



Universitetet
i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering:

MSAMAS
Master i samfunnssikkerhet

Vårsemesteret, 2021

Åpen / ~~Konfidensiell~~

Forfatter: Mads Vigeddal Ommundsen

Fagansvarlig: Claudia Morsut

Veileder(e): Claudia Morsut

Tittel på masteroppgaven:

Security i norsk luftfart- En studie av påliteligheten til indikatorene som brukes for å definere sikkerhetsnivået i norsk sivil luftfart.

Engelsk tittel:

Security in Norwegian Aviation- A study of reliability of indicators used to define the level of security in Norwegian civil aviation.

Studiepoeng: 30

Emneord:

Luftfart, security, terrorisme, compliance, HRO, Governance, tilsyn- og kontroll, inspeksjon, regulering, risikostyring, EU, Avinor, Luftfartstilsynet, trefaktormodellen, forsvar-i-dybden, usikkerhet.

Sidetall: 100

+ vedlegg/annet: 118

Stavanger, 15.06.2021

Security i norsk luftfart

En studie av påliteligheten til indikatorene som brukes for å definere sikkerhetsnivået i norsk sivil luftfart.



Universitetet
i Stavanger

Mads Vigeddal Ommundsen

15.06.2021

Masteroppgave i samfunnssikkerhet
Det teknisk-naturvitenskapelige fakultetet

UNIVERSITETET I STAVANGER

Forord

Denne masteroppgaven markerer slutten på to spennende og lærerike år på masterstudiet i samfunnssikkerhet ved Universitetet i Stavanger. Jeg vil benytte anledningen til å takke forelesere og medstudenter som med sitt engasjement har bidratt til min faglige utvikling.

I forbindelse med masteroppgaven, vil jeg først og fremst takke Avinor, som har stilt opp til samtaler og intervjuer, og som bidro til at jeg fikk muligheten til å undersøke et spennende og aktuelt tema. Uten deres vilje til å dele tanker, erfaringer og data, ville ikke studien vært gjennomførbar. Jeg vil også takke mine informanter fra Luftfartstilsynet og Samferdselsdepartementet, som bidro med interessante innspill og refleksjoner rundt studiens tematikk.

Videre vil jeg takke min veileder Claudia Morsut for et godt samarbeid. Din veiledning førte med seg gode diskusjoner, konstruktive tilbakemeldinger og gode råd.

Til slutt vil jeg takke alle dere som har bidratt med korrekturlesing, diskusjoner og innspill, samt nære og kjære for støtte underveis i arbeidet.

Mads Vigedal Ommundsen

Stavanger, 15.06.2021.

Sammendrag

Denne studien undersøker hvordan Avinor definerer sikkerhetsnivået på deres lufthavner. Studien fokuserer på security-arbeid, som viser til sikkerhetsarbeid rettet mot forebygging av tilsiktede handlinger mot luftfarten. Terrorisme står som den største security-risikoen. Avinor definerer sikkerhetsnivået på bakgrunn av hvordan deres lufthavner samsvarer med ulike security-regler i et felleseuropeisk regelverk. I etterkant av 11. september 2001 angrepene mot USA, utviklet EU et detaljert regelverk som alle lufthavner i EU var forpliktet til å følge. Luftfartsmyndigheten i hver EU-stat skal føre tilsyn med at lufthavnene samsvarer med alle kravene i regelverket. Hvert punkt i regelverket kalles for en KPI (Key performance indicator). I Norge utfører Luftfartstilsynet inspeksjoner av Avinors lufthavner, for å sikre at security-arbeidet er i henhold til EU-kravene. I etterkant av inspeksjonene mottar Avinor en tilsynsrapport hvor graden av samsvar med regelverket fremlegges i form av en score (1-5). 1 er alvorlig avvik fra regelverket mens 5 er svært godt samsvar. Det er på bakgrunn av disse tallene at Avinor definerer og evaluerer sikkerhetsnivået på deres lufthavner.

Studien har som formål å undersøke sammenhengen mellom disse KPIene som brukes for å definere sikkerhetsnivået, og hvordan KPIene faktisk påvirker sikkerhetsnivået. Det er en antakelse at KPIene er sikre og pålitelige indikatorer som kan definere sikkerhetsnivået på lufthavnene. En slik sammenheng er imidlertid aldri bevist. Å definere sikkerhetsnivået på bakgrunn av samsvar med et regelverk, forutsetter at regelverket beskriver alle mulige trusler som er rettet mot luftfarten. Historien har vist at terrorister har klart å utvikle nye metoder som har overlistet de gjeldene sikkerhetstiltakene på lufthavnene.

Studiens empiri er innhentet fra intervjuer med security-ansatte i Avinor, Luftfartstilsynet og Samferdselsdepartementet. I tillegg er det blitt foretatt dokumentanalyser av et utvalg tilsynsrapporter, samt en analyse av datamaterialet som Avinor bruker for å definere sikkerhetsnivået.

Resultatene viser at KPIene i regelverket er utarbeidet på bakgrunn av historiske hendelser, grundige risiko og trusselvurderinger, etterretningsarbeid og i samarbeid mellom en rekke eksperter. Det foreligger derfor en delvis sammenheng mellom KPIene og det faktiske sikkerhetsnivået, da KPIene retter seg mot de fleste risikoene som foreligger mot luftfarten. Funn fra empirien viser imidlertid at sammenhengen er ufullstendig og ikke sterk nok til at sikkerhetsnivået utelukkende kan defineres på bakgrunn et slikt grunnlag. Regelverket

