevnes i sikkerhetsloven. Beskyttelsesgradene som brukes etter denne instruksen er «fortrolig» og «strengt fortrolig», gradert etter skadefølgene det vil kunne få for offentlige interesser, en bedrift, en institusjon eller en enkeltperson dersom innholdet blir gjort kjent for uvedkommende.

3 Problemstilling

3.1 Motivasjon

Med grunnlag i en økende etterretningstrussel rettet mot Norge og norske interesser, er det behov for bedre metoder for å vurdere risikoen knyttet til innsidertrusselen. Formålet med utarbeidelse av et arbeidsverktøy som dette, er at det kan forsterke arbeid med personellsikkerhet. Arbeidet har dessuten tatt meg til litteratur om innsidere som handler mot andre ting enn informasjon og immaterielle verdier, og en modell for innsidervirksomhet kan være generisk og gjelde hele innsider-domenet.

3.2 Oppgavens utforming

Oppgavens problemstilling er som følger:

Hvordan kan bayesianske nettverk brukes til å risikovurdere personell med tilgang til skjermet og gradert informasjon?

Forskningsspørsmål

Jeg har valgt følgende forskningsspørsmål til oppgaven:

- *Hvordan kan en bygge et rammeverk for bayesiansk nettverk med utgangspunkt i personellsikkerhetsmessige sårbarheter, som kan brukes til å risikovurdere med tilgang til skjermet og gradert informasjon?*
- *Er det mulig å bruke modellen til å gi personell en personellsikkerhetsmessig valør eller til å understøtte den daglige sikkerhetsmessige ledelsen?*

- *Vil dette kunne være et visuelt hjelpemiddel i personellsikkerhetsarbeid?*

Avgrensninger og definisjoner

Grunnen til dette er at oppgaven ikke har som formål å presentere en komplett modell for risikovurdering av innsidervirksomhet, men et rammeverk som kan brukes til å vurdere hvorvidt modellen vil kunne la seg bruke i henhold til de formålene som definert i forskningsspørsmålene. Jeg vil derfor ikke gjøre jobben med å vekte modellen, men vurdere hvorvidt dette kan være en mulig videreutvikling av den.

4 Teori

I det følgende vil jeg presentere en del begreper og teorier som er grunnleggende for forståelsen av oppgaven, samt teori som oppgaven baserer seg på. Dette er innledningsvis ulike aktuelle myndigheter og aktører i det offentlige Norge som jobber med innsidertrusselen. Deretter vil jeg kort beskrive en del begrepet i oppgaven, før jeg forklarer teorien som ligger bak bayesiansk nettverk og sannsynlighet.

4.1 Myndigheter

Det er et sammensatt nettverk av nasjonale aktører i Norge som på ulike måter har arbeidsoppgaver og – ansvar når det gjelder innsidervirksomhet. Av disse vil jeg innledningsvis nevne:

Politiets sikkerhetstjeneste (PST): PST er en del av politiet som har ansvar for å forebygge og etterforske trusler mot rikets sikkerhet. Det er politiloven § 17b som regulerer hva PST gjør, og slår fast at PST blant annet skal forebygge og etterforske ulovlig etterretningsvirksomhet.

Nasjonal sikkerhetsmyndighet (NSM): Fagmyndighet for personellsikkerhet, men er avgrenset til det som gjelder innenfor sikkerhetslovens virkeområde. Personellsikkerhet defineres av NSM som «tiltak, handlinger og vurderinger for å hindre at personer som kan utgjøre en sikkerhetsrisiko, plasseres eller er plassert i stillinger eller roller som det er aktuelt å frykte for brudd på sikkerhetsloven.»

Klareringsmyndigheter: En klareringsmyndighet vurderer hvorvidt personer kan gis en sikkerhetsklarering. Klareringsforskriften § 1 fastslår at Forsvaret klarerer nødvendige personer i forsvarssektoren, Sivil klareringsmyndighet klarerer nødvendige personer i sivil sektor mens NSM, Etterretningstjenesten, Politiets sikkerhetstjeneste (PST) og Statsministerens kontor klarerer personer i eller tilknyttet egen virksomhet.

4.2 Begreper

I tillegg vil jeg nevne følgende begreper som jeg vil definere før jeg går videre i oppgaven:

Ekspertvurdering: Vurdering gjort av personer med kunnskap om systemet for å fastslå ukjente verdier.

Node Brukes for å referere til en sirkel eller ellipse i et bayesiansk nettverk som representerer en variabel.

Informasjon. Sikkerhetsloven og forskriftenes bruk av begrepet informasjon legger til grunn en vid forståelse av hva begrepet «informasjon» kan omfatte. Måten informasjon er tilvirket på og hvilken form informasjonen har er ikke relevante momenter i vurderingen av om noe er å betrakte som informasjon. Begrepet omfatter for eksempel opplysninger gitt i fysiske dokumenter, digitale og maskinlesbare signaler, film, lydopptak og muntlige opplysninger.
Personellsikkerhet. NSM (Nasjonal sikkerhetsmyndighet, Kripos, Politiets sikkerhetstjeneste, Økokrim, 2017) definerer personellsikkerhet som *«Forebyggende sikkerhetstiltak overfor ansatte og/eller ansatte for å redusere risikoen for uønsket atferd som truer sikkerheten.»*

4.3 Sannsynlighet

Sannsynlighetsbegrepet oppstod i diskusjon mellom to matematikere om hvordan en vinnerpott skulle fordeles dersom et spill ikke ble spilt ferdig. De tok utgangspunkt i at potten da skulle fordeles proporsjonalt med sannsynligheten for å vinne. Dersom det til eksempel var et terningspill med ett kast igjen, hvor spiller 1 vinner ved 1 og 3 og spiller to ved de resterende. Spiller en vil da vinne ved 2 av 6 utfall mens spiller 2 vinner ved 4 av 6 ulike utfall. Spiller 1 har da 2/6=1/3 sannsynlighet for å vinne, mens spiller to har 4/6=2/3 sjanse for å vinne. Dersom premien da var på 30 kroner, så skulle spiller 1 få 10 kroner mens spiller 2 står igjen med 20 kroner, som er henholdvis 1/3 og 2/3 av den totale vinnerpotten. (Nyberg, 2016).

Sjansen for å slå et gitt tall med en terning er 1/6, under forutsetning at dette er en «normal» terning. Videre vet vi at sjansen for å slå det samme tallet to ganger finner vi ved formelen P(A og B)= P(A) X P(B)= 1/6 x 1/6 = 1/36

Grunnen til at vi kan regne slik på denne sannsynligheten, er fordi vi har en forutsetning om at de to terningkastene er uavhengig av hverandre – om du får en sekser ved første kast, vil ikke påvirke hva du får ved neste kast. Ikke all sannsynlighet fungerer på denne måten. En kan tenke seg at en føler seg relativt trygg når en sitter på et fly på vei til feriedestinasjonen sin, og man vet at kun 1/200 000 flyvninger ender i flykrasj. Man kan da tenke seg at P(flykrasj)=1/200 000. Men er det mulig å tenke slik på et så komplekst system som en høyteknologisk maskin, avhengig av at mennesker, personell og organisasjoner samhandler og med avhengigheter til blant annet komplekse værsystemer?

Det vil være faktorer og hendelser som kan endre denne sannsynligheten dramatisk, for eksempel tap av motorkraft i en motor. Dersom vi vet at ved tap av motorkraft i en motor på fly, så vil 1/10 ende i flykrasj, kan vi derfor si at sannsynligheten for flykrasj gitt tap av motorkraft i en motor er 1/10. En kan tenke seg at forutsetningen og dermed sannsynligheten vil endre seg ved mindre dramatiske faktorer som besetningens erfaringsnivå, tidspresset og erfaringsnivå til bakkemannskaper, værforholdene under flyvningen mm.

Nyberg (Nyberg, 2016) argumenterer for at «bayesianere» strengt tatt ser alle sannsynligheter som betingede, og viser til at sannsynligheten for kron ved at vanlig myntkast, P(kron)=1/2 kan skrives P(kron $\mid$ leserens kunnskap om mynten)=1/2. Han viser til at en så enkel øvelse som kron og mynt går an å manipulere.

4.4 Bayesiansk nettverk

Bayesianske nett er et rammeverk som visuelt illustrer kjente og ukjente mengder av en mulig hendelse, ved å tilordne variabler og deres avhengigheter. Slike nettverk brukes for å modellere variabler og de kausale forholdene som finnes mellom disse. Disse nettene bruker sannsynlighetsteori for å beregne hvilken påvirkning de forskjellige variablene i modellen har på hverandre (Aven, 2008). Bayesianske nettverk er rettede asykliske grafer (DAG), hvilket medfører at nodene i nettverket er rettet, ikke-sykliske og en node lenger ned i systemet kan ikke peke tilbake til en node høyere oppe i systemet.

Bayesianske nett baserer seg på Bayes' teorem. Bayes' teorem brukes for å beregne sannsynligheten til en hypotese gitt en variabel mengde observerte faktorer. Dette teoremet kan brukes for å beregne sannsynligheter i et nettverk av relaterte risikofaktorer. Dette betyr i praksis at en kan finne ut hvor stor sannsynlighet det er for at en variabel har en tilstand basert på andre observerbare faktorer som inngår i modellen. Grunnlaget for bayesianske nettverk er bayes formel:

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}.$$

Figur 1: *Bayes formel.*

Et enkelt eksempel er for som synliggjør dette, er at to brødre har søkt på samme studiet. Studiet har ti plasser, og det er 20 kvalifiserte søkere. De går sammen og åpner postkassen, hvor resultatet i brevs form foreligger. Utgangspunktet for hver bror før de åpner brevene, er

at de har 10/20 = ½ hver seg for at de skal komme inn på studiet. Vi vet da at P(A)=P(bror 1 kommer inn)=10/20 og P(B)=P(bror 2 kommer inn)=10/20.

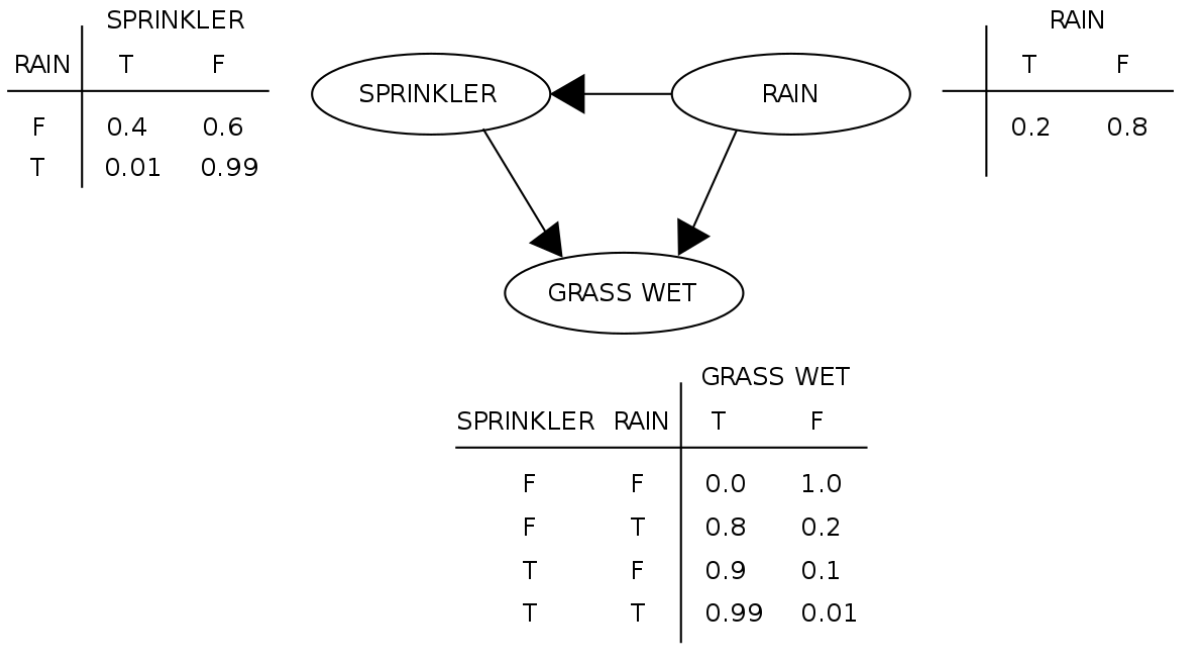
Dersom bror 1 åpner brevet først og han kommer inn, vet vi intuitivt at dette endrer brorens sannsynlighet for å komme inn. Hadde det kun vært èn studieplass, ville nå bror 2 sin sannsynlighet for å komme inn vært P(bror 2 kommer inn)=0. Nå er det fremdeles 9 studieplasser igjen, som vi utfra vår kunnskap, vet skal fordeles og de skal fordeles på 19 stykker. Bror to sin sannsynlig P(bror 2 kommer inn gitt bror 1 har kommet inn)=9/19.

Dette kan vi finne ut ved hjelp av bayes formel. Vi vet at:
$P(B \mid A)=10/20 \text{ X } 9/19 \text{ / } 10/20 = 9/19$

Nyberg (2016) skriver i denne sammenheng at sannsynlighet i klassisk forstand er grad av kunnskap, og beskriver sannsynlighet som mulige brøkverdier for sannheten. Han beskriver videre bayes teorem som en tar inn gamle sannsynligheter og nye data, og lager oppdaterte sannsynligheter. Et svært intuitivt eksempel er dersom bror 2 i eksemplet som ovenfor nevnt har bedre karakterer enn bror 1, og det er eneste kriteriet som er gitt for å komme inn, så vil dette kunne medføre at vi vil vurdere bror to sin sannsynlighet for å komme inn som 100%.

Bayesianske kan for eksempel visualisere og være en representasjon for sannsynlighetsfordelingen for en sykdom gitt et sett med symptomer. Et eksempel på dette kan være at en person få påvist symptomene hevelse i lymfer, feber, hodepine, mens det ikke påvises for eksempel oppkast og diare. Ut fra slike symptomer, eller noder, vil det bayesianske nettverket kunne gi en sannsynlighet P for at vedkommende har en gitt sykdom.

Bayesianske nett har vist seg å være et verktøy innen andre domener, slik som kriminalitet (Roongrasamee Boondao ved Ubon Rajathanee University i Crime risk factor analysis) og medisinske diagnoser. Et bayesiansk nettverk kan se ut som følger:



Figur 2: *Her ser vi en modellering av hvorvidt gresset er vått utfra de to indikatorene «Regn» og «Sprinkler»* (Wikipedia, 2006).

Bayesianske nettverk bygges opp av noder, foreldre- og barnenoder hvor de førstenevnte påvirker den sistnevnte (Aven, 2017). Bayesianske nettverk baserer seg på bruk av indikatorer, heretter omtalt som risikoindikator. Dette er en målbar eller operasjonell variabel som kan brukes til å beskrive tilstanden til et risikopåvirkende forhold. En risikoindikator kan forstås som en målbar variabel som alene eller sett i sammenheng med andre risikoindikatorer, kan beskrive tilstanden til en faktor som kan lede frem til en hendelse. Når jeg bruker begrepet faktor og risikoindikator i denne sammenhengen, er dette snakk om individuelle og konkrete tilstander, forhold eller hendelser ved organisasjon eller individ.

Sintef (Sintef, 2001) skriver at et bayesiansk nettverkt er en asyklisk graf, og har følgende egenskaper:

- Hver node representerer en tilfeldig variabel
- Hver node representerer en variabel A med foreldrenoder som representerer variablene B1, B2....Bn og er tildelt en betinger sannsynlighetstabell, også kalt CPT: P(A gitt B1, b2, ...bn)

Dette forutsetter med andre ord at man setter de betingede sannsynlighetene mellom indikatorer og faktorer, noe min oppgave er avgrenset mot. Dette medfører i praksis at det jeg

bygger, strengt tatt kan kalles et kausalt nettverk. Bortsett fra at jeg ikke vil tildele det en betinget sannsynlighetsmodell så skal modellen ha de øvrige egenskapene for et bayesiansk nettverk.

Et bayesianske nettverk basert på en faktormodell, vil inneholde tre typer faktorer:

1. Faktorer med indirekte påvirkning på hendelsen uten indikatorer.
2. Faktorer med indirekte påvirkning på hendelsen med én eller flere indikatorer.
3. Faktorer med direkte påvirkning på hendelsen.

Figur 3: *Viser hvordan risikoindikatorer kan føre til en faktor, som igjen kan lede til en hendelse. Det er åpenbare utfordringer ved å finne de indikatorene som beskriver tilstanden til en faktor på best mulig måte.*

Kunnskapsmodellering

En modell er en beskrivelse av virkeligheten i matematisk språkdrakt. Kunnskapsmodellering er altså en prosess, hvor målet å formalisere kunnskap og viten om et domene. Gjennom en slik prosess vil man kunne få en modell som blant annet kan brukes av datamaskiner til å gjøre beregninger. En kunnskapsmodellør er en som utfører kunnskapsmodellering. Kunnskapsmodelleringsprosessen består av tre trinn:

- **Bygging**. I dette steget samles informasjon om domenet inn, gjennom bruk av tilgjengelige data og litteratur, samt samtaler og intervjuer med eksperter.
- **Evaluering**. Deretter gjennomgås modellen med eksperter, eller testes mot virkeligheten.
- **Revidering.** Deretter må læringspunkter fra evalueringstrinnet tas med i modellen.

Dette er steg som kan følges trinnvis, eller trinn i prosessen som i praksis går over i hverandre. Gjennom modellering kan ofte domener med stor kompleksitet, usikkerhet og sammensatte årsaksbilder gjøres med enklere og mer forståelige (Korb & Nicholson, 2010).

4.5 Dagens virkemidler

Personellsikkerhet etter sikkerhetslovens virkeområde bygger i dag på grunnpilarene sikkerhetsklarering, autorisasjon og daglig sikkerhetsmessige ledelse. I Norge er det Nasjonal sikkerhetsmyndighet (NSM) som er fagmyndighet for personellsikkerhet etter sikkerhetsloven. Alt personell som skal få tilgang til informasjon gradert høyere enn konfidensielt skal inneha en sikkerhetsklarering, som kan gis av en klareringsmyndighet.

Videre fastsetter sikkerhetsloven at det er virksomhetene som behandler den graderte informasjonen som er pliktig til å autorisere personell som skal ha slik tilgang og for å gjennomføre daglig sikkerhetsmessige ledelse. Blant annet skal autorisasjonssamtale gjennomføres, og autorisasjon skal kun gis dersom ikke autorisasjonsansvarlig har informasjon som gir rimelig grunn til å tvile på vedkommendes sikkerhetsmessige skikkethet. Den daglige sikkerhetsmessige ledelsen følges blant annet opp gjennom sikkerhetsklarert personells orienteringsplikt om forhold av betydning for egen sikkerhetsmessige skikkethet.

Utfordringer og svakheter ved dagens system

Dagens system har noen utfordringer ved seg, slik alle aktiviteter befengt med risiko kan ha. For det første viser bakgrunnssjekker seg å ha lite effekt for å avdekke innsidervirksomhet (Bunn & Sagan, 2016). Slike bakgrunnssjekker ser tilbake i tid, og gir dessuten et øyeblikksbilde. Motivasjoner for å begå innsidervirksomhet kan oppstå etter at slike prosesser er gjort, og diaae kan derfor slippe gjennom likevel.

Dette er likevel noe feilaktig fremstilling, da prosessene sjelden har til hensikt å avdekke innsidere. Hensikten er i hovedsak å forebygge at personell som blir vurdert som ikke skikket til å håndtere virksomhetens verdier, blir plassert i stillinger hvor de får tilgang til disse verdiene. Disse personene ble aldri innsidere, og vil derfor heller aldri bli en del av en statistikk. Det er alltid vanskelig å måle effekten av forebyggende arbeid, da det er vanskelig å føre statistikk av noe som aldri skjedde.

Virksomheter og personell som ikke er underlagt sikkerhetsloven vil også kunne ha lignende, mindre formaliserte mekanismer, blant annet gjennom et personelldirektiv eller lignende.

Bunn og Glynn (Bunn & Glynn, Preventing insider Theft: Lessong from the Casino and Pharmaceutical Industries, 2016) skriver i sin bok om hvordan blant annet legemiddelindustrien sikrer seg mot innsidervirksomhet ved etablerte rutiner for håndtering av virkestoffer med høy gateverdi og misbrukspotensial, bruk av bakgrunnssjekker og lister som gjør at personell med risikoatferd et sted ikke blir ansatt hos en annen legemiddelprodusent.

Historien viser at det man kaller HALO-effekten, eller glorie-effekten, kan vanskeliggjøre arbeidet. Dette beskrives som at positive effekter som en person har på et område, gjør at en antar at vedkommende også er god innen andre felt. Et eksempel på dette kan være en antagelse om at en person med høy utdannelse og med en god jobb, slik som tilfellet kan være innen bransjer som håndterer gradert informasjon, også er pålitelig.

En annen effekt som også gjør seg gjeldende er effekten som beskrives som «not in mye organization»-effekten, NIMO-effekten. Denne kan beskrives som at de fleste kan klare å se for seg at innsidervirksomhet kan skje i en eller annen virksomhet. Men derfra til må se for seg at dette skal skje akkurat der man selv jobber, er vanskeligere (Stern & Schouten, 2016)

4.6 Faglige teorier

Innen forebyggende sikkerhet vil en i mange sammenhenger stå overfor de samme utfordringene som beredskap og arbeid med innen safety-domenet. Når en brann først er i gang, spiller det mindre rolle hvordan den startet. Ved security-hendelser vil dog skille seg noe fra det første ved at handlingen vil ha en intensjon, med andre ord en aktør som vil gjøre sine tiltak for å komme rundt eventuelle sikkerhetstiltak som står i veien nå sitt mål.

Deler av security-feltet tar utgangspunkt i at mennesker begår straffbare handlinger som en følge av et rasjonelt valg utfra hvordan situasjonen er utformet (Lie, 2015). Det er dette som kalles rasjonell aktør-teori, og ligger til grunn for å forklare flere blant annet kriminell atferd. Innsidervirksomhet skiller seg åpenbart fra det meste av kriminelle handlinger som skjer til daglig, men er likevel en type atferd som vil være styrt av et ønske av å oppnå noe bekostning av noen andre og hvor en motstander vil ha et ønske om å avdekke slik atferd. Denne handler om at en gjerningsperson gjør sine kalkyler med grunnlag i mål-middel-kalkyler, hvor en motivert gjerningsperson vil ønske å slå til mot det målet som har minst beskyttelse.

Innsidervirksomhet kan være gjort som følge av press, dårlig økonomi, rus eller lignende, men det vil likevel være snakk om et valg. Valgene som gjøres i forbindelse med utføring av et lovbrudd, handler derfor om kalkulert risiko, hvor sjansen for å lykkes måles oppimot sjansen for å feile.

Rutineaktivitetsteorien tar utgangspunkt i lovbrudd skjer i forbindelse med folks daglige rutiner, slik som i jobb og hjemme. Teorien tar utgangspunkt i at lovbrudd vil skje så lenge forholdene ligger til rette for det, og bygger på en teori om at dersom man har en motivert gjerningsperson, tilgjengelig objekt og mangel på vokter så vil så vil lovbrudd (Lie, 2015)

Når en står overfor en aktør som vil forsøke å komme rundt dine sikkerhetstiltak, står en også overfor en dynamisk motstander. Dette krever tiltak som også er så dynamisk som mulig. Dette er noe som trekkes frem i Sagans (Bunn & Sagan, Insider Threats, 2016), hvor det pekes på at mange som jobber med sikkerheten i ulike virksomheter kommer fra et safety-domene. Et problem som reiser seg da er at sikkerhetsfolket ikke er vant med å jobbe mot en trussel som vil forsøke å omgå dine sikringstiltak.

5 Design og metode

5.1 Design science

Denne oppgaven vil løses gjennom forskningsmetoden «Design Science» (Hevner, 2004) 2004). Formålet vil være å fastsette en modell som kan benyttes i risikovurdering av personell i sikkerhetsmessige sammenheng, som er bygget på ulike sårbarhetsindikatorer. Oppgaver som benytter en prosess som design science, vil primært være å utvikle modellen og dokumentere prosessen. Dette vil skjer gjennom to delprosesser, som er iterasjoner av utvikling og evaluering. Ved å bruke en slik modell, vil man for hver gang kunne komme nærmere en modell som representerer en tilstrekkelig løsning på det problemet en skal løse.

Design science er en meningsfylt måte å løse dette problemet på av flere grunner. For det første skal deler av resultatet være en modell som skal representere et spesifikt domene, og det krever en prosess med evaluering og revidering for å skape en god nok forståelse. For det andre er det et fagområde som av natur er dynamisk, og ettersom det skal representere en modell av virkeligheten slik som den til enhver tid er så må den også endres kontinuerlig.

Det er også slik at dersom metoden skal være meningsfull, så skal resultatet av metoden bli en ny måte å løse et problem på, eller en forbedring av eksisterende. Det finnes andre analyseverktøy innen domenet personellsikkerhet, men jeg har ikke funnet en åpen modell som tar for seg bruken av bayesianske nettverk i denne sammenhengen.

5.2 Metoder for datainnsamling

For å bygge et datagrunnlag for å designe denne modellen, vil jeg innhente informasjon på to ulike måter. Jeg vil bruke dokument- og litteraturanalyse innenfor domenet innledningsvis for å etablere en forståelse. Disse dokumentene vil videre bli brukt for å etablere faktorer, og hvilke sammenhenger som finnes mellom disse. Denne typen data vil også bli brukt som bakgrunnsstoff for intervjuene med ekspertene.

Modellen vil med disse typene datakilder være forankret i både ekspertenes kunnskap om domenet og kjent kunnskap om temaet. Dette er i tråd med metoden for kunnskapsmodellering, og kan gi et solid grunnlag for en valid modell. Ved å bruke disse kildene, tilstreber jeg å plassere modellen innenfor det en kan kalle «best practice» på området.

5.2.1 Litteratur

Jeg vil legge stor vekt på offentlige dokumenter fra blant annet NSM og PST i oppgaven, da dette er nasjonale fagmyndigheter på området. Dette inkluderer temarapporter, veiledere i personellsikkerhet, sikkerhetsstyring med mer, sikkerhetsloven med forskrifter og risikovurderinger. I tillegg har jeg også sett mot ISO-31000, som er den internasjonale standardiseringen av risikostyring. I tillegg har jeg sett til Adjudicative Desk Reference, som er en amerikansk veileder i behandling av personellsikkerhet, som er utarbeidet av det amerikanske Forsvarsdepartementet..

Videre vil jeg se hen til publikasjoner innen temaet. Jeg vil bruke Insider Threats av Bunn & Sagan som har bidrag fra mange fagpersoner innen feltet. Videre har jeg brukt Gelles Insider Threat: Detection, mitigation and deterrence.. Jeg har også brukt Nybergs Statistikk – En bayesiansk tilnærming for å skape en forståelse for bayesianske nettverk og teorien rundt det.

5.2.2 Samtaler med eksperter

Samtalene med ekspertene gjennom kvalitative intervjuer er min andre informasjonsinnhenting i denne oppgaven. Kvalitative intervjuer vil si at man har dybdeintervjuer med objekter, for min del en ekspert på det domenet som jeg skriver om. Gjennom dette vil jeg kunne innhente dybdekunnskap om meninger, vurdering og argumenter innenfor beslutninger og tiltak, slik som hvordan en kan bygge et kausalt nettverk/bayesiansk nettverk.

Dette er en metode som egner seg for mitt formål, da jeg skal bygge en modell basert på tilgjengelig kunnskap om domenet og supplere med datainnsamling gjennom intervjuer. Dybdeintervjuer kan brukes som enkeltstående teknikk, men jeg har vurdert i denne oppgaven at omfanget av feltet er for stort til at en kan diskutere seg til hele modellen.

Intervjuobjektet mine er personer som er ansatt i Forsvarets sikkerhetsavdeling, på avdeling for personellsikkerhet. Dette er personer som jobber med faget, og har bred erfaring innen det. En kan derfor også kalle intervjuet mitt et informantintervju, da dette er personer som vet mye om temaet som jeg skal innhente informasjon om. Formålet med intervjuet er derfor at jeg ønsker at informanten leverer relevant informasjon for min oppgave, og at jeg kan få vurderinger på om de momentene som jeg har gjort har rot i virkeligheten. Intervjuene har jeg delt inn i følgende faser:

- Forberedelse til intervjuet. Dette har jeg gjort gjennom å lage en intervjuguide.
- Gjennomføring av intervjuet. Intervjuet foregår på informantens arbeidssted.
- Etterarbeid. Se gjennom egne notater, og strukturere disse.
- Analyse av svarene. Analyse av svarene blir gitt i drøftingen i iterasjon 3, hvor jeg slår sammen iterasjon 1 og 2, samt ved validering av modellen.

I tillegg til selve intervjuet, har jeg hatt kontakt med ekspertene gjennom prosessen, og stilt enkeltstående spørsmål som ikke er med utgangspunkt i intervjuet og oppfølgingsspørsmål til selve intervjuet. Jeg har også snakket med andre ansatte ved samme tjenestested i en mer uformell setting, og diskutert deler av oppgaven. Dette har jeg funnet verdifullt, og har gjort modellen og de øvrige spørsmålene i oppgaven forankret i både ekspertenes vurderinger og litteraturen.

Intervjuformen vil jeg gjennomføre uformelt gjennom semi-strukturerte intervjuer, da jeg tror dette vil gi en bedre prosess som ikke setter for rigid form på samtalene. Jeg vil også gjennomføre enda mer uformelle samtaler med eksperter i forbindelse med oppgaven, hvor stoffet diskuteres med flere eksperter samtidig. Jeg vil unødig ende opp med å låse meg til faste spørsmål, da dette kan føre til at jeg leder informanten i en retning uten at jeg selv ønsker det. Jeg vil derfor lage en tematisk intervjuguide, med utgangspunkt i modellen og dens temaer.

5.3 Verktøy

Ettersom modellen blir bygget lagvis, har jeg sett det nødvendig å bruke et grafisk grensesnitt or å utvikle kunnskapsmodellen, som er et program som heter GeNIe. Dette er utviklet for å modellere bayesianske nettverk.

5.4 Plan og utførelse

Jeg vil løse denne oppgaven gjennom en iterativ prosess, hvor jeg jeg gjennomgår tre iterasjoner. Bygging av modellen vil derfor ha tre momenter ved seg. Dette er identifisering og etablering av risikoindikatorer og faktorer; etablere relasjonene mellom disse; og vekting, hvor jeg diskuterer muligheter og begrensninger ved dette.

Etter at jeg startet med bygging av modellen, fant jeg tidlig ut at jeg måtte ta et steg tilbake i første iterasjon, og at innsiderrisikoen må kunne sees på som så flerfoldig at det krevde at de de to siste iterasjonene bygger en modell hvor de ulike sidene ved innsiderrisikoen belyses. Den første iterasjonen vil være en generisk og generell modell, som brygger grunnen for at de to neste iterasjonene tar for seg hver sine områder som utgjøre den totale risikoen for innsidervirksomheten.

Jeg satte meg derfor som mål at første iterasjon skulle bygge en modell som beskriver innsiderrisikoen på et overordnet, generisk nivå. Til dette arbeidet har jeg brukt litteratur som beskriver ulike sider ved innsiderrisiko, definisjoner av aktuelle begrepet osv. Denne iterasjon har blitt diskutert med en ekspert i Forsvaret sikkerhetsavdeling med lang erfaring innen personellsikkerhetsfaget.

Jeg har valgt en iterativ prosess fordi det gir mulighet til å jobbe med domenet på en måte hvor arbeidet kontinuerlig evalueres og forbedres. Dette gir også muligheten for å skape en

felles forståelse mellom meg som kunnskapsmodellør og eksperten på domenet. Slik forståelse behøver tid for at man utvikler og gjennom å jobbe med domenet. På denne måten kan feil bli oppdaget og rettet kontinuerlig.

En modell innen innsider-risiko må dessuten være dynamisk og gjenstand for tilpasning kontinuerlig. Dette er kontinuerlig forbedring, og en slik tankegang er også i tråd med Reasons (Reason) om at en sikkerhetskultur er en lærende kultur. Den kontinuerlige prosessen med forbedring gi likeså mye utbytte som resultatet. Det er nødvendig å møte risikoutfordringer med de beste metodene for risikostyring, og gode kartlegging av risikofenomenet er viktig for å kunne identifisere hva slags type risiko det faktisk er snakk om (Kruke, Engen, Lindøe, Olsen, & Pettersen, 2012)-

Til tross for at jeg, som tidligere nevnt, har arbeidserfaring innen temaet, startet jeg relativt uvitende om hvilken vei modellen skulle ta. Jeg startet derfor tidlig med å gruppere risikofaktorer i grupper. Dette hjalp meg selv å holde oversikt over modellen, og var også i den hensikt å gjøre det mer forståelig for ekspertene. Så vidt jeg har klart å finne ut, er ikke dette gjort tidligere med denne hensikt.

Et grep som jeg har gjort for å gjøre oppgaveløsningen mer praksisnær, er at jeg mange steder har lagt inn tekstbokser som viser tilfeller av innsidervirksomhet. Dette står som eksempler på tema som jeg beskriver på de plassene dette er satt inn. Det er åpenbare fallgruver ved å legge inn slike spesifikke enkelthendelser for å belyse det som en nettopp har beskrevet i mer generelle ordelag. Blant annet kan dette fremstå som såkalt «kirkebærplukking», hvor en søker å fremheve fakta som støtter det en selv skriver.

6 Drøfting

Dette kapitlet vil ta for seg den faktiske modelleringsprosessen som jeg har gjort. Hver enkelt iterasjon er samlet under hvert sitt kapittel, med delprosessene bygging, evaluering og revidering.

5.1 Første iterasjon

5.1.1 Generelt

Den første iterasjonen har jeg løst ved å bygge et generisk og generelt rammeverk for modellen min, uten den store detaljrikdommen. I utgangspunktet startet jeg den første

iterasjonen svært bredt, og begynte med å vurdere hvilke risikoindikatorer som man kunne bruke i modellen, især på individnivå, det vil si at jeg startet i det man kan kalle det ytterste laget i modellen. Dette fant jeg fort ut at det ikke gav mening, da jeg ikke klarte å organisere nettverket på en fornuftig måte med denne innfallsvinkelen, da det ble vanskelig å etablere sammenhenger mellom risikoindikatorer og faktorer.

Jeg valgte derfor i fortsettelsen å se mer overordnet på problemstillingen. Dette er gjort ved hjelp av litteratur som gir definisjoner på innsidere, innsidervirksomhet og den grunnleggende kunnskapen om temaet fra for eksempel veileder og offentlige dokumenter, vurdert denne oppimot teori om hva risiko-begrepet innebærer. Det har jeg gjort i den hensikt å finne en definisjon av hva en innsider er, som jeg deretter vil bruke videre i oppgaven.

Tidlig i prosessen ble jeg oppmerksom på en ting. Innenfor det enkelte felt, slik som innen etterretningsmiljøer, beskyttelse av CBRN-installasjoner, forretningshemmeligheter osv., finnes det et begrenset antall kjente saker og begrenset mengde litteratur som omtaler innsiderrisikoen oppimot den enkelte verdien. Især gjelder dette gode detaljer om saker som knytter seg til lekkasje av hemmelig informasjon, da dette ofte stammer fra miljøer som bedriver etterretning- og sikkerhetsarbeid og i natur er underlagt en del hemmelighold. (Bunn & Sagan, Insider Threats, 2016).

Dette medførte at den ene avgrensningen som ligger i oppgaveutformingen om «...kompromittere skjermet og gradert informasjon» blir noe utfordret, da den begrenser oppgaven til å gjelde et utsnitt av det som er beskrevet som innsidervirksomheten i litteraturen. Min konklusjon ble at jeg kan beholde avgrensningen i oppgaven, men likevel bruke litteratur og faktiske eksempler på innsidervirksomhet også fra andre domener. Det blir vanskelig å arbeide med temaet «innsidere» uten at en bruker en definisjon som er strekker seg videre enn innsidervirksomhet rettet mot å kompromittere informasjon. Med dette er kunnskap, erfaring og informasjon fra innsidertrusselen mot andre verdier tatt med.

