Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: MSAMAS Master i samfunnssikkerhet	Vårsemesteret, 2021 **Åpen** / ~~Konfidensiell~~
Forfatter: Julie Dahl Jacobsen	..... (signatur forfatter)

Fagansvarlig:
Sissel Haugdal Jore

Veileder(e):
Sissel Haugdal Jore

Tittel på masteroppgaven:
Hvordan holde innsidere på utsiden?

Engelsk tittel:
How do we keep insiders on the outside?

Studiepoeng:
30

Emneord: Innsidere, innsidetrussel, personellsikkerhet, sikkerhetsloven, barrierer	Sidetall: 57 + vedlegg/annet: 71 Stavanger, 14.06.21

Hvordan holde innsidere på utsiden?

Julie Dahl Jacobsen

14.06.21

Masteroppgave i samfunnssikkerhet

UNIVERSITETET I STAVANGER

Forord

Etter to spennende år på masterstudiet i samfunnssikkerhet markerer denne oppgaven nå avslutningen for min tid ved Universitet i Stavanger. Jeg vil takke forelesere og medstudenter for å ha gjort dette til to så gode år.

I forbindelse med denne oppgaven vil jeg først rette jeg en stor takk til min veileder, Sissel Haugdal Jore. Denne oppgaven hadde ikke vært den samme uten dine gode innspill og råd. Den kunnskapen og tiden du har delt har vært uvurderlig.
Det har vært en utfordrende periode som jeg ønsker å takke mine medstudenter, venner, og ikke minst min samboer for å ha gjort mye bedre gjennom god hjelp og støtte. Til slutt vil jeg også gi en stor takk til min mor, Hege, som alltid stiller opp, hva enn det måtte være. Jeg hadde ikke klart meg uten den hjelpen du har gitt!

Julie Dahl Jacobsen
Stavanger, 14.06.21

Sammendrag

Innsidere er en stor trussel for våre kritiske samfunnsfunksjoner og dermed også vår styringsevne og suverenitet. Hva en innsider er, og på hvilken måte dette er en trussel, er ikke tydelig definert, men det omhandler at personer med tilgang til visse verdier bruker denne tilgangen til uautoriserte formål. En sentral verdi i denne sammenheng er sikkerhetsgradert informasjon, som dersom den blir kjent for uvedkommende kan skade nasjonale sikkerhetsinteresser. Innsidetrusselen er svært kompleks, der god forebygging krever stor kompetanse. Det er et mål i arbeidet med samfunnssikkerhet å kunne øke den forskningsbaserte kunnskapen om hvordan denne risikoen kan motvirkes. På bakgrunn av dette er følgende problemstilling studert: *Hva er en innsider og hvilke barrierer og tilhørende funksjoner er viktige for å forebygge innsideaktivitet?*

Denne problemstillingen besvares gjennom å gjøre en kvalitativ innholdsanalyse. De empiriske dataene om innsidere og forebygging av slik aktivitet er studert i fra et teoretisk grunnlag om forskjellen mellom safety og security (sikkerhet og sikring), og barriereretenkning. Dette danner grunnlaget for å kunne vurdere innsidetrusselen, det forebyggende arbeidet og viktige barrierer i et nytt kontekstuelt rammeverk.

Et av de viktigste virkemidlene for å forebygge innsidere er arbeidet med personellsikkerhet, herunder sikkerhetsklarering, autorisasjon og daglig sikkerhetsmessig ledelse. Funnene viser at dette også er de viktigste barrierene. Den første barrieren omhandler klarering og autorisasjon og skal hindre at personer som ikke er regnet som sikkerhetsmessig egnet får tilgang til verdiene, samt at barrieren også skal skape en forståelse og bevissthet om farer. Den andre barrieren er det daglige arbeidet med sikkerhetsmessig ledelse som kan sies så bygge videre på barriere én. Den skal bruke det kunnskapsgrunnlaget fra klarering og autorisasjonen til å avdekke og varsle om mulige farer. Det konkluderes med at selv om disse barrierene, og deres funksjoner, er tiltak som per i dag er implementert, avdekker de empiriske dataene at de ikke er godt nok egnet til å avdekke innsideaktivitet. Personlighetstrekk er en sentral faktor med betydning for hvordan hvert enkelt menneske tenker og handler, og er vist å ha stor betydning i en persons vei til innsideaktivitet. Dette er dog ikke en faktor som er en del av vurderingsgrunnlaget i sikkerhetsklareringen og autorisasjonen, og svekker dermed også arbeidet med daglig sikkerhetsmessig ledelse. Det er derfor en faktor som bør vurderes implementert for å forbedre det forebyggende arbeidet relatert til innsideaktivitet.

Innholdsfortegnelse

Figurer og tabeller

1. Introduksjon

«*Rekruttering eller plassering av spioner på innsiden av norske virksomheter er en kjerneoppgave for utenlandske etterretningstjenester*» (PST, 2020, s. 10).

I samfunnet er det visse funksjoner som er å anse som kritiske da de «dekker samfunnets generelle behov og befolkningens trygghetsfølelse» (NOU 2006:6, s. 32). Noen av de kritiske funksjonene er knyttet til vår styringsevne og suverenitet, og anses som grunnleggende rammebetingelser for ivaretakelse av andre samfunnsfunksjoner. De er dermed særdeles viktige (DSB, 2016, s.32). En av disse funksjonene er «forsvar», som blant annet er «*knyttet til opprettholdelse av norsk selvstendighet og forsvar mot fremmede makters eventuelle interesse av å ta kontroll over norsk territorium eller norske ressurser (…)*» (DSB, 2016, s.38). De ulike kapabilitetene som må opprettholdes i denne funksjonen er overvåking og etterretning, forebyggende sikkerhet og militær respons (DSB, 2016).

En forutsetning for ivaretakelse av styringsevne og suverenitet er evnen til «å overvåke fremmede aktørers aktiviteter på og nær norsk territorium» (DSB, 2016, s. 39). Mange stater og aktører vil forsøke å skaffe seg informasjon om andre, og flere bruker store ressurser på dette. Metodene for innhenting av informasjon er flere, hvor noen eksempler er fysisk og digital kartlegging, avlytting, avlesning av digitale signaler eller rekruttering av personer. Sistnevnte kan gjøres ved at fremmede etterretningstjenester rekrutterer enten egne eller norske borgere som har tilgang til informasjon, for å få denne eller andre typer verdier (NSM, 2020). Den informasjonen som vil være verdifull for andre stater eller aktører å tilegne seg gjennom slike metoder er sikkerhetsgradert informasjon. Det er informasjon som «kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende», og som således vil representere en fare for vår styringsevne og suverenitet (sikkerhetsloven, 2018, §5-3).

De personene som har tilgang til sikkerhetsgradert informasjon, og som videre misbruker dette for å påføre skade og tap kalles innsidere. Hvordan man definerer denne trusselen er dog ikke lik over alt. Felles er likevel at handlingen som utføres, der konsekvensene av å eksfiltrere informasjon med betydning for nasjonal sikkerhet, kan resultere i tap av samfunnets kritiske funksjoner (NSM, 2019b).

I arbeidet med å forebygge, avdekke og motvirke denne type sikkerhetstruende virksomhet er sikkerhetsloven et viktig virkemiddel (Justis- og beredskapsdepartementet, 2020). Loven skal blant annet bidra til å trygge Norges suverenitet, territorielle integritet og demokratiske styreform (sikkerhetsloven, 2018, §1-1). Sikkerhetsloven og tilhørende forskrifter presenterer en rekke tiltak for å forebygge innsidevirksomhet som er relatert til virksomheters arbeid med personellsikkerhet. Personellsikkerhet omhandler «*å forebygge, avdekke og motvirke sikkerhetstruende virksomhet begått av personer som har legitim tilgang til verdiene vi ønsker å beskytte*» (Justis- og beredskapsdepartementet, 2020, s. 77). Tiltakene som anvendes i dette arbeidet kan overordnet deles inn i tre kategorier: sikkerhetsklarering, autorisasjon og sikkerhetsmessig ledelse og kontroll (NSM, u.å. a, s. 5).

Sikkerhetsklareringen og autorisasjonen er virkemiddel som brukes for å hindre at personer som ikke er sikkerhetsmessig skikket får tilgang til sikkerhetsgradert informasjon, eller at personer som allerede er klarert og autorisert misbruker denne tilgangen. Dette gjøres ved at det foretas en vurdering etter sikkerhetslovens (2018) §8-4, bokstav a-o.

Flere offentlige myndigheter i Norge, som blant annet Politiets sikkerhetstjeneste (PST) og Nasjonal Sikkerhetsmyndighet (NSM) har gjennom flere år hatt fokus på innsidetrusselen, og peker på at dette er en stor utfordring i ulike virksomheter (NSM, 2019a; NSM, 2020; PST, 2016; PST, 2018; PST, 2020). Det er hendelser som kan beskrives som en statistisk sjeldenhet, men er samtidig også hendelser der selv ett enkelt tilfelle kan medføre store konsekvenser. Selv om det har vært få offentlig tilgjengelig registrerte tilfeller i Norge, har det vært flere tilfeller i andre land. At det har vært få tilfeller i Norge betyr ikke at innsidere ikke eksisterer også her, og ei heller at dette er en trussel som ikke vil kunne medføre store tap og skader i fremtiden.
Det er dog ikke en trussel som lett kan forebygges og reduseres. Det er en trussel som innebefatter en menneskelig faktor; både i form av at mennesket selv kan utgjøre en trussel, men også at mennesker kan inneha et sårbarhetspotensial som kan utnyttes (NSM, 2011, s. 3). Det er dermed en trussel som kan anses som svært kompleks, og som så krever stor kompetanse for å forhindre (Justis- og beredskapsdepartementet, 2020). Dette er noe av grunnlaget for at ett av målene i arbeidet med samfunnssikkerhet, som presentert i stortingsmelding 5 (2020-2021), var å øke den forskningsbaserte kunnskapen om motvirkning av innsiderisikoen (Justis- og beredskapsdepartementet, 2020, s. 69).

1.1 Problemstilling

Innsideaktivitet representerer en stor risiko og kan være svært skadelig for både den enkelte virksomhet, men også nasjonal sikkerhet. Det kan, som nevnt, betegnes som en statisk sjeldenhet, men er likevel på bakgrunn av de mulige konsekvensene, en trussel som krever mer oppmerksomhet. Det foreligger ikke stort antall offentlige tilgjengelige studier av innsidere i Norge som tar for seg hva en innsider er og hvordan denne trusselen kan forebygges. NSM har tidligere gitt ut rapporter om innsiderisikoen til veiledning for virksomheter, men det er fremdeles ønskelig med økt kunnskap.

For å øke kunnskapen er det viktig å forstå de underliggende årsakene og virkemåtene til innsidere, men også å vurdere tiltak for å hindre skade eller tap på våre sentrale verdier. Oppgavens problemstilling er derfor: *Hva er en innsider og hvilke barrierer og tilhørende funksjoner er viktige for å forebygge innsideaktivitet?*

For å kunne svare på dette spørsmålet er det videre satt opp noen forskningsspørsmål:

1. Hvordan defineres en innsider i litteraturen?
2. Hvorfor blir noen innsidere, og kan disse sies å ha noen fellestrekk?
3. Hvordan forebygges innsideaktivitet i følge veiledere og forskrifter?

Kunnskapen som en så må tilegne seg er først hvordan en innsider kan defineres, og hvordan de ulike definisjonene av en innsider kan ha en innvirkning på hvordan man forebygger og motvirker denne type trussel. Deretter er det viktig å avklare om, og eventuelt hvordan, man kan identifisere aktørene og mulige fremgangsmåter slik at man kan iverksette tiltak som kan hindre eller begrense denne type handlinger. Til slutt vil denne kunnskapen kunne anvendes til å avdekke hvilke barrierer som er viktige i forebyggingen av innsideaktivitet, noe som videre kan brukes i en vurdering av ytelsen av de nåværende barrierene. «Presise og effektive forebyggingstiltak bygger på et godt kunnskapsgrunnlag» (Justis- og beredskapsdepartementet, 2020, s. 30).

1.2 Avgrensninger

En første begrensning relaterer seg til hvilke type innsidere som studeres. Hvem som blir innsider, og hvorfor, er viktig for å kunne implementere tiltak for å forebygge innsidevirksomhet (NSM, 2019c), men ikke alle typer innsidere kan sies å kreve likt forebyggende arbeid. I denne oppgaven vil det derfor være bevisste innsiderne som undersøkes; det vil si personer som har intensjon om å påføre virksomheten skade eller tap (NSM, 2019b). Forebygging for å hindre såkalte ubevisste

innsidere vil kreve en annen tilnærming ettersom dette ofte kommer som følge av manglende sikkerhetsmessig bevissthet og/eller kompetanse hos enkeltpersoner og mangelfull ledelse (NSM, 2019b).

Videre er en ytterlig avgrensning relatert til hvordan innsidere forebygges i dag. Her vil dette begrenses til forebyggingen som gjøres opp mot offentlige virksomheter som er underlagt sikkerhetslovens krav om sikkerhetsklarering og autorisasjon, med de reservasjoner som bestemmelsene oppstiller. Hvilke virksomheter dette omfatter defineres i lovens §1-2 som «statlige, fylkeskommunale og kommunale organer», samt «leverandører av varer eller tjenester i forbindelse med sikkerhetsgradert anskaffelser» (sikkerhetsloven, 2018).

2. Teori og begrepsavklaring

2.1 Safety og security

I engelske språk er det vanlig å skille mellom begrepene «safety» (sikkerhet) og «security» (sikring), der vi i Norge normalt kun vil bruke begrepet sikkerhet. Det er to begreper som i dagligtalen gjerne brukes om hverandre, og som mange anser som synonymer. Denne «likheten» mellom sikkerhet og sikring gjør at flere mener at det muliggjør at teorier, kunnskap og metodologier kan deles mellom de to retningene. Andre ser på en annen side at en slik sammenslåing mellom de to begrepene ikke er fruktbart, og at sikring dermed burde utvikles som et eget forskningsfelt. Det er således heller ikke konsensus omkring definisjonen på sikring (Smith & Brooks, 2013; Blokland & Reiners, 2020; Jore, 2019a, s. 158).

Historisk omhandlet begrepet sikring sikkerheten for individuelle mennesker. Etter andre verdenskrig ble dette endret, slik at det ikke lenger kun var den individuelle sikkerheten begrepet omhandlet. Begrepet fikk da en bredere betydning, i form av at begrepet innebar statens trygghet. Det har videre utviklet seg ytterligere, og det er nå dekkende for flere nivåer i samfunnet, fra individuelt til internasjonalt nivå. Det er i dag dermed et felles ansvar (Jore, 2019a, s. 159). Som et resultat er det også vanskelig å skulle enes om en felles definisjon som dekker alle nivå, i tillegg til å ta høyde for at begrepet kan sies å være betinget av historiske og politiske kontekster (Jore, 2019a, s. 160).

«Sikkerhet kan beskrives som en frihet fra fare eller risiko for skade» (Smith & Brooks, 2013, s. 9), og omhandler hendelser eller farer som kan anses som ulykker. Sikring på den annen side beskrives ofte som beskyttelse mot tilsiktede handlinger. Dette reflekterer et vanlig skille mellom begrepene (Almklov, Antonsen, Størkersen & Roe, 2018; Smith & Brooks, 2013; Jore, 2019a). Således er skillet om hendelsen er tilsiktet eller ikke (Jore, 2019a, s. 160). Jore (2019a; 2020) viser dog at dette ikke nødvendigvis er riktig. Ideen om at de hendelsene som skjer under hva man referer til som sikkerhet ikke innebærer intensjon er en tanke som flere innen sikkerhetsforskningen er i mot. De hendelsene som kategoriseres under sikkerhet skjer ofte som en følge av mangel på planlegging, organisering eller ressurser. Reason (1997, s. 205) beskriver det som at handlinger enten ikke går som ønsket, eller at konsekvensene av disse handlingene ikke er som ønsket, samt at ulykker også kan inntreffe der en ikke følger rutiner for sikkerhet (Jore, 2019a, s. 161). På denne måten vil intensjon være et relevant aspekt i både sikkerhet og sikring.

Skillet kan derimot trekkes når det gjelder hvorledes handlingen er å regne som ondsinnet. Det er i sikringshendelser at aktøren har en ondsinnet intensjon, og selv om det innen sikkerhet vil kunne være intensjon, vil dette ikke kunne karakteriseres som ondsinnet (Jore, 2019a; Smith & Brooks, 2013). Sikring kan derfor defineres som «*den oppfattede eller faktiske evnen til å forberede seg for, tilpasse seg, motstå og komme seg fra farer og kriser forårsaket av mennesker bevisste, forsettlige og ondsinnede handlinger som terrorisme, sabotasje, organisert kriminalitet eller hacking*» (Jore, 2019a, s. 157).

Det som kan vurderes som en viktig årsak til å etablere et skille mellom de to begrepene, er som tidligere nevnt den tilhørende kunnskapen, teoriene og metodologien. Hvordan man differensierer mellom ulike hendelser i de to begrepene, har en videre betydning for forebygging og håndtering. Hendelser kan således vurderes ulikt mellom sikkerhet og sikring når det gjelder hvordan man skal hindre at de skjer (Almklov et al., 2018). Risikoer som kan kategoriseres under sikkerhet er gjerne knyttet til en organisasjons produksjon. Årsakene til disse risikoene er gjerne godt kjent, og man har ofte historiske data som kan brukes for å motvirke hendelsene (Jore, 2019a, s. 163). Hendelsene som er å anse som sikringstrusler er på en annen side ikke like lett å kontrollere, og har oftes ikke en sammenheng med en virksomhets produksjon. Det er heller ikke like mye kunnskap som kan brukes i arbeidet med å motvirke slike hendelser, slik at usikkerheten omkring disse hendelsene er å anse som større.

En ytterligere faktor som må tas hensyn til når det gjelder sikring er den menneskelige faktoren. Men ondsinnet intensjon vil trusselaktøren aktivt kunne unngå de tiltak og barrierer som er satt for å hindre at en uønsket hendelse inntreffer. De vil således bevisst kunne unytte sårbarheter i virksomheten (Smith & Brooks, 2013; Jore, 2019a, s. 164). Til slutt vil sikringshendelser være hendelser som en ikke lett vil kunne oppdage før hendelsen skjer da trusselaktørene vil holde dette skjult. I noen tilfeller, eksempelvis innsideaktivitet eller spionasje, så vil aktøren ikke ønske at hendelsen noen gang oppdages, i motsetning til for eksempel terrorisme. På denne måten vil arbeidet med å avdekke og motvirke sikkerhetstruende hendelser kreve andre metoder enn hva som kreves relatert til sikkerhetshendelser (Jore, 2019a, s. 165). Dette relaterer seg til oppgavens begrensning til innsidere med ondsinnet intensjon og ikke ubevisste innsidere. Innsideaktivitet gjort av ubevisste innsidere trenger nødvendigvis ikke ha en ondsinnet intensjon, men kan være en følge av manglende sikkerhetsbevissthet eller kompetanse. Videre er det heller ikke slik at alle de samme

metodene og tiltakene for å hindre innsidetrusselen er de samme som kan brukes for å hindre andre uønskede hendelser i en virksomhet.

2.2 Forebygging

> Forebygging omfatter alle tekniske, operasjonelle og organisatoriske tiltak som hindrer at en uønsket hendelse skjer eller som hindrer eller redusere konsekvenser om den uønskede hendelsen skjer. Forebygging er dermed planlagte og forberedte tiltak som bidrar til å indre at uønskede hendelser skjer eller utvikler seg. (Njå, Sommer, Rake & Braut, 2020, s. 266).

Innen samfunnssikkerhet er forebygging en av de mest sentrale oppgavene. Selv om forebygging er viktig, er det likevel viktig å være klar over at man ikke vil kunne forhindre alle hendelser. Det er derfor også svært viktig at man også er forberedt på å håndtere de hendelsene som likevel kan skje (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016).
*«Forebygging innebærer å iverksette tiltak for å redusere muligheten for en uønsket hendelse, eller på forhånd redusere konsekvenser av en mulig hendelse» (*Justis- og beredskapsdepartementet, 2020, s. 30). Et viktig aspekt i arbeidet med forebygging er at en er klar over hvordan ulike hendelser inntreffer; dermed at man er klar over årsaks- og virkningssammenhenger. Det er således viktig å ha så mye kunnskap som mulig for å kunne redusere risikoen relatert til ulike hendelser. Slike sammenhenger er likevel ikke alltid like lette å få innsikt i, da vi i dag har høy grad av kompleksitet og mer sammensatte virkningsforhold (Justis- og beredskapsdepartementet, 2020).

En viktig årsak til hvorfor man trenger mye kunnskap om årsaks- og virkningssammenhenger er for å kunne redusere de sårbarhetene i tiltakene som skal hindre uønskede hendelser. Sårbarhet kan defineres på ulike vis. En definisjon er den som er gitt av Njå et al. (2020, s. 52) som definerer sårbarhet som en «*manglende evne hos et analyseobjekt til å motstå virkninger av en uønsket hendelse og til å gjenopprette sin tilstand eller funksjon etter hendelsen»*. Den sier altså noe om hvordan virksomheter klarer å motstå innsidehendelser, men også mulighetene til å gjenopprette sin funksjon. Virksomhetens funksjon er viktig ettersom sårbarhetene har en innvirkning på virksomhetenes funksjonelle krav, eksempelvis å drive forebyggende sikkerhet «*for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser*» (DSB, 2016, s. 41).

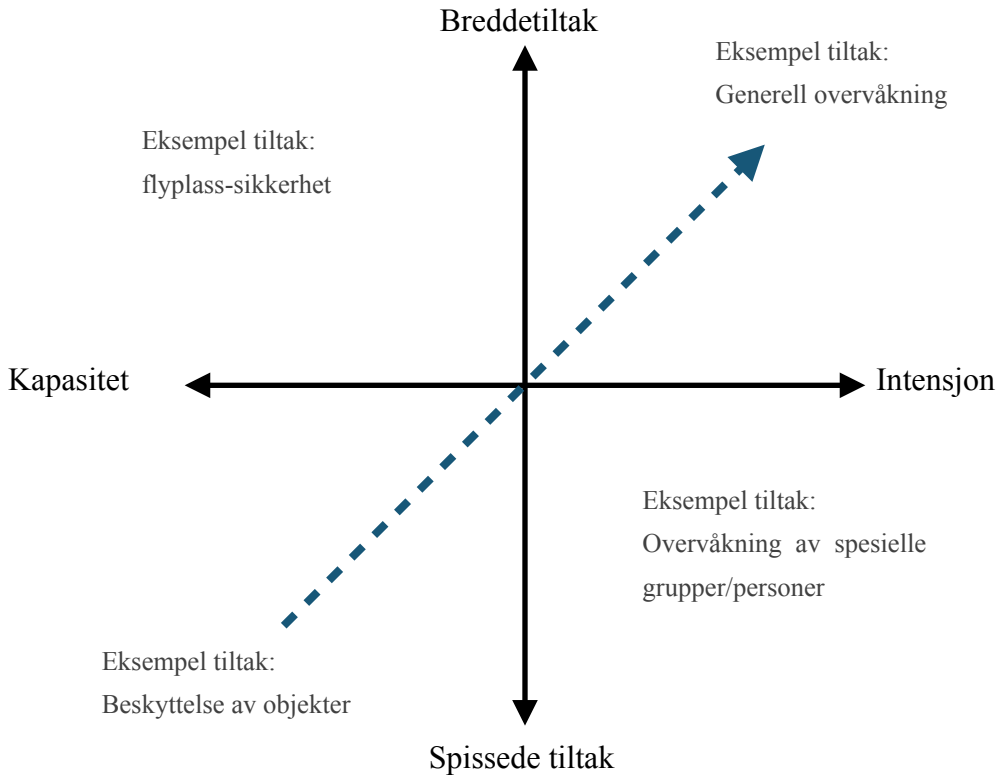
Det å forebygge maktbruk fra fremmede stater og organisasjoner mot Norge er et av forsvarspolitikkens hovedmål (DSB, 2016, s. 39). Forebygging innenfor nasjonalt sikkerhetsarbeid kan gjøres på ulike måter, men det overordnede arbeidet med å øke sikkerheten i samfunnet gjøres gjennom regulering (Forsvarsdepartementet, 2017).

