Sikkerhetsstyringens utvikling

Med tillatelse fra: Forsvarets sikkerhetsavdeling & Joachimart

Masterstudium i samfunnssikkerhet

Universitetet i Stavanger

Oktober 2020

Per Ringstad

Forord

Denne oppgaven har gitt meg mulighet til å undersøke og skrive om temaer jeg har lang erfaring med fra yrkeslivet. Forebyggende sikkerhet har vært fagområdet mitt de siste 15 årene. Men jeg føler etter 10 år i klareringsmyndigheten i forsvarssektoren, hvor av fem som leder for denne virksomheten, en spesiell nærhet for fagfeltet personellsikkerhet. Denne nærheten, erfaring og kunnskap jeg har til forebyggende sikkerhet generelt, og personellsikkerhet spesielt, har tidvis gjort det krevende å holde egne meninger i sjakk. Samtidig mener jeg at den kunnskapen og de erfaringene jeg har innen forbyggende sikkerhet har gjort det mulig å tilnærme meg temaet på en annen måte, enn det som ville vært mulig uten denne kunnskapen og disse erfaringene. Arbeidet med oppgaven har også gjort det mulig å metodisk teste ut om tanker og meninger som har vokst frem gjennom de 15 årene kan forsvares med vitenskapelig argumentasjon.

Jeg vil rette en stor takk til de som har bidratt til denne oppgaven. Takk til nåværende og tidligere arbeidsgiver, som har gitt meg muligheten til å bruke tid på dette. Takk til ekspertene som lot meg teste mine funn og påstander på dem, og på den måten bidro til å kvalitetssikre funn og konklusjoner. Takk til min gode venn Tommy Bugge Hansen, som med sin fagkunnskap og gode evne til konstruktiv kritikk var en god sparringspartner underveis i arbeidet. En stor takk til professor og veileder Odd Einar Falnes Olsen for å ha hatt troen og fått meg på sporet, når jeg selv tvilte og vandret i alle mulige retninger.

Sist men ikke minst, en ekstra stor takk til kona som har støttet, oppmuntret og gitt meg rom til å studere. En snart femti år gammel student i full jobb er ikke alltid så til stede som de nærmeste fortjener. Takk!

Per Ringstad, 15. oktober 2020.

Sammendrag

1. juli 2001 trådte lov om forebyggende sikkerhet i kraft. Dermed ble det forebyggende sikkerhetsarbeidet i Norge for første gang forankret i en egen sikkerhetslov. 1. januar 2019 trådte den reviderte sikkerhetsloven, lov om nasjonal sikkerhet, i kraft. Med den nye loven er det lovmessigforankret flere nye begreper. Ett av disse er sikkerhetsstyring. Begrepet er ikke nytt innen forebyggende sikkerhet, men det er nytt i sikkerhetsloven.

I denne oppgaven undersøkes utviklingen av sikkerhetsstyring innenfor rammene av det nasjonale lovverket for forebyggende sikkerhet. Dette gjøres gjennom å studere offentlig tilgjengelige dokumenter i form av forarbeideider til begge sikkerhetslovene, sikkerhetslovene med relevante forskrifter, relevante veiledninger, åpne trussel- og risikovurderinger fra sikkerhetstjenestene og intervju med eksperter innen forebyggende sikkerhet om utviklingen av lovverket generelt, og fagfeltene sikkerhetsstyring og personellsikkerhet spesielt. Min egen 15-årige erfaring fra arbeid med forebyggende sikkerhet generelt og personellsikkerhet spesielt, har også vært av betydning for studien. Målet med oppgaven er, med fokus på virksomhetsnivået, å øke forståelsen for hvorfor sikkerhetsstyring har utviklet seg de siste 20 årene.

Forklaringen på hvorfor sikkerhetsstyring har utviklet de siste 20 årene blir gitt gjennom å besvare tre forskningsspørsmål:

- Hvordan har forebyggende sikkerhet utviklet seg de siste 20 årene?
- Hvordan har risikooppfatningen knyttet til personellsikkerhet utviklet seg de siste 20 årene?
- Hvordan kan en innside hendelse forklares fra et organisatorisk perspektiv?

High Reliability Organization (HRO) teorien og James Reasons Swiss Cheese model har dannet det teoretiske grunnlaget for studien. Det var spesielt overraskende hvor vanskelig det var å drøfte forskningsspørsmålet hvordan har risikooppfatningen knyttet til personellsikkerhet utviklet seg de siste 20. De innhentede dataene, om i all hovedsak stammet fra myndighetsnivået, fremsto som valide i den empiriske fremstillingen, men ble krevende å omsette når problemet skulle drøftes på virksomhetsnivå. Hvilken betydning myndighetens informasjon har for risikooppfatningen på virksomhets nivå, viste seg vanskelig å forankre vitenskapelig med både kvalitativ- og kvantitativ tilnærming til de tilgjengelige dataene.

Innholdsfortegnelse

Figurer:

Tabeller:

Forkortelser:

EOS-utvalget: Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste
EOS-tjenestene: Etterretnings- og sikkerhetstjenestene (ETJ, NSM og PST)
ETJ: Etterretningstjenesten
FD: Forsvarsdepartementet
JD: Justis- og beredskapsdepartementet
NSM: Nasjonal sikkerhetsmyndighet
NSR: Næringslivets sikkerhetsråd
PST: Politiets sikkerhetstjeneste
HRO: High Reliability Organizations (Høypålitelige organisasjoner)

Sentrale begreper:

Forebyggende sikkerhetstjeneste:

«At sikkerhetstjenesten er forebyggende, innebærer at sikkerhetstiltakene forutsettes planlagt og implementert før en trussel utløses eller materialiserer seg.» (Forsvarsdepartementet, 1997, s. 21)

Personellsikkerhet:

«Personellsikkerhet; tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres.» (Forsvarsdepartementet, 2001, § 1-2)

Sikkerhetsklarering:

«Sikkerhetsklarering er en avgjørelse tatt av klareringsmyndigheten om en persons antatte sikkerhetsmessige skikkethet for behandling av sikkerhetsgradert informasjon. Vurderingsgrunnlaget for sikkerhetsmessig skikkethet er bygget på opplysninger personen selv gir eller har gitt, og informasjon fra relevante registeropplysninger gjennom personkontrollundersøkelser.» (Nasjonal sikkerhetsmyndighet, 2019)

Autorisasjon:

«En autorisasjon er en godkjennelse man må få av autorisasjonsansvarlig i virksomheten for å få tilgang til sikkerhetsgradert informasjon og adgang til skjermingsverdige objekter og infrastruktur.» (Nasjonal sikkerhetsmyndighet, 2020)

Sikkerhetsgradert informasjon:

« En virksomhet som tilvirker informasjon, skal sikkerhetsgradere og merke informasjonen dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Følgende sikkerhetsgrader skal benyttes:

a) STRENGT HEMMELIG dersom det kan få helt avgjørende skadefølger

b) HEMMELIG dersom det kan få alvorlige skadefølger

c) KONFIDENSIELT dersom det kan få skadefølger

d) BEGRENSET dersom det i noen grad kan få skadefølger.»[1] (Forsvarsdepartementet, 2018, § 5-3)

[1] Sikkerhetsgradering etter sikkerhetsloven skrives med store bokstaver, jf. sikkerhetsloven § 5-3

Grunnleggende nasjonale funksjoner:

«Grunnleggende nasjonale funksjoner er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresse.»
(Forsvarsdepartementet, 2018, § 1-5)

1 Innledning

1.1 Bakgrunn

Første januar 2019 trådte ny sikkerhetslov, lov om nasjonalsikkerhet, med tilhørende forskrifter i kraft (Forsvarsdepartementet, 2018). Denne loven erstattet den tidligere sikkerhetsloven, lov om forebyggende sikkerhet av 20. mars 1998, som trådte i kraft i 1. juli 2001 (Forsvarsdepartementet, 1998). Den nye loven danner rammeverket for det forebyggende sikkerhetsarbeid i Norge.

4. februar 2020 la Politiets sikkerhetstjeneste (PST) frem sin årlige trusselvurdering, Nasjonal trusselvurdering 2020 (Politiets sikkerhetstjeneste, 2020), tett fulgt av Etterretningstjenestens trusselvurdering (ETJ) og Nasjonal sikkerhetsmyndighet (NSM) sin årlige risikovurdering. På samme måte som PST, fremhever NSM i sin Risiko 2020 (Nasjonal sikkerhetsmyndighet, 2020) og ETJ i Fokus 2020 (Etterretningstjenesten, 2020), fremmed etterretning som en vesentlig trussel mot vår nasjonale sikkerhet.
Omtrent samtidig med fremleggingen av de nasjonale trussel- og risikovurderingen, oppsto det en hendelse av stor nasjonal- og internasjonal betydning.

Hvilke hendelser som kategoriseres som krise avhenger av størrelse, omfang og ressursene som tas i bruk for å håndtere hendelsen (Engen, et. al, 2017, s. 262). Vinteren 2020 ble Norge og verden rammet av Covid-19 viruset. Størrelse, omfang og ressursene som ble tatt i bruk gjorde Covid-19 til en verdensomspennende krise (Engen, et. al, 2017, s. 262). Vi var i en ekstraordinær, uoversiktlig situasjon som måtte håndteres ved umiddelbar respons, hvor liv og helse i utgangspunktet var det som måtte beskyttes (Engen, et. al, 2017, ss. 300-301). Slik sårbarhetsutvalget, det såkalte Willochutvalget, beskrev det allerede på begynnelsen av 2000-tallet var vi utsatt for en hendelse som hadde potensiale til å true viktige verdier og

svekke virksomhetenes evne til å utføre sine samfunnsfunksjoner (Willochutvalget, 2000, s. 19). Virksomhetenes fleksibilitet, evnen til å tilpasse seg effektivt til foranderlige krav, ble satt på prøve (Reason, 2016).
For å motvirke spredning, og dermed redusere krisens omfang i Norge, iverksatte mange norske statlige- og private virksomheter utstrakt bruk av hjemmekontor. Også i virksomheter underlagt sikkerhetsloven ble dette tiltaket iverksatt. NSM var raskt ute med råd og veiledninger knyttet til sikkerhetsutfordringene som følger med hjemmekontorløsninger[2]. Fokuset rettet seg mot de digitale sårbarhetene knyttet til løsningene. Sårbarheter som trusselaktørene, blant annet fremmed etterretning, vil kunne utnytte.

«Det er ingen grunn til å tro at trusselaktører ikke vil utnytte det mulighetsrommet som nå oppstår når et stort antall virksomheter og deres brukere eksponerer sine systemer, data og tilganger gjennom bruk av løsninger med svak sikkerhet.»[3]

I en slik situasjon blir det krevende å opprettholde effekten av virksomhetenes barrierer. Barrierer som skal hindre at den initierende hendelsen faktisk blir en realitet (Aven, 2015, s. 46). Personellsikkerhet og digital-sikkerhet er to av virksomhetenes sikkerhetsmessige barrierer mot fremmed etterretning. Den skal motvirke innsidehendelser. .
Virksomhetenes daglige sikkerhetsmessige ledelse av klarert og autorisert personell, kan som følge av utstrakt bruk av hjemmekontor sies å ha gått fra å være sentralisert til desentralisert, hvor vurderinger og håndtering av risiko blir overlatt fra virksomheten til den enkelte ansatte. Den sikkerhetsmessige ledelsen, som innbefatter å detektere, identifisere og håndtere sikkerhetstruende virksomhet knyttet til personellet i virksomheten, utfordres når den potensielle angrepsflaten utvides til områder utenfor virksomhetenes kontroll. Tiltakene i barrieren personellsikkerhet, som skal fange opp endringer av betydning for forebyggende sikkerhet hos personellet, er i stor grad knyttet til nærhet og daglig fysisk kontakt md personellet. Risikoen for at personellsikkerhetsmessige hendelser ikke detekteres av virksomhetene kan hevdes å øke som følge av fravær av nærhet og daglig fysisk kontakt. Når konsekvensene av Covid-19 kan bli konkurs hos virksomheter som er leverandører til sikkerhetsgraderte anskaffelser, som igjen resulterer i permitteringer og oppsigelser, så øker de personellsikkerhetsmessige sårbarhetene ytterligere. Virksomhetene og deres ledere må både håndtere usikkerhetene knyttet til virksomhetenes overlevelse, ivaretagelsene av sine

[2] https://nsm.no/aktuelt/mer-hjemmekontor-store-muligheter-men-ogsa-risikoer
[3] https://nsm.no/aktuelt/mer-hjemmekontor-store-muligheter-men-ogsa-risikoer

ansatte og kunder, i tillegg til en endret sikkerhetssituasjon. For Covid-19 har på kort tid gitt endringer i trussel- og risikobildet. Sikkerhetslovens fleksibilitet, sikkerhetsstyringen og personellsikkerheten hos virksomhetene er satt på prøve, i en krisesituasjon som utnyttes av trusselaktører til aktiv kartlegging av sårbarheter[4].

Covid-19 har medført sikkerhetsmessige utfordringer. Samtidig er ikke utfordringer knyttet til personellsikkerhet og økonomi, eller sikkerhetsstyring ukjente og enestående for Corona-krisen. NATO Cooperative Cyber Defence Centre of Excellence (CCDECOE) publiserte i 2015 sin Insider Threat Study, hvor "Financial need or greed" angis som en viktig motivasjonsfaktor i insidesaker. (NATO Coopertive Cyber Defence Centre of Excellence (CCDECOE), 2015). Dette samsvarer med Ivan Homoliak et. al sin studie "Insight Into Insiders and IT: A survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures, hvor økonomiske motiver angis å være en av tre hovedmotivasjoner for utøvelse av innsidervirksomhet (Homoliak et. al, 2019). En studie som forøvrig, blant annet, søker å kategorisere tidligere heterogene innsider studier.

NSM har i lengre tid uttrykt bekymring knyttet til både personellsikkerhet og sikkerhetsstyring. Denne bekymringen kom tydelig frem i Risiko 2019, hvor disse områdene omtales som to av seks risikofaktorer (Nasjonal sikkerhetsmyndighet, 2019, s. 7).

I august 2020 ble en ansatt i DNV GL pågrepet av PST og deretter siktet for overlevering av informasjon til Russiske myndigheter[5]. Tidligere på året ble to forskere ved NTNU siktet for datainnbrudd, mistenkt for ulovlig lekkasje til Iran[6]. Disse to hendelsene var ikke Covid-19 relatert, og de involverte var ikke sikkerhetsklarert. Men fremmed etterretning hadde utnyttet et mulighetsrom for å få tilgang til hemmeligheter, og sammen med Covid-19 gjør dette både sikkerhetsstyring og personellsikkerhet til dagsaktuelle tema.

1.2 Problemstilling

Denne oppgaven har gjennom en historisk tilnærming til hensikt å undersøke årsakene til endringene innen sikkerhetsstyring, og om disse årsakene gjenspeiles i rammebetingelsene for utøvelse av personellsikkerhet knyttet til innsiderisikoen. Vi fikk en ny sikkerhetslov i 2019.

[4] https://www.tv2.no/a/11392834/
[5] https://www.tv2.no/a/11616792/
[6] https://www.nrk.no/trondelag/ntnu-begynte-a-mistenke-de-to-siktede-forskerne-allerede-for-ett-ar-siden-1.14869687

Den gamle loven, som også var den første sikkerhetsloven i Norge, ble utgitt i 2001. Det foreligger mye forskning innen risikostyring, men nasjonalt finnes det lite forskning rettet mot sikkerhetsstyring og personellsikkerhet. Denne oppgaven har følgende problemstilling:

Hvorfor har sikkerhetsstyring innen forebyggende sikkerhet utviklet seg de siste 20 årene?

Det er formulert tre forskningsspørsmål som skal bidra til å undersøke denne problemstillingen. For å se hvorfor det har vært en utvikling er det nødvendig å se på om det har vært noen utvikling, og i så fall hvordan rammene for sikkerhetsstyring har utviklet seg. Dette har ledet frem til det første forskningsspørsmålet:

Hvordan har forebyggende sikkerhet utviklet seg de siste 20 årene?

For å kunne besvare hvorfor sikkerhetsstyringen har utviklet seg, vil det være interessant å forsøke å se hvordan sikkerhetsstyringen har utviklet seg i forhold til de oppfattede risikoene. Forebyggende sikkerhet er et omfattende fagfelt, hvor det er forsket mye på flere av områdene, men i norsk sammenheng finnes lite forskning på personellsikkerhet. Personellsikkerhet ble derfor et fagfelt jeg ønsket å inkludere i denne studien, og ble derfor en naturlig avgrensning for oppgavens tilnærming til risikooppfatning som er et relevant tema for forskningsspørsmål knyttet til utviklingen av sikkerhetsstyring. Dette har ledet frem til det andre forskningsspørsmålet:

Hvordan har risikooppfatningen knyttet til personellsikkerhet utviklet seg de siste 20 årene?

Personellet er både en viktig ressurs, men også en potensiell sårbarhet, for sikkerheten hos virksomhetene. Personellsikkerhet er derfor et vesentlig element i virksomhetenes sikkerhetsstyring, hvor personellsikkerhet skal motvirke trusler, og redusere risiko knyttet til innsidevirksomhet. Forståelsen av hvordan innsidehendelser oppstår er derfor vesentlig i forhold både utviklingen av sikkerhetsstyring og risikooppfatningen knyttet til personellsikkerhet. Tidligere var det sparsomt med offentlig tilgjengelig norsk informasjon knyttet til personellsikkerhet, og veiledning om hvordan virksomhetene skulle praktisere sitt personellsikkerhetsarbeid utover det man kunne lese seg til fra lov, forskrift og autorisasjonshåndboka til NSM. De senere år har EOS-tjenestene, men også andre som for eksempel DNV på vegne av Petroleumstilsynet (Ptil), utarbeidet temarapporter og veiledere

knyttet til innsidertrusselen, en trussel som skal håndteres gjennom personellsikkerhetsmessige tiltak (Det norske veritas (DNV GL), 2019). Forskningen disse dokumentene er basert på stammer i all hovedsak fra utlandet, og retter seg mot sårbarheter og egenskaper hos enkelt individet som årsaksforklaring for innsidervirksomhet. Forskning knyttet til årsaksforklaring på innsidevirksomhet fra et organisatorisk perspektiv, hvor personellsikkerhet settes inni rammene for sikkerhetsstyring er det sparsommelig med. Dette har ledet frem til det tredje og siste forskningsspørsmålet:

Hvordan kan innsiderhendelser forklares fra et organisatorisk perspektiv?

Avgrensning

Oppgaven vil, i tillegg til personellsikkerhet, avgrenses til sikkerhetsstyring på virksomhetsnivå. En virksomhet skal i denne oppgaven forstås som er en organisasjon, statlig, kommunal eller privat, som behandler sikkerhetsgradert informasjon, råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner (Forsvarsdepartementet, 2018, § 1-3).
Oppgaven avgrenses derfor til sikkerhetslovens virkeområde og virksomheter omfattet av sikkerhetsloven, men siden rammene for sikkerhetsstyring legges av myndighetene vil myndighets nivået allikevel omhandles når dette er nødvendig for sammenheng og kontekst. Dermed blir sikkerhetsloven, dens forskrifter og forarbeider også det primære legale rammeverket for besvarelse av problemstillingen. Siden sikkerhetslovens hovedformål er trygging av våre nasjonale sikkerhetsinteresser, så avgrenses også oppgaven til trusselaktører knyttet til statlige etterretningstjenester, som retter sin sikkerhetstruende virksomhet mot virksomheter av betydning for nasjonale sikkerhetsinteresser (Forsvarsdepartementet, 2018, § 1-1). Dette betyr at innsidervirksomhet som rammer nasjonale sikkerhetsinteresser er et relevant tema for oppgaven. Som følge av at det er sparsommelig med informasjon om innsidehendelser på norsk jord, blant annet fordi slike saker ofte er forbundet med hemmelighold, så vil det allikevel benyttes eksempler fra innsidehendelser som ikke nødvendigvis knytter seg til nasjonale sikkerhetsinteresser. Men det legges til grunn som premiss for å bruke dem at PST har, eller har hatt, ansvaret for etterforskningen. Fordi

1.3 Tidligere forskning

Allerede i forarbeidene til den første sikkerhetsloven ble det påpekt at det forelå lite forskning innen forebyggende sikkerhet i Norge.

«Det mangler grunnleggende studier og forskning for å trekke entydige konklusjoner mht hvordan den norske sikkerhetstjenesten har virket, sammenlignet med den teoretiske fremstilling som er gitt ovenfor. Det vil derfor bare være grunnlag for å gi enkelte skjematiske og grove trekk i dette bildet.» (Forsvarsdepartementet, 1997, s. 22)

Innenfor forebyggende sikkerhet er det flere fagfelt hvor det fortsatt er begrenset med forskning. Personellsikkerhet er et slikt fagfelt. Det finnes riktig nok enkelte masteroppgaver innenfor temaet, blant annet, Jon Petter Syvertsen sin masteroppgave Insider Threat (Syvertsen, 2007). Men mye av grunnlaget for vår nasjonale tilnærming til personellsikkerhet er basert på forskning fra andre kanter av verden, blant annet, England og USA.

Det engelske Centre for Protection of National Infrastructure (CPNI) publiserte i 2009 funnene fra sin Insider Data Collection Study (Centre for Protection of National Infrastructure, 2013). Rapporten etter denne studien er senere blitt oppdatert, sist i 2013. Studien kategoriserte uautorisert avsløringer av sensitiv informasjon, prosesskorrupsjon, hjelpe en tredjepart til å få tilgang til en organisasjons verdier, fysisk sabotasje, og sabotasje på IT eller annet elektronisk utstyr, som fem hovedtyper av innsideraktivitet. Videre identifiserte den personlige og felles mønstre knyttet demografi hos innsidere basert på de mer enn 120 undersøkte innsidesakene, og ikke minst ble motivet i disse sakene identifisert. Blant annet, viste studien at menn var overrepresentert (82%), at i ca. halvparten av sakene var innsideren mellom 31 og 45 år, og at de aller fleste var fast ansatte (Centre for Protection of National Infrastructure, 2013, s. 8). Når det gjaldt motivasjonen for de gjennomførte innsidehandlingene så var 47% motivert av økonomi, 20% av ideologi, 14% av et behov for anerkjennelse, 14% som følge av lojalitet til andre enn arbeidsgiver, og 6 % hadde hevnmotiver (Centre for Protection of National Infrastructure, 2013, s. 9).

The Defense Personnel and Security Research Center (PERSEREC) i USA sin forskning på personellsikkerhet, har resultert i et mer enn 400 siders dokument, Adjudicative Desk Reference (ADR), som er ment som et hjelpemiddel for personell som jobber med

personellsikkerhet. Dokumentet gir ikke bare en opplisting av hva som trigger innsidehandlinger på individnivå. Det gir også en forklaring på hvorfor disse triggerne er relevante for vurderingen av individkarakteristikker, som nyttes for bedømmingen av en persons sikkerhetsmessige skikkethet til å kunne få tilgang til hemmeligheter. Sikkerhetsloven, både den nye og den gamle, lister i henholdsvis § 8-4 og § 21 opp hvilke forhold som er relevante for vurderingen av en persons sikkerhetsmessige skikkethet. Disse samsvarer i stor grad med det man finner i PERSEREC sin Adjudicative Desk Reference (The Defense Personnel and Security Research Center (PERSEREC), 2014).

Petroleumstilsynet (Ptil) ga i 2019 Det norske Veritas og Germanischer Lloyd (DNV GL), i oppdrag å utarbeide en rapport om innsiderisiko i petroleumsnæringen. Bakgrunnen for dette var Ptil sine erfaringer fra tilsyn og økt fokus på innsidetrusselen fra sikkerhetsmyndighetenes side. Det var fra Ptil sin side et behov for å øke eget og petroleumsnæringens kunnskapsgrunnlag om innsiderisiko (Det norske Veritas og Germanisher Lloyd (DNV GL), 2019). Rapporten er basert på mye utenlandsk forskning på området, men den gir et grunnlag for fenomenforståelse og tilnærming til beste praksis, som kan føre til bedre og mer systematisk styring av innsiderisiko basert på norske forhold.

Selv om det på nasjonalt nivå finnes lite forskning innen personellsikkerhet, så har myndighetene utgitt publikasjoner knyttet til temaet. PST, NSM, Politiet og Næringslivets Sikkerhetsråd, ga i 2017 ut en veileder for sikkerhet ved ansettelsesforhold. Bakgrunnen for veilederen var sikkerhetstjenestenes egne rapporter, hvor innsiderrisikoen hadde fått økt oppmerksomhet de senere årene. Dette var et tiltak på organisatorisk nivå for å gi norske virksomheter økt bevissthet rundt innsiderisiko. Veilederen skulle gjøre dem bedre i stand til å håndtere denne risikoen før, under og ved avvikling av ansettelsesforhold samt ved innleie av ulike tjenester (PST mfl., 2017). Veilederen retter seg alle mot virksomheter, enten de er underlagt sikkerhetsloven eller ikke. NSM fulgte i 2019 opp med en egen temarapport om innsiderisko som viser at dette også er problematikk som kan ramme norske virksomheter, selv om bare to av syv eksempler i rapporten viser til innsidehendelser i Norge. Veilederen og rapporten gir til sammen et grunnlag for norske virksomheter til å forstå tilnærme seg problematikken, innenfor rammene av norsk lov. I forhold til forskning, så er det et fellestrekk ved de to dokumentene at de ikke henviser til hvilken forskning som ligger til grunn for innholdet i dokumentene.

Høsten 2020 ble NSMs grunnprinsipper for personellsikkerhet publisert[7]. Disse grunnprinsippene er ment å være tverrsektorielle, og et utgangspunkt for alle virksomheter som ønsker å skape et helhetlig system for personellsikkerhet[8]. Dette produktet ble offentliggjort for sent til at det kunne inkluderes i arbeidet med denne oppgaven, men det er et vesentlig tillegg i kunnskapsformidlingen rundt personellsikkerhet og dets eksistens er derfor relevant å nevne.

[7] https://nsm.no/aktuelt/grunnprinsipper-for-fysisk-sikkerhet-personellsikkerhet-og-sikkerhetsstyring
[8] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-personellsikkerhet/introduksjon/

2 Kontekst

Sikkerhetstruende hendelser nasjonalt og internasjonalt har bidratt til en forståelse av at risiko- og trusselbildet er dynamisk. I dette bildet er etterretningstrusselen et helt sentralt element. Derfor vil det i det påfølgende først redegjøres for denne trusselen, som er et eksempel på sikkerhetstruende virksomhet, og etter sikkerhetsloven skal håndteres på individs-, virksomhets- og myndighetsnivå. Deretter vil det, siden denne oppgaven retter seg mot sikkerhetsstyring og tiltak på strukturelt og organisatorisk nivå, redegjøres for de mest sentrale aktørene knyttet til forebyggende sikkerhet på virksomhets- og myndighetsnivå.

2.1 Etterretningstrusselen

Etterretningstrusselen har, siden den første åpne trusselvurderingen til PST i 2004, blitt beskrevet som en alvorlig trussel mot Norge. For å forstå hvilken trussel fremmed etterretning utgjør er tidligere sjef for PST, Benedicte Bjørnland, sin uttalelse til media et viktig supplement. Her bekrefter hun etterretningstrusselen potensiale til å rokke ved vår territoriale integritet:

«Selv om en terrorhendelse vil være et nasjonalt traume, så vil vi som nasjon overleve og gå videre. Men ulovlig etterretningsvirksomhet har potensiale i seg til å forringe vår evne til å beholde territoriet.»[9]

Når det også er en trussel som retter seg mot personell, og utfordrer sikkerhetsstyringen knyttet til personellsikkerhet i virksomhetene, så er det naturlig at det er mot denne trusselen denne oppgaven avgrenses.

Utenlandske etterretningstjenester

Som Andrew Christopher skriver i boka, The Secret World: A History of Intelligence (Christopher, 2019), så er det å samle informasjon og finne hemmeligheter for å bygge kunnskap om motstandere som kan utnyttes til egen fordel, noe mennesker, stater og

[9] https://www.abcnyheter.no/nyheter/norge/2018/04/10/195386264/pst-sjefen-frykter-spionasje-mer-enn-terror

organisasjoner har drevet med oppgjennom hele menneskehetens historie. Kunnskap er makt og denne makten kan avgjøre hvem som går seirende ut av en krig, og den kan brukes rundt forhandlingsbordet til å avverge krig. De aller fleste nasjoner har egne etterretningstjenester til å forestå denne innhentingen av etterretninger[10].

Men, det er ikke bare i situasjoner hvor man ruster til krig, og den territoriale integriteten er truet, at etterretningstjenestene samler informasjon. Som for vår egen etterretningstjeneste, er innhenting og bearbeiding av informasjon om verden rundt oss til beslutningsstøtte for politiske myndigheter, også en hovedoppgave for utenlandske etterretningstjenester (Forsvarsdepartementet, 2020). Informasjonen som innhentes kan, for eksempel, brukes til å komme Norge i forkjøpet i utenrikspolitiske saker eller påvirke norsk politikk slik at den i større grad samsvarer med deres egne interesser (Politiets sikkerhetstjeneste, 2020).
Noe av denne innhentingen foregår fordekt, og noe av den foregår åpent. Som en del av den fordekte virksomheten, vil det å påvirke og rekruttere personer til å bidra til deres innhenting være en viktig oppgave for utenlandske etterretningstjenester i Norge. Gjennom kartlegging vil de søke å rekruttere personer på innsiden av virksomheter knyttet til norsk næringsliv, forsvar og beredskap, og norske forskningsmiljøer, i tillegg til personer knyttet til myndighetenes beslutningsprosesser (Politiets sikkerhetstjeneste, 2020).