I denne sammenheng viser jeg til Hegghammer i Sagan (2016), som viser til at innsider-trusselen er et vanskelig domene å jobbe med av nettopp disse ovenfor nevnte grunnene. Han peker på at dette er blant annet fordi lite informasjon er tilgjengelig i akademisk sammenheng og innsidertrusselen er et komplekst problem. Dette gjør at en må bruke informasjon på tvers av sektorer for å lære om innsidertrusselen. Han etterlyser dessuten en større mengde

informasjon tilgjengelig for akademiske formål, men per tid er ikke dette i særlig grad tilgjengelig.

5.1.2 Bygging

Innsidervirksomhet

Det første begrepet som jeg arbeidet med, er hva en innsider egentlig. I denne sammenheng startet jeg relativt snevert med definisjoner fra offentlige, norske dokumenter. Søken etter en god måte å definere det på, som fanger bredden i hva innsidervirksomhet er, tok meg likevel til annen litteratur også.

I min analyse vil jeg dele definisjonen inn i følgende momenter, i tråd med Gelles (2016) sin måte å definere en innsider:
Subjektet: Hvem kan innsideren være?
Objektet: Hva handler innsideren mot?
Verbal: Hvilken handling utfører innsideren.

NSM (2020) definerer innsideren på denne måten:

«En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.»

Analysert gir dette følgende svar på hva som regnes som en innsider etter denne definisjonen:

Subjektet	En nåværende eller tidlige ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang.
Objekt	Denne personen har eller har hatt legitim tilgang til ulike verdier virksomheten har, slik som systemer, prosedyrer, objekter og informasjon.
Verbal	Handlingen som innsideren utfører er å misbruke den legitime tilgangen til de til ulike momentene nevnt ovenfor på en måte som påfører virksomheten skade eller tap.

Sagan (Bunn & Sagan, Insider Threats, 2016) ser videre på begrepet og skriver at «...person with authorized access to items an organization wishes to protect – information, people, and

dangerous or valuable materials, facilities, and equipment. Insiders are often employees, but they can also be contractors or certain types of visitors."

Dette gir følgende subjekt, objekt og verbal:

Subjektet	*Person som har autorisert tilgang til noe som virksomheten ønsker å beskytte, og kan være ansatte, kontraktører og visse typer gjester.*
Objekt	*Denne personen har tilgang til noe som organisasjonen ønsker å beskytte, herunder nevnes informasjon, folk, farlig eller kostbare materialer, fasiliteter og utstyr.*
Verbal	*Definisjonen trekker ikke frem hvordan vedkommende kan skade det som virksomheten ønsker å beskytte.*

Det som spesielt kan bemerkes etter denne definisjonen er at han legger tilet nytt mulig subjekt til definisjonen, og trekker inn at gjester kan være mulige innsidere. Sagan trekker også inn «dangerous and valuable materials» og «equipment» som objekter i definisjonen. Dette er altså en utvidelse av objektene..

En annen definisjon som PST skriver i sin årlige trusselvurdering av 2020, er at innsideren er «agenten med direkte tilgang til norske verdier». En innsider defineres som *«en person som utnytter eller har intensjon om å utnytte sin legitime tilgang til uautoriserte formål*».

Denne definisjonen snakker ikke om objekter i selve definisjonen. Den snakker dog om «verdier» i samme artikkel, og utelukker eller begrenser derfor ikke hvilke deler av virksomhetens verdier som vedkommende utnytter eller har intensjon om å utnytte. Den har altså, som Sagan, en bred fortolkning av subjektet som innsidervirksomhet kan rettes mot. Det vil være opp til virksomheten selv å definere hva som er sine verdier. Definisjonen taler dessuten om person som «utnytter» eller «har intensjon om å utnytte». I dette begrenses definisjonen til personell med en bevisst intensjon om å utnytte sine legitime tilganger, og begrenser derigjennom seg mot det man kaller ubevisste innsidere.

Subjektet	En person med legitim adgang.
Objekt	Definisjonen sier intet om dette, men det skrives i samme artikkel om begrepet «verdier». Dette gjør at objektet etter denne definisjonen kan fortolkes bredt.
Verbal	Handlingen som personen med legitim adgang kan utføre, er «utnytter» eller «har intensjon om å utnytte» denne tilgangen.

En fullverdig definisjon av hva en innsider er, vil også kreve å involvere hvilke handlinger som innsideren utfører, og som gjør vedkommende til en innsider. Det er flere måter dette kan skje på når det kommer til informasjon. I sikkerhetsloven § 5-1 (2018) nevnes det å påvirke informasjonens konfidensialitet, integritet eller tilgjengelighet. Det utdypes videre i samme loven at dette handler om at informasjonen ikke skal bli kjent for uvedkommende, ikke går tapt eller blir endret, og at den er tilgjengelig ved tjenstlig behov.

Jeg har videre sett på Gelles (Gelles, 2016), som skriver at det er viktig med et holistisk blikk på innsidertrusselen og hvordan man definerer hva en innsider er. Dette, skriver han, handler blant annet om at ulike stakeholdere i en virksomhet, må klare å relatere innsidertrusselen til det som de faktisk driver med.

For min oppgave har jeg landet på at følgende momenter må være med i definisjonen av en innsider som handler mot informasjon:

Subjektet	Innsideren er en nåværende eller tidligere ansatt, konsulent eller kontraktør, eller en gjest som har eller har hatt legitime tilganger til noe som virksomheten ønsker å beskytte.
Objekt	Mot ulike verdier som en virksomhet har behov for å beskytte og som innsideren har legitim adgang til. Min oppgave er dette dog begrenset til å gjelde informasjon.
Verbal	Handlinger som påvirker informasjonens integritet, tilgjengelighet eller konfidensialitet.

Definisjonen blir da:

En innsider er en nåværende eller tidligere ansatt, konsulent/kontraktør, eller en gjest, som har eller har hatt legitim tilgang til informasjon som er gradert og/eller sensitiv, og som gjennom sine handlinger gjør den kjent for uvedkommende, endrer den eller gjør at den går tapt, eller blir gjort utilgjengelig for tjenstlig behov.

5.1.3 Risikoen knyttet til innsidervirksomhet

Konsekvens, sannsynlighet og usikkerhet

Det neste begrepet som jeg har vurdert, er risikoen knyttet til innsidervirksomhet, heretter omtalt som «innsiderrisikoen». Risiko er et begrep med mange definisjoner og tilnærminger.

Aven (Aven, Risikoanalyse, 2017) skriver at ordet risiko kommer fra det italienske ordet «risicare», som betyr å våge. Dette begrepet igjen viser til det som kutter, og stammer fra at handelsskip fra 1200- og 1300-tallets norditalienske handelsflåte kunne stå i fare for å synke og bli knust mot skjær og berg, med den tilhørende faren for både mennesker, varer og skip. Dette viser dog samtidig til den positive siden ved risiko, som noe en må søke for å oppnå en eller annen gevinst.

Det er åpenbart at også dette er gjeldende når det gjelder de verdiene som en forsøker å beskytte ved å redusere innsiderrisikoen. Uten personell med legitim adgang til for eksempel kritisk infrastruktur, så vil det ikke være noen til å drive og vedlikeholde slik infrastruktur. Det er med andre ord tvingende nødvendig å ta en viss risiko også på dette området. Det som en vurdering av innsiderrisiko i så måte må gjøre, er å belyse risikoen og på denne måten være et verktøy for å finne et akseptabelt risikonivå. Beskrivelse av risiko handler i så måte om bevissthet omkring risiko og balansen mellom det å skape verdier på ene siden, og faren for uønskede hendelser og tap på den andre siden (Aven, Risikostyring, 2015).

Aven skriver at risiko er kombinasjonen av konsekvensene C av aktiviteten og tilhørende usikkerhet U (Aven, Risikostyring, 2015). Han skriver videre at risiko derfor kan beskrives gjennom konsekvenser, sannsynligheter og bakgrunnskunnskapen som sannsynlighetene bygger på. En modell som den jeg delvis skal utarbeide gjennom denne oppgaven, vil kunne bruke sannsynligheter som et hjelpemiddel, da den kan vektes og gi kvantitative svar. Konsekvensene knyttet til temaet, er tap av konfidensialitet, tilgjengelighet eller integritet.

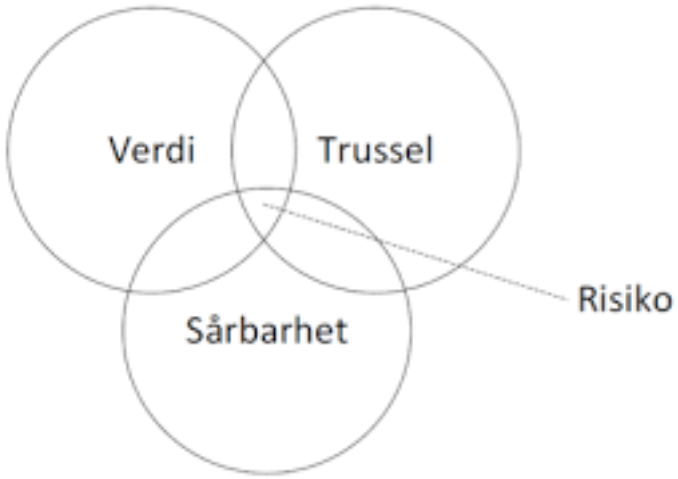
Trefaktormodellen for risiko

En annen tilnærming til risiko, er det som ofte kalles trefaktor-modellen og beskrives i NS5832. Dette kalles sikringsrisiko, og defineres som et uttrykk for forholdet mellom *trusselen* mot en gitt *verdi* og denne verdiens *sårbarhet* overfor den spesifiserte trusselen. Den tar altså utgangspunkt i at man har en verdi som man ønsker å beskytte. Sårbarheten handler

om hvorvidt en trusselaktør kan utføre en handling uten å bli stanset, og handler om hvilke ressurser en trusselaktør har til rådighet sett mot de sikringstiltakene som virksomheten har.

En *trusselaktør* defineres som «en aktør som ønsker å utføre en handling eller påvirke andre på en måte som er i strid med norske sikkerhetsinteresser eller en bestemt virksomhets interesser» (Nasjonal sikkerhetsmyndighet, Kripos, Politiets sikkerhetstjeneste, Økokrim, 2017). Sårbarhet defineres av Aven som den evnen som et system har til å motstå påkjenninger og stress, uten at det medfører tap av noe som har verdi. Med tanke på personellsikkerhet, vil sårbarheter være ulike sider ved en person som enten bevisst kan utnyttes av en trusselaktør for å påvirke virksomhetens verdier, eller det kan være sider ved en person som vil kunne gi utslag i at vedkommende ubevisst påvirker virksomhetens verdier. Det kan også være sårbarheter ved virksomheten som legger til rette for innsidervirksomhet.

Et av argumentene for bruk av denne tilnærmingen til risiko for tilsiktede handlinger, er at den ikke direkte har med sannsynlighet som en faktor i vurderingen. Argumentet om å utelate sannsynlighet som en direkte faktor, er at dette kan medføre at scenarioer med store konsekvenser, men lav sannsynlighet nedprioriteres. Det skal likevel nevnes at gjennom de trusselvurderingene som gjøres etter trefaktormodellen kommer det klart til uttrykk en form for sannsynlighet, da trusselaktører som ikke er vurdert som sannsynlige ikke vil bli tatt med i vurderingene (Busmundrud, Maal, Kiran, & Endregard, 2015).



Figur 4: *Det området hvor verdien, en trussel med intensjon om å ramme denne verdien og sårbarheten mot denne trusselen overlapper, er risikoen* (Proactima, 2016).

Innsiderrisiko

Videre skriver NSM at risikoen for innsidervirksomhet oppstår med bakgrunn i verdiene som virksomheten forvalter, kombinasjonen mellom menneskelige og virksomhetsspesifikke sårbarheter og det overordnede trusselbildet. NSM beskriver i sin Temarapport innsidervirksomhet (NSM, 2020) at innsiderrisikoen kan forklares utfra begrepene intensjon, kapasitet og mulighet.

Intensjon forklares som motivasjonen til å gjennomføre en tilsiktet, uønsket handling mot en virksomhets verdier. Motivasjonen kan oppstå som følge av press eller forledelse fra en trusselaktør, eller det kan oppstå som følge av en indre motivasjon, for eksempel egne overbevisninger. Trusselaktører regnes i denne sammenheng for en aktør som har interesser i å skaffe seg adgang til en virksomhets verdier, for å påvirke disse. En del av sikring mot tilsiktede handlinger, er å gjøre trusselvurderinger, noe som blant annet er beskrevet nærmere i NS503x-serien. I en slik manipulasjonsprosess kan en trusselaktør benytte seg av sårbarheter ved en person, noe som videre i oppgaven blir kalt *individspesifikke sårbarhet*.

Intensjonen kan være til stede før en har fått legitim adgang til verdiene, eller den kan oppstå underveis Jeg vil legge til grunn en vid fortolkning av begrepet individspesifikke sårbarheter og intensjon. Intensjonalitet handler i følge Store Norske leksikon om «bevissthetens rettethet», og handler om noe villet hos individet. Når det gjelder individspesifikke sårbarheter i personellsikkerhetsmessige sammenheng, går disse utover det som individet har som intensjon, noe som også min ovenfor nevnte definisjon av innsideren inkluderer gjennom den ubevisste innsideren. Individspesifikke sårbarheter kan altså omhandle sider ved personen som kan utnyttes av en trusselaktør uten at personen selv har et ønske – eller intensjon – om å påføre virksomhetens verdier skade. Dette kan være handlinger som å la en dør stå en dør som skal låses være åpen, eller at man trykker på linker på en e-post som gir en trusselaktør informasjon eller tilgang til informasjon.

En annen måte ubevisst innsider-virksomhet kan skje, er gjennom forledelse, manipulering og utnyttelse får en person til å foreta en handling (NSM, 2020). Dette kan være for eksempel at man forteller om en virksomhets sårbarheter til en person som egentlig viser seg å være en trusselaktør. Handlinger av denne typen kan henge sammen med lav sikkerhetsmessige bevissthet hos den det gjelder, og virksomhetsspesifikke sårbarheter som dårlig sikkerhetsstyring.

Eksempel fra virkeligheten; Ubevisst innsider
I 2018 satte en person som jobbet i en norsk IKT-virksomhet virksomhetens verdier i fare for å bli tilgjengelig for andre, og gjorde seg på denne måten til det man kan kalle en ubevisst innsider. Som et ledd i å sikre et rom som inneholdt sensitiv driftsteknisk utstyr, satte han opp et kamera for å overvåke dette rommet. Bildene ble overført til hjemmesiden hans, som var offentlig tilgjengelig gjennom internett.

Kapasiteten handler om de faktiske *tilgangene*, kunnskapen og personlig egnethet til å bedrive innsidervirksomhet. Kapasiteten til personen, vil gjenspeile hvor mye skade vedkommende kan utgjøre ved å bli en innsider. Dersom en person har store tilganger, for eksempel adgang til høygraderte systemer og informasjon i offentlig sektor, så vil denne personen ved å bedrive innsidervirksomhet utgjøre et stort skadepotensial. Dette kan man derfor regne som konsekvenssiden av risiko-begrepet.

Muligheten er den faktiske anledningen som personen har for å bedrive innsidervirksomhet, og handler om hvilke rutiner og sikkerhetstiltak som finnes i virksomheten. Dette handler om hvorvidt en virksomhet har gode barrierer for å forhindre innsidervirksomhet, slik som adgangsstyring, sikkerhetskultur og oppfølging av ansatte. Jeg vil i min oppgave kalle dette for virksomhetsspesifikke sårbarhet.

5.1.4 Valg av perspektiv på risiko

Når jeg skal velge tilnærming til risiko i min modell, vurderer jeg at det er mest hensiktsmessige å se disse tilnærmingene i sammenheng fremfor å låse meg til ett perspektiv. De ulike tilnærmingene vurderer i stor grad mange av de samme faktorene, men tar i bruk noen ulike begreper for å beskrive risikoen og kan dermed komplettere modellen. Det er hensiktsmessig at modellen hovedsakelig bygges rundt begrepene *intensjon*, *kapasitet* og *mulighet*. Jeg vil derfor bygge videre rundt disse begrepene, med utgangspunkt i de ulike perspektivene på risiko.

Det er derfor viktig i modellen inneholder sårbarhetene som utgjør innsiderrisikoen. Dette gjelder både innenfor faktoren *intensjon* og *individspefikke sårbarheter*, og innenfor *mulighet* og *virksomhetsspesifikke sårbarhet*. Dette er begge forhold som kan tenkes å bli utfordret av en *trusselaktør*, som definert etter trefaktormodellen, og hvor «systemet», da henholdsvis individet og organisasjonen, blir utsatt for et stress hvor det mulig kan medføre tap av verdi.

Eksempler på førstnevnte kan være at en persons økonomiske problemer kan medføre at en trusselaktør kan bedrive manipulasjon gjennom forledelse og fristelse, mens eksempel på sistnevnte kan være at en person gjennom en stressende arbeidsdag ikke klarer å følge de sikkerhetsrutiner som finnes og derigjennom muliggjør at informasjon eller tilgang til informasjon eller fysiske steder. Manglende sikkerhetskultur eller systemer som fanger opp mistenkelig atferd, kan være virksomhetsspesifikke sårbarheter. Dette er tema som jeg vil drøfte dypere senere oppgaven i iterasjon 2.

Kapasiteten handler om verdiene som personen har tilgang til, En person uten *tilganger* til noe av sensitiv karakter, vil vanskelig kunne bli en innsider utover rene vilkårlige tilganger til informasjon. Dette handler i stor grad om skadepotensialet som vedkommende kan utgjøre gitt at den blir en innsider, og dette gjenspeiler derfor hovedsakelig konsekvenssiden av risikobegrepet, som blant beskrevet i tilnærmingen kombinasjonen av usikkerhet og mulige konsekvenser. Det er derfor naturlig at må gjenspeiles gjennom mulige scenarier som innsidervirksomheten kan lede frem til.

Mulighet, intensjon og kapasitet er tre momenter som jeg vil jeg fra nå av kalles faktorer. Jeg vil videre argumentere for at ved å bygge en modell med basis i disse faktorene, er dette i tråd med teoriene om rutineaktivitet og rasjonell-aktør-teori. I modellen som jeg skal utarbeide gjennom oppgaven så skal individet risikovurderes, og man ser på dens motivasjon som gjerningsperson gjennom de sårbarhetsindikatorene som man finner under faktoren intensjon. Det er videre slik at for mine oppgave så er målet for en eventuell gjerningsperson en virksomhets verdier, mer spesifikt informasjon som er sensitiv eller gradert, og denne sikres blant annet gjennom ulike virksomhetsspesifikke barrierer. Godheten av, eller mangelen på, barrierer er det ment at faktoren mulighet skal gi et mål på, blant annet gjennom risikoindikatorer på virksomhetsspesifikke sårbarheter. Det handler altså om å finne den motiverte gjerningspersonen som befinner seg på et sted hvor målet har minst beskyttelse, for å kunne håndtere denne risikoen.

Intensjon

En viktig del av intensjonen, er at må foreligge grunner til at en person selv velger å bli en innsider, eller at personen kan påvirkes eller manipuleres til å bli det. Dette er det som vi kaller *individspesifikke sårbarheter*. Sårbarheter i denne sammenhengen defineres i rapporten Sikkerhet ved ansettelse (Nasjonal sikkerhetsmyndighet, Kripos, Politiets sikkerhetstjeneste,

Økokrim, 2017) som «forhold ved en person som kan medvirke til at han handler i strid med virksomhetens interesser, enten fordi andre utnytter dem, eller fordi de gir personen motivasjon til å utføre slike handlinger.»

Hensikten med personellsikkerhet er å håndtere den sårbarheten som mennesket kan utgjøre mot en, slik at etter trefaktor-modellen kan en si at sårbarheten på et overordnet nivå er mennesket. Mennesket er videre et komplekst system, med ulike sider som kan påvirke egen sårbarhet i positiv og negativ forstand, og denne listen er ikke uttømmende.

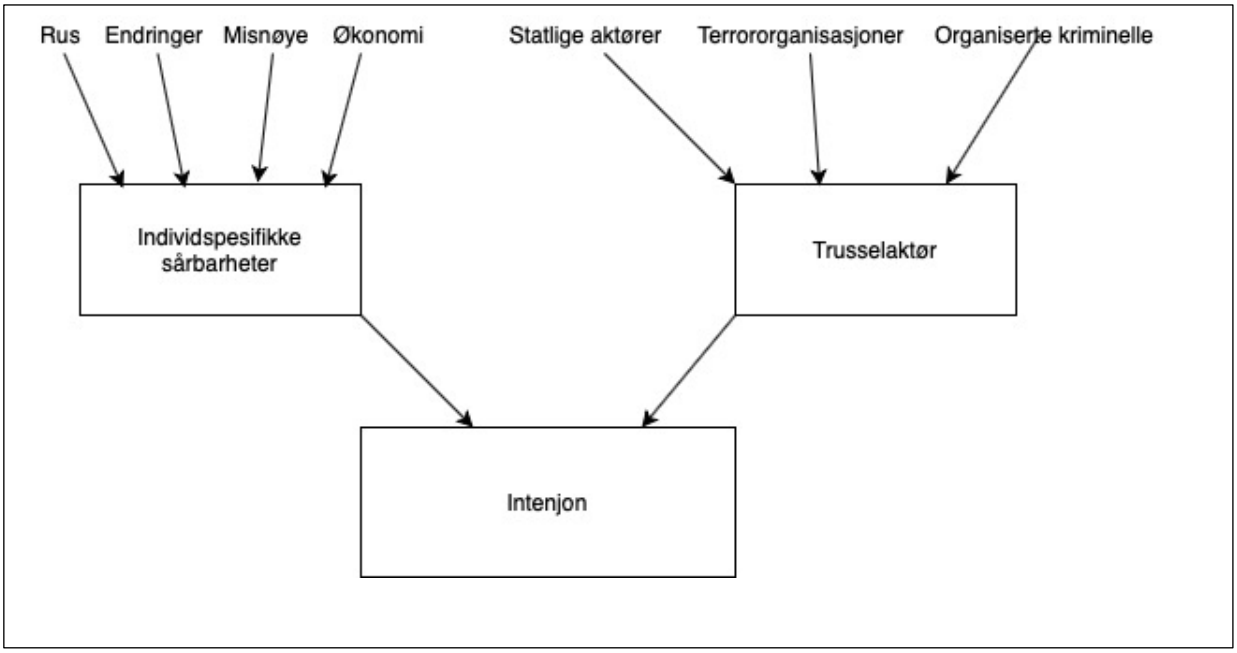
En annen viktig faktor for å vurdere den totale intensjonen for innsidervirksomhet, er om det finnes en trusselaktør. Det kan på den ene siden hevdes at det alltid vil kunne finnes en trusselaktør dersom en først har valgt å gjøre noen av sine verdier konfidensielle eller beskytte disse. Spesielt når en skal gjøre en risikovurdering basert på betingede sannsynligheter gjennom et kausalt nettverk, er det god grunn til å gjøre gode vurderinger hva angår sammenhenger mellom for eksempel trusselaktører og ulike typer informasjon.

Et trinn i trefaktormodellen er å gjøre en trusselvurdering, hvor en skal vurdere hvorvidt det finnes en trussel mot den gitte verdien. Disse truslene kan for eksempel være i form av terror, spionasje, sabotasje eller annen kriminalitet (Forsvarsbygg, 2019). Selv om en på en side kan si at all innsidervirksomhet i sin natur er spionasje, er det viktig å bemerke at trusselaktørene også kan komme fra de andre kategoriene. Terrororganisasjoner kan ha interesser i å skaffe seg gradert informasjon om et gitt objekt, for eksempel i den hensikt å utnytte dette i et terrorangrep. Kriminelle organisasjoner kan ha interesse i å skaffe seg informasjon som kan brukes til å gjennomføre innbrudd eller lignende.

I en trusselvurdering trekker FFI (2015) frem momenter som om det er noen tilstedeværende som kan utføre operasjoner mot verdien, har kapasiteten og vilje til å gjøre det. Når en vurderer trusselaktører, må dette være en konkret vurdering av trusselen oppimot den gitte verdien. I min oppgave er det spesifikt satt å gjelde informasjon. I denne sammenhengen kan man vise til PSTs årlige trusselvurdering (2021) som for eksempel trekker frem land som Kina, Iran, Russland og Pakistan er land som er ventet å drive etterretningsvirksomhet mot norsk forskning og teknologi. En kombinasjon av til informasjon om teknologi, og tilknytning til Pakistan vil i denne sammenheng kunne indikere et forhøyet risikonivå.

Jeg vil i denne sammenhengen videre vise til Hegghammer (2016), som viser hvordan ulike terrororganisasjoner kan virke som en trusselaktør også innen innsiderfeltet. Her trekkes det for frem at det er lite som tyder på at slike organisasjoner bevisst jobber for å rekruttere eller plassere innsidere, men at de bruker disse der hvor de dukker opp. Han viser her til innsider-caser med en omvendt rekruttering, hvor innsideren selv gjør seg tilgjengelig for trusselaktøren. Jeg vil gjøre diskusjoner rundt hvordan en kan definere ulike trusselaktører til et spesielt tema i samtale med ekspert 1.

I vedlegg 1 finnes en tabell for beskrivelse av intensjon etter iterasjon 1.



Figur 5: *Her ser vi hvilke påvirkende faktorer jeg så langt har identifisert for faktoren «intensjon».*

Kapasitet

Den ene delen av innsiderrisikoen, er kapasiteten som et individ har til å bedrive innsiderrisikoen. Dette handler om hvilke tilganger vedkommende har, og hvor sensitiv informasjonen man har tilgang til er. Jeg har innledningsvis arbeidet utfra på hvilken tilknytning personen har til virksomheten og tilganger.

Tilknytningen som en person har til virksomheten vil påvirke hans kapasitet. Jeg har i denne sammenhengen sett til definisjonen av en innsider. Innsideren er snakk om en person med legitim tilgang, og etter definisjon er det snakk om en ansatt, tidligere ansatt, kontraktør eller gjest. Av disse vil den ansatte utgjøre en større enn de øvrige, da vedkommende i uviss

fremtid vil kunne skaffe seg informasjon og trolig kjenner virksomheten bedre. Tidligere ansatte kan besitte svært kritisk informasjon, men vil likevel utgjøre en mindre risiko all den tid de per definisjon ikke lenger skal ha tilgang lengre. Det vil dog innenfor for eksempel teknologi kunne ligge et betydelig skadepotensial ved en tidligere ansatt.

Konsulenter og kontraktører vil kunne ha store tilganger, men som oftest vil dette være begrenset i tid og omfang. Dette er derfor definert som egen node. Gjest er definert som egen node, og en kategori som kan favne relativt bredt, slik som nærstående, forretningspartnere, personell på jobbintervju mm. Det er en vanskelig gruppe å definere, da det vil foreligge en viss usikkerhet knyttet til omfanget og varigheten på deres tilganger. Generelt kan man si at gjester har en begrenset kapasitet gjennom sine legitime tilganger til å påvirke virksomhetens verdier, men det vil åpenbart foreligge et visst skadepotensial dersom for eksempel faktoren mulighet, for eksempel gjennom en dårlig sikkerhets- eller adgangsstyring gir rom for det.

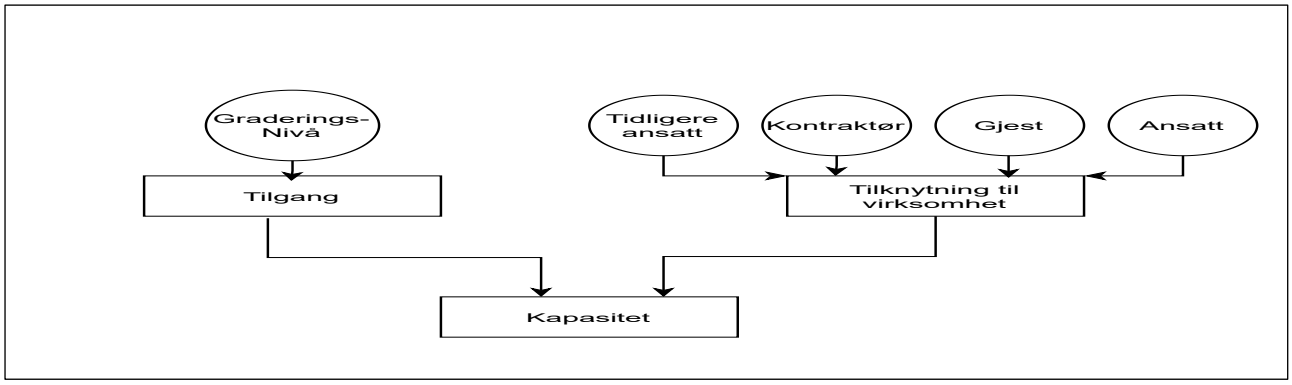
Muligheten for at ulike typer tilknytning til arbeidsplassen kan kombineres, for eksempel en tidligere ansatt som fremdeles har tilgang til lokalene som gjest eller er innleid som konsulent, er grunnen til at jeg har valgt å bruke foreldrenoder for tilstanden «Tilknytning til virksomheten».

Geller (2016) skriver at kontekstuelle faktorer må inn i et program for hvordan en virksomhet skal håndtere innsidertrusselen, og peker på at en stor feil som gjøres er en antagelse om at alle i organisasjonen stiller likt når det gjelder hva slags verdier og informasjon man har tilgang til. Det trekkes frem at ulike roller som personell har, vil være styrende i denne sammenheng. Tilgangene som vedkommende har, kan generelt videre deles opp etter de graderingene som finnes etter norsk standard. Dette går fra ingen, skjermet, begrenset, konfidensielt, hemmelig, strengt hemmelig med tilhørende NATO-graderinger. I tillegg er det noe informasjon som er beskyttet av andre hensyn enn sikkerhetsloven, som er sensitiv. Dette er standarder som finnes innenfor disse domenene og som tar utgangspunkt i hvilket skadepotensial det kan ha dersom informasjonen blir kjent for andre. Dette er enkelt for de virksomhetene som er underlagt disse lovgivningene, men er likevel en måte å klassifisere informasjon innen andre typer virksomheter.

Jeg vil her trekke fram at personell som i utgangspunktet er gitt samme klareringsnivå, ikke nødvendig behøver å utgjøre den samme kapasiteten. Det vil også gjelde hvorvidt personell

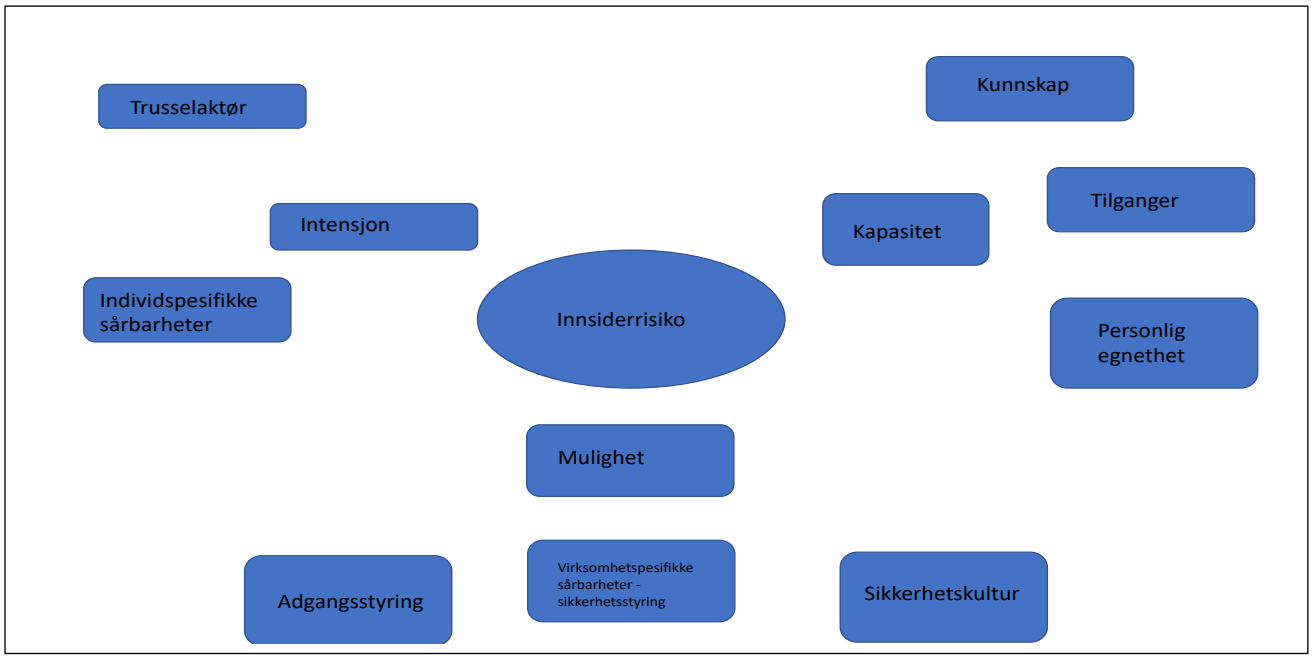
har tilgang til samme system. Kontekstuelle faktorer må inn her også. Det må vurderes om det kan være en egen kategori for spesielle typer personell som har spesielle typer tilganger, adganger eller kunnskap. Dette kan være at personell med administratorrettigheter til et system, sikkerhetspersonell eller lignende. Dette er noe som jeg har valgt å gjøre til et særskilt tema i intervju med eksperter. Jeg legger til grunn at tilgangen kombinert med tilknytningen kombinert vil kunne sies å utgjøre det totale kapasiteten. En konsulent med tilgang til informasjon på høyeste graderingsnivå, vil ha tilgang til ha tilgang til informasjon på samme nivået som en fast ansatt med samme klareringsnivået. Forskjellen vil ligge i varighet og omfang på denne tilgangen.

I vedlegg 1 finnes disse nodene oppsummert i tabellform.



Figur 6: *Kapasitet som en kombinasjon av tilknytning til virksomheten og skadepotensialet.*

Utfra tabellene ovenfor står jeg nå igjen med følgende modell etter første iterasjon:



Figur 7: *Så langt i oppgaven legger jeg til grunn at dette kan sies å være de påvirkende faktorene til innsiderrisiko.*

5.1.5 Type informasjon

Et annet moment som jeg har vurdert kan være relevant i denne sammenhengen oppimot faktoren «Kapasitet», er den typen informasjon som personen har tilgang til. For eksempel vil det kunne være rimelig å tenke seg at en organisert kriminell gruppering vil ha mer interesse av informasjon om beredskapsmessige forhold ved våpenlager enn informasjon om mellomstatlige relasjoner.

Dette er også i tråd med Gelles sine tanker som ovenfor nevnt, da det er en del av den kontekstuelle faktoren i vurderingen av innsiderrisikoen. Et spørsmål som jeg har stilt meg er hvorvidt man kan «parre» typen informasjon som en person har, eller vurderes å få, oppimot hvilke trusselaktører som er aktuelle. Jeg har derfor vurdert at det er mulig å vurdere en node som sier noe om hvilken type informasjon som vedkommende har tilgang til. De nasjonale interessene listes opp i straffeloven § 121, og utfra disse har jeg delt inn informasjonen i følgende kategorier:

- Forsvar/sikkerhet/beredskap
- Politiske beslutningsprosesser og forholdet til andre stater
- Infrastruktur
- Naturressurser

Det fremkommer videre i PSTs årlige trusselvurdering av 2021 at det er påregnelig at statlige etterretningstjenester vil rette etterretningsvirksomhet og ulovlig kunnskapsoverføring mot akademia, teknologi innen romfart, maritim teknologi, forsvarsindustri og helse blant annet gjennom spionasje mot norske virksomheter. Det er derfor naturlig å legge til følgende kategorien «Forskning og teknologi». Temaet om type informasjon er et spørsmål som jeg har valgt å ta med meg inn i intervju med ekspertene.

5.2 Andre iterasjon

Jeg valgte å dele innledende iterasjoner for vurdering av faktorene kapasitet og intensjon fra faktoren mulighet. Grunnen til at dette er gjort, er fordi det krever annen litteratur å bygge delmodellene. I NSMs innsiderrapport (2020) nevnes manglende sikkerhetsstyring og sikkerhetskultur, manglende risikoforståelse og diverse forhold på arbeidsplassen som virksomhetsspesifikke faktorer som kan føre til at muligheten for innsidervirksomhet

inntreffer. Dette har ikke vært veldig enkelt, da mange av de tingene som fører til virksomhetsspesifikke sårbarheter kan være relativt abstrakte og i liten grad målbare.