beskriver ikke alle mulige metoder som terrorister kan ta i bruk, samtidig som at usikkerhet, tilfeldigheter og metodiske svakheter kan påvirke Luftfartstilsynets inspeksjoner. Det kan føre til at resultatene av inspeksjonene gir feilaktige indikasjoner på det reelle sikkerhetsnivået. Studien trekker derfor frem behovet for å erkjenne av at det foreligger en viss usikkerhet utover de tallene som definerer sikkerhetsnivået. Studien konkluderer med at det er forskjell mellom samsvarsnivå med regelverket og sikkerhetsnivå, og at det kan være feil og misvisende å definere sikkerhetsnivået i luftfarten på et slikt grunnlag. Et fokus på organisasjonsprosesser som gir høy pålitelighet, vil føre til at security-arbeidet i luftfarten i større grad vil inneholde en bevissthet om at regelverket ikke dekker alle trusler. Samtidig vil pålitelighet kunne føre til en bevissthet om at security-arbeid er en kontinuerlig prosess som aldri blir fullført, til tross for at Luftfartstilsynet sine resultater tilsier at det ikke ble avdekket avvik og at sikkerhetsnivået derfor er høyt. En slik bevissthet vil føre til at de ansatte vil være klar over at det reelle sikkerhetsnivået kan være et helt annet. På den måten vil de være mer forberedt, bevisste og tilpasningsdyktige ovenfor uventede situasjoner og hendelser som ikke dekkes av KPIene i regelverket.

Innholdsfortegnelse

1. Innledning.....	1
1.1 Security og safety.....	2
1.2 Tema, problemstilling og forskningsspørsmål.....	2
1.3 Tidligere forskning på området.....	5
1.4 Disposisjon.....	11
2. Security i luftfarten: bakgrunn og kontekst.....	12
2.1 Utvikling av security i luftfarten.....	12
2.1.1 Hendelser som har påvirket utviklingen av security.....	13
2.2 Internasjonale aktører og organisering av security i sivil luftfart.....	15
2.2.1 International Civil Aviation Organization (ICAO).....	15
2.2.2 European Civil Aviation Conference.....	16
2.3 Nasjonale aktører og organisering av security i sivil luftfart.....	17
2.3.1 Nasjonalt luftfartssystem.....	18
2.3.2 Samferdselsdepartementet.....	18
2.3.3 Luftfartstilsynet.....	19
2.3.4 Avinor.....	19
3. Teori.....	20
3.1 Risiko og usikkerhet.....	20
3.1.1 Risiko i et security perspektiv.....	23
3.1.2 Trussel, verdi og sårbarhet.....	25
3.2 Risikostyring og regulering.....	26
3.3 High Reliability Organizations (HRO).....	29
3.3.1 Bakgrunnen for HRO.....	31
3.3.2 Hva er en HRO.....	32
3.3.3 Mindfulness i organisasjoner.....	33
3.3.4 Sikkerhetskultur i HRO.....	35
3.4 Forsvar-i-dybden.....	35
3.4.2 Aktive feil og latente forhold.....	37
4. Metode.....	39
4.1 Problemstilling og forskningsspørsmål.....	39
4.2 Forskningsdesign og strategi.....	40

4.2.1 Retroduktiv forskningsstrategi.....	40
4.3 Triangulering av metoder.....	42
4.3.1 Semistrukturerte intervju.....	43
4.3.2 Utvalg av informanter.....	44
4.3.3 Forberedelse og gjennomføring av intervju.....	45
4.3.4 Dokumentanalyse.....	46
4.3.5 Utvalg av dokumenter.....	46
4.4 Reliabilitet og validitet.....	47
4.5 Ethiske betraktninger.....	48
4.6 Styrker og svakheter med metodevalg.....	49
5. Empiri.....	50
5.1 Avinors risikostyring.....	50
5.1.1 Avgrensning av datamaterialet.....	51
5.1.2 Statistikk for Avinors lufthavner.....	54
5.1.3 Overordnet risikobilde Avinor.....	59
5.2 Dokumentanalyse av Luftfartstilsynets tilsynsrapporter.....	60
5.2.1 Inspeksjonsmetoder.....	62
5.2.2 Menneskelige feil og avvik.....	65
5.3 Funn fra intervjuene.....	67
5.3.1 Karakteristikk for security regime, og konsekvenser for norsk luftfart.....	67
5.3.2 Hvor sikre er KPIene, og i hvilken grad er regimet risikobasert og proaktivt?.....	70
6. Drøfting.....	74
6.1 Hva karakteriserer regimet og aktørene som driver med security-arbeid i luftfarten?..	74
6.2 Hvor sikre er dagens KPIer, og hvilke variabler kan påvirke deres pålitelighet?.....	81
6.2.1 Usikkerhet.....	84
6.2.2 «Black swans».....	87
6.2.3 Økonomi.....	88
6.3 Hvordan kan security-arbeidet bli mer proaktivt og risikobaser?.....	89
7. Konklusjon.....	91
7.1 Videre forskning.....	92
Litteraturliste.....	93
Vedlegg 1: Intervjuguide Luftfartstilsynet.....	99
Vedlegg 2: Intervjuguide informant 2 Avinor.....	101
Vedlegg 3: Intervjuguide Samferdselsdepartementet.....	102
Vedlegg 4: Forordning 300/2008.....	104

Oversikt over figurer og tabeller

Figur 1: Oppbygging av securityregelverk (Luftfartstilsynet, u.å)	17
Figur 2: Usikkerhetskilder knyttet til risikoanalyser (DSB, 2014).....	22
Figur 3: Swiss cheese model (Reason, 1997).....	37
Figur 4: Hypotetisk modell av uavhengige og avhengige variabler (Babbie, 2010).....	42
Figur 5: Samsvarsoversikt i henhold til forordning 300/2008.....	50
Figur 6: Kart over Avinors lufthavner.....	53
Figur 7: Samlet statistikk for Avinor 01.01.2015-01.03.2020.....	54
Figur 8: Fremstilling av avvik.....	56
Figur 9: Statistikk for lufthavnkategori A.....	57
Figur 10: Statistikk for lufthavnkategori B.....	58
Figur 11: Statistikk for lufthavnkategori C.....	58
Figur 12: Overordnet risikobilde Avinor.....	59
Figur 13: Forsvarsmekanismer og barrierer i luftfarten.....	82
Tabell 1: Antall passasjerer i kalenderåret 2019 (Avinor, 2021).....	51
Tabell 2: Antall flybevegelser i kalenderåret 2019 (Avinor, 2021).....	51
Tabell 3: Oversiktstabell fra tilsynsrapport.....	62

1. Innledning

«We have some planes» var det første flykontrollørene hørte etter 11. september kaprerne hadde tatt kontrollen over American Airlines 11 med Muhammad Atta som pilot. 20 minutter senere krasjet flyet inn i World Trade Center.