«Rekruttering eller plassering av spioner på innsiden av norske virksomheter er en kjerneoppgave for utenlandske etterretningstjenester.» (Politiets sikkerhetstjeneste, 2020)

PST har flere ganger i sine årlige åpne trusselvurderinger, senest i 2020, presentert hvordan trusselen fra utenlandske etterretningstjenester vil oppleves for enkeltindivider som søkes rekruttert, hvor press er et virkemiddel for rekrutering (Politiets sikkerhetstjeneste, 2020).

«I 2018 forventer vi at enkeltpersoner blir forsøkt rekruttert som kilder og agenter, og at norske virksomheter blir utsatt for kartlegging og nettverksangrep. I tillegg vil beslutningsprosesser bli forsøkt påvirket og undergravet, og norske virksomheter bli utsatt for forsøk på ulovlig anskaffelse av kunnskap og teknologi.» (Politiets sikkerhetstjeneste , 2018)

[10] Ordet etterretning kommer opprinnelig av å rette seg etter noe, men brukes nå også om nyheter, meddelelser og andre opplysninger. (https://www.sprakradet.no/svardatabase/sporsmal-og-svar/ta-til-etterretningorientering/.)

Rekrutteringsforsøk av innsidere kan også rettes mot eget lands borgere som jobber i Norge. Dette kan ha skjedd før de flyttet hit eller når de senere besøker hjemlandet. Rekrutteringen vil da ofte skje i form av press, og med medhold i landets lover som i enkelte tilfeller forplikter privatpersoner, bedrifter, organisasjoner og statlige virksomheter til å samarbeide med landets etterretningstjenester (Politiets sikkerhetstjeneste , 2018).

Innsideren

Tradisjonelt har innsiderbegrepet vært knyttet til finansnæringen[11], og det at personer i finansverdenen utnytter sin innsidekunnskap om bedrifter til å kjøpe seg inn i, eller selge seg ut av, virksomheter på et gunstig tidspunkt. Men som vist, har innsidebegrepet de senere årene fått en bredere betydning og innhold enn dette.
Politiet, Nasjonal sikkerhetsmyndighet, Næringslivets sikkerhetsråd og
Politiets sikkerhetstjeneste har gjennom sin felles veileder til sikkerhet ved ansettelses forhold utarbeidet en omforent definisjon:

«Innsidere er personer med autorisert adgang til en bedrift, som misbruker kunnskap og tilgang, til å utføre handlinger som påfører virksomheten skade eller tap.» (PST mfl., 2017)

Innsidere kan deles inn i tre kategorier, infiltratøren, den selvmotiverte og den rekrutterte. Infiltratøren er den som er vanskeligst å avsløre. Dette er en person som har fått opplæring og trening, og det er gjerne laget en bakgrunnshistorie som tåler både bakgrunnssjekk og personkontroll. Hos denne står det gjerne en statlig etterretningstjeneste bak, som gjennom å infiltrere en trenet person hos en virksomhet utnytter tilgangen denne gis på en måte som skader virksomheten. Den selvmotiverte innsideren er en person som av egen fri vilje og ut fra egen motivasjon, utnytter de tilganger personen har til å utføre handlinger som påfører virksomheten skade eller tap. Den rekrutterte innsideren, er en person som frivillig eller som følge av press velger å jobbe for en tredjepart, for eksempel en statlig etterretningstjeneste (PST mfl., 2017).

Hva som motiverer en innsider er det ikke mulig å lage en uttømmende oversikt over, men innsideraktiviteten er knyttet enten til innsiderens egne behov og motivasjon, eller press, manipulasjon og villedning fra en tredjepart (PST mfl., 2017).

[11] https://lovdata.no/dokument/NL/lov/2007-06-29-75/KAPITTEL_2-1-1#§3-3

Det er ikke mange offentlig tilgjengelige eksempler på saker knyttet til utenlandsk etterretning sine aktiviteter på norsk jord, eller deres bruk av innsidere. Treholt saken er antagelig den mest kjente, selv om han ble omtalt som spion og ikke innsider. Men det finnes også eksempler fra nyere tid. Eksempelvis gikk PST august 2020 til det skritt å sikte en mann for spionasje etter flere møter med det PST mener er en russisk etterretningsoffiser. Selv om den siktede ikke hadde sikkerhetsklarering så er eksemplet, all den tid han blir funnet skyldig, relevant for hvordan fremmed etterretning opererer på norsk jord[12]. Han skal ha hatt flere møter med russisk etterretning, og har erkjent å ha mottatt penger for informasjon. Mannen er ansatt hos DNV, og skal gjennom sitt arbeid der ha hatt kontakt med den norske forsvarsindustrien og forskere innen avansert forsvarsteknologi[13]. Han omtales i media som spionsiktet, men handlingene som har ført frem til pågripelsen og siktelse kan betegnes som innsidevirksomhet og han, hvis han dømmes for forholdet som en innsider.

«En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.» (Nasjonal sikkerhetsmyndighet, 2019, s. 9)

Det er denne forståelsen av begrepet innsider, som er mer detaljert i sin beskrivelse enn den man finner i den felles veilederen i sikkerhet ved ansettelsesforhold, som legges til grunn i denne oppgaven (PST mfl., 2017).

Resultatet av siktelsen er ennå ikke klar, men hendelsen gir grunnlag for å hevde at PST sine trusselvurderinger knyttet til utenlandske etterretningstjenester, som også underbygges av ETJs Fokus 2020 og NSMs Risiko 2020, er realistiske.

2.2 Aktørene

For å beskytte seg mot truslene som retter seg mot våre nasjonale sikkerhets interesser, så har staten utrustet seg med verktøy i form av etterretnings- og sikkerhetstjenester til å motvirke disse truslene. I det følgende vil det gis en redegjørelse for de norske etterretnings- og sikkerhetstjenestene, de såkalte EOS-tjenestene, og deres styrende organer (EOS-utvalget, 2020). For å beskytte borgerne mot overgrep fra staten, har staten også utrustet seg med

[12] https://www.dn.no/teknologi/kongsberg-maritime/harsharn-singh-tatghar/dnv-gl/spionsiktet-nordmann-jobbet-for-kongsberg-maritime/2-1-860651
[13] https://www.dn.no/innenriks/spionsiktet-mann-skal-ha-mott-russisk-agent-pa-restaurant-i-oslo/2-1-859182

verktøy for å motvirke trusselen for slike overgrep. Det vil derfor også bli redegjort for EOS-utvalget, som utøver kontroll med EOS-tjenestene.

Etterretnings- og sikkerhetstjenestene (EOS-tjenestene)

Selv om den virksomheten som forvalter en verdi, som er underlagt sikkerhetsloven, har et selvstendig ansvar for å beskytte og sikre denne verdien. Så har staten, gjennom EOS-tjenestene, verktøy til rådighet for å motvirke etterretningstrusselen mot norske nasjonale sikkerhetsinteresser. I Norge består EOS-tjenestene, i all hovedsak av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA) (EOS-utvalget, 2020).

De norske EOS-tjenestene har forskjellige organisatoriske oppheng, hjemmelsgrunnlag og ansvarsområde. Eksempelvis er det Etterretningstjenesten og Politiets sikkerhets- tjeneste (PST) som har ansvar for å foreta trusselvurderinger for Norge og norske interesser i utlandet. Norges grenser markerer et vesentlig skille, hvor Etterretningstjenesten har ansvar for utenlandsetterretning, mens PST har ansvar for innlandsetterretning. Nasjonal sikkerhetsmyndighet er ansvarlig for nasjonale risikovurderinger, inkludert rapporter med spesielt fokus på trusler i det digitale domenet (Traavikutvalget, 2016, s. 50). I det følgende redegjøres det overordnet om de norske EOS-tjenestene.

Etterretningstjenesten (ETJ)

Etterretningstjenestens forløpere befant seg i Forsvarets Overkommando avdeling II, Etterretningskontoret (Traavikutvalget, 2016, s. 37).

ETJ er Norges militære og sivile utenlands etterretningstjeneste og ligger organisatorisk under Forsvarsdepartementet, hjemmelsgrunnlaget for tjenesten ligger i etterretningsloven. Tjenestens primæroppgaver er å understøtte norske myndigheter med informasjon og vurderinger om utenriks-, sikkerhets- og forsvarspolitiske forhold, fremskaffe informasjon og varsle om forhold som kan true Norge og norske interesser, og støtte Forsvarets operasjoner hjemme og ute[14].

ETJ sitt ansvarsområde ligger utenfor landets grenser, og tjenestens muligheter til å operere på norsk jord er meget begrenset.

[14] https://forsvaret.no/organisasjon/etterretningstjenesten

Politiets sikkerhetstjeneste (PST)

Etter politireformen tidlig på 2000-tallet, endret Politiets overvåkningstjeneste (POT) navn til Politiets sikkerhetstjeneste (PST) 1. januar[15]. På norsk jord er det PST sitt ansvar å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. Dette gjør tjenesten ved å innhente informasjon om mulige trusselaktører, utarbeide ulike analyser og trusselvurderinger, etterforskning og andre operative tiltak, i tillegg til å drive rådgivning [16]. Politilovens § 17 c. Særlige oppgaver for den sentrale enhet i Politiets sikkerhetstjeneste, sier a PST skal utarbeide trusselvurderinger til bruk for politiske myndigheter (Justis- og beredskapsdepartementet, 1995).

PST er organisatorisk underlagt Justisdepartementet.

Nasjonal sikkerhetsmyndighet (NSM)

Forsvarets Overkommando Sikkerhetsstaben var forløperen til Nasjonal sikkerhetsmyndighet (NSM), og Forsvarets sikkerhetsavdeling (Traavikutvalget, 2016, s. 37). NSM ble opprettet i 2003 etter forslag fra Forsvarsdepartementet, og har siden vært sektorovergripende direktorat, fagmyndighet og tilsynsmyndighet innen forebyggende sikkerhet[17]. NSM har ansvar for å gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid. Veiledere, håndbøker, og temarapporter innen forebyggende sikkerhet, er viktige produkter fra NSM, i tillegg til årlig nasjonal risikovurdering basert blant annet på PST og ETJ sine trusselvurderinger.

Forsvarets sikkerhetsavdeling (FSA)

FSA ble opprettet samme år som NSM, og er den andre sikkerhetstjenesten som har sitt utspring i Forsvarets Overkommando Sikkerhetsstaben (Traavikutvalget, 2016, s. 37). FSA har ansvar for forebyggende sikkerhet i Forsvaret, og innenfor enkelte områder også for forebyggende sikkerhet i hele forsvarssektoren, men har også ansvar for militær kontraetterretning ved og på militært område. Ved mistanke om ulovlig etterretningsvirksomhet, er dette noe som skal faller inn under PST sitt ansvarsområde, og FSA er da pliktig å informere PST (Traavikutvalget, 2016, s. 39).

[15] https://nsd.no/polsys/data/forvaltning/enhet/13510/endringshistorie
[16] https://www.pst.no/temasider/oppgaver/
[17] https://www.nsm.stat.no/om-nsm/

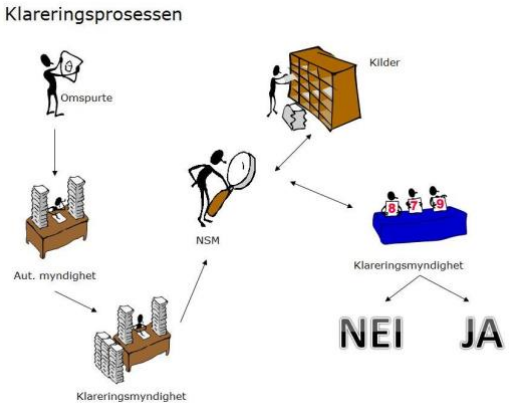
Klareringsmyndighetene

Klareringsmyndighetene er, i all hovedsak, organisert med en klareringsmyndighet for sivil sektor, med navnet Sivil klareringsmyndighet, og en for forsvarssektoren i FSA. I tillegg er de øvrige EOS-tjenestene, Statsministerens kontor og domstolene, i henhold til klareringsforskriften, klareringsmyndigheter for eget personell og personell tilknyttet deres virksomhet (Forsvarsdepartementet, 2018, § 1).

Klareringsmyndighetene er gitt myndigheten til å vurdere og avgjøre om personer som søkes sikkerhetsklarert er sikkerhetsmessig skikket til å gis tilgang til sikkerhetsgradert informasjon. Klareringsprosessen starter med at en person, etter vurdering fra autorisasjonsansvarlig, har et tjenstlig behov for sikkerhetsklarering. Autorisasjonsansvarlige er ofte personer med lederansvar i virksomhetene, som er gitt ansvaret for å autorisere sikkerhetsklarert personell, for tilgang til virksomhetens sikkerhetsgraderte informasjon. Hvordan virksomhetene organiserer autorisasjonsprosessen er opp til virksomheten selv å avgjøre, men utgangspunktet er at dette er et lederansvar (Forsvarsdepartementet, 2018, § 8-9). Sikkerhetsklarering og autorisasjon er sammen med daglig sikkerhetsmessig ledelse viktige tiltak i barrieren personellsikkerhet. Sikkerhetsklarering er en myndighetsoppgave, og selv om denne oppgaven retter seg mot virksomhetsnivået, og denne barrieren omfatter både myndighets-og virksomhetsnivået, så er det for helhetsforståelsen tjenlig å gi en overordnet redegjørelse av klareringsprosessen.

Virksomhetene som har behov for å sikkerhetsklarere personell fremsender en personopplysningsblankett, som er utfylt av den som skal klareres, til klareringsmyndigheten. For tilgang til nasjonal sikkerhetsgradert informasjon gradert KONFIDENSIELT, HEMMELIG og STRENGT HEMMELIG[18] kreves det sikkerhetsklarering og autorisasjon (Forsvarsdepartementet, 2018, § 8-2, jf § 5-3).

[18] Sikkerhetsgradering etter sikkerhetsloven skrives med store bokstaver, jf. sikkerhetsloven § 5-3



Figur 1: klareringsprosessen (NSM, 2011, s. 6)[19]

Figur 1 illustrerer klareringsprosessen. Klareringsmyndigheten ber NSM om personkontroll, som vil si at NSM innhenter opplysninger i ulike registre om personen som søkes sikkerhetsklarert. De innhentede opplysningene sendes til klareringsmyndigheten. Klareringsmyndigheten har mulighet til å, ved behov, innhente ytterligere opplysninger og kalle den som skal sikkerhetsklareres inn til sikkerhetssamtale. Basert på vurdering av tilgjengelige opplysninger, fatter klareringsmyndigheten avgjørelse om personen har den nødvendige, lojalitet, pålitelighet og sunne dømme kraft til å kunne gis sikkerhetsklarering eller ikke.

Gir klareringsmyndigheten den klareringen det er anmodet om, så kan virksomhetene autorisere personen for dette nivået.
Hvis en person bare skal ha tilgang til informasjon som er sikkerhetsgradert BEGRENSET, krever ikke dette en forutgående sikkerhetsklarering (Forsvarsdepartementet, 2018, § 8-2). Autorisasjonsansvarlige har da i all hovedsak, kun den informasjonen den som skal autoriseres fremlegger i autorisasjonssamtalen som grunnlag for sin avgjørelse om autorisasjon. Men ved autorisasjon av utenlandske statsborgere, personer med dobbelt statsborgerskap og statsløse for BEGRENSET[20], så kan den autorisasjonsansvarlige be klareringsmyndigheten om en vurdering av hjemlandets sikkerhetsmessige betydning. Er personen statsborger av en stat som PST mener utgjør en høy sikkerhetsrisiko for Norge, så må den autorisasjonsansvarlige innhente samtykke til autorisasjon fra klareringsmyndigheten (Forsvarsdepartementet, 2018, § 70).

[19] Omspurte er den personen som skal klareres, og benevnes i dag som hovedpersonen.
Aut. myndighet er virksomhetene som har behov for å klarere og autorisere personell, og benevnes i dag som autoriserende myndighet.
[20] Sikkerhetsgradering etter sikkerhetsloven skrives med store bokstaver, jf. sikkerhetsloven § 5-3

Det er hos personell, som gjennom klarerings- og autorisasjonsprosessen er funnet å være sikkerhetsmessig skikket og blir gitt tillit til å få tilgang til sikkerhetsgradert informasjon, man finner sårbarhetene og personkarateristikkene som har potensiale til å gjøre dem til innsidere. Fordi det er disse, og ikke de som blir nektet, som gis tilgang til hemmelighetene. Sikkerhetsklarert og autorisert personell er gjennom lovbestemt varslingsplikt i sikkerhetslovens § 8-11.Varslingsplikten omfatter forhold som kan påvirke sikkerhetsmessig skikkethet, ansvarlig for å rapportere til autorisasjonsansvarlig hvis det oppstår forhold og hendelser som øker sårbarhetene knyttet til egen person (Forsvarsdepartementet, 2018, § 8-11). Tilnærming fra det som antas å være fremmedetterretning, oppståtte økonomiske problemer, misbruk av rusmidler, er eksempler på hva som omfattes av opplysningsplikten (Forsvarsdepartementet, 2018, § 8-5).

De styrende organer

Selv om en del av oppgavene til EOS-tjenestene er forankret i sikkerhetsloven, politiloven og etterretningstjenesteloven, så skisseres tjenestenes økonomiske rammer prioriteringer, resultatmål og rapporteringskrav i tildelingsbrev fra sektordepartementene (Stortinget, 2020). PST og NSM får sine tildelingsbrev fra Justis- og beredskapsdepartementet, Etterretningstjenesten fra Forsvarsdepartementet. Disse tildelingsbrevene er sikkerhetsgradert og ikke tilgjengelige for offentligheten.

Justis- og beredskapsdepartementet (JD)

Justis- og beredskapsdepartementet har, etter samfunnssikkerhetsinstruksen, et særskilt ansvar for et helhetlig, systematisk og risikobasert arbeid med samfunnssikkerhet på nasjonalt nivå på tvers av alle sektorer (Justis- og beredskapsdepartementet, 2017).
Sikkerhetsloven forvaltes av JD. I tillegg til dette er departementet etatsstyrer for NSM og PST. Ansvaret for sikkerhetsloven, og det administrative ansvaret for NSM, ble overtatt fra FD i 2019[21]. Dette gjør departementet til en viktig aktør i forhold til utviklingen av det nasjonale regelverket og tjenestene, som utgjør rammene og er forutsetningene for kongerikets utøvelse av forbyggende sikkerhet. Herunder sikkerhetsstyring og personellsikkerhet. NSM rapporterer fortsatt til FD, så ansvaret for NSM er fortsatt delt mellom de to departementene.

[21] https://www.regjeringen.no/no/aktuelt/endringer-i-departementsstrukturen/id2626358/

Forsvarsdepartementet (FD)

FD var frem til våren 2019, før dette ble overført til JD, forvalter av sikkerhetsloven og etatsstyrer av NSM.

«*Endringen innebærer at JD vil ha det overordnede administrative og budsjettmessige ansvaret for NSM, mens ansvaret for den faglige etatsstyringen er delt mellom FD og JD. NSM skal fortsatt ivareta utøvende funksjoner for det forebyggende sikkerhetsarbeidet i forsvarssektoren på vegne av FD.*» (Nasjonal sikkerhetsmyndighet, 2019)

NSM sine bånd til FD er ikke brutt med den nye organiseringen, og FD vil fortsatt ha instruksjonsmyndighet overfor NSM i saker knyttet til forsvarssektoren. Det at FD deler den faglige etatsstyringen av NSM med JD, og at FD er overordnet departement for Etterretningstjenesten gjør FD til en sentral aktør innen forebyggende sikkerhet. Ikke minst finner man mye av informasjonen og hemmelighetene, som fremmed etterretning leter etter, innenfor forsvarssektoren. Noe som har blitt poengtert gjentatte ganger av PST i deres trusselvurderinger.

«*Etterretningsvirksomhet kan også føre til kompromittering av militær og annen sensitiv informasjon. Dette kan bidra til å svekke eller vanskeliggjøre eventuelle militære operasjoner hjemme og ute, og kan i verste fall sette norsk personell i fare.*»
(Politiets sikkerhetstjeneste , 2005)

Det kontrollerende organ (EOS-utvalget)

Stortingets kontrollutvalg for etterretnings-, overvåkings- og sikkerhetstjeneste (EOS-utvalget)[22] har en helt sentral rolle i å motvirke at det på organisatorisk- og strukturelt nivå, begås rettssikkerhetsmessige overgrep mot enkelt individer, som følge av virksomheter og myndigheters arbeid med forebyggende sikkerhet.
For å motvirke slike overgrep er det, i et demokrati som Norge, viktig at EOS-tjenestene er underlagt demokratisk kontroll. Derfor oppnevnte Stortinget et eget uavhengig utvalg som skulle føre kontroll med EOS-tjenestene. Stortingets kontrollutvalg for etterretnings-, overvåknings- og sikkerhetstjeneste, det såkalte EOS-utvalget, ble oppnevnt i 1996.

[22] https://eos-utvalget.no/hjem/om-eos/eos-tjenestene/

«Utvalgets oppgave er å føre løpende kontroll med de såkalte EOS-tjenestene. Disse består i dag av Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST), Nasjonal sikkerhetsmyndighet (NSM) og Forsvarets sikkerhetsavdeling (FSA).»[23]

Noe av bakgrunnen for oppnevnelsen av utvalget kan man finne i den langvarige politiske debatten som pågikk i første halvdel av 1990-tallet, knyttet til de hemmelige tjenestenes virksomhet. Debatten kom som følge av mye offentlig oppmerksomhet på de hemmelige tjenestene i Norge. Debatten medførte at Stortinget 1. februar 1994 nedsatte den såkalte Lundkommisjonen. Kommisjonen skulle undersøke virksomheten til de hemmelige tjenestene. I sin rapport 28. mars 1996, samme år som oppnevnelsen av EOS-utvalget, konkluderte kommisjonen med at, Politiets overvåkningstjeneste (POT) hadde drevet en omfattende og ulovlig politisk overvåkning av personer og organisasjoner på venstresiden av norsk politikk[24] POT var førløperen til dagens PST.

[23] https://eos-utvalget.no/hjem/om-eos/eos-tjenestene/
[24] https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/?lvl=0

3 Relevant teori

3.1 Risiko

Risiko og risikovurdering

Risiko er et vesentlig begrep, innen forbyggende sikkerhet, sikkerhetsstyring og personellsikkerhet. Det er også et begrep som anvendes i forhold til innsidervirksomhet, noe som gjenspeiles blant annet i NSM sin temarapport med navnet Innsiderrisko (Nasjonal sikkerhetsmyndighet, 2019)

I denne oppgaven er fokuset rettet mot innsiderrisikoen. Det vil si risikoen for at en nåværende eller tidligere ansatt, konsulent eller kontraktør, som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, misbruker denne kunnskapen og tilgangen til å utføre handlinger som påfører virksomheten skade eller tap (Nasjonal sikkerhetsmyndighet, 2019, s. 9). Det er mange definisjoner på begrepet risiko, og det finnes ingen fastsatt og omforent fremgangsmåte for risikovurderinger knyttet til tilsiktede uønskede handlinger, som også kan benevnes sikkerhetstruende virksomhet (Forsvarsdepartementet, 2018).

Trefaktormodellen

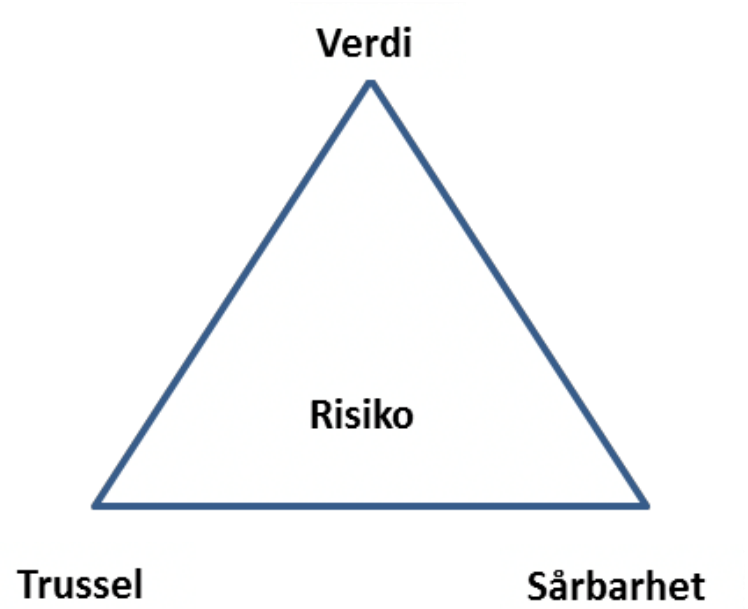
Forsvarets forskningsinstitutt (FFI) gir i sin rapport, *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger*, en vurdering av to forskjellige tilnærminger til risiko, hvor den ene tilnærmingen er basert på Norsk Standard (NS) 5814:2008 (Forsvarets forskningsinstitutt (FFI), 2015). I NS 5814:2008 defineres risiko som et "uttrykk for kombinasjonen av sannsynligheten for og konsekvensen av en uønsket hendelse". I den andre tilnærmingen, som er basert på NS 5832: 2014, er sikringsrisiko definert som et "uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen". Denne tilnærmingen kalles ofte trefaktormodellen. FFI fremstiller i sin rapport at forskjellen på disse to tilnærmingene er at i tilnærmingen basert på NS 5814 foretas en separat vurdering av muligheten for at et angrep finner sted og er vellykket, og denne vurderingen er basert på en kunnskapsbasert sannsynlighetsvurdering.

Risikokommunikasjonen i de to modellene, fremstilles som både forskjellig og med

tilhørende styrker og svakheter. NS 5814 kritiseres for at modellen gjennom risikomatrisen, som riktig nok kan være enkel å forstå, overforenkler og gir inntrykk av større sikkerhet enn det er grunnlag for. Usikkerheten kommuniseres ikke, noe også trefaktormodellen kritiseres for (Forsvarets forskningsinstitutt (FFI), 2015, s. 3).

NSM sin tilnærming til risiko begrepet tar utgangspunkt i trefaktormodellen. Siden NSM er den nasjonale sikkerhetsmyndigheten, og derfor en premissleverandør for det nasjonale arbeidet med forebyggende sikkerhet, vil NSM sin tilnærming til begrepet risiko legges til grunn i denne oppgaven. Samtidig, basert på FFI sin vurdering, fremstår kunnskapsbasert sannsynlighetsvurdering som nødvendig og uunngåelig i en risikovurdering for tilsiktede uønskede handlinger (Forsvarets forskningsinstitutt (FFI), 2015). I denne oppgaven vil derfor tilnærmingen til risiko og risikovurdering baseres på trefaktormodellen i kombinasjonen med vurdering av usikkerhet og konsekvens, eller utfall av en gitt aktivitet, (Aven, et. al, 2016, s. 37)

Trefaktormodellen omtales ofte som Risikotrekanten, slik den illustreres i figur 2 på neste side, og blir også illustrert på denne måten, som en varseltrekant (Nasjonal sikkerhetsmyndighet, 2015, s. 12). Risikotrekanten består av tre hjørner som ikke nødvendigvis er likevektige, de tre hjørnene er avhengige av hvilket fokus virksomheten har. Alle virksomheter underlagt sikkerhetsloven må være trusselbildet bevisst, men trusselbildet kan ofte ligge utenfor virksomhetens kontroll. Dette medfører at fokuset ofte rettes mot virksomhetens verdier og sårbarheter, som enklere kan utbedres av virksomheten selv (Nasjonal sikkerhetsmyndighet, 2015, s. 12)



Figur 2: Risikotrekanten (Nasjonal sikkerhetsmyndighet, 2015, s. 12)

Verdi

Verdi er et begrep som benyttes innenfor flere områder, og om både materielle- og immaterielle objekter og ting. Samfunnsverdier i form av liv og helse, stabilitet, natur og miljø, og økonomi er en tilnærming til begrepet (Engen, et. al, 2017, s. 375).
Innenfor forebyggende nasjonal sikkerhet er verdibegrepet knyttet til konsekvensen sikkerhetstruende virksomhet har for verdiene (Forsvarets forskningsinstitutt (FFI), 2015). Verdiene er knyttet til grunnleggende nasjonale funksjoner og våre nasjonale sikkerhetsinteresser, og finnes i form av skjermingsverdig informasjon, eller produksjon og virksomhet, hos virksomheter underlagt sikkerhetsloven (Forsvarsdepartementet, 2018).

Trussel

En trussel kan i bred forstand forstås som en kilde til risiko, hvor det foreligger intensjon om en eller annen form for angrep med hensikt om å påføre skade, frykt, smerte og fortvilelse. Det er med andre ord noe annet enn en fare, som også kan sies å være en kilde til risiko. Fare kan også medføre fysisk- og psykisk skade, men da foreligger det ikke noe ønske eller intensjon bak. Fare knytter seg derfor mer til sikkerhetsbegrepet brukt i forbindelse med utilsiktede hendelser, og det som på engelsk kalles «safety» (Aven, 2020, s. 62).
Trussel i en forebyggende sikkerhetskontekst, handler om tilstedeværelse, kapasitet, intensjon, historie hos potensielle trusselaktører (Forsvarets forskningsinstitutt (FFI), 2015), og det som i sikkerhetslovens § 1-5 er definert til å være: *«...tilsiktede handlinger, som direkte*

eller indirekte kan skade nasjonale sikkerhetsinteresser.» (Forsvarsdepartementet, 2018, § 1-5).

Etterretningstrusselen fra utenlandske etterretningstjenester, er eksempel på en trussel og en trusselaktør. Ved hjelp av ulike metoder søker trusselaktøren å tilegne seg kontroll, oversikt over og tilgang til informasjon, prosesser og produkter de kan utnytte til egen fordel. Det å benytte seg av innsidere er et eksempel på en trussel, som materialiseres gjennom fremmed etterretnings tilstedeværelse, kapasitet, intensjon og historie.