2.2.1 Regulering

Regulering er et bredt begrep som omhandler flere aspekter, men gjerne deles inn i ulike hovedtema. Et av disse temaene er spesifikke ordre eller presise regler. Dette kan være regler og krav som lover eller forskrifter, eksempelvis sikkerhetsloven (Engen et al., 2016, s. 223; Fintland & Braut, 2012). Slike presise regler er en kontrollmekanisme som «skal bidra til å håndtere ulike farekilder og trusler mot infrastruktur og sentrale samfunnsfunksjoner» (Engen et al., 2016, s. 224).

En styringsordning eller rettslig ordning som regulerer et bestemt område omtales gjerne som et reguleringsregime. Her er det ytterligere noen tema som er sentrale. Den første gjelder de trusler og den risikoen som en ønsker å påvirke, redusere eller styre. Dette omhandler således de farer som utgjør en trussel for våre verdier, som infrastruktur, kritiske samfunnsfunksjoner eller liv og helse (Engen et al., 2016, s. 229). Ytterligere vil også offentligheten og interessenter ha en påvirkning på regimet. Det kan være ulike interessenter som på ulike måter påvirkes av risikoen, og som kan ha en påvirkning gjennom ulike forståelser av både risikoen og hvilke interesser som står på spill. Gjennom vårt politiske system vil offentligheten ha mulighet til å påvirke for å sikre et godt grunnlag og legitimitet i både prosessen og beslutninger relatert til regulering (Baldwin, Cave & Lodge, 2012; Engen et al., 2016).

De hendelser som er å regne som sikringshendelser representerer noen særlige utfordringer i tilknytning til lovgivning og myndighetskontroll. Virkemidlene og tiltakene som brukes av myndighetene opp mot ondsinnede handlinger er flere, og kan illustreres gjennom figur 1.



Figur 1: Virkemidler og tiltak mot ondsinnede handlinger (Engen et al., 2016, s. 233; Hammerlin, 2011, s. 148).

De tiltak som vises langs den horisontale aksen sikter på å redusere trusselaktørens intensjon og kapasitet. Den andre, vertikale aksen, viser til enten spissede tiltak eller breddetiltak. Spissede tiltak vil være tiltak som retter seg mot spesifikke aktører, eksempelvis overvåkning av enkeltmennesker eller miljøer med høyere risiko, mens breddetiltak dermed vil være tiltak som retter seg mot den generelle befolkningen. Tiltakene som sikter mot kapasitet eller intensjon kan således også deles inn i breddetiltak eller spissede tiltak (Hammerlin, 2011, s. 148; Engen et al., 2016, s. 233).
Den stiplede linjen peker på en av de særlige utfordringene innen sikring. Den beskrives av Hammerlin (2011, s. 154) som en indikasjon på de demokratiske kostnadene som kan være forbundet med tiltakene. En slik demokratisk kostnad relaterer seg blant annet til individers rettssikkerhet. Myndighetens utforming av lover og regler med tilhørende kontroll må derfor veies opp slike hensyn (Engen et al., 2016, s. 224).

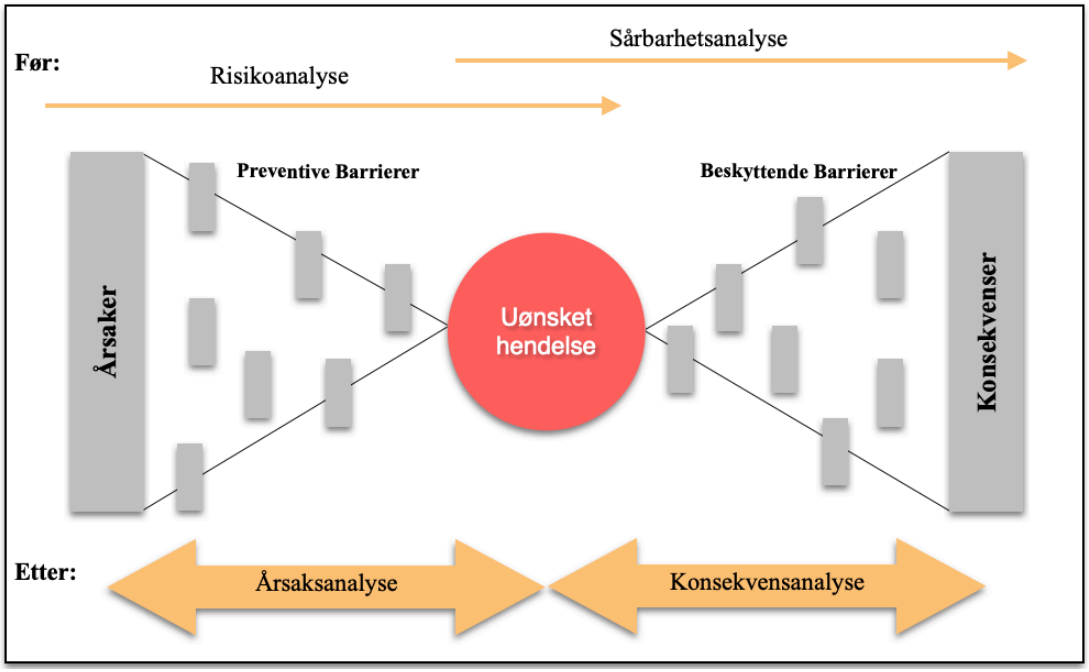
Regulering innebærer således en vurdering av verdier, som for eksempel individets rettssikkerhet og nasjonale sikkerhetsinteresser. Dette kan vurderes til å være overordnede verdier, som beskyttes gjennom konkrete tiltak på virksomhetsnivå (NSM, u.å. b). Eksempler på slike konkrete forebyggende tiltak på virksomhetsnivå er bruk av barrierer.

2.2.2 Barrierer

De ulike tiltakene som skal redusere risiko i en virksomhet omtales gjerne som barrierer. Barrierer kan defineres som «*de systemer eller funksjoner som skal hindre eller begrense videre utvikling av en faresituasjon*» (Njå et al., 2020, s. 262). De er dermed sentrale i arbeidet med å hindre at en hendelse skjer eller får utvikle seg, samt å redusere konsekvensene dersom en hendelse likevel skulle skje (Njå et al., 2020; Busmundrud, Maal, Kiran & Endregard, 2015).

Det kan skilles mellom ulike former for barrierer. Noen barrierer kan kategoriseres som et teknologisk tiltak, i form av fysiske barrierer. De kan for eksempel gi beskyttelse mot ukontrollert overføring av energi eller farlige substanser. Andre barrierer betegnes som organisatoriske eller menneskelige, herunder både formelle (skriftlige) eller uformelle (Schiefloe, 2012, s. 4). Eksempler på formelle barrierer kan være krav til klarering og autorisasjon i virksomheter som er underlagt sikkerhetsloven. Uformelle barrierer beskrives på den annen side å ikke være «vedtatt eller ha formell status» (Schiefloe, 2012, s. 5). Dette kan være å ha fokus på gode holdninger eller viktigheten av sosialt samhold for å hindre uforsvarlig eller mangelfull gjennomføring av oppgaver (Schiefloe, 2012).

En overordnet måte å skille barrierer på er å å skille mellom preventive, også kalt forebyggende barrierer, og beskyttende eller konsekvensreduserende barrierer. Risikobilde for en hendelse, og bruken og funksjonen av barrierene relatert til dette, kan presenteres med en Bow-tie-modell (Lunde, 2018; Schiefloe, 2012). Foruten å illustrere forskjellen mellom prevantive og beskyttende barrierer viser også denne modellen forholdet mellom ulike analyser, både før og etter en uønsket hendelse (Schiefloe, 2012, s.6).

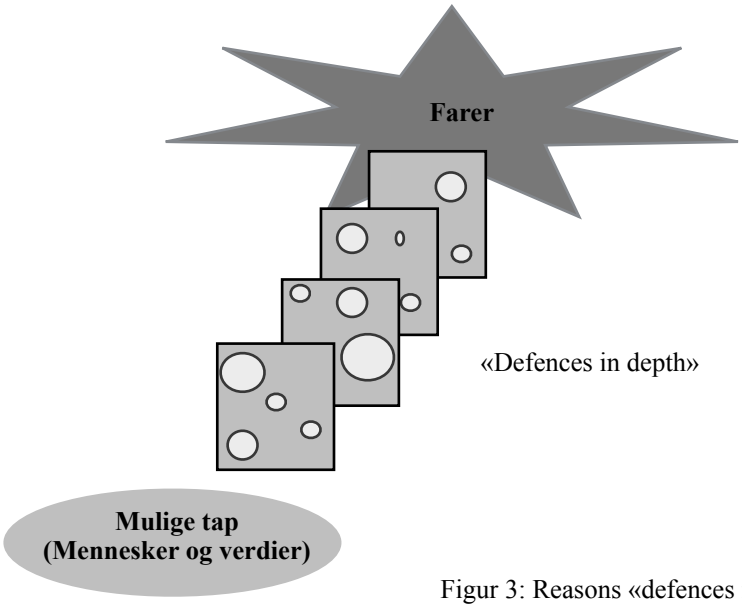


Figur 2: Bow-tie-modell inspirert av Schiefloe (2012, s. 7)

2.2.2.1 Swiss cheese model of defences

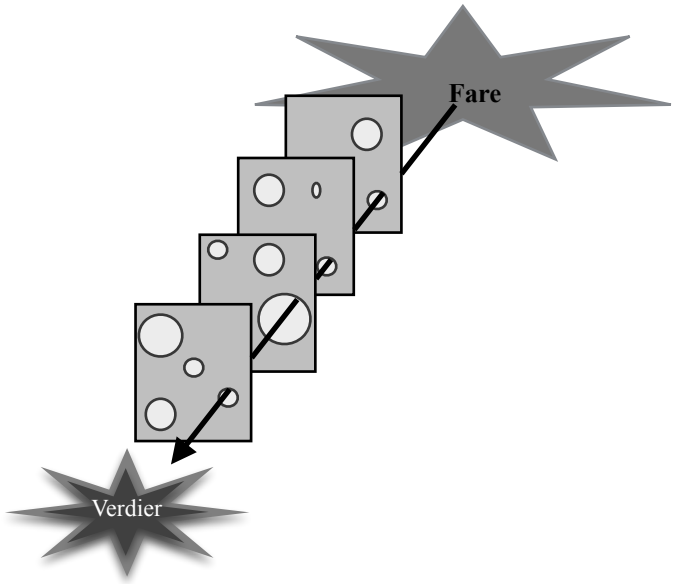
Sentralt i barrieretenkningen er Reasons (1997) «swiss cheese model of defences». Han peker på at barrierer kan skilles enten ut i fra den funksjonen de har eller hvordan disse funksjonene nås. De ulike funksjonene kan være at de skal skape en forståelse eller bevissthet om farer, at de skal gi veiledning til hvordan man skal handle, at de skal varsle farer, at de skal gjenopprette systemet, at de skal sikre verdiene fra farer, eller sørge for at man kan unnslippe faren dersom den ikke kan begrenses. Alle barrierer har i følge Reason minst én av disse funksjonene (Reason, 1997, s. 7).

Videre bygger teorien på at barrierene med disse funksjonene ligger etter hverandre. Dette betyr at dersom den førstnevnte barrieren, som skal skape forståelse og bevissthet, ikke hindrer en fare, vil den neste barrieren prøve å beskytte verdiene. Dette er det han kaller «defences-in-depth» (Reason, 1997, s. 7).



Figur 3: Reasons «defences in depth» (Reason, 1997).

Risikoen relatert til slike barrierer er dersom de alle svikter. Sentralt i teorien er at hver barriere i realiteten vil ha hull som illustrerer sårbarheter. Hvor mange, eller hvor store disse er, kan variere, da modellen ikke er statisk slik som den er illustrert over. Det er en konstant bevegelse i både barrierer og sårbarhetene i dem (Reason, 1997). Dette betyr at selv om det er hull i en barriere, så vil ikke dette nødvendigvis innbære at ulykke vil skje. Skulle det dog være hull i alle barrierer, og at alle disse hullene er like relatert til plassering i barrierene, så vil en ulykke kunne inntreffe. Faren visualiseres, som vist i figur 4, som en pil som kan gå gjennom alle barrierenes hull dersom de alle ligger på linje (Reason, 1997).



Figur 4: Resons (1997) «Swiss cheese» modell

Utfordringen er således hullene i barrierene, men årsaken til at disse hullene oppstår kan være flere. Reason (1997) skiller mellom det han kaller aktive feil og latente forhold. Aktive feil viser til menneskelige feil som gjøres av de som sitter i «førstelinjen». Selv om dette er feil som gjerne gjøres av én person eller noen få mennesker, peker Reason på at det likevel ikke er deres feil alene. Det har derimot en sammenheng med virksomhetens virkemåte eller kultur. Hendelsene «sees mer på som konsekvenser enn årsaker» (Reason, 1997, s. 10).

Siden det, som tidligere nevnt, ikke er mulig å forutse alle mulige fremtidige hendelser vil det derfor gjerne være noen sårbarheter i barrierene fra begynnelsen av som en ikke kan avdekke. Det kan videre også hende at disse hullene eller sårbarhetene utvikler seg over tid, men at det ikke fanges opp (Reason, 1997, s. 12). Disse omtaler Reason som latente forhold; forhold som er skjult og som enda ikke har kommet frem. Det kan være for eksempel feil eller mangler når det gjelder design, tilsyn, prosedyrer, opplæring/trening o.l., og har ofte en sammenheng med avgjørelser som er tatt på høyere nivåer enten i virksomheten eller hos myndighetene. De kan dermed være tilstede over lang tid før de manifesterer seg. Dette skjer som oftest i forbindelse med endringer i lokale forhold eller i sammenheng med aktive feil (Reason, 1997, s. 10).

3. Metode

Metode relaterer seg til hva vi ønsker kunnskap om, og kan generelt beskrives som de systematiske og planmessige fremgangsmåtene for å nå et bestemt mål (Grønmo, 2016). Valg av metode har betydning for hvordan man velger, samler inn, organiserer og analyserer data, og «utgjør retningslinjer for hvordan pålitelig kunnskap og holdbare teorier om samfunnet kan bygges opp» (Blaikie & Priest, 2019; Grønmo, 2016, s. 42).

Ulike typer informasjon eller data kan studeres gjennom ulike metoder, men for å kunne utvikle interessant kunnskap, må vi basere oss på hensiktsmessige metoder (Grønmo, 2016, s. 15). Det er i denne oppgaven et mål å kunne øke kunnskapen om innsidere og hvordan innsideaktivitet kan forebygges. Det er således ønskelig å få en økt forståelse av konkrete personer og sosiale prosesser; av fenomenets egenskaper eller spesielle kjennetegn. Kvalitative metoder er utviklet for å belyse dette gjennom at det muliggjør en dypere forståelse av fenomenet, og det er derfor også denne metoden som her er valgt (Brinkmann & Tanggaard, 2010; Madsbu, 2011; Johannessen, Tufte & Christoffersen, 2010).

3.1 Forskningsstrategi

For å kunne trekke konklusjoner eller argumentere for spørsmålene som oppgaven skal besvare kan en bruke ulike strategier. En skiller mellom induktiv, deduktiv, abduktiv og retroduktiv strategi, som alle kan sies å være ulike måter å gå fra en ting til en annen (Danermark, Ekström, Jakobsen & Karlsson, 2002, s. 79).

I denne oppgaven skal spørsmålene besvares gjennom å ta i bruk en abduktiv forskningsstrategi. Danermark et al. (2002, s. 80) beskriver den grunnleggende strukturen i denne strategien som det å «tolke og forstå noe på en ny måte i et nytt konseptuelt rammeverk». Det er ikke en empirisk generalisering som ved induksjon, heller ei en strengt formell logikk slik som ved deduksjon, men en kan sies å være en rekontekstualisering (Danermark et al., 2002, s. 90). Studie av et fenomen brukes her sammen med teori for å kunne gi en ny tolkning av det gitte fenomenet (Dey, 2004). Det er en forskningsstrategi der man søker en dypere forståelse av et fenomen, da ved å se det i en ny kontekst. «Vi ser på koblinger og relasjoner, som ikke er direkte observerbare, som vi kan bruke til å forstå et allerede kjent fenomen på en ny måte» (Danermark et al., 2002, s. 91). I denne oppgaven

vil så innsidere og innsideaktivitet studeres gjennom andre «briller» for å få en dypere forståelse av hva dette fenomenet innebærer relatert til forebygging.

Et viktig aspekt ved abduksjon, noe som skiller det fra eksempelvis deduksjon, er at en abduktiv strategi ikke innebærer en logisk slutning. «Det gir en mulig tolkning av noe, heller enn en logisk slutning» (Dey, 2004, s. 91). En kan ikke si at den slutningen som trekkes ved bruk av denne strategien vil være sann eller ikke, konklusjonen er derimot en av mange mulige konklusjoner (Dey, 2004). Konklusjonene som trekkes omkring innsidere og forebygging av innsideaktivitet gjennom en abduktiv strategi vil derfor «vise hvordan det *kanskje* er» (Danermark et al., 2002, s. 91).

3.2 Informasjonsskilder

Det er flere måter å samle informasjon om innsidere, deres karakteristikker, og hvilke barrierer som er sentrale i forebygging av innsideaktivitet. Grønmo (2016, s. 134) skiller mellom tre hovedtyper informasjonskilder: aktører, respondenter og dokumenter. Valget av hvilke kilder en skal bruke vil være avhengig av den informasjonen man ønsker samle inn, hvilke kilder som kan bidra med denne informasjonen og hvilke kilder som er tilgjengelige (Grønmo, 2016, s. 133).

Hovedfokuset i denne oppgaven er å få en bedre forståelse av innsidere som fenomen, hvorfor noen blir innsidere, og til slutt kun si noe om forebygging av innsideaktivitet. Gitt dette grunnlaget er det ansett som fruktbart å anvende dokumenter som informasjonskilde. Den informasjonen som trengs for å besvare problemstillingen krever en dybdeforståelse av innsidere. Det vil videre også kreve en forståelse av deres handlinger, samt hvordan virksomheter kan forebygge disse.

Valget av informasjonskilde grunner i hvilke kilder som er tilgjengelige og som som kan bidra med denne informasjonen. Selv om andre metoder for innsamling som for eksempel intervju ville kunne gitt enda dypere forståelse og ikke minst relevante aktørers egne perspektiver, vil avstanden til mulige studieobjekt ikke gjøre at andre metoder ville vært like hensiktsmessige. Som kilder vil dokumenter derimot kunne gi informasjon om forhold over langt større avstander i både tid og rom (Grønmo, 2016, s. 135). Til slutt er informasjonen som er nødvendig for å besvare oppgavens problemstilling gjerne gradert, og andre metoder for innsamling ville ikke hatt en påvirkning på denne tilgjengeligheten.

Innsamlingen er utført ved å ta i bruk ulike søkemotorer på nett. Fordelen med å gjennomføre en analyse på denne måten er tilgjengeligheten av data, da det meste av informasjon tilgjengelig på ulike sider og databaser (Asdal & Reinertsen, 2020). En utfordring omkring nettsøk er blant annet at søkemotorer er algoritmestyrt. Søkeresultatene kan påvirkes av ens tidligere søk, lokasjon, antall

treff på siden og betalt plassering. «*Et nettsøk er aldri en nøytral kilde til informasjon*» (Asdal & Reinertsen, 2020, s. 207).

3.3 Innholdsanalyse

En kvalitativ innholdsanalyse velges da det er valgt å gjøre en kvalitativ analyse med dokumenter som informasjonskilde. Analysen innebærer at innholdet i dokumenter gjennomgås systematisk for å finne den informasjonen som er relevant for studien. De relevante delene blir så «bearbeidet, systematisert og registrert på en slik måte at de kan brukes som datagrunnlag». Innsamlingen og analysen, samt utvelgelsen av data foregår dels parallelt (Grønmo, 2016, s. 175). I forbindelse med innholdsanalysen er det visse aspekter som må på plass. Dette er først at en må avklare tema som skal prioriteres under innsamlingen, så hvilke tekster som skal velges ut og til slutt «hva en skal se etter i den systematiske gjennomgangen av innholdet i tekstene» (Grønmo, 2016, s. 176).

Temaet i innsamlingen bygger på oppgavens problemstilling og er dermed også retningsgivende for hvilke enheter som skal inngå (Grønmo, 2016). Informasjon som var nødvendig for å besvare problemstillingen kan deles inn i to hovedtema. Det første kan overordnet si å være informasjon om innsidere og det andre fokusområdet kan sies å gjelde forebygging av innsideaktivitet i dag. Dette kan så studeres i en ny kontekst for å vurdere viktige barrierer.
Alle dokumenter med informasjon om innsidere og dokumenter med informasjon om forebygging av innsideaktivitet kan ikke studeres. Det måtte derfor gjøres et utvalg av enheter som skal inngå i studien og som skal brukes til å danne et kunnskapsgrunnlag (Blaikie & Priest, 2019, s. 167).

Utvalget er gjennomført ved strategisk utvalg. Denne måten å velge ut tekster baserer seg på «systematiske vurderinger av hvilke enheter som ut fra teoretiske og analytiske formål er mest relevante og mest interessante» (Grønmo, 2016, s. 103). Utvelgingen er således basert på denne vurderingen med sikte på teoretisk generalisering, der formålet er å kunne utvikle begreper ut fra et teoretisk resonnement og å kunne utvikle helhetlig forståelse fra utvalget (Grønmo, 2016). I sammenheng med det strategiske utvalget er det også anvendt det som gjerne kalles snøballmetoden. Det vil si at den informasjonen man samler inn brukes for å finne annen data som kan være relevant, eksempelvis gjennom kildehenvisninger (Johannessen et al., 2010; Asdal & Reinertsen, 2020). Selv om dette kan være en fruktbar metode for å avdekke relevant data, er det

likevel viktig å være klar over at dette kan medføre en ensformighet i det empiriske materialet. Kildekritiske vurderinger er dermed desto viktigere.