5.2.1 Sikkerhetskultur

Når en ser på teorier og forskning innen sikkerhet og ulykker, er det fremtredende at det er en viss endring i forståelsen av sårbarhet og organisering de siste tiårene (Kruke, Engen, Lindøe, Olsen, & Pettersen, 2012). Man ser i dag utover det man kan kalle individuelle feil og misforståelser fra enkeltpersoner, og fra et systemisk perspektiv. Enkelt forklart er det nå mange som argumenterer for at feil på individnivå ikke skal behandles som en årsak, men en konsekvens av en systemfeil. Det skal dog være sagt at mye av denne forskningen og teoriene på feltet, blant annet kjente teorier fra Perrow, Turner og Reason, baserer seg på ulykker og katastrofer. Det er med andre ord ikke gjort direkte for risiko knyttet til innsidere spesifikt eller tilsiktede handlinger mer generelt.

Sikkerhetskultur handler om atferd som er knyttet til sikkerhet, og handler om blant annet kunnskap, holdninger, motivasjon og atferd. NSM (2010)skriver at sikkerhetskultur kan defineres som

*«En **sikkerhetskultur** kan defineres som et sett med verdier som deles av medarbeidere i en virksomhet, og som er med på å påvirke deres tanker og forventinger til sikkerhet. Ved å motivere medarbeiderne til å handle på en måte som ivaretar sikkerheten, kan virksomheten skape en god **sikkerhetskultur.**»*

Zegart (Plassholder1) viser til at fire momenter fra forskning på storulykker som belyser hvorfor amerikanske myndigheter feilet med å stoppe angrepet på Fort Hood, av en voldelig innsider som utførte et terrorangrep på militærbasen. Disse fire momentene er at slike hendelser aldri egentlig er overraskelser, at det ligger «gjemte» farer innbakt i organisasjoners rutiner, karriereinsentiver som virket galt til feil tid og at organisasjoner betyr mer enn man tenderer til å tro.

Jeg vil argumentere for at sikkerhetskultur, enn dog så abstrakt et begrep, er av en slik karakter at man kan se til denne forskningen for å vurdere godheten av en sikkerhetskultur. Jeg vil derigjennom finne relevante momenter som gjør det mulig å måle sikkerhetskultur og gjøre det til en del av modellen. Et moment som naturlig må drøftes når det gjelder sikkerhetskultur, er hvorvidt en virksomhet er under stort tids- og effektivitetspress. Perrow (1999) skriver at søkelys på ledelse og kultur kan flytte fokus over på andre kritiske spørsmål som må stilles, og dette kan også være tale om spørsmål som vekter balansen mellom for eksempel hensynet til sikkerhet og hensynet til effektivitet. Mål om fokus på effektivitet og

produksjonspress, vil kunne føre til konsekvenser for fokuset som er på sikkerhetsmessige spørsmål.

En egen node i denne sammenhengen må derfor bli «Tids- og produksjonspress». Dette synliggjør også hvordan en slik modell må være dynamisk, da ulike virksomheter kan ha variasjoner i slikt press. Denne kan settes til tilstanden høyt, middels og lavt. Et tenkt eksempel på en virksomhet med høyt tids- og effektivitetspress kan være operative avdelinger med høyt operasjonstempo og operative leveranse.

Et moment som i denne sammenhengen er viktig, er virksomhetens sikkerhetsorganisasjon. Jeg vil argumentere for at virksomheter med det en kan betegne som en *svak* sikkerhetsorganisasjon, over tid vil kunne være mer sårbar for at sikkerheten og derfor sikkerhetskulturen nedprioriteres. Å vurdere godheten av en sikkerhetsorganisasjon er dog ingen selvsagt oppgave.

Jeg har sett til Antonsen (2009) som har skrevet om hvordan makt og sikkerhetskultur henger sammen. Denne makten har tre dimensjoner, hvorav de to første handler om hvorvidt en kan få andre til å gjøre som en vil, mens den andre er hvorvidt man har definisjonsmakt til å sette en agenda.

Dersom en sikkerhetsorganisasjon skal være god i denne sammenhengen, må den ha makt til å kunne få personell til å handle som de vil, for eksempel ved å følge gitte prosedyrer og rutiner, samt ha evnen til å sette sikkerhet på agendaen. Jeg vil legge til grunn følgende faktorer, med tilstandene «Lav», «Middels» og «Høy», som kan være medvirkende:
Sikkerhetsorganisasjonens plassering i virksomheten. Er den plassert lav i et hierarki, eller svarer den direkte for en sjef.
Vurdering av sikkerhetslederen. Her må momenter som sikkerhetslederens erfaring, tid i stillingen o.l. trekkes inn.
Sikkerhetsorganisasjonens størrelse. Å etablere et godt system for å håndtere forebyggende sikkerhet, herunder et styringssystem som tar høyde for innsidervirksomhet, er krevende og krever både tid, kompetanse og personell. Sikkerhetsorganisasjonens størrelse relativt til virksomheten størrelse vil derfor kunne være en indikator på tilstanden til virksomhetens sikkerhetsstyring.

Jeg har også vurdert at mengden av sikkerhetsbrudd kan stå som en indikator på hvor god sikkerhetskulturen er i avdelingen. Det er åpenbare problemer med å konkludere med at en virksomhet med et høyt antall sikkerhetsbrudd har dårlig sikkerhetskultur, da dette i seg selv kan indikere at avdelingen har en god rapporterende kultur. Jeg har likevel satt det som en foreldrenode til sikkerhetskultur, men hvor vektingen bør gjøres forsiktig.

5.2.2 Sikkerhetsstyring

Manglende sikkerhetsstyring trekkes frem som en faktor som kan medvirke til at innsidervirksomhet vil kunne finne sted innenfor en virksomhet. Sikkerhetsstyring kan defineres som systematiske aktiviteter for å oppnå og opprettholde et sikkerhetsnivå i tråd med organisasjonens mål og oppdrag. Det er ikke åpenbart hvordan man skiller hvilke risikoindikatorer som påvirker sikkerhetsstyringen og hvilke som påvirker sikkerhetskultur, og i mange tilfeller vil de påvirke begge.

Ifølge James Reason (1997) består en fungerende sikkerhetskultur av fire subkulturer, blant annet rapporteringskultur. At en kultur er rapporterende, betyr at den har effektive og gode rutiner og systemer for varsling om forhold, for eksempel sikkerhetsbrudd og nesten-ulykker. Dette forutsetter et rapporteringssystem, og en beskyttelse mot sanksjoner så langt som mulig, enkelthet i rapporteringen, mulighet for anonymitet og tilbakemelding trekkes frem som viktige momenter ved et slikt system (Reason, 1997) Hvordan man skal vurdere et rapporteringssystem er vanskelig. Jeg viser i denne sammenhengen til Gelles (Gelles, 2016), som skriver at det et åpenbart problem på dette området er at mange virksomheter mangler rapporteringssystem. En risikoindikator er derfor om hvorvidt det finnes et rapporteringssystem for uønskede hendelser.

Et moment som trekkes frem i NSMs temarapport om innsidere (2020), er hvordan en manglende risikoforståelse i seg selv kan gjøre at virksomheter utsetter seg for risiko som de selv ikke evner å identifisere. Et eksempel som kan trekkes frem i denne sammenheng, er universitets- og forskningsmiljøer som tar inn studenter fra land som har etterretningsmessige interesser mot norske verdier.. (Bunn & Glynn, Preventing insider Theft: Lessong from the Casino and Pharmaceutical Industries, 2016)

Eksempel fra virkeligheten: Manglende risikoforståelse og gjester
29.10.2021 meldte NRK at en tysk-iransk forsker ved NTNU var tiltalt for å ha gitt iranske gjesteforskere tilgang til informasjon om teknologi som kunne gi de informasjon om oppbygging av atomvåpen, og som derfor var i strid med lov og forskrift. Dette var en hendelse hvor NTNU selv hevder de hadde rutiner for, og meldte selv om forholdet til PST. Det ble likevel gjort da forskerne ikke fulgte disse rutinene. En annen ting som dette belyser er hvordan en gjest også kan være en innsider, da dette er personer som er invitert til universitetet og kan ha fått tilgang til informasjon gjennom dette oppholdet som kan være til fremmed stats fordel. (Norsk rikskringskasting, 2021)

For min modell, har jeg valgt en enkel tilnærming til dette. Jeg vurderer at det i denne kategorien kan opprettes en node for «Utsatt bransje», hvor en vurdering av hvorvidt bransjen som personen som vurderes befinner seg innen generelt kan vurderes å ha en god risikoforståelse. Dette er en node som i stor grad må vurderes av en ekspert for at den skal operasjonaliseres, og vil utvilsomt være avhengig av subjektive vurderinger.

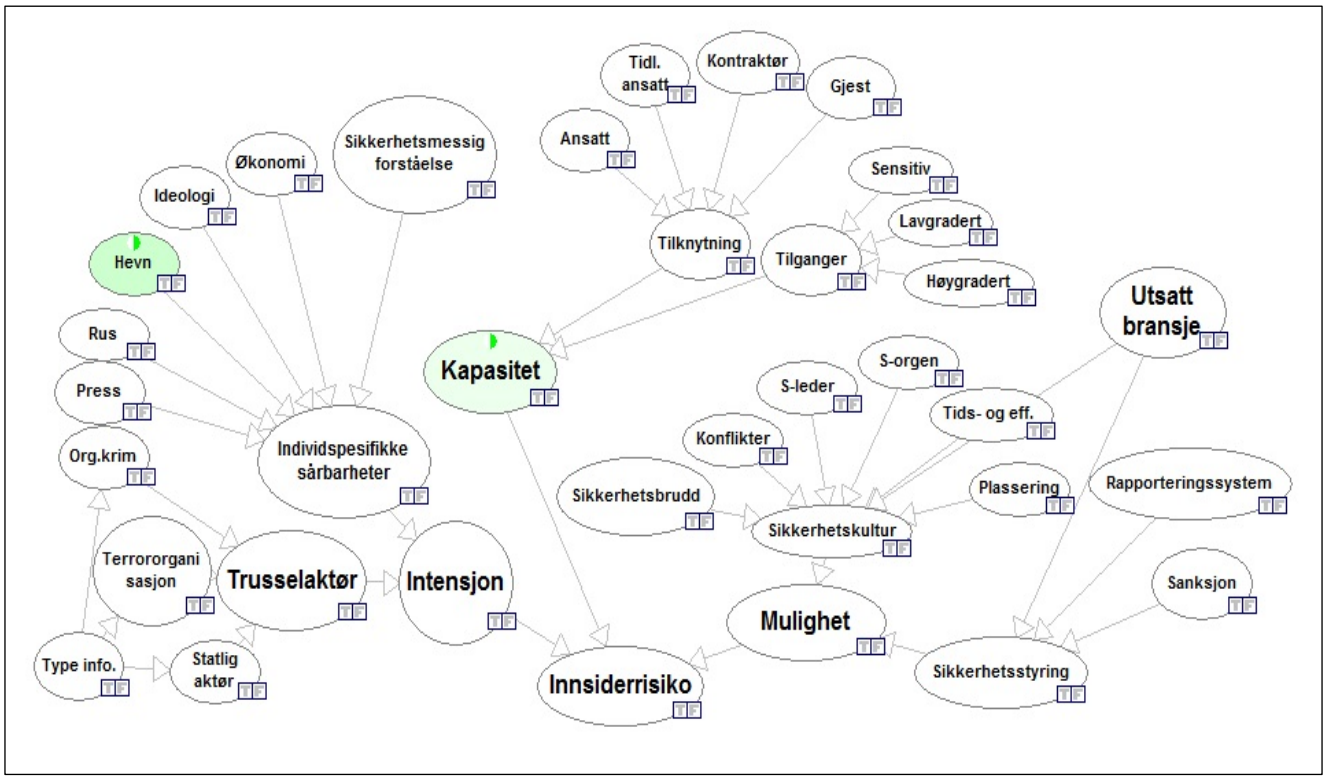
Forhold på arbeidsplassen

Ulike hendelser og tilstander på arbeidsplassen vil medføre at det kan foreligge en noe større sannsynlighet for innsidervirksomhet og lekkasje av informasjon, for eksempel fra hevngjerrige ansatte i en prosess som de er uenige i. Dette kan være en vanskelig node å definere, men kan være en sekkepost for om det foreligger konflikter, store forandringer eller annet som kan skape misnøye ved arbeidsplassen.

I juni 2020 stod daværende forsvarsminister, Frank Bakke-Jensen, i Stortinget og pekte på at det var dokumenter i forbindelse med en omstridt prosess som gjelder nedleggelse av Andøya flystasjon som hadde kommet ut. Han pekte på at dette var snakk om utro tjenere. Dersom disse opplysningene stemmer, er det gode grunner til å anta at dette kan være snakk om innsidere som lekker informasjon som følge av en pågående konflikt som følge av omstrukturering. (Bladet vesterålen, 2020)

5.2.3 Noder og modell andre iterasjon

Utfra dette har jeg utarbeidet en tabell, som finnes i vedlegg 2. Modellen etter iterasjon 2 ser ut som følger:



Figur 8: *Dette er nettverket etter andre iterasjon.*

5.2.3 Evaluering av iterasjon 1 og 2

Det er gjort ett intervju med en ekspert i iterasjon 1 og 2. Intervjuet er foretatt med en rådgiver i Forsvarets sikkerhetsavdeling, som har utdanning på mastergradsnivå innen organisasjonsvitenskap og med over 10 års erfaring fra Forsvaret og justissektoren, hvorav cirka halvparten innenfor fagfeltet personellsikkerhet.

Ved intervjuet i iterasjon 1 og 2, presenterte jeg ikke en midlertidig modell for eksperten, men presenterte modellen lagvis og spurte spørsmål spesifikt knyttet til mine forskningsspørsmål. Jeg startet intervjuene med å forklare hva et bayesiansk nettverk er, og tegnet blant annet opp et enkelt ett. Jeg forklarte i denne sammenhengen oppbygningen med risikoindikatoren, faktorer og hendelser. Generelt så vurderte jeg at eksperten hadde god forståelse for hvordan et bayesiansk nettverk kan fungere i personellsikkerhetsmessig sammenheng, noe som gjorde at intervju-situasjonen foregikk med en gjensidig forståelse av oppgaven.

Da jeg hadde oppsummert svarene til eksperten, gikk jeg gjennom oppsummering og så gjennom om det fremdeles var momenter som fremstod uklare for meg eller steder hvor jeg ønsket en videre utgreiing. Disse momentene sendte jeg deretter til eksperten på e-post, hvor han svarte meg ut. Dette er også tatt med i den følgende oversikten. Jeg har oppsummert intervjuet i resymeform, en rapport som eksperten selv fikk lese gjennom og komme med sine rettelser og tilføyelse til gjennom et oppfølgende intervju. Disse er også tatt med videre. Resyme av samtalen ligger som vedlegg til oppgaven, vedlegg 5.

5.2.4 Revidering iterasjon 1 og 2

Jeg står igjen med følgende hovedpunkter som vil være nødvendig å gjøre utbedringer i forhold til ved iterasjon 3:

Enkelthet i modellen: Eksperten var gjennomgående opptatt av brukergrensesnittet og brukervennligheten i modellen. Jeg tenker at dette er et vesentlig moment, og det er liten hensikt i å lage et system som ikke blir brukt etter hensikten fordi brukeren ikke forstår den fullt ut. Den direkte følgen av dette for iterasjon 3, er at jeg vil se ha fokus på å holde antallet noder på et fornuftig nivå og at de skal være intuitive. Et komplekst nettverk kan tenkes å kunne gi mer nøyaktige risikovurderinger, og kan gjøre at man unngår falske positive. Jeg ser likevel i denne sammenhengen til ekspertens uttalelse om at falske positive i seg selv ikke trenger å være veldig negativt, da behov for undersøkelser skaper en dynamisk og god sikkerhetsorganisasjon.

Særskilte personellgrupper: Eksperten trekker frem at det i organisasjoner vil være slik at personell som hovedregel er mer eller mindre avskåret fra informasjon som ikke tjenstlig relevant for dem, og at man for å skape et helhetsbilde av et prosjekt, en teknologi mv., vil trenge å innhente informasjon fra svært mange. Han peker likevel på at det vil være noen nøkkelfunksjoner i en virksomhet som ha en kapasitet og mulighet til å skaffe til veie store mengder informasjon uten at dette nødvendigvis hindres av et system eller vekker mistanke. Den direkte konsekvens for iterasjon tre er at jeg vil se nærmere på denne faktoren, og forsøke å definere den nærmere.

Risikoindikatorer på individnivå: Eksperten trakk under samtalen frem sikkerhetsloven § 8-4, fjerde ledds bokstav a til o som et godt utgangspunkt for å bygge et nettverk. Jeg vil derfor se primært til denne lovbestemmelsen i byggingen av nettverket. Det vil trolig likevel være behov for å se til annen litteratur. Han viser også til «MICE-modellen» for innsidervirksomhet, og jeg vil forsøke å vurdere om dette kan gjøres til faktorer i modellen, det vil si det midterste laget med påvirkende faktorer i modellen.

Kontraktører: Kontraktører må gis tung vekt i modellen, og det vises i denne sammenhengen til at et rådende standpunkt i mange bransjer er at kunnskap og rutiner enten bevisst eller ubevisst forsvinner ut av bedriften med personell
Gradering av sikkerhetsstyringen: Eksperten sa at kravene i sikkerhetsloven kan brukes ovenfor de som er underlagt denne. Jeg tenker at jeg uansett vil søke mer informasjon fra denne i denne sammenheng, da momenter som trekkes frem i denne også kan være aktuelle momenter for virksomheter som ikke er underlagt den.
Rapporteringssystem: Eksperten mener at det mulig ikke er hensiktsmessige med en Ja/nei-tilstand som gjelder om virksomheten har et rapporteringssystem for uønskede hendelser eller andre varslinger innen sikkerhetsarbeidet. Det vil derfor være nødvendig å definere en slags tredje node som står for at man har et rapporteringssystem, men som av ulike grunner ikke i stor grad i bruk.
Bruk av kontraktører og joint events: Eksperten snakket om situasjoner med bruk av kontraktører og joint events, hvor ulike deltagere i et prosjekt kan være underlagt ulike sikkerhetsopplegg og -rutiner og det kan være uavklarte forhold, blant annet knyttet til ansvar. Han vurderte at en slik situasjon i seg selv kunne medføre en forhøyet sannsynlighet for innsidervirksomhet, men at han mente det var vanskelig å se hvordan dette kunne gjøre seg gjeldende i vurderingen av individet. Jeg vil se på muligheten for å vurdere hvorvidt dette kan påvirke de virksomhetsspesifikke sårbarhetene, og derigjennom kunne øke muligheten for at innsidervirksomhet vil kunne finne sted.

5.3 Tredje iterasjon

I den tredje iterasjonen, vil jeg gjennomføre funnene fra iterasjon når det gjelder virksomhetsspesifikke sårbarheter, og legge til momenter til modellen i forhold til de to første iterasjonene. Dette vil bli gjort gjennom en bygging av faktorene kapasitet, intensjon og mulighet.

Som følge av måten jeg valgte å bygge ut modellen stegvis i prosessen, ble noe av utfordringen å skape ulike noder på de forskjellige lagene i modellen i iterasjon 3. Det var derfor viktig å skape punkter som kunne brukes som variabler på input i modellen, altså gode risikoindikatorer som kunne gi grunnlag for å vurdere faktorer som kan lede frem til de faktiske hendelsene. Dette ledet meg videre inn på ideen om å bygge modellen videre med bakgrunn i hjelpevariabler, og bruke ekspertens innspill om å bruke MICE-modellen og sikkerhetsloven som styrende dokumenter. Modellen er derfor delt lagvis, hvor det ytterst er

risikindikatorer, som igjen kan føre til utslag på en eller to faktorer, hvorav de fire siste vil være bygget på MICE-modellen samt en node som tar høyde for ubevisst innsidervirksomhet.

Når jeg kopler de ulike risikoindikatorene med faktorer, så vil disse lede frem til faktorer som igjen kan si noe om risikoen knyttet til hvorvidt individet vil utgjøre en innsiderrisiko og størrelsen på denne. Det er ikke mitt mål å kvantifisere modellen, men jeg vil likevel drøfte de ulike tilstandene som en node kan ha. For enkelthets skyld har jeg i de tilfellene det er naturlig satt dette til «Ja» eller «Nei», og der det er rom for en gradering brukt et trafikklys-system med lav (grønn), middels (gul) og høy (rød).

5.3.1 Bygging

Kapasitet

Kapasitet skal utgjøre konsekvensdelen av analysen, og jeg vil i det følgende definere ulike hendelser, eller scenario, som skal inn i modellen. Når det gjelder hvordan en definerer ulike hendelser/scenario, så har jeg sett dette utfra faktorene tiden som personen kan levere informasjon i eller fra, hvilken gradering det er på informasjonen og tatt høyde for at det finnes særskilt personell i virksomheter med andre muligheter for innsidervirksomhet enn andre.

Ansatte vil kunne kompromittere informasjon i lang fremtid. Gjester og konsulenter vil kunne levere informasjon i kort fremtid, mens gjester er av en slik karakter at de også trolig vil kunne levere en begrenset mengde informasjon da det ligger i kategorien at det trolig er snakk om en midlertidighet i tilknytningen. Tidligere ansatte vil kunne levere informasjon om fortid, og skal i teorien ikke kunne levere informasjon i tiden framover dersom tilganger er fjernet. Jeg har gradert informasjonen i ingen, lav, middels og høy.

TABELL 1: *Kombinasjonen av tidsaspektet og skadepotensialet til informasjon som kan kompromitteres.*

TILGANGER / **TILKNYTNING**	INGEN	LAV	MIDDELS	HØY
ANSATT	Ingen innsiderrisiko	Kompromittering av sensitiv og eller begrenset informasjon lang fremtid	Kompromittering av lavgradert informasjon lang fremtid	Kompromittering av høygradert informasjon lang fremtid
TIDLIGERE ANSATT	Ingen innsiderrisiko	Kompromittering av sensitiv og/eller begrenset informasjon fortid	Kompromittering av konfidensiell/hemmelig informasjon fortid	Kompromittering av strengt hemmelig informasjon fortid
KONSULENT	Ingen innsiderrisiko	Kompromittering av sensitiv og/eller begrenset informasjon kort fremtid	Kompromittering av konfidensiell eller hemmelig informasjon kort fremtid	Kompromittering av strengt hemmelig informasjon kort fremtid
GJEST	Ingen innsiderrisiko	Kompromittering av sensitiv og/eller begrenset informasjon svært kort fremtid	Kompromittering av konfidensiell og/eller hemmelig informasjon svært kort fremtid	Kompromittering av strengt hemmelig informasjon svært kort fremtid
SÆRSKILT PERSONELL		Kompromittering av sensitiv og/eller begrenset informasjon i ukontrollerbar mengde	Kompromittering av konfidensiell og/eller hemmelig informasjon i ukontrollerbar mengde	Kompromittering av strengt hemmelig informasjon i ukontrollerbar mengde

Med denne inndelingen i ulike scenarioer, ender man med 15 ulike scenarioer som kan gi lekkasje av informasjon som krever beskyttelse. Utfordringen er at det er mange og at flere av de er relativt like, og dette gir grunnlag for å kutte ned på antallet. Dette har jeg kuttet til fire, med et skille mellom sensitiv og begrenset informasjon, som benevnes lavgradert, og konfidensielt til streng hemmelig, som benevnes høygradert. Videre har jeg skilt mellom lang og kort tid, hvor ansatt vil være lang tid, mens gjest, kontraktør og tidligere ansatt er kort tid.

Jeg har videre brukt noden som også er lagt til grunn ved første iterasjon om at det finnes personell med særskilte tilganger og muligheter, som kan gi ekstra stort skadepotensial gitt at vedkommende bedriver innsidervirksomhet. Dette har jeg videre valgt å kalle «Høyrisikopersonell», og er en kategori av personell i organisasjonen som har ekstra store muligheter til å bedrive innsidervirksomhet ukontrollert gjennom sin funksjon, for eksempel fordi de sitter med særskilte tilganger eller muligheter til å utvide disse.

Dette er for eksempel arkivaren som eksperten nevnte i intervju ved revidering av iterasjon 1, som kan ha store tilganger som er vanskelig å begrense utfra tjenstlig behov. For mange funksjoner, for eksempel en saksbehandler, er det ofte enklere å definere hvilke tilganger og adganger personen trenger utfra sitt virke. Da kan man i større grad styre scenarioet og innsiderrisikoen knyttet til den enkelte.

Dette handler blant annet om det som Aven (2017) beskriver som styrbarheten knyttet til en risiko. Ved enkelte personellkategorier vil det være mulig å styre innsiderrisikoen de utgjør, blant annet ved klare skiller mellom hvilken informasjon som inngår i det tjenstlige behovet. Ved enkelte funksjoner, vil dette være vanskeligere å styre det tjenstlige behovet eller behovet er svært stort. Disse utgjør videre en node som jeg har kalt «Lite styrbar kompromittering».

Med dette ender vi med slutthendelsene «Lavgradert – kort tid», «Lavgradert – lang tid», «Høygradert kort tid», «Høygradert – lang tid» og «Lite styrbar kompromittering».

Intensjon

I intervju med ekspert foreslo han at man kunne bruke MICE-modellen som et utgangspunkt i modellen min. MICE er et akronym brukt av etterretnings- og sikkerhetstjeneste for å beskrive motivasjonen til en innsider (Burkett, 2013). Disse bokstavene står for følgende ord:
Money: Penger, eller den tryggheten disse kan medføre gjennom skolegang for barn, eiendom osv., fremstår som en rasjonell grunn for å utøve innsidervirksomhet.
Ideology: Ideologi, det vil si en overbevisning for eksempel av politisk karakter, kan være en sterk driver for innsidervirksomhet. Det trekkes også frem som en motivasjon som kan skape innsidere med stort skadepotensial.
Coersion: Press, det vil si ulike former for tvang, trusler e.l. ovenfor en person, er en motivasjon som er enkel å forstå. Dette kan komme fra feil eller hemmeligheter som personen har, og kan også være iscenesatt av trusselaktør.

Ego eller excitement: Av de to beskrives ego som den sterkeste driveren. Sistnevnte er tanken om at livet som «spion» er preget av spenning. Når det gjelder ego, så er det tale om personer som er del av et system som kan ha gjort dem feil og hvor det foreligger et ønske om å ta igjen eller bevise seg selv som kompetent. Dette kan være snakk om personell som «venter på å bli rekruttert».

Denne modellen møter dog noe kritikk, og beskrives som noe utdatert av Burkett (2013). Han begrunner dette med at disse faktorene kun er overflatiske faktorer som bidrar til at folk lar seg verve til å bedrive innsidervirksomhet. Han viser til at med bakgrunn i nyere forskning innen psykologi kan peke på helt andre faktorer som bidragsytende til innsidervirksomhet, og nevner akronymet RASCLS. Dette står dog for steg i en faktisk rekrutteringsprosess og hvordan en tilnærming ovenfor en person bør foregå. Dette inkluderer blant annet å sette personen i en liten gjeld for eksempel gjennom å gi noe til vedkommende; og vise autoritet ved å fremstå som en kommer fra en stor og mektig organisasjon med mer.

Eksempel fra virkeligheten: Aldrich Ames
Amerikaneren spionerte til fordel for Sovjetunionen, og møtte selv opp på den sovjetiske ambassaden i Washington for å motta penger for informasjon. Planen hans var at dette skulle være et engangstilfelle med økonomiske motiver. Da den sovjetiske kontraetterretningssjefen tok imot Ames på en god måte, og blant annet viste at han brydde seg om hans sikkerhet, satte han i en situasjon hvor han følte han skyldte noe og at de jobbet sammen om et felles mål, forble Ames innsider for en lang periode.

Jeg har, til tross for de ovenfor nevnte svakhetene ved MICE-modellen, besluttet at faktorene økonomi, ideologi og grunnlag for press skal ligge til grunn som faktorer i modellen. Dette vil være del av det midterste laget i modellen, og beskriver i faktorer for bevisst innsidervirksomhet. Dette fordi RASCLS-modellen har fokus på rekrutteringsprosessen mer enn de bakenforliggende faktorene. Dette vil være noder som gis en sannsynlig tilstand med bakgrunn i risikoindikatorer som brukeren legget inn med bakgrunn i kjent informasjon knyttet til personen som vurderes.

Disse dekker dog ikke ubevisst innsidervirksomhet. Gelles (Gelles, 2016) skriver også at det er tre typer innsider. Han snakker om den ondsinnede (malicious), den selvtilfredse (complacency) og den ignorante (ignorant). De to sistnevnte gjør det ubevisst, mens forskjellen er at den førstnevnte gjør det som følge av en avslappet tilnærming til prosedyrer og rutiner mens den andre gjør det som følge av lav forståelse og oppmerksomhet om de

rutinene som virksomheten har. Begge utsetter derigjennom virksomheten for eksterne trusler. Jeg vil utfra dette opprette en faktor som jeg kaller «Sikkerhetsmessig forståelse», og som er ment å være en faktor som skal bestå av ulike risikoindikatorer for ubevisst innsidervirksomhet.

Det kunne vært hensiktsmessig å skille disse to begrepene i modellen, men jeg har funnet at det er hensiktsmessig eller mulig å operasjonalisere risikoindikatorer på en måte som gjør at disse får et faktisk skille i modellen. En av grunnene til at jeg har ønsket å skille disse to typen innsidere, er med tanke på modellens funksjon i det daglige sikkerhetsmessige arbeidet. Begge de to ubevisste innsiderne kan tenkes å forebygge gjennom ulike tiltak, men det kan være hensiktsmessige å identifisere hvilken type det faktiske individet er og derigjennom bruke egnede tiltak og tilnærminger for å redusere risikoen.

Videre vil jeg bruke «Økonomi», «Grunnlag for press», «Ideologi» og «Sikkerhetsmessige forståelse» som faktorer i modellen, som de risikoindikatorer skal bygge rundt.

Sikkerhetslovens bestemmelser

Videre anbefalte eksperten at sikkerhetsloven § 8-4 oppsummerer ulike individspesifikke sårbarheter. Dette er de forholdene kan ligge til grunn for vurderingen av hvorvidt personer skal gis sikkerhetsklarering eller ikke. Dette er ikke en uttømmende liste, og blant annet er bestemmelsen bokstav o en slags sekkepost. Denne omhandler annet som kan gi grunn til å frykte at vedkommende vil handle i strid med nasjonale sikkerhetsinteresser. Jeg har i det videre sortert disse bestemmelsene med bakgrunn MICE-modellen, og etablert ulike risikoindikatorer til disse.

Sikkerhetsloven 8-4, fjerde ledd bokstav a

Bestemmelsen har følgende ordlyd:
«spionasje, planlegging eller gjennomføring av terror, sabotasje, attentat eller lignende, og forsøk på slik virksomhet»

Dette er med andre ord virksomhet som ligger tett oppimot, og i bred forstand i seg selv kan være, innsidervirksomhet. Det første jeg vil dra ut av bestemmelsen er ordene «planlegging», «gjennomføring» og «forsøk». Det er viktig at ikke bare den fullbyrdede handlingen

gjenspeiles i modellen, men at også faser i forkant gjennom enhver forberedelse, samt forsøk må reflekteres i modellen.

Det neste begrepet i denne sammenhengen er «spionasje». Spionasje ble etter sikkerhetsloven fra 1998 definert som «innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt». Denne definisjonen er ikke videreført i ny sikkerhetslov. Det er naturlig å se til bestemmelser som behandles i straffelovens kapittel 17, «Vern av Norges selvstendighet og andre grunnleggende nasjonale interesser» for en mer utfyllende beskrivelse av spionasje, men det skal dog nevnes at begrepene som brukes i straffeloven er «ulovlig etterretningsvirksomhet» og «avsløring av statshemmeligheter».

Det er spesielt straffeloven §§ 121-126 som dekker ulike former for ulovlig etterretningsvirksomhet og avsløring av statshemmeligheter. Straffeloven § 121 og § 122 dekker det som kalles etterretningsvirksomhet mot statshemmeligheter, og omfatter at etterretningsvirksomhet rettet mot hemmelige opplysninger knyttet til nasjonale interesser og at opplysningene må være av en slik karakter at de kan utgjøre en faktisk skade på den interessen de knyttet til (Store norske leksikon.). De nasjonale interessene listes opp i straffeloven § 121, og knytter seg blant annet til forsvars-, sikkerhets- og beredskapsmessige forhold, naturressurser, forholdet til andre stater, infrastruktur, de øverste statsorganers sikkerhet og handlefrihet mm.

Videre nevnes planlegging og gjennomføring av terror, sabotasje, attentat eller lignende. I denne sammenhengen ser jeg til straffelovens kapittel 18 «terrorhandlinger og terrorrelaterte handlinger» sine bestemmelser som gjelder terrorisme, som er et utfyllende regelverk. Etter straffeloven § 131 slås det fast at det er et bredt utvalg av straffbare handlinger som kan anses som en terrorhandling. Det spesielle for at terrorhandling skal være aktuelt, er at det foreligger en terrorhensikt.

Terrorlovgivningen i Norge rammer også flere former for forberedelser til terrorisme, og beskrives av Engene (2013) som at enhver planlegging av terrorisme kan straffes og gir mulighet til å gripe inn ovenfor personer som planlegger terrorisme. Dette regelverket forbyr blant annet deltagelse i trening for terrorisme, finansiering mm. Det vil derfor være god grunn til å legge den brede norske terrorlovgivningen, til grunn for hva som kan regnes som planlegging av eller gjennomføring av terrorisme i et personellsikkerhetsmessig perspektiv.

Når det gjelder personellsikkerhet, så knyttes terrorvirksomhet seg til flere av nodene. Den mest åpenbare risikoen er at personell med tilgang til informasjon bruker den til å planlegge eller bistå med planlegging, eller at en bruker adganger for å utføre terrorisme, for eksempel mot materiell eller personell innenfor et beskyttet område som for eksempel forsvarsinstallasjoner eller kraftforsyning. Terrorisme vil videre ofte knytte seg til ideologi, og for eksempel nevnes høyreekstremisme, ekstrem islamisme og venstreekstremisme som ideologier det i Politiets sikkerhetstjeneste sine siste årlige vurderinger. Det er videre viktig å ikke la seg begrense av disse tre bolkene av ideologier som kan føre til terrorisme, og i PST siste årlige trusselvurdering (2021) nevnes også at anti-statlige strømninger og miljøsak vil kunne radikalisere personer det kommende året. En åpenbar kopling når det gjelder terrorisme er derfor ideologi. Det kan også derigjennom medføre knytninger til ulike organisasjoner, som vil bli drøftet videre under bokstav l. Det vil også være et spørsmål om lojalitet til lovverk.

Nodene etter denne bestemmelser vil være «terrorlovgivning» og «vern av Norges selvstendighet og nasjonale interesser», med en gradering lav, middels og høy.

Eksempel fra virkeligheten: Fort Hood-skytingen
En amerikansk major og psykiater, motivert av ideologi, begikk i 2009 voldelig innsidervirksomhet på den amerikanske militærbasen Fort Hood. Ved å skyte mot personell innenfor det beskyttede området som han var gitt legtitim adgang til gjennom sitt arbeid i den amerikanske Hæren, drepte han 13 stykker og skadet enda flere.

Bestemmelsen har følgende ordlyd:

- straffbare handlinger eller forberedelser eller oppfordringer til straffbare handlinger

At personell er villig til å følge de regler som finnes i samfunnet, er en grunnleggende forutsetning for at personer skal få tilgang til statens hemmeligheter (US Departement of Defence, 2014). Dette er blant annet fordi det gir et bilde av en persons lojalitet til å følge de lover og regler som personen er underlagt, noe som også vil være viktig i behandlingen av informasjon som er beskyttet. Den samme utgivelsen beskriver at blant annet følgende momenter bør være av betydning i vurderingen av hvorvidt personell skal få klarering som gir tilganger:

- En alvorlig, eller flere mindre alvorlige, straffbare forhold.

- Mistanker eller anklager om kriminelle handlinger, uavhengig av om denne mistanke er gjennom en formell siktelse eller mistanke fra politi eller rettsvesen.