Sårbarhet

Utnyttelse av personell som har, eller har hatt tilgang til virksomhetenes verdier, handler om utnyttelse av dette personellets sårbarheter.

Men sårbarheter handler i denne sammenheng også om organisatoriske sårbarheter, og sårbarheter i systemer. Sårbarheter som utenlandske etterretningstjenester kan benytte, ikke bare til å rekruttere innsider, men også til å infiltrere egne innsidere (PST mfl., 2017).

Sårbarheter kan derfor forstås som:

«... et systems forutsetninger for eller manglende evne til å fungere under og etter at det utsettes for en uønsket hendelse.» (Engen, 2017, s. 47)

Sårbarhet blir derfor ofte betraktet som mer eller mindre det motsatte av robusthet, som kan defineres som:

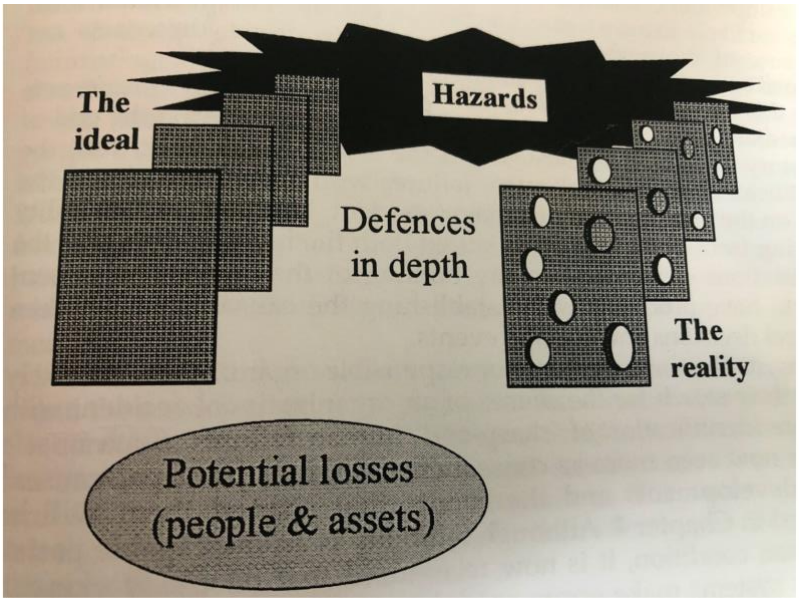
«Et systems evne til å opprettholde sin funksjon når det utsettes for påkjenninger.» (Aven, et. al, 2016, s. 124)

Sårbarhet handler med andre ord, i denne sammenheng, om forhold, enten hos enkeltpersoner eller hos virksomheten som system, som en trusselaktør kan utnytte til å oppnå sine målsettinger. I denne studien er det virksomheten som er i fokus.

3.2 Swiss cheese

Risikoen knyttet til uønskede hendelser, i denne sammenhengen innsidevirksomhet, kan altså forklares gjennom trefaktormodellen.

For å forklare hvordan en uønsket hendelse oppstår, er det nødvendig å se til andre modeller og teorier. James Reasons Swiss cheese modell, illustrert i figur tre nedenfor er en slik modell.



Figur 3: Swiss Cheese model (Reason, 2016, s. 9)

Modellen har til hensikt å beskrive hvordan organisatoriske ulykker oppstår. Dette gjøres ved å beskrive hvordan sammenfall av latente feil og menneskelige feilhandlinger skaper forutsetninger for en ulykkeshendelse. Årsakene finnes både hos menneskene teknologien og organisasjonene.

Relevans

Modellen er i utgangspunktet tiltenkt organisatoriske ulykker hvor det ikke forelå en intensjon om å skade virksomheten eller dens verdier. Men modellen er også, fra et organisatorisk perspektiv, anvendbar for å årsaksforklare sikkerhetstruende hendelser hvor det forelå både intensjon, vilje og evne.

En sikkerhetstruende hendelse knyttet til personellsikkerhet og innsidevirksomhet, kan også beskrives gjennom denne modellen. Sårbarheter hos personellet kombinert med feil og mangler i tekniske sikkerhetstiltak, og det samme innen organiseringen av personellsikkerheten i virksomhetene, gir mulighet for trusselaktørene til å ramme verdiene.

Barrierer

Svakheter og feil i barrierene til virksomhetene er utgangspunktet for Reasons tilnærming. Barrierene skal hindre at hendelser oppstår, og begrense konsekvensene av dem hvis de

allikevel inntreffer (Aven, Risikostyring, 2015, s. 46). Barrierer kan i denne sammenheng beskrives som, tiltak som skal ha som funksjon å beskytte i feil, fare- og ulykkessituasjoner. Funksjonen til disse ivaretas av barriereelementer som kan være tekniske, organisatoriske og operasjonelle (Petroleumstilsynet, 2017, s. 3). Barrierer kan kategoriseres som aktive-, eller passive barrierer. Aktive barrierer krever enten manuell, eller automatisk aktivering, mens passive barrierer uavhengig av ekstern aktivering (Aven, et. al, 2016, s. 122).

«The Dangers of The Unrocked Boat»

Reason snakker også om farene ved «The Unrocked Boat», som betegner hvordan perioder med fravær av alvorlige hendelser medfører erosjon i sikkerhetstiltakene, og dermed er en faktor i årsaksforklaringen til organisatoriske ulykker (Reason, 2016, s. 6). Vedlikehold, oppgradering og tilpassing av sikkerhetstiltakene blir nedprioritert i forhold til tiltak som gir økt produktivitet, lønnsomhet og inntjening fordi det er vanskelig å argumentere for å prioritere tiltak rettet mot noe som aldri skjer. Gapet mellom virksomhetens utvikling på andre områder og sikkerhetstiltakene vil i en slik sammenheng øke. Dermed vil sikringstiltakene etterhvert ikke korrespondere med sikringsbehovet, noe som igjen gir økt risiko for en katastrofe (Reason, 2016, s. 6). Innsidehendelser skjer ikke ofte. De oppdages uansett ikke ofte, og tiltakene man engang iverksatte kan derfor av ulike årsaker erodere over tid. «The Dangers of The Unrocked Boat» er således relevant, også når man skal forklare en hvordan en sikkerhetstruende hendelse har oppstått. Den er også relevant i forhold til sikkerhetsstyringens rolle og tilnærming til utvikling, vedlikehold og forbedring av sikkerhetstiltak.

Latente feil og menneskelige feilhandlinger

James Reason beskriver i sin teori om organisatoriske ulykker hvordan latente feil og menneskelige feilhandlinger kan utløse storulykker, og at årsakene er å finne i samspillet mellom menneske, teknologi og organisasjon (Reason, 2016, s. 10). Et samspill som også er av betydning for personellsikkerhet og sikkerhetsstyring. Jens Rasmussen understøtter i sin artikkel, Risk Management In a Dynamic Society: A Modelling Problem, denne årsakssammenhengen, og påpeker også hvordan krav knyttet til økt produksjon påvirker fokuset til lederne knyttet til risikostyring (Rasmussen, 1997). Reason viser videre til hvordan krav til sikkerhet og krav til produksjon, ofte blir konkurrerende krav, og de forhold som bidrar til at sikkerhetstiltakene eroderes og dermed økt risiko for ulykker (Reason, 2016, s. 6).

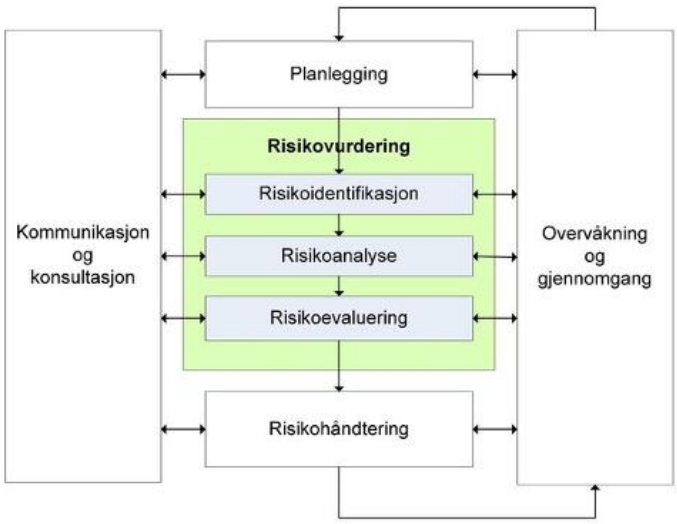
Reasons og Rasmussens forskning handler om hvordan ulykker oppstår i dynamiske, komplekse miljøer i stadig endring, og kan også årsaksforklare sikkerhetstruende hendelser fra et organisatorisk perspektiv. Reason prøver i tillegg med sin mulige årsaksforklaring på organisatoriske ulykker å bygge bro mellom det som kalles Normal accidents-teorien (NAT), og High Reliability Organization (HRO) teorien. Sosiologen Charls Perrow fremlegger i sin bok Normal accidents fra 1984 at ulykker og katastrofer er en naturlig konsekvens av vår teknologiske ekspansjon og invasjon i naturen (Engen, 2017, s. 143). HRO teorien på sin side fremlegger at ulykker kan unngås gjennom en system tilnærming til sikkerhet. Et tema hos Perrow som er relevant for denne oppgaven er det han beskriver som tettekoplinger i systemer hvor nærhet mellom deler og enheter som normalt ikke hører sammen kan skape uforutsette interaksjoner (Engen, 2017, s. 144). Tettekoplinger vil i denne oppgaven ses i sammenheng med det som i forarbeidene til sikkerhetsloven kalles økte gjensidige avhengigheter, som omtales senere (Traavikutvalget, 2016, s. 18).
Hvordan sikkerhetstruende hendelser kan unngås gjennom styring og organisering, sikkerhetsstyring, og relevant teori knyttet til dette, er neste tema i denne oppgaven.

3.3 Sikkerhetsstyring

Sikkerhetsstyring er et lovpålagt krav, for virksomheter underlagt sikkerhetsloven, hvor hensikten er å unngå sikkerhetstruende hendelser i det samme dynamiske og raskt endrende samfunnet. Det som kreves er at det etableres et styringssystem for sikkerhet, som gjør at forebyggende sikkerhet blir en del av virksomhetens styringssystem (Forsvarsdepartementet, 2018).

«Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier.» (Nasjonal sikkerhetsmyndighet, 2019)

Det teoretiske grunnlaget for sikkerhetsstyring etter sikkerhetsloven, baserer seg på teorier knyttet til risikostyring.



Figur 4: Risikostyringsprosessen (Proactima) [25]

Risikostyring er en prosess som vist i figur 4 over, som handler om å få innsikt i risikoforhold, effekt av tiltak, i hvilken grad man kan styre sårbarhet osv., men samtidig handler det også om metoder, prosesser og strategier for å kartlegge og styre risikoer. Hensikten med risikostyring er ikke å ensidig redusere risiko, men å sikre en balanse mellom å det å utvikle og skape verdier, og det å unngå ulykker, skader og tap (Aven T. , 2015, s. 14). Gjennom forskning på organisatoriske ulykker, og erfaringene fra disse, har man kommet til faktorer som kjennetegner virksomheter som lykkes med innføringen av risikostyring[26]:

- Proporsjonalitet: samsvar mellom ressursbruk på risikostyring og risikoene.
- Synkronisert: Risikostyringsaktivitetene synkroniseres i tid med øvrige aktiviteter.
- Omfattende: alle deler av organisasjonen inkluderes, slik at vesentlige risikoer kan identifiseres og håndteres.
- Integritet: Risikostyring integreres i kjerneprosessene.
- Dynamisk: Risikostyringen må være dynamisk og respondere på nye risikoer eller endringer i risikobildet.

Styring av de tidligere nevnte barrierene, er også en vesentlig del av risikostyringen.

Skal barrierene i virksomhetene kunne hindre at hendelser oppstår, og begrense konsekvensene av dem hvis de allikevel inntreffer, så må de styres. Fordi endringer i barrierenes ytelse endrer risikonivået (Aven T. , 2015, s. 154). Fraværet av barrierestyring

[25] https://docplayer.me/373087-Risikostyring-i-kraftbransjen.html
[26] https://proactima.com/kurs-og-opplaering/rammeverk-for-risikostyring/

hvor barrierene ikke oppdateres og eroderer, vil påvirke effekten av barrierene slik Reason beskriver i sin teori om «The Dangers of the Unrocked Boat. Barrierestyring, som en del av virksomhetenes styringssystem for sikkerhet, handler om at en systematisk og kontinuerlig sikrer at de nødvendige barrierer er identifisert og til stede for å beskytte i feil, fare- og ulykkessituasjoner (Petroleumstilsynet, 2017).

High Reliability Organization (HRO)

Den kulturen som råder i en organisasjon vil påvirke hvorvidt sikkerhetsstyringen oppnår sin hensikt. High Reliability Organization (HRO) teorien, det som på norsk kalles høypålitelige organisasjoner, forklarer hvordan organisasjoner har lykkes med å unngå ulykker og hevder at alvorlige ulykker knyttet til komplekse organisasjoner kan unngås (Engen, et. al, 2017, s. 151).

«Serious accidents with hazardous technologies can be prevented through intelligent organizational design and management» (Sagan, 1993, s. 14)

HRO-Teorien baserer seg på empirisk forskning på organisasjoner med høy grad av pålitelighet, altså HRO. Det som karakteriserer en HRO er at den innehar fire kulturelt betingede komponenter, som sammen danner sikkerhetskultur. Disse komponentene er en rapporterings-, rettferdighets-, fleksibel-, lærende-og en informert kultur (Reason, 2016, ss. 195-196). Sikkerhetskultur er også en viktig faktor i sikkerhetsstyring, og manglende sikkerhetskultur er den viktigste årsaken til at sikkerhetsnivået i mange situasjoner er for lavt (Sikkerhetsutvalget (Traavikutvalget), 2016, s. 84).
Det finnes mange definisjoner på hva kultur er. Men det handler om felles verdier, oppfatninger og normer, i, for eksempel, grupper og organisasjoner. Reason legger følgende definisjon til grunn:

«Shared values (What is important) and beliefs (how thing work) that interact with an organization´s structures and control systems to produce behavioral norms (the way we do things around here)» (Reason, 2016, s. 192)

I HRO- teorien handler rapporteringskulturen om en kultur der det er evne og vilje til å rapportere om hendelser, også de som impliserer feil begått av en selv eller kolleger.

Hensikten med rapporteringen er å lære av dem, sett i lys av at også små hendelser kan bidra til større ulykker og katastrofer.
Det er flere faktorer som er avgjørende, i henhold til teorien, for å skape en rapporteringskultur. Faktorene enkelhet og hurtighet handler om at det må være enkelt å få tilgang til og fylle ut rapporteringsformularet, og at det må gis tilbakemelding på rapportene på en måte som er lett tilgjengelig, forståelig og nyttig for de det angår (Reason, 2016, s. 197). Faktorene disiplinære forføyninger, konfidensialitet og håndtering av rapportene, knytter seg til tillit. Tillit til at det er rettferdighet knyttet til eventuelle disiplinære tiltak, at rapportene behandles på en måte som beskytter rapportørens anonymitet, og at de som analyserer rapportene ikke er de samme som de som har disiplinærmyndigheten i organisasjonen (Reason, 2016, s. 197).

Tillit har også betydning for rettferdighetskultur-komponenten. Denne komponenten har et mer idealistisk preg enn de øvrige. Den er kanskje uoppnåelig, men den er noe å strekke seg etter. Det handler om rettferdighet i forhold skillet mellom å straffe de handlinger som er intensjonelt dårlige, og de handlinger hvor det å tildele skyld, hverken er passende eller tjenlig (Reason, 2016, s. 205).

Det å ha en fleksibel kultur, handler om evnen til å tilpasse seg effektivt til foranderlige krav. Synet på desentralisering og sentralisering er et viktig element i HRO-perspektivet. Når man snakker om HRO, så er dette gjerne store komplekse organisasjoner som preges av byråkratiske og hierarkiske strukturer, med klare autoritets- og kommandolinjer ved normaltilstand. Produksjonen og operasjonene utføres gjerne etter testede standard prosedyrer, som det trenes på. Teorien forfekter at en HRO ved en krisesituasjon vil kunne gjøre et skifte i autoritets- og kommandolinjene, slik at beslutningsmyndighet gis til den som er nærmest hendelsen og presumptivt har best erfaring og kunnskap om de faktorer som påvirker situasjonen (Reason, 2016, ss. 213-216).

Når det gjelder komponenten lærende kultur, så hevdes det at dette er den letteste å skape men vanskeligst å få til å virke. Det handler om å ta lærdom av den i informasjonen man får gjennom sikkerhetssystemene, og være villig til å gjennomføre endringer og reformer basert på denne informasjonen. Bestanddelene i en lærende kultur er at den er observerende, reflekterende, skapende og handling. Det er den siste som er komplisert, fordi det

beslutningen om å iverksette nødvendige endringer ofte blir satt til side for andre mer presserende aktiviteter (Reason, 2016, ss. 218-219).

Den siste bestanddelen, en informert kultur, kommer som en følge av de øvrige. Dette fordi det i dette ligger å ha kunnskap om alle de faktorer som har betydning for sikkerheten. Reason kaller dette en sikkerhetskultur (Reason, 2016, s. 195).

Ledelse er en vesentlig faktor i HRO-teorien. Ledelse sammen med kulturelle forhold er vesentlige for hvordan en organisasjon er i stand til å håndtere komplekse utfordringer (Engen, et. al, 2017, s. 152).

Redundans og resiliens, er andre sentralt begrep som knytter seg sterkt til Høypålitelighets-teori. Redundans er altså, enkelt forklart beskyttelse i flere separate lag. Resiliens handler om evnen til å gjenopprette sikkertilstand, og kan igjen splittes opp i proaktiv- og reaktiv resiliens. Begrepet er også knyttet til evnen til improvisasjon og utnyttelse av ressursene kreativt for å håndtere hendelser. Proaktiv resiliens er evnen til å tilrettelegge og håndtere endringer uten katastrofale feil eller ulykker, mens reaktiv resiliens er det å, etter rask respons, å komme raskt tilbake med økt robusthet etter alvorlige hendelser og katastrofer (Engen, et. al, 2017, s. 154).

3.4 Oppsummering av teorikapittelet

I dette kapittelet har det blitt redegjort for de teoriene som legges til grunn for drøftingen av denne oppgavens problemstilling og forskningsspørsmål. De valgte teoriene gir mulighet til å belyse problemstillingen fra ulike perspektiver. Swiss Cheese modellen er en teori som gir en mulig forklaring på organisasjonsulykker. Men den gjør det også mulig å forklare hvordan fremmed etterretning kan utnytte både organisatoriske og individuelle sårbarheter i sin sikkerhetstruende virksomhet. I tillegg til at den ved en barrieretilnærming kan brukes til å forklare det norske systemet for personellsikkerhet. Et system med både styrker og svakheter. Hvor svakhetene, gitt de rette forholdene, kan forårsake alvorlige følger for vår nasjonale sikkerhet. Latente feil, menneskelige feilhandlinger og farene ved the Unrocked Boat kan med utgangspunkt i personellsikkerhet bidra til å årsaksforklare sikkerhetstruende hendelser rettet mot våre nasjonale sikkerhetsinteresser.

På samme måte som Swiss Cheese modellen, retter HRO teorien seg mot organisasjonsulykker. Men HRO teorien kan også forklare hvordan man kan lykkes med å forhindre sikkerhetstruende virksomhet, også ut ifra et personellsikkerhetsperspektiv. Samtidig er det som karakteriserer en HRO, også det som gir HRO utfordringer når det kommer til forebyggende sikkerhet, sikkerhetsstyring og personellsikkerhet. Sikkerhetsstyring er ved å være lovpålagt for virksomheter underlagt sikkerhetsloven et vesentlig verktøy for å håndtere risiko og sårbarheter, og beskytte mot trusler og trusselaktører sin sikkerhetstruende virksomhet.

For å analysere hvordan sikkerhetsstyring innen forebyggende sikkerhet har utviklet seg de siste 20 årene, vil det være nødvendig å se dette i forhold til den samtidige risikoforståelsen. I denne oppgaven betyr dette forståelsen av usikkerheten knyttet til hvorvidt trusselaktører kan, og vil, utnytte personellmessige sårbarheter eller svikt i personellsikkerheten, for på den måten å skade virksomhetens verdier. Trefaktormodellens forklaring av risiko, i kombinasjon med vurdering av usikkerhet og konsekvens, gir et utgangspunkt for dette. Herunder også introduksjonen og anvendelsen av denne modellen i denne tidsperioden.

4 Forskningsmetode

I det følgende kapittelet beskrives valg av metode, forskningsdesign, prosess og fremgangsmåte for innsamling av data. Arbeidet med denne oppgaven har vært preget av dokumentstudier. Hvorfor vil jeg redegjøre for i det som følger nedenfor.

4.1 Valg av problemstilling

Jeg ønsket å se nærmere på sikkerhetsstyring og personellsikkerhet, samtidig som jeg i lengre tid har vært opptatt av og hatt meninger om hvorvidt rammene for forebyggende sikkerhet utvikler seg i riktig retning i forhold til trussel- og risikobildet. Et bilde som offentlige myndigheter omtaler som dynamisk og raskt skiftende (Forsvarsdepartementet, 2017, ss. 15-17). Rammene for forebyggende sikkerhet er lagt gjennom offentlige dokumenter, som forarbeidene til sikkerhetsloven og sikkerhetsloven, i tillegg til veiledninger fra fagmyndighetene som gir anbefalinger om utførelse av sikkerhetsarbeidet. Dokumentstudier ble derfor viktig for innhentingen av empiri (Tjora, 2017). Ved å benytte dokumentstudier

som primærkilde i tillegg til fokuserte intervjuer, har jeg også redusert belastningen på andre (Tjora, 2017).

Siden det er ca. 20 år siden vi fikk den første sikkerhetsloven, ble en historisk tilnærming med de siste 20 årene som ramme et naturlig valg for det jeg ønsket å undersøke. jeg har derfor startet med den gamle sikkerhetsloven, med tilhørende forarbeider, som utgangspunkt for å undersøke utviklingen av sikkerhetsstyring frem til våren 2020.
Den nye loven har vært gjeldende i snart to år. De to lovene, med tilhørende forarbeider, gir et grunnlag for sammenligning av rammebetingelsene for sikkerhetsstyring slik de forelå for 20 år siden, og slik de foreligger nå.

Selv om det har vært gjort endringer av loven innen avgrensede områder, i henholdsvis 2005, 2008 og 2017, så er det først i forbindelse med utviklingen av den nye sikkerhetsloven, lov om nasjonal sikkerhet, at det er foretatt en helhetlig lovrevisjon (Forsvarsdepartementet, 2017). Disse endringene har i stor grad knyttet seg til myndighetsnivået på områder som jeg anså mindre relevante for denne oppgaven. Av hensynet til dette og omfanget av studien har ikke dokumentene knyttet til disse endringene vært en del av studien. Endringene er også i stor grad fanget opp i de øvrige dokumentene som har blitt studert.

Forskningsdesign

Med et historisk perspektiv på utviklingen sikkerhetsstyring, innenfor en ramme på 20 år, fant jeg det tjenlig å se på hvordan forebyggende sikkerhet, som utgjør rammen for sikkerhetsstyring og risikooppfatningen har utviklet seg i samme periode.

Siden personellsikkerhet er noe det er forsket lite på i norsk sammenheng og er et fagfelt jeg har stor interesse for, ble det naturlig å avgrense undersøkelsene av risikooppfatningens utvikling til dette fagområdet. Motvirkning av innsiderhendelser er kjernen i personellsikkerhet, og siden den forskningen som finnes innen personellsikkerhet i stor grad omhandler karakteristika knyttet til enkelt individet for å forklare en innsidehendelse, så fant jeg det både interessant og relevant for helheten i denne oppgaven å undersøke hvordan en slik hendelse kan forklares fra et organisatorisk perspektiv. Min overordnede plan har vært å se på årsaks- virkning forholdet mellom sikkerhetsstyring, forebyggende sikkerhet, og risiko- og trusselpersepsjonen i denne perioden. Dette fordi jeg mener at det vil det være mulig å

forklare hvorfor sikkerhetsstyringen har utviklet seg slik den har gjort, gjennom å undersøke disse faktorene og sammenhengen mellom dem, Forskningsdesignet som anvendes er derfor en kausal tilnærming (Blaikie & Priest, 2019, s. 22).

Valg av forskningsmetode

Min egen bakgrunn og erfaring, forkunnskap og nærhet til det som skulle undersøkes, gjorde at jeg hadde kunnskaper om hvor jeg kunne starte mine undersøkelser og innhenting av data. Forarbeidene til sikkerhetslovene og sikkerhetslovene ble derfor et naturlig utgangspunkt. Dette er normative dokumenter, som i stor grad skal gi regler for hvordan forebyggende sikkerhetsarbeid skal utføres, eller for hvordan reglene skal tolkes. Forarbeidene og de andre dokumentene er benyttet til å analysere allerede eksiterende dokumenter, for å hente inn informasjon nedtegnet på ulike tider i den hensikt å bidra til å forklare utviklingen av sikkerhetsstyring (Tjora, 2017, s. 183). Forkunnskapen min gjorde at jeg også visste at NSM sine årlige risikovurderinger, og PST sine årlige trusselvurderinger, ville være relevante kilder for datainnhenting. Disse dokumentene beskriver risiko- og trusselbildet og er derfor deskriptive i form og innhold.

Siden det var nødvendig å beskrive og årsaksforklare sammenhengen mellom ulike dokumenter som både var normative og deskriptive i form og innhold, hvor dataene i liten grad ville finnes i form av tall eller andre mengdetermer og derfor i stor grad måtte genereres ved fortolkning av teksten, ble det valgt en kvalitativ metodisk tilnærming for å undersøke problemstillingen (Johanessen, 2018, s. 26).

Forskningsprosessen

I tabellen nedenfor gir en skjematisk fremstilling av gjennomføringen av forskningsprosessen i arbeidet med denne studien.

Formål	Hva	Hensikt	Resultat
Valg av problemstilling	• Problemstillingen og forskningsspørsmålene ble revidert flere ganger under arbeidet, for å sikre gyldigheten i studien	• Skrive om sikkerhetsstyring og personellsikkerhet	• Fikk etablert problemstilling og forskningsspørsmål, som var valide.

Forskningsdesign	• Innholdsanalyse av dokumenter ble brukt til datainnsamling og datagenerering • Sammenligning av styrende dokumenter og trussel- og risikovurderinger ble gjort for å undersøke årsak-virkningsforholdet mellom disse • Intervju med eksperter ble brukt for datainnsamling, kontroll og sikring av funn og konklusjoner	Årsaksforklare den historiske utviklingen av sikkerhetsstyring	• Fikk samlet inn relevante data • Årsaksforklaring var mulig • Mengden data gjorde det utfordrende å avgrense oppgaven. Noe som også ble påvirket av min egen forkunnskap
Valg av forskningsmetode	• Kvalitativ metode ble den valgte metoden, selv om kvantitative teknikker ble anvendt for enkelte deler av datainnsamling- og generering	• Analysere meningen i ulike dokumenter og kunne sammenligne ulike data innhentet i disse.	• Gjorde det mulig med bakgrunn i innsamlede og genererte data å beskrive sammenhenger mellom ulike dokumenter

Data innsamling	• Innholdsanalyse av relevante dokumenter var primær kilde for datainnsamlingen • Fokuserte intervjuer av eksperter på fagområdet forebyggende sikkerhet, hvor jeg la frem funn og konklusjoner og disse ble diskutert. Funnene og konklusjonene som ble diskutert var knyttet til temaene: - Bakgrunn for sikkerhetslovene - Sikkerhetsstyring - Personellsikkerhet - Innsider	<u>Innholdsanalyse:</u> • Gi innsikt i myndighetenes vurderinger, og bakgrunnen for disse • Innhente data for å undersøke kontekstuelle sammenhenger og årsaks-virkningsforholdet mellom dokumentene • <u>Intervjuene:</u> • Kvalitetssikre funn og konklusjoner • Redusere innflytelsen fra mine meninger.	• Dataene fra de ulike dokumentene var mulig å sammenligne • Dataene kunne brukes til å årsaksforklare en historisk utvikling • Intervjuene underbygget funnene og konklusjonene, og ga i tillegg relevant tilleggs informasjon som underbygget mine funn og konklusjoner. • Intervjuene antas å ha redusert innflytelsen fra mine egne meninger, men planen om korte fokuserte intervjuer ble utfordret av informantenes vilje til å dele kunnskap og erfaring. Dette var utelukkende positivt da det ga mer tid og rom for å diskutere mine funn og påstander
Data generering	• Hermeneutisk tilnærming, hvor jeg gjennom lesning fortolket budskapet i ulike dokumenter, og sammenliknet innholdet. • Ordsøk med flere sentrale begreper ble gjort i de ulike dokumentene.	• Forstå budskapet i de ulike dokumentene, vurdere effekten av dem, undersøke den kontekstuelle sammenhengen mellom dem, og formidle en kausal forklaring på den historiske utviklingen av sikkerhetsstyring. • Ordsøk ble benyttet for å undersøke når, i hvilken utstrekning og i hvilke dokumenter sentrale begreper ble benyttet.	• Data generert fra innholdsanalysen ble kvalitetssikret i intervjuene, og ga i kombinasjon med intervjuene mulighet til å besvare problemstillingen – • Resultatene fra ordsøkene kunne brukes til å stadfeste tid for innføringen av nye sentrale begreper, vurdere vektleggingen og betydningen de er tillagt i de ulike dokumentene

Tabell 1: Forskningsprosessen

4.2 Datainnsamling

Datagrunnlaget i denne oppgaven er innsamlet fra ca. 80 ulike offentlige dokumenter og publikasjoner fra myndighetene, som har vært av betydning for utviklingen av forebyggende

sikkerhetstjeneste. Dette inkluderte forarbeidene til de to sikkerhetslovene, disse lovene og deres forskrifter, andre relevante lover, forskrifter og bestemmelser, trussel- og risikovurderinger, veiledningsmateriale knyttet til forbyggende sikkerhet, og rapporter og notater utarbeidet av relevante aktører i både inn og utland. I tillegg var tekster fra media også en kilde for informasjonsinnhentingen.