3.3.1 Trustworthiness

For å beskrive det som gjere kalles interne- og eksterne validitet, reliabilitet og objektivitet vil det her tas utgangspunkt i det naturalistiske rammeverket gitt av Lincoln og Guba (1985). I stedet for å anvende de begrepene som nevnes over, som er vanlige innen et mer konvensjonelt perspektiv, vil oppgavens funn vurderes basert på «sannhetsverdi», «overførbarhet», «konsistens» og «nøytralitet». Disse vil kunne si noe om troverdigheten relatert til oppgavens funn basert på de underliggende kriteriene om «kredibilitet, overførbarhet, pålitelighet og bekreftbarhet» (Lincoln og Guba, 1985). Disse begrepene velges grunnet at de er å anse som mer passende gitt oppgavens forskningsmetode enn de mer konvensjonelle begrepene fra det Lincoln & Guba (1985) refererer til som realismen.

Det første punktet Lincoln & Guba (1985) presenterer er sannhetsverdi. Dette vil innen realismen innebære å finne et kausalt forhold mellom variablene en studerer, da det å finne isomorphisme (et en-til-en forhold) i praksis er umulig. Dersom en kan etablere at det er et kausalt forhold betyr dog ikke at funnene er sanne og bevist, men at de kan falsifiseres. Dersom de ikke kan falsifiseres kan de for øyeblikket regnes som en «sannhet». For naturalister på den annen side, vil isomorphismen likevel være den ønskelige metode. Sannhetsverdi, eller «truth value», relaterer seg til forholdet mellom funnene og virkeligheten, der det i stedet for å vurdere den interne validiteten er ønskelig å bevise at rekontekstualiseringen som gjøres er troverdig. Dette gjøres gjennom å studere fenomener på en slik måte at en øker sannsynligheten for at funnene blir ansett som troverdige, og å demonstrere kredibiliteten.

Å demonstrere kredibiliteten kan gjøres på flere måter. I denne oppgaven er dette gjort blant annet ved triangulering, der ulike data som brukes sees opp mot hverandre. Kredibiliteten vil i følge Lincoln og Guba (1985, s.305) øke dersom ulike kilder presenterer de samme funnene, eksempelvis at flere kilder finner de samme fellestrekkene hos ulike innsidere. Rekontekstualiseringen kan dermed sees knyttet til virkeligheten da den baserer seg på kredible empiriske grunnlag. Videre kan økt kredibilitet også nås dersom en søker etter data som ikke understøtter eksisterende funn. Dette er det Lincoln og Guba (1985, s. 309) refererer til som «negativ case analysis». Dette vil kunne øke kredibiliteten ved at man underveis driver en form for falsifisering. Således vil de påstander som ikke kan sies å basere seg på kredible kilder og som ikke understøttes i andre empiriske data, ikke uttrykkes som godt empirisk grunnlag. Kredibiliteten kan ytterligere sikres gjennom «peer

debriefing», der man sammen med andre kan foreta en vurdering og utforske aspekter ved forskningen (Lincoln & Guba, 1985). Dette er i denne oppgaven gjort i gjennom diskusjoner med veileder underveis i arbeidet.

Det andre punktet om overførbarhet («applicability»), handler om «hvordan man kan avgjøre om funnene i oppgaven er anvendelige i andre kontekster eller andre respondenter» (Lincoln & Guba, 1985, s. 290). Her relaterer det seg til en overførbarhet av det empiriske materialet, noe som er avhengig av likheter mellom de to kontekstene. Lincoln & Guba (1985) skriver dog at dette ikke er noe som kan sikres av forskeren som kun tar for seg den ene konteksten; overførbarheten må kunne vises av den som skal bruke funnene i en annen kontekst. Forskeren som gjør en studie kan ikke vite på hvilken måte noen vil kunne ønske å overføre materialet, og er dermed kun ansvarlig for å gi en «tykk beskrivelse» (Nowell, Norris, White & Moules, 2017, s. 3). Dette kan overordnet si å være «alt en leser kan trenge å vite for å forstå funnene» (Lincoln & Guba, 1985, s. 125).
Det første som så må vurderes opp mot denne oppgaven er hvorvidt det empiriske dataene som denne oppgaven bygger på kan sies å være overførbart til Norge. En stor del av empirien som anvendes i denne oppgaven er fra andre land; mye fra USA. Årsakene til dette ligger i manglende empiriske data fra Norge på slike hendelser, og det er da viktig å være klar over, og ikke utelukke, kulturspesifikke variasjoner. Likevel vil de grunnleggende aktørkarakteristikkene og modellene som hentes fra empirien vurderes som å være overførbare og anvendelige i en denne konteksten. Også kriteriene for vurdering av sikkerhetsmessig skikkethet er grunnleggende like i begge kontekstene, da kun med små variasjoner.
For å sikre at funnene i denne oppgaven vil kunne være overførbare til andre kontekster eller respondenter er det i så stor grad som mulig gitt tykke beskrivelser av modeller og rammeverk som presenteres.

Det tredje punktet, «consistency» eller «konsistens», baserer seg på kriteriet pålitelighet. Lincoln og Guba (1985, s. 316) beskriver at "uten kredibilitet vil man ikke kunne ha pålitelighet, slik at det å kunne demonstrere det første vil kunne være tilstrekkelig for å etablere det sistnevnte». De presiserer dog også at dette likevel ikke er tilstrekkelig nok, slik at en en annen metode anbefales. Denne andre metoden er det de kaller «inquiry audit» eller hendelsesrevisjon. Dette innebærer at prosessen undersøkes, og at funnene undersøkes. Prosessen skal være «logisk, sporbar og tydelig dokumentert» (Nowell et al., 2017, s. 3).

Det siste kriteriet er «confirmability» («bekreftbarhet») og skal sikre nøytralitet. Dette går ut på at det er et forhold mellom data og realitet, at det er anvendt en passende metodologi, eller at undersøkelsen er verdi-fri. Det handler om sammenhengen mellom dataene eller funnene; om de er troverdige, faktabaserte, og mulige å bekrefte (Lincoln & Guba, 1985, s. 300). Det avhenger av at man kan vise hvordan tolkninger og konklusjoner er nådd gitt de empiriske data (Nowell et al., 2017).

3.3.2 Utvalg av tekster

Som nevnt vil informasjonen som trengs kunne deles inn i to hovedtema. Omfanget av studier på det første temaet, innsidere, var ikke svært utstrakt sett opp mot mengde eller geografisk område. På grunn av at antallet innsidere er registrert over et lengre tidsperspektiv ble det ikke ansett som fruktbart å søke etter studier på enkelte innsidere. Dette ble det heller ikke funnet stort materiale på. Studier av enkeltpersoner som tidligere har drevet med innsideaktivitet er ikke nødvendigvis heller like fruktbart hvis man ønsker å øke den forskningsbaserte kunnskapen om innsidere og deres handlingsmåter. Dette ville ha krevd et stort antall utvalg av innsidere som skulle studeres, i tillegg til at det ville ha krevd et visst antall studier på hver innsider.

Det som ble funnet av studier opp mot dette første temaet var større studier gjort på et større antall innsidere; noen innenfor spesifikke tidsrom. Disse tekstene ble valgt ut for å sikre et datamateriale med omfattende kunnskapsgrunnlag og som inkluderte flere variabler på innsidere.

Studier av innsidere preges ytterligere av å i stor grad å være utført av ulike myndigheters departementer. Dette kan forklares delvis med tilgjengeligheten av informasjon. Innsideaktivitet i offentlige virksomheter kan i flere tilfeller vurderes gradert, og vil derfor ikke ligge offentlig tilgjengelig. Informasjon om innsidere har derfor blitt samlet i myndigheters databaser som videre benyttes for å gjennomføre studier.

Eksempel på noen slike studier, der innsidere studere ut fra spesifikke tidsrom og fra egne databaser, er de rapportene som er gjort av «The Defense Personnel and Security Research Center» (PERSEREC). Sentralt er 4 ugraderte rapporter som baserer seg på data fra deres egen database. Dette er data omhandlende blant annet spionasje og lovbrudd som forsøk på spionasje, konspirasjon om spionasje og «tyveri eller ulovlig innsamling av tett holdt nasjonal forsvarsinformasjon med den hensikt å begå spionasje» (Herbig, 2017, s. v). I denne oppgaven har kun den siste rapporten blitt tatt i bruk (Herbig, 2017). Alle de fire rapportene bygger på data fra

samme database, men etterhvert som mer informasjon og data om innsidere blir tilgjengelig, har de laget en ny rapport for å ta høyde for de nyere innsidesakene. Den nyeste rapporter er derfor å anse som en oppdatert versjon av de tidligere studiene på foregående tidsperioder.
I nyere tid har PERSEREC også utvidet prosjektene sine til å gjelde alle offentlig kjente hendelser som involverte ressurseksfiltrering. Dette har resultert i en rapport som også er å anse som en sentral rapport i denne oppgaven (Jaros, Rhyner, McGrath & Gregory, 2019).

Det var ønskelig med et utvalg som representerte hendelser i flere geografiske områder, men dette var noe om skulle vise seg å ikke være så utbredt. Dette har gjerne en sammenheng med at informasjonen om innsidere i hovedsak ligger hos spesifikke departementer hvis hovedmål er på å beskytte offentlige virksomheters verdier. Da ønskes det gjerne ikke at alle slike hendelser, med detaljerte beskrivelser av innsidernes virkemåter skal bli offentlig kjent. Det er heller ikke alle områder er funnet til å ha like stort antall av innsidehendelser basert på den informasjonen som er offentlig tilgjengelig. En oversikt over litteraturen om innsidere som er sentrale for denne oppgaven er gjengitt i tabell 1 under.

Forfatter(e)	År	Tittel	Dokumenttype
Baweja, J.A., Burchett, D. & Jaros, S.L.	2019	An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks	Rapport
Centre for the Protection of National Infrastructure (CPNI)	2013	CPNI Innsider Data Collection Study: report of main findings	Rapport
Charney, D.L. & Irvin, J.A.	2016	The Psychology of Espionage	Artikkel
CIA	2014	Psychology of Treason	Artikkel
Herbig, K.L.	2017	The Expanding Spectrum of Espionage by Americans 1947-2015	Rapport
Jaros, S. L., Rhyner, K.J., McGrath, S. M. & Gregory, E.R.	2019	The Resource Exfiltration Project: Findings from DoD cases, 1985-2017	Rapport
Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. & Osula, A-M.	2015	Insider Threat Detection Study	Rapport
Nasjonal Sikkerhetsmyndighet (NSM)	2019	Temarapport Innsiderisiko	Rapport
Nurse, J.R.C., Legg, P., Buckely, O. & Wright, G.R.T.	2014	Understanding Insider Threat: A framework for characterising Attacks.	Konferanseinnlegg/ artikkel
Shechter, O.G. & Lang, E.L.	2011	Identifying Personality Disorders that are Security Risks: Field Test Results	Rapport
Wilder	2017	The Psychology of Espionage	Artikkel

Tabell 1: Oversikt over litteratur omhandlende innsidere

Datainnsamlingen relatert til det andre hovedtemaet, hvordan innsideaktivitet forebygges i dag, baserer seg på noen andre dokumenter. Dette er data som i flere tilfeller vil kunne være gradert, ettersom det vil kunne omhandle virksomheters metoder. De vil dermed kunne beskrive hvordan innsidere har kunnet forbigå barrierer tidligere, og det finnes dermed ikke så stort datagrunnlag av ugraderte studier og beskrivelser av nettopp dette.
Noen av metodene for å forebygge og avdekke innsidere, eksempelvis prosessen med klarering og autorisasjon er dog nedfelt i loven, og det er dermed data tilgjengelig for analyse. Videre har også Nasjonal Sikkerhetsmyndighet gitt ut rapporter og veiledere som skal bistå blant annet klareringsmyndigheter i prosessen med klarering, og disse vil dermed også kunne bidra til å belyse hvordan innsideaktivitet forebygges. En oversikt over de mest sentrale dokumentene relatert til dette er vist under i tabell 2.

Flere av rapportene som nevnt i tabell 1 vil være viktige også opp mot forebyggingen, eksempelvis i form av kunnskapsgrunnlaget det gir om innsidere, men vil ikke nødvendigvis alene si noe om hvordan forebygging gjøres i de relevante virksomheter i dag. Det er derfor noen dokumenter som kan sies å være dekkende for begge hovedtemaene i oppgaven, mer er plassert i tabellene etter hovedinnholdet.
For å avdekke hvilke barrierer som er sentrale i forebyggingen av innsidere vil informasjonen basere seg på dokumentene for å avdekke innsidernes handlingsmønstre, men vil også basere seg på hvordan innsidere forebygges i norsk sammenheng.

Et viktig punkt relatert til dokumentene om forebygging er at en ny sikkerhetslov trådte i kraft i 2019 (Forsvarsdepartementet, 2017). Som et resultat av dette har NSM oppdatert tilhørende veiledere, men denne prosessen er enda ikke fullført. Noen veiledere er derfor eldre enn nåværende sikkerhetslov, eksempelvis veilederen for autorisasjon og autorisasjonssamtale. NSM presiserer at håndboken likevel fremdeles er i bruk, da selve autorisasjonsprosessen fremdeles er lik (NSM, 2011).

Forfatter(e)	År	Tittel	Dokumenttype
Det Norske Veritas GL	2019	Håndtering av innsiderisiko	Rapport
Forsvarsdepartementet	2017	Lov om nasjonal sikkerhet (sikkerhetsloven).	Proposisjon til Stortinget (Prop. 153 L)
Justis- og beredskapsdepartementet	2020	Samfunnssikkerhet i en usikker verden	Stortingsmelding (5 2020-2021)
Klareringsforskriften	2018	Forskrift om sikkerhetsklarering og annen klarering	Forskrift
Nasjonal sikkerhetsmyndighet (NSM)	u.å. a	Veileder i personellsikkerhet	Veileder
Nasjonal sikkerhetsmyndighet (NSM)	u.å. b	Veileder i sikkerhetsstyring	Veileder
Nasjonal sikkerhetsmyndighet (NSM)	2011	Håndbok i autorisasjon og autorisasjonssamtale	Veileder
Office of the Director og National Intelligence (DNI)	2017	Security Executive Agent Directive 4: National Security Adjudicative guidelines	Direktiv
PST, NSM, Politiet & Næringslivets sikkerhetsråd (NSR)	2017	Sikkerhet ved ansettelsesforhold - før, under og ved avvikling.	Rapport
Sikkerhetsloven	2018	Lov om nasjonal sikkerhet (sikkerhetsloven).	Lov

Tabell 2: Oversikt over litteratur relatert til forebygging

3.3.3 Kategorisering

Under innsamlingen er det viktig å foreta en kategorisering av det relevante innholdet (Grønmo, 2016, s. 179). Som nevnt vil innsamling og analyse kunne foregå parallelt, slik at man under innsamling kan registere relevante punkter i ulike kategorier. Kategorier som inndelingen skal foregå etter kan gjerne være bestemt før innsamlingen starter. Det ble i denne oppgaven satt opp kategorier etter forskningsspørsmålene som var ønskelig å besvare, da eksempelvis ulike definisjoner og forståelsesmåter av begrepet innsider. En annen forhåndsbestemt kategori var om det ble registrert noen fellestrekk ved innsidere. I innsamlingen og analysen ble det videre dannet underkategorier underveis, som baserte seg på funnene. Dette var for eksempel funn som relaterte seg til varighet på innsideaktivitet, kjønn eller ulike personlighetstrekk. De kategorier som til slutt ikke ble funnet til å kunne understøttes gjennom triangulering ble så ikke tatt med som et fellestrekk, men ble likevel registrert som et funn av mulig fremtidig relevans. Flere av dokumentene var omfattende i omfang, og omhandlet dermed faktorer omkring innsidere eller

forebygging som ikke var å anse som relevant for oppgaven, slik at innsamlingsprosessen og analysen av relevant informasjon krevde omfattende databehandling. Eksempler på ulike kategorier som ikke ble ansett som relevant for oppgaven var blant annet sivilstatus, antall barn, høyeste utdanning og statsborgerskap (Jaros et al., 2019).

De ulike utdrag ble merket med referanse og beskrivelser av kontekstuelle forhold. Oversikten ble systematisert tematisk, med underkategorier som eksempelvis geografisk område for å kunne ta høyde for mulige kulturspesifikke variasjoner (Grønmo, 2016). Den samme metoden om tematisk systematisering ble brukt i oversikten over hvordan forebyggingen foregikk i dag. Dette muliggjorde at de ulike aspektene ved innsidere så kunne sammenlignes med det forebyggende arbeidet, noe som dermed kunne brukes i en vurdering av barrierenes ytelser. Noe av den samme oversikten eller oppsettet over hvordan informasjonen ble systematisert er også anvendt i oppgavens empirikapittel.

3.4 Etiske vurderinger og personvern

Samfunnsvitenskapelig virksomhet reguleres av ulike forskningsetiske normer, hvor noen av disse er nedfelt i formelle regelverk. Dette gjelder blant annet innsamling av personopplysninger. At dataene en forsker samler inn og bruker håndteres på en korrekt måte er svært viktig sett opp mot god forskningsetikk. Dette gjelder spesielt der det foregår innsamling og lagring av informasjon om enkeltpersoner. Slik innsamling av personopplysninger er strengt regulert, og krever derfor gjerne godkjennelse fra Norsk Senter for Forskningsdata (NSD) (Grønmo, 2016). Med personopplysninger menes «enhver opplysning om en identifisert eller identifiserbar enkeltperson» (Asdal & Reinertsen, 2020, s. 213). Det ble i sammenheng med denne oppgaven foretatt en vurdering fra NSD relatert til om prosjektet kan anses å være meldepliktig. Selv om innsamling av personopplysninger er regulert, er det likevel slik at en ren innholdsanalyse som kun tar i bruk offentlig tilgjengelige dokumenter ikke anses som meldepliktig av NSD (Asdal & Reinertsen, 2020).

3.5 Metodiske utfordringer

En første utfordring relatert til det metodiske i denne oppgaven omhandler innsamling av kvalitative data gjennom en innholdsanalyse. Når det gjelder en slik analyse er det ofte store mengder data som gjerne er ustrukturerte (Johannessen et al., 2010, s. 163). Dataene inneholder også mye informasjon

og er tidkrevende både å lese og analysere. Prosessen med utvelging av empiriske data er dermed svært krevende, både opp mot at alle relevante faktorer må tas høyde for, samtidig som at man må kunne være restriktiv nok til å utelukke data som ikke er relevant for oppgavens problemstilling.

En annen utfordring medfølger av oppgavens tema og problemstilling, og relaterer seg til at informasjon og data kan være gradert og således ikke tilgjengelig. Dette gjelder spesielt omkring barrierer og forebygging av innsideaktivitet. At det er begrenset mengde informasjon som er tilgjengelig for offentligheten grunner i at virksomheter ønsker å beskytte kilder og metoder (Charney & Irvin, 2016). Dette er selvfølgelig et positivt aspekt, da det kan anses som en barriere for å hindre at mennesker uten tilgang til virksomheten mulig kan få tilgang til verdiene, men det representerer en utfordring opp mot oppgavens problemstilling og siktemål.

Videre er det en utfordring med denne type analyse at forskeren selv vil påvirke både utvalg og tolkning av dokumentene. Dersom forskerens perspektiv er for snevert kan dette på en side begrenset tolkningsmulighetene, noe som også kan resultere i at ikke alle relevante tekster tas med i utvalget. Utvalget kan således bli skjevt (Grønmo, 2016). Relatert til tolkningen er det slik at ved en abduktiv strategi så vil konklusjonen sies å være en av flere, da det nettopp er en tolkning. Det er likevel viktig å være klar over at man kan ha for snevert perspektiv, slik at alle interessante eller viktige dokumenter vurderes. Samtidig kan man også underveis i utvalg og analyse studere de tekster som i første omgang ikke virker som de mest relevante for å vurdere nye applikasjonsmuligheter.

4. Empiri

"*Innsiderisikoen virksomheten utsettes for er kompleks og bygger på en rekke ulike faktorer*» (NSM, 2019b, s.9).

Kapittelet vil presentere funnene av innholdsanalysen, og vil overordnet følge den retningen som er gitt i oppgavens problemstilling og forskningsspørsmål. Dette kan som tidligere nevnt deles inn i to hovedkategorier. Først vil de empiriske funnene omkring innsidere presenteres, noe som også krever en avklaring av hva en innsider er. De empiriske funnene om innsidere; deres handlinger og motiver, vil så presenteres. Det andre hovedpunktet omhandler hvordan slik aktivitet forebygges i dag. Her vil gangen for gjennomføring av autorisasjon og sikkerhetsklarering først gjøres rede for, før det rettslige grunnlaget med betydning for problemstillingen beskrives.

4.1 Innsidere

NSMs beskrivelse av innsiderisikoen som presentert først i dette kapittelet peker på at det er ulike faktorer ved innsidere som gjør at det er å anse som et komplekst problem. En av de første utfordringene som trekkes frem i flere av dokumentene er hvordan en innsider defineres. Det finnes flere definisjoner og betydninger av begrepet innsider, men de ulike forståelsene kan i hovedsak deles inn i to hovedperspektiver. Den første forståelsen vises i blant annet Baweja, Burchett, & Jaros (2019) og Nurse, Legg, Buckley & Wright (2014), som ser en innsider som «individer som har autorisert tilgang til en organisasjons informasjon, fasiliteter, nettverk, ressurser og mennesker» (Baweja et al., 2019, s. 10). Dersom en person med slik tilgang så gjør noe som kan skade organisasjonen, vil de være å anse som en innsidetrussel. De setter dermed et skille mellom en innsider og en innsidetrussel.

Denne forståelsen deles også av NATOs Cooperative Cyber Defence Centre of Excellence (CCDCOE), men de skiller videre mellom ytterligere tre kategorier. Dette er tre kategorier som alle sier noe om på hvilket grunnlag en er å regne som en innsider, uten at man nødvendigvis utgjør en trussel. De tre kategoriene er at en innsider kan være en som har eller er gitt: *spesifikk kunnskap*, *tilgang* og *tillit*. Det som er felles for alle disse tre kategoriene er at også aktører som ikke er tilknyttet virksomheten kan bli en innsider, så lenge de har én eller flere av de overnevnte tre kategoriene (Kont, Pihelgas, Wojtkowiak, Trinberg & Osula, 2015, s. 12).

I norsk sammenheng er forståelsen av begrepet innsider noe annerledes. NSM (2019b, s. 9) definerer en innsider 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*». Kunnskapen kan brukes «til fordel for annen virksomhet, stat, eller til egen vinning». En innsider er dermed et begrep som først brukes etter at en person har gjort handlinger som påfører virksomheten skade eller tap. Denne forståelsen finner vi også hos Englands «Centre for the Protection of National Infrastructure" (CPNI) som definerer innsidere som «en person som utnytter, eller har intensjonen om å utnytte, deres legitime tilgang til en organisasjons verdier for uautorisert formål» (CPNI, 2013, s. 6). Således er fellestrekket mellom de to forståelsene at en innsider har tilgang til visse verdier, men de skiller på begrepets bruk basert om personen har begått en ondsinnet handling eller ikke.