Terrorangrepene i USA den 11. september 2001 hadde omfattende konsekvenser for sikkerhetsspørsmål knyttet til terrorisme rundt om i hele verden. Innen den sivile luftfarten ble angrepene dystre bevis på at sikkerhetssystemet konstruert for å forhindre terrorangrep var mangelfullt. Som en direkte konsekvens av angrepene overtok EU ansvaret for å samle europeisk sivil luftfartsikkerhet under ett og samme regelverk. Ved å sette til side nasjonale regler og forskrifter i EU-landene, innebar dette nye regelverket, forordning 2320/2002, at alle flyplassene innenfor EU var forpliktet til å følge det samme regelverket. Hensikten var at alle lufthavnene skulle ha det samme nivået av sikkerhet.

I Norge som i resten av Europa og verden, er terrortrusselen reell, også i luftfarten. «Vi har tatt inn over oss at samfunnet har økt terrortrussel, og at luftfarten er et attraktivt mål for terrorister», sier Dag Hansen, fagsjef Security i Luftfartstilsynet (Luftfartstilsynet, 2017). «Det oppdages stadig nye planer for anslag mot luftfarten. Luftfartstilsynet er i tett dialog med andre relevante myndigheter, som politi, etterretning og departementer. Det foregår også et utstrakt samarbeid på internasjonalt nivå. Terrorister blir smartere, og vi må henge med. Vi har både synlige og usynlige metoder for å hindre terror i norsk luftfart», sier Dag Hansen (Luftfartstilsynet, 2017).

Som et ikke-EU-medlem var Norge allikevel forpliktet av EØS-avtalen til å implementere de samme forskriftene som EU-landene for å unngå å bli utestengt fra det såkalte «One-Stop Security-regimet». Regimet innebærer at enhver passasjer som er sikkerhetskontrollert på en lufthavn innenfor systemet, skal unngå å måtte bli kontrollert i en ny sikkerhetskontroll innenfor det samme systemet. Av den grunn krever EU at alle lufthavner innenfor systemet, uavhengig av lokasjon og størrelse på flyplassen, skal iverksette tiltak som sikrer at EUs reguleringsnivå holdes på samme forhåndsdefinerte nivå. I lys av reguleringsregimet skal en liten flyplass i Nord-Norge ha det samme sikkerhetsnivået som Charles de Gaulle i Paris eller Schiphol i Amsterdam.

For å sikre at alle lufthavner underlagt regimet har samme nivå av sikkerhet, ble det utviklet en forskriftsmessig regulering, basert på hoveddokumenter fra FNs sivile luftfartsorganisasjon, International Civil Aviation Organization (ICAO), som tidligere hadde blitt brukt som veiledende dokumenter for nasjonale luftfartsregler og lovgivning. Disse dokumentene hadde tidligere gitt anbefalinger som hvert land kun var forpliktet til å rapportere avvik fra, men etter 11. september 2001 ble disse obligatoriske i den nye EU-forskriften.

1.1 Security og safety

Sikkerhetsbegrepet er todelt i det engelske språket. Vi snakker «security» og «safety». Denne studien vil fokusere på security arbeidet i luftfarten- sikkerhetsarbeid rettet mot forebygging av tilsiktede handlinger i luftfarten. Security defineres som *«sikkerhet mot uønskede hendelser som er resultat av overlegg og planlegging»*, mens safety blir definert som *«sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfældigheter»* (NOU 2006: 6, s. 38). Forskjellen beror altså på om skaden er påført med motiv (security) eller uten motiv (safety). Risiko i en security kontekst omhandler en rekke farer og trusler som oppstår som følge av ulike kriminelle aktiviteter, og strekker seg fra ordinær kriminalitet i form av hacking, sabotasje, tyveri, spionasje, hærverk til terrorisme. Innenfor luftfarten handler safety om å forhindre ulykker, mens security skal forhindre ulovlige handlinger og anslag mot luftfarten (Luftfartstilsynet, 2017). Begrepet security vil anvendes i denne studien, for å skille mellom sikkerhetsbegrepene.

1.2 Tema, problemstilling og forskningsspørsmål

EU regelverket for sivil luftfart kan karakteriseres som svært forskriftsmessig og detaljert. Regelverket innebærer blant annet kontroll og screening av passasjerer og bagasje, teknisk standard på utstyr, områdekontroll på flyplassene, kontroll av varer og tjenester, kontroll av ansatte etc. Gjennom å implementere en detaljert regulering for den sivile europeiske luftfarten, måtte styrkene ved de nasjonale organisasjonsprinsippene vike plass (Olsvik, 2015, s. 8). I systemer som krever høy pålitelighet, som luftfarten er et eksempel på, er detaljnivået vanligvis høyt. Her er praksis og prosedyrer forhåndsdefinert og grundig beskrevet i et regelverk for å unngå avvik, tvetydighet, slakk etc. Det foreligger en antakelse om at samsvar med regelverket, vil være det samme som pålitelighet. Kritikken mot et slikt detaljfokusert regime handler på den andre siden om at en slik risikostyring kan oppfattes som reaktiv og lite i tråd med et

trusselbilde i kontinuerlig endring. Reglene blir oppdatert i etterkant av avvik, terrorforsøk eller reelle terrorangrep, noe luftfartshistorien har vist. Kritikerne av et slikt regime tar til orde for at risikostyringen i en industri hvor terrortrusselen er reell, i større grad må være proaktiv og fleksibel slik at sikkerhetssystemet vil være i forkant av eventuelle terrorister, og ikke omvendt (Jore, 2015; Hopkins, 2011).