I flere av dokumentene som har blitt studert, finnes det grundige referanse lister. Petroleumstilsynets sin innsiderapport er et eksempel på dette (Det norske veritas (DNV GL), 2019). Men, når det gjelder relevant forskning, spesielt knyttet til personellsikkerhet, så vises det i stor grad til utenlandsk forskning. I de nasjonale myndighetene sine veiledere finner sjelden de samme utførlige referanselistene, og når det er fotnoter og kildehenvisninger, så vises det i stor grad til utenlandske forskningskilder. Dette gjør det utfordrende å få tak i hvordan kildene vurderes opp imot norske forhold, når det gjelder innsiderutfordringen. Det henvises til sikkerhetsloven, og dens forskrifter, men hvilken forskning som har gitt oss det rammeverket vi har i dag må man lete for å finne. Dette har gjort arbeidet med oppgaven både krevende og interessant.

Valg av dokumenter og litteratur til dokumentstudiene, ble gjort uti fra at de alle er dokumenter på nasjonalt og strategisk nivå, som har bidratt til utviklingen av sikkerhetsstyringen, forebyggende sikkerhet og personellsikkerhetsarbeidet i Norge, eller gitt føringer for tilnærmingen til innsiderisikoen og håndteringen av denne. De er skrevet på ulik tid og med tidvis forskjellig formål, men allikevel knyttet til hverandre (Tjora, 2017, s. 183). Lovproposisjonene inneholder også tilbakemeldinger på høringsutkast fra mange virksomheter, og kunne derfor også brukes til datainnsamling fra virksomhetene. I tillegg er de offentlig tilgjengelige. De er studert i den hensikt å samle inn data for kartlegging av utviklingen de siste 20 årene. Derfor er ulike revisjoner og årganger av flere av dokumentene blitt studert i kartleggingen. PST sin årlige trusselvurdering, er et eksempel på et dokument hvor ulike årganger er brukt for datainnsamling og sammenlikning, for å kunne vurdere utviklingen av trusselpersepsjonen knyttet til innsidevirksomhet.

I studien av de ulike dokumentene har jeg søkt etter det som er mest relevant for problemstillingen. De aller fleste dokumentene ble lastet ned i Portable Document Format (PDF) fra internett og lest ved hjelp av Adobe Acrobat Reader. Internett har dermed vært en kilde til datainnsamling, og brukt både til å innhente dokumenter og søk etter supplerende

data. Det ble ikke benyttet noen form for analyseverktøy under studien (Tjora, 2017, s. 226). Men i flere tilfeller ble det benyttet en kombinasjon av søkeord og de innebygde mulighetene Adobe Acrobat Reader[27] gir til ordsøk, for å finne frem til relevant tekst for innhenting av kvalitative data i dokumentene. Denne metoden ble også benyttet til enkelte relevante søk etter kvantitative data. Hensikten med dette har ikke vært å kvantifisere, men å kunne avdekke endringer i fokus og tilnærming i de ulike dokumentene. Sikkerhetsstyring er et eksempel på et ord som ble benyttet til både kvalitativ- og kvantitativdatafangst. Ved bruk av dette søkeordet har jeg kunnet slå fast at 2010 var første gang NSM brukte ordet sikkerhetsstyring i sin årlige risikovurdering, og at ordet ikke benyttes i forarbeidene forut for den første sikkerhetsloven, mens det benyttes 10 ganger i forarbeidene til den nye. Betydningen av dette fremsto som relevant, fordi det ved å undersøke dette kan avdekkes om innføringen av begrepet betydde en endring i tilnærming til styring av sikkerhet. Et annet eksempel er hvordan omfanget på PST sin åpne trusselvurdering har økt, fra 984 til over 5000 ord. Dette er interessant fordi det kan si noe om økt åpenhet om trusselen, som igjen gjør det mulig for virksomhetene å danne seg den samme oppfatningen om risikoene, som EOS-tjenestene.

Intervjuene som ble gjennomført hadde til hensikt å kvalitetssikre funn og konklusjoner, men i dialogen så tilfløt det også supplerende data. Planen var å gjennomføre fokuserte intervjuer. Dette er korte intervjuer, som er anvendbare når det ikke er veldig følsomme eller vanskelige temaer som tas opp, og temaet er sterkt avgrenset samt at man antar at tillit kan etableres relativt raskt i intervjusituasjonen (Tjora, 2017, s. 126). Intervjuene ble lagt til sluttfasen av arbeidet, når dokumentstudiene i all hovedsak var ferdig, slik at de kunne bidra til å teste ut mine egne funn og konklusjoner.

4.3 Datagenerering

Dokumentstudier, hvor jeg har brukt dokumenter som er produsert for andre formål enn forskning, har vært den viktigste kilden til datagenerering i denne oppgaven (Tjora, 2017). I dokumentstudier er det nødvendig å sette dokumentene i inn i en kontekst. Formålet med dokumentene, når og hvor teksten er skrevet, av hvem og til hvem er viktig for forståelsen av dokumentene (Tjora, 2017, s. 183). I denne studien har tekstene i de ulike dokumentene gjensidig bidratt til den kontekstuelle forståelsen ved at jeg, i tillegg til fortolkning av teksten i det enkelte dokumentet, har sett dokumentene i sammenheng og hvordan de gjensidig

[27] https://acrobat.adobe.com/no/no/acrobat/pdf-reader.html

påvirker hverandre (Johanessen, 2018, s. 42). Dette har vært viktig for å kunne generere data knyttet til hvorfor sikkerhetsstyring har utviklet seg. Forarbeidene til loven er grunnlaget for hvordan loven blir, loven legger rammene for utøvelsen av forebyggende sikkerhet, samtidig danner utøvelsen av forebyggende sikkerhet grunnlaget for sikkerhetstjenestenes vurderinger, som igjen påvirker situasjonsforståelsen til de som utarbeider loven. Denne sammenhengen har vært viktig for den kontekstuelle forståelsen under studien, og dermed også datagenereringen. Analysene av dokumentene, som er benyttet i denne oppgaven, har blitt gjort med den hensikt å generere data om hvordan de øverste statsorganer som har utviklet og bestemt rammebetingelsene for sikkerhetsstyring har forstått den virkeligheten som sikkerhetsstyringen skal ivareta. En virkelighet som er presentert i form av skriftlige trussel- og risikoanalyser, av direktorat og etat på lavere nivå i stats hierarkiet.
Dette hadde et potensiale til å kunne avdekke forhold i utviklingen, hvor maktforholdet mellom lovgiver, EOS-tjenestene og virksomhetene har vært av betydning for utviklingen. Har lovgiver definert sin egen sannhet, som følge av andre behov, eller har lovgiver forholdt seg til den etablerte virkeligheten slik den beskrives av EOS-tjenestene i deres trussel- og risikovurderinger? Og hvordan forholder virksomhetene seg til både lovgiver og EOS-tjenestenes offentliggjorte oppfatninger? Disse spørsmålene knytter seg til problemstillingen og forskningsspørsmålene i denne oppgaven, fordi det er vesentlig for forståelsen av utviklingen. Både hvorfor sikkerhetsstyring har utviklet seg, og hvordan utviklingen har vært påvirkes av dette maktforholdet.

De strategiske fokuserte intervjuene har vært viktige supplement for å kunne generere data om utviklingen av sikkerhetsstyringen her til lands. Intervjuene ble gjort med personer med erfaring fra strategisk nivå, myndighetsnivået. Bakgrunnen for dette er at jeg hadde behov for å stille enkelte utfyllende spørsmål knyttet til utviklingen av sikkerhetsstyring, forebyggende sikkerhet og utviklingen av risikooppfatningen knyttet til personellsikkerhet, som jeg ikke fant svar på i dokumentene som er utarbeidet av myndighetene.

Testing av funn og konklusjoner

Jeg har lang erfaring fra arbeid med forebyggende sikkerhet generelt, og personellsikkerhet spesielt. Derfor ville jeg også benytte intervjuene til å kontrollere og teste de funnene og konklusjonene jeg fremla i oppgaven. Jeg ønsket å minimere risikoen for at mine egne erfaringer og meninger, skulle påvirke datainnsamlingen, datagenereringen og dermed påliteligheten til oppgaven. For å veie opp for min egen kunnskap valgte jeg derfor å

henvende meg til to eksperter, som begge har lang erfaring innen forebyggende sikkerhet. Den ene informanten var, i tillegg til sin lange erfaring fra forbyggende sikkerhetsarbeid, delaktig i forarbeidene til både den gamle og nye sikkerhetsloven. Den andre informanten har over lengre tid hatt en sentral rolle i det nasjonale arbeidet med forebyggende sikkerhet på myndighetsnivå. Siden jeg har lagt store deler av studien til det strategiske nivået anså jeg at disse to informantene med sin ekspertise, ville være tilstrekkelig for å komplementere de data jeg fant i dokumentene (Tjora, 2017, s. 130). Intervjuene og spørsmålene hadde med andre ord til hensikt å gi støtte til eller svekke mine funn og tilhørende konklusjoner etter dokumentstudiet. Intervjuene ble derfor gjennomført i sluttfasen av arbeidet med oppgaven. Planen var å gjennomføre fokuserte intervjuer (Tjora, 2017, s. 126). Intervjuobjektenes omfattende kunnskap om temaet, og utstrakt vilje til å dele denne gjorde at tiden som gikk med til intervjuene var i overkant av det tanken bak fokuserte intervjuer legger opp til. Dette var allikevel utelukkende positivt da det ga mer tid og rom for å diskutere mine funn og påstander. Det ene intervjuet ble gjennomført via telefon. Opprinnelig var det planlagt med videomøte, men tekniske problemer gjorde det nødvendig å benytte telefon. Dette intervjuet varte i 51 minutter, etter 10 minutter med forsøk på utbedring av de tekniske problemene med videooverføring. Det andre intervjuet ble gjennomført på intervjuobjektets kontor, og varte i 42 minutter. Min oppfatning er at intervjuene tjente sin hensikt, og at det var en god og uformell intervjusituasjon (Tjora, 2017, s. 119). Intervjuobjektene er anonymisert, og benevnes som henholdsvis I1 og I2 når det refereres til dem.

4.4 Kvalitetskriterier

En viktig del av alt forskningsarbeid er vurderingen av kvaliteten på forskningen. Det er ulike tilnærminger til hvilke metodiske krav som skal stilles til kvalitative metoder. Pålitelighet, gyldighet er kriterier som kan anvendes som kvalitetskriterier (Tjora, 2017, s. 231). I tillegg vil overførbarhet kunne være et tredje kvalitetskriterium.

Pålitelighet

Forskerens forhold og engasjement til forskningstemaet er et vesentlig aspekt i forhold til vurderingen av kvaliteten på forskningen. Nøytralitet er vanskelig å oppnå, men det er avgjørende at forskeren er bevisst de bias som følger av faglig og annen forutinntatt mening og forståelse, og er forberedt på å justere forståelsen underveis. Selv om forskerens forkunnskaper og engasjement kan være en forutsetning for resultatet av forskningen, er det

avgjørende at forskeren er bevisst hvordan dette kan påvirke arbeidet. Videre er det avgjørende at forskeren redegjør for dette og hvordan kunnskapen og erfaringene er brukt i analysen og diskusjonen av funnene (Tjora, 2017, s. 235).

Min kunnskap og lange erfaring innen det undersøkte temaet innbefatter også kunnskap som ikke er offentlig tilgjengelig, som følge av at informasjonen kunnskapen bygger på er sikkerhetsgradert. Det har derfor vært viktig for meg å forholde meg til informasjon som er tilgjengelig for offentligheten, og være bevisst at jeg besitter bakenforliggende kunnskap som ikke kan benyttes. Dette både fordi det ville medføre kompromittering av sikkerhetsgradert informasjon, og fordi det ut ifra et etisk perspektiv ville være uredelig å legge til grunn forhold som vanskelig vil kunne etterprøves.
Mine erfaringer og kunnskap er bygget oppgjennom mer enn 15 år i stillinger knyttet til forebyggende sikkerhet, dette har medført at jeg har et engasjement og en forståelse av tematikken. Dette bidrar til påliteligheten i oppgaven fordi vurderingene som ble gjort underveis er tuftet på lang erfaring og kompetanse om temaet. jeg har vært bevisst mine forkunnskapers mulige påvirkning av arbeidet, og intervjuene har bidratt til å balansere forholdet mellom fagkunnskap og egne meninger. Arbeidet med oppgaven har gitt meg mulighet til å utfordre mine egne antagelser og meninger.

Gyldighet

Gyldighet handler om hvorvidt man faktisk svarer på det man spør om, og om genereringen av dataene besvarer både problemstillingen og forskningsspørsmål. Dette omtales også som validitet (Tjora, 2017). Dette har jeg opplevd som et krevende kvalitetskriterium. Dette skyldes blant annet den nærheten jeg har til tematikken. Det har vært krevende å holde seg til det som er relevant for studien, og ikke ta med andre funn og vurderinger som følge av at disse ble oppfattet som interessante, og kunne fortjent å bli diskutert. Noe informasjon har også måtte avvises fordi den ville økt studiens omfang, slik at den hadde blitt uhåndterlig. Samtidig har informasjonen også vært bidragende til behovet for å endre problemstilling og forskningsspørsmål underveis. Gyldighet har vært en rettesnor gjennom mitt arbeid med oppgaven, Det å filtrere, for meg, både gammel og ny informasjon, slik at den som ble brukt skulle være relevant for studien har vært viktig i arbeidet.

Overførbarhet

Overførbarhet som kvalitetskriteriene handler om hvorvidt funnene har gyldighet utover den gitte konteksten og er relevant og anvendbart i andre situasjoner. Det som etterspørres er om man kan kjenne igjen meningen og om denne meningen gir innsikt av betydning.

Mitt forskningsprosjekt er avgrenset til en begrenset tidsperiode, i tillegg til at den er avgrenset til deler av det større fagfeltet forebyggende sikkerhet. Hvordan forebyggende sikkerhet har utviklet er at av forskningsspørsmålene, men avgrensningene mot personellsikkerhet, virksomhetsnivået og det at problemstillingen retter seg mot sikkerhetsstyring, gjør at ikke alle fagområdene i forebyggende sikkerhet berøres. Riktig nok påvirkes overførbarheten til andre samfunnsområder av oppgavens avgrensninger, men for virksomheter underlagt sikkerhetsloven kan funnene gi mening og innsikt, blant annet fordi det er lite forskning på personellsikkerhet fra et virksomhetsperspektiv i norsk sammenheng. Enkelte av funnene har antagelig en begrenset overførbarhet til virksomheter utenfor sikkerhetsloven, men når det gjelder innsidetrusselen vil de antagelig ha gyldighet og være relevante for virksomheter som ikke er underlagt loven. Dette fordi også disse kan rammes av innsidevirksomhet som påfører virksomheten verditap, selv om verdiene ikke er knyttet til nasjonale sikkerhetsinteresser eller det ligger en fremmed etterretningstjeneste bak hendelsen.

4.5 Metodiske styrker og svakheter

Gjennom studie av offentlig tilgjengelige dokumenter har jeg hatt mulighet kartlegge og vurdere de siste 20 års utviklingstrekk, knyttet spørsmålet hvorfor sikkerhetsstyring har utviklet seg. Hvordan utviklingen har vært, innenfor rammen av forskningsspørsmålene mine, har også vært mulig å studere, og vurdere, i de samme dokumentene. Min egen bakgrunn kan hevdes å gi en svakhet, fordi mine kunnskaper om, meninger, oppfatninger og holdninger til tematikken kan overskygge relevant informasjon. Selv om dette er noe som kvalitativ forskning ofte kritiseres for, hvor forskernes og informantenes subjektivitet er fokuset for kritikken, så ligger noe av styrken i denne studien nettopp i min egen bakgrunn og erfaring. Disse to faktorene har gjort det mulig for meg å finne frem til relevant informasjon i et hav av offentlige dokumenter, fordi jeg har hatt kunnskap om hvor jeg skulle lete (Blaikie & Priest, 2019, s. 79). Kunnskapen og erfaringen jeg har kan også styrke studien, fordi forkunnskapene mine muliggjør presis og relevant spørsmålsstilling knyttet til problemstillingen.
Når intervjuobjektene også har et strekt profesjonelt forhold til tematikken i denne studien, i tillegg til å kvalifisere for å være eksperter på området, så kan dette argumenteres for å gi en

svakhet. Deres kunnskap kan overskygge funn, og gi skjevhet i vurdering av funnenes relevans. Også i denne sammenheng blir min egen kunnskap en styrke, ved at den gir meg mulighet til å gjøre faglig begrunnede vurderinger av ekspertenes uttalelser.

Det kan være vanskelig å få virksomheter til å respondere på spørreundersøkelser og intervjuer om denne forebyggende sikkerhet, fordi den kan oppfattes som sensitiv for virksomhetene. Dette er erfart blant annet i tidligere studie knyttet til innsideproblematikk (Syvertsen, 2007). Derfor er det i denne studien valgt å nytte NSM sine årlige risikovurderinger til datafangst om de deler av virksomhetenes sikkerhetsarbeid som er relevant for denne oppgaven. NSM sine vurderinger baseres på tilsyn og undersøkelser av sikkerhetstilstanden hos mange virksomheter. De kan, på tross av et naturlig bias knyttet til forebyggende sikkerhet, bidra til både økt objektivitet og helhet i datafangsten.

Kombinasjonen av dokumentstudier, min bakgrunn og intervjuer med eksperter, har gitt god kontakt til det jeg har studert. Forståelsen av utviklingen, hvordan ulike faktorer og sammenhenger bidrar til helheten i det jeg har undersøkt, har blitt mulig som følge av denne kombinasjonen. Det er dette som er styrken ved denne studien.

Etiske betraktninger

I innledningen og gjennom hele arbeidet, har etiske betraktninger vært et vesentlig element i avveiningene jeg har gjort i forhold til fremgangsmåtene jeg har valgt. Det å ha et bevisst forhold til at dette arbeidet er noe jeg gjør som privat person, og ikke i kraft av min rolle som fagdirektør i Justis- og beredskapsdepartementet, har vært et forhold jeg har vært meget bevisst. Mulighetene jeg har, gjennom min stilling, til å tilegne meg informasjon som ikke er offentlig tilgjengelig og inkorporer dette i oppgaven, er en fallgruve jeg har hatt fokus på å unngå. Dette mener jeg ville vært både uredelig i et forskningsperspektiv, og ikke minst, ville dette kunne komme i konflikt med arbeidsgivers eventuelle ønske om å ikke offentliggjøre pågående interne prosesser. Bruk av sikkerhetsgradert informasjon har vært uaktuelt, men fokus på å ikke utlevere slik informasjon uintendert har fulgt meg i hele arbeidet.
Min yrkesrolle har også gitt grunn til ettertanke i forbindelse med intervjusituasjonen, blant annet, fordi avdelingen jeg tilhører er etatsstyrer for den virksomheten som en av informantene er ansatt i. Siden jeg skriver denne oppgaven som privatperson og den ikke er noe bestillingsverk fra arbeidsgiver, i tillegg til at jeg ikke har involvert min arbeidsgiver i oppgaveskrivingen eller valg av informanter, noe jeg informerte om før intervjuene, så anser

jeg at relasjonen mellom meg og informanten ikke ga negativ påvirkning i intervju situasjonen. Men avveininger i forhold til min relasjon til informantene og behovet for å få informasjon til besvarelse av mine forskningsspørsmål, var vært sentrale for hvordan jeg valgte å legge opp intervjuene og metodisk utforme og utføre intervjuene.

5 Empiri

I det videre vil det basert på fokuserte intervjuer og dokumentstudier av, i all hovedsak, forarbeidene til sikkerhetslovene, sikkerhetslovene med forskrifter og PST sine trusselvurderinger, men også andre relevante dokumenter, gjøres rede for empiriske funn som er relevant for denne oppgaven.

5.1 Trusselbildet

I den 20-års perioden som er den historiske rammen for denne oppgaven, viser forarbeidene til sikkerhetslovene og trusselvurderingene at det har vært utvikling og endringer i trusselbildet. Det trusselbildet som tegnes i forarbeidene til loven er en kilde til å kunne redegjøre for hvilken persepsjon av risiko og trusler man hadde når loven var i støpeskjeen. Sikkerhetsloven er et verktøy for å håndtere risiko og motvirke trusler. Hvilken persepsjon man hadde på risiko og trusler, knyttet til forbyggende sikkerhet når man utferdiget lovene, er derfor av betydning for hvorfor sikkerhetsstyring innen forebyggende sikkerhet har utviklet seg de siste 20 årene.

Forarbeidene

Ved inngangen til 2000-tallet fremgår det av forarbeidene til det som skulle bli den første sikkerhetsloven i Norge, lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste, at man hadde vært gjennom en avspenningsperiode etter den Kalde krigen (Forsvarsdepartementet, 1997, s. 23). Man sto nå ovenfor et mer uklart trusselbilde, som gjorde at man også var usikker på hva som trengte beskyttelse og hvorfor. Man var kjent med utenlandske etterretningstjenesters måte å operere på i perioden før Berlin murens fall.

«Det er kjent at de sovjetiske og øst-europeiske etterretningstjenester var meget aktive, bl.a med tanke på å verve personer til tjeneste for seg eller få fremmede lands tjenestemenn til å komme i situasjoner som kunne utnyttes med sikte på å få vedkommende til å handle illojalt.» (Forsvarsdepartementet, 1997, s. 23)

Men det tradisjonelle fiendebildet med Sovjetunionen og Warszawapakten, som den dimensjonerende fienden var for lengst borte, og man hadde i stor utstrekning endret oppfatningen av hvor tiltak mot spionasje burde settes inn (Forsvarsdepartementet, 1997, s. 23) Man erkjente allikevel at det fortsatt ble drevet etterretningsvirksomhet mot Norge og norske interesser, og at det var et for fortsatt beskyttelse dette og andre sikkerhetstrusler.

«Behovet for å iverksette forebyggende sikkerhetstiltak vil mest sannsynlig ikke minske i fremtiden, snarere tvert imot.» (Forsvarsdepartementet, 1997, s. 23)

For trusselbildet inneholdt også andre elementer enn utenlandsk etterretningstjeneste. Selv om Norge enda ikke hadde vært utsatt for større terroraksjoner var terror akseptert som en potensiell trussel, og en del av trusselbildet (Forsvarsdepartementet, 1997, s. 24)

Sabotasje i form av aksjoner rettet mot informasjonssystemer, og trusselaktørenes forsøk på penetrasjon av informasjonssystemer blir også fremhevet som elementer i trusselbildet. Tilnærmingen og forståelsen av risikoen knyttet til informasjonssikkerhet i det digitale rom, var økende men ikke på det nivået vi ser i dag (Forsvarsdepartementet, 1997, s. 29)

For ser man hen til omtalen av trusselen knyttet til informasjonssikkerhet i proposisjonen forut for nåværende sikkerhetslov, så har det vært en utvikling i knyttet til oppfattelsen av risiko knyttet til det vi i dag ofte kaller trusler i det digitale rom (Forsvarsdepartementet, 2017, s. 16). Selv om man anerkjente risiko, trusler og sårbarheter knyttet til informasjonssikkerhet, også ved innføringen av den gamle sikkerhetsloven, har denne annerkjennelsen økt. For etter innføringen av den første sikkerhetsloven har det blitt utarbeidet flere offentlige dokumenter som viser til at teknologiutviklingen fører til økte sårbarheter, som kan utnyttes av trusselaktørene. Prop. 153 L viser blant annet til NOU 2015: 13 Digital sårbarhet – sikkert samfunn, Meld. St. 38 (2016 – 2017) IKT-sikkerhet – Et felles ansvar, og Samfunnssikkerhetsmeldingen Meld. St. 10 (2016 – 2017) Risiko i et trygt samfunn (Forsvarsdepartementet, 2017, s. 10).

Basert på disse og NOU 2016:19, Etterretningstjenestens- og PST sine trusselvurderinger for 2017, og NSM sin Risiko 2017, fremheves det i Prop. 153 L at den økte avhengigheten av internett, gjør at nettverksbaserte angrep kan ha omfattende skadevirkninger og har potensial til å ramme hele spekteret av norske interesser (Forsvarsdepartementet, 2017, s. 17).

Truslene og sårbarhetene i det digitale rom, har medvirket til at en egen IKT-sikkerhetslov, nå er i støpeskjeen (Regjeringen, 2020).

I Ot.prp.nr.49 (1996-1997) - Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), kan man lese at trusselbildet ved inngangen til 2000-tallet var uklart, og dermed også hva som måtte beskyttes og hvilken rolle og oppgaver sikkerhetstjenestene skulle ha (Forsvarsdepartementet, 1997, s. 25).

Ut ifra Prop. 153 L, og NOU 2016:19 som lovproposisjonen bygger på, tegner det seg et mer konkret bilde av trusler og risiko gjennom disse dokumentenes kapiteler om dagens

sikkerhetsutfordringer. Men det påpekes i Prop. 153. L at den overordnede sikkerhetspolitiske situasjonen, som påvirker trussel og risiko, hadde blitt mer kompleks enn ved inngangen til 2000-tallet (Forsvarsdepartementet, 2017, s. 15). det beskrives store endringer i samfunnet og virkelighetsbildet innenfor sikkerhetsområdet. Det vises, blant annet til et mer sammensatt trusselbilde enn ved innføringen av den gamle sikkerhetsloven i 2001 (Forsvarsdepartementet, 2017, s. 15).

Utgangspunktet for den trussel- og risikopersepsjonen, som legges til grunn i forarbeidene, til sikkerhetsloven, både til den gamle og den nye, er hentet fra EOS-tjenestene sine vurderinger. Dette følger blant annet av den lovpålagte oppgaven den sentrale enhet i PST er gitt, etter § 17 c. Særlige oppgaver for den sentrale enhet i Politiets sikkerhetstjeneste i politiloven, om å utarbeide trusselvurderinger til bruk for politiske myndigheter. Det er derfor naturlig at det i det følgende gjøres rede for sentrale trekk i utviklingen av trusselvurderingene til PST.

PSTs årlige trusselvurdering

Formålet med PST sine trusselvurderinger er, etter politiloven, å gi beslutningsstøtte til bruk for politiske myndigheter (Justis- og beredskapsdepartementet, 1995, § 17c). Etter PST instruksens § 6, skal PST også utarbeide trusselvurderinger og gi råd om tiltak av betydning for norske interesser, virksomheter og enkeltpersoners sikkerhet (Justis- og beredskapsdepartementet, 2005).

Med den første åpne trusselvurderingen til PST i 2004, og risikovurderingen til NSM året før, ble grunnlaget for myndighetenes trusselpersepsjon mer tilgjengelig for allmenheten.
Det at PST skal utarbeide trusselvurderinger til bruk for politiske myndigheter, og at disse offentliggjøres med en åpen og ugradert versjon, gjør disse trusselvurderingene til et autorativt dokument, som er utgangspunkt for beslutningstakerne, og allmenhetens trusselpersepsjon (Justis- og beredskapsdepartementet, 1995). Utviklingen av dette dokumentet, og endringer som kommer til uttrykk der, er derfor relevant for å forstå den risikopersepsjonen som har ligget til grunn for hvordan har sikkerhetsstyring innen forebyggende sikkerhet utviklet seg de siste 20 årene.
Fra PST sin første åpne trusselvurdering og frem til i dag, har trusselvurderingen blitt utviklet både med tanke på innhold, omfang og presisjon. Den første åpne trusselvurderingen var på 984 ord, hvorav kapittelet om etterretningsvirksomhet inneholder 155 ord. Til sammenligning

er trusselvurderingen i 2020 på over 5000 ord, og over 2000 av dem er knyttet til statlig etterretning.

Internasjonal terrorisme, politisk ekstremisme, etterretningsvirksomhet, spredning av masseødeleggelsesvåpen, og trusler mot norske interesser i utlandet, blir i den første åpne trusselvurderingen fra PST beskrevet som de fremtredende truslene mot vår nasjonale sikkerhet (Politiets sikkerhetstjeneste, 2004). Den generelle terrortrusselen mot norske interesser i Norge beskrives som lav, men for noen utenlandske interesser vurderes terrortrusselen som noe høyere. (Politiets sikkerhetstjeneste, 2004). Trusselaktørene identifiseres som al-Qaida.

Statlig etterretningsvirksomhet, politisk motivert vold, og trusler mot myndighetspersoner blir i den siste åpne trusselvurderingen fra PST beskrevet som de fremtredende truslene mot vår nasjonale sikkerhet (Politiets sikkerhetstjeneste, 2020). I 2020 anses det lave omfanget av radikalisering til ekstrem islamisme i Norge forventes å vedvare. En trussel som i 2013 ble tillagt en helt annen vurdering. Da ble radikalisering og mulige påfølgende terrorhandlinger som følge av dette, vurdert til å utgjøre den mest alvorlige terrortrusselen i Norge. En utvikling som kunne ses i sammenheng med utviklingen i Europa (Politiets sikkerhetstjeneste, 2013).