Der definisjonen skaper et skille i hvordan en innsider defineres, er andre aspekter som det enes om som videre kan utdype forståelsen av hva en innsider er. Et første overordnet skille, som tidligere er presentert, er skillet mellom ubevisste og bevisste innsidere. En bevisst innsider er beskrevet som en person med intensjon om å påføre skade og tap. Der den ubevisste innsideren kun har kapasitet og mulighet til å påføre skade, har den bevisste innsideren i tillegg intensjon. Bevisste innsidere er således klar over at handlingene går i mot virksomhetens interesser (NSM, 2019b).
I kategorien bevisste innsidere kan man ytterligere skille mellom tre typer: i) infiltratører, ii) de som rekrutters og iii) de selvmotiverte. Infiltratører er innsidere som kan være plassert i en organisasjon av andre, for eksempel en annen stat. Den andre kategorien, de som rekrutteres, er en betegnelse som brukes om de som får betaling eller som på noen måte blir presset eller truet. Til slutt vil den siste kategorien være de innsidere som utfører innsideaktivitet på eget initiativ (DNVGL, 2019).

Foruten å skille mellom type innsidere skiller noen også mellom innsidere ut i fra ulike «modus operandi». Det kan være flere ulike inndelinger, men vanlig er den som presenteres i CPNI (2013, s. 4). De har identifisert fem ulike typer av innsideaktivitet: uautorisert utlevering av informasjon, korrupsjon av prosesser, tilrettelegge for at en tredjepart får tilgang til en organisasjons verdier, fysisk sabotasje og elektronisk/IT sabotasje. Uautorisert utlevering viser til at man utleverer gradert informasjon enten til en tredjepart eller til media. Prosess-korrupsjon innebærer at man «på ulovlig vis enten endrer en intern prosess eller et system i virksomheten for å oppnå et spesifikt, ikke autorisert mål» (CPNI, 2013, s. 4). Til slutt kan det å tilrettelegge for at en tredjepart får tilgang til

verdier i virksomheten gjøres gjennom at man gir noen fysisk tilgang til en lokasjon, eller tilgang til informasjon og personer.

Noe av kompleksiteten som innsiderisikoen presenterer kommer som en følge av de ulike kategoriene og deres ulike handlingsmetoder. Dette krever følgelig ulike metoder for å kunne forebygge og detektere slik aktivitet (NSM, 2019b). Hvilke tiltak som kreves for å forebygge en ubevisst innsider er en annen enn hva som vil kreves for å forebygge bevisste innsidere. En person som har tilgang til tilgang til verdiene og kunnskap om hvilke barrierer og tiltak virksomheten har, og som i tillegg har en ondsinnet intensjon, vil kunne omgå de tiltakene som er satt for å hindre innsideaktivitet. De kan således bevisst unngå barrierene som er satt for å hindre dem (NSM, 2019b; Jore, 2019b; Kont et al., 2015).

4.2 En persons vei til innsideaktivitet

Hvordan noen får, eller hvorfor noen har, en motivasjon til å utføre handlinger som de bevisst vet vil skade virksomheten, vil være forskjellig fra person til person. Det er i litteraturen avdekket en rekke faktorer som kan ha betydning for om en person kan bli innsider eller ikke.

For å kunne forbedre arbeidet med forebygging og deteksjon av innsidere er det tidligere forsøkt å lage en profil på hva som er den typiske innsideren. Dette for å kunne ha et grunnlag i vurderingen om personer er sikkerhetsmessig skikket. Ser man på de mer generelle fellestrekkene til innsidere er det noen få ting som kan trekkes ut. Et første punkt er at en innsider er en mann mellom 31 og 45 år, der gjennomsnittsalderen er er 35 år (NSM, 2019c; Jaros, Rhyner, McGrath, & Gregory, 2019, s. 14). Det har vært eksempler på kvinnelige innsidere, men de er likevel i fåtall sett opp mot gjennomsnittet. De faller dermed også utenfor de generelle fellestrekkene som blir trukket frem. Den gjennomsnittlige innsider har videre vært ansatt i en virksomhet i mellom 3 og 5 år før de blir innsidere, og er gjerne selvmotiverte (NSM, 2019c). CPNI (2013) fant i deres studie at hele 76% av innsiderne de studerte var selvmotiverte.

Disse karakteristikkene viser til hvem den gjennomsnittlige innsider har vært, men vil ikke være fruktbare å anvende i det forebyggende arbeidet da de ikke er særlig begrensende. Det å lage en profil på innsidere har således vist seg å ikke være helt mulig, da én enkelt typologi ikke kan dekke kompleksiteten i hver enkelt innsider (CIA, 2014; NSM, 2019c; Wilder, 2017, s. 21).

Det videre også vanlig å vurdere mulige innsidere basert på hva som er motivene. Når man snakker om innsidere, så vel som andre individer som utfører ulovlige handlinger, vil det for mange være naturlig å se på hvorfor de utførte disse handlingene. Flere har tidligere sett på innsidere for å avdekke nettopp hvorfor noen vil gå i mot nasjonale sikkerhetsinteresser, og funnet at de mest vanlige inndelingene av motiver for innsidere er penger, ideologi, kompromiss/tvang og ego. Selv om dette er en antagelse som brukes i flere virksomheter, er det dog funnet at disse kategoriseringene ikke nødvendigvis er basert på forskning, men konvensjonell kunnskap (Charney & Irvin, 2016, s. 72). Ved en gjennomgang av empirisk data finner man derimot noen ytterligere motiver basert på studier av innsidere. Her fant de at i tillegg til penger, ideologi og tvang, så er også lojalitet, misnøye, hevn, ønske om å behage, spenning og anerkjennelse viktige motiver (Jaros et al., 2019; CPNI, 2013; NSM, 2019b; Charney & Irvin, 2016; Wilder, 2017; Herbig, 2017; CIA, 2014; Nurse et al., 2014). Det er således en rekke motiver som kan være årsak til at person blir en innsider.

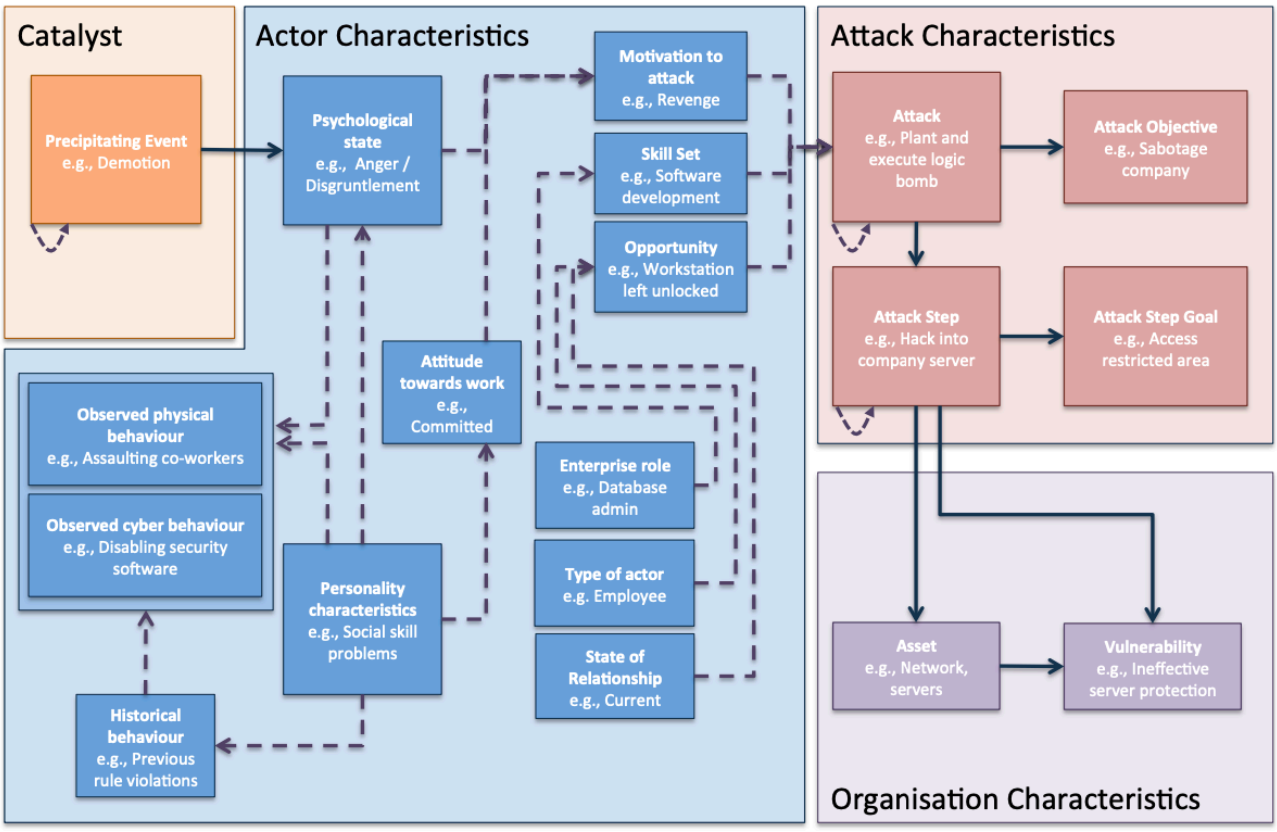
Det som er viktig å være klar over når det kommer til innsidernes motiver er at de er preget av høy kompleksitet. Det er sjeldent slik at innsidere har kun én årsak til hvorfor de startet med, eller var involvert i, innsideaktivitet. Årsakene er ofte mer sammensatte, og det er ikke vanlig å kun ha én enkelt motiverende faktor. I flere undersøkte eksempler finner man at innsideren har ett motiv som kan regnes som «hovedmotiv», men at årsakene til hvorfor de startet med innsideaktivitetene er flere og mer sammensatte (CPNI, 2013).

Et interessant funn relatert til viktigheten av den eller de motiverende faktorene en innsider har, er at CPNI (2013) fant at en sammenheng mellom hva som var den motiverende faktoren og hvilke regelbrudd som ble gjennomført. Eksempelvis ble det funnet at de som hadde ideologiske motiver eller de som hadde et ønske om anerkjennelse, i de fleste tilfeller drev innsideaktivitet gjennom at de avslørte sensitiv informasjon. I 83% av tilfellene der noen begikk prosess-korrupsjon var derimot penger den sentrale motiverende faktoren (CPNI, 2013, s. 7).

Motivene er selvfølgelig et viktig punkt i forståelsen av innsidere, men det er dog ikke bare motivet i seg selv som er viktig. Ut over motivene er også årsakene til hvorfor en person har nettopp disse motivene viktig å studere; et motiv utvikles fra en viss bakgrunn. Dette er i litteraturen avdekket å omhandle «hvem innsideren er», samt hvordan dette kommer til syne. Derfor er det, selv om det

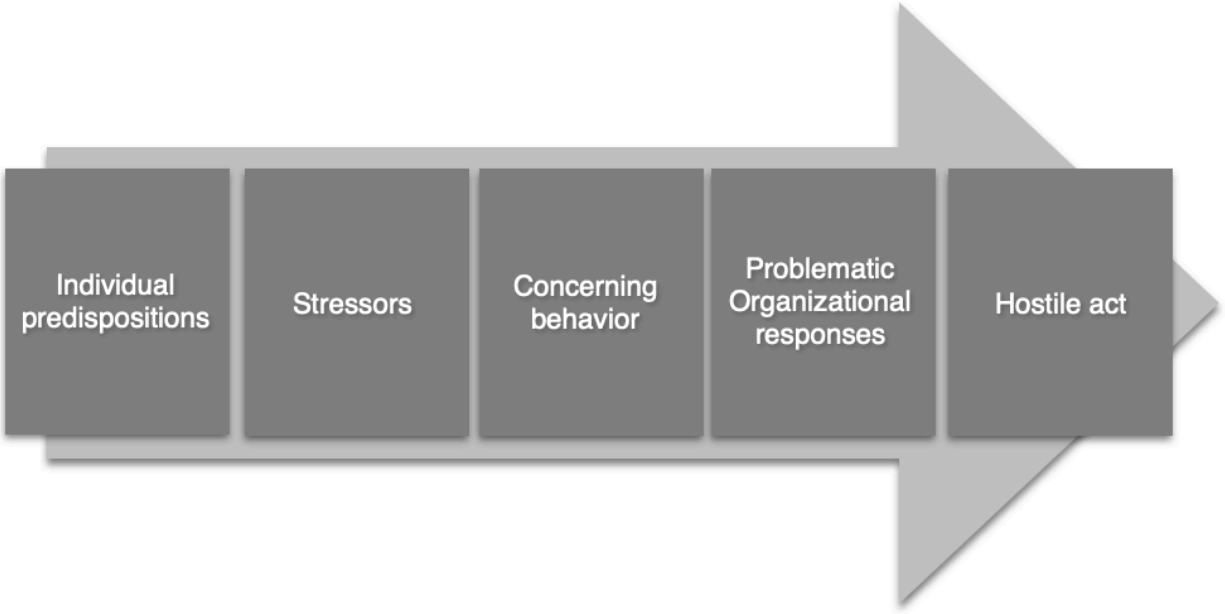
ikke er mulig å lage en profil som passer alle, mulig å trekke frem noen andre fellestrekk blant tidligere innsidere som ikke angår kjønn, alder, eller hvor lenge de har vært ansatt.

For å kunne beskrive, forstå og karakterisere hvem og hvorfor noen mennesker blir innsidere vil Nurse et al. (2014) sitt rammeverk brukes som et utgangspunkt. Ettersom dette rammeverket har et bredere perspektiv enn denne oppgaven omhandler, vil kun de relevante punktene i rammeverket videre beskrives.



Figur 5: «Rammeverk for å karakterisere innsideangrep» (Nurse et al., 2014., s. 3).

Rammeverket fra Nurse et al. (2014) peker på 4 hovedkategorier som er av betydning: en katalysator, karakteristikker ved en person, karakteristikker ved angrepet og organisatoriske karakteristikker. Figuren fungerer som en visuell fremstilling der sammenhenger mellom faktorer uttrykkes, dog uten uten å nødvendigvis presentere en kronologisk fremstilling i de ulike kategoriene. For å illustrere en noe mer kronologisk fremstilling av en persons vei til innsideaktivitet vil en illustrasjon fra Baweja et al. (2014, s. 10) være mer fruktbar å anvende. Denne figuren innehar de samme hovedaspektene som rammeverket til Nurse et al. (2014), men presenterer en mer oversiktlig fremstilling.



Figur 6: «The Critical Pathway Model» (CPM) (Baweja et al., 2019, s. 10).

4.2.1 Personlighetstrekk

En av de tingene som er funnet å være fellestrekk hos innsidere er relatert til det som kan kalles individuelle faktorer eller trekk ved den enkeltes personlighet (Baweja et al., 2019; Charney & Irvin, 2016; CIA, 2014; CPNI, 2013; Nurse et al., 2014; Shechter & Lang, 2011; Wilder, 2017). Personlighet kan defineres som «et sett av psykologiske trekk og mekanismer ved et individ som er organisert og relativt varige, og som påvirker en persons samhandling med, og tilpasninger til, omgivelsene» (Larsen & Buss, 2010, s. 4). Personligheten er således et sett av psykologiske trekk, og disse beskriver de gjennomsnittlige tendensene til en person (Larsen & Buss, 2010).

I det empiriske grunnlaget er innsidere funnet til å ha trekk som kan være av betydning i vurderingen om en person er sikkerhetsmessig skikket til å ha tilgang til eller kunnskap om sikkerhetsgradert informasjon. Personligheten og sammensetningen av personlighetstrekk hos innsidere har overordnet vist et ønske om spenning, et forhøyet selvbilde, at de anser seg selv til å ha høyere rett på visse goder, og et ønske om makt og kontroll. Videre er det også funnet at disse trekkene gjerne også innebærer at enkelte andre personlighetstrekk, som er å anse som ønskelige, hos innsidere er svake eller totalt fraværende (Wilder, 2017, s. 20).

Det er vanlig å snakke om at disse personene viser typiske trekk relatert til narsissisme, antisosial personlighetsforstyrrelse/psykopati eller sosiopati (CIA, 2014; CPNI, 2013; Wilder, 2017; Nurse et al., 2014; Shechter & Lang, 2011; Baweja et al., 2019). Det presiseres at dette ikke betyr at

personene har disse diagnosene, selv om dette også er mulig. Begrepene brukes for å beskrive karakteristikker eller trekk ved disse personene, som ofte er de samme trekke som finnes hos de med disse diagnosene (CIA, 2014).

De trekkene som er funnet hos innsidere er et ekstremt selv-fokus, en patologisk selv-absorpsjon, der denne opptattheten av seg selv går på bekostning av alt annet. Personer med disse trekkene har en følelse av berettigelse og anser seg selv til å være spesiell, og overdriver gjerne også egne prestasjoner. De utnytter de rundt seg, og har derfor også dårlige forhold med andre mennesker, men er ofte ikke klar over deres egen adferd (Larsen & Buss, 2010, s. 319; CIA, 2014, s. 9).

Dette er alle trekk som er sentrale hos en narsissist. En utfordring i denne sammenheng er det man referer til som det narsissistiske paradoks; der selv om personen virker å ha høy selvtillit, så er det derimot helt motsatt. De krever ros og anerkjennelse fra andre, og tar ikke godt i mot kritikk. De tar seg selv selvhøytidelig, og er svært sårbare når det gjelder noe som kan såre selvtilliten (Larsen & Buss, 2010, s. 319; CIA, 2014, s. 9; Shechter & Lang, 2011; Wilder, 2017). Når en person innehar slike narsissistiske trekk føler de seg i mange tilfeller som et offer i relasjoner med andre mennesker der det har foregått overtredelser, mye oftere enn de som ikke har narsissistiske trekk (Larsen & Buss, 2010, s. 488; CIA, 2014, s. 9).

Andre fellestrekk er relatert til det som omtales som psykopati. Dette er en rekke personlighetstrekk som ofte innebærer "uansvarlighet og upålitelighet, egosentrisk atferd, impulsivitet, en manglende evne til å danne varige relasjoner, overfladisk sosial sjarm, og en mangel på sosiale følelser som skam, kjærlighet, skyld og empati» (Larsen & Buss, 2010, s. 255).

Videre er det også funnet trekk som er vanlige indikatorer på sosiopati eller «machiavellisme». Dette er mennesker som i likhet med psykopatien har problemer med samvittighet og moral. De har ikke problemer med å «krenke andres rettigheter for å tjene sine egne behov» (CIA, 2014, s. 9; Shechter & Lang, 2011; Wilder, 2017).

Til slutt er også umodenhet et trekk som er funnet hos flere innsidere. Et av karakteristikkene dette innebærer er vanskeligheter med å skille fantasi og realitet. Personer med trekkene som nevnes her og i avsnittene over kan alle sies å ha aktive fantasier, men umodne personer bruker gjerne mye tid på å dagdrømme. I motsetning til andre har også umodne voksne større problemer med å skille fantasi og realitet. Dette kan medføre at de forventer realiteten å samsvare med fantasiene om seg selv og hvordan andre relaterer seg til dem. Videre vil dette kunne føre til at de føler en misnøye og

hat mot den virkelige verden, skulle den ikke måle seg opp mot fantasiene deres (Wilder, 2017, s. 27).

De ulike trekkene som er vanlig i de overnevnte diagnosene er således alle trekk som i en eller annen sammensetning er funnet hos flere tidligere innsidere (CPNI, 2013; CIA, 2014, Wilder, 2017, Charney & Irvin, 2016; Shechter & Lang, 2011; Baweja et al., 2019). Nurse et al. (2014) beskriver videre at en person som innehar flere trekk fra de ulike diagnose i teorien kan ansees som en større risiko enn de som ikke gjør det. Det som likevel er svært viktig å presisere er at selv om en person har noen slike trekk, betyr ikke dette at de har en av diagnosene, ei heller at de kommer til å bli innsidere.

4.2.2 Utløsende hendelser

Det er mer enn visse personlighetstrekk eller et motiv som skal til for at noen skal bli innsidere. Den tidligere gjennomgangen av mulige motiver viser at de alle i en viss grad kan sies å være personlige. Dette har en sammenheng med at motivet for innsidehandlinger gjerne stammer fra en opplevelse innsideren har hatt, der han eller hun ser at endringer må til, på bakgrunn av holdningene eller verdiene de har (CIA, 2014; NSM, 2019b). Motivene for handlingene er viktige, men for å kunne forklare hvorfor noen blir innsidere må en også kunne se hvilke opplevelser individet har hatt som kan sies å ha utløst behovet for et motiv; hva som gjorde at de så behovet for starte med innsideaktivitet.

Denne andre faktoren er eksterne faktorer, eller det som Baweja et al. (2019, s. 10) referer til som «stressors». Personlighetstrekk kan ikke alene medføre at en går i mot nasjonale sikkerhetsinteresser (Wilder, 2017; CIA, 2014; Nurse et al., 2014). Det som er viktig i utviklingen til en innsider er utløsende faktorer eller utløsende hendelser.

Eksempler på slike utløsende hendelser kan være å bli sagt opp, uenigheter med arbeidsgivere, eller familieproblemer som skilsmisse, og helseproblemer. Dette er hendelser i personens liv som for dem vil oppleves som en krise. En viktig faktor er her formuleringen av at de for dem kan oppleves som en krise. Det som en person med slike trekk oppfatter som en krise, trenger ikke å være de samme hendelser som personer uten disse karakteristikkene vil vurdere som en krise. Personer med visse personlighetstrekk vil kunne oppleve urettferdighet der andre ikke vil det. De kan oppleve en situasjon der de selv føler at en urett er gjort dem, der andre personer i samme situasjon ikke vil

kjenne det slik. En viktig karakteristikk hos personer med blant annet et forhøyet selvbilde er at de ikke anser negative hendelser, eller tilhørende følelser, som noe som kommer fra dem selv, men heller noe som er påført dem utenfra (CIA, 2014). En slik opplevd urettferdighet for den enkelte personen kan derfor også anses som en utløsende hendelse.

Ut i fra de hendelsene som personen opplever, de eksterne faktorene, vil det da også medfølge en følelsesmessig respons eller psykologisk tilstand. Dette kan enkelt forklares som ulike følelser som glad, lei seg, deprimert, sint o.l. (CIA, 2014; Nurse et al., 2014). Hvorfor disse psykologiske tilstandene er viktige forklares gjennom sitatet: «*no one ever defected because he was happy*» (CIA, 2014, s. 1).
Et eksempel er en tidligere innsider som selv beskrev de følelsene han hadde før han valgte å selge sikkerhetsgradert data. Han skal, etter å ha blitt ansatt i CIA, vært svært misfornøyd med stillingen han fikk fordi han selv mente at en person med hans evner fortjente mer. Etter hans arrest skal han så ha forklart at «i *was pissed off in the fact that all my expectations on what the job would be like were falling short and I guess I was perhaps bitter about the situation (...)»* (Wilder, 2017, s. 31). En annen tidligere innsider skal under rettssaken fortalt at hans hovedårsak for å selge gradert informasjon til Sovjet Unionen og Russland, var at han «ga etter for et urimelig sinne» (Thomas, 1997; Masters, 1997).

De utløsende hendelsene og den medfølgende psykologiske tilstanden, eller de følelsene er person får etter en opplevd hendelse, har derfor også mye å si for at en person starter med innsideaktivitet (Nurse et al., 2014). Innsideaktivitet kan sees som en «respons på en overveldende livskrise eller en akkumulering av kriser eller skuffelser» (CIA, 2014, s. 2).