Det vil også være naturlig at tilstanden til de ulike nodene kan settes fra ingen, lav, middels og høy. Vurderingen vil være avhengig av hvorvidt det finnes mange lovbrudd innenfor samme kategori, og må fange opp dersom det er ett alvorlig lovbrudd i kategorien. Kriminelle trender er skiftende, og modellen må kontinuerlig forbedres gjennom at kunnskapsmodellør og de som bruker modellen følger med i kriminalitetsutviklingen.

Det er videre et spørsmål om hvordan en skal klassifisere ulike straffbare forhold, da det trolig er noen typer forhold som vil være med relevante i vurderingen av noens sikkerhetsmessige skikkethet enn andre. Jeg har sett til straffelovens kapitteloversikt for å skaffe meg en oversikt, og funnet at følgende kategorier bør stå som selvstendig risikoindikator og foreldrenode til «lojalitet til lovverk»:

Vern av den personlige frihet og fred. Dette er handlinger som menneskehandel, ulike former for utførelse av tvang mot personer, trusler, menneskehandel og lignende. Dette er tatt med som egen foreldrenode til straffbare forhold, ettersom dette er en form for kriminalitet som en ofte vil finne innenfor organiserte kriminelle miljøer, noe blant annet Økokrim trekker frem i sin Trendrapport for 2020.
Voldslovbrudd og ordensforstyrrelser. En node som inkluderer ulike voldslovbrudd, fra krenkelse mot andre og til mishandling i nære relasjoner, og til forstyrrelse av den offentlige ro og orden.
Seksuallovbrudd. Avvikende seksualatferd, slik som straffbare forhold innen kapitlet seksuallovbrudd etter straffeloven er, kan påvirke en person sikkerhetsmessige skikkethet på mange måter. Det er et forhold som kan utnyttes gjennom at det kan skape et grunnlag for press. Det vil derfor også utgjøre en foreldrenode for «Grunnlag for press» som drøftet i neste bestemmelse, i tillegg til lojalitet til lovverk.

Eksempel fra virkeligheten: Honningfelle
Sovjetisk etterretning var kjent for å ha noen attraktive kvinner som skulle lure amerikanske og andre vestlige borgere til å bli spioner. En sersjant som tjenestegjorde på ambassaden i Moskva hadde et seksuelt forhold til en sovjetisk kvinne, og da han fikk vite at hun var gravid fikk han ikke forlate landet med mindre han samarbeidet. Han godtok å samarbeide, og fortsatte med det også etter at han kom tilbake til USA.
(US Departement of Defence, 2014)

Profittmotivert kriminalitet. Dette inkluderer kapitlene «økonomisk kriminalitet» og «vinningslovbrudd». Økonomi er et forhold av stor betydning for en persons sikkerhetsmessige skikkethet, noe som drøftes nærmere under. Lovbrudd under kategorien økonomisk kriminalitet er derigjennom en svært viktig node for modellen. Noen økonomiske lovbrudd, slik som økonomisk utroskap hvor man handler mot andres interesser som en er satt til å styre over, er dessuten svært beslektede handlinger til innsidervirksomhet. Det kan også si noe om en persons pålitelighet, og hvorvidt personer er tilbøyelig til å ta noe som ikke tilhører dem. Begge disse tjener som foreldrenode til «Lojalitet til lovverk», «Økonomi» og «Forbindelse til organisert kriminell gruppering».

Trafikale lovbrudd. I tillegg er trafikale forhold en så stor del av den anmeldte kriminaliteten, at det er nødvendig at det er en egen node for dette. SSB (Statistisk sentralbyrå, u.d.) viser at cirka 45 000 av totalt 300 000 anmeldte forhold i Norge i 2020 var trafikale lovbrudd. Dette er foreldrenode til «Lojalitet til lovverk».

Organisert kriminalitet. I straffeloven § 79 beskriver ulike forhold som kan medføre høyere fastsettelse av straff, hvorav bokstav c favner handlinger utøvet som ledd i aktiviteten til en organisert kriminell gruppe og er av den grunn spesielt relevant i vurderingen av innsiderrisiko. Etter denne bestemmelsen betegnes en «Organisert kriminell gruppe» som et samarbeid mellom 3 eller flere personen som har som hovedformål å begå en handling som kan straffes med fengsel i minst 3 år, eller som går ut på en ubetydelig del av aktivitetene består i å begå slike handlinger. Etter sikkerhetsloven er forbindelse til organisasjoner med ulovlig formål et relevant forhold i vurderingen av sikkerhetsmessig skikkethet, og det er derfor en risikoindikator. Denne er foreldrenode til både «Lojalitet til lovverk» og «Forbindelse til organisert kriminell organisasjon».

Narkotikakriminalitet. Narkotikakriminalitet har jeg valgt å sette som en egen node i modellen. Dette har jeg gjort av tre grunner. Den første er at narkotikalovbrudd utgjør en stor del av den totale mengden av lovbrudd, med cirka 39 000 anmeldelser under posten «Rusmiddellovbrudd» i SSBs statistikker for 2020 (Statistisk sentralbyrå, 2021). Den neste er at narkotika er relevant ved to bestemmelser etter sikkerhetsloven § 8-4, fjerde ledd ved at bokstav e omhandler misbruk av alkohol og *andre rusmidler.* Omgang med narkotika kan være en risikoindikator ved at det kan indikere en svekket dømmekraft, mentale utfordringer

og kriminell aktivitet (US Departement of Defence, 2014). Som profittmotivert kriminalitet gjør det seg også gjeldende ved for «Forbindelse til organiserte kriminell gruppering».

Andre forhold straffbare forhold. Dette er en «sekkepost», som er ment å favne alle de andre lovbruddstypene som personer kan pådra seg. Det er foreldrenode for «Lojalitet til lovverk».

Sikkerhetsloven § 8-4, fjerde ledd bokstav c
Bestemmelsen er som følger:

forhold som kan føre til at personen selv, eller personens nærstående, utsettes for trusler mot liv, helse, frihet eller ære, slik at personen kan bli presset til å handle i strid med nasjonale sikkerhetsinteresser

Det første som er viktig å avklare i denne sammenheng, er at modellen må gjenspeile bredden i det som kan medføre pressgrunnlag. Et eksempel på dette er seksuallovbrudd kan medføre et selvstendig press grunnlag mot en person, forhold som en person ønsker å holde skjult for omgivelsene som for eksempel helsemessige ting eller rusbruk med mer. Det kan også være ting som en person ønsker å holde skjult fordi vedkommende frykter administrative konsekvenser som følge av sikkerhetsbrudd på jobb eller andre forhold som kan få direkte konsekvens for arbeidsforholdet.

Eksempel fra virkeligheten: Arne Treholt og pressmidler
Arne Treholt er den kanskje mest omtalte innsider-saken i norsk historie. Treholt var tjenestemann i Utenriksdepartementet, og ble i 1985 dømt for spionasje til fordel for Sovjetunionen og Irak. Flere dokumentarserier er laget om saken, og NRK gav i 2019 ut en hvor følgende skal være sitater fra avhørsrapportene:
«Titov gikk raskt på sak, og sa at gjenytelser ville være nødvendig om ikke siktedes kone, Kari, skulle få tilsendt bilder. Bildene viste siktede i en sterkt kompromitterende situasjon.»

Titov var tjenestemann i den sovjetiske etterretningstjenesten KGB, og skal i den situasjonen ha vist til bilder fra en fest som viste Treholt i en kompromitterende situasjon, i den hensikt å få Treholt til å samarbeide om å overlevere graderte opplysninger som han hadde tilgang til gjennom sitt virke.

Når det gjelder denne bestemmelsen så er det flere ting som på et overordnet nivå vil kunne bidra til å styrke et pressgrunnlag. For det første må det være forhold som personen kan la seg presse for gjennom trusler om liv, helse, frihet eller ære. Det neste momentet er hvorvidt det

finnes trusselaktører som har interesse av tilgang til den informasjonen som vedkommende har tilgang til, for eksempel slik som en stat eller en organisasjon.

Det neste momentet er hvorvidt det faktisk finnes individspesifikke sårbarheter som er rettet direkte relevant mot en trusselaktør. Dette vil bli nærmere drøftet etter bokstav l og n som omhandler henholdsvis forbindelse til ulike typer organisasjoner og tilknytning til andre stater.

Et annet viktig moment, som også dekkes av bestemmelsene om opplysningsplikt til klareringsmyndighet og orienteringsplikt til autoriserende leder, er åpenhet rundt sårbarheter. For det første vil en slik åpenhet kunne indikere at et forhold ikke er av en slik skambelagt karakter, og må tas med i betraktningen i vurderingen av grunnlag for press. Tilbakeholdelse av informasjon til sin autoriserende leder, eller for leder i virksomheter som ikke er underlagt sikkerhetsloven, vil i seg selv kunne medføre et grunnlag for press rettet mot en person.

Det synes også nødvendig med en vurdering rundt en persons generelle åpenhet rundt mulige sårbarheter. For eksempel ved tilfellet hvor Arne Treholt ble utsatt for press, ville en måte å fjerne grunnlaget for press på være å fortelle om hendelsen til sin kone.

Bestemmelsen tar også høyde for at dette kan gjelde personer som etter loven regnes som personens nærstående.

a) *nærstående: personer som er i nær familie eller som har annen nær tilknytning som kan ha betydning for om en person er sikkerhetsmessig skikket*

Loven er på dette punktet svært fleksibel, ved at også andre enn de som inngår i den nære familien kan inngå i vurderingen. Dett er viktig å ta høyde for, og at også familiære bånd og forhold ved nærstående og personer med tilknytning til personen kan utgjøre et pressgrunnlag. Nærstående må derfor utgjøre en egen node i modellen ved for eksempel forbindelser til organisasjoner.

Sikkerhetsloven § 8-4, fjerde ledd bokstav n
Bestemmelsen sier følgende:

«tilknytning til andre stater»

Det er flere grunner til at en tilknytning til fremmed stat kan utgjøre en personellsikkerhetsmessig sårbarhet. Norge utgjør en stadig mer globalisert befolkning. I tillegg spiller teknologi en viktig rolle. På den ene siden har kommunikasjonsteknologi gjort det enklere å kommunisere med personer på tvers av landegrensen. Også på konsekvenssiden har teknologi bidratt til å øke denne risikoen, da tilgang til lagringsmuligheter som gjør det mulig å overføre store mengder informasjon er tilgjengelig for mange (Gelles, 2016).

I veileder for personellsikkerhet kommer det frem tydelig at det må gjøres konkrete vurderinger av både tilknytningen til staten og hvordan statens faktiske sikkerhetsmessige betydning kan påvirke en persons sikkerhetsmessige skikkethet. Med dette legger jeg til grunn at i vurderingen av en persons tilknytning til annen stat i et ledd i å risikovurdere innsiderrisiko, må bestå av nodene «Tilknytning til staten» og «Statens sikkerhetsmessige betydning».

Når det gjelder vurderingen av tilknytning til staten, bemerker NSM i veileder i personellsikkerhet at vurderes om det foreligger konkrete forhold som kan gjøre personen sårbar for press, fristelse eller forledelse, og om det foreligger forhold som kan gjøre at personen kan komme i en lojalitetskonflikt. I vurderingen legges det til grunn at begrepet må tolkes vidt. Jeg har primært sett til faktorene som nevnes i veileder for personellsikkerhet, samt spørsmålene som stilles i Personopplysningsblankett[1] (POB) fra NSM:

Statsborgerskap: Statsborgerskap er en status man kan ha i et land, og medfører en rekke retter og plikter ovenfor dette landet, som for eksempel verneplikt (Store norske leksikon, 2020). I tillegg til å medføre slike plikter, kan det også være en indikator på en tilknytning til landet dersom noen ikke ønsker å frasi seg et slikt statsborgerskap om man har fått et i landet man bor (US Departement of Defence, 2014). Dette er et ja/nei-spørsmål og nodens tilstander er derfor «Ja» eller «Nei».
ID-dokumenter. I POB punkt 11.7 blir det spurt om den som anmoder om klarering har ID-papirer eller pass fra andre stater, og er følgelig et forhold av betydning for den sikkerhetsmessige skikketheten og noe som må adresseres i modellen. At noen velger å beholde slikt kan være av rene praktiske hensyn, men kan likevel være en indikator på en

[1] Personopplysningblankett er en egenerklæring som fylles ut av den som skal anmodes sikkerhetsklarert for en klareringsmyndighet.

forsterket tilknytning og noe som kan bli brukt mot personen ved en innreise til landet. Dette er for enkelhets skyld satt til «Ja» og «Nei».

Myndighetskontakt. Det blir i POB pkt. 11 spurt både om hvorvidt personen selv eller nærstående har utført tjeneste for fremmed stat, og om personen selv har hatt kontakt med ambassader eller myndigheter i av andre stater. Dette er en noe mer diffus node, og det må foreligge en konkret vurdering av omfanget av kontakten, konteksten for kontakten, for eksempel om det er som en søknad om et visum, hva slags tjeneste som er utført for staten mv. Jeg vil derfor sette denne noden til lav, middels eller høy.

Gjenboende relasjoner: Det skrives videre at gjenboende relasjoner i landet må vurdere konkret, og familie, slekt og venner nevnes spesifikt. Det er dog ikke like enkelt å sette tilstander for denne noden, og jeg setter den derfor til lav, middels og høy hvor konkrete vurderinger rundt hvor nær de faktiske relasjonene er, hvor mange det er snakk om, hvorvidt det er snakk om reisevirksomhet til disse.

Økonomiske interesser: Økonomiske interesser i et land kan tenkes å være gjennom investeringer, bankkonti, eiendommer og lignende, noe som også kommer frem i POB ved spørsmål i kapittel 11. Økonomiske interesser indikerer en tilknytning til staten da forvaltning av slikt skjer gjennom statens lov- og forvaltningssystem. Dette er en risikoindikator og en node som krever flere tilstander, da det kan tenkes å være forskjell på om man har noe økonomiske interesser og store økonomiske interesser. Den settes til lav, middels og høy.

Interesseorganisasjoner eller lignende. Personer som har medlemskap eller engasjement i organisasjoner eller konflikter rundt opprinnelseslandet, for eksempel støttegrupper eller som er en aktiv debattant, kan ha større grad av splittet lojalitet (US Departement of Defence, 2014). Slikt engasjement kan være vanskelig å vite om, men jeg legger til grunn at en vurdering av ja eller nei for noden er hensiktsmessige, da det er vanskelig å gradere slikt engasjement.

Det neste momentet som må inn i denne vurderingen, er da statens sikkerhetsmessige betydning. Det er ikke åpenbart hvilke momenter som inngår i vurderingen av en stats sikkerhetsmessige betydning. Man vil uansett i denne vurderingen, kunne bruke informasjon som kommer fra ulike åpne trusselvurderinger, fra for eksempel PST og

Etterretningstjenesten. Der fremkommer for eksempel per tid at Russland, Kina, Iran og Pakistan er landene som blir nevnt som land med etterretningsmessige interesser rettet mot Norge.

Videre er det noen land som en kan tenke seg utgjør en noe sikkerhetsmessige betydning. I ADR (US Departement of Defence, 2014) trekkes blant frem at land som er i konflikt med etter eller flere av nabolandene sine kan utgjøre en etterretningsmessig trussel, da de kan ha interesse i å vite etterretning om naboland eller informasjon om hvordan andre stater posisjonerer seg politisk i slike konflikter. Dette er en kategori land som jeg fra nå av vil kalle land fra ustabile områder.

ADR skriver videre at et moment som må tas i betraktning når det gjelder personells tilknytning til fremmede stater, er hvorvidt staten er et aktuelt område for terrorisme. Det vil også for denne kategorien finnes offentlig tilgjengelig informasjon fra for eksempel Etterretningstjenesten og PSTs årlige trusselvurderinger.

Konkurrerende land og, eller land med konkurrerende virksomheter, på teknologi og forretningsmessige forhold kan også tenkes å utgjøre en forhøyet sikkerhetsmessig betydning. Det trekkes dessuten frem fra PSTs årlige trusselvurdering (2020) at i flere land bistår nasjonal etterretning næringslivet, og at det derfor kan være vanskelig å skille mellom industrispionasje og den vanlige statlige etterretningsvirksomheten. Med dette står jeg igjen med følgende tilstander til noden «Statens sikkerhetsmessige betydning»:

Høy: Land med høy statlig sikkerhetsmessige betydning rettet mot Norge og norske interesser, og er typisk stater som trekkes frem i PSTs og Etterretningstjenestens trusselvurderinger som stater med slike interesser.
Middels: Dette er en sekkepost av land hvor det, som ovenfor drøftet, foreligger noen indikator på en viss sikkerhetsmessige betydning. Dette er som følge av

- landet har utbredt terrorisme og/eller terrorgrupper,
- det ligger i et ustabilt og konfliktfylt område,
- landet er en direkte konkurrent til Norge generelt eller virksomheten spesielt, innen teknologiske og forretningsmessige forhold.

Lav: Dette er typisk land som Norge og virksomheten har et tett samarbeid med, for eksempel gjennom internasjonale avtaler. Eksempelvis vil dette gjelde de fleste landene som Norge har samarbeid med gjennom NATO, EØS osv.

Eksempel fra virkeligheten: Etterretning mot allierte
Land som i utgangspunktet ikke har et stort etterretningstrykk rettet mot hverandre, vil likevel kunne ha interesse av tilgang til andre lands etterretningsrapporter, blant annet om eget land. Filipinene og USA er i utgangspunktet to allierte nasjoner, med en felles forsvarspakt. Likevel ble en amerikansk statsborger med filipinsk opphav, som heter Leandro Aragoncillo i 2007 dømt for spionasje mot USA da han brukte sine tilganger til å skaffe amerikanske etterretningsrapporter om Filipinene og overleverte disse til opposisjonen til filipinske styresmakter (US Departement of Defence, 2014)

Sikkerhetsloven § 8-4, fjerde ledd bokstav l «forbindelse»
Bestemmelsen har følgende ordlyd:

- forbindelse med organisasjoner som har ulovlig formål, og som kan true den demokratiske samfunnsordenen, eller som anser vold eller terrorhandlinger som akseptable virkemidler

NSM skriver i sin veileder til personellsikkerhet at denne bestemmelsens bruk av begrepet «forbindelse» ikke må oppfattes til å være avgrenset til straffbare forbindelser. I dette tolker jeg flere ting. For det første, så inkluderer det at forbindelser til slike organisasjoner gjennom sine nærstående er et relevant tema i risikovurderingen av innsidervirksomhet, til tross den åpenbare urettferdigheten i at folk skal lide under andre personers handlinger. Videre er det ikke slik at kun forbindelser til det en kan regne som ulovlige, kriminelle organisasjoner som er relevant i denne vurderingen.

Videre har jeg dratt følgende begrepet ut av lovens tekst:

- Organisasjoner som har ulovlig formål,
- ...som kan true den demokratiske samfunnsorden,
- ...som anser vold eller terrorhandlinger som akseptable virkemidler.

Når det gjelder det førstnevnte, har jeg valgt å klassifisere dette som organisasjoner som bedriver kriminell virksomhet, altså organiserte kriminelle. Ved drøfting av straffbare forhold, ble organisert kriminalitet drøftet som en egen node under straffbare forhold under premissene om at organisert kriminalitet er definert som tre eller flere personer som har som formål med sin aktivitet å gjøre handlinger som kan medføre 3 års fengsel. Det fremheves også at internasjonale, kriminelle nettverk vil ønske å etablere seg sterkere i Norge. Et annet

tema når det gjelder organiserte kriminelle er MC-klubber, eller såkalte 1%-klubber. Dette er klubber som definerer seg selv som lovløs og på siden av et lands lovverk (Kripos, 2021). Disse er relevante ettersom de er kjent for å drive kriminell aktivitet, samt at de har et sett med regler og lover som gjør at en kan frykte at medlemmers lojalitet til lover innen sikkerhetsdomenet vil være underordnet. En egen node i modellen under forbindelser er «Organiserte kriminelle nettverk».

Videre har jeg sett på organisasjoner som «kan true den demokratiske samfunnsorden». Dette er en vanskelig faktor å vurdere, da det er et diffust skille mellom lovlig politisk virksomhet og det å representere en slik organisasjon. For modellen må det foreligge en konkret vurdering av hver enkel organisasjon der hvor disse kommer opp, men jeg vil belyse kategorien utfra et eksempel, Den nordiske motstandsbevegelsen (DNM).

DNM er en nynazistisk organisasjon, med medlemmer i de nordiske landene, inklusive i Norge. Det har riktig nok vært tilfeller der hvor medlemmer av organisasjonen har vært knyttet til og utført voldelige angrep, men organisasjonen er i utgangspunktet ikke åpen for bruk av vold eller terrorisme utad og blir heller ikke omtalt i offentlige publikasjoner fra sikkerhetsmyndigheter som en voldelig organisasjon. Den kan derfor vanskelig kategoriseres derunder. Det er likevel en organisasjon som har som mål å endre det norske styresettet drastisk, og beskrives blant annet av PST (Politiets sikkerhetstjeneste, 2020) som en organisasjon som ønsker å avskaffe demokratiet. Det er derfor en organisasjon som kan gjøre seg gjeldende i denne sammenhengen.

Jeg vil i denne sammenhengen argumentere for at denne kategorien bør være noe videre enn hvorvidt de ønsker å avskaffe en demokratisk styreform. Jeg vil i denne sammenhengen vise til Gules (2012) som definerer det han kaller normativ ekstremisme. Han beskriver en deskriptiv ekstremisme som avviker sterkt fra godt begrunnede etiske, moralske politiske og juridiske normer. Han legger i denne forbindelse demokratiet og rettstatens styringsprinsipper, samt menneskerettighetene, til grunn for slike normer. Jeg vil argumentere for at dette er en vei å gå med tanke på hvilke forutsetninger en kan legge til grunn for organisasjoner som kan benevnes i denne kategorien. Ulike ideologiske organisasjoner, som kan være av lovlig art og som ikke anerkjenner vold som et akseptabelt virkemiddel, men som likevel har et budskap som strider med prinsippet som et demokrati er bygget på, og forbindelse vil kunne utgjøre en innsiderrisiko ved at personer begynner å interessehevde på vegne av organisasjonen.

Den siste kategorien som nevnes innenfor forbindelser, er organisasjoner som anser terror og vold som akseptable virkemidler. Dette inkluderer åpenbart de store internasjonale terrororganisasjonene som har utvist evne og vilje til å utføre terroraksjoner nasjonalt og globalt. Dette kan med andre ord være snakk om for eksempel Al Qaida, ISIL og Al-shabaab. For det første vil slike organisasjoner kunne ha interesse av ulike typer informasjon, om for eksempel politiske prosesser, teknologi og kunnskap knyttet til våpen og bomber og ikke minst kunnskap om som kan muliggjøre for at personen selv kan utføre terrorangrep.

Det er videre ikke slik at det kun er grupperinger som har terrorisme som et av sine virkemidler som er innenfor denne kategorien, men også voldelige grupperinger. Dette kan være forbindelser til ulike ideologiske eller religiøse grupperinger som har vold eller terror som anerkjente virkemidler i sine aktiviteter, herunder både innen- og utenlands. Jeg vil for enkelthets skyld slå sammen organisasjoner som er voldelig og ekstremistiske til en node som heter «Ekstremistiske eller grupperinger som er voldelige/anerkjenner terror».

Til dette temaet er det viktig å definere organisasjoner relativt bredt. I denne sammenheng kan det vises til PSTs årlige trusselvurderinger i tidsrommet 2017 og frem til 2021, som utelukkende nevner Den nordiske motstandsbevegelsen som en organisasjon innen den norske høyreekstremismen. Det er derfor viktig at deltagelse i det som normalt vil karakteriseres som et «miljø», «gruppe» og kanskje også chatteforum, kanaler og nettsider på internett skal regnes inn under denne kategorien. Dette følger også av at miljøene beskrives som at en stor del av aktiviteten skjer på nett og i uformelle og uorganiserte former.

Dette er noe som også kommer frem av veileder i personellsikkerhet, og at det ikke er avgjørende hvilken form en forbindelse har. Jeg har ikke klart å finne noen litteratur som beskriver hvordan en kan vurdere noens forbindelse til en organisasjon, men har lagt noen av de samme kriteriene som ved vurdering av tilknytning til stater til grunn.

For tilknytning ble statsborgerskap vurdert som en indikasjon på tilknytning, og for forbindelse til organisasjon vil jeg legge til grunn at et «medlemskap» er i nærheten av å ligne på denne faktoren. Medlemskap i en organisasjon, åpent eller skjult, er også en klar måte å vise tilhørighet og derigjennom forbindelse til en organisasjon. Tilstanden settes til lav, middels eller høy.

For tilknytning var reisevirksomhet en faktor, og en indikator innen vurderingen av forbindelse til organisasjon som jeg vil sammenligne med dette er «deltagelse i aktiviteter». Dette er en noe diffus node, og vil inkludere aktiviteter som deltagelse i demonstrasjoner og markeringer, deltagelse i nettbaserte aktiviteter gjennom chattekanaler, lese stoff på organisasjonens hjemmesider eller andre publikasjoner eller «propagandavirksomhet» som å dele ut flyveblader, henge opp plakater og lignende. Dette er ikke en «Ja»/ «Nei»-tilstand, og må graderes i tilstandene lav, middels eller høy utfra hvor aktiv personen har vært i organisasjonen. Deltagelse i aktiviteter som i seg selv er ulovlige, for eksempel vold, narkotikasalg eller ulovlige markeringer, bør som hovedregel medføre at noden settes «Høy».

Videre ble det vurdert økonomiske interesser som del av tilknytningen til en stat. Dette vil også gjøre seg gjeldende i forbindelse med organisasjoner, men i en noe annen form. Økonomiske forbindelser til en organisasjon kan være snakk om innbetalinger til organisasjonen og på den andre siden at personen har fått penger fra organisasjonen. Dette kan mulig stamme fra utbytte fra straffbar handling eller andre ting, men vil uansett være et forhold som kan sette vedkommende i en slag gjeld til organisasjonen. Jeg vil uansett ha en node som beskriver den økonomiske forbindelsen, men der for eksempel alle former for pengeoverføringer fra organisasjon til person innenfor et visst tidsrom vil gi risikoindikatoren tilstanden «Høy».

Slik som ved tilknytninger, vil videre også en forbindelse kunne oppstå gjennom nærstående og andre som kan påvirke noens sikkerhetsmessige skikkethet. Jeg har derfor satt en node og risikoindikator som «Forbindelse gjennom nærstående», hvor en noe lik vurdering som det som er gjort av personen selv bør gjøres. Denne noden kan settes til lav, middels og høy. Inn i denne totalvurderingen må også personens egen relasjon til denne nærstående vurderes. Det vil altså si at en nærstående som personen ikke har noe kontakt med, kan ha en relativt sterk forbindelse til en organisasjon uten at dette nødvendigvis utgjør en stor personellsikkerhetsmessig sårbarhet.

Sikkerhetsloven § 8-4, fjerde ledd bokstav d, h, i og j

Bestemmelsenes ordlyd er som følger:

- forfalskning av eller feilaktig eller unnlatt framstilling av faktiske forhold som personen måtte forstå har betydning for sikkerhetsklareringen

- ikke å orientere den autorisasjonsansvarlige om egne forhold av betydning for sikkerheten
- nektelse eller unnlatelse av å gi personopplysninger om seg selv
- nektelse av å gi taushetsløfte, tilkjennegivelse av ikke å ville være bundet av taushetsløfte eller nektelse eller unnlatelse av å delta i sikkerhetssamtale

Disse forholdene er av så lik karakter at jeg velger å drøfte de i felles kapittel. Dette er atferd som kan indikere en lav grad av lojalitet, integritet og ærlighet hos personen, og er en type atferd som kan utgjøre et mønster hos en person (US Departement of Defence, 2014). I henhold til veileder i personellsikkerhets (2020), berører forfalskning, unnlatelse og feilaktig fremstilling kjernen av det som ligger i disse begrepene, og er av den oppfatning at det skal føres en streng praksis ved slike forhold.

Gelles (2016) skriver at innsidervirksomhet sjelden skjer som følge av en utløsende faktor, men at man ved granskning og etterforskning finner et spor av atferd som har ledet fram til slik virksomhet. Dette er en type atferd som nettopp kan tegne et bilde av en persons atferd. I Adjudicative desk reference står det at det er to måter som man kan vurdere slik atferd på. Man kan se på alvorligheten i hvert enkelt tilfelle av atferden, og vurdere det utfra det. Det andre alternativet er å se på antall hendelser, og bredden som slike hendelser finner sted innenfor. Det argumenteres der for at jo større bredde det er i denne typen atferd, jo større sjanse er det for at det kan påvirke personens evne til å håndtere sensitiv og gradert informasjon. Jeg vil velge en tilnærming hvor jeg vil se på antallet slike hendelser, og gradere faktorenes tilstand utfra denne tilnærmingen.

Bestemmelsen etter sikkerhetsloven er ment å favne utelukkende informasjon i forbindelse med en klareringsprosess og som del av den daglige sikkerhetsmessige ledelsen gjennom autoriserende leder. Jeg har derfor valgt å sette en egen node som jeg kaller «Tilbakeholdelse, forfalskning eller feilaktig av sikkerhetsrelevant informasjon», noe som er ment å dekke informasjon om de individspesifikke sårbarhetene og øvrige forhold i forbindelse med ansettelse. Dette kan inkludere dokumentasjon på kurs, føring av arbeidstimer mv.

En videre konsekvens av tilbakeholdelse av informasjon, er at det kan skape et pressgrunnlag. Dersom det er informasjon som man ellers skulle ha informert autorisasjonsansvarlig eller klareringsmyndighet om, eventuelt andre forvaltningsorgan eller lignende, vil dette kunne

være et påskudd for en pressaktør om å innlede en tilnærming mot personen. I denne sammenhengen må det også nevnes at det er enkelte forhold som kan være mer potente som pressmidler enn andre, slik som for eksempel forhold som kan medføre skam.

Dette er risikoindikatorer som vil gjøre seg gjeldende for flere punkter lenger inn i nettverket. For det første vil det være en indikator på en persons sikkerhetsmessige forståelse og integritet, og kan medføre at en person gjør handlinger som fører til ubevisst innsidervirksomhet. Jeg vil etablere nodene «Tilbakeholdelse mv. av sikkerhetsinformasjon», og «Tilbakeholdelse mv. av annen informasjon», som for eksempel i tilknytning til en ansettelsesprosess og dokumentasjon i den forbindelse. Grunnen til at jeg vil ha to noder for disseer at de vil kunne vektes noe ulikt ved kvanitative analyser.

Sikkerhetsloven § 8-4, fjerde ledd, bokstav e «misbruk av alkohol eller andre rusmidler»
Denne bestemmelsen sier som følger:

- misbruk av alkohol eller andre rusmidler

Eksempel fra virkeligheten: Rekruttering av narkotikabrukere
Sgt. Rodderick Ramsey er en straffdømt spion fra USA, og misbruk av narkotika var den viktigste kvalifikasjonen for å finne personer som han kunne samarbeide med. Han begrunnet ikke dette primært med at de var «misbrukere», men at de ved å innta illegale rusmidler allerede hadde vist en villig til å bryte Hærens reglement og at de var villig til å ikke rapportere ulovlig aktivitet. Bruk av illegale rusmidler kan altså indikere en villighet til å handle utenfor reglementet, i tillegg til at det må sies å kunne være en faktor som kan indikere en svekket dømmekraft og årvåkenhet.

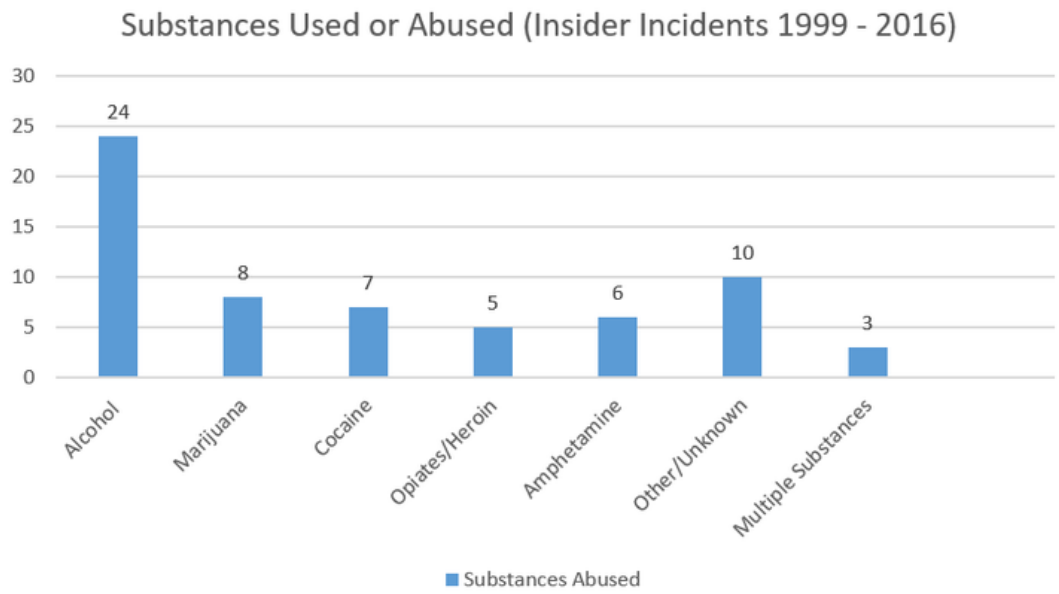
Etter denne bestemmelsen er det aktuelt å vurdere både det som etter norsk lov er å regne som illegale rusmidler, samt legale rusmidler og legemidler som utskrives av lege (Nasjonal sikkerhetsmyndighet, 2019). Jeg har videre sett hen til legemiddelloven § 24, hvor bruk og besittelse av narkotika er straffbart etter bestemmelsens bokstav a og dopingmidler etter bestemmelsens bokstav b. Det synes derfor, utfra et juridisk perspektiv, logisk å inkludere dopingmidler under denne bestemmelsen i modellen. Da står vi så langt igjen med følgende noder for modellen

- Misbruk av illegale rusmidler, legemidler og dopingmidler
- Misbruk av legale rusmidler (alkohol)

Misbruk av illegale rusmidler kan indikere flere ulike sårbarheter i vurderingen av en persons risiko for å bedrive innsidervirksomhet. For det første kan det indikere en vilje til å handle i

strid med de lover og regler man er underlagt, en egenskap som er viktig innen sikkerhetsdomenet, og er foreldrenode for «Lojalitet til lovverk». Misbruk kan, spesielt mens man er påvirket, svekke den nødvendige dømmekraften for å forvalte skjermet og gradert informasjon og er derfor foreldrenode for «Sikkerhetsmessige forståelse». Bruk kan dessuten gjøre personer sårbare for press, for eksempel dersom det kan koste dem jobben om det avdekkes, og dessuten i form av at vanebasert atferd og avvikende atferd kan utnyttes av utenlandske myndigheter dersom personen befinner seg i utlandet. Det kan i flere tilfeller også være en indikator på et større helseproblem, et tema som blir mer drøftet i forbindelse med bokstav f. (US Departement of Defence, 2014).

Bruk av rusmidler kan altså føre til bevisst innsidervirksomhet, for eksempel gjennom tyveri av intellektuell eiendom eller andre måter å finansiere misbruk. Det kan også medføre en svekket dømmekraft med en tilhørende risiko for ubevisst innsidervirksomhet. I en studie gjort ved CERT Insider Threat Center, hvor totalt 1048 innsidersaker ble vurdert, ble det konkludert med at ved cirka 5 % av disse var rusmidler en sentral del av årsaksbildet. Under følger en tabell som viser fordelingen av forekomst av ulike rusmidler i slike innsidersaker. (Cassidy & Cert Insider Threat Center, 2018)



Figur 9: Tabellen viser at alkohol er det enkelte rusmidlet som utgjør størst andel av rusrelaterte innsider saker. Det foreligger åpenbare statistiske utfordringer for å fastslå farligheten av alkohol i seg selv målt oppimot andre stoffer som følge av utbredelsen av alkohol antas å være større enn noe annet stoff. Det er likevel gode grunner til å konkludere med at lovlig ikke nødvendigvis betyr ufarlig i denne sammenhengen (Cassidy & Cert Insider Threat Center, 2018).