«Antall ekstreme islamistiske terrorangrep mot Vesten har gått dramatisk ned sammenliknet med toppåret 2017.» (Politiets sikkerhetstjeneste, 2020)

Trusselen fra det høyreekstreme miljøet, handlet i 2004 mye om rekruttering av medlemmer, selv om de høyreekstremes vilje til voldsutøvelse fremstilles som bekymringsfullt. I forkant av årets trusselvurdering (2020) har Norge, med noen års mellomrom, vært utsatt for to terrorhandlinger som knytter seg til høyreekstremisme. Senest i 2019. PST vurderer det som mulig at høyreekstremister vil forsøke å gjennomføre terrorhandlinger i Norge, også i 2020 (Politiets sikkerhetstjeneste, 2020).

I 2020 er den teknologiske utviklingen angitt som bidragsyter til truslene fra både fra fremmed etterretning og høyreekstreme. For etterretningstrusselen handler dette om datanettverksoperasjoner som utgjør en vedvarende og langsiktig trussel mot Norge, og for trusselen fra høyreekstreme om internett som en arena for rekruttering (Politiets sikkerhetstjeneste, 2020).

Når det gjelder internett, så blir dets betydning som arena for ulike trusselaktører tydeligere og tydeligere i trusselvurderingene, fra første gang dette nevnes i 2005 og frem til 2020 (Politiets sikkerhetstjeneste , 2005). Det digitale roms betydning i trussel sammenheng gis økende grad av oppmerksomhet.

Beskrivelsen av trusselen fra fremmed etterretning finnes i alle PSTs vurderinger. Selv om detaljeringsnivået etter hvert gir et mer konkret bilde på hvordan PST opplever denne trusselen, tegnes det et bilde av en trussel som er, og vedvarende har vært, alvorlig og høy. Noe som sjef PST og andre medarbeidere i tjenesten har stadfestet i media flere ganger over flere år.

«Så håper jeg også at man har fått med seg at vi over år har advart om en høy og vedvarende etterretningstrussel mot Norge...»[28]

Et vesentlig utviklingstrekk er hvordan trusselen fra fremmed etterretning mot forsknings og utdanningsmiljøer ser ut til å ha økt. Innsiderhendelsene i 2020 gir vekt til en slik vurdering, som fra 2005 har utviklet seg til å handle om mer enn forskning knyttet til kjemiske, bakteriologiske, radioaktive og nukleære-midler (CBRN-midler) (Politiets sikkerhetstjeneste , 2005). Fra 2009 tegnes det et bredere bilde av at trusselen er knyttet forskning og utvikling generelt, til det i 2013 omhandles detaljert under overskriften «Etterretning mot norske forsknings- og teknologimiljøer» (Politiets sikkerhetstjeneste, 2013)**.** Etterretningstrusselen mot forskningsmiljøene er tema i alle påfølgende trusselvurderinger.

Trusselbildet beskrives, i flere årganger av trusselvurderingene, som preget av en rekke sammensatte utfordringer (Politiets sikkerhetstjeneste, 2016, s. 3). I 2020 beskrives et trusselbilde hvor sammensatt virkemiddelbruk, hvor virkemidler kombineres, kan utgjøre såkalte hybride trusler (Politiets sikkerhetstjeneste, 2020).

NSM sine årlige risikovurderinger

Selv om det er PST og Etterretningstjenesten som har ansvaret for trusselbildet, og NSM for risikobildet, så er risikovurderingene til NSM en viktig bestanddel for det nasjonale trussel- og risikobildet. Risikovurderingene baseres blant annet på samarbeidet med PST og Etterretningstjenesten, og trusselvurderingene deres (Nasjonal sikkerhetsmyndighet, 2019). Dette samarbeidet beskrives allerede i risikovurderingen for 2004 (Nasjonal

[28] https://www.aftenposten.no/norge/i/0EOaJ/pst-sjefen-grunn-til-bekymring

sikkerhetsmyndighet , 2004, s. 2). I de ulike årgangene av NSM sine risikovurderinger, ser man at det er stor grad av sammenheng mellom de truslene som PST beskriver, og de risikoene NSM legger frem. Risiko knyttet til Etterretningstrusselen omtales i alle NSMs vurderinger.

«Etterretningstrusselen mot Norge er omfattende og har et bredt nedslagsfelt.» (Nasjonal sikkerhetsmyndighet, 2020)

NSM har over flere år hatt et spesielt fokus på truslene i det digitale rom, og gitt ut en rekke veiledere knyttet til temaet. Trusselbildet har gitt utgangspunkt for bred omtale av risiko og sårbarheter i det digitale rom i risikovurderingene.

Oppsummering

Trusselbildet har utviklet seg fra et mer diffust beskrevet bilde, til et bilde hvor det gis detaljerte beskrivelser av trusselaktørene og deres modus operandi. Trusselbildet gjenspeiles i stor grad i myndighetenes oppfatning av risiko, og ulike tiltak er iverksatt for å redusere denne risikoen. Spesielt gjelder dette truslene i det digitale rom. Generelt kan man si at trusselbildets utvikling er sterkt knyttet til den teknologiske utviklingen. Sårbarhetene har økt og dermed også mulighetene for trusselaktørene. Vi står i dag ovenfor et trusselbilde, som er mer sammensatt og preget av trusselaktørenes kombinasjon av ulike virkemidler, enn det vi gjorde ved inngangen til 2000-tallet.

5.2 Hvordan har forebyggende sikkerhet utviklet seg de siste 20 årene?

Forarbeidene til de to sikkerhetslovene, og sikkerhetslovene i seg selv er vesentlige kilder for å kunne undersøke hvordan forebyggende sikkerhet har utviklet seg de siste 20 årene. I tillegg er produkter i form av risikovurderinger og veiledninger fra NSM, som er nasjonal fagmyndighet innen forebyggende sikkerhet, relevant for en slik undersøkelse. I det som følger vil det, gjennom fremlegging av empiri fra disse dokumentene, redegjøres for hvordan forebyggende sikkerhet har utviklet seg de siste 20 årene.

Forarbeidene

Stortingsproposisjon 153 L, er basert på Traavikutvalget sin rapport NOU 2016: 19 Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en

omskiftelig tid (Traavikutvalget, 2016). Disse to dokumentene utgjør de mest vesentlige forarbeidene til den nye sikkerhetsloven.

Rettssikkerhet og personvern

En hovedhensiktene med innføring av den gamle sikkerhetsloven var å lovregulere etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene). Disse tjenestene hadde vært gransket av en Stortingsoppnevnt kommisjon, den sålte Lundkommisjonen, som undersøkte hvorvidt tjenestene hadde vært engasjert i ulovlig eller irregulær overvåking av norske borgere (Forsvarsdepartementet, 1997, s. 4). Rettsvern var med andre ord et vesentlig argument for en egen sikkerhetslov, hvor regulering av sikkerhetstjenestene sto sentralt. Den ene informanten påpekte at hensynet til den enkeltes rettigheter, og tilliten til de hemmelige tjenestene (EOS-tjenestene) var drivere for å lov forankre rettigheter og plikter (I1). Ifølge informanten er dette årsaken til at personellsikkerhet er gitt så stor plass i lovene, og rettsvern og nødvendigheten av at sikkerhetsarbeid utøves på en tillitsfull måte forankret i begge lovenes formålsparagrafer (Forsvarsdepartementet, 1998, § 1).
EOS-utvalget har i begge de to sikkerhetslovenes levetid vært sentralt for oppfølging og kontroll av sikkerhetstjenestenes virksomhet, slik at brudd mot rettssikkerhet og personvern fra EOS-tjenestenes side kan oppdages og håndteres[29].

Fleksibilitet og gjensidige avhengigheter

I forarbeidene til den nye sikkerhetsloven kan man lese at rettsvern fortsatt ble vektlagt, men i tillegg var det behov for et mer fleksibelt regelverk som gjorde det lettere å tilpasse seg et stadig mer komplekst og hurtig skiftende trusselbilde (Forsvarsdepartementet, 2017, s. 15). Økte gjensidige avhengigheter på tvers av samfunnssektorer, som gir behov for økt samarbeid mellom statlige organer og private virksomheter, var også en sentral begrunnelse for behovet for en ny sikkerhetslov (Traavikutvalget, 2016, s. 18).
Innføringen av begrepet grunnleggende nasjonale funksjoner (GNF), som er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser, er et av de mest sentrale elementene i utviklingen av forebyggende sikkerhet de siste 20 årene (Forsvarsdepartementet, 2018, § 1-5).

[29] https://eos-utvalget.no/hjem/om-eos/hva-kontrollerer-utvalget/

Traavik-utvalget fremhevet et behov for at den nye sikkerhetsloven, sett i lys av samfunnsutviklingen, også kunne beskytte de funksjonene som er helt avgjørende for statens evne til å ivareta de verdiene sikkerhetsloven skal beskytte. Funksjoner som, fra trusselaktørenes perspektiv, vil være attraktive mål for deres sikkerhetstruende virksomhet (Traavikutvalget, 2016). Det var slike vurderinger som lå til grunn for innføringen av begrepet grunnleggende nasjonale funksjoner (GNF), slik vi finner det definert i sikkerhetslovens § 1-5 i dag.

Selv om formålet med sikkerhetsloven, slik man finner det i formålsparagrafen til de to sikkerhetslovene, ikke er vesentlig endret, så er det mulige virkeområdet endret. Virksomheter som vurderes å ha avgjørende betydning for GNF, kan nå etter vedtak fra sektordepartementene, og forutgående varsling, underlegges sikkerhetsloven. Selv om den utvidelsen av sikkerhetsloven dette innebærer er ment å være begrenset, så er dette vesentlig for utviklingen av forebyggende sikkerhet (Forsvarsdepartementet, 2017, s. 17). Lovens virkeområde avgrenses ikke lenger til å bare gjelde forvaltningsorgan i stat eller kommune, leverandør av varer eller tjenester til slike i forbindelse med en sikkerhetsgradert anskaffelse og anskaffelser til kritisk infrastruktur (Forsvarsdepartementet, 1998, § 2). Det er nå den sikkerhetsmessige betydningen i forhold til GNF, og dermed våre overordnede nasjonale sikkerhetsinteresser som avgjør om virksomheter skal underlegges (Forsvarsdepartementet, 2018, § 1-3). Departementene er ved dette gitt større handlingsrom til å drive sikkerhetsstyring i sin sektor, når de kan underlegge nødvendige virksomheter sikkerhetsloven, og styre disse også med tanke på sikkerhet.

Kostnytte

Selv om virksomhetene ikke gis føringer på hvilke metoder de skal benytte for vurdering av risiko, hverken i ny eller gammel sikkerhetslov, og at det i forarbeidene til begge lovene er lagt vekt på et kostnytte perspektiv, så har man ved innføringen av den nye sikkerhetsloven tatt et steg videre i å vektlegge dette perspektivet. Dette følger av at den nye loven er en funksjonsrettet ramme lov, med fokus på hva som skal oppnås, ikke hvordan. Dette finner man blant annet i virksomhetssikkerhetsforskriften § 15 (Forsvarsdepartementet, 2019). Prinsipper ved valg og utforming av sikkerhetstiltak. I den gamle sikkerhetslovens forskrift om informasjonssikkerhet § 6-15. Bruksnøkler, var det detaljerte bestemmelser for bruk og oppbevaring av nøkler, adgangskort og (Forsvarsdepartementet, 2001, § 6-15). Dette er et eksempel på deskriptive minimumsstandarder, som man fant i den gamle loven og dens

forskrifter, i motsetning til det man nå finner i virksomhetssikkerhetsforskriftens § 15, hvor det nå tydeliggjøres at virksomhetenes sikkerhetstiltak skal tilfredsstille et sett med prinsipper, og ikke et sett med minimumskrav (Forsvarsdepartementet, 2018, § 15). Av prinsippene som skal legges til grunn, ser man at funksjonaliteten og kompleksiteten til tiltakene ikke skal overstige behovet, noe som da forutsetter en vurdering av risiko. Tiltakene skal begrense tilgangen til verdiene, og de skal være redundante, samordnet og ikke minst stå i et rimelig forhold til det som kan oppnås ved tiltaket. Forarbeidene til den nye loven forsterker kost-nytte perspektivet som en viktig faktor i virksomhetenes risikovurderinger (Traavikutvalget, 2016, s. 144) .

Sikkerhetsstyring

Innføringen av, nettopp, begrepet sikkerhetsstyring er annet vesentlig element i utviklingen av forebyggende sikkerhet de siste 20 årene.

Forarbeidene til den gamle sikkerhetsloven, Ot.prp. 49 (1996-1997), snakker ikke om sikkerhetsstyring, men risikostyring er omtalt. (Forsvarsdepartementet, 1997).

Første gangen NSM bruker begrepet sikkerhetsstyring er i Rapport om sikkerhetstilstanden 2010. Begrepet brukes i forbindelse med deres beskrivelse av at ledere, og personell tillagt konkrete sikkerhetsoppgaver, ofte mangler kompetanse om hvordan oppgaver tilknyttet forebyggende sikkerhet skal eller kan løses (Nasjonal sikkerhetsmyndighet, 2010, s. 10). I rapporten fra året før påpekes det at forebyggende sikkerhet i stor grad ikke synes å være omfattet av virksomhetenes øvrige styringssystem. Men som begrep nyttes sikkerhetsstyring først i 2010, hvor styringssystem for sikkerhet er en egen kapitteloverskrift. I 2015 gir NSM ut en veileder i sikkerhetsstyring (Nasjonal sikkerhetsmyndighet, 2015). I den reviderte utgaven av denne veilederen, som kom ut i 2019, forklares sikkerhetsstyring som systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier (Nasjonal sikkerhetsmyndighet, 2019, s. 3). Sikkerhetsstyring var, med andre ord, et etablert begrep innen forebyggende sikkerhet før Traavikutvalget, som ble oppnevnt ved kgl. resolusjon av 27. mars 2015, fikk i oppdrag å utarbeide et nytt lovgrunnlag og den nye loven trådte i kraft fire år senere.

Den ene informanten (I2) påpekte at før sikkerhetsstyring ble et tydelig og definert begrep, så hadde også den gamle sikkerhetsloven elementer av styringssystem for sikkerhet i seg, og at

risikostyringsfenomenet ivaretok sikkerhetsstyringssystemet. Behovet for tydeliggjøring av ansvaret virksomhetens leder har for forebyggende sikkerhet kan, ifølge informanten, årsaksforklare innføringen av begrepet.

Man kan lese i de fleste av NSM sine årlige risikorapporter fra 2009 og utover, at fraværet av system for sikkerhetsstyring, altså sikkerhetsstyring, er vurdert som en risikofaktor og at manglende lederforankring av det forebyggende sikkerhetsarbeidet er en av årsakene til dette (Nasjonal sikkerhetsmyndighet, 2009). I følge den ene informanten har man sett at sikkerhetsleder har utgjort rammen for sikkerhetsarbeidet og at sikkerhetsarbeidet har vært et sidespor i forhold til organisasjonens ledelse og organisasjonens virksomhetsledelse, hvor sikkerhetsstyring bør være en naturlig del (I2). Informanten legger frem at man har observert en fragmentering av sikkerhetsarbeidet, hvor for eksempel innsideproblematikken har blitt lagt som et HR (Human Resources) spor, digital sikkerhet hos driftsavdelingen og fysisk sikring har vært et anliggende for sikkerhetsleder.

I Prop 153 L vises det blant annet til Traavik utvalgets omtale av helhetlig nasjonal sikkerhetsstyring. Man ønsket å legge til rette for en helhetlig tilnærming til forebyggende sikkerhet, for å sikre et harmonisert sikkerhetsnivå, på tvers av ulike virksomheter og ulike samfunnssektorer (Forsvarsdepartementet, 2017, s. 57). Det tas her til orde for at forebyggende sikkerhet skal innarbeides som en del av virksomhetens styringssystem, og at dette forankres i loven.

«Sikkerhetsstyring er helt sentralt for det systematiske arbeidet med sikkerhet.»
(Forsvarsdepartementet, 2017, s. 80)

Dette forslaget ble innarbeidet i sikkerhetslovens § 4-1, hvor det tydeliggjøres at ansvaret for forebyggende sikkerhet i virksomhetene påligger virksomhetens leder, og at arbeidet med forbyggende sikkerhet skal være en del av den øvrige virksomhetsstyringen (Forsvarsdepartementet, 2018). Informant I1 hevdet at en vesentlig faktor i innføringen av begrepet sikkerhetsstyring var nettopp å tydeliggjøre det ansvaret virksomhetene har for forbyggende sikkerhet.

Risiko

Når det gjelder vurdering av risiko sier stortingsproposisjon 153 L at:

«Ettersom forslaget er en såkalt rammelov som forutsettes utfylt med en rekke forskrifter, vil det ikke bli tatt stilling til ulike mulige faglige tilnærminger og metoder for risikovurdering og risikoanalyse. Hvilke tilnærminger og metoder som velges i konkrete tilfeller, vil i stor grad være avhengig av hvilke typer objekter eller systemer som skal vurderes. Systemer som inne-holder mye informasjonsteknologi, vil eksempelvis ofte kreve andre tilnærminger enn rene fysiske objekter og systemer.» (Forsvarsdepartementet, 2017, s. 15)

Man tar med andre ord ikke stilling til, eller kommer med føringer på hvilke metoder som skal brukes ved risikoanalyser- og vurderinger hos virksomhetene som er underlagt sikkerhetsloven. Det vises allikevel til NOU 2016:19 og dennes drøfting av trefaktormodellen, hvor det vises til Forsvarets forskningsinstitutt sin vurdering av at det ikke eksisterer noen beste fremgangsmåte for å vurdere risiko knyttet tilsiktede uønskede hendelser (Forsvarsdepartementet, 2017, ss. 44-45). Det blir, med begrunnelse i at loven i størst mulig grad skal være uavhengig av den videre utviklingen av trussel- og sårbarhetsbildet, ikke gitt føringer på at virksomhetene skal bruke trefaktormodellen (Forsvarsdepartementet, 2017, s. 15).

I virksomhetsforskriftens § 12 og 13 gis det allikevel noen føringer for hva som skal hensyn tas i vurderinger av risiko, og hva som skal vurderes ved håndtering av risiko. I tillegg til vurdering av virksomhetens verdier i forhold til de grunnleggende nasjonale funksjonen og nasjonale sikkerhetsinteresser, skal hensynet til hvilken sikkerhetstruende virksomhet som kan ramme verdiene, sannsynligheten for at sikkerhetstruende virksomhet kan inntreffe, og sårbarheter og konsekvens knyttet til verdiene hensyn tas i vurderingen av risiko (Forsvarsdepartementet, 2018, §§ 12 - 13). Når det gjelder håndteringen av risiko, så skal denne innbefatte vurdering av om risikoen er akseptabel, om sikringstiltakene bør endres, om konsekvensene kan påvirkes, om det er mulig å gjøre seg mindre avhengig av andre virksomheter, og om det er mulig å håndtere risikoen på andre måter (Forsvarsdepartementet, 2018).

I den gamle lovens forskrift om sikkerhetsadministrasjon, § 4-2 Risikovurdering**,** fant man også bestemmelser om risikovurdering. Her ble det gitt føringer på at risikovurderingen skulle ta hensyn til lokale forhold av sikkerhetsmessig betydning og bidra til kosteffektive tiltak, men minimumskravene i sikkerhetsloven skulle legges til grunn (Forsvarsdepartementet, 2001, § 4-2). Det var med andre ord sikkerhetslovens og dens forskrifter sine minimumskrav

som skulle tilfredsstilles i utgangspunktet, noe som altså skiller seg fra den tilnærmingen man har i dagens lov.

Sikkerhetskultur

Et annet, i denne sammenheng, viktig utviklingstrekk for forebyggende sikkerhet er forståelsen av kulturelle betingelser sin innvirkning på forebyggende sikkerhet. Det som kalles sikkerhetskultur, og som på NSMs hjemmesider under temaet sikkerhetsstyring defineres til å være summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd (Nasjonal sikkerhetsmyndighet, 2020). Sikkerhetskultur er ut ifra det man kan forstå fra NSMs hjemmesider, en vesentlig faktor i sikkerhetsstyring.

Sikkerhetskulturens betydning fremkommer av, blant annet, NSM sin omtale av sikkerhetskultur, eller rettere sagt omtale av fraværet av sikkerhetskultur, i flere av de årlige risikorapportene.

«*Manglende sikkerhetskultur kan føre til at risikoatferd opprettholdes, at ledelsen ikke har oversikt over sikkerhetstilstanden og at sannsynligheten for kompromitteringer og alvorlige hendelser øker*» (Nasjonal sikkerhetsmyndighet, 2012, s. 12).

Fraværet av sikkerhetskultur forklares av NSM, blant annet, med at manglende sikkerhetsfaglig kompetanse hos lederne for virksomhetene, medfører manglende lederforankring av det forebyggende sikkerhetsarbeidet. Første gangen NSM bruker begrepet sikkerhetskultur i sine risikovurderinger er i 2006 (Nasjonal sikkerhetsmyndighet, 2006, s. 8). Man finner ikke dette begrepet i hverken den gamle eller nye sikkerhetsloven, eller i deres forskrifter, men begrepet omtales av Traavikutvalget i forarbeidene til sikkerhetsloven. Her vises det blant annet til at NSM og FFI peker på at manglende sikkerhetskultur er den viktigste årsaken til at sikkerhetsnivået i mange situasjoner er for lavt (Traavikutvalget, 2016, s. 84). Sikkerhetskultur omtales i de aller fleste av NSMs årlige risikovurderinger etter 2006. Senest i 2020, hvor man kan lese at virksomheten må legge til rette for en god sikkerhetskultur gjennom å øke de ansattes forståelse av sikkerhetsregler og rutiner samt legge til rette for oppfølging av de ansatte (Nasjonal sikkerhetsmyndighet, 2020, s. 23).

I 2010 påpeker NSM at få ledere har skolering i sikkerhetsstyring, sammenlignet med det de har for eksempel innen økonomistyring (Nasjonal sikkerhetsmyndighet, 2010, s. 10). I tillegg

påpeker en av informantene at når NSM ønsker å få ledere på kurs, så er det nesten utelukkende sikkerhetsledere som deltar, og ikke linjeledere (I2).

Oppsummering

Sikkerhetsloven har, både i gammel og ny versjon, utgjort en betydelig del av rammeverket for forebyggende sikkerhet de siste 20 årene. Lov utviklingen er et resultat av politisk vilje til endring, som følge av dynamikken og raske endringer i både samfunnet og trusselbildet. For virksomhetene har forebyggende sikkerhet utviklet seg fra å være et relativt regelstyrt fagområde, til et fagområde som i større grad lar reelle sikkerhetsbehov hos virksomhetene styre hvilke sikkerhetstiltak som skal implementeres, og hvordan dette gjøres. I stor utstrekning er detaljkravene for hvordan sikkerhetstiltakene skal gjennomføres, erstattet med krav om hva som skal oppnås. Den lovmessige forankringen av begrepet sikkerhetsstyring har tydeliggjort at ansvaret for forebyggende sikkerhet i hovedsak ligger på virksomhetene, og at dette må være et helhetlig arbeid, som inngår i den øvrige virksomhetsstyringen. Noe som betyr at sikkerhetsarbeid ikke kan anses som et fagfelt adskilt fra den øvrige utviklingen, produksjonen og prosessene i virksomheten. Gjennom innføringen av begrepet grunnleggende nasjonale funksjoner, har man også gjort loven mer dynamisk i forhold til hvilke virksomheter som kan, og vil bli underlagt loven. Sikkerhetskultur benyttes ikke som begrep i sikkerhetsloven. Men begrepet har fått en sentral posisjon i det forebyggende sikkerhetsarbeidet ved at NSM fremhever det som en vesentlig faktor for forbyggende sikkerhet generelt, men også sikkerhetsstyring spesielt. Ut ifra dette kan man hevde at forebyggende sikkerhet de siste 20 årene har utviklet seg til et fagområde med et fleksibelt juridisk rammeverk, hvor ansvaret og betydningen av sikkerhetskultur er tydeliggjort.

5.3 Hvordan har risikooppfatningen knyttet til personellsikkerhet utviklet seg de siste 20 årene?

I det følgende vil det redegjøres for utviklingen av risikooppfatningen knyttet til personellsikkerhet de siste 20 årene.

Personellsikkerhet

Personellsikkerhet ble i den gamle sikkerhetslovens forskrift om personellsikkerhet definert som tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres (Forsvarsdepartementet, 2001, § 2).

Den nye loven, og dens tilhørende forskrifter gir ikke en definisjon av personellsikkerhet. NSM gir på sine hjemmesider følgende definisjon av begrepet:

«Tiltak, handlinger og vurderinger for at personer som kan utgjøre en sikkerhetsrisiko ikke plasseres i stillinger som kan bryte sikkerhetsloven.» (Nasjonal sikkerhetsmyndighet, 2019)

Denne definisjonen fremstiller reduksjon av risikoen for brudd på sikkerhetsloven som formålet med personellsikkerhet. I den tidligere forskrift om personellsikkerhet var formålet knyttet til å hindre innsiderhendelser.

«Personellsikkerhet; tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres.» (Forsvarsdepartementet, 2001, § 1-2)

I forarbeidene til den gamle sikkerhetsloven, Ot.prp.nr.49 (1996-1997) Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), sies det at:

«Personellsikkerhet er et viktig element i den forebyggende sikkerhetstjenesten. Tatt i betraktning at det er rikets og våre alliertes sikkerhet som står på spill, og at store skadevirkninger kan oppstå som følge av sikkerhets- og taushetsbrudd, må det legges stor vekt på den grunnleggende forutsetning at det bare er personer man fullt ut kan stole på, som kan gis sikkerhetsklarering.» (Forsvarsdepartementet, 1997, s. 53)

Ut ifra forarbeidene til den gamle sikkerhetsloven, og definisjonen av personellsikkerhet i lovens forskrift om personellsikkerhet, fremgår det dermed at man erkjenner et betydelig risikopotensial knyttet til personellsikkerhet. I forarbeidene til den nye sikkerhetsloven ser man at denne erkjennelsen står ved lag (Traavikutvalget, 2016, s. 21).

Innsiderbegrepet

Innsiderbegrepet har, vært et vesentlig element ved trussel- og risikooppfatningen knyttet til personellsikkerhet hos PST og NSM i flere år.

Når det gjelder lovarbeidet, i forbindelse med den nye sikkerhetsloven, så er innsidebegrepet omtalt flere ganger i Traavikutvalgets NOU 2016:19 - *Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid* (Traavikutvalget, 2016). Mens det i lovproposisjonen vises til PST sin vurdering av at skadepotensialet for innsidevirksomhet i

kombinasjon med datanettverksoperasjoner er stort (Forsvarsdepartementet, 2017, s. 16). Utover dette benyttes ikke innsiderbegrepet i dette dokumentet. Begrepet spionasje benyttes og omtales i begge dokumentene, og gis sin innholdsmessige forklaring i Traavikutvalgets NOU 2016:19. Her forklares spionasje som Innsamling av informasjon ved hjelp av fordekte midler i etterretningsmessig hensikt (Traavikutvalget, 2016, s. 292). Hverken i den gamle eller nye sikkerhetsloven benyttes begrepet innsider, mens spionasje med samme definisjon som man finner i Traavikutvalgets NOU 2016:19 er forankret i begge lovene. Spionasjebegrepet omfatter innsidevirksomhet, men det er gjennom PST og NSM sine vurderinger og veiledere at innsiderbegrepet defineres.

Innsiderbegrepet ble først tatt i bruk av PST i trusselvurderingen for 2013, og NSM ga sin første innholdsforståelse av begrepet i risikovurderingen for 2010:

«Innsideraktivitet kan begås av nåværende eller tidligere ansatte, konsulenter, vedlikeholds personell eller andre. En innsider behøver ikke nødvendigvis selv å ha onde hensikter, men kan være sårbar overfor uvedkommende som er ute etter skjermingsverdig informasjon, enten gjennom forledelse, overtalelse eller press.» (Nasjonal sikkerhetsmyndighet, 2010).

I 2014 gir NSM i sin risikovurdering, innsiderbegrepet følgende innhold:

««Innsidere» er personer som har, eller har hatt, autorisert tilgang til en virksomhet, og som legger til rette for at uvedkommende får uautorisert tilgang til informasjon, objekter eller systemer. En innsider behøver ikke nødvendigvis selv å ha onde hensikter, men kan ha egenskaper som gjør han eller henne utsatt for å bli lurt, fristet eller truet. Gjennom kunnskap om virksomhetens interne rutiner, systemer, sårbarheter og verdier vil en innsider kunne utrette stor skade.» (Nasjonal sikkerhetsmyndighet, 2014)

Dette er en forklaring på innsiderbegrepet som utfyller NSMs senere raffinering av begrepet:

«En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.» (Nasjonal sikkerhetsmyndighet, 2019, s. 9)

PSTs årlige trusselvurdering

I PST sine trusselvurderinger kan man også lese at fremmed etterretning utgjør en trussel mot personellsikkerheten. I trusselvurderingen for 2005 forventes det at utenlandske etterretningstjenester vil forsøke å verve nordmenn med tilgang til sensitiv og skjermingsverdig informasjon (Politiets sikkerhetstjeneste , 2005). Eksempelvis gis det også i 2008 en vurdering av at fremmede staters etterretningsaktivitet mot Norge og norske interesser er på et vedvarende høyt nivå (Politiets sikkerhetstjeneste, 2008). Når PST for første gang navngir kinesisk- og russisk etterretningstjeneste som en trussel i 2015, så er dette med på å gi en klarere oppfatning av hvor trusselen som påvirker risikoen knyttet til personellsikkerhet kommer fra (Politiets sikkerhetstjeneste, 2015).

«De to statene som Norge ikke har et sikkerhetspolitisk samarbeid med, og som samtidig har den desidert største etterretningskapasiteten, er Russland og Kina. Av disse vurderer vi russisk etterretning til å ha det største skadepotensialet for norske interesser.» (Politiets sikkerhetstjeneste, 2015)

Den samme navngivningen, med henvisning til vurderinger fra PST og Etterretningstjenesten, finner man også året etter i Traavik utvalgets utredning (Traavikutvalget, 2016, ss. 57-60).