4.2.2.1 Individuell psykologi og omstendigheter i livet

Hva som vil kunne fungere som en utløsende faktor påvirkes av andre omstendigheter i livet, men akkurat hva dette vil si vil variere basert på enkeltindividet. Noen har gjerne hatt en oppvekst i visse geografiske omstendigheter, der de har en lojalitet til en familie eller gruppe, men ikke noe større. Dette kan eksemplifiseres med at man har en kulturell heller enn en nasjonal lojalitet. Andre har gjerne ingen slike tilknytninger, og kan dermed ha lett for å «skifte eller dele lojalitet». Til slutt kan en også ha vokst opp under det som er ansett som mer «vanlige» omstendigheter, men kan med trekk som umodenhet ha «uløste problemer». Dette kan så eksempelvis medføre et ønske om å gå i mot sine foreldre, som så i voksen alder kan erstattes med deres arbeidsgiver (CIA, 2014, s. 6-7).

Slike ulike utgangspunkt vil kunne ha stor påvirkning på hvilke hendelser en person vil anse som utløsende hendelser. En person som har sterkere kulturell lojalitet enn nasjonal lojalitet vil for eksempel kunne oppleve en større effekt av hendelser som påvirker deres kultur enn deres nasjon. Dette vil videre også ha en påvirkning hvilken psykologisk tilstand ulike hendelser vil kunne gi.

Individuelle faktorer eller den individuelle psykologien er således til dels bestemmende i å lage omstendighetene (CIA, 2014). Det som viser seg hos personer som har de personlighetstrekkene som nevnt over er at de i større grad påvirkes av de negative hendelsene eller omstendighetene de opplever. Med dette menes at en hendelse som for eksempel vil oppleves som urettferdig for de aller fleste, vil kunne ha en enda større påvirkning på den psykologiske tilstanden hos personer med disse personlighetstrekkene. Ytterligere vil disse trekkene også medføre at slike personer i gjennomsnitt har et høyere antall slike «personlige kriser». Dette kommer som en følge av at de trekkene som personen innehar gjør at de har dårligere mellommenneskelig kommunikasjon, og at de kan ha større reaksjoner på hendelser enn andre. Å ha slike trekk «svekker moralsk resonnement, dømmekraft og kontroll over impulsiv atferd» (Wilder, 2017, s. 33). Disse trekkene vil så forsterkes når en står i en situasjon en selv opplever som en krise.

Individuell psykologi og en persons omstendigheter i livet vil ikke kunne forklares uavhengig av hverandre. CIA (2014, s. 3) har beskrevet innsideaktivitet som «reaksjoner på endringer i livet som spiller på en allerede eksisterende karakterstruktur». Det er satt opp en forenklet ligning for å forklare denne sammenhengen: I x C = D. «I» står for «individual psychology», og peker mot den personligheten og medfølgende trekkene en person innehar. «C» står for «circumstances of life», dvs. de hendelsene eller krisene som kan ha en innvirkning på om en person starter med innsideaktivitet. Til slutt står «D» for handlingene som defineres som innsideaktivitet. Ligningen peker dermed mot at en kombinasjon av psykologi og omstendigheter fører til innsideaktivitet. Det som er viktig i denne sammenhengen er at jo større hendelsen eller krisen oppleves for personen, jo færre «avvik» kreves i den individuelle psykologien for at en person starter med innsideaktivitet, og motsatt (CIA, 2014). Dette er gjeldende for alle personer da ulike livshendelser vil påvirke de aller fleste. Det er likevel slik at siden disse personene opplever en større påvirkning og effekt av disse hendelsene, samt at de også i gjennomsnitt opplever flere slike hendelser, så kan det peke på at de således har en større sannsynlighet for å bli innsidere (CIA, 2014; Wilder, 2017). «Sårbarheter på et område skaper sårbarheter i et annet» (Wilder, 2017, s. 20).

4.2.3 Atferd

De ulike trekkene og den påvirkningen ulike hendelser har på personen vil få konsekvenser i form av deres atferd, og atferden kan derfor sies å være koblet til eller influert av personligheten (Nurse et al., 2014; CIA, 2014). Dette gjelder både det Nurse et al. (2014) i rammeverket kaller observert atferd og historisk atferd. Det er likevel også her viktig å presisere at selv om en person har den atferden som det vises til her, så betyr ikke dette at en person vil bli en innsider.

Den observerte atferden er hvordan en person oppfører seg enten sammen med kolleger, eller hvilken atferd de har relatert til deres tilgang til virksomhetens verdier eller ressurser. Bekymringsfull atferd mot kolleger kan være alt fra truende eller aggressiv atferd, mens bekymringsfull atferd relatert til virksomheten kan være å uttrykke negative holdninger eller bryte regler og normer (Nurse et al., 2014, s. 6).

Et stort antall tidligere innsidere har blitt vist å hatt slike tegn på bekymringsfull atferd. Kont et al. (2015, s. 10) viser til én innsider som aktivt hadde deltatt i protester mot handlinger virksomheten drev med, mens en annen hadde flere konfrontasjoner med sine ledere. Videre hadde en tredje innsider flere ganger uttrykt radikale overbevisninger. Dette er atferd som kolleger eller ledere kan observere underveis og som således kan være en indikasjon på mulig innsideaktivitet.

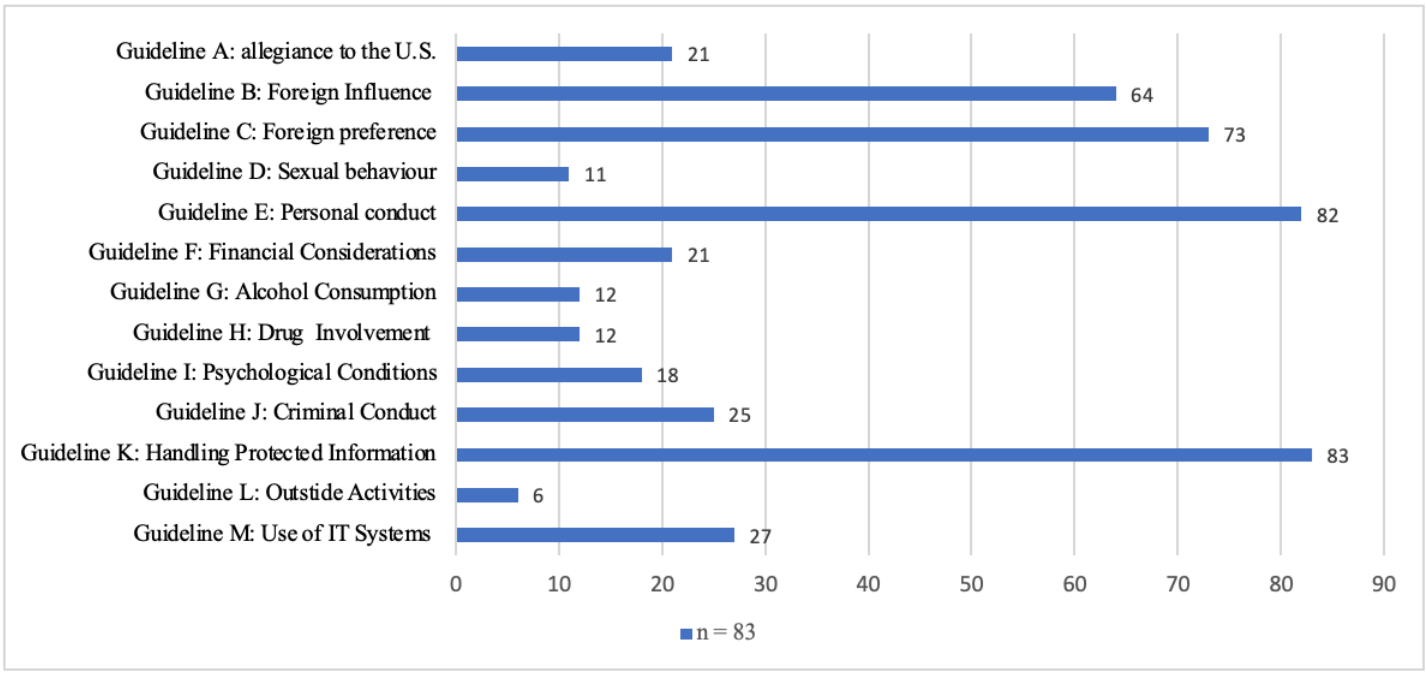
En annen type atferd som også er relevant er det som i rammeverket til Nurse et al. (2014) er referert til som «historisk atferd». Dette viser til atferd som personen har vist tidligere, da gjerne før ansettelse i en virksomhet.

PERSERECs rapport omhandlende ressurseksfiltering fra 1985-2017 tar for seg tidligere innsidere og den atferden som innsiderne hadde før de ble arrestert (Jaros et al., 2019). Her tas det utgangspunkt i 13 «adjudicative guidelines»; det som i norsk sammenheng vil kunne sies å være ekvivalent til de 15 forhold som nevnes i sikkerhetslovens §8-4, bokstav a-o. Dette er de forhold som legges til grunn i vurderingen av hvorledes en person er skikket til å kunne få tilgang til klassifisert informasjon (DNI, 2017; sikkerhetsloven, 2018; Jaros et al., 2019). Ytterligere i de 13 retningslinjene er det også 75 underliggende diskvalifiserende faktorer, dvs. faktorer som peker mot brudd på de ulike retningslinjene (Jaros et al., 2019). Alle retningslinjene og tilhørende diskvalifiserende faktorer er presentert i sin helhet i vedlegg 2.

Jaros et al. (2019) fant at de ti mest vanlige diskvalifiserende faktorene var i 4 av de 13 adjudikative retningslinjene. Dette var i retningslinje B (utenlandsk innflytelse), C (utenlands preferanse), E

(personlig oppførsel) og K (håndtering av gradert informasjon). Alle innsiderne i undersøkelsen hadde utført handlinger som gikk i strid med retningslinje K, omhandlende håndtering av gradert informasjon, og 82 av 83 innsidere i undersøkelsen hadde utført minst én handling i de diskvalifiserende faktorene i kategori E, om personlig oppførsel.

De minst vanlige diskvalifiserende faktorene var innenfor retningslinjene som gjelder seksuell oppførsel, økonomiske hensyn, alkoholmisbruk, narkotikamisbruk og aktiviteter i andre organisasjoner (Jaros et al., 2019, s. 21-23). Oversikten over antallet innsidere som hadde utført diskvalifiserende handlinger etter de adjudikative retningslinjene er presentert i figur 7.



Figur 7: Oversikt over diskvalifiserende atferd før arrestasjon (Jaros et al., 2019, s. 21)

Foruten de 13 retningslinjene har PERSEREC også vurdert «the behavioural threat assessment framework» for å kunne identifisere mulige indikatorer på innsideaktivitet (Jaros et al., 2019). I dette atferds-rammeverket nevnes det 5 ulike kategorier (behavioural indicators) som relaterer seg til atferd innsidere har hatt før arrest: bekymringsfull kommunikasjon, bekymringsfulle interesser, planleggings-atferd, signifikante livshendelser og bekymrede bekjente. Førstnevnte kategori, bekymringsfull kommunikasjon, relaterer seg til om personen har snakket om innsideaktivitet til noen som ikke var involvert. Bekymringsfulle interesser henviser til om personen har vist interesse om noe relatert til innsideaktivitet, eksempelvis interesse i overvåkning, eller om de har deltatt på protester mot myndighetene. Med planleggings-atferd menes om personen planla innsideaktivitet, eller om de laget planer for å redusere skadevirkningene dersom de skulle bli tatt. Videre vil

signifikante livshendelser vise til om de hadde problemer relatert til familie, ekteskap, profesjonell status eller personlige tap. Det siste punktet, bekymrede bekjente, peker til om noen oppdaget bekymringsfull atferd eller endringer i atferd hos personen. Ut i fra dette rammeverket ble det funnet at flest innsidere hadde vist atferd relatert til kategoriene planlegging, signifikante livshendelser og bekymrede bekjente (Jaros et al., 2019, s. 23).
Både når det gjelder de 13 retningslinjene og de fem ulike atferdskategoriene vil en innsider kunne vise atferd som faller innenfor flere av punktene før de blir tatt for innsideaktivitet (Jaros et al., 2019).

En utfordring som ble funnet relatert til de diskvalifiserende faktorene i de 13 adjudikative retningslinjene var at på det tidspunktet der brudd oppdages, så har personen mest sannsynlig allerede utført en ulovlig handling. Jaros et al. (2019, s. 25) fant at 81 av 83 trusselaktørene hadde brutt reglene relatert til å «beskytte klassifisert informasjon eller informasjon som på annet vis var unntatt offentligheten». De kan således allerede ha begått handlinger som kan karakteriseres som innsideaktivitet. Det ble derfor funnet at for å best mulig forhindre innsideaktivitet, og hindre at innsidere ble en trussel før det ble skade for virksomhetens verdier, så er de ulike atferds-indikatorene i «behavioral threat assessment» mer hensiktsmessige å bruke.

En ytterligere utfordring med de 13 retningslinjene er at det i studien ble funnet at det som er den vanligste antagelsen relatert til indikatorer for innsideaktivitet, nemlig gjeld, vises minst igjen blant trusselaktørene. Dette selv om penger er det mest vanlige motivet (Jaros et al., 2019).
De diskvalifiserende faktorene relatert til punkt F (økonomiske forhold) omhandler blant annet eksisterende gjeld, en tidligere manglende evne til å betale gjeld, useriøs eller uansvarlig bruk av penger i forbindelse med eksisterende gjeld og historie relatert til ulovlig finansielle handlinger (Jaros et al., 2019, s. 31). Dette peker mot at selv om penger er et av de vanligste motivene, så har de færreste innsidere så høy gjeld at det kunne kvalifiseres som diskvalifiserende i en klareringssak. Det er således ikke er gjeld, men grådighet som gjerne er årsaken til innsideaktivitet med finansielt motiv (Jaros et al., 2019, s. 25-26). Dette er for mange relatert til kulturelle oppfattelser relatert til suksess (Charney & Irvin, 2016, s. 71). Den kulturelle oppfattelsen om hva det vil si å være suksessfull vil være varierende basert på kulturen, men hvordan en person opplever og ser seg selv i denne sammenhengen er relatert til deres personlighetstrekk. Personene med de omtalte personlighetstrekk har et forhøyet selvbilde, og gjerne en fantasi om hvordan de forventer at deres liv skal være, slik at selv om deres økonomiske situasjon vil kunne beskrives som gjennomsnittlig,

vil dette for mange ikke være nok (Wilder, 2017). Et eksempel på dette er en innsider som på tross at han levde et middelklasse-liv, følte stor ydmykelse da han ikke kunne gi hans barn et bedre liv i form av en mer velstående og sofistikert livsstil. Dette ble så et viktig motiv for at denne personen startet med innsideaktivitet (Wilder, 2017, s. 31).

4.3 Forebygging av innsideaktivitet

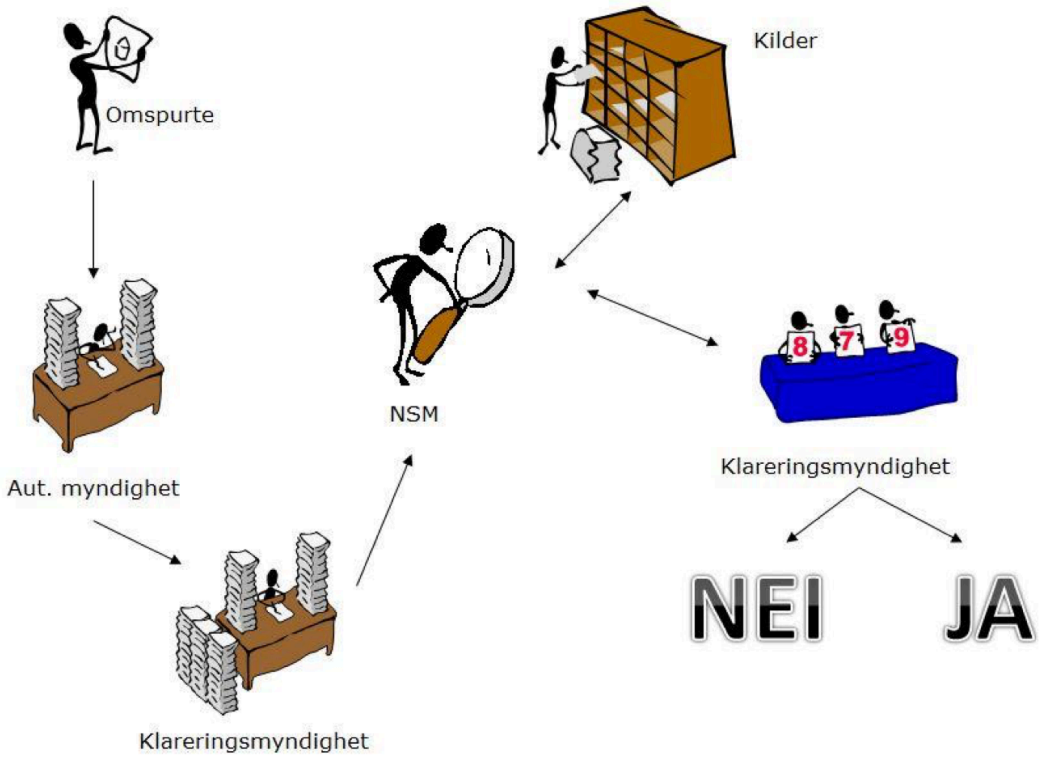
Når så de ulike faktorene og karakteristikkene med betydning for hvorfor noen blir innsidere er beskrevet, er det videre viktig å beskrive hvordan denne type aktivitet forebygges. Forebygging av innsideaktivitet handler som tidligere nevnt om å hindre at personer som ikke er sikkerhetsmessig skikket får tilgang til virksomhetens verdier, samt å kunne hindre at personer som har gyldig tilgang utvikler seg til å bli innsidere. Dersom en person så skulle starte med innsideaktivitet, er det viktig at man så kan oppdage dette så tidlig som mulig (DNVGL, 2019, s. 18). Hvordan, og med hvilke virkemidler dette gjøres, vil videre gjennomgås.

4.3.1 Sikkerhetsklarering og autorisasjon

Hva som menes med sikkerhetsgradert informasjon er tidligere beskrevet, men ytterligere foreligger det graderinger av denne informasjonen. Med dette menes at ulike typer informasjon gis ulike graderinger etter de mulige skadefølgene det kan få dersom informasjonen blir kjent for uvedkommende. Sikkerhetsgraden BEGRENSET skal brukes dersom det i noen grad kan få skadefølger, KONFIDENSIELT dersom det kan få skadefølger, HEMMELIG dersom kan få alvorlige skadefølger og STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger (sikkerhetsloven, 2018, §5-3).

For å få tilgang til sikkerhetsgradert informasjon må det først foreligge et tjenstlig behov. Dersom et slikt behov foreligger, og det kreves tilgang til informasjon gradert KONFIDENSIELT eller høyere, så krever dette en gyldig sikkerhetsklarering (sikkerhetsloven, 2018, §8-1). Det tjenstlige behovet kan komme som en følge av at en søker på en ny jobb som vil innebære en tilgang til sikkerhetsgradert informasjon, eller det kan komme som en følge av at en søker ny stilling som vil kreve sikkerhetsklarering for et høyere graderingsnivå.
Arbeidsgiver vil først anmode om at klareringsprosessen iverksettes, og den som skal autoriseres må i denne sammenheng fylle ut en personopplysningsblankett (NSM, 2011, s.7).

Ansvaret for å gjennomføre sikkerhetsklareringen ligger hos klareringsmyndigheten tilknyttet den virksomheten personen søker i. Forsvaret klarerer nødvendige personer i forsvarssektoren, mens Sivil klareringsmyndighet klarerer nødvendige personer i sivil sektor. Til slutt vil Nasjonal sikkerhetsmyndighet, Etterretningstjenesten, Politiets sikkerhetstjeneste og Statsministerens kontor klarere personer i eller tilknyttet egen virksomhet (klareringsforskriften, 2018, §1). NSM har ytterligere fag- og kontrollansvar for personellsikkerhetstjenesten etter sikkerhetsloven, og administrerer det elektroniske saksbehandlingssystemet som klareringsmyndighetene benytter (NOU 2016:19; NSM, 2011). Den generelle gangen i sikkerhetsklareringsprosessen er illustrert i figur 8.



Figur 8: Sikkerhetsklareringsprosessen (NSM, 2011, s. 6).

«En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket». Denne vurderingen av sikkerhetsmessig skikkethet baserer seg på en personkontroll der det legges vekt på personens pålitelighet, lojalitet og dømmekraft (sikkerhetsloven, 2018, §8-4).

Sikkerhetsloven (2018, §8-4) presiserer videre hvilke forhold som kan tillegges vekt i denne vurderingen, jf. bokstav a-o. Alle punktene er presentert i sin helhet i vedlegg 1. Bestemmelsens

ordlyd om at disse forhold *kan* tillegges vekt innebærer ikke at klareringsmyndigheten kan se bort fra relevante forhold i sin vurdering (NSM, u.å. a, s. 11).

Det som beskrives i §8-4 bokstav a-o kan være atferd som tidligere er utført, som er planlagt utført eller atferd som pågår på tidspunktet av klareringen. For eksempel kan dette være straffbare handlinger, terror, sabotasje, attentat, misbruk av alkohol eller andre rusmidler, tilknytning til organisasjoner som har ulovlig formål, kompromittering av skjermingsverdig informasjon eller tilknytning til andre stater. Videre vil vurderingen også kunne basere seg på faktorer som i fremtiden kan medføre at personen har eller får økt sårbarhet. Dette kan for eksempel være forhold som kan føre til at personen eller deres nærstående kan utsettes for trusler, eller enhver sykdom som kan medføre svekkelse av pålitelighet og dømmekraft. Til slutt er også observert atferd under selve klareringen et vurderingsgrunnlag, da for eksempel manglende mulighet til å gjennomføre tilfredsstillende personkontroll, nektelse eller unnlatelse av å gi personopplysninger, forfalskning av eller feilaktig eller unnlatt framstilling av faktiske forhold med betydning for sikkerhetsklareringen (sikkerhetsloven, 2018, §8-4).

Det siste punktet i listen av forhold som kan tas høyde for i vurderingen om en person er sikkerhetsmessig skikket er punkt o; «*annet som kan gi grunn til å frykte at en en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser»* (sikkerhetsloven, 2018, §8-4). I NSMs veileder om personellsikkerhet utdypes dette punktet. Her bemerkes det at «*det ikke er mulig å gi noen uttømmende oversikt over alle forhold som kan være av betydning for en persons sikkerhetsmessige skikkethet*» (NSM, u.å. a, s. 13). Dette punktet relaterer seg dermed til andre forhold av betydning som ikke er nevnt i punkt a-n. Noen av eksempler som nevnes her er religion, usikker identitet, forhold tilknyttet manglende dømmekraft eller manglende evne til sikkerhetsmessig forståelse (NSM, u.å a, s. 13).

Opplysninger om nærstående personer, dvs. «personer som er i nær familie eller som har annen nær tilknytning som kan ha betydning for om en person er sikkerhetsmessig skikket», skal tillegges vekt dersom de er sikkerhetsmessig relevante (sikkerhetsloven, 2018, §§1-5, 8-4).

Til slutt presiseres også de forhold som ikke skal vurderes. Dette omhandler en persons tilknytning og engasjement i politikk eller andre lovlige organisasjoner.