Luftfartsmyndigheten i hver europeisk stat, er ansvarlig for å føre tilsyn med at alle aktørene innen sivil luftfart overholder kravene i det gjeldende security regelverket. Dette utføres gjennom inspeksjoner, revisjoner og tester. Regelverket er gjeldende for alle flyplasser med kommersiell luftfart, alle operatører som bruker flyplassene, selskaper som leverer tjenester eller forsyninger til flyplasser og alle personer som arbeider på eller i forbindelse med en flyplass (Luftfartstilsynet, u.å). Basert på regelverket fra EU og Luftfartsloven, har norske myndigheter implementert en egen forskrift for security i luftfarten- BSL SEC 1-1. Gjennom denne forskriften kan Norge gjøre security reglene strengere, dersom det er behov. Hver flyplassoperatør og hvert flyselskap kan også innføre strengere security regler for sitt eget selskap. Hovedregelen er likevel at alle kravene i EU-regelverket skal være oppfylt til enhver tid (Luftfartstilsynet, u.å).

I Norge eier og driver Avinor 43 av landets lufthavner, og er ansvarlig for å sikre at security arbeidet på lufthavnene samsvarer med EU-kravene (Avinor, 2020, s. 3). Luftfartstilsynet foretar jevnlig inspeksjoner, revisjoner og tester av Avinors lufthavner, for å sikre at kravene i EU-regelverket er oppfylt. Avinor definerer og evaluerer deres interne sikkerhetsnivå primært på bakgrunn av de inspeksjonene som blir foretatt av Luftfartstilsynet. Luftfartstilsynet forholder seg til punktene i EU-regelverket, og kontrollerer graden av samsvar med punktene på Avinors lufthavner. Det gjeldende regelverket for security i luftfarten er forordning 300/2008, og forordningen inneholder 73 punkter med detaljerte krav til security-arbeidet.

I etterkant av inspeksjonene mottar lufthavnsjefen på den inspiserte lufthavnen, og security avdelingen i Avinor, en tilsynsrapport fra Luftfartstilsynet. I rapporten informerer Luftfartstilsynet om hvilke punkter som ble kontrollert, graden av samsvar med kravene og eventuelle beskrivelser og pålegg om tiltak dersom det avdekkes avvik fra regelverket. Graden av samsvar blir fremstilt i form av en karakter fra 1 til 5, hvor 1 er alvorlig avvik og 5 er bedre enn samsvar med krav. Lufthavnoperatøren får en frist på når avviket må være utbedret og lukket, og må sende dokumentasjon til Luftfartstilsynet om iverksatte tiltak og ønsket virkning

av tiltakene. Dersom avvik ikke korrigeres og utbedres, kan det føre til sanksjoner. I ytterste konsekvens kan lufthavnen bli stengt for en periode.

Avinor har et internt system hvor de mottar alle resultatene fra Luftfartstilsynets inspeksjoner. Avvik overvåkes og behandles sentralt, og svares ut lokalt på de flyplassene hvor eventuelle avvik avdekkes. Avinor anvender resultatene for å definere sikkerhetsnivået på lufthavnene, og for å overvåke og studere trender, utviklinger og variasjoner. Avinor definerer derfor sitt interne sikkerhetsnivå på bakgrunn av samsvar (compliance) med EU-regelverket. Det er direkte styring opp imot et detaljert regelverk.

Hver av de 73 ulike punktene i EU-regelverket kalles for KPI (Key performance indicators). Ifølge min informant fra Avinor er det aldri bevist at det foreligger en sammenheng mellom de KPIene som i dag benyttes for å definere sikkerhetsnivået, og hvordan disse KPIene faktisk påvirker sikkerhetsnivået. Det er en antakelse at KPIene er sikre og pålitelige kilder som kan definere sikkerhetsnivået på lufthavnene. Ifølge Avinor foreligger det en grunnleggende antakelse i bransjen om at sikkerheten vil være robust og pålitelig dersom Avinor samsvarer med alle punktene i forordning 300/2008. Denne studien har som formål å undersøke i hvilken grad det finnes en slik sammenheng.

Security regelverket i luftfarten skrives nemlig ofte i etterkant av alvorlige avvik, terrorforsøk eller reelle hendelser. Dette så man i kjølvannet av 9/11 angrepene, som førte til radikale endringer innenfor sikkerheten i luftfarten. For eksempel ble det krav om at cockpit døren i flyet skulle være låst til enhver tid. I Norge ble dette tiltaket for fullt implementert i kjølvannet av Kato-Air hendelsen i 2004, da en asylsøker på en flygning mellom Narvik og Bodø tok seg inn i cockpit, slo pilotene bevisløse med en øks og forsøkte å styrte flyet. Passasjerene og pilotene klarte imidlertid å overmanne gjerningsmannen, og landet flyet trygt på Bodø Lufthavn. I etterkant av 11. august 2006 ble det ikke lov å ha med seg mer enn 100ml væske ombord i fly, etter at tre menn forsøkte å sprengte passasjerfly ved å blande flytende sprengstoff ombord i flyet (Nordstoga, 2009). I 1985 ble Air India Flight 182 sprengt over Atlanterhavet, etter at en bombe gikk av i lasterommet på flyet. 329 mennesker omkom i terroraksjonen. I 1988 skjedde det samme med Pan Am Flight 103, som ble sprengt over byen Lockerbie i Skottland. 270 mennesker omkom. I etterkant av disse angrepene ble nye sikkerhetstiltak innført (Tønnessen, 2008).