I 2017 sier PST at vervingsforsøk av personell med stillinger om gir dem tilgang til sensitiv informasjon vil forekomme også dette året (Politiets sikkerhetstjeneste, 2017). Seniorrådgiver i PST, Annett Aamodt, sa på nrk.no 1. september 2020, at trusselnivået for utenlandsk etterretning ikke har økt, fordi det har vært svært høyt de tre siste årene (Norsk rikskringkastning, 2020). Dette, sammen med trusselvurderingene for tidligere år, slår fast at risikoen knyttet personellsikkerhet også er vedvarende og høy. Tidligere PST sjef Benedikte Høyland ga den samme beskrivelsen av trusselnivået i 2014 (Aftenposten, 2014). Hvordan trusselen materialiseres gjennom metoder, hensikt og mål, blir beskrevet i flere av de årlige trusselvurderingene. Når da rekruttering av innsidere også er et gjengangstema fra 2013 med en, eksempelvis, grundig beskrivelse av fremgangsmåte for slik rekruttering i 2018, så fremstiller dette en vedvarende oppfatning om trussel og risiko knyttet til personellsikkerhet (Politiets sikkerhetstjeneste, 2018).

NSMs årlige risikovurdering

I risikovurderingen for 2010, sier NSM at risikoen for at virksomheter blir utsatt for uønsket aktivitet mot graderte og ugraderte systemer antas å være økende, og at plassering eller

utnyttelse av en innsider er en metode, og et virkemiddel, for tilgang til virksomhetens skjermingsverdige informasjon (Nasjonal sikkerhetsmyndighet, 2010). Allerede i sin første risikovurdering påpeker NSM at det alltid vil være et mål for fremmed etterretning å verve folk på innsiden av en virksomhet (Nasjonal sikkerhetsmyndighet, 2003, s. 20). Uten at ordet innsider benyttes er rekruttering av innsidere, og innsideproblematikken tema i rapporten. Det vises blant annet til den interne trussel, som personellsikkerhetsarbeidet er spesielt rettet mot.

Så sent som i 2020 påpeker NSM at de i en årrekke har pekt på at mangelfull sikkerhetsstyring er en av de viktigste årsakene til utilfredsstillende sikkerhetstilstand, og at mangler i sikkerhetsstyringen kan både skyldes, og føre til, en svak sikkerhetskultur i virksomheten (Nasjonal sikkerhetsmyndighet, 2020). I den samme rapporten hevder NSM å ha sett eksempler på manglende oppmerksomhet og kompetanse knyttet til personellsikkerhet, og understreker samtidig at manglende prioritering av personellsikkerhet vil gi en innsider mulighet til å utføre stor skade mot virksomhetens verdier.

Når det gjelder digital sikkerhet, så sier direktøren for NSM i forordet til risikovurderingen for 2019, at NSM opplever at særlig IKT-sikkerhet står stadig høyere på agendaen blant norske ledere (Nasjonal sikkerhetsmyndighet, 2019).

Risiko og andre hensyn

Fokuset på rettsvern og det må være et alminnelig prinsipp at det i forbindelse med utførelse av forebyggende sikkerhetstjeneste ikke skal nyttes mer inngripende midler enn det som er strengt nødvendig, som man også hadde i OT.prp.nr.49. har vært en vesentlig faktor i myndighetenes forståelse av personellsikkerhet gjennom de siste 20 årene (Forsvarsdepartementet, 1997, s. 27). At rettssikkerhet var vesentlig ved innføringen av den gamle sikkerhetsloven, ble tydeliggjort ved hva som ble ansett nødvendig å lovfeste i sikkerhetsloven.

«Departementet har imidlertid begrenset seg til å medta bestemmelser som anses sentrale av hensyn til rettssikkerheten, eller som av andre grunner anses viktig å få nedfelt i en samlet lov om forebyggende sikkerhetstjeneste.» (Forsvarsdepartementet, 1997, s. 6)

I Prop. 53 L, fremgår det at risikoen knyttet til personellsikkerhet har to dimensjoner. Formålet med personellsikkerhet beskrives å være å sikre at personell som skal ha tilgang til sikkerhetsgradert informasjon eller skjermingsverdige objekter og infrastruktur, har den

nødvendige lojaliteten og påliteligheten slik at man kan ha begrunnet tillit til at personen er sikkerhetsmessig skikket. Samtidig understrekes det at, personellsikkerhet er et område hvor myndighetene gis hjemmel til å innhente og behandle til dels meget sensitive personopplysninger om den enkelte. Personellsikkerhet har således fortsatt klare grenseflater mot enkeltindividets rettssikkerhet og personvern. (Forsvarsdepartementet, 2017, s. 114)

Risikooppfattelsen knyttet til personellsikkerhet, har også vært gjenstand for andre risikoavveininger enn rettssikkerhet. Dette ser man blant annet i Traavikutvalgets utredning, hvor man sier at regelverket for personellsikkerhet i hovedsak har en hensiktsmessig tilnærming. Men, for å få en mer effektiv behandling av klareringssaker og dels for å gjøre regelverket mer fleksibelt for individuelle tilpasninger anbefales det å gjøre enkelte justeringer i loven (Traavikutvalget, 2016, s. 21). Risikoen knyttet til personellsikkerhet ble derfor gjenstand for avveining opp imot, oppfattelsen at det var risiko for at behandlingen av klareringssaker ikke var effektiv nok, og at det regelverket ikke var fleksibelt nok. Risikoen knyttet til fleksibilitet medførte noen endringer. Dette gjaldt, blant annet, virksomhetenes adgang til å autorisere utenlandske statsborgere, hvor de ikke var behov for eller forelå sikkerhetsklarering gitt av klareringsmyndigheten, for informasjon gradert BEGRENSET.

Etter den gamle lovens forskrift om personellsikkerhet, måtte virksomhetene innhente tillatelse til slik autorisasjon (Forsvarsdepartementet, 2001, § 2-2). Det samme gjaldt for personer som var nektet klarering av klareringsmyndigheten (Forsvarsdepartementet, 2001, § 5-2). I den nye lovens forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetssikkerhetsforskriften), gjelder kravet kun for utenlandske statsborgere som kommer fra en stat som PST mener utgjør en høy sikkerhetsrisiko for Norge (Forsvarsdepartementet, 2019, § 70). For øvrige utenlandske statsborgere, skal den autorisasjonsansvarlige gjøre en risikovurdering før en eventuell autorisasjon for BEGRENSET kan gis. Til støtte for denne risikovurderingen, kan autorisasjonsansvarlige kan be klareringsmyndigheten om en vurdering av hjemlandets sikkerhetsmessige betydning (Forsvarsdepartementet, 2019, § 70). For personell som er nektet klarering, er det ikke lenger noen bestemmelser om at tillatelse må innhentes før autorisasjon til BEGRENSET kan gis, utover at autorisasjon bare kan gis dersom den autorisasjonsansvarlige ikke har opplysninger som gir rimelig grunn til å tvile på om en person er sikkerhetsmessig skikket (Forsvarsdepartementet, 2018, § 8-9).

Virksomhetsnivået

På virksomhetsnivå skal PST og NSM sine vurderinger, bidra til økt forståelse for truslene og risikoene knyttet til forebyggende sikkerhet, herunder personellsikkerhet. Dette fremgår, blant annet, av PST-forskriftens § 6 (Justis- og beredskapsdepartementet, 2005). Således er disse å anse som viktige for den risikooppfatningen knyttet til personellsikkerhet på virksomhetsnivå. I den forbindelse er det relevant å nevne Næringslivets sikkerhetsråds kriminalitets- og sikkerhets undersøkelse (KRINOS) fra 2019, som bygger på et utvalg ledere og sikkerhetsansvarlige i 2000 private og 500 offentlige virksomheter. Etter kvantitative undersøkelser fremgår det av KRINOS at i bare 17 prosent av virksomhetene er det en eller flere som har lest PSTs trusselvurdering, mens tilsvarende tall for NSMs risikovurdering er 10 prosent. Begge ble lest i noe større grad i offentlige virksomheter enn i private og i store virksomheter i større grad enn i små. Ifølge undersøkelsen så hadde 15% av virksomhetene i privat sektor lest PST sin risikovurdering, mot 26% i offentlig sektor. Når det gjaldt hvor mange som hadde lest NSMs risikovurdering var fordelingen 8% i privat sektor og 19% i offentlig sektor (Næringslivets sikkerhetsråd, 2019, s. 6). Samme type undersøkelse i 2015 viste at kun 4% totalt sett hadde hentet inn trusselvurderingen.

I NSM risikovurdering fra 2018 fremgår det at NSM registrerer at for store ulikheter i risikoerkjennelsen mellom virksomhetenes fag- og sikkerhetsansvarlige i noen tilfeller utfordrer forebyggende sikkerhetsaktivitet på virksomhetsnivå. Problemstillingen er særlig fremtredende i forbindelse med rekruttering av nøkkelpersonell (Nasjonal sikkerhetsmyndighet, 2018, s. 16). Det fremstilles ved dette et innbyrdes konkurranseforhold mellom sikkerhetshensyn og behovet for kompetanse.

Hvis man ser hen til høringsuttalelser i forbindelse med den nye sikkerhetsloven, kan man lese at enkelte anser at praksisen hos klareringsmyndighetene, knyttet til vurderingen av mangelfull personhistorikk var for streng (Forsvarsdepartementet, 2017). LO/NTL uttalte at det var nødvendig å i større grad tilpasse personellsikkerheten til et globalisert og multikulturelt samfunn. Da værende praksis rammet, etter LO/NTL sine uttalelser, deres medlemmer uforholdsmessig hardt. Telenor fremlegger at det å få autorisert en person som ikke er norsk statsborger og/eller har vært bosatt i Norge over lengre tid, som en tilnærmet umulighet (Forsvarsdepartementet, 2017, s. 122). Politidirektoratet utrykker, i sin uttalelse om krav til personhistorikk, bekymring for at en mindre restriktiv linje vil innebære en uthuling av regelverket på et sentralt punkt (Forsvarsdepartementet, 2017, s. 127). Disse eksemplene

uttrykker et forskjellig utgangspunkt for oppfattelsen av risikoen knyttet til personellsikkerhet.

Oppsummering

Myndighetenes risikooppfatning knyttet til personellsikkerhet, har ikke endret seg betydelig de siste 20 årene. Men risikooppfatningen knyttet til personellsikkerhet har, i perioden vært gjenstand for avveining opp imot andre områder. Rettsikkerhet har hele tiden vært et slikt område, mens fleksibilitet og effektivitet har blitt klarere avveiningsområder i perioden. På virksomhetsnivå ser man av forarbeidene til den nye sikkerhetsloven og i NSM sine risikovurderinger, at det er ulik oppfatning av risiko knyttet til personellsikkerhet.
Det er også usikkert i hvilken grad trussel- og risikovurderingene til PST og NSM, som skal bidra til virksomhetenes risikooppfatning knyttet til personellsikkerhet, faktisk lese av virksomhetene.

5.4 Hvordan kan en innsiderhendelse forklares fra et organisatorisk perspektiv?

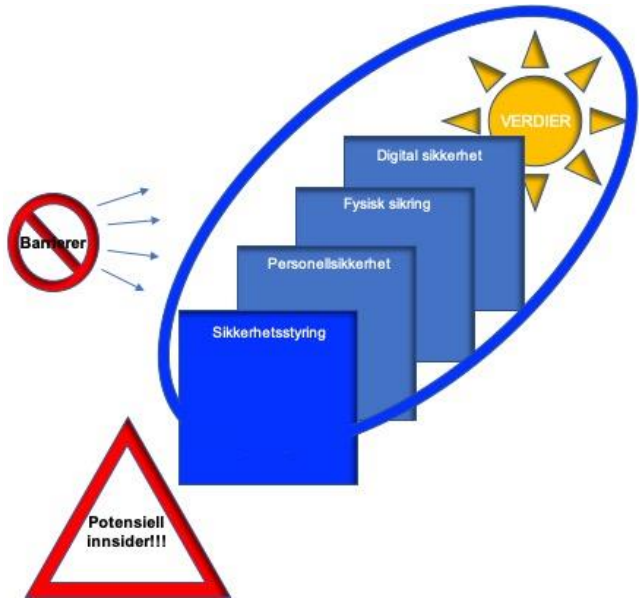
For å forklare en innsidehendelse fra de organisatorisk perspektiv vil jeg i det følgende, med utgangspunkt i sikkerhetsstyringsprosessen, redegjøre for de barrierer som skal motvirke en innsidehendelse.

Personellsikkerhet om tales som en barriere i risikovurderingen for 2019 (Nasjonal sikkerhetsmyndighet, 2019, s. 18). I tillegg er NSMs fagområder på deres hjemmeside[30] delt inni sikkerhetsstyring, fysisk sikkerhet, digital sikkerhet og personellsikkerhet. NSMs beskrivelse av personellsikkerhet som barriere, og inndeling av fagområder er en måte å kategorisere barrierene innen forebyggende sikkerhet. I det videre vil en slik kategorisering legges til grunn for redegjørelsen av virksomhetenes barrierer, som skal motvirke en innsidehendelse. Siden sikkerhetsstyring og personellsikkerhet er mest relevante for denne oppgaven, vil disse vies mest oppmerksomhet.

NSM fremlegger i sine grunnprinsipper om fysisk sikkerhet at, uten et helhetlig perspektiv på sikkerhet vil det være vanskelig for virksomheten å oppnå et akseptabelt sikkerhetsnivå. Akseptabelt sikkerhetsnivå oppnås først når virksomheten har identifisert og implementert

[30] https://nsm.no

både fysiske, IKT-messige og personellmessige sikkerhetstiltak (Nasjonal sikkerhetsmyndighet, 2020, s. 13). Figur 5 under illustrerer dette.

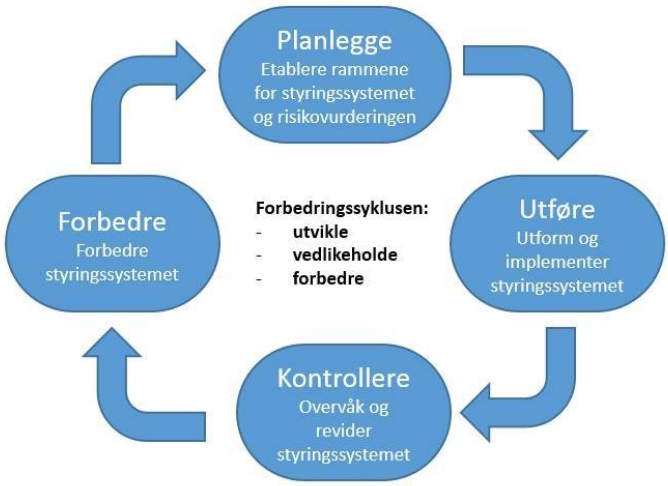


Figur 5: Sikkerhetsstyring er en prosess som styrer alle barrierene som skal motvirke innsidehendelser: Etter inspirasjon av James Reasons Swiss Cheese modell)

Dette helhetlige perspektivet er en av sikkerhetsstyringens flere formål. Hensikten med barrierer er at de skal tidlig skal oppdage feil, fare- og ulykkessituasjoner, redusere muligheten for at disse utvikler seg og begrense skader og ulemper (Petroleumstilsynet, 2017, s. 3).

Sikkerhetsstyring

«Sikkerhetsstyring handler om systematiske aktiviteter som er nødvendige for å oppnå og opprettholde et forsvarlig sikkerhetsnivå for virksomhetens skjermingsverdige verdier.» (Nasjonal sikkerhetsmyndighet, 2019)



Figur 6: Sikkerhetsstyringsprosessen (Nasjonal sikkerhetsmyndighet, 2019, s. 4)

Organiseringen av sikkerhetsarbeidet i virksomhetene, herunder planlegging, utføring, kontroll og forbedring utgjør, som vist i figur 6 over, hovedelementene i sikkerhetsstyring (Nasjonal sikkerhetsmyndighet, 2019).

Utgangspunktet for organiseringen skal være at virksomhetens leder er ansvarlig, beslutter og prioriterer både hvordan sikkerhetsarbeidet skal organiseres, og hvilke tiltak som skal implementeres i barrierene (Nasjonal sikkerhetsmyndighet, 2019, s. 15). Tiltakene bør være basert på risikovurderinger, som ivaretar prinsippene for valg og utforming av sikkerhetstiltak (Forsvarsdepartementet, 2019, §15). At tiltakene er redundante og medfører at det ikke gis mer omfattende tilgang til skjermingsverdige verdier enn nødvendig, at tiltakene er samordnet, og i tillegg til står i et rimelig forhold til hva de er ment å oppnå, er forankret i virksomhetssikkerhetsforskriftens § 15 (Forsvarsdepartementet, 2019). Alle som utfører aktiviteter med betydning for sikkerhet, og ikke bare dedikert sikkerhetspersonell, må deretter bistå i operasjonaliseringen av tiltakene (Nasjonal sikkerhetsmyndighet, 2019, s. 17). Styringssystemet for sikkerhet skal evalueres og øves, minst en gang i året (Forsvarsdepartementet, 2019, § 9). Ett overordnet styrings dokument for det forebyggende sikkerhetsarbeidet skal fastsettes av virksomhetens leder, og dokumentere at styringssystemet for sikkerhet og sikkerhetstiltakene gir et forsvarlig sikkerhetsnivå. Dette fremkommer av kapittel 2. Sikkerhetsstyring i virksomhetssikkerhetsforskriften (Forsvarsdepartementet, 2019, s. 32).

Sikkerhetsstyring kan med andre ord sies å være det som binder alt sikkerhetsarbeidet i organisasjonen sammen og muliggjør et helhetlig perspektiv på sikkerhet, hvor også

vurdering av innsderisikoen er en vesentlig del for dette perspektivet. Kravene som stilles til sikkerhetsstyring er i all hovedsak rettet mot hva som skal oppnås og ikke hvordan. Dette stiller store krav til sikkerhetsfagligkompetanse hos ledernivået i virksomhetene, men også hos de andre nivåene. En av informantene påpekte betydningen av kompetanse hos virksomhetene og sa følgende: « Kompetanse er et nøkkelord.» (I2). Manglende sikkerhetsfagligkompetanse hos virksomhetene, som gir svikt i sikkerhetsstyringen kan derfor være en måte å forklare en innsidehendelse fra et organisatorisk perspektiv.

I det videre vil det redegjøres for den enkelte barrieres betydning for å forklare en innsidehendelse fra dette perspektivet.

Fysisk sikring

Fysisk sikring i form av fysiske barrierer er også et tiltak, som er viktige for å motvirke innsidehendelser, blant annet, fordi de kan bidra til redusert risiko knyttet til innsidertrusselen.

«Formålet med fysiske barrierer er å hindre og forsinke trusselaktører tilstrekkelig før de kommer frem til verdiene slik at planlagt reaksjon kan iverksettes.» (Nasjonal sikkerhetsmyndighet, 2020)
Fysiske barrierer som, for eksempel, dører, låser, og andre tekniske sikkerhetstiltak, i kombinasjon med sone inndeling, hvor det kreves ulik autorisasjon for tilgang til de ulike sonene, kan redusere innsiderisikoen ved at alle ikke har tilgang til alle verdiene i virksomheten (Nasjonal sikkerhetsmyndighet, 2020). Fysiske barrierer kan ofte kategoriseres under passive barrierer. Et gjerde, eller en forsterket vegg, trenger ikke aktivisering for å oppnå sitt ytelsesmål. Det er ut ifra dette mulig å forklare en innsidehendelse fra et organisatorisk perspektiv, med at mangler i tiltakene til barrieren fysisk sikring motvirker en effektiv soneinndeling og gir ukontrollert tilgang til virksomhetenes verdier.

Digital sikkerhet

På virksomhetsnivå er kryptering, passordbeskyttelse, autorisasjonsskiller og brannmurer og overvåkning av IKT-systemet, er sentrale verktøy i barreien digital sikkerhet. På samme måte som barrieren fysisk sikkerhet, skal den redusere innsiderisikoen ved at alle ikke har tilgang til alle verdiene i virksomhetens informasjonssystemer. Tiltakene i barrieren kan være enten passive eller aktive og ofte rettes de mot digitale angrep utenfra, men de kan også nyttes for å motvirke innsidehendelser. Gjennom å overvåkning av IKT-systemene kan unormal aktivitet

fra innsiden i virksomheten detekteres og analyseres for å vurdere om det kan være innsideraktivitet. Fra et virksomhets perspektiv er derfor en mulig forklaring på en innsidehendelse manglende evne til å detektere unormal intern aktivitet i virksomhetenes IKT-systemer.

Personellsikkerhet

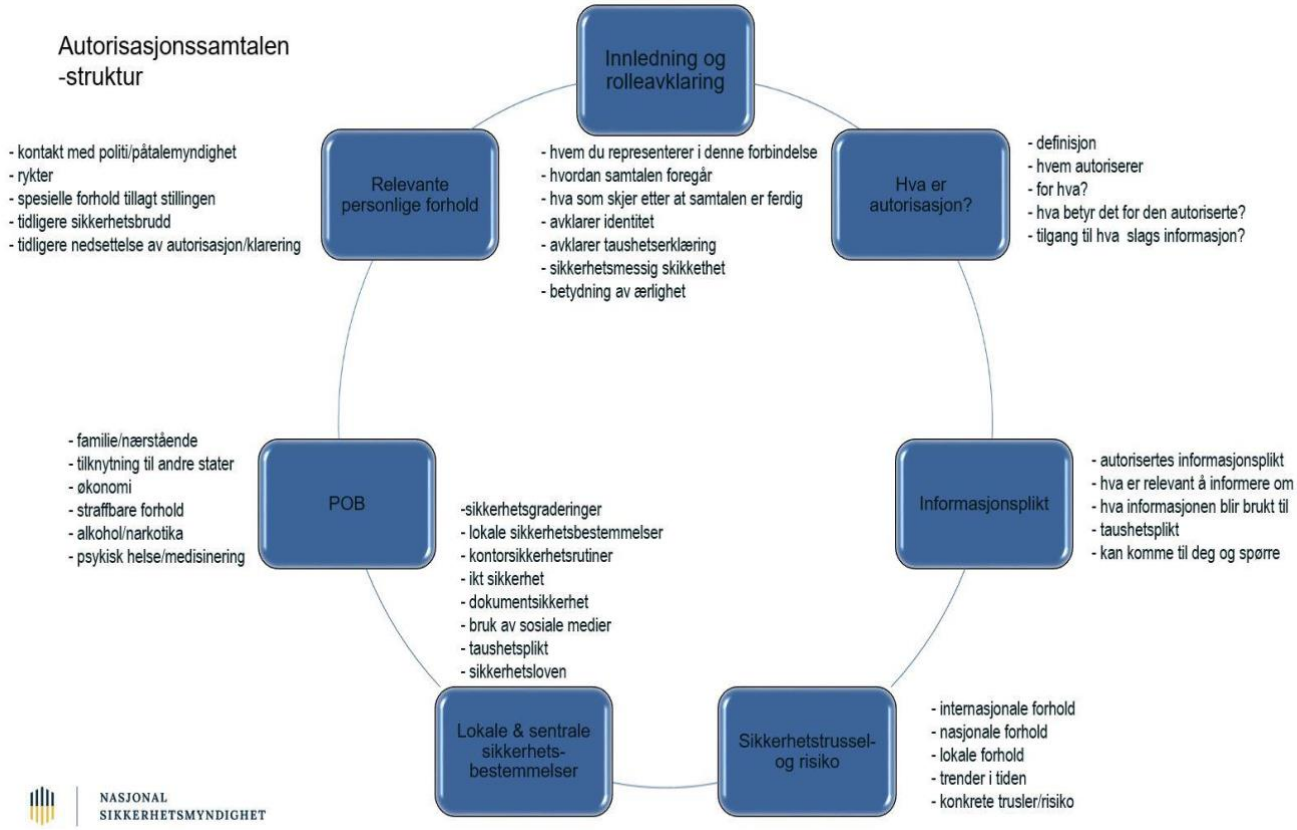
Personellsikkerhet er en barriere, som omfatter alle de tiltak, handlinger og vurderinger som gjøres for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres (Forsvarsdepartementet, 2001). De mest sentrale tiltakene, handlingene og vurderingene innen personellsikkerhet er sikkerhetsklarering, autorisasjon og daglig sikkerhetsmessig ledelse av personellet. Personellsikkerhet er en aktiv barriere, fordi den i stor grad krever aktivisering gjennom autorisasjonsprosessen, dagligsikkerhetsmessig ledelse, og rapportering. Den daglige sikkerhetsmessige ledelsen hos virksomhetene er ment å fange opp endringer hos autorisert personell, som er av sikkerhetsmessig betydning.

Autorisasjon

«Forenklet kan vi si at autorisasjonsprosessen er spørsmålet om lederen har den nødvendige grad av tillit til at den autoriserte håndterer sikkerhetsgradert informasjon på den måten den skal håndteres.» (Nasjonal sikkerhetsmyndighet, 2011, s. 3)

Autorisasjon kan gis av den, eller de i virksomheten som er utpekt til autorisasjonsansvarlige. Autorisasjon er en prosess, hvor gjennomføring av en autorisasjonssamtale med den som skal autoriseres er en vesentlig del av denne prosessen.

Figur 7 på neste side, viser autorisasjonssamtalens struktur og innhold. Hvem som gjennomfører denne samtalen er ikke lovbestemt. Men en viktig del av autorisasjonssamtalen er informasjonsoverføring fra autorisasjonsansvarlige til den som skal autorisere. Informasjonen den som leder samtalen gir om sikkerhetstrussel og risiko, og lokale og sentrale sikkerhetsbestemmelser, skal bidra til den sikkerhetsmessige forståelsen og kunnskapen hos den som autoriseres. Informasjon fra den som skal autoriseres skal autorisajonsansvarlig benytte til å vurdere sin egen tillit til den som skal autoriseres.



Figur 7: Autorisasjonssamtalen – struktur (NSM)[31]

Når samtalen er gjennomført og dokumentert, kan autorisasjon gis. Men autorisasjonssamtalen er ikke en engangsaffære. Den skal, etter den første samtalen før den første autorisasjonen ble gitt, gjennomføres når en autorisert person selv ber om det, ved reklarering eller når en autorisasjonsansvarlig ellers finner grunn til det (Forsvarsdepartementet, 2019, § 68). Autorisasjonen er etter dette gyldig så lenge den autoriserte er tilknyttet virksomheten, det ikke har oppstått forhold ved den autoriserte som har gjort at autorisasjonen har blitt nedsatt, suspendert eller tilbakekalt, og vedkommende har nødvendig sikkerhetsklarering når dette er et krav(Forsvarsdepartementet, 2019, § 68).

Ut ifra et organisatorisk perspektiv kan derfor en mulig forklaring på en innsidehendelse være at virksomheten ikke har fanget opp forhold ved den autoriserte som burde vært gjenstand for vurdering i forhold til mulig innsidevirksomhet.

[31] https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/autorisasjon/

Evnen til å fange opp slike forhold henger sammen med det andre vesentlige tiltaket innen personellsikkerhet.

Daglig sikkerhetsmessig ledelse

Tiltaket daglig sikkerhetsmessig ledelse innebærer at autorisasjonsansvarlige følger opp det autoriserte personellet i virksomheten, og griper inn når denne blir klar over forhold ved den som er autorisert som antas å være av sikkerhetsmessig betydning. Tiltaket er et av de viktigste faktorene for å motvirke innsidehendelser[32].

Ut ifra et organisatorisk perspektiv kan derfor en mulig forklaring på en innsidehendelse være fravær av daglig sikkerhetsmessig ledelse, som gjør at virksomheten ikke har fanget opp forhold ved den autoriserte som burde vært gjenstand for vurdering i en autorisasjonsprosess.

Oppsummering

Manglende sikkerhetsfagligkompetanse hos virksomhetene, som gir svikt i sikkerhetsstyringen kan være en måte å forklare en innsidehendelse fra et organisatorisk perspektiv, som blant annet vill påvirke styringen av virksomhetenes barrierer. På barriere nivå er det mulig å forklare en innsidehendelse fra et organisatorisk perspektiv med at mangler i tiltakene til barrierene medfører at det er ukontrollert tilgang til virksomhetenes verdier, og at forhold som kan indikere innsidevirksomhet ikke detekteres, analyseres og håndteres. Sikkerhetsfaglig kompetanse er nøkkelord for virksomhetenes evne til å motvirke slike hendelser.

[32] https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/autorisasjon/

6 Drøfting

I det følgende vil forskningsspørsmålene, basert på de empiriske funnen, bli drøftet opp imot valgte teorier.

6.1 Hvordan har forebyggende sikkerhet utviklet seg de siste 20 årene?

I et nasjonalt sikkerhetsperspektiv, er hensikten med forbyggende sikkerhet å unngå organisatoriske ulykker i form av skade på våre grunnleggende nasjonale funksjoner og nasjonale sikkerhetsinteresser som er forårsaket av sikkerhetstruende virksomhet.
HRO teorien er derfor relevant for denne oppgaven fordi at den forklarer hvordan organisasjoner har lykkes med å unngå ulykker på tross av dynamikken og de raske endringene i samfunnet, og hevder videre at sikkerhetskultur kan motvirke alvorlige ulykker knyttet til komplekse organisasjoner.