Etter gjennomført klarering vil personen som klareringen gjelder bli sent et svar, som vist i figuren over som enten godkjent klarering eller avslag om klarering. Dersom personen får avslag på

klareringen vil begrunnelse bli sendt til personen det gjelder, mens personen som har sendt anmodning om klarering ikke mottar noen form for begrunnelse (NSM, 2011, s. 7).

Dersom personen derimot får godkjent klarering på forespurt nivå vil virksomheten selv gjennomføre en autorisasjon. Autorisasjonen kan overordnet beskrives som at personens overordnede i virksomheten, eller autorisasjonsansvarlige, «har tillit til den autorisertes evne og vilje til å håndtere sikkerhetsgradert informasjon på en god måte», og utføres gjennom en autorisasjonssamtale (NSM, 2011, s. 3). Autorisasjonssamtalen skjer lokalt hos den enkelte virksomhet og skal rutinemessig avholdes før autorisasjon gis (NSM, 2011, s. 8). Det er viktig at personen som skal arbeide med sikkerhetsgradert informasjon får innføring i de rutiner og det regelverk som er tilknyttet håndtering av sikkerhetsgradert informasjon. Dette gjøres for å sikre at personen «er i stand til å løse sine oppgaver knyttet til behandling av sikkerhetsgradert informasjon på en god måte» (NSM, 2011, s. 8). Når autorisasjonssamtalen avholdes skal den autorisasjonsansvarlige i) informere om lokale sikkerhetsmessige forhold, ii) forsikre seg om at vedkommende kjenner sikkerhetsmessige risikofaktorer og aktuelle sikkerhetsbestemmelser, iii) kontrollere at opplysninger avgitt i personopplysningsblanketten er korrekte og oppdaterte, og iv) få eventuelle ytterligere opplysninger av sikkerhetsmessig betydning (NSM, 2011, s.).

Den autorsasjonsansvarlige er så ansvarlig for å videre følge opp personen gjennom sikkerhetsmessig ledelse og kontroll (sikkerhetsloven, 2018, §8-9). Oppfølgningen av autorisasjonen gjennom sikkerhetsmessig ledelse og kontroll følger personen i hele perioden de har tilgang til sikkerhetsgradert informasjon (NSM, 2011, s.3). Skulle det underveis i ansettelsesforholdet avdekkes opplysninger som gir grunn til å tro at en autorisert person ikke er sikkerhetsmessig skikket, må klareringsmyndigheten varsles (sikkerhetsloven, 2018, §8-10).

4.3.2 Før, under og etter ansettelsesforholdet

Overordnet kan prosessen med klarering, autorisasjon og sikkerhetsmessig ledelse og kontroll beskrives gjennom tre faser: før-, under og etter et ansettelsesforhold (DNVGL, 2019). Det som er sentralt i den første fasen, før ansettelse, er at en person som ikke er sikkerhetsmessig skikket får tilgang, kompetanse og tillit. Dette relaterer seg så til arbeidet med klarering og autorisasjon før en person ansettes i virksomheten.

I andre fase er det å hindre at en person som har lovlig tilgang utvikler seg til å utgjøre en trussel mot virksomheten. Trusselen som innsidere representerer er en noe annerledes trussel. Det er en intern trussel, noe som betyr at det er en trussel som de selv kan påvirke i større grad enn eksterne. Det er dermed viktig å være klar over at «*de menneskelige sårbarhetene kan oppstå og endres i løpet av tidsperioden personen er klarert»* (Justis- og beredskapsdepartementet, 2020, s.78). Dette betyr at arbeidet med klarering og autorisasjon ikke avsluttes dersom en person ansettes i virksomheten. De faktorene som har en innvirkning på om man er sikkerhetsmessig skikket kan endre seg undervis, og må derfor vurderes også under ansettelsesforholdet. Empirien viser at det ofte er tre til fem år inn i ett arbeidsforhold at de fleste innsiderne starter sine «karrierer». Samtidig har NSM observert at det på dette tidspunktet også er da flere virksomheter får avtagende bevissthet og oppfølgning av ansatte (NSM, 2018).

Denne kontinuerlige prosessen fortsetter også når en person skal avslutte sitt ansettelsesforhold. De samme forpliktelsene relatert til sikkerhetsmessig atferd gjelder også da. I denne fasen er det viktig å gjøre personer klar over dette ansvaret, samtidig som virksomheten også må sørge for at alle tilganger til sikkerhetsgradert informasjon slettes (PST, NSM, Politiet & NSR, 2017). Dette vil hindre at en personer som i etterkant av et ansettelsesforhold utvikler seg til å bli en innsider, har tilgang til verdiene.

5. Drøfting av funn opp mot teori

Målrettet motvirkning av innsiderisikoen er en kompleks oppgave som krever betydelig med kompetanse og fokus på mer enn klareringen, da menneskelige sårbarheter kan oppstå eller endres i løpet av tidsperioden personen er klarert (Justis- og beredskapsdepartementet, 2020, s. 78).

Hvilke barrierer som er viktige for å forebygge innsideaktivitet henger sammen med karakteristikker og faktorer ved denne trusselen. For å kunne drive et godt forebyggende arbeid, og for å implementere de beste tiltakene og barrierene, er det dermed viktig å basere dette på trusselen, hvordan trusselaktørene opererer og de ulike årsaks- og virkningssammenhengene.

5.1 Innsider og innsidetrussel

Den manglende konsensusen omkring definisjonen av begrepet innsider og den trusselen de representerer er et viktig aspekt relatert til det forebyggende arbeidet. En utfordring i denne sammenhengen er at det i utgangspunktet er den samme trusselen det refereres til, men at trusselen omtales med to ulike begreper.

Det er tidligere vist til at forståelsen av hva en innsider er kan deles inn i to perspektiver, noe som her kan refereres til som perspektiv A og perspektiv B. Den første, perspektiv A, ser en innsider som en person med tilgang, kunnskap og tillit. Dersom en person misbruker tilgangen, så refereres det til som en innsidetrussel. Den andre forståelsen, perspektiv B, ser en innsider som en som har tilgang, og som så misbruker denne for å påføre virksomheten skade eller tap.

Det første og grunnleggende problemet er således hva en innsider er; er det en person med tilgang, eller en person med tilgang som påfører virksomheten skade eller tap? Forskjellen har betydning for kunnskapsutvikling og informasjonsutveksling. Hvis noen skriver en oppgave der fokuset er forebygging av innsidere, vil dette gi mening i perspektiv B, men ikke i perspektiv A. I perspektiv A vil oppgaven handle om å forebygge det som enkelt kan refereres til som en ansatt i en virksomhet. I perspektiv B vil oppgaven derimot handle om å forebygge personer med ondsinnede intensjoner. Det er dermed også knyttet negative konnotasjoner til begrepet innsider i perspektiv B, noe det ikke er i perspektiv A.

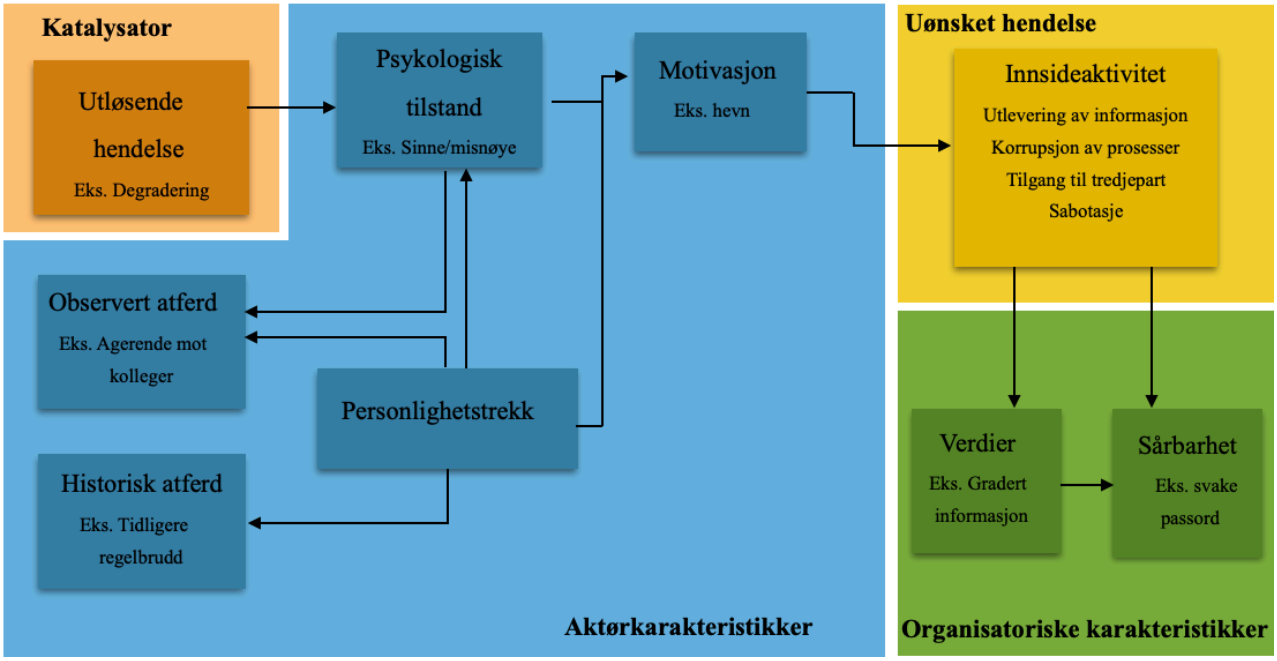
I dagligtalen, som i perspektiv A, vil en innsider gjerne brukes om en person som har en viss tilgang. Dersom personen så misbruker denne tilgangen, vil det kunne representere en trussel og man snakker da om innsidetrussel. Det kan dog argumenteres for at alle personer med en tilgang, kunnskap og tillit utgjør en mulig trussel, slik at det å skille mellom innsidere og innsidetrusler vil kunne være problematisk i det forebyggende arbeidet. Alle innsidere må tas høyde for når en skal vurdere den mulige trusselen, da det er knyttet stor usikkerhet til hvem dette kan være. Dette vil dermed ha en betydning for de forebyggende tiltakene en anvender eller skal implementere. At det er en mulig trussel mot virksomheten stammer grunnleggende fra den tilgangen eller kapasiteten de har, og ikke først basert på hvilke handlinger de gjør.

Et interessant aspekt ved forebygging av innsiderisikoen, som kan være knyttet til hvorfor det er utfordringer omkring å skape konsensus ved definisjonen, er skillet mellom sikkerhet og sikring. De hendelser som anses som sikringshendelser har ofte ikke en sammenheng med virksomhetens produksjon eller drift. Innsidehendelser er derimot karakterisert ved at det er en trussel som oppstår og utvikler seg i relasjon til virksomheten, og er på sin side sterkt knyttet til virksomhetens produksjon. Dette vil så kunne diskuteres om dette er hendelser som overskrider skillet mellom sikkerhet og sikringshendelser.
Det som derimot kan sies å være avgjørende for hvordan hendelsene karakteriseres, og som gjennom en avklaring kan muliggjøre et godt kunnskapsgrunnlag og utvikling av det forebyggende arbeidet, er de avgrensingene av begrepet som er vist i de empiriske dataene. En avklaring av om det er bevisste eller ubevisste innsidere vil først kunne sies å være avgjørende for om det er å regne som en sikrings- eller sikkerhetshendelse. Det er kun de bevisste innsidere som kan sies å ha en ondsinnet intensjon, og som dermed ut i fra det teoretiske grunnlaget som er gitt, vil kunne ansees som sikringshendelser. Innsidehendelser knyttet til ubevisste innsidere skjer gjerne som følge av at en ikke følger rutiner for sikkerhet, og er kan dermed vurderes å være sikkerhetshendelser. Videre vil forståelsen av begrepet ytterligere kunne avklares gjennom å beskrive hvorvidt innsiderne som studeres er en eller flere av de ulike typene bevisste innsidere, eller om det skilles mellom modus operandi. Innsidere er et komplekst og sammensatt problem, og de ulike kategoriene vil kunne kreve andre metoder for forebygging. Dette er således et viktig aspekt å være klar over i det generelle arbeidet med forebygging og hvordan man avdekker innsidere eller innsidetrusler. Det er også et aspekt som kan vurderes å være bakenforliggende for utfordringene omrking definisjon av en innsider og en innsidetrussel.

5.2 Forebygging av innsidere

Gjennomgangen av innsidere presenterer et bilde over kompleksiteten i hvert enkelt menneske og dermed også kompleksiteten i hvordan arbeidet med forebygging bør foregå. Det er, som tidligere nevnt, ikke én enkel profil på innsidere som kan brukes som en veileder i vurderinger av personer innen personellsikkerhet. Det er likevel funnet noen trekk som er vist til å øke sårbarheten hos mennesker, og dermed også risikoen i den enkelte virksomheten. For å kunne redusere risikoen i virksomhetene er det viktig at det forebyggende arbeidet tar høyde for, og iverksetter tiltak, som er i overensstemmelse med empirisk forskning på innsidere.

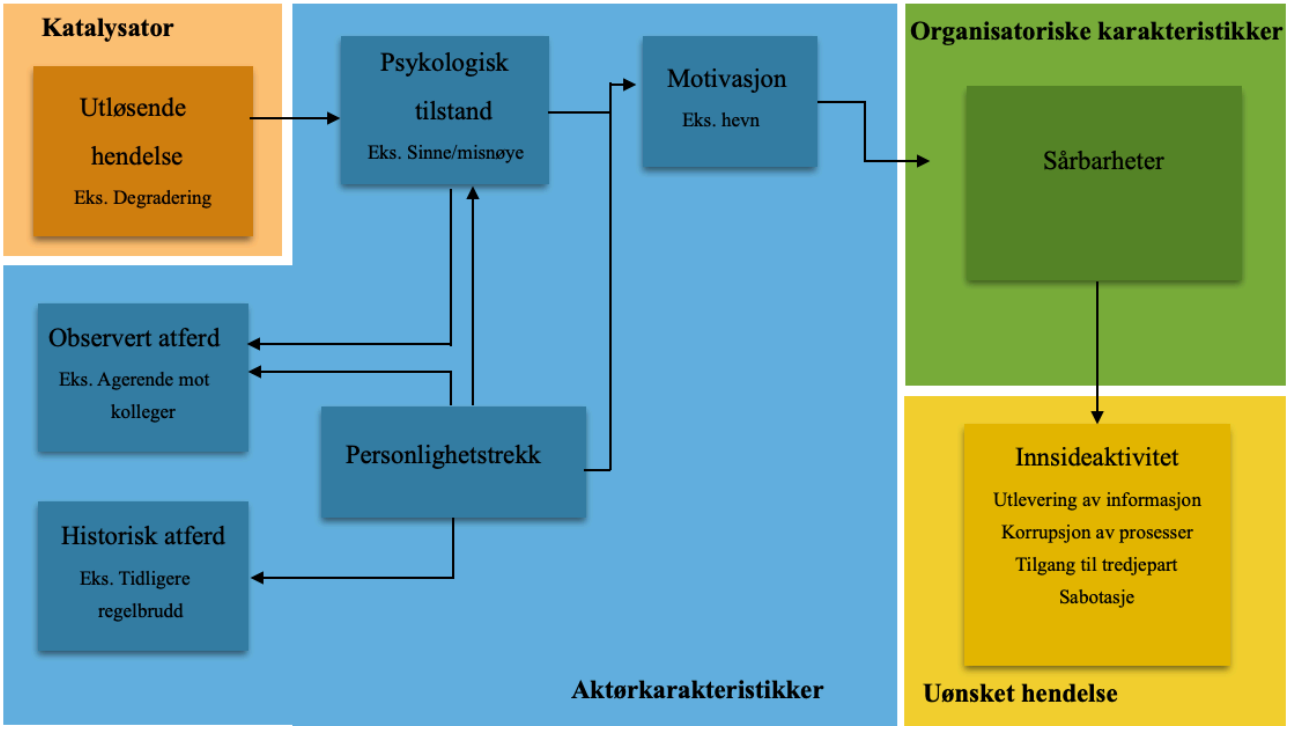
Funnene i litteraturen oppsummeres godt gjennom det tidligere refererte rammeverket fra Nurse et al. (2014). Det presenterer flere av de mulige sårbarhetene i personer, men har et noe bredere perspektiv enn denne oppgaven omhandler. For å tydeliggjøre sammenhengen av de aspektene som er relevant for oppgavens problemstilling kan det orginale rammeverket justeres som vist i figur 9.



Figur 9: Rammeverk for innsideaktivitet - etter inspirasjon fra Nurse et al. (2014, s. 3)

En utfordring med dette rammeverket er likevel at det viser de organisatoriske karakteristikkene, og således også sårbarhetene, som noe som er en følge av en uønsket innsidehendelse. Sårbarhetene som presenteres i rammeverket til Nurse et al. (2014) er relatert til beskyttelse av verdiene, og viser til evnen for å hindre eksfiltrering av verdiene. For eksempel vil dette kunne være dårlige passord

eller manglende kontroll av personell når de forlater arbeidsplassen. Dette kan dermed sies å ikke være en reell fremstilling av mulige sårbarheter i virksomheten. En mulig endring av dette rammeverket presenteres derfor under i figur 10.



Figur 10: Revidert rammeverk for innsideaktivitet - etter inspirasjon fra Nurse et al. (2014, s. 3)

Sårbarhetene som er presentert i det opprinnelige og det justerte rammeverket (figur 5 og 9), er flyttet i det reviderte rammeverket (figur 10) for å vise at de uønskede hendelsene i virksomheten kommer som en følge av sårbarhetene. Hvilke sårbarheter det er snakk om er derfor også endret, gjennom at det ikke lenger kun representerer sårbarheter omkring eksfiltrering av verdiene. Verdiene er også tatt ut av rammeverket da alle personer i disse virksomhetene har en viss tilgang på verdier kun i form av at de har godkjent sikkerhetsklarering og autorisasjon, og dermed også kunnskap. Metodene for å hente ut disse verdiene er flere, men ikke alle krever tilganger utenom den individene har i sitt daglige arbeid. Verdiene er således mer en bakenforliggende faktor som individene har tilgang til i kraft av godkjent klarering og autorisasjon, og er derfor ikke inkludert i rammeverket. Det endelige rammeverket i figur 10 viser nå de relevante aspekter i en persons vei til innsideaktivitet.

Selv om rammeverket til Nurse et al. (2014) godt illustrerer de ulike forholdene med betydning for en persons vei til innsideaktivitet, går det ikke i dybden på hvilke sårbarheter som kan medføre en

slik uønsket hendelse. Disse sårbarhetene vil videre presenteres ut i fra en gjennomgang av en persons ansettelsesforhold, og de barrierene og funksjonene som er sentrale i forebyggingen.

5.2.1 Viktige barrierer

I den første fasen, før ansettelsesforholdet viser de empiriske dataene at arbeidet med sikkerhetsklarering og autorisasjon er en særdeles viktig barriere. Dette vil hindre at personer som ikke er sikkerhetsmessig skikket får tillit, tilgang, kunnskap om verdiene. Hovedfunksjonen til det som kan omtales som barriere 1, er at den skal sikre verdiene fra farer, og å skape en forståelse og en bevissthet om farer. En annen svært viktig barriere er virksomhetenes arbeid med sikkerhetsmessig ledelse og kontroll; barriere 2. Denne barrieren har også den funksjon at det skal sikre verdiene, men skal ytterligere også varsle om farer.

Grunnlaget for den første barrieren, og dets funksjon om å sikre verdiene fra farer, er klareringen og autorisasjonen. Dette baserer seg på sikkerhetslovens (2018) bestemmelser gitt i §8-4, bokstav a-o. Her presenteres en rekke punkter som er veiledende kriterier for å vurdere den enkeltes egnethet, og som da også utgjør grunnlaget for opprettholdelse av barrierens funksjon.
Punktene fokuserer i dag i hovedsak på en persons atferd, det som tidligere er presentert som den historiske og observerte atferden. Det er vist i det empiriske grunnlaget at dette er faktorer som har betydning for om en person er sikkerhetsmessig skikket, og vil dermed delvis oppfylle barrierens funksjon om å sikre verdiene fra farer.

Selv om punktene i sikkerhetsloven §8-4, bokstav a-o (2018) er funnet å ha betydning for en persons skikkethet, er det i empirien avdekket at noen av punktene har varierende relevans ovenfor forebygging av innsideaktivitet. Dette er for eksempel lovens bestemmelser om økonomiske forhold som kan friste en person til å handle i strid med nasjonale sikkerhetsinteresser (sikkerhetsloven, 2018, §8-4, bokstav k). At en person har svak personlig økonomi, som mye gjeld, er i de empiriske dataene ikke vist å være av stor betydning for om en person blir innsider. Det er ikke personer med svak personlig økonomi som utvikler økonomiske motiv for å drive med innsideaktivitet, men det er personer som har god økonomi, men som ønsker bedre. Det er dermed grådighet som er funnet til å være av størst betydning sett opp mot punktet om økonomiske forhold. Samtidig er det også funnet andre punkter som misbruk av alkohol eller andre rusmidler ikke har vært avgjørende faktorer for innsideaktivitet (Jaros et al., 2019; Wilder, 2017).

Likevel er ikke disse punktene en vurdering av disse forholdene alene. Med dette menes at vurderingsgrunnlaget omkring eksempelvis personlig økonomi ikke kun har det forhold å avdekke personer som mulig kan bli fristet. De økonomiske forhold kan også være en indikator på en persons «evne og vilje til å ivareta sine forpliktelser». Det peker altså ut over de rene økonomiske forhold mer generelt også til en persons karakter, og kan således anses som av stor betydning da det er en del av å skape et helhetsinntrykk av hver person (NSM, u.å. a, s.12).

Den andre funksjonen som barriere 1 skal oppfylle er å skape en forståelse og en bevissthet om farer. Dette gjøres i sammenheng med barriere 2, da menneskelige sårbarheter kan oppstå og endres under klareringsperioden. Det handler således om å drive forebyggende arbeid gjennom hele klareringsperioden.
Forståelsen og bevisstheten utvikles i barriere 1 ved at det først skapes et kunnskapsgrunnlag om personer som søker klarering. Dette gjøres gjennom innsamling av opplysninger om dem, og vil kunne fortelle personens nærmeste leder om forhold som i fremtiden vil kunne utgjøre en fare. Det er dermed også tilknyttet barriere nummer 2; arbeidet med sikkerhetsmessig ledelse og kontroll. Barriere 1 sin funksjon om å skape forståelse og bevissthet om farer vil muliggjøre at barriere 2 kan registere endringer i forhold som har betydning for klareringen eller autorisasjonen. Dersom det oppfattes negative endringer i en persons liv som kan øke sannsynligheten for innsideaktivitet, for eksempel endringer som gjør at de på en eller annen måte kan blir presset til å selge gradert informasjon, så kan virksomheten drive oppfølgning og veiledning med personen for å hindre en uønsket hendelse. Dette danner så videre grunnlaget for funksjonen i barriere nummer 2, der slike endringer og observert atferd vil kunne varsle om mulig fare.

Barrierene som brukes i dag kan i hovedsak sies å være sentrale for å avdekke en mulig innsider, gjennom at de forebygger denne type aktivitet ved at personer sikkerhetsklareres og autoriseres, og videre at personene følges opp gjennom sikkerhetsmessig ledelse og kontroll. Det er likevel avdekket faktorer som ikke tas med i vurderingen. Dette medfører at selv om barrierene som eksisterer i dag kan sies å være viktige, vil denne mangelen gjøre at barrierene også har hull som således kan gjøre virksomheten sårbar for farer.