Opp gjennom luftfartens historie er det en rekke eksempler på at tiltak er blitt iverksatt som en direkte respons på hendelser. På det grunnlaget kan det derfor stilles spørsmål ved om security-arbeid basert på et detaljert og forhåndsdefinert regelverk er en proaktiv og risikobasert tilnærming som vil kunne forebygge nye terrorangrep i fremtiden. Terrorister har vist at det er mulig å finne hull og svakheter i et etablert sikkerhetssystemet. Terrorisme er en dynamisk risiko, hvor usikkerhet, kompleksitet og tvetydighet er sentrale kjennetegn. Terrorforebygging er derfor krevende, særlig i en globalisert og kompleks industri som luftfarten hvor skadepotensialet er enormt. Vil security-systemet i luftfarten, som i stor grad er konstruert på bakgrunn av statiske regler, være i stand til å forebygge slike dynamiske og uforutsigbare terrortrusler?

På bakgrunn av denne argumentasjonen, har studien som formål å besvare følgende problemstilling:

Er det sammenheng mellom de KPIene som Avinor benytter for å definere deres sikkerhetsnivå, og hvordan disse KPIene faktisk påvirker sikkerhetsnivået?

Videre har jeg utformet tre forskningsspørsmål som skal bidra til å besvare studiens problemstilling:

- 1. Hva karakteriserer dagens security-regimet i luftfarten, og hvilke følger har dette for norsk luftfart?*
- 2. Hvorfor benyttes de 73 KPIene som indikatorer for å avgjøre om sikkerhetsnivået er akseptabelt eller ikke, og hvilke variabler kan påvirke påliteligheten til KPIene slik at sikkerhetsnivået defineres på et feilaktig grunnlag?*
- 3. Hvordan kan security-regimet i luftfarten bli mer risikobasert og proaktivt, for å øke sannsynligheten for at regimet er i forkant av eventuelle terrorister?*

1.3 Tidligere forskning på området

Etter et litteratursøk på tidligere forskning, har jeg ikke funnet frem til forskning som har gått detaljert inn for å studere påliteligheten til KPIene som benyttes for å definere sikkerhetsnivået i luftfarten. Informanten fra Avinor understreker at slik kritisk tenkning er

mangelfull i EU, og formålet med denne studien er derfor å bidra til å belyse tematikken og til en viss grad tette et slikt forskningshull. Imidlertid er det blitt foretatt mer generell forskning som konsentrerer seg om hvordan innføringen av EUs reguleringsregime har påvirket norsk luftfart. Min studie tar utgangspunkt i deler av denne forskningen, da den belyser konsekvensene av innføringen av reguleringsregime i norsk luftfart. Det er i tillegg blitt foretatt europeisk forskning på området. Europeisk forskning er generaliserbart i forhold til denne studien, da europeisk luftfart er underlagt samme regimet som norsk luftfart. Likevel vil denne studien avgrenses til å fokusere på norske forhold.

I det følgende vil jeg presentere funn fra tidligere forskning som er relevant for å belyse studiens problemstilling. Funnene er hentet fra en doktoravhandling skrevet av Olsvik (2015), en artikkel av Engen og Olsvik (2010) og en FFI-rapport fra 2008.

I sin doktoravhandling fra 2015 forsket Olsvik på hvilke konsekvenser det hadde for norsk luftfart å innføre det omfattende EU security- regelverket. EU regelverket var konstruert for store internasjonale flyplasser, og Olsviks funn viste at utfordringene var store da samme regelverk ble innført på små lufthavner i Norge (Olsvik, 2015). Olsvik gjennomførte feltarbeid på tre norske lufthavner av ulik størrelse. Hun så hvordan innføringen av et rigid og detaljert regelverk som langt fra var tilpasset lokale forhold, snudde opp-ned på de ansattes arbeidshverdag. Oppgavene var i større grad forhåndsbestemt og detaljert beskrevet, og de ansattes lokale ekspertise og erfaring ble satt til side. De ansatte skulle håndheve regler og rutiner som var lite tilpasset og til tider virket malplassert. Flere informanter uttrykte at arbeidet til tider opplevdes som meningsløst, og at den eneste måten å «overleve» på, var å slutte å tenke. Olsvik satte spørsmålsteget ved hva dette gjør med sikkerheten i luftfarten. En avgjørende faktor for et pålitelig sikkerhetsarbeid, er våkne operatører som ser meningen med arbeidet sitt (Olsvik, 2015).

Utfordringene med innføringen av regelverket var størst på de minste flyplassene. Gardermoen var den eneste flyplassen som var konstruert, både med tanke på bygninger og antall ansatte, for å implementere regelverket. Jo mindre lufthavnen er, jo flere oppgaver faller på hver enkelt ansatt. Av 46 norske lufthavner er over halvparten av dem regnet som små. Det vil si at det arbeider rundt 20-30 ansatte på hver av de små lufthavnene. Ifølge Olsvik adresseres ikke den type risiko som norsk luftfart er sårbar og utsatt for. Det finnes ingen bevis på om de 1,2 milliard kronene som brukes på security-tiltak i luftfarten

hvert år, brukes riktig (Olsvik, 2015). Det er mangel på studier som belyser tematikken, og få som stiller spørsmål ved effektiviteten og kostandsbruken. I avhandlingen kritiserer Olsvik en utdatert og retrospektiv måte å regulere sikkerhet i luftfarten på. Mens man i andre bransjer jobber mot mindre detaljstyring der tiltakenes effektivitet skal dokumenteres, går man bakover i tid når det gjelder terror. Nye regler blir innført etter hvert som det skjer en hendelse. Olsvik karakteriserer regelverket som gammeldags og rigid. Symbolikken i terror er så sterk at terrørsikkerhet trumfer alt. Samfunnet krever håndtering og godtar tiltak som man ikke nødvendigvis kan dokumentere effekten av (Olsvik, 2015).