Den første risikoindikatoren som jeg vil sette for modellen er «Misbruk av illegale rusmidler». Dette er en node som dekker all bruk av illegal rusmidler, inklusive illegale medikamenter og dopingmidler. Dette er en node som kan vurderes til lav, middels og høy. Oppgaven min handler ikke primært om å vekte faktorer, men faktorer som frekvensen, type stoff, tid, misbruk/avhengighet, rusrelaterte hendelser og motivasjon må vurderes (US Departement of Defence, 2014).

Den neste noden er «Bruk og misbruk av alkohol». Noe bruk av alkohol er vanlig, men for mye alkohol kan ha flere negative effekter med tanke på vurdering av innsiderrisiko. For eksempel kan det være utbredt bruk som kan medføre kognitiv svekkelse, deltagelse i høyrisiko-aktiviteter og ubevisst innsidervirksomheten som følge av skjødesløs atferd og håndtering av sikkerhetsbestemmelser.

Noden «Misbruk av alkohol» er en node som settes til lav, høy og middels. Følgende faktorer bør vurderes for å gradere noden:

- Påvirket personens evne til utførte sine plikter innen skole, jobb, hjemme eller lignende, og fortsetter til tross for det.
- Tegn til misbruk, slik som problemer med å kontrollere mengde alkohol når en først har startet å drikke, inntak av alkohol i situasjoner som ikke er «normalt»,
- Drikker store mengder alene.
- Uheldige hendelser knyttet til alkohol, for eksempel straffbare handlinger,
- Drikker for å håndtere egne følelser eller livshendelser kan indikere en dypere forankring i mentale problemer.
- Eventuelt ved et tidligere misbruk eller ved behandlingshistorikk – vurdere avstanden i tid, om vedkommende anerkjenner sitt tidligere alkoholproblem og status på alkoholinntak per tid, og om vedkommende har fullført sitt behandlingsprogram.

Rusmidler kan ha den effekten at det påvirker våre kognitive funksjoner utover når vi faktisk er påvirket av dem, men den største effekten vil i så måte være mens man er påvirket av dem. Kunnskap, i tillegg til mulige ting som adgangskort og informasjon i skriftlig form, er ting vi kan ha med oss også når vi er påvirket. At en person har begått handlinger eller kommet oppi situasjoner av alvorlig karakter, eller gjentatte mindre alvorlige, kan gi grunn til å frykte at personen også kan kompromittere informasjon mens vedkommende er under påvirkning.

Begge disse to nodene vil samles under en faktorer som heter «Rus», som skal måle tilstedeværelsen av rusproblemer hos personen.

Eksempel fra virkeligheten: Alkohol og innsidere
Amerikansk forskning har vist at forekomsten av alkoholproblemer hos personer dømt for spionasje er større enn i befolkningen ellers. Den spiondømte Aldrich Ames var kjent for å drikke for mye, og skal flere ganger i ruspåvirket tilstand ha gjort handlinger som kunne være til fare for sikkerheten. Blant annet skal han ha lagt igjen en jakke som inneholdt adgangskort til CIA-lokaler og informasjon om et møte. (US Departement of Defence, 2014)

Sikkerhetsloven § 8-4, fjerde ledd, bokstav f
Bestemmelsens ordlyd er som følger:

- enhver sykdom som på medisinsk grunnlag kan gi forbigående eller varig svekkelse av påliteligheten, lojaliteten eller dømmekraften

Til denne bestemmelsen har NSM i veileder for personellsikkerhet (2019) bemerket at denne bestemmelsen ikke er ment å dekke kun sykdommen i seg selv, men også om den medfører en nødvendig medisinering som kan medføre svekkelse av sikkerhetsmessige skikkethet.

Mental helse er relevant ettersom det påvirker hvordan en person opplever verden, gjør valg og håndterer stress. Det er likevel slik at det faktum at en person har eller har hatt en mental, emosjonell eller psykisk tilstand eller sykdom i seg selv ikke gir grunn til å nekte vedkommende tilgang til sensitiv og gradert informasjon. Det er til syvende og sist et spørsmål om følger, at vedkommende kan gjøre dårlige valg og faktisk opptreden. Dette kan blant annet handle om hvordan en person håndterer negative livshendelser, både i privat og i arbeidssammenheng. Personer som har en personlighet som er dårlig tilpasset sosialt eller har en mental sykdom vil i slike situasjoner kunne reagere med selvdestruktiv atferd eller til og med negativ atferd rettet mot arbeidsgiver (US Departement of Defence, 2014).

Jeg vil innledningsvis dele denne bestemmelsen i to noder – som er «Sykdom som medfører forbigående eller varig svekkelse» og «Medisiner som medfører forbigående eller varig svekkelse»». Begge må sees i sammenheng med atferd. Det nevnes flere diagnoser som er sentrale i vurderingen av hvorvidt noen bør behandle slik informasjon, som blant annet inneholder angstlidelser; stemningslidelser som depresjon eller bipolar lidelse; kognitive lidelser som demens; personlighetsforstyrrelser som antisosial atferd, ondsinnet narsissisme,

paranoid; og psykotiske tilstander som schizofreni. Diagnose settes som en node, med ja eller nei som tilstander.

Videre har for eksempel den amerikanske Executive Order 12968, datert August 4, 1995, gitt klart uttrykk for at en mental lidelse ikke alene kan stå som grunnlag for at noen nektes adgang til gradert informasjon. Dette må sees i sammenheng med hvorvidt en person mottar, eller har mottatt, behandling for sin lidelse. Generelt kan man si at en person som har mottatt eller mottatt behandling må kunne gis en større grad av tillit, da dette indikerer en innsikt i egne sårbarheter. «Behandling» er derfor en egen foreldrenode til «Sykdom som medfører forbigående eller varig svekkelse»

Eksempel fra virkeligheten: Sjukdom eller personlighet?
En person har enkelte trekk ved seg som kan indikere et sykdomsbilde, men likevel ikke møte de standarder som kreves for å sette en diagnose. Dette var tilfelle med Jonathan Pollard, den amerikanske etterretningsanalytikeren som spionerte til fordel for Israel. Han ble fratatt sikkerhetsklareringen for å ha utvist narsissistisk og grandios oppførsel, blant annet ved at han ble tatt i løgn, men fikk en helseattest på at han ikke hadde noen diagnose. Han fikk derfor tilbake tilgangen til gradert informasjon og ble innsider, til tross for at det var tegn gjennom hans atferd på at han ikke var skikket til å behandle slik informasjon. (US Departement of Defence, 2014)

Den neste noden som jeg vil drøfte, er «Medisiner som medfører svekkelse». Dette kan være svært mange ulike typer medisiner, mot svært mange ulike lidelser. Noen tilstander som kan medføre behov for medisinering med sterke medisiner, kan være uten relevans for sikkerhetsmessig skikkethet. Dette kan være medisiner mot smerte og lignende, som både i kortere og lengre tidsrom kan være nødvendig for at en person skal opprettholde funksjonsnivå. Til tross for at tilstanden i seg selv ikke vil medføre særlig påvirkning på personens sikkerhetsmessige skikkethet, kan altså medisiner brukt i forbindelse med den gjøre det.

Sikkerhetsloven § 8-4, fjerde ledd bokstav g
Bestemmelsen sier:

- kompromittering av skjermingsverdig informasjon eller brudd på sikkerhetsbestemmelser

Jeg vil innledningsvis dele denne bestemmelsen inn i to, som er «Kompromittering av skjermingsverdig informasjon» og «Brudd på sikkerhetsbestemmelser». Førstnevnte betyr i henhold til virkesomhetssikkerhetsforskriften at informasjonen blir gjort kjent for uautoriserte

personer. Brudd på sikkerhetsbestemmelser er brudd på de bestemmelsene som virksomheten er underlagt i kraft av sine sikkerhetsrutiner- og -regler. Dette kan være et stort sett utvalg av ulike bestemmelser som kan være sikkerhetsbrudd, fra å glemme å lukke skap og dører til å ta med seg personell inn i et område de ikke skal være.

Begge disse nodene kan settes til lav, middels eller høy. Det må ligge en konkret vurdering av hvorvidt det foreligger enten alvorlige brudd på de ovenfor nevnte forholdene, eller mange mindre alvorlige. De tjener begge som foreldrenode for «Sikkerhetsmessige forståelse» og «Lojalitet til lovverk».

Sikkerhetsloven § 8-4, fjerde ledd bokstav k «økonomiske forhold»
Denne bestemmelsen sier som følger:

- økonomiske forhold som kan friste ham eller henne til å handle i strid med nasjonale sikkerhetsinteresser

NSM bemerker i veileder for personellsikkerhet at økonomiske forhold kan være relevante på mange måter i vurderingen av en person. De peker først på de tilfellene hvor en person kan la seg friste til økonomisk vinning, for eksempel som følge av gjeld eller et forbruk over det økonomien tilsier. Videre påpekes det at vedkommendes evne og vilje til å ivareta egne forpliktelser være av stor betydning, da også kan være overførbart til hvorvidt personen vil være i stand til å utføre sine forpliktelse i behandling av sensitiv og gradert informasjon.
Med utgangspunkt i MICE-modellen har jeg etablert «Økonomi» som en egen faktor som kan lede til innsidervirksomhet. Denne vil ha fire foreldrenoder, som er «Gjeld», «Mistenkelige transaksjoner», «Misligholdt gjeld» og «Overforbruk».

Overforbruk, som kan handle om «Affluence», eller det å ha en stor økonomisk rikdom, beskrives som et viktig moment. Overforbruk beskrives som en likeså viktig indikator på mistenkelig atferd, da det et slikt overforbruk på en eller annen måtes må finansieres. Noen innsider-saker har avdekket at det har skjedd gjennom innsidervirksomhet, mens det også kan komme fra annen aktivitet av relevans for personellsikkerhetsmessige sårbarheter. Det kan være for eksempel kriminell aktivitet, som kopler vedkommende til et kriminalt miljø og derigjennom et grunnlag for press. Et viktig moment som trekkes frem for å avdekke overforbruk er mistenkelige transaksjoner som ikke kan forklares. Dette er også et moment

som må sees i sammenheng med pengeoverføringer til fremmede stater. Også en stor gjeld sett i forhold til inntekt er beskrevet som en mulig indikator på både overforbruk og en vanskelig økonomisk situasjon (US Departement of Defence, 2014).

Typiske tegn på overforbruk kan være:

- Kjøp av materielle goder utover det som er normalt for folk med tilsvarende inntektsnivå, slik som dyrere bolig, luksusvarer som kunst, klokker, smykker osv., dyre ferier med mer.
- Personen begynner å oppføre seg som storforbruker, for eksempel gjennom små tegn
- Betaling av store beløp med kontanter.
- Personen forklarer sin tilgang på penger med gevinster på ulike pengespill, arv eller store utbytter fra aksjer e.l.

Eksempel fra virkeligheten: Innsideraktivitet og overforbruk
Robert Hansen var sovjetisk/russisk spion i FBI, og brukte ulovlig inntekt fra dette til å betale for privat utdanning for sine seks barn og til å kjøpe diamanter. Etter at han ble arrestert, sa han under etterforskningen at dersom FBI hadde gjort undersøkelser rundt hans økonomi, så ville de kunne fattet mistanke om aktiviteten hans (US Departement of Defence, 2014)

Når det gjelder misligholdt gjeld, så vil jeg inkludere alle typer informasjon om misligholdt gjeld inn i modellen. I POB blir det spurt om personen har hatt krav som har ført til særskilte avtaler med kreditor, inkasso eller tvangsinndrivelse siste ti årene. I vurderingen av misligholdt gjeld er det viktig å vurdere både størrelsen på den misligholdte gjelden, men også om det finnes et mønster for misligholdt gjeld, for eksempel gjennom mange små misligholdte krav. Tidvis likevel gjeld som også ikke er mislighold kunne være så stort, at det ikke vil være forsvarlig å gi noen tilganger i det hele tatt. Dette gir derfor behovet for noden «Gjeld».

Slike forhold som ovenfor nevnt, trenger ikke å være diskvalifiserende for at vedkommende gis adgang til informasjon. Det kan skape behov for enten å bygge tiltak ovenfor personen for å demme opp for sårbarheten på den ene siden, men kanskje like viktig vil det være at man starter en innhentingsprosess for å finne ut av personens økonomiske situasjon.

Videre har jeg lagt til grunn at mistenkelige transaksjoner kan være en risikoindikator på økonomiske avvik, og jeg viser i denne sammenhengen til spørsmål i POB pkt. 11 om pengeoverføringer til utlandet samt det ovenfor nevnte i forhold til at mistenkelige

transaksjoner kan for eksempel indikere et overforbruk. Det settes derfor som en foreldrenode til faktoren «Økonomi».

Sikkerhetsloven § 8-4, fjerde ledd, bokstav o
I denne bestemmelsen står det som følger:

- annet som kan gi grunn til å frykte at en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser.

Beskyttelse av gradert informasjon krever en atferd som i stor grad er i samsvar med et bredt sett av regler og reguleringer. Det er dog vanskelig å utarbeide et lovverk som kan favne all slik atferd, og det er derfor anvendelig å ha en bestemmelse som er så fri for tolkning som denne bestemmelsen. Hvordan en person reagerer på påkjenninger i livet, kommer i stor grad an på deres ærlighet og integritet. En persons atferd vil kunne bidra til å stille spørsmålstegn ved en hvorvidt en person har de personlige ferdighetene som ovenfor nevnt. Dette er et eksempel på hvordan en i personellsikkerhet må jobbe i et «helhetlig perspektiv», og at for eksempel en stor grad av gjeld må vurderes i lys av øvrige opplysninger og eventuelle risikoindikatorer som finnes om vedkommende. (US Departement of Defence, 2014)

Gelles (Gelles, 2016) peker på at virtuell atferd som mistenkelige innloggingstidspunkt, bruk av administrator-rettigheter til arbeidsoppgaver som ikke krever det, samt ikke-virtuell atferd som fallende prestasjoner og negative tilbakemeldinger alle kan være forløpere til innsideraktivitet. Dette er to typer atferd som man i daglig sikkerhetsmessig ledelse er avhengig av å monitorere. Med et mer fleksibelt arbeidsliv, blant annet ved bruk av hjemmekontor-løsninger, kan dog parameteret ikke-virtuell atferd bli vanskelig å oppdage. I en hverdag der man møter folk på daglig basis, så vil mange av de ovenfor nevnte atferdstypene, slik som rusmisbruk og mental helse, være langt mer synlig enn i en verden av hjemmekontor. Dette vil også gjelde andre typer avvikende atferd.

Når det gjelder virtuell atferd, vil jeg bruke en egen node som kalles «Mistenkelig virtuell atferd», som graderes etter lav, middels og høy. Denne er ment å være en node som skal ta høyde for at det for eksempel blir oppdaget slike avvik i personens atferd i virksomhetens datasystem, og bør ta høyde for hvorvidt det finnes et høyt antall mindre alvorlige

enkelttilfeller eller enkeltstående alvorlige tilfeller. Dette er en foreldrenode for «Sikkerhetsmessige forståelse».

Når det gjelder ikke-virtuell atferd, ser jeg det nødvendig å dele dette noe inn. Seksuell atferd er et tema som spesifikt nevnes i Adjudikative desk reference som et forhold som kan være av betydning for vurderingen av noens sikkerhetsmessige skikkethet dersom atferden er straffbar, indikerer en emosjonell er personlig forstyrrelse, når den gir grunn til å stille spørsmålstegn ved noens dømmekraft og dersom det kan gjøre personen sårbar for press, forledelse eller manipulasjon. Forskning på temaet har dog vist at sammenhengen mellom seksuell atferd og innsidervirksomhet er langt mer kompleks enn man kan intuitivt anta, og at en persons personlige egenskaper som selvkontroll, sosial modenhet og dømmekraft er langt viktigere enn den type seksuell aktivitet som personen tar del i.

Eksempel fra virkeligheten: Seksuell atferd
I en artikkel fra New York Times fra July 13, 1985 fremkommer det at Sharon Scranage, som jobbet som sekretær i CIA på ambassaden i Accra, Ghana, ble rekruttert som spion for ghanesisk etterretning som en følge av sitt forhold til en ghaneser som jobbet for staten. Informasjonen hun overleverte skal ha bidratt til at CIA-informanter i Ghana ble drept (US Departement of Defence, 2014)

Jeg vil derfor opprette en node som heter «Seksuell atferd». En annen foreldrenode er «Seksuelle lovbrudd», da straffbar, seksuell atferd alltid vil være aktuell for vurderingen av innsiderrisiko. Et annet tema som nevnes spesifikt i ADR, er såkalt «sex-turisme». Dette er reiser med det formål om at man kan ha en «fast partner» gjennom et opphold på et sted. Dette er en type atferd som kan tenkes å være mulig å utnytte for utenlandsk etterretning, blant annet fordi man setter seg selv i en kompromitterende situasjon, det kan medføre en viss skam ved at informasjon om slike reiser kommer ut og det er i tillegg atferd som skjer på annet lands jord. I forhold til sistnevnte kan dette være land hvor utenlandske etterretningstjenester eller andre trusselaktører vil kunne ha større handlingsrom. Noen av disse reisene kan også tenkes å gå til høyrisikoland, slik som Russland. «Sex-turisme» er derfor en foreldrenode for noden «Seksuell atferd». Noden «seksuell atferd» påvirker videre faktoren «Press» og «sikkerhetsmessige forståelse».

Jeg vil videre ta med en siste indikator som jeg kaller «Ikke-virtuell atferd», som favner bredt. Dette er en node som skal fange forhold som fall i profesjonelle prestasjoner, trusler eller

annen destruktiv atferd rettet mot kollegaer. Det er også en node som kan fange opp atferd som i ekstreme tilfeller kan være forbundet med en medisinsk diagnose for mental sykdom, men som uavhengig av om det foreligger diagnose kan være gode grunner til å nekte noen tilganger med bakgrunn i. Slik atferd kan handle om antisosial atferd, narsissisme og grandiost selvbilde, se på seg selv som overordnet regler og ordninger som andre må føye seg etter, mangel på sympati, paranoia med mer.

Trusselaktør

I henhold til sikringsrisikovurderinger, så er tilstedeværelsen av en trusselaktør et moment i vurderingen som gjøres for å fastsette risikonivået. En trusselaktør kan ønske å angripe gjennom voldelige angrep, slik som et terrorangrep, eller det kan være for å skaffe seg informasjon, for eksempel gjennom et angrep mot et informasjonssystem. Dette er relevant i oppgaven fordi det kan være nettopp informasjon om sårbarheter, sikkerhetsrutiner eller andre forhold som kan muliggjøre et slikt angrep på organisasjonen.

Eksperten sa i intervju 1 at de vanlig inndeling av trusselaktører er statlige aktører, terrorisme, sabotasje og kriminelle. Dette samsvarer med arbeidet som Forsvarsbygg har lagt ned i sin sikringshåndbok. Han var videre enig i at kommersielle aktører også bør være node i modellen, da ulike bedrifter og lignende kan ha nytte av slik informasjon for å nå sine mål. Jeg har vurdert at jeg bruker nodene «Statlige aktører», «Terror», «Organiserte kriminelle» og «Kommersielle aktører» som de trusselaktørene som brukes i oppgaven. Når det gjelder utelatelsen av aktører innen sabotasje, som også vil ha interesser i å samle informasjon om infrastruktur, men i denne sammenhengen så vil dette per definisjon også være aktører som kan kategoriseres innenfor den allerede nevnte kategoriene.

Et relevant spørsmål videre blir da hvordan man kan bygge ut denne vurderingen av tilstedeværelsen av en trusselaktør. FFI-rapport om Tilnærming til Risiko ved vurdering av tilsiktede handlinger (Busmundrud, Maal, Kiran, & Endregard, 2015) skriver at en klassisk tilnærming til bygger på en verdivurdering, det vil si hvilke verdier det som virksomheten har og som en ønsker å beskytte, som for min oppgave er avgrenset til å gjelde informasjon. Det skrives at vurderingen tar utgangspunkt i om det finnes noen som har intensjon eller vilje til å handle mot verdiene, det vil si for min modell skaffe den aktuelle informasjonen som personen besitter. Videre vurderes det om det finnes noen som kan gjøre det, som har

kapasitet til å gjøre det, trusselaktørens modus operandi og om den aktuelle virksomheten og dens verdier er et aktuelt mål.

Dette er dog vanskelige momenter å operasjonalisere. Hovedpoenget er å etablere en sammenheng mellom hva personen har tilgang til, altså verdien, og hvilken type trusselaktører som kan ha interesse for nettopp denne informasjonen. Dette er en node som beskrives under faktoren «kapasitet», og heter «Type informasjon». Det skal sies at det vil kreve et svært dynamisk system, med løpende vurderinger og etterretninger, for at slike sammenhenger skal være operasjonalisert på en god måte.

Det kan argumenteres for at en sannsynlighetsvurdering av trusselaktør ikke er i tråd med NS5830-serien og trefaktormodellen, da noe av argumentet for denne tilnærmingen kontra en del andre metoder for risikovurderinger er at sannsynlighet ikke tas med. Dette er dog en sannhet med modifikasjoner, da det ligger en indirekte sannsynlighetsberegning i vurderingen av hvilke trusselaktører som en tar med seg inn i risikovurderingen. Argumentet, blant annet i FFI (Busmundrud, Maal, Kiran, & Endregard, 2015) er at man ikke tar med trusler som synes helt usannsynlige utfra blant annet de ovenfor nevnte parameterne.

I denne sammenhengen legges en bayesiansk tilnærming til sannsynlighetsbegrepet til grunn, ved at man legger til grunn elementer som logikk, historikk, etterretning og tilgjengelig informasjon i vurderingene. Dette skiller seg fra en ren matematisk tilnærming, som man i større grad kan legge til grunn ved for eksempel naturhendelser som det foreligger større empirisk grunnlag for (Busmundrud, Maal, Kiran, & Endregard, 2015).

Jeg står derfor igjen med at vurderingen av type informasjon som personen besitter, for eksempel om dette er knyttet til forskning, vil være relevant å vurdere oppimot hvilke trusselaktører som kan ha intensjon om å skaffe seg denne informasjonen. Dette vil igjen kunne påvirke faktoren «Press», «Økonomi», «Sikkerhetsmessige forståelse» og «Ideologi» da disse indirekte aktualiserer at faktorene skal aktualisere seg som grunn til innsidervirksomhet. Jeg vil i denne sammenhengen likevel vise til ekspertens vurdering av dette forholdet og operasjonalisering av en slik node, hvor han mente at ingen av de ulike kategoriene kunne være gjensidig utelukkende. Han mente dog at i et sannsynlighetsperspektiv så vil det kunne være av relevans for vurderingen.

Et eksempel på en situasjon hvor en slik type input vil kunne ha betydning, kan være dersom en har en ansatt med en forbindelse til en ekstremistisk organisasjon med voldspotensial, for eksempel gjennom en nærstående. Vedkommende er per tid gitt tilgang til informasjon som omhandler forskning på teknologi, men i forbindelse med en ny jobb skal vedkommende jobbe med sikring av kritisk infrastruktur og beredskap. Dette vil være et tilfelle hvor modellen kan flagge, ved kombinasjonen «tilgang til informasjon om kritisk infrastruktur» og forbindelse til en slik gruppering, da en vet gjennom trusseletterretning at dette er en type verdi som slike organisasjoner kan være interessert i å få tak i. Dette kan derfor medføre en endring i innsiderrisikoen knyttet til personen, og tiltak kan bli gjort utfra dette.

Mulighet

I denne iterasjonen har jeg valgt å fokusere mest på sikkerhetsstyringen som parameter, og gjort som eksperten har anbefalt og sett mot sikkerhetslovens bestemmelser for sikkerhetsstyring. I tillegg til dette har jeg sett til veileder i sikkerhetsstyring fra NSM, samt ISO-31000, som omhandler en standardisering av risikostyringen, et tema som henger klart sammen med det som sikkerhetsloven refererer til som sikkerhetsstyring. Jeg har med utgangspunkt i kravene som sikkerhetsloven oppstiller lagt følgende foreldrenoder til grunn for vurdering av sikkerhetsstyring.

Risikovurderinger. Etter sikkerhetsloven slås det fast at sikkerhetsstyring skal gjøres med bakgrunn i risikovurderinger. Enten man har informasjon som er gradert etter sikkerhetsloven, eller som er beskyttet av andre lovverk eller behov, så er det naturlig at sikkerhetsstyring skjer på denne måten. Jeg viser i denne sammenheng til Aven (Aven, Risikostyring, 2015) og ISO-31000 som skriver at risikovurdering er en sentral del av risikostyringsprosessen, og skal ligge til grunn for de tiltak som gir grunnlag for håndteringen av risiko. Dette er det man kaller en risikobasert tilnærming.

En node vil derfor være «Risikovurdering», som sier noe om hvorvidt organisasjonen har en risikovurdering og om denne er oppdatert, godheten av denne og etterlevelsen. Risikovurdering skal etter sikkerhetsloven gjøres årlig, og jeg finner det naturlig å sette en slik tidshorisont på vurderingen for at noden skal være grønn og skal oppdateres årlig. Videre må den inneholde en vurdering av virksomhetens verdier, hvilken type virksomhet de kan utsettes for og hvilke trusselaktører som finnes, usikkerhet knyttet til de premissene man legger til grunn i vurderingen, konsekvensen av at sikkerhetstruende virksomhet rettes mot

dem og hvilke sårbarheter som er knyttet til verdiene. Dette er momenter som legges til grunn både etter sikkerhetsloven § 4-2 og ISO-31000. Noden settes til lav, middels og høy.

Eksterne aktører. Et moment som det legges opp til at skal vurderes i henhold til Veileder i sikkerhetsstyring er ulike aktører som er involvert i virksomheten, herunder om dette er eksterne aktører. Jeg vil i denne sammenhengen legge til at hvorvidt eksterne gjør store deler av arbeidet må tas med. Dette begrunner jeg både med veilederen, samt eksperten som gav råd om at nettopp hvorvidt eksterne aktører er involvert kan være en utfordring for å drive med god sikkerhetsstyring. Nodens tilstand kan være ja og nei.

Sikkerhetsdokumentasjon. Sikkerhetsdokumentasjon kan videre være et moment i vurderingen av sikkerhetsstyringen i en avdeling. I henhold til sikkerhetsloven § 4 skal en virksomhet underlagt sikkerhetsloven ha et styringsdokument for sikkerhet, som skal inneholde hvilke deler av virksomheten som er underlagt sikkerhetsloven, roller og ansvar i det forebyggende sikkerhetsarbeidet og prinsipper for sikkerhetsarbeidet. Sikkerhetsdokumentasjonen bør i henhold til veileder i sikkerhetsstyring bestå av styrende dokumenter som beskriver overordnede føringer for sikkerhetsarbeidet, utførende dokumenter som beskriver aktiviteter med betydning for sikkerhet og kontrollerende dokumenter som beskriver resultater fra aktiviteter med betydning for slik som registreringer og rapporter.
Sikkerhetsdokumentasjonen graderes høy, middels og lav.

Kontroll av styringssystemet. Kontinuerlig forbedring er et prinsipp som trekkes frem i ISO-31000, og dessuten er en del av det å være en lærende organisasjon som beskrives blant annet i Reason (1997). Han beskriver videre at dette er en enklere del av sikkerhetskultur å bygge, og at det blant annet består av at man observerer og reflekterer over kulturen man har, her under analyserer og vurderer den. I denne sammenhengen er det viktig at det foreligger jevnlige vurderinger av sikkerhetsstyringen. Momenter som kan legges til grunn i vurderingen av kontrollsystemet er hvorvidt dette gjøres av noen andre enn de som lager systemet, om det gjøres periodisk og om kontrollen omfatter alle delene av sikkerhetsstyringen.

Øvelser. Sikkerhetsloven § 4-3, 3.ledd pålegger videre virksomhetene å gjennomføre øvelser for å vurdere effekten av tiltak. Dette henger også sammen med prinsippet om kontinuerlig forbedring, som blant annet er et viktig prinsipp for risikostyring etter ISO310000.

Individspesifikke forhold. Etter hvert som jeg jobbet med emnet, ble det klarere for meg at det vanskelig kan være slik at alle i samme virksomhet har de samme mulighetene til å utøve innsidervirksomhet uten å bli oppdaget. Jeg vurderte at det måtte finnes noen forhold som kunne gjøre at enkelte individer i større grad enn andre vil kunne utøve innsidervirksomhet enn andre, og at det måtte være forhold utover det å være høyrisikopersonell som allerede er drøftet i modellen. Spesielt har dette behovet gjort seg synlig i forbindelse med at hjemmekontor for veldig mange ble den nye normen i forbindelse med pandemi-restriksjoner som ble innført våren 2020. Dette beskrives som kontekstuelle faktorer av Gelles (Gelles, 2016). Jeg har ikke funnet spesifikke forhold som kan legge til rette for innsidervirksomhet på individnivå, men har funnet at forholdene «Hjemmekontor», «Reisevirksomhet» og «Grad av lederoppfølging/grad av individuelt arbeid» kan være med på å predikere om vedkommende har en ekstra stor mulighet til å utføre innsidervirksomhet. Siden jeg mangler litteratur som beskriver dette i detalj, så har jeg tatt det med som spesifikt tema i samtaler med ekspert.

5.3.2 Evaluering

Ved evaluering av modellen i tredje iterasjoner, har jeg gjennomgått modellen node for node med utgangspunkt i del-nettverk og hele nettverket. Jeg gjorde dette med samme eksperten som ved iterasjon en og to. Eksperten sa umiddelbart at dette så ut som en omfattende modell, men erkjente at når en arbeidet med folk så vil det være komplekst. Eksperten sa videre at når man fargesatte tabellen ble den noe lettere å lese, da personens sårbarheter ble synlige ved bruk av farger. Videre kommenterte eksperten ved følgende forhold:

Økonomisk kriminalitet: Videre ble det kommentert at også økonomisk kriminalitet til tider har blitt brukt for å finansiere rusmisbruk, og viser blant annet til ulike underslag som har blitt begått. Eksperten kommenterte deretter at det kan være en link mellom ideologi og økonomisk kriminalitet, da noen velger å gjøre økonomisk kriminalitet, sabotere økonomiske systemer eller lignende motivert av ideologiske overbevisninger.

Avvikende virtuell atferd: Eksperten mener at dette er et forhold som må være med i modellen, og peker på at veldig mange personer har en atferd på internett som i seg selv kan indikere problemer med tanke på sikkerhetsmessig skikkethet.

Helsemessige forhold: Eksperten kommenterer at flere kjente innsider-saker har økonomi som følge av sjukdom på personen selv eller nærstående vært en faktor. Som følge av oppstående

sykdom har dette gått på husholdningens økonomi, ikke vilje til å endre forbruk. Dette har gitt økonomiske incentiver til å bedrive innsidervirksomhet, da mange kan være villig til må gå langt for å komme seg ut av en slik situasjon.

Seksuelt avvikende atferd: Eksperten peker på at uønsket seksuell atferd kan være en indikasjon på andre ting som er i ubalanse hos personen, for eksempel sjukdom og manglende impulskontroll. Eksperten mener derfor at det kan være en node mellom slik atferd og helsemessige forhold.

Tilknytning: Eksperten mener at man i modellen også må ta hensyn til nærstående med tilknytning til fremmede stater, for eksempel ektefeller med statsborgerskap og lignende. Eksperten mener at det i sikkerhetsloven er et hull i denne sammenheng, og viser til sikkerhetsloven § 8-7, og mener at ektefelles statsborgerskap bør veie tyngre i etter loven.

Forbindelser: Eksperten mener dette er et svært vanskelig område å jobbe med, da det er noe som er vanskelig å detektere og enkelt å skjule. Det er for eksempel ikke noe som detekteres med atferdsendring. Eksperten mener at det er vanskelig å tilføye noe til det som allerede er i modellen, men indikerer at som følge av vanskeligheten med å detektere slikt så bør det tas tak i på et tidlig stadium.

Mulighet. Eksperten mener at det bør være noe som tar høyde for at enkelte bransjer må tåle å ta større risiko enn andre. Eksperten viser til teknologi-bedrifter, som kan være for eksempel Kongsberg-gruppen, tidvis kan trenge kompetanse som ikke finnes i Norge. Dette kan medføre at disse virksomhetene kan måtte hente inn personell med sårbarheter som tilknytning til andre stater eller annet. Det samme kan også gjøre seg gjeldende når en handler med enkelte aktører, for eksempel fremmede stater. Jeg spurte eksperten om hva han tenker om å inkludere denne typen vurderinger til noden «Utsatt bransje», noe han var enig i at det kunne være en god måte å operasjonalisere det på.

Pågående konflikt: Eksperten mener også at det er nødvendig med en risikoindikator som viser at individet har pågående konflikter, slik som samlivsbrudd, sykdom osv.

5.3.4 Revidering

Virtuell atferd – privat. Jeg ser behovet for at individets virtuelle atferd, herunder for eksempel på sosiale medier, nettfora, hvilke sider de oppsøker mm. i privat sammenheng også tas høyde for i modellen. Dette tas allerede høyde for når det gjelder forbindelser til organisasjoner, da det vurderes som del av «Aktiviteter». Jeg har vurdert å inkludere det som del av sekkeposten «Avvikende atferd», men funnet at det både ved deteksjon og oppfølging er sårbarheter så ulike at det er hensiktsmessige at det kommer frem av modellen som egen node, blant annet for den rent kvalitative og visuelle bruken av modellen. Noden «Avvikende virtuell atferd – privat» opprettes derfor, og «Avvikende virtuell atferd» endres til «Avvikende virtuell atferd – arbeid». Denne påvirker likt som «Avvikende atferd».

Livshendelser. Eksperten var enig i at pågående konflikter ved virksomheten måtte gjenspeiles i modellen, men at det også kunne være hensiktsmessige med en node som gjenspeilet dersom personen selv hadde lignende, pågående forhold, for eksempel dramatiske livshendelser, sykdom i nær familie, samlivsbrudd osv. Jeg oppretter derfor en node som heter «Negative livshendelser» under intensjon, som igjen påvirker «Press», «Økonomi» og «Sikkerhetsmessige forståelse».

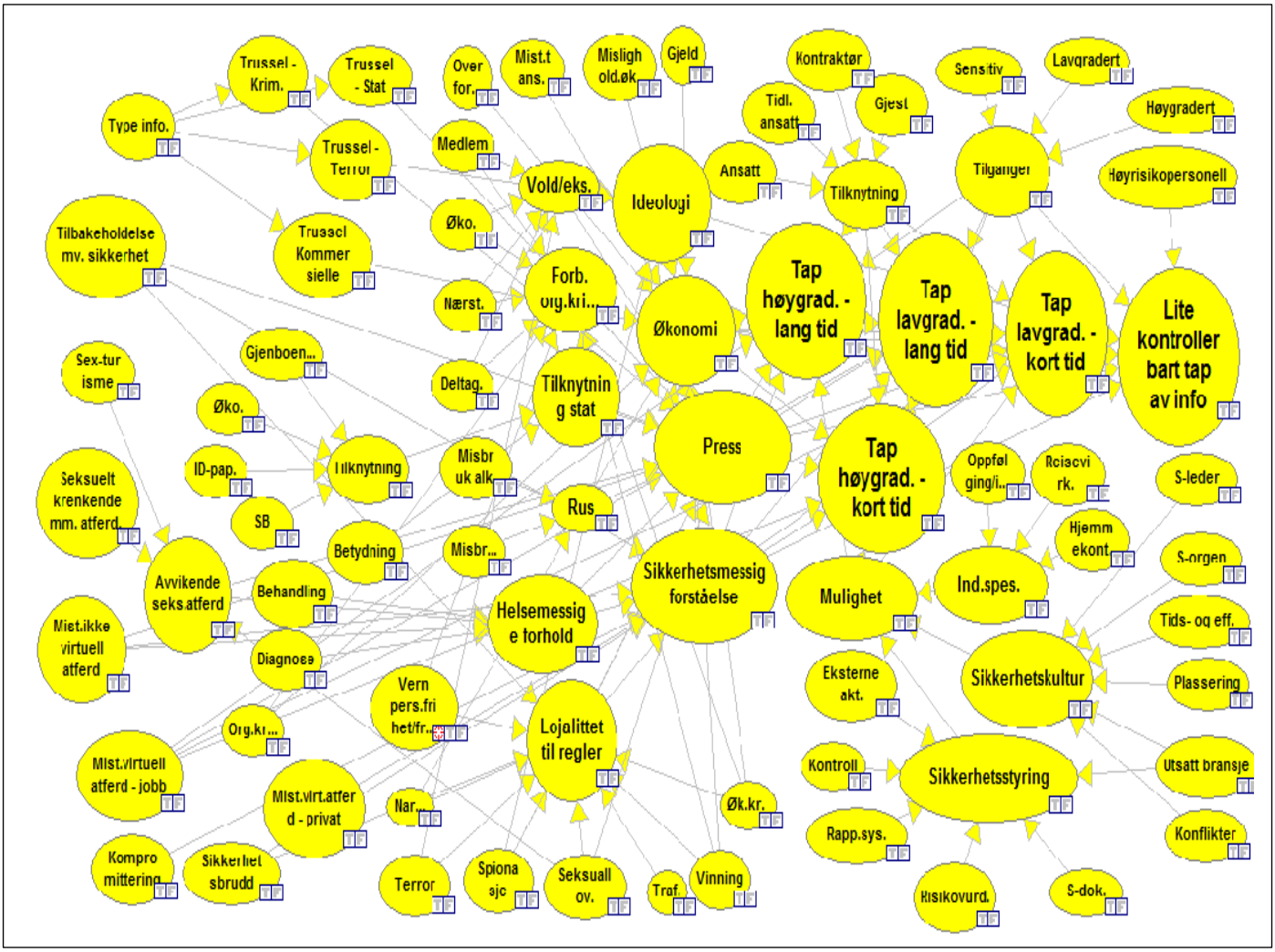
Helsemessige forhold og avvikende seksuell atferd. Eksperten pekte på at det ved vurdering av avvikende seksuell atferd, også bør tas høyde for at en slik atferd kan være en indikasjon på andre forhold, for eksempel helsemessige. Dette er en tanke som jeg har tatt noe videre, og sett i lys i drøftingen av helsemessige forhold og forholdet mellom diagnoser og atferd. Jeg har derfor funnet det nødvendig å opprette en node mellom forhold som beskriver avvikende atferd og helsemessige forhold, slik at det er mulig for modellen å ta høyde for kombinasjon mellom nettopp indikasjoner på helsemessige forhold og avvikende atferd.