Rettssikkerhet og personvern

Enkeltindividets rettsvern og bestemmelsene om at sikkerhetstiltakene ikke skal være mer inngripende enn nødvendig, kan hevdes å ikke ha vært gjenstand for endring innen forebyggende sikkerhet. Men disse prinsippene, som var noen av hoved driverne for lovfesting av forebyggende sikkerhet, står like støtt i dag som de gjorde ved inngangen til 2000-tallet. HRO-teoriens tilnærming er at alle deler av organisasjonen inkluderes, slik at vesentlige risikoer kan identifiseres og håndteres [33]. En slik altomfattende tilnærming er, som følge av rettsikkerhet og personvern ikke ønskelig, når det kommer til forebygging av sikkerhetstruende virksomhet. Slik er det i ny lov, og slik var det i den gamle (Forsvarsdepartementet, 1998, § 6).
Dette illustrerer på den ene siden en forskjell mellom tilnærmingen til sikkerhet når det gjelder intenderte og ikke intenderte hendelser, i tillegg til at det er et eksempel på et område hvor det ikke er ønskelig å ta ut full effekt av sikkerhetsstyringen. På den andre siden kan lovens fokus på rettssikkerhet og personvern hevdes å imøtegå HRO-komponenten rettferdighetskultur. Ingen skal utsettes for uforholdsmessig urettferdig, hverken etter sikkerhetsloven eller HRO-teorien. Selv om rettferdighetskomponenten i HRO-teorien har et idealistisk preg, og så ledes kan hevdes å burde tilleggs mindre vekt i sammenheng med nasjonal sikkerhet, så er den en vesentlig komponent i et demokratisk samfunn. Fraværet av

[33] https://proactima.com/kurs-og-opplaering/rammeverk-for-risikostyring/

endring i rettssikkerhet og personverns betydning for forebyggende sikkerhet kan således hevdes å være en ønsket utvikling.

Fleksibilitet

Den gamle sikkerhetsloven inneholdt flere deskriptive krav, og var i all hovedsak avgrenset til å omfatte forvaltningsorgan i stat eller kommune, leverandør av varer eller tjenester til slike i forbindelse med en sikkerhetsgradert anskaffelse og anskaffelser til kritisk infrastruktur (Forsvarsdepartementet, 1998, § 2). Når man i den nye sikkerhetsloven innførte begrepet grunnleggende nasjonale funksjonene (GNF), hvor virksomhetens betydning for GNF er avgjørende for om de skal underlegges sikkerhetsloven eller ikke, så var dette en vesentlig endring fra gammel lov i forhold til fleksibilitet. Når vi nå har en lov som ikke avgrenser virkeområdet til stat og kommune, og den har langt færre deskriptive krav, så har dette bidratt til en utvikling mot større grad av fleksibilitet innenfor forbyggende sikkerhet.
Dette sammenfaller med det som i HRO-teorien benevnes som fleksibel kultur, og samtidig er en av de faktorer som kjennetegner virksomheter som lykkes med innføringen av risikostyring (Aven, et. al, 2016, s. 59). Dette handler om evnen til å tilpasse seg effektivt til foranderlige krav. Forutsetningen for at virksomhetene, som er av betydning for våre nasjonale sikkerhets interesser, skal kunne sikre våre nasjonale sikkerhetsinteresser mot et trussel- og risikobilde i stadig endering er forankret i både lov og teori. Dermed kan man, med utgangspunkt i HRO-teorien, og forskjellene mellom den gamle og den nye lovens krav og virkeområde, argumentere for at utviklingen har gitt større grad av fleksibilitet innen forebyggende sikkerhet de siste 20 årene, og at utviklingen har vært gunstig.

Kostnytte

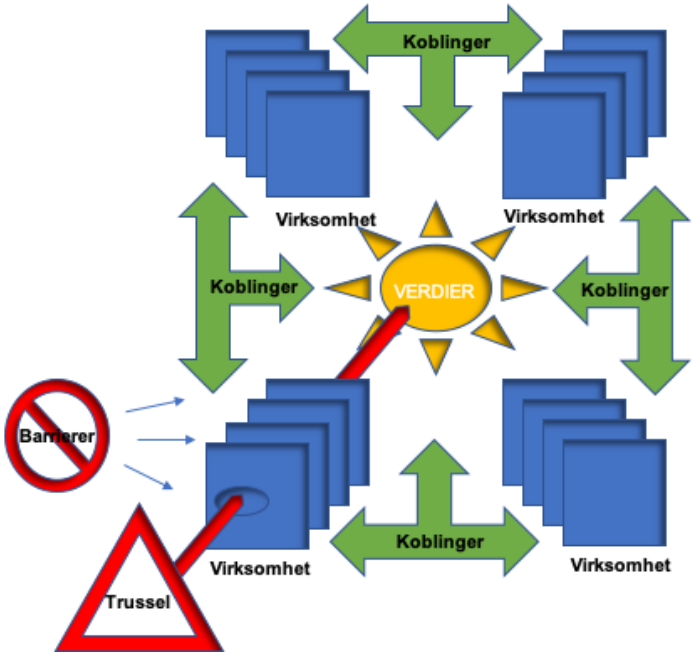
Samsvar mellom ressursbruk på risikostyringen og risiko, ble fremhevet både i forarbeidene til den gamle og den nye sikkerhetsloven. Men i forarbeidene til den nye er kostnytte aspektet ytterligere forsterket, ved at det understrekes at kostnadene ved sikkerhetstiltak etter loven skal stå i et rimelig forhold til det som oppnås ved tiltaket (Traavikutvalget, 2016, ss. 144-145). Sikkerhetsloven § 3-6 forankrer dette i loven (Forsvarsdepartementet, 2018). Dette samsvarer med det som i HRO teorien kalles proporsjonalitet, og er ifølge denne teorien en faktor som kjennetegner virksomheter som har lykkes med risikostyringen[34]. Fleksibiliteten i

[34] https://proactima.com/kurs-og-opplaering/rammeverk-for-risikostyring/

den nye loven gir større muligheter til å ivareta kostnytte perspektivet, fordi virksomhetene ut ifra egen risikovurdering og ikke regulatoriske krav, kan avgjøre hvor mye ressurser det er nødvendig å avsette til sikringstiltakene.
På den ene siden kan man derfor hevde at utviklingen av et mer fleksibelt regelverk har gitt muligheten til en utvikling av større mulighet for ivaretagelse av kostnytte perspektivet, og at dette ut ifra HRO-teorien taler for at utviklingen har vært positiv.

Gjensidige avhengigheter

På den andre siden kan man hevde at tette koblinger, det som i forarbeidene til ny sikkerhetslov kalles økte gjensidige avhengigheter og er noe av bakgrunnen for den nye loven, gjør fleksibilitet og proporsjonalitet til svakheter og at utviklingen derfor har vært negativ (Traavikutvalget, 2016, s. 18). Utgangspunktet for dette argumentet, er at de grunnleggende nasjonale funksjonene (GNF) som gir evne til ivaretagelse av våre nasjonale sikkerhetsinteresser, som kan benevnes som verdier, i mange tilfeller understøttes av flere virksomheter. Når det er slik at flere virksomheter kan understøtte samme grunnleggende nasjonale funksjon, så gjør dette at beskyttelsen av denne verdien avhenger av adekvat sikringsnivå i alle virksomhetene som understøtter samme GNF. Figur 8 nedenfor illustrer dette.



Figur 8: Gjensidige avhengigheter og ulikheter i virksomhetenes sikkerhetsnivå sin konsekvens for verdien som skal beskyttes: Inspirert av Jams Reasons Swiss Cheese model

Fraværet av minimumsstandarder, slik man fant dem i den gamle sikkerhetsloven, gjør at det kan oppstå ulikheter i sikringsnivået hos de ulike virksomhetene. Ulikhetene kan komme av manglende prioritering av forebyggende sikkerhet, lav sikkerhetsfaglig kompetanse, og bidra til latente feil i sikkerhetsstyringen og feilhandlinger. Dermed oppstår det svakheter, som på tross av adekvat sikkerhetsstyring med tilhørende adekvate sikringstiltak hos øvrige virksomheter, gir mulighetsrom for trusselaktørene. Fleksibilitet og proporsjonalitet kan dermed, som følge av gjensidige avhengigheter, argumenteres for å ha bidratt til at forebyggende sikkerhet har utviklet seg i feil retning, på tross av samsvar mellom lovverk og teori.

Sikkerhetsstyring

Samtidig kan det hevdes at svakheter i utviklingen av forebyggende sikkerhet som følger av økt fleksibilitet, økte gjensidige avhengigheter og økt fokus på kostnytte, motvirkes av at lovgivningen og virksomhetssikkerhetsforskriftens kapittel to og tre forutsetter at sikkerhetsstyring dekker hele det forebyggende sikkerhetsarbeidet, også gjensidige avhengigheter, og er dimensjonert i forhold til risikoen for sikkerhetstruende virksomhet (Forsvarsdepartementet, 2019, ss. 1-6). De gjensidige avhengighetene skal dermed omfattes av den risikovurderingen virksomhetene gjør, og sikre at sikkerhetsnivået ikke bare er adekvat hos den enkelte virksomheten, men hos alle virksomheten som understøtter samme GNF. Sikkerhetsloven fastslår at forebyggende sikkerhet skal være en del av virksomhetens øvrige virksomhetsstyring (Forsvarsdepartementet, 2018, § 4-1). Sikkerhetsstyring skal dermed bidra til en helhetlig tilnærming til det forebyggende sikkerhetsarbeidet innad og på tvers av virksomhetene, og motvirke fragmentering av dette arbeidet. Innføringen av begrepet sikkerhetsstyring, og at dette begrepet er forankret i sikkerhetsloven, kan ut ifra dette hevdes å være sentralt for utviklingen av forebyggende sikkerhet. Dette gir argument for at innføringen av begrepet sikkerhetsstyring også forutsetter at virksomhetenes arbeid med forebyggende sikkerhet skal være synkronisert med, og integrert i, deres øvrige produksjon og aktiviteter.
I forarbeidene til sikkerhetsloven kan man lese at det fra virksomhetene påpekes et behov for lovregulering som motvirker fragmentering av det forebyggende sikkerhetsarbeidet (Forsvarsdepartementet, 2017, s. 76 og 109).
Denne forståelsen av forebyggende sikkerhet skal være synkronisert med, og integrert i, virksomhetenes øvrige produksjon og aktiviteter underbygges av HRO-teorien, som fremlegger at dette er noe som kjennetegn ved virksomheter som lykkes med å styre risikoen og derigjennom unngå ulykker. Utviklingen av forebyggendesikkerhet til å bli integrert i den

øvrige virksomhetsstyringen, med innføringen av begrepet sikkerhetsstyring som verktøy for større grad av tilnærming til fagområdet, kan derfor hevdes å være påvirket av erfaringer på virksomhetsnivå.

På den ene siden kan man ut ifra dette hevde at forbyggende sikkerhet har utviklet seg til å bli et fagområde hvor helhetlig tilnærming er helt sentralt. På den andre siden kan man hevde at dette også var tilfelle under den gamle sikkerhetslovens regime. Men det fantes ingen krav til overordnet styring og integrering av forebyggende sikkerhetsarbeid i den gamle loven og dens forskrifter. Riktignok var virksomhetens leder også etter den gamle lovens § 5 ansvarlig for det forebyggende sikkerhetsarbeidet i virksomheten (Forsvarsdepartementet, 1998). Men ut ifra denne lovens forskrift om sikkerhetsadministrasjon kan man tolke at forebyggende sikkerhet i stor grad handlet om håndtering av risiko etter en risikovurdering, lokalt hos den enkelte virksomhet (Forsvarsdepartementet, 2001, §§ 4-1 og 4-2). Den overordnede styringen av forebyggende sikkerhet og tildelingen av ansvaret for den, som tydeliggjør at forebyggende sikkerhet skal være en del av virksomhetenes øvrige styringssystem, og at det innbefatter mer enn lokal håndtering av risiko, fant man med andre ord ikke krav om i den gamle sikkerhetsloven og dens forskrifter.

Man kan derfor, med utgangspunkt innføringen av begrepet sikkerhetsstyring og HRO-teoriens vektlegging av synkronitet og integrering som kjennetegn ved virksomheter som lykkes med å styre risikoen, hevde at forebyggende sikkerhet har utviklet seg til et mer helhetlig og omfattet fagområde og at dette er en positiv utvikling.

Sikkerhetskultur

At forebyggende sikkerhet har utviklet seg til et mer helhetlig og omfattet fagområde, kan også underbygges med det økte fokuset på sikkerhetskultur. Fra begrepet introduseres i NSM sin risikovurdering i 2006, har betydningen av sikkerhetskultur gjentatte ganger blitt vektlagt som vesentlig element i arbeidet med forebyggende sikkerhet i de etterfølgende risikovurderingene. I forarbeidene påpeker Traavikutvalget gjentatte ganger sikkerhetskulturens betydning for forebyggende sikkerhet, med henvisning til NSM sine vurderinger (Traavikutvalget, 2016, s. 84). Selv om begrepet ikke benyttes i den nye loven, eller dens forskrifter, så gir forarbeidenes vektlegging av begrepet grunn til å hevde at

sikkerhetskultur har vært en vesentlig faktor i utviklingen av sikkerhetsloven, og dermed også for utviklingen av forebyggende sikkerhet.

«Nasjonal sikkerhetsmyndighet definerer sikkerhetskultur til å være summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.»[35]

Det kan med utgangspunkt i både NSMs definisjon av sikkerhetskultur og HRO-teoriens tilnærming til at sikkerhetskultur innehar komponentene rapporterings-, rettferdighets-, fleksibel-, lærende-og en informert kultur, hevdes at den økte vektleggingen av sikkerhetskultur de siste 20 årene er den faktoren som er har hatt mest betydning for hvordan forebyggende sikkerhet har utviklet seg (Reason, 2016, ss. 195-196).
Innholdet i NSM sin definisjon og HRO-teoriens komponenter, tilsier at sikkerhetskultur er en forutsetning for helhetlig tilnærming til forebyggende sikkerhetsarbeid ved at sikkerhetskultur utgjør virksomhetenes totale sikkerhetsatferd og derfor er en forutsetning for at sikkerhetsstyringen integreres i den øvrige virksomheten. Sikkerhetskulturen i virksomhetene vil etter dette bety at verdier og oppfatninger knyttet til forebyggende sikkerhet må deles på alle nivåer i virksomhetene (Reason, 2016, s. 192). Samtidig kan det hevdes at kunnskapsbasert forankring av forebyggende sikkerhet på ledernivå er det mest avgjørende for sikkerhetskulturen. Dette fordi sikkerhetsstyringen i virksomheten avgjør hvordan forebyggende sikkerhet prioriteres i forhold til de øvrige produksjonsmålene og økonomiske målsettingene i virksomheten. Uten en slik forankring kan det hevdes at risikoen for virksomhetens ledelse ikke vil ha eller opprettholde fokus på og prioritere forebyggende sikkerhet, når andre krav gjør seg gjeldende (Rasmussen, 1997). Dette underbygges av den ene informantens henvisning til at det er mange og forskjellige virksomheter som er underlagt sikkerhetsloven, og at formålet for virksomhetene sjeldent er sikkerhet men produksjon av noe annet (I2). Lederes fokus er ofte på bunnlinja og store avtaler, mens sikkerhet bare er noe som skjer. Dermed ligger forholdene til rette for at gapet mellom sikkerhetsnivået og risikoen øker, ved at de iverksatte sikkerhetstiltakene eroder (Reason, 2016, s. 6).
Virksomhetenes sikkerhetskultur kan derfor hevdes å være en forutsetning for at de stadig mer omfattende og detaljerte trussel- og risikovurderingene til PST og NSM, til adekvate sikkerhetstiltak etter sikkerhetsfagligfunderte risikovurderinger.

[35] https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/

Selv om NSM gjentatte ganger har påpekt svakheter i virksomhetenes sikkerhetskultur, så kan det hevdes at den økte vektleggingen av sikkerhetskultur har vært vesentlig for hvordan forebyggende sikkerhet har utviklet seg de siste 20-årene utvikling. Dette fordi sikkerhetskultur er en viktig faktor for hvordan virksomhetene organiserer seg, forstår og styrer risikoen i forhold til et dynamisk trusselbilde.

Oppsummering

Siden den nye loven med sine fleksible rammer trådte i kraft så sent som 1. januar 2019, så kan det fremstå som prematurt å si noe om virkningen av den nye loven, i forhold til sikkerhetsstyring, utover at begrepet sikkerhetsstyring er blitt et begrep forankret i en lov. Men selv om det er utfordrende å vurdere virkningen av den nye loven enda, så kan man hevde at utviklingen med innføring av nye begreper som grunnleggende nasjonale funksjoner og sikkerhetsstyring, og sikkerhetskultur som en fremhevet faktor innenfor forebyggende sikkerhet, har flere av HRO-teoriens elementer i seg og at det derfor kan hevdes at utviklingen av forbyggende sikkerhet har gått i riktig retning.

6.2 Hvordan har risikooppfatningen knyttet til personellsikkerhet utviklet seg de siste 20 årene?

Det er naturlig å tenke at den oppfatningen virksomhetene har av risiko knyttet til personellsikkerhet, bør være tuftet på vurderingene fra PST og NSM. I denne delen vil jeg derfor ta utgangspunkt i sikkerhetsmyndighetens og virksomhetenes oppfatning av sikringsrisikoen for å drøfte utviklingen.
I den følgende vil utviklingen av risikooppfatningen knyttet til personellsikkerhet bli drøftet opp imot valgte teorier.

Myndighetene

I den gamle lovens forskrift om personellsikkerhet var personellsikkerhet definert som tiltak, handlinger og vurderinger for å hindre at personer som vil kunne utgjøre en sikkerhetsrisiko, plasseres eller er plassert slik at risikoen aktualiseres (Forsvarsdepartementet, 2001, § 1-2). Ut ifra forarbeidene kan man se at risikoen i personellsikkerhetsbegrepet var knyttet til risikoen for at skadevirkninger kan oppstå som følge av sikkerhets- og taushetsbrudd, og at personer man ikke kunne stole på fikk tilgang til verdiene som skulle beskyttes. Verdier som på den tiden i all hovedsak handlet om sikkerhetsgradert informasjon.

I dagens lov og dens forskrifter er ikke personellsikkerhet definert, og dermed har heller ikke definisjonen lenger den samme regulatoriske forankringen som den hadde. NSM har allikevel gitt begrepet en definisjon, som sier at personellsikkerhet er tiltak, handlinger og vurderinger for at personer som kan utgjøre en sikkerhetsrisiko ikke plasseres i stillinger som kan bryte sikkerhetsloven [36]. Rent ordlydsmessig, når NSM knytter risikoen så tett til brudd på sikkerhetsloven, kan man på den ene siden hevde at risikooppfatningen knyttet personellsikkerhet hos den nasjonale sikkerhetsmyndigheten har utviklet seg til at det er det regulatoriske som er verdien som skal beskyttes.

På den andre siden vektlegger forarbeidene til den nye sikkerhetsloven, på samme måte som forarbeidene til den gamle, at det er betydelig risikopotensiale knyttet til personellsikkerhet (Traavikutvalget, 2016, s. 21). Når også veiledninger og informasjon gitt av NSM knyttet til personellsikkerhet uttrykker at risikoen knyttet til personellsikkerhet er sterkt knyttet til trusselen fra fremmed etterretning, så tilsier dette at det blir en for snever fortolkning av NSM sin nye definisjon at det er risikoen for regulatoriske brudd som er avgjørende for tilnærmingen til personellsikkerhet. Dette underbygges av at forarbeidene til loven og NSM sine veiledninger og informasjon, er bygger på trusselen fra fremmed etterregning slik den beskrives i PST sine trusselvurderinger. Noe som igjen gjør det vanskelig å underbygge at ordlyden skyldes at NSM har endret oppfatning av risikooppfatningen knyttet til personellsikkerhet, og nå har en oppfatning som avviker fra lovgivers oppfatning og PST sine vurderinger av trusselen knyttet til fagfeltet.

Virksomhetene

Hvordan begrepet personellsikkerhet defineres av myndighetene er allikevel vesentlig for hvilken oppfatning som knytter seg til risikoen innenfor fagfeltet på virksomhetsnivå, og hvordan denne utvikler seg. Dette fordi det påvirker sikkerhetskulturen hos virksomhetene. En kultur som etter forarbeidene til sikkerhetsloven og NSM sine vurderinger, men også i HRO-teorien er viktig for sikkerhetsarbeidet i en organisasjon (Reason, 2016, s. 191). Virksomheter med høy grad av sikkerhetskultur vil etter HRO-teorien være preget av vilje til å lære, og søke informasjon for læring og kompetansebygging. Når PST og NSM over tid har utgitt stadig mer omfangsrike og detaljerte trussel- og risikovurderinger, hvor også trusler og risiko knyttet il personellsikkerhet i økende grad beskrives og detaljeres, så kan det hevdes at forholdene i økende grad har ligget til rette for at utviklingen av virksomhetenes

[36] https://nsm.no/fagomrader/personellsikkerhet/hva-er-personellsikkerhet-1/

risikooppfatning knyttet til personellsikkerhet skal ha utviklet seg i tråd med disse vurderingene. Med en slik forståelse av utviklingen, kan man også hevde at definisjonen av personellsikkerhet ikke er avgjørende. Virksomhetene har gradvis fått tilgang på mer og mer informasjon om trusler og risiko knyttet til personellsikkerhet, og har dermed økte muligheter til å utvikle en kunnskapsbasert risikooppfatning knyttet til personellsikkerhet, som ikke avhenger av en godt fundert definisjon. Utviklingen av risikooppfatningen knyttet til personellsikkerhet de siste 20-årene kan ut ifra dette hevdes å i økende grad ha blitt kunnskapsbasert.

Samtidig kan man på den ene siden hevde at når det, etter Næringslivets sikkerhetsorganisasjons kriminalitets- og sikkerhets undersøkelse (KRINOS) fra 2019, synes som at trussel- og risikovurderingene leses av et fåtall virksomheter, så gir dette argument for at utviklingen av risikoforståelsen knyttet til personellsikkerhet ikke nødvendigvis er kunnskapsbasert (Næringslivets sikkerhetsråd, 2019). Undersøkelsen er basert på informasjon hentet fra 2000 private og 500 offentlige virksomheter, og viser at i 17% av virksomhetene ble PST sin trusselvurdering lest mens 10 % leste NSMs risikovurdering.
På den andre siden kan man med utgangspunkt i KRINOS hevde at det har vært en utvikling mot mer kunnskapsbasert risikooppfatning knyttet til personellsikkerhet mellom 2015 og 2019 (Næringslivets sikkerhetsråd, 2015). Dette fordi samme type undersøkelse i 2015 viste at kun 4% totalt sett hadde hentet inn trusselvurderingen. Forutsetningene for kunnskapsbasert utvikling av risikooppfatningen knyttet til personellsikkerhet hos virksomhetene kan med utgangspunkt i KRINOS hevdes å ha økt, fordi flere har lest trusselvurderingene.
Samtidig gir utvalgskriteriene i KRINOS grunn til å hevde at undersøkelsen ikke nødvendigvis er valid i forhold til personellsikkerhet innen forebyggende sikkerhet i rammen av sikkerhetsloven. Dette fordi sikkerhetslovens begrensede utvidelse hvor flere private virksomheter kan antas å kunne omfattes av loven, kom med den nye sikkerhetsloven 1. januar 2019, og det derfor er grunn til å anta at de færreste av de 2000 undersøkte private virksomhetene var underlagt sikkerhetsloven på tidspunktet for undersøkelsen. Når det i KRINOS fra 2019 fremkommer at undersøkelsen av offentlige virksomheter baserte seg på et tilfeldighetsutvalg, så påvirker også dette validiteten av undersøkelsen i forhold til personellsikkerhet innen forebyggende sikkerhet i rammen av sikkerhetsloven (Næringslivets sikkerhetsråd, 2019). Noe som følger av at selv offentlige virksomheter, etter både gammel og ny lov, er omfattet av sikkerhetsloven, så er ikke sikkerhetsloven i like stor grad relevant for alle offentlige virksomheter. Eksempelvis vil biblioteker, som er offentlige virksomheter,

kunne hevdes å mindre grad ha behov for PST sin trusselvurdering for å beskytte egen virksomhet eller nasjonale sikkerhetsinteresser. Hvis de da var omfattet av undersøkelsen, så er det en faktor i vurderingen av undersøkelsens validitet, fordi man kan anta at de ville svare at de ikke har innhentet vurderingene. Undersøkelsens kvantitative tilnærming begrenser dermed validiteten.

For å undersøke hvordan risikooppfatningen knyttet til personellsikkerhet har utviklet seg hos virksomhetene de siste 20 årene, fremstår det som mer hensiktsmessig å legge til grunn NSM sine risikovurderinger, som er basert på deres tilsyn med virksomheter underlagt sikkerhetsloven, innrapporterte hendelser, medieovervåkning og PST sine trusselvurderinger. Uti fra disse så kan det argumenteres for at utviklingen av risikooppfatningen knyttet til personellsikkerhet, på tross av økt tilfang av informasjon og kunnskap, hos flere virksomheter ikke har gått i ønsket retning. I flere av NSMs risikovurderinger fremgår det at det er store svakheter i virksomhetenes arbeid med forebyggende sikkerhet generelt, men også personellsikkerhet spesielt (Nasjonal sikkerhetsmyndighet, 2020). Ut ifra dette kan man hevde at selv om det kunnskapsbaserte grunnlaget utviklingen av risikooppfatningen knyttet til personellsikkerhet er til stede, så har ikke kunnskapen blitt operasjonalisert hos flere virksomheter.
På den ene siden er omfanget av manglende operasjonalisering vanskelig å si noe om, siden dataene for en slik undersøkelse ikke er offentlig tilgjengelig. På den andresiden kan det være mulig å årsaksforklare denne manglende operasjonaliseringen, som medfører at NSM hevder at det er store svakheter i virksomhetenes arbeid med forebyggende sikkerhet generelt, men også personellsikkerhet spesielt (Nasjonal sikkerhetsmyndighet, 2020)

Selv om informasjonsgrunnlaget som skal bidra til en kunnskapsbasert risikooppfatning knyttet til personellsikkerhet er til stede, og risikoen blir oppfattet i tråd med kunnskapsgrunnlaget, så kan andre hensyn påvirke operasjonaliseringen. Dette vil bli drøftet i det neste kapitelet om hvordan kan en innsiderhendelse, som er en hendelse som personellsikkerheten i virksomheten skal motvirke, kan forklares fra et organisatorisk perspektiv.

Oppsummering

Det er vanskelig å vurdere om det har vært en utvikling i sikkerhetstjenestenes risikooppfatning knyttet til personellsikkerhet, fordi de bakenforliggende dataene for å undersøke dette er sikkerhetsgradert. Samtidig har det vært en utvikling i hvordan tjenestene beskriver denne risikoen. De er mer presise og detaljerte i sine beskrivelser. Språkmessige endringer i definisjonen av personellsikkerhet kan ved første øyekast gi inntrykk av at NSM oppfatter risikoen knyttet til personellsikkerhet handler om risiko for at noen skal bryte bestemmelsene i sikkerhetsloven. En nærmere undersøkelse av andre dokumenter og veiledninger fra NSM gir ikke hold for en slik påstand.

Hvordan risikooppfatningen knyttet til personellsikkerhet har utviklet seg på virksomhetsnivå er utfordrende å undersøke. Hvorvidt trussel- og risikovurderingene faktisk har blitt lest er av betydning for dette. Valide undersøkelser av dette i forhold til virksomheter underlagt sikkerhetsloven synes ikke å ha vært gjennomført.

Ser man så hen til resultatene av NSM sine tilsyn og undersøkelser av sikkerhetstilstanden, så kan det allikevel synes som flere virksomheter ikke har utviklet den oppfatningen av risikoen knyttet til personellsikkerhet som informasjonen fra tjenestene gir mulighet til. Dette fordi det rapporteres om store svakheter i virksomhetenes arbeid med personellsikkerhet hos flere virksomheter. Noe som kan gi argument for å hevde at risikoen knyttet til personellsikkerhet ikke er oppfattet hos disse.

6.3 Hvordan kan en innsiderhendelse forklares fra et organisatorisk perspektiv?

Med utgangspunkt i James Reasons Swiss Cheese Model kan en innsiderhendelse forklares som en hendelse hvor latente feil i sikkerhetsstyringen og barrierene sammenfaller i tid og rom med menneskelige feilhandlinger (Reason, 2016, s. 10).

Sikkerhetsstyring

Gjennom sikkerhetsstyring skal virksomhetens sikkerhetsmessige barrierer virke sammen for å gi effekt mot innsidetrusselen. Den ene informanten legger frem at man har observert en fragmentering av sikkerhetsarbeidet, hvor for eksempel innsideproblematikken har blitt lagt som et HR (Human Resources) spor, digital sikkerhet hos driftsavdelingen og fysisk sikring har vært et anliggende for sikkerhetsleder (I2). En slik fragmentering kan på den ene siden hevdes å være det motsatte av sikkerhetsstyring. På den andre siden kan man hevde at ansvarsdeling innenfor forbyggende sikkerhet bidrar til integrering av forebyggende sikkerhet

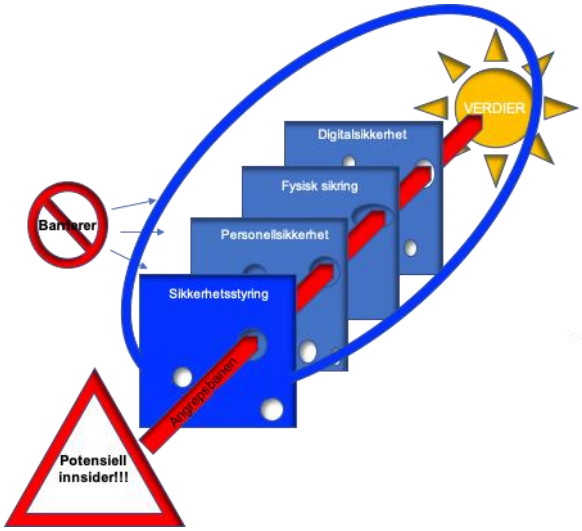
i flere deler av virksomheten, noe som ønskelig både ut ifra sikkerhetsloven og HRO-teorien. Poenget er at hvis ansvarsdelingen medfører at innsideproblematikken håndteres som noe eget utenfor virksomhetens styringssystem for sikkerhet, så er dette fragmentering. Fragmentering av sikkerhetsstyringen kan da hevdes å være et latent forhold i sikkerhetsstyringen, som følger av beslutninger virksomhetenes ledelse har tatt om organiseringen av det forebyggende arbeidet.