Olsvik poengterer at sikkerheten i norsk luftfart er blitt betydelig bedre siden 11. september 2001. Hun ser helt klart fordelene med metalldetektorer, væskeforbud og bagasje som tas av flyet dersom eieren ikke dukker opp. Olsvik stiller likevel spørsmål ved hvorfor Norge valgte å innføre hele EUs modell, uten diskusjoner. Olsvik intervjuet nøkkelpersoner i norsk luftfart fra Samferdselsdepartementet, Luftfartstilsynet, Avinor og fagforeninger for luftfartspersonell. Hun synes ikke begrunnelsene for innføring av regelverket er gode nok. Norske myndigheter argumenterer med at det er fordelaktig å være en del av *one-stop-security*, og at alle passasjerer skal ha rett til den samme sikkerheten når de reiser. Olsvik stiller spørsmål ved det som virker som en enten- eller- holdning: enten ikke noen sikkerhetstiltak eller full EU-pakke (Olsvik, 2015).

I 2010 publiserte Olsvik og Engen en artikkel som tok for seg spesifikke egenskaper ved security- reguleringen av norsk luftfart i etterkant av 9/11. Formålet var å diskutere eventuelle konsekvenser ved en slik risikoregulering, men de dro også frem styrker ved en slik regulatorisk praksis som europeisk luftfart er underlagt. En slik praksis gir blant annet mulighet for god koordinering av security- arbeidet i den europeiske luftfarten, samt at det fører til en lik standard blant lufthavnene og dermed bedre kontroll og oversikt. Hemmeligholdet rundt security reglene vil også være ivaretatt da beslutninger tas sentralt i EU med et lite utvalg av involverte aktører.

Olsvik og Engen (2010) ønsket å undersøke muligheten for å benytte et styringssystem i luftfarten som åpner opp for mer tilpasning og kontekstualisering, gjennom en «Risk Governance» og «High Reliability Organization (HRO) tilnærming, og hvorvidt en slik tilnærming vil sørge for at sikkerheten i luftfarten blir ivaretatt. Kjennetegn ved «good goverance» er ifølge Renn (2008) at risikostyringen blant annet baserer seg på åpenhet, lokalt

engasjement og kulturell tilpasning. HRO kjennetegnes ved at organisasjonene har gjennomslitlige styringsstrukturer og kollegiale, desentraliserte myndighetsmønstre, og at kompetansen dermed flyttes ned til de lavere nivåene og den «skarpe enden» av organisasjonen. Olsvik og Engen (2010) sine funn indikerte derimot at reguleringsregimet i luftfarten i liten grad samsvarer med slike kjennetegn fra teoriene om «good governance» og HRO.

Reguleringsregimet i luftfarten er i stor grad preget av hemmeligholdte og effektive beslutninger som ikke gir tid og rom for relevante interessenter i å bidra i styringsarbeidet. Engen og Olsvik (2010) karakteriserer også regimet for å være reaktivt da det i stor grad er hendelsesbasert. Kravet om at security-regelverket i stor grad skal være hemmelig, er dermed ikke forenlig med prinsippene om at regimet må inneholde gjennomslitlige styringsstrukturer og desentraliserte myndighetsmønstre.

Forsvarets forskningsinstitutt (FFI) publiserte i 2008 en rapport som tok for seg luftfartsindustrien som terrormål, med fokus på trender og utviklingstrekk etter 2001. Rapporten bidrar til å belyse hvorfor luftfarten er et attraktivt terrormål, og hvordan tidligere metoder er blitt brukt for å ramme industrien. Rapporten ble skrevet på oppdrag fra Luftfartstilsynet. For å kunne danne seg et bilde over terrortrusselen luftfarten står overfor, er det nødvendig å svare på de grunnleggende spørsmålene: Hvem har kapasitet og intensjon om å angripe luftfarten, hva slags mål vil de ramme og hvilke metoder kan de ta i bruk for å klare dette? En hovedkonklusjon i rapporten er at luftfartens attraktivitet som terrormål i stor grad bestemmes av målets symbolske karakter og potensialet for et spektakulært angrep (Tønnessen, 2008). Dette preger også målutvelgelsen på den måten at et mål med høy symbolsk betydning innenfor luftfarten er et mer attraktivt mål enn et mål med mindre symbolsk betydning. Dette gjelder i stor grad for alle typer terrormål, men luftfarten er preget av bedre sikkerhet enn mange andre typer mål. Attraktivitet må derfor ses i sammenheng med sikkerhetsnivå. I tillegg har også flysektorens høye sikkerhetsnivå ført til en slags evolusjonsprosess mellom terroristene og luftfartssikkerheten hvor nye taktikker blir utviklet som et svar på nye sikkerhetsbarrierer og vice versa (Tønnessen, 2008).

Til tross for at gjennomførte angrep mot luftfart kun utgjør en liten prosentandel av gjennomførte terrorangrep totalt sett, er det imidlertid god grunn til å anta at luftfartssektoren har vært og fortsatt er et attraktivt terrormål (Tønnessen, 2008). 9/11 angrepene viste at det

var mulig å gjennomføre massedrapsangrep ved hjelp av fly, og det har blitt avdekket en rekke angrepsforsøk mot fly planlagt av al-Qaida-inspirerte terrorister i Europa også etter 9/11. Hvilke eller hva slags type mål blir ansett som så attraktive at terroristene investerer ressurser de kunne ha brukt mot andre mål hvor sannsynligheten for suksess er større? En viktig forklaring er den oppmerksomheten et angrep mot luftfarten fører med seg, selv om angrepet blir avverget. Terrorforskeren William Crenshaw har hevdet at angrep mot fly får langt større oppmerksomhet sammenliknet med andre typer angrep, til tross for at angrep mot luftfarten forekommer langt sjeldnere enn mot andre typer mål. Det var nettopp denne oppmerksomheten terrorgrupper fikk som følge av flykapringer som sterkt bidro til at flysektoren ble et relativt populært terrormål på slutten av 1960-tallet og 1970-tallet. Et vellykket angrep kan være verdt en rekke mislykkede forsøk ettersom suksessene huskes bedre en fiaskoene. Dette er trolig en viktig grunn til at terrorister fortsatt prøver å finne hull i sikkerhetsbarrierene på flyplasser, til tross for det høye sikkerhetsnivået og sikkerhetsfokuset (Tønnessen, 2008). De vellykkede angrepene, særlig 9/11, har også økt risikoen for «copycataksjoner». Dette kan illustreres ved at flere av de avvergede forsøkene mot flysektoren de seneste årene er basert på taktikker som al-Qaida nettverket utviklet og eksperimenterte med i løpet av 1990-tallet.