5.2.2 Sårbarheter

Gitt de faktorene som er avdekket om hvorfor og hvordan noen blir innsidere kan det diskuteres om dagens forebygging av innsidere gjennom grunnlaget som skal vurderes i sikkerhetslovens (2018) kapittel 8-4 bokstav a-o, er egnet for å forhindre og avdekke innsidere. Dette vil som en følge bety at de funksjoner som barriere skal ha, ikke oppfylles. Menneskers individuelle forskjeller påvirker sårbarheten i virksomheten. Det er dermed viktig at virksomheten ser hele mennesket i det helhetlige sikkerhetsarbeidet, for å kunne implementere tilpassede tiltak (NSM, 2019c, 27:08).

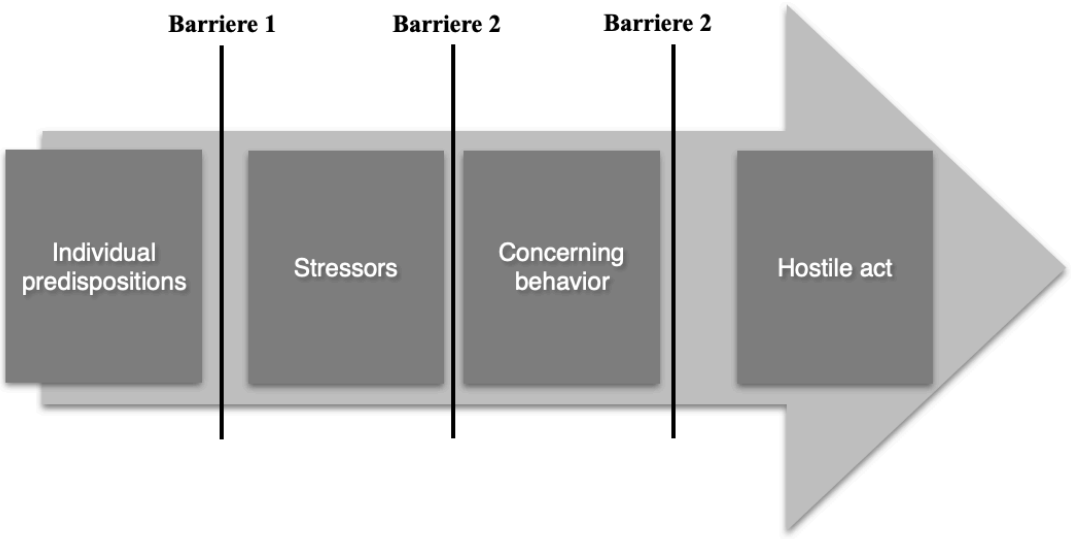
Som de empiriske dataene viser er personlighetstrekk en grunnleggende faktor som har betydning for vår fremtidige atferd (Larsen og Buss, 2010, s. 6). Det har en innvirkning på hvordan vi tenker og handler, og dermed også hvilke hendelser vi opplever, og hvordan vi opplever dem. Dersom faktoren om personlighetstrekk ikke vurderes i barriere 1 under klareringen og autorisasjonen, vil dette kunne representere en sårbarhet i mennesket som virksomheten ikke er bevisst. Det vil fra Reasons (1997) perspektiv så kunne være et latent forhold, som etter lengre tid vil få konsekvenser for virksomheten.

Latente forhold manifesterer seg ofte i forbindelse med endringer i lokale forhold eller i sammenheng med aktive feil (Reason, 1997). Dette kan være hendelser som at noen personer blir forbigått for forfremmelse, eller endringer i personens private forhold. Som det er vist vil dette kunne fungere som en utløsende hendelse, og er dermed svært viktig at det er grunnlag for å oppdage disse i barriere 2. Dersom man ikke er klar over hvilke personer som kan få en sterkere følelsesmessig respons, vil det skape hull, og faren forbigår barrierene. Barrierenes funksjoner om å varsle om mulige farer, vil da ikke oppfylles.
Enhver person vil kunne oppleve utløsende hendelser. Det som viser seg å være spesielt med en person med de nevnte personlighetstrekkene, er at de i gjennomsnitt vil oppleve flere slike hendelser, og videre også få større psykologiske responser (Wilder, 2017). Et eksempel er dersom virksomheten går gjennom en omorganiseringsprosess. Det er selvfølgelig mulig at det ikke vil resultere i en uønsket hendelse, men det er samtidig vist at slike trekk er en sårbarhet som øker sannsynligheten. Det er videre også en type sårbarhet som følger personer over tid. Personen med disse trekkene innehar spesifikke egenskaper som utgjør en risiko for virksomheten, og som, dersom de ikke plukkes opp, er en sårbarhet for virksomheten som blir liggende latent. Risikoen er at dette vil kunne resultere i en uønsket hendelse som får konsekvenser for nasjonens sikkerhet.

At personer innehar visse personlighetstrekk forstås ikke her som et grunnlag for å vurdere en person som ikke å være sikkerhetsmessig skikket, men det er en faktor på lik linje med de andre forhold i sikkerhetsloven (2018) §8-4, bokstav a-o. Hvis man kan foreta en vurdering av personlighetstrekk i første fase vil man kunne være klar over mulige sårbarheter hos mennesker i virksomheten, på lik linje med andre mulige sårbarheter som avdekkes på bakgrunn av vurderingen i sikkerhetslovens §8-4, bokstav a-o. At personen har disse trekkene er som nevnt ikke nødvendigvis en diskvalifiserende faktor alene, men er i likhet med andre utfordringer, heller en mulig sårbarhet som må følges opp under ansettelsesforholdet gjennom sikkerhetsmessig ledelse og kontroll. Det vil være her man kan avdekke mulige utløsende hendelser og uønsket atferd, og dermed iverksette hjelpetiltak. Dette vil som et resultat øke følelsen av tilhørighet til virksomheten, og dermed også lojaliteten hos den enkelte (NSM, 2019 c). Å inkludere personlighetstrekk vil således kunne vil muliggjøre bedre veiledning og oppfølging underveis i klareringsperioden.

Dersom man har en kontinuerlig prosess relatert til oppfølgning av personer vil man kunne hindre innsideaktivitet selv om man ikke oppdager den utløsende hendelsen. «Behavioural indicators» fra «the behavioural threat assessment framework» er vist i litteraturen å være vel så effektive i å avdekke innsidere enn de diskvalifiserende faktorene, fordi man vil kunne observere endringer i den psykologiske tilstanden og personens atferd. En vurdering av individers personlighetstrekk vil dermed kunne sies å være en mer proaktiv metode for å forebygge og avdekke innsideaktivitet.

De barrierene og underliggende funksjoner som er relevante, dvs. hensiktsmessig og retningsgivende for virksomhetens forebyggende arbeid innen arbeidet med personellsikkerhet, kan forenklet illustreres som vist i figur 10:



Figur 11: Barrierer for forebygging av innsidekativiet. Inspirert av modell fra Baweja et al. (2019, s. 10).

Barriere 2 er satt på to ulike plasser i figur 10 for å illustrere viktigheten av det kontinuerlige arbeidet. Dette kunne også vært illustrert med én sammenhengende strek under både utløsende hendelser og bekymringsfull atferd. Det er likevel valgt å dele denne opp i to for å presisere at barrieren kan avdekke innsideaktivitet både ved utløsende hendelser og atferd alene.

Overordnet kan det forebyggende arbeidet opp mot innsidere beskrives gjennom at det er ikke nok å kun foreta en vurdering av personen som en del av barriere nummer 1, og ikke nok å kun følge opp personer dersom de opplever hendelser eller utviser bekymringsfull atferd i barriere 2. Det må være en kontinuerlig prosess som krever begge barrierene, der man også må opprettholde sikkerhetsmessig bevissthet og oppfølgning lengre enn de registere tre til fem år (NSM, 2018).
Det er likevel viktig å være klar over at dette er menneskelige og organisatoriske barrierer, og at aktive feil fra personene på det Reason kaller «frontlinjen» kan redusere barrierenes ytelse og dermed funksjon. Det som likevel kan bedre dette, på tross av aktive feil, er dersom alle i virksomheten er klar over mulig bekymringsfull atferd. Rutiner for varsling og rapportering fra alle i virksomheten er en avgjørende faktor for å hindre innsideaktivitet, men har implikasjoner og utfordringer som ikke kan dekkes av denne oppgavens omfang.

Barrierene som vist ovenfor er formelle preventive barrierer gjennom at de er nedfelt i loven og har det formål at de skal forebygge at en innsidehendelse skjer. Ut ifra rammeverket til Hammerlin (2011) er den sikkerhetsmessige vurderingen av en persons skikkethet å regne som et spisset tiltak, da det er tiltak som er rettet mot de aktørene som har et tjenstlig behov for å klareres og autoriseres. Videre er dette et tiltak som vil påvirke både en persons intensjon og kapasitet; prosessen med

klarering og autorisasjon vil avdekke de personene som har en underliggende intensjon om å påføre virksomheten skade, samtidig som det ved å ikke gi tilgang til personer vil redusere personers kapasitet. Gitt at dette så er spissede tiltak vil det etter Hammerlin (2011) sitt rammeverket ha færre demokratiske kostnader, men det er likevel kostnader som må vurderes.

5.3 Individers rettssikkerhet

«Personellsikkerhet er et område hvor myndighetene gis hjemmel til å innhente og behandle til dels meget sensitive personopplysninger om den enkelte» (Forsvarsdepartementet, 2017, s. 114). Dette arbeidet, og en mulig innføring av personlighetstrekk som vurderingsgrunnlag, har utfordringer i form av at det er klare grenseflater mot individers rettssikkerhet.

Rettssikkerhet har flere betydninger, men det omhandler i denne sammenheng borgernes grunnleggende rettigheter (Kjønstad & Syse, 2012). Her er to betydninger som tillegges rettssikkerhetsbegrepet, der de to kan sies å være motstridende interesser. Det første omhandler det som skal «verne individet mot vilkårlighet, uforutsigbarhet og overgrep fra myndighetene». Den andre er rettsvernet, som omhandler statens plikt til å verne borgerne og garantere for deres sikkerhet (Ryssdal, 2005, s. 55).

Det som de empiriske dataene avdekker at bør være en del av vurderingsgrunnlaget vil kunne implementeres sammen med det allerede eksisterende vurderingsgrunnlaget i sikkerhetsloven (2018) §8-4, bokstav a-o, men det kan dog ansees som mer inngripende ovenfor rettssikkerheten. Slike endringer i reguleringer vil ikke alene basere seg på det behovet som kan vurderes etter rettsvernet, men vil også påvirkes av offentligheten og interessenter, og deres vurdering av trusselen og medfølgende risiko, samt hvilke interesser som står på spill (Baldwin et al., 2012; Engen et al., 2016). Tiltakenes nytte kan være vanskelig å forstå, samt at det kan være usikkerhet til effektene og den mulige utviklingen av disse tiltakene.

Likevel er det slik at «noen trusler og risikoer kan (…) være så alvorlige at de underlegges strengere krav til risikoreduksjon» (Justis- og beredskapsdepartementet, 2020, s. 33). Det er dog et prinsipp som følges, som er presisert i forarbeidet til sikkerhetsloven (2018): «forslag som innebærer inngrep i den enkeltes rettssikkerhet og personvern, skal være godt begrunnet, forholdsmessige og ha en sikkerhetsmessig effekt som overstiger personvernulempene» (Forsvarsdepartementet, 2017, s. 118). Dette er således en vurdering som bør foretas.

En måte denne balansen mellom individers rettssikkerhet og nasjonale sikkerhetsinteresser til en viss grad kan holdes er å implementere et tiltak der man vurderer personlighetstrekk, men dog som et tiltak som kan anses som mer spisset. Det å skulle foreta en personlighetsvurdering av alle personer som har tjenstlig behov for sikkerhetsklarering vil ikke nødvendigvis være å anse som hensiktsmessig da det vil være svært omfattende. En slik vurdering vil kreve betydelig med ressurser, både i form av tid og kompetanse hos klareringsmyndigheten.

En vurdering av de trekkene som er funnet å være indikatorer for mulig innsideaktivitet vil måtte gjøres av personell som er kvalifisert til å foreta en slik vurdering. Dette er ikke noe som kan antas at eksisterer i de ulike klareringsmyndighetene i dag. Det vil også svært tidkrevende å gjennomføre dette på hver enkelt person som søker klarering. Dette kan eksemplifiseres med Forsvarets Sikkerhetsavdeling som er den største klareringsmyndigheten i Norge, og som sikkerhetsklarerer flere tusen personer i Forsvaret per år (NOU 2016:19, s. 39). Det kan dermed vurderes om det er nødvendig med en slik dyptgående vurdering på alle, eller om det er mulig å innføre et mer spisset tiltak. Personlighetsvurderinger kan eksempelvis ansees som å være hensiktsmessige å foreta i de tilfeller der personer søker klarering for HEMMELIG eller høyere, eller personer som søker stillinger der en får tilgang til bred, og særskilt sensitiv aksess. Dette vil redusere de demokratiske kostnadene for individers rettssikkerhet, men vil også gjøre at barrierene har sårbarheter da funksjoner ikke fullt oppfylles.

5.4 Sårbarhet og usikkerhet

Det kan argumenteres for at et vurderingsgrunnlag basert på personlighetstrekk ikke er så hensiktsmessig gitt at dette er en utfordring som har en kostnad opp mot individers rettssikkerhet og som også kan sies å innebærer usikkerhet. Det er ikke slik at alle personer som har disse trekkene blir innsidere, og det er ikke sikkert at alle innsidere vil ha disse trekkene. Gitt usikkerheten, og gitt de negative konsekvensene for individets rettssikkerhet en slik vurdering kan ha, så kan dette dermed anses som å være mindre fruktbart for det forebyggende arbeidet. Likevel er det slik at alle risikoer er relatert til usikkerheter, og hvordan man så skal håndtere denne usikkerheten er viktig i denne sammenhengen. En vurdering av mulige risikoer i fremtiden er ikke fakta, men en skjønnsmessig vurdering (Jore, 2019b, s.4047). Målet er å ta velinformerte beslutninger basert på den informasjonen man har. Det er derfor sentralt å ta med både hva man vet, men også hva man ikke vet, i denne vurderingen. Å kunne si noe om hva man ikke vet er selvsagt et paradoks, men usikkerhet handler om at man ikke har fullstendig kunnskap, enten dette er på på grunn av

manglende kunnskap eller tvetydig kunnskap (Jore, 2019b, s. 4049). Usikkerheten omkring innsidere kan sies å være stor, og de faktorene som er vist i oppgaven vil ikke være definitive indikasjoner for om en person blir innsider eller ikke. Usikkerheten må derfor også tas høyde for, da det vil sette oss i en bedre posisjon for å kunne styre denne mulige fremtidige risikoen (Jore, 2019b). Samtidig må usikkerheten vurderes opp mot de verdiene vi ønsker å beskytte. Dette er verdier som har betydning, ikke bare for enkeltindivider eller individene i den aktuelle virksomheten, men det er verdier som ved tap og skade vil kunne få store konsekvenser for hele nasjonen.

Det å kunne avdekke personer som kan representere en trussel i fremtiden, ut i fra at de har visse sårbarheter, vil således være fruktbart for å dermed redusere usikkerheten omkring virksomhetens risiko. Når en så har avdekket at disse trekkene er mulige sårbarheter, vil det, for å kunne redusere risikoen i virksomhetene, være hensiktsmessig å sørge for at tiltakene, barrierene og deres tilhørende funksjoner tar høyde for dette.

6. Konklusjon

Formålet med denne oppgaven var å øke den forskningsbaserte kunnskapen om motvirkning av innsiderisikoen, ved å undersøke problemstillingen «*hva er en innsider og hvilke barrierer og tilhørende funksjoner er viktige for å forebygge innsideaktivitet?*

Dette ble gjort gjennom å studere innsidere, deres karakteristikker og handlemåte, gjennom et teoretisk grunnlag, for å kunne vurdere forståelsen av innsidere og innsidetrusselen i et annet perspektiv. Dette empiriske grunnlaget ble så også brukt for å vurdere de barrierer som er viktige for å forebygge innsidere, samt at de ulike barrierenes funksjoner ble vurdert opp mot de empiriske funnene som ble avdekket.

En første viktig forståelse som kreves for å kunne øke kunnskap om innsidere og hvordan man bør forebygge denne er hva en innsider er, og hvordan dette begrepet forstås i litteraturen. Det ble funnet at begrepet innsider overordnet kan sies å være todelt. Noen anser en innsider som en person med tilgang, tillit og kunnskap om sikkerhetsgradert informasjon. En innsider kan således forså som en ansatt. Andre ser derimot en innsider som en person med den samme tilgangen, tillit og kunnskapen, men som gjennom dette påfører virksomheten skade og tap. Den manglende konsensusen om definisjonen skaper utfordringer, og konsensus bør dermed nås. Det er likevel funnet at innsidere er et svært komplekst problem, som i sin helhet ikke nødvendigvis er mulig å definere. Det er et begrep som omfatter hendelser som kan sies å være innenfor begge feltene sikring og sikkerhet, da det omhandler en menneskelig faktor som kan være enten ubevisst eller ha ondsinnede intensjoner. I arbeidet med å øke kunnskapen om innsidere og forebygging av disse bør det dermed skilles klart mellom hvilke typer innsidere som studeres og hvilke typer innsidere en ønsker å forebygge.

For å forebygge bevisst innsideaktivitet er det i denne oppgaven avdekket to svært viktige barrierer. Den første barrieren er vurderingen av en persons sikkerhetsmessig skikkethet etter sikkerhetslovens §8-4, bokstav a-o (2018). Den andre barrieren er utøvelsen av sikkerhetsmessig ledelse og kontroll i virksomheten. Disse barrierene anvendes i dag, og har de funksjoner at de skal sikre verdier gjennom å skape en forståelse og bevissthet om trusler, og varsle om disse. Det forebyggende arbeidet er dermed en kontinuerlig prosess, der personer bør følges opp gjennom hele klareringsperioden.

Selv om disse barrierene er implementert og anvendes i dag, anses det at barrierenes funksjoner kun kan sies å være delvis oppfylt. Dette medfører at det er latente forhold, som i sammenheng med såkalte aktive feil, vil kunne medføre konsekvenser for virksomhetens verdier, samt Norges suverenitet, territorielle integritet og demokratiske styreform. Sikkerhetslovens bestemmelser i kapittel 8, og i særdeleshet §8-4, synes ikke å vurdere forhold som ut fra empiriske funn er fastslått å være svært relevante.

Funnene viser at de fleste innsidere ikke søker tilgang til en organisasjon med ondsinnede intensjoner; mange utvikler innsidemotivasjon under et ansettelsesforhold, og da ofte som selvmotiverte innsidere. Selv om det å vurdere den tidligere eller historiske atferden i sammenheng med den observerte atferden gir et visst helhetsinntrykk av en person, kan det vurderes å være manglende grunnlag for å redusere usikkerhet og styre risikoen relatert til personens fremtidige atferd.

Personligheten og personlighetstrekkene har en påvirkning på våre omstendigheter i livet, den psykologiske responsen på våre omgivelser og vår atferd. Det er funnet fellestrekk hos innsidere som er relatert til narsissisme, antisosial personlighetsforstyrrelse/psykopati, sosiopati eller machiavellisme. En person som har flere slike trekk kan ansees som en større risiko for virksomheten enn de som ikke har det. Hvordan personligheten kan lede til innsideaktivitet er også knyttet til utløsende hendelser, eller livskriser. Innsideaktivitet er funnet å være en respons på kriser vi opplever, og jo større krise desto færre avvik kreves i den psykologiske fungeringen for at en uønsket hendelse kan skje. Har en person slike personlighetstrekk vil de også være mer sårbare for ytre påvirkning, og de har i gjennomsnitt flere slike kriser. Kombinasjonen av personlighetstrekk og utløsende hendelser er vist å være av stor betydning for sannsynligheten for skadelig innsideaktivitet. Likevel er ikke dette en sårbarhet som er en del av vurderingsgrunnlaget i sikkerhetslovens bestemmelser, på tross av at virksomhetene da vil ha et handlingsrom og mange muligheter til å forhindre at ansatte utvikler skadelige intensjoner. Dette innebærer således at en grunnleggende sårbarhet i mennesket oversees, og medfører dermed også en stor risiko for virksomheten og vår styringsevne og suverenitet.

6.1 Forslag til videre forskning

Med bakgrunn i at personlighetstrekk er funnet til å være av stor betydning for om en person kan bli innsider eller ikke, kan dette være en faktor som er ønskelig å inkludere som en vurdering i

sikkerhetslovens kapittel 8 (2018). En slik vurdering vil dog kreve store ressurser og kompetanse i de ulike virksomhetenes klareringsmyndigheter. Det foreligger ulike verktøy for denne typen vurderinger, som for eksempel «Shedler-Westen Assessment Procedure (SWAP) og «dispositional Indicators of risk exposure» (DIRE) (Schechter & Lang, 2011). Om dette så er verktøy som kan anvendes i norske klareringsmyndigheter, i hvor stort omfang de skal brukes og tiltakets innvirkning på den enkeltes rettssikkerhet og personvern, vil kunne være ønskelige studier for å videre kunne øke den forskningsbaserte kunnskapen om motvirkning av innsiderisikoen.

Litteraturliste

Almklov, P.G., Antonsen, S., Størkersen, K.V. & Roe, E. (2018). Safer Societies. *Safety Science, 110* (Part C), 1-6. Hentet fra https://doi.org/10.1016/j.ssci.2018.03.018 [Lest: 26.06.21].

Asdal, K. & Reinertsen, H. (2020). *Hvordan gjøre dokumentanalyse: en praksisorientert metode*. Oslo: Cappelen Damm Akademisk

Baldwin, R., Cave, M. & Lodge, M. (2012). Understanding Regulation: theory, strategy and practice (2.utg.).. Oxford: Oxford University Press.

Baweja, J.A., Burchett, D. & Jaros, S.L. (2019). *An Evaluation of the Utility of Expanding Psychological Screening to Prevent Insider Attacks* (OPA Report 2019-067/PERSEREC-TR-19-05). Hentet fra https://www.dhra.mil/Portals/52/Documents/perserec/reports/TR-19-05-Evaluation-of-Utility-Expanding-Psychological-Screen.pdf

Blaikie, N. & Priest, J. (2019). *Designing Social Research* (3.utg.). Cambridge: Polity Press

Blokland, P. J. & Reiners, G. L. (2020). The Concepts of risk, safety og security: A Fundamental Exploration and Understanding of Similarities and Differences. I C. Bieder & K.P. Gould (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 9-16). Hentet fra https://link.springer.com/book/10.1007%2F978-3-030-47229-0

Brinkmann, S. & Tanggaard, L. (Red.). (2010). *Kvalitative metoder*. København: Hans Reitzels Forlag.