Eksperten mente at det var nødvendig at individets nærstående knyttes nærmere oppimot tilknytning til fremmede stater, og «Nærstående» legges derfor til som en foreldrenode til vurderingen av grad av tilknytning til fremmed stat. Denne skal ta høyde for de lignende forholdene som vurderingen av personens egen tilknytning.
Risikoaksept og utsatt bransje. Jeg har vurdert at det er nødvendig med en node som gjenspeiler at enkelte virksomheter har behov for en høy risikoaksept for å kunne drive i sin bransje. Jeg har likevel ikke sett behov for å opprette en egen node, men har endret teksten til «Utsatt bransje», slik at denne også tar høyde for dette også.

Økonomi, rus og ideologi. Eksperten mente at det i enkelte saker kunne være en link mellom personers behov for å utøve økonomisk kriminalitet og behovet for å finansiere dette forbruket, samt at enkelte handlet i strid med en virksomhets økonomiske interesser som et resultat av ideologiske overbevisninger. Jeg har likevel ikke funnet behov for å opprette en formell sammenheng mellom disse, da slike motivasjoner i så fall må avdekkes gjennom eventuell granskning og etterforskning, og at det da vil gjenspeiles i modellen gjennom nodene som finnes. Jeg har likevel lagt til grunn at det kan være sammenheng mellom faktoren «Rus» og faktoren «Økonomi» og opprettet en kobling mellom disse.

5.4 Den endelige modellen

Den siste evalueringen som gjøres av modellen er en praktisk bruk av den, slik som nedenfor nevnte hvor bruksområdene gjøre. Modellen vil bestå av risikoindikatorer, som er indikatorer hvor brukeren selv kan legge inn tilstandene til noden utfra kjent kunnskap om personen. Videre vil faktorene, som ligger noe lengre inn i modellen kunne gjøre utregninger av tilstanden til disse. Den endelige modellen ser ut som følger:



Figur 10 *Endelig modell. Denne blir i neste avsnitt gjennom figur 11-14 brutt ned til delnettvekt.*

5.5 Problemer med kunnskapsmodelleringsprosessen

Gjennom prosessen har det vært få problemer, utover at innsider-feltet er komplekst og at det er større utfordringer knyttet til å begrense antall indikatorer og faktorer enn omvendt. Et problem i starten var for min egen del at jeg startet for spesifikt med å modellere for eksempel individspesifikke sårbarheter, uten at dette ledet frem til noe konkret i modellen. Ettersom jeg ikke kunne finne litteratur eller forskning som beskriver nettopp bruk av bayesianske nettverk i denne sammenhengen, ble det derfor nødvendig med et steg tilbake og begynne med definisjonen av en innsider.

Et annet problem med prosessen har vært å finne godt datamateriale, især når det gjelder faktiske innsider-saker og forholdene som har ledet frem til det. Dette har tatt meg til en «best practice»-tilnærming, hvor i stor grad veiledere og offentlige publikasjoner har vært grunnlaget for fastsettelse av noder. Dette har fungert på en tilstrekkelig god måte for å bygge modellen i denne oppgaven, men vil by på langt større utfordringer om modellen skal vektes. Jeg har videre brukt mer tid for å lete etter informasjon gjennom litteratur enn hva jeg har gjort ved å snakke med eksperter. En av grunnene til dette har vært at det har vært en svært omfattende prosess med å faktiske bryte ned innsiderrisikoen til noe som kan modelleres. Som følge av at dette ikke per tid er en vanlig arbeidsmetodikk innen personellsikkerhet, har jeg sett det nødvendig å stille til de ulike intervjuene med et godt bearbeidet materiale. Dersom jeg skulle utviklet denne modellen ytterligere, ville jeg har fra brukt betydelig mer tid med en ekspert.

6 Bruk av modellen – styrker og svakheter

I dette kapitlet vil jeg gjøre et praktisk eksempel på bruk av modellen, med utgangspunkt i en fiktiv person, med tenkte sårbarheter, tilhørighet til virksomhet og tilganger. Dette er gjort for å vise bruken av systemet i flere ulike scenarioer, herunder belyse styrker og svakheter.
Det første kapitlet vil vise en praktisk koding av nettverket, riktignok uten at disse er vektet. Deretter vil jeg prøve å bruke nettverket i ulike situasjoner. Dette er som et visuelt hjelpemiddel, til for eksempel et saksmøte; en drøfting av vekting og kvantitativ bruk; oppimot sikkerhetsmessig valør; og bruk som utgangspunkt for en tredimensjonal graf.

Personen som jeg har tatt utgangspunkt er del av en militæravdeling, hvor han er ansatt som systemadministrator på et system som er godkjent for informasjon gradert begrenset. Han har tilganger som gir grunn til en middels kapasitet, men er kategorisert som høyrisikopersonell i kraft av å være systemadministrator. Han har svært store tilganger innenfor sitt tjenstlige behov og dessuten kan utvide sine tilganger om han ønsker det, og derfor er kapasiteten utregnet til å være høy.

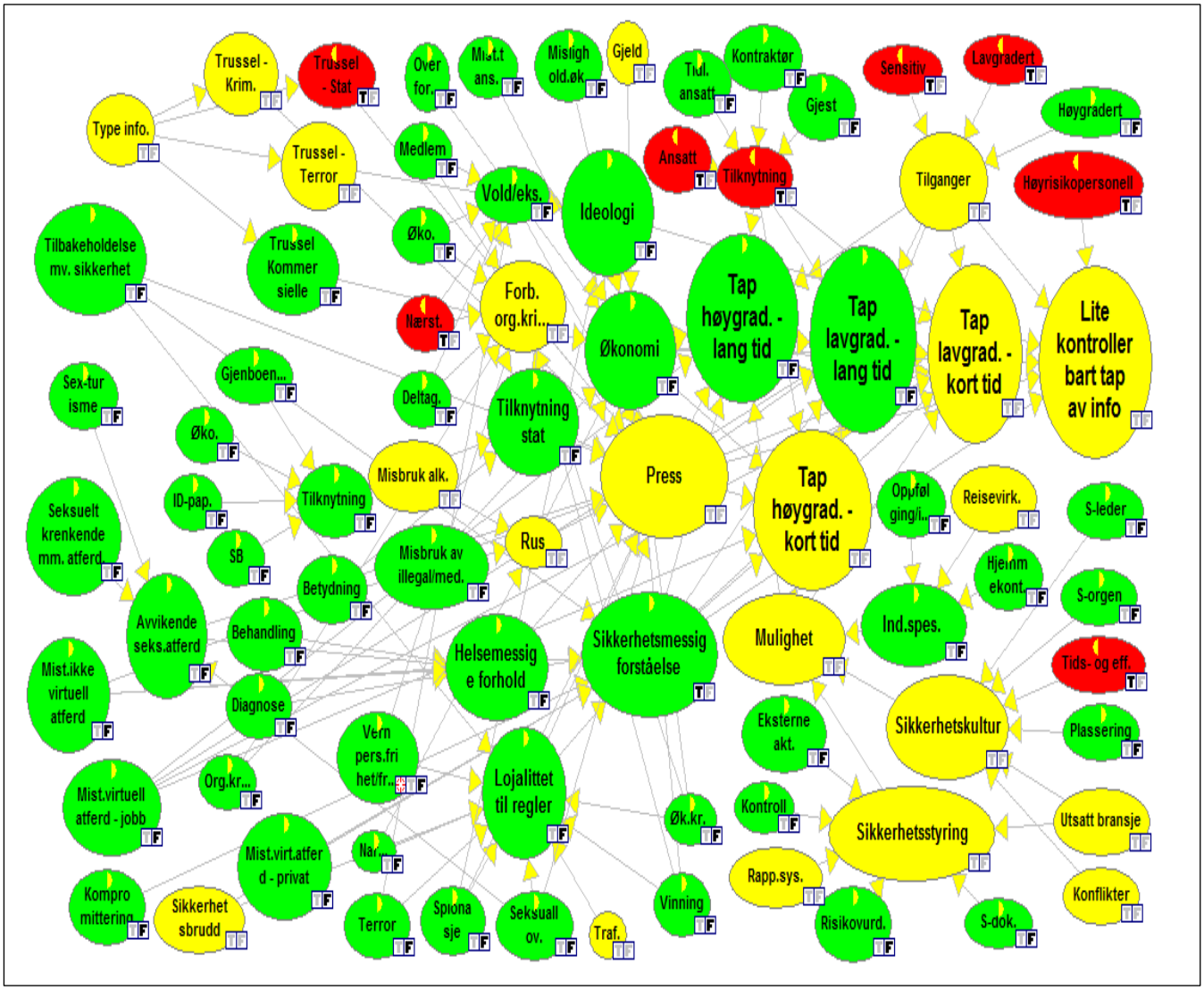
Avdelingen han jobber i har en god sikkerhetsorganisasjon og -styring. De et fungerende, men tungvint rapporteringssystem for sikkerhetshendelser. Avdelingen har et høyt tidspress, da de leverer operative leveranser til Forsvaret. Dette gjør at avdelingen sjelden er samlet, og mange er til enhver tid bortreist. Det har historisk sett blitt utført en del sikkerhetsbrudd i avdelingen. Dette har medført at til tross for en svært kompetent sikkerhetsavdeling, så ersikkerhetskulturen har vært skadelidende av dette. Dette er også vurdert i å gjenspeile hvor stor del sikkerhetsorganisasjonen får ta i for eksempel beslutningsprosesser. Personens arbeidsoppgaver kan dog utelukkende løses fra kontoret, og til tross for at hans arbeidsoppgaver i stor grad løses individuelt han han tett oppfølging av en datasikkerhetsleder. Han reiser ikke mye utover deployeringer til krise- og konfliktområder. I sum medfører dette at muligheten vurderes til middels.

Operativ bransje har over tid hatt stort operativt press, og det er derfor ansett som en noe utsatt bransje som følge av vanskeligheter med å prioritere sikkerhet. I tillegg har det siste tiden vært noe konflikter og misnøye i avdelingen, da det foregår politiske forslag som vil medføre langt høyere bokostnader, lavere lønninger for operativt personell ved å fjerne tillegg med mer.

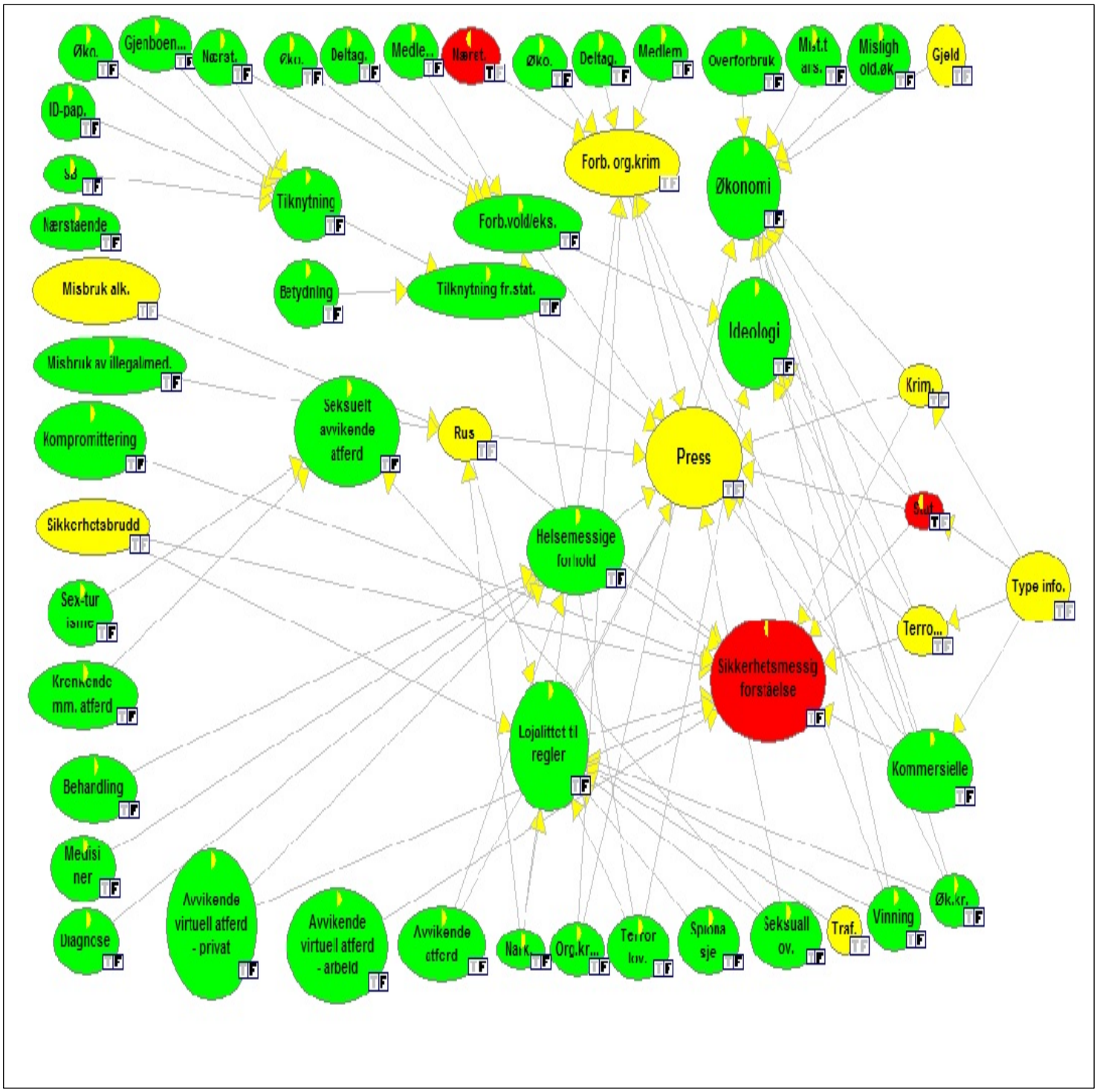
Vedkommende har en god økonomisk situasjon uten mistenkeligheter. Han er dog ung og i en etableringsfase, og har høy lånegrad som er vurdert til middels. Totalt så er hans økonomiske situasjon vurdert til å ha lav risiko knyttet til seg. Han har en bror som har et langt rulleblad og er involvert i et kriminelt miljø, men dette er uten at personen vår har hatt noen involvering i miljøet selv. Miljøet er et tungt kriminelt miljø, med forgreininger til utlandet, og er kjent kriminalitet med stort utbytte og vilje til å benytte seg av utpressing og vold. Det medfører en middels risiko for tiknytning til organisert kriminelt miljø, som igjen påvirker tilstedeværelsen av grunnlag for press. Han har ved flere anledninger hatt uheldige hendelser knyttet til alkoholpåvirkning, blant annet ved avdelingsfester, noe som gir utslag i en middels tilstand på

«Misbruk av alkohol», som igjen gir en gul tilstand på faktoren «Rus», som påvirker grunnlaget for press.
Videre foreligger det noen sikkerhetsbrudd på personen, noe som ikke skiller seg nevneverdig fra avdelingen ellers. Ingen av disse har vært veldig alvorlige, men som følge av at det er flere er tilstanden på indikatoren middel. Han har også en rekke trafikale lovbrudd ved fartsovertredelse, noe som gjør at denne noden er gitt middels. Begge disse påvirker «Lojalitet til regelverk», men denne er likevel utregnet til å være lav og grønn.

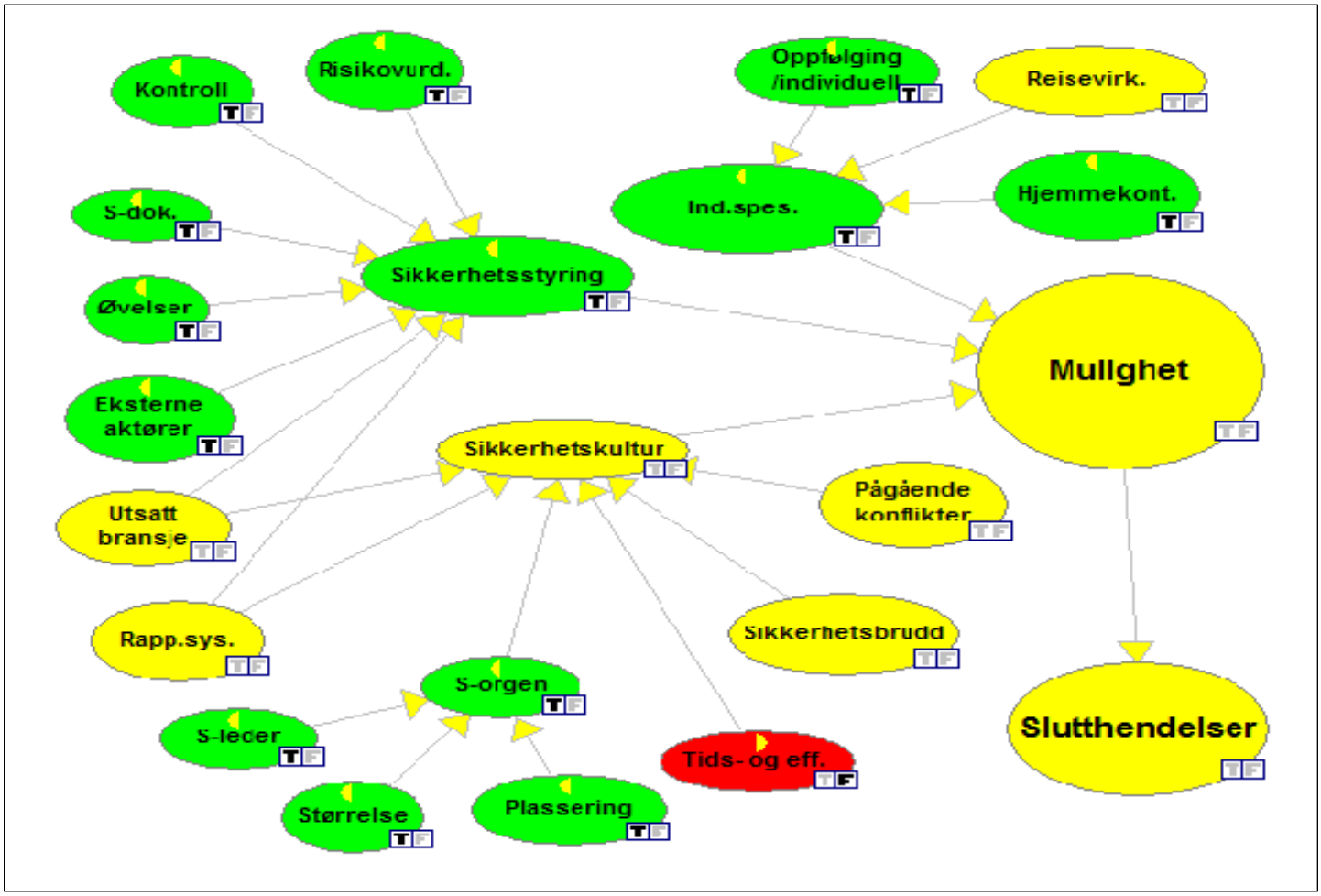
Han har tilgang til informasjon om militære kapabiliteter. Aktører innen terror og organisert kriminalitet er vurdert til å kunne ha noe interesse av operasjonsprosedyrer og kjennskap til våpenlagre Det er vurdert at statlige aktører vil kunne ha stor interesse av verdiene han forvalter. Trusselaktør statlig aktør er derfor vurdert til høy. Som følge av forbindelse til organisert kriminelle, typen informasjon og hendelser knyttet til alkohol er faktoren «Press» vurdert til å være gul. Utfra disse parametrene, vil et bayesiansk nettverk for denne personen se ut som følger:



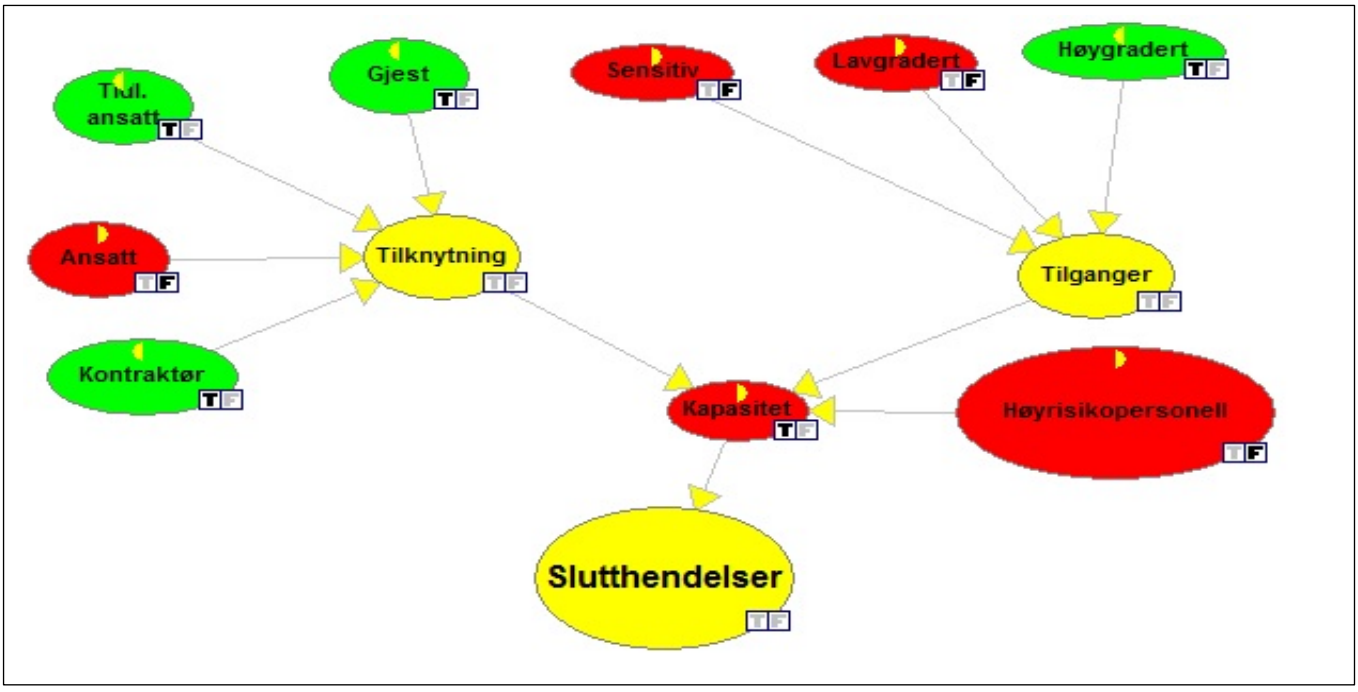
Figur 11: *Eksemplet viser en totaloversikt av en risikovurdering av den fiktive personen i eksemplet.*



Figur 12: *Eksempel intensjon fiktiv person i eksemplet.*



Figur 12: Eksempel mulighet fiktiv person i eksempel.



Figur 16: *Eksempel kapasitet fiktiv person i eksempel.*

6.1 Som visuelt hjelpemiddel

Bayesianske nettverk kan brukes for å visualisere kvalitative årsakssammenhenger, altså uten at man lager en CPT-tabeller og legger sannsynligheter til nodene (Aven, Risikoanalyse, 2017). Det har jeg heller ikke gjort i min oppgave, da det blir for omfattende og det foreligger mulig for lite informasjon tilgjengelig for meg til et slikt arbeid, men drøftes likevel i oppgaven min. Jeg ser to mulige måter som man kan bruke et bayesiansk nettverk som et visuelt hjelpemiddel.

For det første kan det brukes i typisk saksbehandling eller hvor en vurderer en person konkret oppimot for eksempel ulike tiltak, hvor en enten selv ønsker å sette seg inn i de ulike sammenhengene som finnes ved en person eller hvor en raskt ønsker å opplyse andre om personen. Da kan man ved enten en enkeltstående modell som viser hele innsiderrisikoen, eller ved å dele inn nettverkene i intensjon, kapasitet og mulighet. Dette muliggjør en fremstilling uten særlig mye tekst, og et godt grunnlag for å prate rundt ved en presentasjon. Det er for eksempel ved hjelp av en fargekoding veldig enkelt å se hvilke deler av innsiderrisikoen knyttet til personen i eksemplet som i størst grad bidrar til risikobildet, noe som kan bidra inn i beslutningsprosesser. Eksperten sa ved intervju at modellen med fargekoding gir et raskt og oversiktlig bilde av personen.

Når det gjelder personen i eksemplet, ser man raskt hvilke forhold som fører til risiko. På den ene siden er dette gjennom kapasiteten, en størrelse som i utgangspunktet ikke alltid er ønskelig å endre særlig på uten ved behov. Man ser da at på den ene siden er den ene sårbarheten til personen gjennom hans nærstående, noe han ikke i særlig grad selv kan kontrollere. Det kan likevel gi grunnlag for samtaler som omhandler bevisstgjøring av denne sårbarheten, som en slags «security awerness»-tilnærming. Videre kommer det frem klart at en av tingene som kan være en utfordring ved denne avdelingen, er at den som følge av tids- og effektivitetspress ikke alltid evner å sette sikkerheten høyt nok i prioriteringsrekkefølgen.

Videre er bayesianske nettverk intuitive, og i sin enkleste form enkel å forstå for folk. Eksperten i intervju 1 sa at et slikt nettverk kan være et lovende utgangspunkt for en funksjon som dette, og at en slik fremstilling vil kunne gi en mer dynamisk av individets sikkerhetsrisiko enn en mer utbredt skjematisk og punktvis fremstilling. Spesielt vil jeg si at det å fremstille dette nettverket på denne måten ved de ulike delnettverkene for intensjon, mulighet og kapasitet gir en slik visuelt enkelt fremstilling. Sett oppimot ulike tiltak enn kan

vurdere å iverksette ovenfor en person i personellsikkerhetsmessig sammenheng, slik som færre tilganger, bevisstgjøring av egne sårbarheter og oppfølging, administrative tiltak osv., vil kunne være enklere å se ved en visuell fremstilling. Det vil kunne gjelde dersom en står ovenfor en etterforskning eller gransking av en person som er mistenkt for innsidervirksomhet ved at man kan identifisere ulike informasjonsbehov som man har ved hjelp av modellen.

Dette henger også sammen med det som ekspert sa i samtale ved første og andre iterasjon, om at det kan være med på å gi organisasjonen et helhetlig bilde av innsiderrisikoen som en står ovenfor, men at det uavhengig av hvor godt verktøyet i seg selv er vil være svært avhengig av en fungerende organisasjon og ledere. Når det gjelder innsidervirksomhet, er det i de casene som jeg har studert vanskelig å peke på enkelthendelser eller -faktorer som har ledet frem til slik virksomhet. Det er svært mange faktorer som kan være bidragsytende til innsidervirksomhet, noe som lett kan skape et uoversiktlig nettverk. Dette kan gå utover brukervennlighetesom et rent visuelt hjelpemiddel. Videre er en svakhet at de komplekse sammenhengene ikke alltid er enkel å identifisere, noe som kan medføre at input til modellen på et nivå ikke vil kunne ha nødvendig påvirkning på de riktige faktorene lenger inn i modellen.

For det andre bruksområdet vil jeg vise til samtale med to eksperter ved Forsvarets sikkerhetsavdeling, hvorav den ene mente at dette kunne være en fornuftig måte fremstille innsiderrisikoens kompleksitet ved hjelp av ett bilde. Blant annet ble det trukket frem at dette kan brukes i opplæringsøyemed. Dette henger også sammen med den visuelt enkle fremstillingen som et bayesiansk nettverk kan tilby.

Det er likevel i denne sammenhengen behov for å presisere at spesielt nettverket som inneholder både intensjon, kapasitet og mulighet er et svært komplekst nettverk, med mange årsakssammenhenger, kan lide under at det er svært mange noder som henge sammen og at dette gjør at en kan miste noe av oversikten. For det bayesiansk nettverk i opplæringsøyemed ville det kanskje derfor være mer hensiktsmessig med en noe enklere struktur, for eksempel slik som strukturen var ved iterasjon 1 og 2.

6.2 Vekting og bruk av kvantitativ modell

Jeg har valgt å avgrense oppgaven min mot å vekte variabler i det bayesianske nettverket. Jeg vil likevel skrive noe om det da en slik bruk er en av metodens største fordeler, og et umulig tema å unngå.

Vekting av et bayesiansk nettverk vektes ved at de betingede sannsynlighetene til en nodes tilstander gis en verdi. Man kan finne frem til disse verdiene ved å innhente data, ved at eksperter gjør vurderinger eller ved at man bruker litteratur som foreligger innen domenet (Korb & Nicholson, 2003). For min oppgave har jeg hentet inn informasjon fra eksperter og via litteraturen, og det ville vært mest naturlig å legge disse til grunn for en slik fastsettelse. Fastsettelsen ville dog vært avhengig av at man også i større grad kunne innhente informasjon fra reelle innsider-saker og inkluderte det også i fastsettelsen av verdier. Det som vil gjøre denne jobben noe enklere, er at risikoindikatorene og foreldrenodene i modellen vil være mulig for brukeren å selv fastsette basert på informasjonen som man har om individet. Det ville derfor vært nødvendig å fastsette sannsynligheter mellom tilstanden på de nodene og faktorene. Disse vil aldri kunne bli helt nøyaktige, og det kan også være akseptabelt for modellen. Grunnen til at dette kan være akseptabelt er at modellens primæroppgave ikke er å avdekke hvem som faktisk bedriver innsidervirksomheten, risikovurdere hvem som kan komme til å bli det og hvilke konsekvenser det kan få. Sånn sett kan en si at modellen skal fremstille sannsynligheten på den ene siden, gjennom intensjon og mulighet, og på den andre siden konsekvenser gjennom kapasiteten.

Dersom det senere blir mer informasjon tilgjengelig, vil det føre til at modellen kan testes og evalueres i sin helhet. Videre vil den da kanskje kunne tas i bruk i praksis. En modell som denne beror på at en har store mengder informasjon om personer tilgjengelig og som i kraft av de juridiske hjemlene som ligger til grunn for innsamlingen, gjør at en kan bruke det til dette formålet. Dette er ikke et spesifikt tema for min oppgave.

Den største svakheten med å bruke et bayesiansk nett for risikovurdering for innsidervirksomhet, er at det vil være vanskelig å generere vekting utfra data. Mange nettverk genererer vekting ved bruk av metoder hvor man bruker data for å etablere bayesianske nettverk. Det finnes også metoder for å bruke eksperter til å finne disse vektene. Det har dog gjennomgående blitt utvist noe skepsis til å koble slike sammenhenger fra ekspert-hold, da det er vanskelig å vekte ulike forhold oppimot hverandre. Ved studier av faktiske innsider-saker

så ser man også at ingen er like, og intensjonen, motivasjonen og bakgrunnen for slik atferd varirer. Dersom jeg hadde brukt ekspertene til å gjøre dette ville man trolig senere ved bruk av data finjustere modellen for å være nøyaktig.

Det mest åpenbare problemet med bruk av bayesianske nettverk innenfor dette domenet, er at en *ikke* kjenner til alle innsidere og deres bakgrunn, motivasjon og utløsende faktorer. Dette gjør at en ikke vil ha all bakgrunnskunnskap tilgjengelig i modellen. Dette kan en si gjelder for mange fenomener som man kan tenke seg er belagt med store mørketall, da dette naturlig vil henge sammen med at man ikke har alle tilgjengelige data. Man kan videre se til de teoriene som ligger til grunn for security-området, og især sikring av verdier, hvor man står ovenfor en motstander som kan komme til å endre sin handlingsmåte utfra våre sikringstiltak. Dette kan bety at dagens kunnskap ikke trenger å være riktig i morgen.

Aven beskriver at bayesianske nettverk har vist seg hensiktsmessig i risikovurdering ved komplekse årsakssammenhenger. Et eksempel på bruk av bayesianske nettverk i en kontekst som kan ligne på den som oppgaven min legger opp til, er bruk innen finans og kredittvurdering av kunder. I denne sammenhengen legger man inn ulike faktorer, for eksempel alder og inntekt, og låser på denne måten ulike noders tilstand. På denne måten vil denne inputen kunne gi en output, som er en sannsynlighetsberegning for om en kunde ikke kommer til å betale for seg i en gitt tid fremover (Aven, Risikoanalyse, 2017). Det er med andre ord en usikkerhet knyttet til slike risikovurderinger, og kan umulig bli en modell som uten usikkerhet vil kunne slå fast at en person er eller kommer til å bli en innsider.

Med utgangspunkt i eksemplet med kredittvurderinger vil jeg videre drøfte noe rundt muligheten for å sette en personellsikkerhetsmessig valør for personell. Eksperten var ved første intervju klar på at dersom en skal motivere sikkerhetspersonell til å bruke en modell som denne, må det komme noe konkret ut av den. Et av momentene som vil kunne komme ut av en slik modell, er en slik sikkerhetsvalør basert på den sannsynlighetsberegningen modellen gjør gjennom inputen. Dette kan være som en totalverdi og/eller ved at man for eksempel deler inn en valør etter intensjon, mulighet og kapasitet. Jeg har ved bruk av modellen valgt å bruke en «trafikklys-modell» for å visualisere de tre tilstandene «Lav», «Middels» og «Høy», noe som gir modellen en mer intuitiv fremstilling. Dette var også noe som eksperten anbefalte, nettopp fordi det gir den et lettfattelig bilde.

Dersom en tar utgangspunkt i personen i eksemplet mitt, har jeg lagt inn at modellen gir vedkommende en viss negativ skår på grunnlag for press, blant annet gjennom sin brors tilknytning til et kriminelt miljø. Dersom en finner at hans individspesifikke sårbarheter skal forverres ytterligere, vil man med utgangspunkt i en inndeling i del-skår som ovenfor nevnt, kunne se hvor man kan sette inn tiltak for å senke innsiderrisikoen. Ved det spesifikke eksemplet finner man fort ved å analysere outputen i figur 13 og 15 at dette kan være at han skifter stilling slik at han har en bedre sikkerhetsorganisasjon eller -kultur rundt seg, og at man på denne måten kan senke risikoen. Det kan også i det tenkte tilfellet gjøres ved å fjerne de tilgangene som gir grunnlag for at han er klassifisert som høyrisikopersonell, og dermed finne et akseptabelt risikonivå. Dette handler om å gjøre målrettede tiltak for å etablere barrierer der hvor disse gjør størst nytte. Derigjennom kan en oppnå en risikobasert tilnærming til personellsikkerhet, noe som nevnes av Gelles (Gelles, 2016) som en av de viktigste momentene i et innsider-program.