En annen forklaring på hvorfor luftfarten er et attraktivt terrormål, er alle de symbolske målene flyindustrien tilbyr. Mange av de mest kjente flyselskapene blir oppfattet som representanter for deres land, samtidig som flysektoren representerer internasjonal økonomi og globalisering. Det er med andre ord ikke tilfeldig at amerikanske, israelske, britiske og franske flyselskaper har vært offer for flere terroranslag og forsøk på anslag. I tillegg muliggjør angrep mot flysektoren massedrap som ikke rammer helt tilfeldig. Til tross for at terrorgrupper ønsker å forårsake massedrap er det ikke slik at de ønsker å ramme helt tilfeldig. De fleste terrorgrupper skiller mellom legitime og illegitime mål og det er hver enkelt gruppes ideologi som avgjør hvilke mål det er legitimt å ramme (Tønnessen, 2008).

En annen faktor er at det høye sikkerhetsnivået i seg selv kan gjøre flysektoren til et fristende mål. Det vil være en stor seier for terroristene dersom de kun en gang er i stand til å trenge igjennom sikkerhetsbarrierene og faktisk lykkes med å gjennomføre et angrep. Enorme summer og ressurser blir investert i sikkerhetsarbeidet i luftfarten, og store deler av sivilbefolkningen har selv opplevd ubekvemme og tidskrevende sikkerhetstiltak på nært hold hver gang de flyr. Hvis terroristene kan vise at selv ikke luftfarten er godt nok sikret, hva da

med andre deler av samfunnet hvor sikkerheten er betydelig lavere. Dette vil skape en stor frykt i befolkningen, som nettopp er terroristenes mål og hensikt. Det har også blitt hevdet at å ødelegge et fly demonstrerer Vestens sårbarhet samtidig som det fremhever terroristenes kompetanse. Dette ble godt illustrert med 9/11 angrepet hvor 19 terrorister var i stand til å overliste sikkerhetsapparatet i verdens dominerende supermakt. Som følge av stadig nye sikkerhetstiltak innen luftfarten, har terrorgrupper hele tiden måttet utvikle og eksperimentere med nye angrepsmetoder. Det har på mange måter utviklet seg en slags «katt og mus-lek» hvor sikkerhetstiltak og angrepsmetoder utvikler seg som svar på hverandre. En rask gjennomgang av utviklingstrendene i terroranslagene rettet mot luftfart viser hvordan angrepsmønstrene har endret seg i takt med et strengere sikkerhetsregime. Et generelt funn i FFI sin rapport, er at de nye angrepsmetodene mot luftfarten baserer seg på gamle metoder, men at det legges til et nytt element. Terrortaktikker har også en sterk smitteeffekt; terrorister overtar taktikker fra andre grupper når de er klar over taktikkens eksistens. Dette betyr at ulike taktikker er populære, og dermed mer sannsynlige, i en periode. Den store utfordringen blir dermed å være i forkant av terroristene og nøye undersøke de avvergede terrorforsøkene mot luftfarten for å se etter elementer som kan brukes på en ny og annerledes måte (Tønnessen, 2008).

Terrorister har opp gjennom historien tatt i bruk flere ulike metoder for å angripe luftfarten, men i takt med økt sikkerhet og en trend mot mer spektakulær, massedrapsbasert terrorisme har terrorister forsøkt å utvikle nye angrepsmetoder. Ifølge FFI rapporten synes taktikken som går ut på å smugle eksplosiver om bord på fly å være et høyaktuelt scenario. Å kapre fly på samme måte som ved 9/11 virker å være vanskeligere etter at nye sikkerhetstiltak ble innført for å hindre at kaprere får tilgang til cockpiten. En mer langsiktig metode for å unngå sikkerhetstiltakene generelt er infiltrering. Terrorgrupper kan forsøke å rekruttere personer som allerede jobber i luftfarten og som dermed har tilgang til områder på innsiden av sikkerhetssonen. I et lengre perspektiv kan de forsøke å få ansatt sympatisører i flysektoren.

Det har forekommet få terrorangrep rettet mot norsk luftfart, men det har imidlertid vært flere tilfeller av kapringer av norske fly eller fly på vei til Norge. De fleste angrep og kapringer av norske fly er blitt gjennomført av psykisk ustabile personer og/eller personer som har ønsket å flykte til Norge. Angrepene har, muligens med unntak av Kato Air hendelsen, ikke vært motivert av et ønske om å utføre massedrap. I flere av disse tilfellene ble det brukt små fly og flyplasser, da sikkerheten tidligere var dårligere der sammenliknet med de større flyene og

lufthavnene. I sin trusselvurdering for 2021 vurderer PST det som *mulig* at ekstreme islamister og høyreekstremister vil forsøke å gjennomføre terrorhandlinger i Norge det kommende året (PST, 2021, s. 17). Kritisk infrastruktur er et mulig terrormål, hvor luftfarten inngår.

Olsvik (2015), Olsvik og Engen (2010) og Forsvarets forskningsinstitutt (2008) sine funn har bidratt til å belyse og kontekstualisere min studie.