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

Centre for the Protection of National Infrastructure (CPNI). (2013). *CPNI Innsider Data Collection Study: report of main findings*. Hentet fra https://www.cpni.gov.uk/system/files/documents/63/29/insider-data-collection-study-report-of-main-findings.pdf

Charney, D.L. & Irvin, J.A. (2016). The psychology of espionage. *The Intelligencer: Journal of U.S. Intelligence studies, 22*(1), 71-77. https://www.afio.com/publications/CHARNEY_and_IRVIN_Psychology_of_Espionage_from_AFIO_INTEL_SPRING2016_Vol22_no1.pdf

Central Intelligence Agency (CIA). (2014). Psychology of treason. *The IC's Journal for the Intelligence Professional.* Hentet fra https://www.cia.gov/readingroom/document/0006183135

Danermark, B., Ekström, M., Jakobsen, L. & Karlsson, J. (2002). *Explaining society: Critical realism in the social sciences*. London: Routledge.

Dey, I. (2004). Grounded theory. I C. Seale, G. Gobo, J.F. Gubrium & D. Silverman (Red.), *Qualitative Research Practice* (s. 80 - 93). London: Sage Publications

Direktoratet for samfunnssikkerhet og beredskap (DSB). (2016). *Samfunnets kritiske funksjoner*. Hentet fra https://www.dsb.no

Det Norske Veritas (DNVGL). (2019). *Håndtering av innsiderisiko* (2019-0280, Rev. 1). Hentet fra https://www.ptil.no/contentassets/d0de842c25b84fcebda5c24fe6daa6fa/handtering-av-innsiderisiko-rev-1.pdf

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

Fintland, I. & Braut, G.S. (2012). Tilsyn og regulering av risiko i fortid og notid. I P.H. Lindøe, J. Kringen & G.S. Braut (Red.), *Risiko og tilsyn: risikostyring og rettslig regulering* (s. 31-50).

Forsvarsdepartementet. (2017). *Lov om nasjonal sikkerhet (sikkerhetsloven)* (Prop. 153 L (2016-2017). Hentet fra https://www.regjeringen.no/contentassets/0fcee45affd24280896b88b5413a00aa/no/pdfs/prp201620170153000dddpdfs.pdf

Grønmo, S. (2016). *Samfunnsvitenskapelige metoder* (2.utg.). Bergen: Fagbokforlaget

Hammerlin, J. W. (2011). *Terror og demokrati: fra 11. september til 22.juli.* Oslo: Manifest

Herbig, K.L. (2017). *The Expanding Spectrum of Espionage by Americans, 1947-2015*. (PERSEREC-TR-17-10). Hentet fra https://fas.org/irp/eprint/spectrum.pdf

Jaros, S. L., Rhyner, K.J., McGrath, S. M. & Gregory, E.R. (2019). *The Resource Exfiltration Project: Findings from DoD cases, 1985-2017* (PERSEREC-TR-19-02/OPA-2019-021). Hentet fra https://www.hsdl.org/?view&did=831490

Johannessen, A., Tufte, P. A. & Christoffersen, L. (2010). *Introduksjon til samfunnsvitenskapelig metode* (4. utg.). Oslo: Abstrakt forlag

Jore, S. H. (2019a). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research, 4*(1), 157-174. Hentet fra https://link.springer.com/article/10.1007/s41125-017-0021-9

Jore, S. H. (2019b). The Multifaceted Aspect of Uncertainty – the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism. *Proceedings of the 29th European Safety and Reliability Conference (ESREL) 22-26*

September 2019, Hannover, Germany, 4044–4051. Hannover: Research Publishing. Hentet fra http://itekcmsonline.com/rps2prod/esrel2019/e-proceedings/index.html

Jore, S. H. (2020). Security and Safety Culture - Dual or Distinct phenomena? I C. Bieder & K.P. Gould (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 43-52). Hentet fra https://link.springer.com/book/10.1007%2F978-3-030-47229-0

Justis- og beredskapsdepartementet (2020). *Samfunnssikkerhet i en usikker verden* (Meld. St. 5 (2020-2021)). Hentet fra https://www.regjeringen.no/contentassets/ba8d1c1470dd491f83c556e709b1cf06/no/pdfs/stm202020210005000dddpdfs.pdf

Kjønstad, A & Syse, A. (2012). *Velferdsrett I: Grunnleggende rettigheter, rettssikkerhet og tvang* (5.utg). Oslo: Gyldendal Juridisk.

Klareringsforskriften. (2018). Forskrift om sikkerhetsklarering og annen klarering (FOR-2018-12-20-2054). Hentet fra https://lovdata.no/dokument/LTI/forskrift/2018-12-20-2054

Kont, M., Pihelgas, M., Wojtkowiak, J., Trinberg, L. & Osula, A-M. (2015). *Innsider Threat Detection Study*. Hentet fra https://www.nationalinsiderthreatsig.org/

Larsen, R. L. & Buss, D. M. (2010). *Personality Psychology: Domains of knowledge about human nature* (4. utg.). New York: McGraw-Hill.

Lincoln, Y.S. & Guba, E.G. (1985). *Naturalistic Inquiry*. Beverly Hills: SAGE Publications.

Lunde, I.K. (2018). *Praktisk krise- og beredskapsledelse* (2.utg). Oslo: Universitetsforlaget

Madsbu, J. P. (2011). Hvordan etablere vitenskapelig kunnskap om samfunnet? I Madsbu, J. P., Pedersen, M. (Red.), *I verdens rikeste land: samfunnsvitenskapelige innganger til norsk samtid.* Hentet fra https://core.ac.uk/download/pdf/30916718.pdf

Masters, B. (1997, 24.juni). Ex-FBI agent gets 27 years for passing secrets to Moscow. *The Washington Post*. Hentet fra https://www.washingtonpost.com/archive/politics/1997/06/24/ex-fbi-agent-gets-27-years-for-passing-secrets-to-moscow/54ea8da1-566b-48da-ad73-3b512ed42b24/ [Lest: 07.05.21]

Nasjonal sikkerhetsmyndighet (NSM). (u.å. a). *Veileder i personellsikkerhet.* Hentet fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/veileder-i-personellsikkerhet/sikkerhetslovens-kapittel-8/8-4-avgjorelse-om-klarering/

Nasjonal sikkerhetsmyndighet (NSM). (u.å. b). *Veileder i sikkerhetsstyring.* Hentet fra https://nsm.no/getfile.php/132933-1591350417/Demo/Dokumenter/Veiledere/veileder-i-sikkerhetsstyring.pdf

Nasjonal sikkerhetsmyndighet (NSM). (2011). *Håndbok i autorisasjon og autorisasjonssamtale*. Hentet fra https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/handbok-i-autorisasjon-og-autorisasjonssamtale/

Nasjonal sikkerhetsmyndighet (NSM). (2018). *Risiko 2018*. Hentet fra https://nsm.no/getfile.php/133720-1592915838/Demo/Dokumenter/Rapporter/nsm_risiko_2018_web.pdf

Nasjonal sikkerhetsmyndighet (NSM). (2019a). *Risiko 2019. Krafttak for et sikrere Norge.* Hentet fra https://nsm.no/getfile.php/133696-1592910347/Demo/Dokumenter/Rapporter/nsm_risiko_2019_final_enkeltside.pdf

Nasjonal Sikkerhetsmyndighet (NSM). (2019b). *Temarapport Innsiderisiko.* Hentet fra https://www.nsm.stat.no

Nasjonal Sikkerhetsmyndighet (NSM). (2019c, 21.mars). *Sikkerhetskonferansen 2019 – Kristine Borglin* [videoklipp]. Hentet fra https://www.youtube.com/

Nasjonal Sikkerhetsmyndighet (NSM). (2020). *Risiko 2020*. Hentet fra https://www.nsm.stat.no

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

Nurse, J.R.C., Legg, P., Buckley, O. & Wright, G.R.T. (2014). Understanding insider threat: A framework for Characterising Attacks. Innlegg presentert ved IEEE Computer 2014 society Security and Privacy Workshops (SPW14), San Jose, CA. Hentet fra https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6957307

NOU 2006:6. (2006). *Når sikkerheten er viktigst*. Hentet fra https://www.regjeringen.no

NOU 2016:19. (2016). *Samhandling for sikkerhet.* Hentet fra: https://www.regjeringen.no/contentassets/03960058f3f94fbe9d290593bee22c1a/no/pdfs/nou201620160019000dddpdfs.pdf

Nowell, L.S., Norris, J.M., White, D.E. & Moules, N.J. (2017). Thematic Analysis: striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1-13. https://doi.org/10.1177%2F1609406917733847

Office of the Director of National Intelligence (DNI). (2017). *National Security Adjudicative Guidelines* (Security Executive Agent Directive 4). Hentet fra https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf

Politiets sikkerhetstjeneste (PST). (2016). *Trusselvurdering 2016*. Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/trusselvurdering-2016.pdf

Politiets sikkerhetstjeneste (PST). (2018). *Trusselvurdering 2018.* Hentet fra https://www.pst.no/globalassets/artikler/trusselvurderinger/psts-trusselvurdering-2018.pdf

Politiets sikkerhetstjeneste (PST). (2020). *Nasjonal trusselvurdering 2020.* Hentet fra https://www.pst.no/globalassets/artikler/utgivelser/2020/nasjonal-trusselvurdering-2020-print.pdf

Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM), Politiet & Næringslivets Sikkerhetsråd (NSR) (2017). *Sikkerhet ved ansettelsesforhold - før, under og ved avvikling*. Hentet fra https://www.nsr-org.no/uploads/documents/Publikasjoner/sikkerhet_ved_ansettelsesforhold_2017_utskrift.pdf

Reason, J. (1997). *Managing the Risks of Organizational Accidents.* New York: Ashgate Publishing

Ryssdal, A. (2005). Rettsstaten under press. *Nytt Norsk Tidsskrift, 22*(1), 48-59. https://doi.org/10.18261/ISSN1504-3053-2005-01-04

Schiefloe, P.M. (2012). *En modell for samfunnssikkerhet* (22.juli-kommisjonen, notat 10/12). Hentet fra https://docplayer.me/14073065-Notat-10-12-en-modell-for-samfunnssikkerhet-professor-per-morten-schiefloe-dr-philos.html [Lest: 25.05.21].

Shechter, O.G. & Lang, E.L. (2011). *Identifying Personality Disorders that are Security Risks: Field Test Results* (PERSEREC TR 11-05). Hentet fra https://swapassessment.org/wp-content/uploads/2015/06/TR-11-05-Identifying-Personality-Disorders-that-are-Security-Risks-Fiel....pdf

Sikkerhetsloven. (2018). Lov om nasjonal sikkerhet (LOV-2018-06-01-24). Hentet fra https://lovdata.no

Smith, C. L., & Brooks, D. J. (2013). Security science: The theory and practice of security. Amsterdam: Elsevier, BH.

Thomas, E. (1997, 6. juli). Inside the mind of a spy. Hentet fra https://noir4usa.org/resources/inside-the-mind-of-a-spy/ [Lest: 07.05.21].

Wilder, U.M. (2017). The Psychology of Espionage. *Studies in Intelligence, 61*(2), 19-36. Hentet fra https://www.cia.gov/static/30b273c621d0896f13104ff48840b68f/psychology-of-espionage.pdf

Vedlegg

Vedlegg 1 - Sikkerhetsloven §8-4: Avgjørelse om klarering

En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket. Klareringsmyndigheten fatter avgjørelse om klarering.

I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur. Vurderingen skal gjøres på grunnlag av en personkontroll.

Klareringsmyndigheten skal se til at klareringssaken er så godt opplyst som mulig. Dersom det er tvil om en person er sikkerhetsmessig skikket, skal klareringsmyndigheten holde en sikkerhetssamtale med personen.

Opplysninger om følgende forhold kan tillegges vekt:

a) spionasje, planlegging eller gjennomføring av terror, sabotasje, attentat eller lignende, og forsøk på slik virksomhet
b) straffbare handlinger eller forberedelser eller oppfordringer til straffbare handlinger
c) 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.
d) forfalskning av eller feilaktig eller unnlatt framstilling av faktiske forhold som personen måtte
e) forså har betydning for sikkerhetsklareringen
f) misbruk av alkohol eller andre rusmidler
g) enhver sykdom som på medisinsk grunnlag kan gi forbigående eller varig svekkelse av påliteligheten, lojaliteten eller dømmekraften
h) kompromittering av skjermingsverdig informasjon eller brudd på sikkerhetsbestemmelser
i) nektelse eller unnlatelse av å gi personopplysninger om seg selv
j) ikke å orientere den autorisasjonsansvarlige om egne forhold av betydning for sikkerheten

k) nektelse av å gi taushetsløfte, tilkjennegivelse av ikke å ville være bundet av taushetsløfte eller nektelse eller unnlatelse av å delta i sikkerhetssamtale
l) økonomiske forhold som kan friste ham eller henne til å handle i strid med nasjonale sikkerhetsinteresser
m) forbindelse med organisasjoner som har ulovlig formål, og som kan true den demokratiske samfunnsordenen, eller som ansvar vold eller terrorhandlinger som akseptable virkemidler
n) manglende mulighet til å gjennomføre tilfredsstillende personkontroll
o) tilknytning til andre stater
p) annet som kan gi grunn til å frykte at en person vil kunne opptre i strid med nasjonale sikkerhetsinteresser

Politisk engasjement og annet lovlig samfunnsengasjement, som medlemskap i, sympati med eller aktivitet for lovlige politiske partier eller organisasjoner, skal ikke tillegges vekt i vurderingen av om en person er sikkerhetsmessig skikket.

Opplysninger om nærstående personer skal bare tillegges vekt dersom de er sikkerhetsmessig relevante.

Kongen kan gi forskrift om klarering og gjennomføring av sikkerhetssamtale.

Vedlegg 2 - «Adjudicative guidelines» (DNI, 2017)

ADJUDICATIVE GUIDELINE & DISQUALIFYING FACTOR
GUIDELINE A: ALLEGIANCE TO THE UNITED STATES
Conditions that could raise a security concern and may be disqualifying include:
(a) involvement in, support of, training to commit, or advocacy of any act of sabotage, espionage, treason, terrorism, or sedition against the United States; (b) association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts; and (c) association or sympathy with persons or organizations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to: (1) overthrow or influence the U.S. Government or any state or local government; (2) prevent Federal, state, or local government personnel from performing their official duties; (3) gain retribution for perceived wrongs caused by the Federal, state, or local government; and (4) prevent others from exercising their rights under the Constitution or laws of the United States or of any state.
GUIDELINE B: FOREIGN INFLUENCE
Conditions that could raise a security concern and may be disqualifying include:
(a) contact, regardless of method, with a foreign family member, business or professional associate, friend, or other person who is a citizen of or resident in a foreign country if that contact creates a heightened risk of foreign exploitation, inducement, manipulation, pressure, or coercion; (b) connections to a foreign person, group, government, or country that create a potential conflict of interest between the individual's obligation to protect classified or sensitive information or technology and the individual's desire to help a foreign person, group, or country by providing that information or technology; (c) failure to report or fully disclose, when required, association with a foreign person, group, government, or country; (d) counterintelligence information, whether classified or unclassified, that indicates the individual's access to classified information or eligibility for a sensitive position may involve unacceptable risk to national security; (e) shared living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion; (f) substantial business, financial, or property interests in a foreign country, or in any foreign-owned or foreign-operated business that could subject the individual to a heightened risk of foreign influence or exploitation or personal conflict of interest; (g) unauthorized association with a suspected or known agent, associate, or employee of a foreign intelligence entity;

(h) indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, inducement, manipulation, pressure, or coercion; and

(i) conduct, especially while traveling or residing outside the U.S., that may make the individual vulnerable to exploitation, pressure, or coercion by a foreign person, group, government, or country.

GUIDELINE C: FOREING PREFERENCE

Conditions that could raise a security concern and may be disqualifying include:

(a) applying for and/or acquiring citizenship in any other country;

(b) failure to report, or fully disclose when required, to an appropriate security official, the possession of a passport or identity card issued by any country other than the United States;

(c) failure to use a U.S. passport when entering or exiting the U.S.;

(d) participation in foreign activities, including but not limited to:

(1) assuming or attempting to assume any type of employment, position, or political office in a foreign government or military organization; and
(2) otherwise acting to serve the interests of a foreign person, group, organization, or government in any way that conflicts with U.S. national security interests;

(e) using foreign citizenship to protect financial or business interests in another country in violation of U.S. law; and

(f) an act of expatriation from the United States such as declaration of intent to renounce U.S. citizenship, whether through words or actions.

GUIDELINE D: SEXUAL BEHAVIOUR

Conditions that could raise a security concern and may be disqualifying include:

(a) sexual behavior of a criminal nature, whether or not the individual has been prosecuted;

(b) a pattern of compulsive, self-destructive, or high-risk sexual behavior that the individual is unable to stop;

(c) sexual behavior that causes an individual to be vulnerable to coercion, exploitation, or duress; and

(d) sexual behavior of a public nature or that reflects lack of discretion or judgment.

GUIDELINE E: PERSONAL CONDUCT

Conditions that could raise a security concern and may be disqualifying include:

(a) deliberate omission, concealment, or falsification of relevant facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine national security eligibility or trustworthiness, or award fiduciary responsibilities;

(b) deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative;

(c) credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but which, when considered as a whole, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information;

(d) credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of:

(1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information;
(2) any disruptive, violent, or other inappropriate behavior;

(3) a pattern of dishonesty or rule violations; and
(4) evidence of significant misuse of Government or other employer's time or resources;

(e) personal conduct, or concealment of information about one's conduct, that creates a vulnerability to exploitation, manipulation, or duress by a foreign intelligence entity or other individual or group. Such conduct includes:

(1) engaging in activities which, if known, could affect the person's personal, professional, or community standing;
(2) while in another country, engaging in any activity that is illegal in that country;
(3) while in another country, engaging in any activity that, while legal there, is illegal in the United States;

(f) violation of a written or recorded commitment made by the individual to the employer as a condition of employment; and

(g) association with persons involved in criminal activity.

GUIDELINE F: FINANCIAL CONSIDERATIONS

Conditions that could raise a security concern and may be disqualifying include:

(a) inability to satisfy debts;

(b) unwillingness to satisfy debts regardless of the ability to do so;

(c) a history of not meeting financial obligations;

(d) deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, expense account fraud, mortgage fraud, filing deceptive loan statements and other intentional financial breaches of trust;

(e) consistent spending beyond one's means or frivolous or irresponsible spending, which may be indicated by excessive indebtedness, significant negative cash flow, a history of late payments or of non-payment, or other negative financial indicators;

(f) failure to file or fraudulently filing annual Federal, state, or local income tax returns or failure to pay annual Federal, state, or local income tax as required;

(g) unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that are inconsistent with known legal sources of income;

(h) borrowing money or engaging in significant financial transactions to fund gambling or pay gambling debts; and

(i) concealing gambling losses, family conflict, or other problems caused by gambling.

GUIDELINE G: ALCOHOL CONSUPTION

Conditions that could raise a security concern and may be disqualifying include:

(a) alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace, or other incidents of concern, regardless of the frequency of the individual's alcohol use or whether the individual has been diagnosed with alcohol use disorder;

(b) alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, drinking on the job, or jeopardizing the welfare and safety of others, regardless of whether the individual is diagnosed with alcohol use disorder;

(c) habitual or binge consumption of alcohol to the point of impaired judgment, regardless of whether the individual is diagnosed with alcohol use disorder;

(d) diagnosis by a duly qualified medical or mental health professional (e.g., physician, clinical psychologist, psychiatrist, or licensed clinical social worker) of alcohol use disorder;

(e) the failure to follow treatment advice once diagnosed;

(f) alcohol consumption, which is not in accordance with treatment recommendations, after a diagnosis of alcohol use disorder; and

(g) failure to follow any court order regarding alcohol education, evaluation, treatment, or abstinence.

GUIDELINE H: DRUG INVOLVEMENT & SUBSTANCE MISUSE

Conditions that could raise a security concern and may be disqualifying include:

(a) any substance misuse (see above definition);

(b) testing positive for an illegal drug;

(c) illegal possession of a controlled substance, including cultivation, processing, manufacture, purchase, sale, or distribution; or possession of drug paraphernalia;

(d) diagnosis by a duly qualified medical or mental health professional (e.g., physician, clinical psychologist, psychiatrist, or licensed clinical social worker) of substance use disorder;

(e) failure to successfully complete a drug treatment program prescribed by a duly qualified medical or mental health professional;

(f) any illegal drug use while granted access to classified information or holding a sensitive position; and

(g) expressed intent to continue drug involvement and substance misuse, or failure to clearly and convincingly commit to discontinue such misuse.

GUIDELINE I: PSYCHOLOGICAL CONDITIONS

Conditions that could raise a security concern and may be disqualifying include:

(a) behavior that casts doubt on an individual's judgment, stability, reliability, or trustworthiness, not covered under any other guideline and that may indicate an emotional, mental, or personality condition, including, but not limited to, irresponsible, violent, self-harm, suicidal, paranoid, manipulative, impulsive, chronic lying, deceitful, exploitative, or bizarre behaviors;

(b) an opinion by a duly qualified mental health professional that the individual has a condition that may impair judgment, stability, reliability, or trustworthiness;

(c) voluntary or involuntary inpatient hospitalization;

(d) failure to follow a prescribed treatment plan related to a diagnosed psychological/psychiatric condition that may impair judgment, stability, reliability, or trustworthiness, including, but not limited to, failure to take prescribed medication or failure to attend required counseling sessions; and

(e) pathological gambling, the associated behaviors of which may include unsuccessful attempts to stop gambling; gambling for increasingly higher stakes, usually in an attempt to cover losses; concealing gambling losses; borrowing or stealing money to fund gambling or pay gambling debts; and family conflict resulting from gambling.

GUIDELINE J: CRIMINAL CONDUCT

Conditions that could raise a security concern and may be disqualifying include:

(a) a pattern of minor offenses, any one of which on its own would be unlikely to affect a national security eligibility decision, but which in combination cast doubt on the individual's judgment, reliability, or trustworthiness;

(b) evidence (including, but not limited to, a credible allegation, an admission, and matters of official record) of criminal conduct, regardless of whether the individual was formally charged, prosecuted, or convicted;

(c) individual is currently on parole or probation;

(d) violation or revocation of parole or probation, or failure to complete a court-mandated rehabilitation program; and

(e) discharge or dismissal from the Armed Forces for reasons less than "Honorable."

GUIDELINE K: HANDLING PROTECTED INFORMATION

Conditions that could raise a security concern and may be disqualifying include:

(a) deliberate or negligent disclosure of protected information to unauthorized persons, including, but not limited to, personal or business contacts, the media, or persons present at seminars, meetings, or conferences;

(b) collecting or storing protected information in any unauthorized location;

(c) loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium;
(d) inappropriate efforts to obtain or view protected information outside one's need to know;

(e) copying or modifying protected information in an unauthorized manner designed to conceal or remove classification or other document control markings;

(f) viewing or downloading information from a secure system when the information is beyond the individual's need-to-know;

(g) any failure to comply with rules for the protection of classified or sensitive information;

(h) negligence or lax security practices that persist despite counseling by management; and

(i) failure to comply with rules or regulations that results in damage to the national security, regardless of whether it was deliberate or negligent.

GUIDELINE L: OUTSIDE ACTIVITIES

Conditions that could raise a security concern and may be disqualifying include:

(a) any employment or service, whether compensated or volunteer, with:

(1) the government of a foreign country;
(2) any foreign national, organization, or other entity;
(3) a representative of any foreign interest; and
(4) any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology; and

(b) failure to report or fully disclose an outside activity when this is required.