Dette henger sammen med det som Aven (Aven, Risikoanalyse, 2017) skriver om at en risikoanalyse ikke gir beslutningen, men gir grunnlag for å fatte den. Dette kan være tiltak som virker sannsynlighetsreduserende, for eksempel en tettere oppfølging gjennom samtaler, og konsekvensreduserende, som å begrense tilgangene til vedkommende. Dette kan blant styres av risikoakseptkriterier, som er forhåndsbestemte verdier som en beregnet risiko skal ligge under. Dersom den ikke er det, gir det behov for tiltak.

I den daglige sikkerhetsmessige ledelsen kan dette være et verktøy. Gelles (Gelles, 2016) skriver at to av de tipsene som han i sin bok om å bygge programmer for å beskytte mot innsidertrusselen er at man må klare å avdekke og detektere forløpere til innsidervirksomhet ,look for precursors, og at man må evne å se disse i sammenheng, connect the dots. Bruk av bayesianske nettverk kan være nettopp en mulighet til å bruke de forløperne man i en organisasjon leter etter, «lagre» disse i individets risikovurdering og kunne bruke til å hente ut en output som sier noe om at vedkommende kan utgjøre en sikkerhetsmessig trussel dersom vedkommende gir utslag på gitte kriterier i modellen. At en slik modell kan ligge til grunn for å ta høyde for endringer over tid basert på en «pool» av historikk, pekte også ekspert på som noe som kan gi en mer dynamisk tilnærming til personellsikkerhet ved første intervjuet,

Grunnen til at dette er viktig, er fordi innsidervirksomhet sjelden skjer impulsivt, og innsidervirksomhet skjer ofte langs en kronologisk linje hvor det starter med flere forløpere til

slik virksomhet og ender opp med innsidervirksomhet. Ved å ha et system som dette, som kan brukes til å kontinuerlig vurdere personellets sikkerhetsmessige skikkethet, vil man derfor kunne se sammenhenger mellom hendelser og tilstander ved vedkommende av betydning for innsiderrisikoen. Det samme vil gjelde for hendelser eller tilstander ved virksomheten. Et viktig moment for bruk av en modell som dette i en kvantitativ sammenheng, vil derfor være at den kan si fra dersom inputen gir grunnlag for endring, for eksempel ved at en stakeholder i virksomheten melder inn at personens tilganger er endret eller at det foreligger informasjon som tjener som risikoindikatorer for innsidervirksomhet.

En av utfordringene ved en slik tilnærming er faren for at det vil oppstå falske positive, det vil si at modellen sier ifra ved personer som ikke reelt har til intensjon om å bedrive innsider-virksomhet. Jeg har diskutert dette med ekspert i intervju, og vedkommende så ikke problemer ved dette, da han uansett la til grunn at en slik modell bare indikerte at det var behov for enkelte tiltak. Dette, mente han, ville uansett bare skape en mer dynamisk sikkerhetsorganisasjon. Problemet i så måte, som jeg kan identifisere, er en overbelastning av sikkerhetsorganisasjonen ved for mange som «flagges» i systemet.

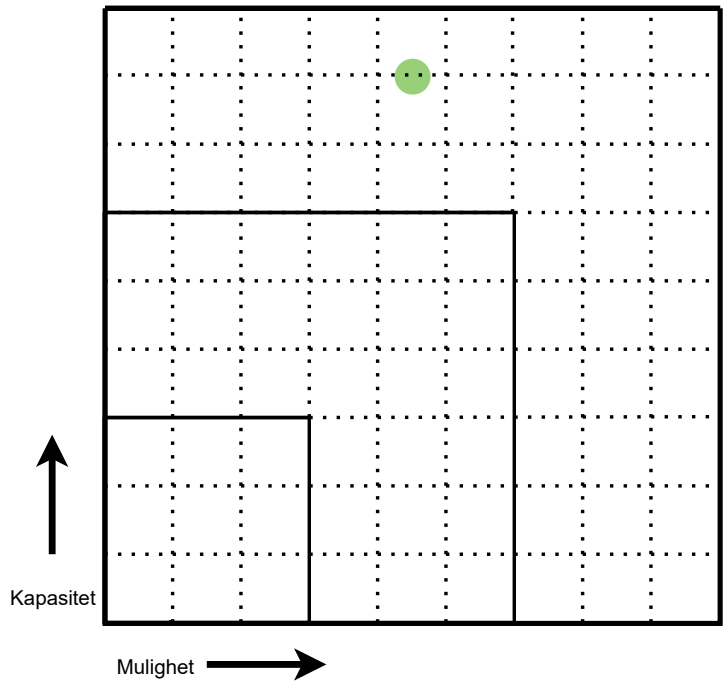
Modellens formål er å sette en risikoverdi på en person ut fra observerbare forhold ved vedkommende. I et fullt utviklet system ville denne prosessen fungert på samme måte, men trolig ville dette skjedd gjennom et mer brukervennlig verktøy. GeNIe er et verktøy for utvikling av bayesianske nett, men som verktøy for å risikovurdere en stor mengde personer ville det ikke vært hensiktsmessige. Det er mer sannsynlig at mange av disse dataene ville bli direkte lest inn i systemet fra en database dersom systemet ble tatt i bruk.

En av de største utfordringene i denne sammenhengen, vil være at mye av inputen i modellen vil være basert på ekspertvurderinger, for eksempel informasjon som blir tilgjengeliggjort for en sikkerhetsleder og som må analyseres før den brukes i modellen. Eksperten sa ved samtale at han har bekymringer knyttet til hvor mye opplæring som vil være nødvendig for at for eksempel sikkerhetspersonell forstår hvilken type informasjon som er relevant for spesifikke deler av modellen. Et enkelt brukergrensesnitt vil derfor være helt avgjørende for at en slik software skal har verdi i praksis.

6.3 Visuelt og kvantitativ i kombinasjon

Ekspert 1 sa i intervju i forbindelse med iterasjon 1 og 2 at det var viktig at det kom noe ut av en slik modell som kunne gi noe. Jeg har sett hen til de to forskningsspørsmålene som gjelder personellsikkerhetsmessige valør til understøttelse i den daglige sikkerhetsmessige ledelsen, og spørsmålet om det kan benyttes som et visuelt hjelpemiddel. Disse to spørsmålene har jeg valgt og sett i kombinasjonen, og se på mulighetene for å fremstille innsiderrisikoen i tredimensjonelle tabeller. Måten jeg har tenkt å visualisere dette med er ved å plassere kapasiteten langs y-aksen og muligheten langs x-aksen, hvor fargekodingen på markøren i grafen angir om intensjonen er lav (grønn), middels (gul) eller høy (rød).

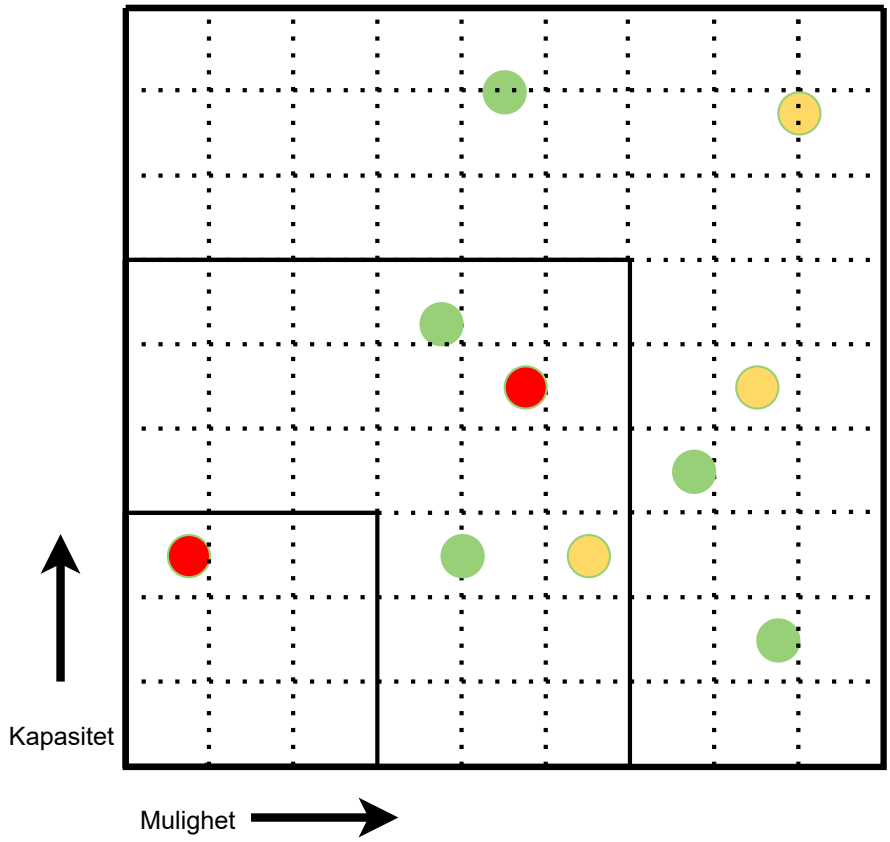
For individet kan denne modellen se slik ut:



Figur 15: *Her ser vi at den fiktive personen i oppgaven min gjennom sine tilganger og at han har en høyrisikorolle som systemadministrator, at muligheten som følge av tids- og effektivitetspress og en derigjennom svak sikkerhetskultur kombinert med en grønn intensjon plasserer han her i diagrammet.*

Dette er en enkel måte å ta resultatene fra det bayesianske nettverket, eventuelt delnettverkene, videre til nye måter å visualisere det på. Jeg legger til grunn at visualisering av denne ene personen, ikke gir noe mer informasjon enn hva man får fra å lese ut av

modellen eller delmodellene. Jeg har derfor sett på mulighetene som ligger i å plassere flere fra samme avdeling inn i denne modellen. Dette kan bli gjort i den hensikt å skaffe en totaloversikt over avdelingens personellsikkerhetsmessige situasjon. Dette kan se ut som følger:



Figur 16: *Her er en avdeling lagt inn i et diagram og vurdert etter parameterne mulighet, kapasitet og intensjon. De fargede prikkene representerer ansatte.*

Dette kan være en måte for en sikkerhetsleder å skaffe seg en oversikt over avdelingen sin. Grunnen til at personell tilhørende samme avdeling, men har ulik mulighet for å utøve innsiderrisiko kan handle om persons- og funksjonsspesifikke forhold ved arbeidsforholdet. Dette kan være forhold som hvor selvstendig individet løser sine arbeidsoppgaver, om vedkommende har stor grad av reisevirksomhet eller hjemmekontor med mer.
Det er flere måter jeg tenker at et slikt diagram kan benyttes, herunder blant annet knyttet til risikoaksept-kriterier, styring under spesielle hendelser eller endring og for å plukke ut hvilke individer man bør følge opp. En av grunnene til at dette kan være en måte å visualisere og bruke til beslutningstøtte, er fordi den ved ett enkelt bilde kan presentere risikobildet ovenfor en beslutningstager.

Denne metoden er mulig å bruke som et styringsverktøy ved at bruker de tre områdene som er skravert med heltrukken strek som områder som en indikator på risikoaksept-kriterium. Da kan for eksempel en si at alle som befinner seg i det ytterste området skal være grønn, i det nest ytterste skal være maksium gul og man kan ha aksept for rødfargede i det innerste området. Eventuelt kan det gi grunnlag for hvilket personell som en skal gjøre tiltak ovenfor.

Et av argumentene for å bruke en slik tilnærming, er at det innenfor domenet innsidertrusler er vanskelig å operasjonalisere sannsynlighetsbegrepet, da sannsynligheten for det enkelte individ i det aller fleste tilfeller vil være svært lav. På denne måten vil man i større grad kunne måle sårbarheten avdelingen har for slike hendelser i et helhetlig perspektiv, og kan være et godt styringsverktøy. Dette er blant annet noe av argumentasjonen som ulike aktører bruker til å argumentere i FFIs rapport om tilnærming til risikobegrepet i sikringskontekst (Busmundrud, Maal, Kiran, & Endregard, 2015) mot å benytte sannsynlighetsbegrepet i en security-sammenheng.

En annen måte som en kan benytte denne tilnærmingen er for eksempel dersom en virksomhet som gjøre en stor forandring i noen av sine avdelinger, for eksempel en relokalisering. Både eksemplet ved forsvarsminister Bakke som sa at det i forbindelse med saksbehandlingen rundt flyttingen av Andøya ble lekket, ekspert 1 sine uttalelser knyttet til endring i organisasjonen peker i retning av at enkelte prosesser i en virksomhet vil føre med seg en øket risiko for innsidervirksomhet. Ved å sammenstille informasjon tilknyttet de ulike avdelingene som kan bli gjenstand for en slik forandring, vil man da kunne bruke det til beslutningsstøtte for hvor man legger inn ulike avbøtende tiltak. På samme måte kan dette brukes til å beslutte hvilke avdelinger man for eksempel skal utføre inspeksjoner og lignende mot.

Noen av de utfordringene som er nevnte ved forrige avsnitt, vil åpenbart også kunne gjøre seg gjeldende innen dette bruksområdet. Det kan likevel være at man ved denne modellen, hvor man ikke utelukkende låser seg til individet, men kan få en hel oversikt vil kunne få en bedre nytte av risikovurderingene som gjøres av det bayesianske nettverket. Når man bruker det på denne måten, kan ikke bare se hvordan modellen vurderer et individ, men man anledning til å vurdere hvordan modellen vurderer individet i forhold til mange andre. Brukt på denne måten, vil man i større grad kunne jobbe utfra status i virksomheten, eller ulike enheter innen virksomheten, enn der man utelukkende jobber kun med tallene til individet.

6.4 Samsvar med tidligere forskning

Jeg har ikke funnet at det tidligere er gjort forskning på dette temaet spesifikt. At innsideraktivitet kan modelleres i bayesianske nettverk, og derigjennom fremstilles kvalitativt og kvantiativt, er dog med bakgrunn i de lignende domener i stor grad i samsvar med tidligere forskning og bruk av metoden.

6.5 Behov for ytterligere forskning

Behovet for ytterligere forskning på dette temaet er åpenbart knyttet til å bruke annen type software for modellen. På denne måten kan man vekte modellen. Utover dette anser jeg mulighetene for å bruke denne eller lignende modell innen personellsikkerhet som tilstedeværende, og noe som eventuelt må fases inn steg for steg.

7. Konklusjon

Man kan bygge et bayesiansk nettverk for å risikovurdere personell ved å bygge utfra parameterne intensjon, mulighet og kapasitet. Intensjonen i denne sammenhengen er motiver, og handler om tilstedeværelsen av trusselaktører og individspesifikke sårbarheter. Disse kan man bygge utfra det som er «best practice» på området, ved hjelp av utgivelser innen faget både fra norske og utenlandske myndighetsorgan, litteratur og ekspert-kunnskap.

Videre må man ta høyde for omgivelsene som personellet jobber under, ved å modellere muligheten for innsidervirksomhet med bakgrunn i virksomhetsspesifikke sårbarheter. Noder i denne sammenhengen kan hentes fra ISO-31000, veiledere i sikkerhetsstyring og lignende. Kapasiteten til en person er en kombinasjon av de tilgangene som virksomheten har gitt vedkommende, og den tilknytningen som personen har til virksomheten. Sistnevnte kan handle om alt personell med legitim tilgang til virksomhetens verdier, og kan være fra ansatte til gjester. Enkelt personer vil ha tilganger som gjør de til høyrisikopersonell når det gjelder kapasitet.

Den største utfordringen med å bygge et slikt nettverk er at mange av de forholdene som ovenfor nevnt, er vanskelig å operasjonalisere i en modell, og ikke minst vanskelig å gradere da flere er lite målbare. En praktisk utfordring ved bruken av nettverket er å innhente all denne informasjonen.

Et bayesiansk nettverk kan brukes på flere måter i personellsikkerhetsarbeid. Den enkleste måten å bruke det på er gjennom visuelle fremstillinger, det vil si som en ren kvalitativ analyse. Dette vil gi en lettfattelig og enkel fremstilling av de forholdene som bidrar til å senke eller øke innsiderrisikoen ved personen. Dette kan gi grunnlag for å se sammenhenger, presentere risiko og det kan også brukes som et utgangspunkt for å finne informasjonsbehov dersom en gjør vurderinger rundt en person. En trafikklys-modell, med bruk av fargene grønn, gul og rød, for å visualisere tilstandene lav, middels og høy gir det et enkelt visuelt bilde.

Når det gjelder den rene kvantitative vurderingen av personell, har jeg konkludert med at det foreligger noe mer usikkerhet ved bruksområdet. Med en god programvare, og med bakenforliggende ekspertvurderinger som gjør at en låser noder knyttet til risikoindikatorer til en gitt tilstand, vil man kunne gi en output innenfor gitte risikonivåer. Hvorvidt det vil være mulig å hente informasjon fra for eksempel en database, som igjen låser nodenes tilstand, er noe mer usikkert. Presisjonen i et slikt nettverk vil dog neppe bli godt nok til at man kan avdekke innsidere, noe som heller ikke har vært intensjon med oppgaven.

En måte å kombinere visuell fremstilling og kvantitative vurderinger er ved å gi de tre parameterne intensjon, kapasitet og mulighet en fargekoding, for deretter plassere dette inn i et tredimensjonalt diagram hvor y-aksen gir kapasiteten til personen, x-aksen gir muligheten og fargekoding av punktene representerer enkeltindividets intensjon. På denne måte kan en fremstille hele eller deler av virksomheten, og dette kan gi utgangspunkt for å understøtte den daglige sikkerhetsmessige ledelsen gjennom for eksempel se hvem man kan sette inn tiltak ovenfor, hvem som er risikopersonell og ved bruk av risikoakseptkriterier.
Ved å fargekode disse parameterne, vil man kunne gi personell en sikkerhetsmessig valør, som vil være en kombinasjon av de tre nevnte parameterne.

Det er dog flere utfordringer ved bruk av bayesianske nettverk i denne sammenhengen. Det vil være avhengig av kompetanse i sikkerhetsorganisasjonen, samt
god programvare som kan kommunisere med en database. Videre handler spesielt de individspesifikke sårbarhetene om delvis svært sensitive personopplysninger,
og det vil være åpenbare juridiske utfordringer ved en slik innsamling og lagring av personopplysninger

8 Referanser

(n.d.).

Antonsen, S. (2009). Safety Culture Assessment: A Mission Impossible?

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

Aven, T. (2017). *Risikoanalyse.* Oslo: Universitetsforlaget.

Bladet vesterålen. (2020, 12 3). *Bladet vesterålen*. Retrieved from www.blv.no: https://www.blv.no/nyheter/utro-tjenere-lekker-informasjon/

Bunn, M., & Glynn, K. M. (2016). Preventing insider Theft: Lessong from the Casino and Pharmaceutical Industries. In M. Bunn, & S. D. Sagan, *Insider Threats* (pp. 121 - 144). Ithaca og London: Cornell University Press.

Bunn, M., & Sagan, S. (2016). *Insider Threats.* Ithaca and London: Cornell University Press.

Burkett, R. (2013). Rethinking an old approach. 7-13.

Busmundrud, O., Maal, M., Kiran, J. H., & Endregard, M. (2015). *FFI-rapport 2015/00923: Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* Kjeller: Forsvarets Forskningsinstitutt.

Cassidy, T., & Cert Insider Threat Center. (2018, 04 12). *https://insights.sei.cmu.edu*. Retrieved from https://insights.sei.cmu.edu/blog/substance-use-and-abuse-potential-insider-threat-implications-for-organizations/

Engene, J. (2013). Mer overvåking, mer kontroll – Noen utviklingstrekk etter 22. juli 2011. *Tidsskrift for Samfunnsforskning*.

Forsvarsbygg. (2019). *Sikringshåndboka.* Oslo: Forsvarsbygg.

Gelles, M. (2016). *Insider threat: Prevention, Detection, Mitigation, and Deterrence.* Elsevier - Health Sciences Division.

Gule, L. (2012). *Ekstremismens kjennetegn.* Oslo: Spartacus forlag.

Hegghammer, T. (2016). Insiders and Outsiders: A survey of Terrorist Threats. In M. Bunn, & S. D. Sagan, *Insider Threats* (pp. 10-41). Ithaca og London: Cornell University Press.

Korb, B., & Nicholson, A. (2010). *Bayesian artificial intelligence.* Boca Raton, FL: CRC Press.

Korb, K. B., & Nicholson, A. E. (2003, 01). Review of Bayesian artificial intelligence. *Chapman and Hall*, pp. 289-298.

Kripos. (2021). *Politiets trusselvurdering 2021.* Oslo: Politidirektoratet.

Kruke, B.-I., Engen, O. H., Lindøe, P. H., Olsen, K. H., & Pettersen, K. A. (2012). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm akademisk.

Lie, E. L. (2015). *I forkant - kriminalitetsforebyggende arbeid.* Oslo: Gyldendahl akademisk.

Nasjonal sikkerhetsmundighet. (2021). *Veileder i verdivurdering av informasjon.* Kolsås: Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet. (2010). *Årsmelding 2010: Sikkerhetskultur.* Kolsås: Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet. (2019). *Veileder i personellsikkerhet.* Kolsås: Nasjonal sikkerhetsmyndighet.

Nasjonal sikkerhetsmyndighet, Kripos, Politiets sikkerhetstjeneste, Økokrim. (2017). *Sikkerhet ved ansettelsesforhold.* Oslo: Politiets sikkerhetstjeneste.

Norsk rikskringskasting. (2021, 09 29). *www.nrk.no*. Retrieved from https://www.nrk.no/norge/slapp-iranske-gjesteforskere-inn-pa-laboratorium-_-ntnu-forsker-tiltalt-1.15670346

NSM. (2020). *Temarapport innsidervirksomhet.* Nasjonal sikkerhetshetsmyndighet.

Nyberg, S.-O. (2016). *Statistikk - en bayesiansk tilnærming.* Universitetsforlaget: Oslo.

Politiets sikkerhetstjeneste. (2020). *Årlig trusselvurdering.* Oslo: Justisdepartementet.

Politiets sikkerhetstjeneste. (2020). *Årlig trusselvurdering* . Oslo: Justisdepartementet.

Politiets sikkerhetstjeneste, Økokrim, Kripos og Nasjonal sikkerhetsmyndighet. (2017). *Sikkerhet ved ansettelsesforhold.* Oslo: Politiets sikkerhetstjeneste.
Proactima. (2016). *www.proactima.no*. Retrieved from https://www.proakt.no/single-post/2014/12/09/et-rasjonelt-valg-om-trefaktortilnærmingen-til-sikringsrisiko
Reason, J. (1997). *Managing the risks of organizational accidents.* Ashgate publishing.
Sintef. (2001). *Sintefrapport: Metodikk for utarbeidelse av organisatoriske risikoindikatorer.* Trondheim: Sintef.
Statistisk sentralbyrå. (2021, 06 16). *www.ssb.no/*. Retrieved from Statistisk sentralbyrås hjemmeside: https://www.ssb.no/sosiale-forhold-og-kriminalitet/kriminalitet-og-rettsvesen/statistikk/anmeldte-lovbrudd-og-ofre)
Statistisk sentralbyrå. (n.d.). *www.ssb.no*. Retrieved from Statistisk sentralbyrå: https://www.ssb.no/sosiale-forhold-og-kriminalitet/kriminalitet-og-rettsvesen/statistikk/anmeldte-lovbrudd-og-ofre)
Stern, J., & Schouten, R. (2016). Lessons from the Anthrax Letters. In S. Sagan, & M. Bunn, *Insider Threats* (pp. 74 - 102). Ithaca og London: Cornell University Press.
Store norske leksikon. (2020, 10 23). *www.snl.no*. Retrieved from https://snl.no/statsborgerskap
US Departement of Defence. (2014). *Adjudicative Desk Reference.* Defense Personnel and Security Research Center / Defense Manpower Data Center.
Wikipedia. (2006, 09 16). *www.wikipedia.no*. Retrieved from https://no.m.wikipedia.org/wiki/Fil:SimpleBayesNet.svg
Økokrim. (2020). *Økokrim - Årlig trusselvurdering 2020.* Oslo: Økokrim.
Zegart, A. B. (2016). The Fort Hood Terrorist Attack. In M. Bunn, & S. Sagan, *Insider Threats* (pp. 42-73). Ithaca og London: Cornell university press.

9 Vedlegg

De fire første vedleggene til denne oppgaven er oppsummeringene av iterasjonene i tabellform. Disse ble vurdert tatt med i oppgaven, men ville gjort at oppgaven ble svært lang og ville vært forstyrrende ved gjennomlesning av den.

9.1 Vedlegg 1: Tabell intensjon – iterasjon 1:

Nodenavn	Beskrivelse	Tilstand	Foreldrenode(r)
Intensjon	Motivasjonen som vedkommende har til å bedrive innsidervirksomhet	Høy Middels Lav	Trusselaktør Individspesifikke sårbarheter
Trusselaktør	Hvorvidt det finnes en aktør(er) som har interesse av tilgang til virksomhetens verdier, i min oppgave virksomhetens sensitive eller graderte informasjon. Dette er en spesifikk vurdering av mulige trusselaktører sett oppimot informasjonen som individet har tilgang til.	Konkret ja/nei-vurdering.	n/a Et mulig forslag er «stalige aktører», «kriminelle aktører», «ideologiske aktører» og kommersielle aktører. Dette blir gjort til særskilt tema i samtale med ekspert ved første intervju.
Individspesifikke sårbarheter	Graden av forhold ved en person som kan medvirke til at han handler i strid med virksomhetens interesser, enten fordi andre utnytter dem, eller fordi de gir personen motivasjon.	Høy Middels Lav	Det nevnes for eksempel «Rus», «Økonomiske forhold», mm.

9.2 Vedlegg 2: Tabell, kapasitet – iterasjon 1

Nodenavn	Beskrivelse	Tilstand	Foreldrenode(r)
Tilknytning til virksomheten	Beskriver i hvor stor grad personen har tilknytning til virksomheten	Ingen Lav Middels Høy	Ansatt Tidligere ansatt Konsulent Gjest
Ansatt		Ja Nei	N/a
Tidligere ansatt		Ja Nei	N/a
Kontraktør		Ja Nei	N/a
Gjest		Ja Nei	N/a
Tilganger	Om hvorvidt personen har tilgang til gradert/sensitiv informasjon og graden av denne.	Ingen[2] Lav (sensitiv og informasjon gradert begrenset) Middels (Informasjon på konfidensielt og hemmelig) Høy (Informasjon på strengt hemmelig)	n/a
Særskilte funksjoner	Om vedkommende sitter i en stilling/funksjon med særskilte tilganger	Ja Nei	n/a Tema som må diskuteres nærmere med ekspert.

[2] Personell uten tilganger kan fungere som spioner, men at det ikke per definisjon vil gjøre disse til innsidere.

9.3 Vedlegg 3: Tabell, mulighet, iterasjon 2

Nodenavn	Beskrivelse	Tilstand	Foreldrenode(r)
Sikkerhetskultur	Hvorvidt virksomheten har en sikkerhetskultur som indikerer at det er vanskelig å bedrive innsidervirksomheten i virksomheten	Lav Middels Høy	Tids- og effektivitetspress Sikkerhetsorganisasjon Pågående konflikter Utsatt bransje Sikkerhetsbrudd
Tids- og effektivitetspress	Hvorvidt virksomheten er under et stort tids- og effektivitetspress på generelt grunnlag, eventuelt i en gitt periode.	Lav Middels Høy	n/a
Virksomhetens sikkerhetsorganisasjon	Grad av «godhet» i sikkerhetsorganisasjonen	Lav Middels Høy	Sikkerhetsleder Sikkerhetsorganisasjonens størrelse Sikkerhetsorganisasjonens plassering
Sikkerhetsleder			n/a
Sikkerhetsorganisasjonens størrelse	Hvor stor er sikkerhetsorganisasjonen sett i forhold til virksomheten totalt sett	Lav Middels Høy	n/a
Sikkerhetsorganisasjonens plassering	Hvor i organisasjonen er sikkerhetsorganisasjonen	Lav Middels Høy	n/a
Utsatt bransje	Hvorvidt virksomheten befinner seg i en bransje	Ja	n/a

	hvor man på generelt grunnlag kan si at det finnes en forståelse for den risikoen som en står overfor.	Nei	
Pågående konflikter	Hvorvidt virksomheten er i en endringsprosess, pågående konflikter, det foreligger usikkerhet som følge av politiske prosesser mm.	Ja Nei	n/a
Sikkerhetsbrudd	Hvorvidt virksomheten har et stort antall sikkerhetsbrudd, og vurdering av alvorligheten av disse.	Lav Middels Høy	n/a
Sikkerhetsstyring	Status på virksomhetens sikkerhetsstyring	Lav Middels Høy	Rapporteringssystem Utsatt bransje
Rapporteringssystem	Hvorvidt virksomheten har et rapporteringssystem	Ja Nei	n/a
Utsatt bransje	Hvorvidt virksomheten er innenfor det som kan defineres som en bransje som kan generelt har lav sikkerhetsmessige forståelse.	Ja Nei	

9.4 Vedlegg 4: Tabell intensjon, kapasitet og mulighet, iterasjon 3

Dette er en komplett modell for det endelige nettverket presentert i oppgaven.

INTENSJON			
Terror og spionasje			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r) (til)**
Terrorvirksomhet (Terrorhandlinger og terrorrelaterte handlinger)	Om det foreligger domfellelse eller mistanke om brudd på terrorlovgivningen, at vedkommende har vært involvert i gjennomføring av, forsøk på eller enhver forberedelse til terrorvirksomhet.	Høy Middels Lav	*Lojalitet til lovverk* *Forbindelse til voldelig gruppe eller terrororganisasjon* *Ideologi*
Spionasjevirksomhet (*Forbrytelser mot Norges selvstendighet og grunnleggende nasjonale interesser)*	Om det foreligger domfellelse eller mistanke brudd på straffelovens bestemmelser om ulovlig etterretningsvirksomhet, eller om at vedkommende har vært involvert i gjennomføring av, forsøk på eller enhver forberedelse til spionasjevirksomhet.	Høy Middels Lav	*Sikkerhetsmessig forståelse* *Ideologi* *Økonomi*
Straffbare forhold			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r) (til)**
Lojalitet til lovverk	Et mål på hvorvidt personen har en atferd som indikerer en	Høy Middels Lav	*Foreldrenode for: Sikkerhetsmessig forståelse*

	manglende evne og lojalitet for å følge lover og regler.		*Press*
Vern av den personlige frihet og fred		Høy Middels Lav	*Foreldrenode for:* *Forbindelse organisert kriminalitet* *Lojalitet til lovverk*
Seksuallovbrudd.		Høy Middels Lav	*Foreldrenode til grunnlag for press* *Lojalitet til lovverk*
Vinningslovbrudd		Høy Middels Lav	*Foreldrenode for:* *Økonomi* *Lojalitet til lovverk*
Økonomisk kriminalitet		Høy Middels Lav	*Foreldrenode for:* *Organisert kriminalitet* *Økonomi* *Sikkerhetsmessig forståelse* *Lojalitet til lovverk*
Trafikale lovbrudd		Høy Middels Lav	*Foreldrenode for:* *Lojalitet til lovverk*
Narkotikakriminalitet		Høy Middels Lav	*Foreldrenode for:* *Organisert kriminalitet* *Rus*
Organisert kriminalitet		Høy Middels Lav	*Forbindelse til organiserte kriminelle grupper*
Tilknytning til fremmed stat			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**

Tilknytning til fremmed stat		Høy Middels Lav	*Grad av tilknytning* *Statens sikkerhetsmessige betydning*
Grad av tilknytning		Høy Middels Lav	*Statsborgerskap* *ID-dokumenter* *Myndighetskontakt* *Gjenboende relasjoner* *Økonomiske interesser* *Interesseorganisasjoner* *Nærstående*
Statsborgerskap	Hvorvidt personen har statsborgerskap til den fremmede staten.	Ja Nei	*n/a*
ID-dokumenter	Hvorvidt personen har ID-dokumenter fra den fremmede staten.	Ja Nei	*n/a*
Myndighetskontakt	Hvorvidt personen har eller har hatt myndighetskontakt med den fremmede staten, og graden av denne.	Høy Middels Lav	*n/a*
Gjenboende relasjoner	Hvorvidt personen har gjenboende nærstående eller slektninger i den fremmede staten, og graden av denne.	Høy Middels Lav	*n/a*
Økonomiske interesser	Hvorvidt personen har økonomiske interesser i den fremmede staten, og graden av denne.	Høy Middels Lav	*n/a*
Interesseorganisasjoner	Hvorvidt personen er engasjert i	Ja Nei	*n/a*

	interesseorganisasjoner for den fremmede staten.		
Nærstående	Hvorvidt personen har nærstående med tilknytning til den fremmede staten, og graden av denne	Høy Middels Lav	*n/a*
Forbindelse til organisasjoner			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Forbindelse til organiserte kriminelle nettverk		Høy Middels Lav	*Medlemskap* *Deltagelse i aktiviteter* *Økonomiske interesser* *Gjennom nærstående*
Økonomiske interesser	Vurdering av hvorvidt det foreligger pengeoverføringer fra/til organisasjonen. Fra organisasjon til person vil alltid medføre at tilstanden er «høy».	Høy Middels Lav	*n/a*
Medlemskap	Hvorvidt personen er eller har vært medlem i organisasjonen Høy (er medlem) Middels (har vært) Lav (har ikke vært)	Høy Middels Lav	*n/a*
Deltagelse i aktiviteter	I hvor stor grad personen har deltatt i aktiviteter sammen med eller for	Høy Middels	*n/a*

	organisasjonen, herunder fester, propagandavirksomhet, ulovlige aktiviteter,	Lav	
Gjennom nærstående	En vurdering av om personen har nærstående som kan påvirke hans sikkerhetsmessige skikkethet i organisasjonen, og en vurdering av relasjonen og forbindelsen.	Høy Middels Lav	*n/a*
Forbindelse til ekstremistisk organisasjon		Høy Middels Lav	*Medlemskap* *Deltagelse i aktiviteter* *Økonomiske interesser* *Gjennom nærstående*
Økonomiske interesser	Vurdering av hvorvidt det foreligger pengeoverføringer fra/til organisasjonen. Fra organisasjon til person vil alltid medføre at tilstanden er «høy».	Høy Middels Lav	*n/a*
Medlemskap	Hvorvidt personen er eller har vært medlem i organisasjonen	Høy (er medlem) Middels (har vært) Lav (har ikke vært)	*n/a*
Deltagelse i aktiviteter	I hvor stor grad personen har deltatt i aktiviteter	Høy Middels	*n/a*

	sammen med eller for organisasjonen, herunder fester, propagandavirksomhet, ulovlige aktiviteter, nettaktiviteter, lese flyveblader o.l. med mer.	Lav	
Gjennom nærstående	En vurdering av om personen har nærstående som kan påvirke hans sikkerhetsmessige skikkethet i organisasjonen, og en vurdering av relasjonen og forbindelsen.	Høy Middels Lav	*n/a*
Tilbakeholde, feilaktig fremstilling eller forfalskning			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Tilbakeholdelse, forfalskning eller feilaktig av informasjon om forhold vedrørende egen sikkerhet.	En vurdering av hvorvidt det foreligger informasjon om slik handlinger knyttet til flere mindre alvorlige eller enkeltstående alvorlige tilfeller.	Høy Middels Lav	
Tilbakeholdelse, forfalskning eller feilaktig av informasjon om andre forhold vedrørende personens ansettelsesforhold.	En vurdering av hvorvidt det foreligger informasjon om slik handlinger knyttet til flere mindre alvorlige eller enkeltstående alvorlige tilfeller.	Høy Middels Lav	
Sikkerhetsbrudd			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**