Latente feil og menneskelige feilhandlinger

Ifølge James Reason så er det latente feil i alle systemer (Reason, 2016, s. 11). Selv om Reasons teori retter seg mot uintenderte hendelser og ikke intendert sikkerhetstruende virksomhet som er forebyggende sikkerhet sitt domene, så kan man ut ifra Reasons teori også hevde at det vil ære feil i virksomhetenes styringssystem for sikkerhet innenfor sikkerhetslovens rammer. Reason beskriver i sin bok Managing the Risks of Organizational Accidents hvordan, blant annet, huller i tilsyn, uoppdagede produksjonsfeil og manglende trening, som følge av strategiske beslutninger kan medføre slike latente feil (Reason, 2016, s. 10). Slik vil det også være innen forebyggende sikkerhet. Strategiske beslutninger hos virksomhetene om organiseringen av sikkerhetsarbeidet, som medfører fragmentering av sikkerhetsarbeidet, betyr ikke nødvendigvis at det oppstår, for eksempel, en innsidehendelse umiddelbart. Innside hendelsen kan komme mange år senere som følge av at beslutning om organisering av sikkerhetsarbeidet i tid og rom sammenfaller med andre beslutninger og hendelser, som gjør at innside aktiviteten trenger gjennom alle virksomhetens sikkerhetsbarrierer.

Hvis for eksempel en virksomhet har besluttet å gi HR-avdeling ansvaret for å lede personellsikkerhetsarbeidet i virksomheten, og der igjennom håndteringen av risikoen knyttet til insidertruslen, og det som følge av beslutninger om bruk av virksomhetenes ressurser som ikke prioriteres å bygge og opprettholde kompetanse på personellsikkerhet, så kan dette kalles et latent forhold. Kunnskapen om indikatorer på innsidevirksomhet hos personellet i virksomheten, hvis kunnskapen noen gang var der, forvitrer og gjør virksomheten ute avstand til å detektere, vurdere og håndtere en potensiell innsider. Det kan til og med hende at menneskelige feilhandlinger, som følge av manglende kompetanse, gjør at virksomhetene ikke handler adekvat selv om indikatorene oppfattes. Hvis virksomheten i tillegg har besluttet at ressursene knyttet til digital sikkerhet skal rettes mot dataangrep utenfra, og ikke bruker ressurser på autorisasjonsskiller i systemene og dermed gir ukontrollert tilgang til virksomhetens verdier, så kan også dette kalles et latent forhold. Er i tillegg vedlikehold og

oppgradering av sikringstiltakene i barrieren fysisksikring nedprioritert, slik at det er fysisk ukontrollert tilgang til maskinene i virksomhetens IKT-systemer, så kan dette være et eksempel på enda et latent forhold. Hvis da en potensiell innsider i virksomheten bestemmer seg for å utføre en innsidehandling, som man godt kan kalle en bevisst menneskelig feilhandling, så ligger forholdene til rette for dette som følge av de to nevnte latente feilene. Figur 9 nedenfor, illustrerer hvordan en innsidehendelse kan forklares fra et organisatorisk perspektiv.



Figur 9: Mangler i virksomhetenes sikkerhetsstyring og barrierer, som årsaksforklaring på innsidehendelse far et organisatorisk perspektiv. Etter inspirasjon av James Reasons Swiss Cheese modell.

Sikkerhetsstyring og barrierens, latente feil og menneskelige feilhandlinger gjør virksomhetens sikkerhetskultur til en faktor i å forklare en innsidehendelse fra et organisatorisk perspektiv.

Sikkerhetskultur

HRO-teorien som handler hvordan høypålitelige organisasjoner evner å unngå organisatoriske ulykker, legger til grunn at de fire kulturelt betingende komponentene rapporterings-, rettferdighets-, fleksibel-, lærende-og en informert kultur sammen danner sikkerhetskultur (Reason, 2016, ss. 195-196). En sikkerhetskultur som bidrar til at organisatoriske ulykker unngås, og som også etter NSM sine risikovurderinger fremheves som viktig i arbeidet med forebyggende sikkerhet (Nasjonal sikkerhetsmyndighet, 2020, s. 23).

Autorisasjonsprosessen skal tilføre sikkerhetsfaglig kunnskap hos de som autoriseres hos virksomhetene (Nasjonal sikkerhetsmyndighet, 2011). Autorisasjonsprosessen er derfor vesentlig for etablering av det James Reason kaller en lærende-og en informert kultur i boka Managing the Risks of Organizational Accidents (Reason, 2016, ss. 195-196). Samtidig gjør dette at ledere med autorisasjonsansvar blir viktige for etablering av sikkerhetskultur i virksomhetene. Det er de som er ansvarlige for gjennomføringen av prosessen, som slik figur 7 på side 76 viser skal bidra til informasjon og kunnskapsoverføring. Manglende sikkerhetsfaglig kompetanse hos ledere er noe som NSM spesielt fremhever som forbundet med risiko, fordi det gir risiko for at sikkerhetsstyringen ikke fungerer som følge av manglende lederforankring (Nasjonal sikkerhetsmyndighet, 2019, s. 13). Fra et virksomhetsperspektiv kan dermed manglende sikkerhetsfaglig kompetanse hos virksomhetenes ledere, fordi det motvirker informasjon- og kunnskaps utveksling om forebyggende sikkerhet, være et element i å årsaksforklare innsidehendelser.

The Danger of the Unrocked Boat

I HRO-teorien og Normal Accident litteraturen, er også ledelse fremhevet som en vesentlig faktor i håndteringen av risiko (Reason, 2016, s. 122). Sikkerhetsstyringsprosessen skal, etter både sikkerhetsloven, teoriene og beste praksis knyttet til risikostyring være lederforankret. Prosessen krever ressurser, i form av tid, personell og penger. Den må prioriteres av virksomhetens ledelse for å ta effekt.

Det er over 40 år siden den såkalte Treholtsaken, og siden den gang har det vært få innsidesaker som har blitt gjenstand for offentlig oppmerksomhet og debatt. Unntakene er de to innsidesakene i 2020 som er under etterforskning av PST, hvor innsidersaken hos DNV GL er den siste[37]. Det er derfor få nære eksempler på offentlig kjente alvorlige innsiderhendelser knyttet til påvirkning fra fremmed etterretning. Dette kan bidra til at virksomhetene ikke oppfatter innsiderisikoen. Men det kan også bidra til at selv om de oppfatter og forstår risikoen, så er den krevende å fokusere på når frekvensen har vært så lav. Følger man logikken i «The Danger of the Unrocked Boat» vil dette medføre erosjon i personellsikkerhetstiltakene, og være en del av årsaksforklaringen til vellykkede innsideoperasjoner. Dette fordi vedlikehold, oppgradering og tilpassing av sikkerhetstiltakene, blir nedprioritert i forhold til tiltak som gir økt produktivitet, lønnsomhet og inntjening (Reason, 2016, s. 6). Det vil være er vanskelig for en leder å argumentere for prioritering av

[37] https://www.tv2.no/a/11616792/

tiltak rettet mot noe som aldri skjer. Økonomiske mål og krav sammen med produksjon mål og krav, hvor hendelser knyttet til andre fagfelt har høyere frekvens, vil påvirke fokuset og prioriteringene til lederne. Jens Rasmussen påpeker i sin artikkel Risk Management In a Dynamic Society: A Modelling Problem, at fokuset og prioriteringene til lederne påvirkes av omgivelsenes krav (Rasmussen, 1997).

Men det er nødvendigvis ikke bare i høyere frekvens på hendelser innen andre fagfelt som gjør at lederne i fokuserer på personellsikkerhet. Høyere frekvens på hendelser innen andre sikkerhetsfaglige områder kan også bidra til ubalanse mellom barrierene i virksomhetenes styringssystem for sikkerhet. Når direktøren for NSM sier i forordet til risikovurderingen for 2019 at NSM opplever at særlig IKT-sikkerhet står stadig høyere på agendaen blant norske ledere, og det i den samme risikovurderingen fremheves at NSM har sett eksempler på at personellsikkerhet vies for lite oppmerksomhet og at kompetansen på feltet er lav, kan dette gi argument for at det er skjevheter i den innbyrdes prioriteringen av de sikkerhetsmessige barrierene hos virksomhetene (Nasjonal sikkerhetsmyndighet, 2019, ss. 5 og 18). Som igjen kan årsaksforklares med en mye høyere frekvens på antall offentlig kjente alvorlige hendelser knyttet til digital sikkerhet. IT-angrepet på Stortinget høsten 2020 er et eksempel på dette[38]. Når også store deler av samfunnet har utviklet særlig avhengighet til internett og IKT-systemer, hvor et angrep kan få umiddelbare konsekvenser, så er det ut ifra dette lett for virksomhetene å prioritere ressurser og kompetanse rettet mot denne risikoen. Ut ifra et kostnytte perspektiv, frekvens og konsekvens av slike hendelser, fremstår prioritering av digital sikkerhet, fremfor personellsikkerhet som forståelig. Lav frekvens på offentlig kjente innsidehendelser i kombinasjon med en høyere frekvens på offentlig kjente digitale angrep, kan dermed årsaksforklare manglende fokus på personellsikkerhet hos virksomhetene. Dette kan igjen være et element i å forklare innsidehendelser fra et organisatorisk perspektiv.

Oppsummering

Sammen med fragmentering av arbeidet med forebyggende sikkerhet, som bidrar til at latente feil og menneskelige feilhandlinger gir mulighetsrom for en innsidehandling, er manglende sikkerhetsfaglig kompetanse som bidrar til svak sikkerhetskultur, manglende prioritering av forebyggende sikkerhet generelt og personellsikkerhet spesielt faktorer som kan forklarer en innsidehendelse fra et virksomhets perspektiv.

[38] https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2019-2020/it-angrep-mot-stortinget/

7 Konklusjon

I dette kapittelet vil problemstillingen bli besvart:

Hvorfor har sikkerhetsstyring innen forebyggende sikkerhet utviklet seg de siste 20 årene?

Det er flere mulige forklaringer på denne problemstillingen, og det er flere faktorer som har spilt inn på utviklingen. Men det faktum at forebyggende sikkerhet er et område som er regulert ved lov, tilsier overordnet at lovgiver har ønsket den utviklingen som har vært. Det har med andre ord vært politisk ønske og vilje om utvikling.

På et mer detaljert nivå kan utviklingen av sikkerhetsstyring forklares med at:

- Utviklingen av et trusselbilde, som er blitt mer sammensatt og preget av trusselaktørenes kombinasjon av ulike virkemidler, for eksempel insider og nettverksoperasjon, har på myndighetsnivå medført erkjennelse av behov for mer helhetlig styring av forebyggende sikkerhet både på nasjonalt- og virksomhetsnivå
- De økte gjensidige avhengighetene som gjorde det nødvendig å utvide sikkerhetslovens virkeområde, slik at alle virksomheter av avgjørende betydning for våre nasjonale sikkerhetsinteresser kunne omfattes av sikkerhetsloven, har sammen med avdekkede mangler og svakheter i den forebyggende sikkerheten hos virksomhetene gitt et ønske fra myndighetenes side om å tydeliggjøre virksomsomhetenes ansvar for det forebyggende sikkerhetsarbeidet
- Sikkerhetsstyring har blitt et begrep forankret i lov, og dermed gjort sikkerhetsstyring til et lovpålagt krav for virksomhetene som er underlagt sikkerhetsloven

Med bakgrunn i funnene i studien kan hvorfor sikkerhetsstyring innen forebyggende sikkerhet har utviklet seg begrunnes med at man på myndighetsnivå, basert på EOS-tjenestenes vurdering har sett en negativ utvikling i sammenhengen mellom trusselbildet utvikling, og virksomhetens håndtering av truslene gjennom sitt arbeid med forebyggende sikkerhet. Selv om dette er en noe forenklet fremstilling, siden det også gjøres mye godt sikkerhetsarbeid ute hos mange av virksomhetene, så vil det nok fra myndighetenes side ha vært et behov for å tydeliggjøre at forebyggende sikkerhet ikke bare er et myndighetsansvar, men et ansvar vi alle også virksomhetene deler. Det handler om ivaretagelsen av sikkerhetsinteressene til den nasjonen vi alle er en del av.

7.1 FORSLAG TIL VIDERE FORSKNING

Med bakgrunn i at trusselvurderingene til ETJ og PST, sammen med risikovurderingene til NSM utgjør et vesentlig grunnlag for den trussel- og risikopersepsjonen knyttet til nasjonal sikkerhet, som til enhver tid råder i samfunnet, ville en komparativ studie av disse tjenestenes vurderinger kunne være interessant. Hva er sammenhengen mellom dem, og er det en mulighet at sammenhengen dem imellom medfører sirkelrapportering, som er et kjent fenomen innen etterretningsfaget og utgjør en svakhet fordi den kan medføre at beslutninger fattes på feil grunnlag.

8 Litteraturliste

Abcnyheter. (2018, April 11). *PST-sjefen frykter spionasje mer enn terror.* Hentet fra Abcnyheter.no: https://www.abcnyheter.no/nyheter/norge/2018/04/10/195386264/pst-sjefen-frykter-spionasje-mer-enn-terror

Aftenposten. (2014, Desember 13). *PST-sjefen: - Grunn til bekymring*. Hentet fra Aftenposten.no: https://www.aftenposten.no/norge/i/0EOaJ/pst-sjefen-grunn-til-bekymring

Aftenposten. (2016, februar 13). *Russland:-En ny kald krig har brutt ut.* Hentet fra Aftenposten.no: https://www.aftenposten.no/verden/i/XqRW/Russland---En-ny-kald-krig-har-brutt-ut

Arbeids- og sosialdepartementet. (2006, Januar 1). *Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven.* Hentet fra Lovdata.no: https://lovdata.no/pro/#document/NL/lov/2005-06-17-62?searchResultContext=1857&rowNumber=1&totalHits=9864

Aven, et. al. (2016). *Samfunnssikkerhet.* Oslo: Universitetsforlaget.

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

Aven, T. (2020). *The Science of Risk Analysis - Foundation and Practice.* Oxon: Routledge.

Centre for Protection of National Infrastructure. (2013). *CPNI INSIDER DATA COLLECTION STUDY - REPORT OF MAIN FINDINGS.* UK: CPNI.

Christopher, A. (2019). *The Secret World - A History of Intelligence.* Milton Keynes: Penguin Random House UK.

Dagens Næringsliv. (2020, August 17). *Spionsiktet mann skal ha møtt russisk agent på restaurant i Oslo*. Hentet fra Dn.no: https://www.dn.no/innenriks/spionsiktet-mann-skal-ha-mott-russisk-agent-pa-restaurant-i-oslo/2-1-859182

Dagens Næringsliv. (2020, August 19). *Spionsiktet nordmann jobbet for Kongsberg Maritime*. Hentet fra Dn.no: https://www.dn.no/teknologi/kongsberg-maritime/harsharn-singh-tatghar/dnv-gl/spionsiktet-nordmann-jobbet-for-kongsberg-maritime/2-1-860651

Det norske veritas (DNV GL). (2019). *Håndtering av innsiderisiko.* Høvik: DNV.

Det norske Veritas og Germanisher Lloyd (DNV GL). (2019). *Håndtering av innsiderisiko.* Høvik: DNV GL.

Engen, e. (2017). *Perspektiver på samfunnssikkerhet.* Cappelen Damm AS.

EOS-utvalget. (2020, Juni 1). *EOS-tjenestene*. Hentet fra EOS-utvalget: https://eos-utvalget.no/hjem/om-eos/eos-tjenestene/

Etterretningstjenesten. (2011). *Fokus 2011.* Oslo: Forsvaret.

Etterretningstjenesten. (2013). *Etterretningsdoktrinen.* Oslo: Forsvaret.

Etterretningstjenesten. (2015). *Fokus 2015.* Oslo: Forsvaret.

Etterretningstjenesten. (2017). *Fokus 2017.* Oslo: Forsvaret.

Etterretningstjenesten. (2020, Februar 10). *Fokus 2020*. Hentet fra Forsvaret.no: https://forsvaret.no/fokus

Forsvaret. (2020, Mai 27). *Etterretningstjenesten*. Hentet fra Forsvaret.no: https://forsvaret.no/organisasjon/etterretningstjenesten

Forsvarets forskningsinstitutt (FFI). (2015). *FFI-rapport 2015/00923 - Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger.* Kjeller: Forsvarets forskningsinstitutt.

Forsvarsdepartementet. (1997). *Ot.prp.nr.49 (1996-1997) Om lov om forebyggende sikkerhetstjeneste (sikkerhetsloven).* Oslo: Forsvarsdepartementet.

Forsvarsdepartementet. (1998). *Lov om forebyggende sikkerhet.* Oslo. Hentet fra Lovdata.
Forsvarsdepartementet. (2001, Juli 1). *Forskrift om informasjonssikkerhet.* Hentet fra Lovdata.no: https://lovdata.no/pro/#document/SFO/forskrift/2001-07-01-744?searchResultContext=1481&rowNumber=1&totalHits=828
Forsvarsdepartementet. (2001, Juli 1). *Forskrift om personellsikkerhet.* Hentet fra Lovdata.no: https://lovdata.no/pro/#document/SFO/forskrift/2001-06-29-722?searchResultContext=2175&rowNumber=1&totalHits=171
Forsvarsdepartementet. (2001, Juni 26). *Forskrift om sikkerhetsadministrasjon.* Hentet fra Lovdata.no: https://lovdata.no/pro/#document/SFO/forskrift/2001-06-29-723?searchResultContext=1202&rowNumber=1&totalHits=48
Forsvarsdepartementet. (2017). *Prop. 153 L (2016 –2017) - Lov om nasjonal sikkerhet (sikkerhetsloven).* Oslo: Departementenes sikkerhets- og serviceorganisasjon.
Forsvarsdepartementet. (2018, Desember 20). *Forskrift om sikkerhetsklarering og annen klarering (klareringsforskriften).* Hentet fra Lovdata.no: https://lovdata.no/dokument/LTI/forskrift/2018-12-20-2054
Forsvarsdepartementet. (2018, Desember 20). *Ikraftsetting av lov 1. juni 2018 nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.* Hentet fra Lovdata.no: https://lovdata.no/dokument/DEL/forskrift/2018-12-20-2052
Forsvarsdepartementet. (2018, juni 1). *Lov om nasjonal sikkerhet.* Hentet fra Lovdata: https://lovdata.no/dokument/NL/lov/2018-06-01-24#KAPITTEL_2
Forsvarsdepartementet. (2019, Januar 1). *Forskrift om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).* Hentet fra Lovdata.no: https://lovdata.no/dokument/SF/forskrift/2018-12-20-2053
Forsvarsdepartementet. (2020). *Prop. 80 L (2019 – 2020) - Lov om Etteretningstjenesten (etterretningstjenesteloven).* Oslo: Forsvarsdepartementet.
Hegna, B. S., & Hidlago, A. (2020, September 4). *Innlegg: På høy tid å sette datasikkerheten høyere på agendaen*. Hentet fra Dagens Næringsliv.no: https://www.dn.no/innlegg/datasikkerhet/cybersikkerhet/cyberangrep/innlegg-pa-hoy-tid-a-sette-datasikkerheten-hoyere-pa-agendaen/2-1-869341
Homoliak et. al, I. (2019). *Insight Into Insiders and IT: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures.* ACM Computing Surveys.
Isbrekken, A. T. (2017, Februar 1). Omleggingen av Forsvaret satt langt inne. Oslo, Oslo, Norge. Hentet fra http://forskning.no/2017/01/dragkamp-om-forsvaret-og-forsvarspolitikken/produsert-og-finansiert-av/norsk-utenrikspolitisk-institutt
Justis- og beredskapsdepartementet. (1995, Oktober 1). *Lov om politiet (politiloven).* Hentet fra Lovdata.no: https://lovdata.no/dokument/NL/lov/1995-08-04-53
Justis- og beredskapsdepartementet. (2017, September 6). *Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen).* Hentet fra Lovdata.no: https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349
Kolstø, P. e. (2016, desember 29). *Russlands samtidshistorie*. Hentet fra Store norske leksikon: http://snl.no/Russlands_samtidshistorie
Lia, B. (2017, Juni 20). *Terrorisme*. Hentet fra Store norske leksikon: https:snl.no/terrorisme
Nasdjonal sikkerhetsmyndighet. (2014). *Sikkerhetstilstanden 2014.* Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet (NSM). (2015, Mars 10). *Veileder i sikkerhetsstyring*. Hentet fra NSM.stat.no: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/veileder-i-sikkerhetsstyring--endelig.pdf

Nasjonal sikkerhetsmyndighet. (2003). *Risikovurdering 2003.* Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2009). *Rapport om sikkerhetstilstanden 2009.* Kolsås: NSM. Hentet fra nsm.no: https://nsm.no/getfile.php/133792-1592988787/Demo/Dokumenter/Rapporter/rst_2003.pdf
Nasjonal sikkerhetsmyndighet. (2010). *Rapport om sikkerhetstilstanden 2010.* Kolsås: Nasjonal sikkerhetsmyndighet. Hentet fra Risikorapporter fra 2019 og tidligere.
Nasjonal sikkerhetsmyndighet. (2012). *Rapport om sikkerhetstilstanden 2011.* Kolsås: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2015). *Veileder i sikkerhetsstyring.* Sandvika: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2019). *Innsiderisiko.* Sandvika: RK grafisk.
Nasjonal sikkerhetsmyndighet. (2019, Mai 7). *Nasjonal sikkerhetsmyndighet overføres til Justis- og beredskapsdepartementet*. Hentet fra nsm.stat.no: https://www.nsm.stat.no/aktuelt/nasjonal-sikkerhetsmyndighet-overfores-til-justis--og-beredskapsdepartementet/
Nasjonal sikkerhetsmyndighet. (2019, Mars 12). *Personellsikkerhet*. Hentet fra Nsm.stat.no: https://nsm.no/fagomrader/personellsikkerhet/hva-er-personellsikkerhet-1/
Nasjonal sikkerhetsmyndighet. (2019). *Risiko 2019.* Oslo: RK grafisk.
Nasjonal sikkerhetsmyndighet. (2019, mars 12). *Slik blir du sikkerhetsklarert*. Hentet fra nsm.no: https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/slik-blir-du-sikkerhetsklarert/
Nasjonal sikkerhetsmyndighet. (2019). *Veileder i sikkerhetsstyring.* Sandvika: Nasjonal sikkerhetsmyndighet.
Nasjonal sikkerhetsmyndighet. (2020, februar 14). *Autorisasjon*. Hentet fra nsm.no: https://nsm.no/fagomrader/personellsikkerhet/sikkerhetsklarering/autorisasjon/
Nasjonal sikkerhetsmyndighet. (2020, Mars 16). *Mer hjemmekontor – store muligheter, men også risikoer*. Hentet fra nsm.stat.no: https://www.nsm.stat.no/aktuelt/mer-hjemmekontor--store-muligheter-men-ogsa-risikoer/
Nasjonal sikkerhetsmyndighet. (2020). *Risiko 2020.* Oslo: RK grafisk.
NATO Coopertive Cyber Defence Centre of Excellence (CCDECOE). (2015). *Insider Threat Study.* Tallinn: CCDECOE.
Norsk rikskringkastning. (2020, September 1). *Mange spionsaker: Etterretningstjenester bruker «name and shame»-metoden*. Hentet fra Nrk.no: https://www.nrk.no/norge/mange-spionsaker_-etterretningstjenester-bruker-_name-and-shame_-metoden-1.15141399
Norsk rikskringkastning. (2020, Januar 21). *NTNU begynte å mistenke de to siktede forskerne allerede for ett år siden*. Hentet fra nrk.no: https://www.nrk.no/trondelag/ntnu-begynte-a-mistenke-de-to-siktede-forskerne-allerede-for-ett-ar-siden-1.14869687
Norsk senter for forskningsdata. (2020, Juli 9). *Politiets sikkerhetstjeneste*. Hentet fra NSD forvaltningsdatabasen: https://nsd.no/polsys/data/forvaltning/enhet/13510/endringshistorie
NSM. (2019, August 26). *Om NSM*. Hentet fra nsm.stat.no: https://www.nsm.stat.no/om-nsm/
NUPI. (2015, september 23). *Trusselbilder og forsvar i endring*. Hentet fra NUPI: www.nupi.no/Nyheter/Trusselbilder-og-forsvar-i-endring
Petroleumstilsynet. (2017). *BARRIERENOTAT 2017.* Stavanger: Petroleumstilsynet.
Politiets sikkerhetstjeneste . (2005, Mars 29). *Trusselvurdering 2005*. Hentet fra Pst.no: https://www.pst.no/alle-artikler/trusselvurderinger/trusselvurdering-2005/
Politiets sikkerhetstjeneste . (2018). *Trusselvurdering 2018.* Oslo: Politiets sikkerhetstjeneste Den sentrale enhet.

Politiets sikkerhetstjeneste. (2004). *Trusselvurdering 2004.* Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2008). *Trusselvurdering 2008* . Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2013). *Åpen trusselvurdering 2013.* Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2014). *Åpen trusselvurdering 2014.* Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2015). *Åpen trusselvurdering 2015.* Den sentrale enhet. Oslo: PST.
Politiets sikkerhetstjeneste. (2016). *Trusselvurdering 2016.* Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2017). *Trusselvurdering 2017.* Oslo: Politiets sikkerhetstjeneste.
Politiets sikkerhetstjeneste. (2018). *Trusselvurdering 2018.* Oslo: Politiets sikkerhetstjeneste .
Politiets sikkerhetstjeneste. (2020, Februar 4). *Nasjonal trusselvurdering 2020*. Hentet fra Pst.no: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/
Politiets sikkerhetstjenste. (2010). *Trusselvurdering 2010.* Oslo: Politiets sikkerhetstjeneste.
Proactima. (u.d.). Riskostyring.
PST. (2017, Oktober 10). *Oppgaver*. Hentet fra Pst.no: https://www.pst.no/temasider/oppgaver/
PST, NSM, Politiet og NSR. (2017). *Sikkerhet ved ansettelsesforhold - før, under og ved avvikling.* Oslo: Kripos.
Reason, J. (2016). *Managing the Risks of Organizational Accidents.* New York: Routledge.
Regjeringen. (2017, juni 16). *Prop. 153 L (2016–2017).* Hentet fra Regjeringen.no: https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/sec1?q=kritisk%20infrastruktur
Regjeringen. (2019, Januar 22). *Endringer i departementsstrukturen.* Hentet fra Regjeringen.no: https://www.regjeringen.no/no/aktuelt/endringer-i-departementsstrukturen/id2626358/
Regjeringen. (2020, September 6). *Høring – NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett*. Hentet fra Regjeringen.no: https://www.regjeringen.no/no/dokumenter/horing-nou-2018-14-ikt-sikkerhet-i-alle-ledd-og-utkast-til-lov-som-gjennomforer-nis-direktivet-i-norsk-rett/id2623252/
Sagan, S. (1993). *The Limits of Safety.* New Jersey: Princeton university Press.
Sikkerhetsutvalget (Traavikutvalget). (2016). *NOU 2016:19 Samhandling for sikkerhet - Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid* . Oslo: Departementenes sikkerhets- og serviceorganisasjon Informasjonsfor valtning.
Statsministerens kontor. (2002, April 5). *Trusselvurdering for Politiets sikkerhetstjeneste for år 2002*. Hentet fra Regjeringen.no: https://www.regjeringen.no/no/dokumenter/trusselvurdering-for-politiets-sikkerhet/id105701/
Stortinget. (1996, Mars 28). *Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»).* Hentet fra Stortinget.no: https://www.stortinget.no/no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/?lvl=0
Stortinget. (2020, Mai 6). *Skriftlig spørsmål fra Jenny Klinge (Sp) til justis- og beredskapsministeren*. Hentet fra Stortinget.no: https://www.stortinget.no/no/Saker-og-publikasjoner/Sporsmal/Skriftlige-sporsmal-og-svar/Skriftlig-sporsmal/?qid=79410
Stortinget. (2020, Juli 23). *Tildelingsbrev, instruksar og årsrapportar*. Hentet fra Stortinget.no: https://www.regjeringen.no/no/dokument/tildelingsbrev-og-arsrapportar/id2357472/

Syvertsen, J. P. (2007, Oktober 30). *Insider Threat.* Hentet fra ntnuopen.ntnu.no: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143847/Syvertsen%20-%20Insider%20Threat.pdf?sequence=1&isAllowed=y

The Defense Personnel and Security Research Center (PERSEREC). (2014). *Adjudicative Desk Reference (Version 4).* Defense Manpower Data Centre.

Tjora, A. (2017). *Kvalitative forskningsmetoder i praksis.* Oslo: Gyldendal Norsk Forlag AS.

Traavikutvalget. (2016). *NOU 2016:19 Samhandling for sikkerhet-Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Oslo: 07 PrintMedia AS.

TV 2. (2020, September 3). *TV 2 Nyheter: Slik vervet russisk etterretning spionsiktet nordmann (50).* Hentet fra TV2.no: https://www.tv2.no/a/11616792/

TV2. (2020, April 21). *«Trusselaktører driver aktiv kartlegging av sårbarheter»*. Hentet fra TV2.no: https://www.tv2.no/a/11392834/

Willochutvalget. (2000). *NOU 2000:24 Et sårbart samfunn - Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Oslo: Statens forvaltningstjeneste - Informasjonsforvaltning.