Brudd på sikkerhetsbestemmelser	En vurdering av hvorvidt det foreligger informasjon om slik handlinger knyttet til flere mindre alvorlige eller enkeltstående alvorlige tilfeller.	Høy Middels Lav	*«Sikkerhetsmessig forståelse»*
Kompromittering av sensitiv eller gradert informasjon.	En vurdering av hvorvidt det foreligger informasjon om slik handlinger knyttet til flere mindre alvorlige eller enkeltstående alvorlige tilfeller.	Høy Middels Lav	*Må gå til «Sikkerhetsmessig forståelse», Bevisst innsider.*
Misbruk av alkohol eller andre rusmidler			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Rus	En faktor som måler tilstedeværelsen av indikatorer for rusmisbruk eller problematisk bruk av rus hos individer	Høy Middels Lav	*Misbruk illegale rusmidler* *Misbruk legale rusmidler*
Misbruk av illegale rusmidler	Vurdering av om personen har et forhold til illegale rusmidler eller medikamenter som utgjør en personellsikkerhetsmessig sårbarhet og graden av denne.	Høy Middels Lav	*Må gå til «Grunnlag for press», «Straffbare forhold», «Sikkerhetsmessig forståelse», «Helse».*
Misbruk av alkohol		Høy Middels	*Må gå til «Grunnlag for press»,*

		Lav	*«Sikkerhetsmessige forståelse», «Helse»*
Økonomi			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Økonomi	Hvorvidt det foreligger indikasjoner på personens økonomi som tilsier at det foreligger et grunnlag for fristelse til å handle imot virksomhetens interesser med tanke på informasjon, og til egen vinning.	Høy Middels Lav	*Gjeld* *Mistenkelige transaksjoner* *Overforbruk* *Misligholdt gjeld*
Gjeld	Om personen har stor gjeld sett i forhold til sin inntekt.		*n/a*
Mistenkelige transaksjoner	Hvorvidt det forekommer det foreligger informasjon om mistenkelige transaksjoner hos hovedpersonen, for eksempel store beløp, overføringer til utenlandske konti mm.	Ja Nei	*n/a* *Denne noden må også koples til «Pengeoverføringer» i vurderingen av tilknytningen til fremmede stater, dersom overføringen er til utlandet.*
Overforbruk	Hvorvidt og i hvilken grad personen har et forbruk av penger som er over det som inntekten tilsier.	Høy Middels Lav	*n/a*

Misligholdt gjeld	Om personen har misligholdt gjeld og størrelsen på denne.	Høy Middels Lav	*n/a* *Denne noden må også kobles oppimot ubevisst innsidervirksomhet*
Helsemessige forhold			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Sykdom som medfører forbigående eller varig svekkelse	Hvorvidt personen har en sykdom eller medisinsk tilstand som kan medføre at vedkommende har en forbigående eller varig svekkelse av pålitelighet, dømmekraft eller lojalitet, slik at den påvirker en sikkerhetsmessige skikkethet.	Høy Middels Lav	*Diagnose* *Behandling*
Diagnose	Har personen en diagnose av en mental lidelse.	Ja Nei	*n/a*
Behandling	Mottar eller har personen mottatt behandling mot diagnosen	Ja Nei	*n/a*
Medisiner	Medisiner som medfører svekkelse av årvåkenhet eller dømmekraften	Ja Nei	*n/a*
Andre forhold			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
Virtuell atferd - arbeid	En vurdering av hvorvidt personen har et høyt antall tilfeller av mistenkelig virtuell atferd (store e-poster, besøker	Høy Middels Lav	*Foreldrenode til «Sikkerhetsmessige forståelse»*

	nettsider, mistenkelige søk mv.) på virksomhetens systemer.		
Seksuell atferd	En vurdering av hvorvidt det foreligger indikasjoner på om personen har seksuell atferd som gjør seg gjeldende i vurderingen av innsiderrisikoen.	Høy Middels Lav	*Seksuelt krenkende atferd* *Seksuelle lovbrudd* *Sex-turisme* *Foreldrenode til «Grunnlag for press».*
Sex-turisme	Hvorvidt personen utfører reiser hvor seksuelle tjenester mot betaling er et av hovedmålene.	Ja Nei	*n/a*
Seksuelt krenkende atferd mm.	En node for bla. Seksuelt krenkende og annen avvikende seksuell atferd	Høy Middels Lav	*n/a*
Ikke-virtuell atferd	En node som skal fange opp andre typer hendelser enn de ovenfor nevnte, knyttet til mistenkelig atferd eller hendelser som som er kjent for å kunne indikere personellsikkerhetsmessig sårbarhet, slik som fallende prestasjoner, usososial atferd, stor misnøye mm. .	Høy Middels Lav	*n/a*
Avvikende virtuell atferd - privat	Hvorvidt personen har en atferd på internett, sosiale medier, diskusjonsforum	Høy Middels Lav	*n/a*

	mv. er avvikende eller mistenkelig.		
Trusselaktør			
Type informasjon	Ulike noder som beskriver hvilken type informasjon vedkommende har tilgang til, herunder med nodene Forsvar/sikkerhet/beredskap, Politiske beslutningsprosesser og forholdet til andre stater, Infrastruktur, Naturressurser og Forskning og teknologi	De ulike typer informasjon	*Trusselaktørene «statlige aktører», «Voldelige, terror og ekstremistiske organisasjoner», «organiserte kriminelle», «kommersielle aktører».*
Trusselaktører	Tilstedeværelsen av en trusselaktør med evne, vilje, tilstedeværelse, kapasitet mv. til å angripe verdiene som individet har tilgang til.	Høy Middels Lav	Organiserte kriminelle Statlige aktører Terror Kommersielle aktører
Organiserte kriminelle	Organiserte kriminelle grupperinger, med hovedmål om å begå alvorlige straffbare handlinger.	Høy Middels Lav	*n/a*
Terror	Grupperinger eller enkeltpersoner med målsetning om å begå brudd på norsk terrorlovgivning.	Høy Middels Lav	*n/a*

Kommersielle aktører	Aktører som ledd i forretningsvirksomhet innsamler informasjon.	Høy Middels Lav	*n/a*

MULIGHET			
Nodenavn	Beskrivelse	Tilstand	Foreldrenode(r)
Sikkerhetsstyring	Status på virksomhetens sikkerhetsstyring	Lav Middels Høy	Rapporteringssystem Utsatt bransje Risikovurderinger Eksterne aktører Sikkerhetsdokumentasjon Kontroll av styringssystem Øvelser Individspesifikke forhold
Rapporteringssystem	Hvorvidt virksomheten har et rapporteringssystem, og hvor godt det er	Lav Middels Høy	n/a
Utsatt bransje	Hvorvidt virksomheten er innenfor det som kan defineres som en bransje som kan generelt har lav sikkerhetsmessige forståelse, eller hvor det er nødvendig med en høy risikoaksept.	Ja Nei	

Risikovurderinger	Hvorvidt det foreligger risikovurderinger for sikkerhetsstyringen, og om disse inneholder momenter i henhold til best practice og standarder beskrevet i litteratur.	Lav Middels Høy	n/a
Eksterne aktører	Hvorvidt og i hvor stor grad virksomheten har eksterne aktører med egne sikkerhetsopplegg, og som virker inn i virksomhetens aktiviteter.	Lav Middels Høy	n/a
Sikkerhetsdokumentasjon	Hvorvidt det foreligger sikkerhetsdokumentasjon for sikkerhetsstyringen, og om disse inneholder momenter i henhold til best practice og standarder beskrevet i litteratur.	Lav Middels Høy	n/a
Kontroll av styringssystemet	Hvorvidt det gjennomføres kontroller av		n/a

	styringssystem, og om disse inneholder momenter i henhold til best practice og standarder beskrevet i litteratur.		
Øvelser	Hvorvidt virksomheten gjennomfører øvelser for å måle effekten av sikkerhetstiltsak.	Lav Middels Høy	n/a
Individspesifikke forhold	I hvilken grad det foreligger individspesfikke forhold ved personens arbeidsforhold som muliggjør innsidervirksomhet.	Lav Middels Høy	*Hjemmekontor* *Grad av lederoppfølging* *Reisevirksomhet*
Hjemmekontor	Hvorvidt, og i hvor stor grad, personen utøver sitt arbeid på hjemmekontor	Lav Middels Høy	*n/a*
Grad av lederoppfølging/individuelt arbeid	I hvor stor grad personen har direkte lederoppfølging/ løser sitt arbeid indiduelt.	Lav Middels Høy	*n/a*
Reisevirksomhet	I hvor stor grad personen har reisevirksomhet i sitt arbeid	Lav Middels Høy	*n/a*

Sikkerhetskultur	Hvorvidt virksomheten har en sikkerhetskultur som indikerer at det er vanskelig å bedrive innsidervirksomheten i virksomheten	Lav Middels Høy	Tids- og effektivitetspress Sikkerhetsorganisasjon Pågående konflikter Utsatt bransje Sikkerhetsbrudd Rapporteringssystem
Tids- og effektivitetspress	Hvorvidt virksomheten er under et stort tids- og effektivitetspress på generelt grunnlag, eventuelt i en gitt periode.	Lav Middels Høy	n/a
Virksomhetens sikkerhetsorganisasjon	Grad av «godhet» i sikkerhetsorganisasjonen	Lav Middels Høy	Sikkerhetsleder Sikkerhetsorganisasjonens størrelse Sikkerhetsorganisasjonens plassering
Sikkerhetsleder			n/a
Sikkerhetsorganisasjonens størrelse	Hvor stor er sikkerhetsorganisasjonen sett i forhold til virksomheten totalt sett	Lav Middels Høy	n/a
Sikkerhetsorganisasjonens plassering	Hvor i organisasjonen er sikkerhetsorganisasjonen	Lav Middels Høy	n/a
Utsatt bransje	Hvorvidt virksomheten befinner seg i en bransje hvor man på generelt grunnlag kan si at det finnes en forståelse for den risikoen som en står overfor.	Ja Nei	n/a

Pågående konflikter	Hvorvidt virksomheten er i en endringsprosess, pågående konflikter, det foreligger usikkerhet som følge av politiske prosesser mm.	Ja Nei	n/a
Sikkerhetsbrudd	Hvorvidt virksomheten har et stort antall sikkerhetsbrudd, og vurdering av alvorligheten av disse.	Lav Middels Høy	n/a
Rapporteringssystem	Hvorvidt virksomheten har et rapporteringssystem, og hvor godt det er	Lav Middels Høy	n/a

KAPASITET			
Nodenavn	**Beskrivelse**	**Tilstand**	**Foreldrenode(r)**
De fem ulike scenarioene – høygradert informasjon over kort tid, høygradert informasjon over lang tid, lavgradert informasjon over kort tid og lavgrader informasjon over lang tid samt «lite styrbar kompromittering»	Slutthendelser i modellen	Lav Middels Høy	Tilganger Tilknytning til virksomheten Høyrisikopersonell
Tilganger	Om hvorvidt personen har tilgang til gradert/sensitiv informasjon		Høygradert Lavgradert

Tilknytning til virksomhet	Graden av tilknytningen personen har til virksomheten	Sterk Middels Svak Ingen	Ansettelsesforhold Tidligere arbeidsforhold Konsulent Gjest
Høyrisikpersonell[3]	Individ som gjennom sin funksjon høye tilganger og som på ulike måter har mulighet til å utnytte dett, slik som for eksempel systemadministratorer, arkivarer osv.	Ja Nei	En node som leder direkte til scenario/hendelse

9.4 Vedlegg: Resyme av intervju 1 med ekspert

Tema	**Ekspertens vurderinger**
Ekspertens tanker om oppgaven.	Eksperten mener oppgaven er interessant, og peker spesielt på at fagmyndighet innen personellsikkerhet er de som dikterer fagfeltet. Han beskriver de som at de følger med i trenden, men at personellsikkerhet fort kan bli reaktivt. Et slikt system kan være med på å gi organisasjonen det komplette informasjonsbildet når det gjelder innsiderrisikoen, men er likevel avhengig av en fungerende organisasjon og ledere. En god informasjonsflyt til sikkerhetsorganisasjonen er essensielt. Han peker videre på at en slik modell kan være med på ta høyde for endringer over tid, og kan basere seg på en pool av historikk. Med et slikt komplett bilde så vil organisasjonen kunne gjøre en god vurdering på om personen bør ha de tilgangene som vedkommende har.
Bruksområde sikkerhetsvalør	Eksperten blir introdusert for en ide om å bruke en «trafikklys»-modell for vurdering av personell. Han mener det er vanskelig for han å si hvordan dette kan bli gjort, men at han ser for seg at det kan være mulig ved å se på en skår på de ulike faktorene med bakgrunn i risikoindikatorer. Han mener at dette kan være verdt et forsøk, og peker på at ved å bruke en modell som denne så er det viktig at det kommer en outout i

[3] Det vil være virksomhetsspesifikke vurderinger, blant annet med basis i verdivurderinger, som ligger til grunn for hvem som kan defineres som høyrisikopersonell.

	ene enden og at dette kan være et alternativ. Det kan gjøre det til et program for oppfang av mulige innsidere.
Visuell fremstilling	Eksperten mener at det er et lovende utgangspunkt for en slik funksjon, og at en slik fremstilling vil kunne gi en mer dynamisk fremstilling av individets sikkerhetsrisiko enn en mer utbredt skjematisk og punktvis fremstilling. Eksperten ser dog noen utfordringer knyttet til personellets kompetanse ved modellens praktiske bruk. Han peker for det første på om personell vil ha forståelsen for hvilke typer opplysninger som skal legges inn i ulike deler av modellen, og hvordan man skal lese den. Han mener det må være et enkelt brukergrensesnitt for en slik modell, og at brukere må ha de riktige inngangsverdier slik at de plasserer de operasjonelle faktorene på riktig plass. Samtalen med eksperten dreier inn på muligheten for at en slik modell vil skape falske positive, altså personell som gir utslag på modellen uten at de faktisk utgjør en sikkerhetsrisiko. Eksperten mener at dette også vil komme tilbake til personellets kompetansenivå, og at undersøkelse ved mistanker uansett vil skape en mer dynamisk og god sikkerhetsorganisasjon. Med en tredelt modell for fremstilling -

Tema	Ekspertens vurderinger
Kapasitet	Eksperten mener at kapasiteten er en grunnleggende ting å vurdere, og at det må sees som en stilling-funksjon-variabel og at innsiderrisikoen må vurderes utfra hvorvidt de finnes et mulighetsrom i utgangspunktet og hvor stort dette er. Virksomheter må våge å stille seg spørsmålet om hvem som vil kunne gjøre størst skade dersom de skulle bli innsidere, og innen hvilke domener som personen kan påføre virksomheten skade.
Tilknytning til virksomheten	Eksperten mener at dette kan være en hensiktsmessig måte å dele inn tilknytningen til virksomheten. Han bemerker at når det gjelder kontraktører så er dette en assymmetrisk arbeidsrelasjon. Dette kan gi grobunn for ulike problemer. For det første kan det medføre at til tross for at man jobber med et

	felles prosjekt så har man ikke nødvendigvis de felles overordnede målene, og det kan by på lojalitetskonflikter. Videre kan det medføre friksjon i form av for eksempel uavklarte arbeidsforhold. Eksperten anser derfor kontraktører som personell med en relativt høy innsiderrisiko knyttet til seg. Han påpeker at det i mange bransjer er en felles enighet om at dersom en person slutter i virksomheten og begynner i en annen, så må en anta at den kompetansen og næringsspesifikke informasjonen er overført til ny arbeidsgiver. Dette kan medføre et problem knyttet til kontraktører, som det kan være et stort antall av innom en virksomhet. Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Eksperten peker på at asymmetrisk arbeidsforhold er mer en arbeidssituasjon, som kan være preget av uavklarte forhold og ansvar. Dette er ikke bare ved bruk av kontraktører, men kan også oppstå ved «joint events». Dette er ulike virksomheter som jobber mot samme mål. I slike tilfeller vil også kontraktører kunne ta informasjon fra hverandre. Eksperten vurderer at slike tilfeller av uavklarte forhold i seg selv vil kunne medføre en høynet sannsynlighet for innsidervirksomhet, men er usikker på hvordan dette vil kunne brukes i en modell som skal representere individet. Eksperten snakket også om hvordan kunnskap flyttes mellom virksomheter, for eksempel ved et jobbskifte. En del av den kompetansen som en virksomhet får ved en person, kan være nettopp kunnskap som ikke skal tilflyte andre enn den arbeidsgiveren man kommer fra. Dette blir på en måte den

	enkelte persons eget konkurransefortrinn. Han peker derfor på at innsidervirksomhet kan forekomme som følge av jobbskifte, og at dette også kan sees på som en form for innsidervirksomhet.
Tilganger	Eksperten er enig i at en slik inndeling av tilgangene for enkelhets skyld kan fungere for de virksomhetene som er underlagt sikkerhetsloven, men at det åpenbart vil være utfordringer for virksomhetet som ikke har en slik lovpålagt innlagt inndeling. De vil måtte finne egne inndelinger som fungerer for dem.
Spesielle funksjoner	Eksperten er enig i at det er enkelte funksjoner som kan utgjøre et særlig stort skadepotensial dersom de skulle bedrive innsidervirksomhet, som går utover den graden eller viktigheten informasjonen isolert sett har. Dette kan være funksjoner som for eksempel en arkivar, hvor det for eksempel kan være mindre grunn til å vekke mistanke ved at vedkommende behandler dokumenter og informasjon som er utenfor tjenestelig behov. Det er en personellkategori som det er vanskelig å fastslå hvilke domener de har tilganger innenfor. Han peker også på for eksempel prosjektledere, som kan sitte på hele oversikten i et prosjekt og som derfor for eksempel kan gi informasjon om en teknologi som helhet. Dette til motsetning til for eksempel en enkelt ingeniør i et prosjekt, som kan være avskåret fra og mangle kompetanse om en teknologi som helhet. Dette gjør også at for eksempel det kan være fristende for trusselaktører å rette aktiviteten sin mot en slik person, fremfor å måtte rette det mot flere av ingeniørene. Han peker også på systemadministratorer rundt omkring. Han viser til at mange snakker om at man skal avskjære personell fra å få kjennskap til ting som ikke ligger innenfor deres

	tjenstlige behov, og at det samtidig sitter systemadministratorer i ulike virksomheter som har tilgang til det meste av informasjonen. Han peker i denne sammenhengen på Edward Snowden, og den skaden han påførte amerikanske etterretningstjenester som kontraktør. Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Eksperten påpeker at det er trusselaktørenes informasjonsbehov som først og fremst vil være styrende for hvor/hvem de retter seg mot. I noen tilfeller vil de vite veldig mye om for eksempel et produkt, og trenger kun en liten del av informasjon fra for eksempel en ingeniør for å ha det komplette bildet.
Trusselaktør	Eksperten peker i denne sammenhengen på at man som kunnskapsmodellør har definisjonsmakten, og at man må være spesifikk og konkret på akkurat dette punktet. Eksperten peker på at en trusselaktør må defineres som noe større enn et individ, og at aktøren må bære preg av å være organisert. Han peker i denne sammenhengen spesielt på fiendtlige stater, organiserte kriminelle og ekstreme ideologiske eller religiøse grupperinger. Eksperten peker også på at hvilke trusselaktører som er aktuelle for det spesifikke individet, blant annet må bestemmes utfra hvilken type informasjon om vedkommende har tilgang til. I denne sammenhengen peker han også på at det ikke bare er trusselaktører som kan oppsøke individer, men at dette også kan skje på motsatt måte.

	Eksperten er også enig i at kommersielle aktører også kan være en trusselaktør, da de kan ha behov for ulike typer informasjon i sin forretningsvirksomhet. Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Han mener at de fleste er dekket gjennom fiendtlige stater, religiøste/ideologiske grupperinger og organiserte kriminelle. Han nevner også hackergrupper, men tenker at disse faller innunder kategorien organiserte kriminelle. Han nevner videre dette med «selvmotiverte aktører», det vil individ som utfra egne overbevisninger finner ut at de vil bedrive innsidervirksomhet. Eksperten mener videre at en inndeling av typen informasjon som personen har tilgjengelig kan gjøres etter straffeloven § 121, selv om man kan bryte den ned ytterligere. Med tanke på å «parre» typen informasjon vedkommende skal ha tilgang til med de ulike trusselaktørene, er eksperten noe mer usikker. Han tenker at ingen av de nevnte kategoriene er gjensidig utelukkende, og at ulike aktører kan ha ulike motivasjoner for å hente inn informasjon om graderte og sensitive forhold. Han viser til at det kan være interessant for en fremmed, fiendtlig stat å innhente informasjon om forhold knyttet til helseberedskap av strategiske årsaker knyttet til landets beredskap, men at en kommersiell aktør kan ha like store interesser knyttet til dette temaet med tanke hvilke produkter de for eksempel kan selge inn til helsevesenet.

	Han mener det vil være mot sin hensikt å sette for rigide grenser for hvem som ønsker informasjon om hva. Det er åpenbart at det er noen aktører som kan ha større interesse for noen typer informasjon, men at det ikke vil være mulig å utelukke. Han mener dessuten at en inndeling av både trusselaktører og typen informasjon er så store, overordnede variabler at det er vanskelig å sette disse sammen.
Individspesifikke sårbarheter	Eksperten peker på at det er mye tilgjengelig informasjon om de store innsidersakene er analysert, gransket og tilgjengelig. Det som går igjen trang økonomi, at man har hatt syk kone og andre definerende faktorer, hendelser i livet med mer. Han sier at det er vanskelig å lage en komplett liste på hvilke forhold som kan føre til at noen begår innsidervirksomhet, men at sikkerhetsloven § 8-4, fjerde ledd bokstav a til o gir en veldig god liste over forhold som er sentrale i en slik vurdering.[4] Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Med tanke på de individspesifikke sårbarhetene trekker eksperten frem hvordan ulike forhold kan forsterke hverandre. Han drar frem Edward Snowden, som av overbevisningsårsaker ønsket å varsle om et overvåkningssystem i amerikansk etterretningsarbeid, og ifølge seg selv flere ganger forsøkte å melde fra om dette i «linjen». Hans trang om må varsle om dette skal ha blitt forsterket av disse avvisningene. Eksperten trekker også frem MICE-modellen for innsidervirksomhet, som kan være et grunnlag for modellen. MICE er et akronym og står for «Money», «Ideologi», «Coersion» og «Ego».

[4] Eksperten sa dette uten at jeg spurte, jf. at dette også er et spesifikt spørsmål i intervjuguiden.

Virksomhetsspesfikke sårbarheter:

Tema	Ekspertens vurderinger
Sikkerhetsstyring	Eksperten mener at her går det et skille mellom de som er underlagt sikkerhetsloven og de som ikke er det. De som er underlagt sikkerhetsloven vil kunne bli vurdert utfra lovens krav og graderes deretter. Der vil avvik kunne gå inn i en vurderingsskala og de kan vurderes utfra det. Han lurer mer på hvordan virksomheter som ikke er underlagt sikkerhetsloven skal bygge opp et slik system, når de ikke har en lov som stiller opp kravene. Han peker på at muligheten for å drive sikkerhetstjeneste uansett vil stå og falle på om man klarer å styre virksomheten kulturelt på en måte som tilrettelegger for det. Han peker også på hvordan «tonen på toppen» i stor grad vil styre hvordan denne kulturen vil spre seg nedover i organisasjonen. Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Eksperten legger til at det blir sannsynligvis en Best practice-tilnærming.
Virksomhetens sikkerhetsorganisasjon	Eksperten peker på at man må måle sikkerhetsorganisasjonen på hvilken effekt den har i virksomheten.
Sikkerhetsleder	Eksperten drar her tråden i forhold til effekt til sikkerhetsorganisasjonen videre. Han peker her på at et moment som kan være styrende for om en sikkerhetsleder fyller sin funksjon, er hvilke fora han deltar på. Han peker på at det forskjell på om sikkerhetslederen deltar på ulike ledermøter og lignende, kontra om han kun får kjøre egne internmøter.
Rapporteringssystem	Eksperten blir innledningsvis introdusert for tanken om at denne noden bare skal ha to noder – altså om virksomheten har eller ikke har et rapporteringssystem. Han mener at dette kan være en tilnærming, og viser til at dersom dette er forankret i akademisk litteratur er det ikke problematisk. Han mener dog at det kan være mulig å definere «diffus mellomsjikte» her, som tar høyde for forhold som om det

	faktisk finnes en sunn informasjonsflyt i virksomheten og hvorvidt rapporteringssystemet blir brukt. Brukergrensesnitt, evt. hvor stor arbeidsmengde det medfører, trekkes frem som mulig ting å legge til grunn i en slik vurdering. På spørsmål mener han også at det vil kunne være mulig å la eksterne vurdere rapporteringssystemet.
Generelle betraktninger virksomhetsspesifikke faktorer	Eksperten peker i denne sammenheng på funn fra egne studier, hvor han fant det var stor forskjell på virksomheters sikkerhetsstyring utfra hvorvidt de gjorde det som en integrert del av egen virksomhet eller om det var noe en gjør for «compliance». Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer:
Sikkerhetskultur	
Tids- og effektivitetspress	Eksperten er enig i at dette er en klar risikoindikator på en manglende sikkerhetskultur, da fokuset på leveranser vil kunne overskygge et nødvendig fokus på sikkerhet. Han peker spesielt på en situasjon hvor man har mange leveranser med deadliner som skal overholdes vil være en risikoindikator for sikkerhetskulturen.
Utsatt bransje	Ved en gjennomlesning med eksperten i forhold til intervjuet, fremkom videre følgende presiseringer: Eksperten peker på at det er gode grunner til å ha «fordommer» til enkelte bransjer, og viser blant annet til enkelte etater hvor det uttrykkes lite forståelse for at noen taper sikkerhetsklareringer. Han viser i denne sammenhengen til tilfellet med Robert Hansen, og hvordan dette fremstod som en «blame-game», hvor CIA og FBI kranglet om hvor det lekket informasjon og ingen var villig til å erkjenne at det kunne komme fra noen av dem. Han viser til tilfeller fra departementer, forskning og justis-sektoren i denne sammenhengen.

Pågående konflikter	Eksperten er enig i at dette er en viktig faktor i modellen, og at en del prosesser på en arbeidsplass kan medføre store påvirkninger på enkeltindividets holdninger. Han peker spesielt på en motstand mot endringer, og at dette kan påvirke individers holdninger og tilnærming til for eksempel sikkerhet. Dette kan direkte påvirke sikkerhetskulturen. Han peker på at virksomheter i slike prosesser kan ha behov for mange tiltak for hvordan man håndterer folk, og at det er krevende for en sikkerhetsorganisasjon å være «på ballen» hele veien.

I tillegg til et semistrukturert intervju diskutert med ekspert 1, gjennomførte jeg en samtale med to eksperter fra Forsvarets sikkerhetsavdeling som var så vidt interessant at jeg ønsker å ta med momenter fra disse i revideringen og den videre oppgaven:

Tema	**Ekspertens vurderinger**
Ekspertens tanker om oppgaven.	Den ene eksperten var noe usikker på hvordan dette ville slå ut, da han ikke er sikker på om det vil være et tilstrekkelig kunnskaps- og kompetansenivå ute i organisasjonene. Han var videre på den ene siden usikker på om man i operasjonaliseringen av faktorene ville ende opp med at personell tilpasser inputen sin til personen man har foran seg for å få dette til å passe inn i eget bilde. Når det gjelder antall noder i modellen, var den ene eksperten veldig usikker på antall, og var frem og tilbake på om et stor eller et lite antall var å foretrekke. Han landet på at et relativt begrenset antall var å foretrekke, og trakk fram at dersom det blir for mange noder så vil mange være tilbøyelige til å vurdere risikoen for høyere enn den kanskje er dersom det skulle være treff på flere noder.
Bruksområde sikkerhetsvalør	Han mener det kan være åpenbare problemer med et slikt system, da det kan være vanskelig for personell i gi god input. Dette vil i andre rekke kunne føre til dårlig output. De tenker at det kan være en god øvelse for en sikkerhetsorganisasjon å plassere personellet sitt i en slik modell, gjerne to personer uavhengig av hverandre. Det kan videre være interessant å føre et diagram som en øvelse for virksomheten, og kan gi en oversikt over hvor man ligger i avdelingen hva angår personellsikkerhet og hvor man

	bør sette inn støtet. Prosessen som leder frem til slike diagram og modeller trekkes frem som ekstra viktig.
Bruksområde - visuelt	Jeg viste først ekspertene den enkleste formen for at nettverket kan brukes som visuelt hjelpemiddel i modellen, altså som et rent kvalitativt nettverk. Ekspertene er usikre på hvor mye dette vil gi trenet sikkerhetspersonell, men at det kan være en interessant fremstilling spesielt i opplæringsøyemed.

9.5 Vedlegg 5: Resyme av intervju 2 med ekspert

Generelt om intervjuet

Dette intervjuet ble gjort uten en formalisert intevjuguide, men gjennomført likt som forrige intervju når det gjelder tilnærming som et semistrukturert intervju. Intervjuet er gjennomført ved at en og en node er gjennomgått med eksperten, hvor vedkommende er instruert til å kommentere noden i seg selv, hvilke faktorer den tjener som foreldrenode for og om den burde være foreldrenode for andre faktorer. Nodene er først presentert med hele nettverket, før nodene ble gjennomgått med utgangspunkt i delnettverkene for intensjon, mulighet og kapasitet.

Generelt om modellen

Eksperten ble umiddelbart fremvist modellen i sin helhet og gitt en sjanse til å se over den. Han sa umiddelbart at dette så ut som en omfattende modell, men erkjente at når en arbeidet med folk så vil det være komplekst. Det ble dog uttrykt noe bekymring knyttet til om det ville være for komplekst for brukeren, dersom dette ikke var erfarent sikkerhetspersonell.

Eksperten ble deretter presentert for modellen hvor den fiktive personen i oppgaven var lagt inn i nettverket. Eksperten mente at det med en slik trafikklys-tilnærming fremgår langt klarere hvilke sårbarheter som personen har, og gir derfor et raskt overblikk over hvor vedkommende kan være sårbar.

Eksperten kommenterte deretter at MICE-modellen er en enkel tilnærming som passer til modellen, men at RASCLS-modellen mulig gir et bedre bilde på hvordan innsidervirksomhet faktisk fungerer ved at det fokuserer på den som håndterer personell for å rekruttere til slik virksomhet.

Intensjon

Eksperten ble deretter forelagt delnettverket for intensjon, og ble bedt om å kommentere node for node.

Øk.krim: Eksperten sa innledningsvis at de fleste ting kan påvirke faktoren press. Når det gjelder økonomisk kriminalitet så er dette noe alle vet er feil. Videre ble det kommentert at også økonomisk kriminalitet til tider har blitt brukt for å finansiere rusmisbruk, og viser blant annet til ulike underslag som har blitt begått.

Eksperten kommenterte deretter at det kan være en link mellom ideologi og økonomisk kriminalitet, da noen velger å gjøre økonomisk kriminalitet, sabotere økonomiske systemer eller lignende motivert av at de har en ideologi.

Vinning: Eksperten mener at dette mangler en ideologisk komponent, og at man derfor kan anta at dette er handlinger utført for personlig vinning.

Trafikk. Eksperten er enig i at det ved gjentatte trafikkforhold så er det lojalitet til regler som er det springende, og at det burde gå noen lamper dersom det begynner å bli sterke indikatorer på trafikk. Eksperten uttrykker dog at det skal utvises forsiktighet med å konkludere for mye rundt folks sikkerhetsmessige skikkethet som følge av trafikk-lovbrudd. Det bør derfor være et betydelig antall slike hendelser før det får særlig vekt.

Seksuallovbrudd: Eksperten mener at generelt så er seksualitet et mulig problem og noe som kan benyttes som et pressmiddel, og peker på at det ved slike saker er en skamkomponent som går igjen. Eksperten mener at dette også kan være et spørsmål om legning, der det er forhold som er ønsket å holde skjult. Dette kan også være et spørsmål ved personens preferanse i denne sammenhengen, hvor vedkommende føler en trang til å reagere på denne.

Terror: Eksperten mener at dette er et punkt som må være med i modellen, da det finnes et stort utvalg av lover som kan innunder terrorlovgivningen. Han peker på at personer kan bli involvert i slike lovbrudd uten at man selv har en direkte intensjon om selv å utføre terror.

Avvikende atferd: Eksperten sier at dette også kan være en type atferd som kan lede til press, og kan bli gjenstand for å være skambelagt. Det kan være ulike typer atferd, som nervøsitet, ubegrunna handlinger og personer som sliter med svært mange ulike ting.

Avvikende virtuell atferd: Eksperten mener at dette er et forhold som må være med i modellen, og peker på at veldig mange personer har en atferd på internett som i seg selv kan indikere problemer med tanke på sikkerhetsmessig skikkethet.

Eksperten blir gjort oppmerksom på at dette er tenkt som en node som skal fange opp slik atferd på egne systemer. Han er videre enig i at dette er en type atferd som må logges, og peker på at det er viktig å finne atferd som er i strid med sitt tjenstlige behov. Han mener dog at dette er et avvik som i de fleste tilfeller vil være aktuelt å løse gjennom oppfølging og bevisstgjøring, da det ofte ikke er den onde hensikten som er det mest sentrale i slike tilfeller.

Helsemessige forhold: Eksperten kommenterer at flere kjente innsidersaker har økonomi som følge av sjukdom på personen selv eller nærstående vært en faktor. Som følge av oppstående sykdom har dette gått på husholdningens økonomi, ikke vilje til å endre forbruk. Dette har gitt økonomiske incentiver til å bedrive innsidervirksomhet, da mange kan være villig til må gå langt for å komme seg ut av en slik situasjon.

Eksperten blir gjort oppmerksom på at noden primært er tenkt å brukes for lidelser som direkte kan påvirke dømmekraften. Eksperten vil da la nodene bli stående.

Seksuelt avvikende atferd: Eksperten peker på at uønsket seksuell atferd kan være en indikasjon på andre ting som er i ubalanse hos personen, for eksempel sjukdom og manglende impulskontroll. Eksperten mener derfor at det kan være en node mellom slik atferd og helsemessige forhold.

Sikkerhetsbrudd og org.krim: Logistikk i NAMMO – høysensitiv, sympati, kan være hensiktsmessige å vite hva det gjelder. Bevisste sikkerhetsbrudd. Til stater – med tanke på sikkerhetsbrudd – det som aktualiseres over lang tid. Kan interessehevde for andre plutselig – f.eks. en konkurrent.

TIljnytning: Eksperten mener at man i modellen også må ta hensyn til nærstående med tilknytning til fremmede stater, for eksempel ektefeller med statsborgerskap og lignende. Eksperten mener at det i sikkerhetsloven er et hull i denne sammenheng, og viser til sikkerhetsloven § 8-7, og mener at ektefelles statsborgerskap bør veie tyngre i etter loven.

Forbiondelser: Eksperten mener dette er et svært vanskelig område å jobbe med, da det er noe som er vanskelig å detektere og enkelt å skjule. Det er for eksempel ikke noe som detekteres med atferdsendring. Eksperten mener at det er vanskelig å tilføye noe til det som allerede er i modellen, men indikerer at som følge av vanskeligheten med å detektere slikt så bør det tas tak i på et tidlig stadium.

Kapasitet
Eksperten hadde ingen tilføyelser eller rettelser til dette delnettverket.

Mulighet
Eksperten mener at det bør være noe som tar høyde for at enkelte bransjer må tåle å ta større risiko enn andre. Eksperten viser til teknologi-bedrifter, som kan være for eksempel Kongsberg-gruppen, tidvis kan trenge kompetanse som ikke finnes i Norge. Dette kan medføre at disse virksomhetene kan måtte hente inn personell med sårbarheter som tilknytning til andre stater eller annet. Det samme kan også gjøre seg gjeldende når en handler med enkelte aktører, for eksempel fremmede stater.

Jeg spurte eksperten om hva han tenker om å inkludere denne typen vurderinger til noden «Utsatt bransje», noe han var enig i at det kunne være en god måte å operasjonalisere det på.

Individspesifikke forhold: Jeg spurte eksperten i løpet av intervjuet om hva han spesifikt tenker om de individspesifikke forholdene knyttet til muligheten. Eksperten sa at han deler synet om at «noen vil ha mer» og hadde ingen rettelser eller tilføyelser til de punktene som lå til grunn i modellen.

Pågående konflikt: Eksperten sa at han mente det var viktig at forhold som pågående konflikt med gjenspeiles i modellen, da det i flere tilfeller har drevet personer til å handle på en måte som har gjort de til innsidere. Eksperten mener også at det er nødvendig med en risikoindikator som viser at individet har pågående konflikter, slik som samlivsbrudd, sykdom osv.