1.4 Disposisjon

I kapittel 1 presenteres studiens tematikk, problemstilling og forskningsspørsmål. Kapitlet inneholder også tidligere forskning på området, med den hensikt å kontekstualisere min studie inn i en større sammenheng. I kapittel 2 presenteres bakgrunn og kontekst for studien, hvor utviklingen på security feltet i luftfarten, sentrale aktører og regelverk blir presentert. Deretter presenteres studiens teoretiske rammeverk i kapittel 3. Første del av teorikapitlet består av en beskrivelse av risiko- og usikkerhetsbegrepet, med et særlig fokus på risiko i en security-kontekst. Andre del presenterer kjennetegn ved risikostyring og regulering, hvor kjennetegn ved reguleringsregime som luftfarten er underlagt står sentralt.

Tredje del tar for seg «High Reliability Organization» teori, som anvendes som et verktøy for å forstå kjennetegn og rammebetingelser security ansatte i luftfarten må arbeide innenfor. Til slutt i kapitlet presenteres Reason sine teorier om «forsvar-i-dybden», med den hensikt å beskrive hvordan barrieresystemet i luftfarten er konstruert. Videre vil studiens metodiske fremgangsmåter beskrives i kapittel 4. For å besvare min problemstilling har jeg foretatt intervjuer med fire informanter fra Avinor, Luftfartstilsynet og Samferdselsdepartementet, samt foretatt dokumentanalyser av Luftfartstilsynets tilsynsrapporter og analyse av Avinors datamateriale. I kapittel 5 presenteres empirien fra de forskningsmetodene jeg har tatt i bruk. I kapittel 6 vil funn fra empirien diskuteres i lys av teorien for å besvare forskningsspørsmålene og problemstillingen. Diskusjonen vil lede frem til kapittel 7, hvor jeg vil understreke studiens viktigste funn og fremme forslag til videre forskning.

2. Security i luftfarten: bakgrunn og kontekst

Etter at kommersiell luftfart hadde sin inntreden på 1920-tallet, gikk det ikke lang tid før industrien ble offer for ondsinnede handlinger. Fra den første registrerte flykapringen i Peru i 1931, til «Christmas Day Bomber» i 2009 og til de komplekse angrepene mot USA den 11. september 2001, har luftfarten vært offer for en rekke ulike hendelser av ulik karakter. Utviklingen av sikkerhetstiltak innen luftfarten tilsvarer i stor grad de angrepene som er blitt rettet mot industrien. Som en respons på de ulike angrepene og truslene har internasjonale organisasjoner og et omfattende regelverk blitt utviklet, for å sikre fortsettelsen av sivil luftfart.

Hovedmålet med dette kapittelet er todelt: for det første å skildre forholdet mellom forsettlig angrep mot sivil luftfart og utviklingen av organisasjoner, regelverk, dokumenter og forskrifter. Hensikten er å fremstille hvordan reguleringsystemet knyttet til security i luftfarten er hendelsesbasert, samt å plassere regulering innenfor en internasjonal og europeisk ramme. For det andre vil jeg skildre luftfarts-security innenfor en norsk ramme, ved å beskrive hovedaktørene og regelverket som de norske aktørene må forholde seg til. Kapittelet vil derfor bidra til å gi en forståelse over hvordan dagens reguleringsregime for sivil luftfart er konstruert.

2.1 Utviklingen av security i luftfarten

Angrepene mot USA den 11. september 2001 skiller seg ut som det hittil største og mest vidtrekkende angrepet i sivil luftfarts historie. Angrepene førte med seg omfattende endringer i organiseringen av sikkerheten i luftfarten. Imidlertid startet angrep mot luftfarten lenge før den tid, og det har vært ulike perioder med likhetstrekk innen trender og metoder som er blitt brukt for å ramme industrien. Dette har ført til en kontinuerlig utvikling av lover, regler og forskrifter. Det er tre hovedfaser i trusler som har dannet grunnlaget for den generelle utviklingen av security i luftfarten:

- Fase 1: 1948-1968: Flykapringer
- Fase 2: 1968-1994: Den politiske fasen
- Fase 3: 1994-nåtid: Fly brukt som ødeleggelsesvåpen
(Irish Aviation Authority & Aviasolution, 2004).

Fase 1: Dette var en periode hvor enkeltpersoner kapret fly for å unngå forfølgelse eller tiltaler. Flyet ble brukt som ett effektiv virkemiddel for å flykte fra en stat for å unngå tiltale. Et eksempel var en kapring hvor tre besetningsmedlemmer (inkludert piloten) sammen med 21 av de totalt 26 passasjerene, kapret et fly i 1948 på en innenriksrute mellom Praha og Bratislava. Flyet landet i den amerikanske okkupasjonssonen i München. Kaprerne flyktet fra jernteppet i øst for å søke asyl i Vesten (Irish Aviation Authority & Aviasolution, 2004).

Fase 2: Denne perioden blir kalt den politiske fasen, og blir ansett som begynnelsen på «moderne terrorisme» innen luftfarten. Hensikten til terroristene i denne perioden var å legge press på myndighetene, gjennom ulike former for terrorisme. Et av de mest kjente eksemplene er Pan Am Flight 103, som ble bombet over Lockerbie i Skottland i 1988, på vei fra London til New York. Libya tok senere på seg skylden for angrepet (Gillen & Morrison, 2014).

Fase 3: I denne fasen endret terrorister sitt formål til å bruke fly som masseødeleggelsesvåpen. Denne fasen regnes som den farligste og vanskeligste å forsvare seg mot. På julaften i 1994 ble et Air France fly kapret av algeriske terrorister, hvor deres mål var å styrte flyet i sentrum av Paris. Pilotene klarte å lure terroristene til å tro at flyet måtte mellomlande i Marseille for å fylle drivstoff, og politiet stormet flyet og pågrep terroristene (Irish Aviation Authority & Aviasolution, 2004). Dette var starten på fasen hvor terroristene bevisst skulle bruke flyet som våpen mot sivile mål.

2.1.1 Hendelser som har påvirket utviklingen av security

I det følgende presenteres tre hendelser som på ulike måter har ført til endringer i security-regimet i luftfarten.

11. september 2001

Nærmere 3000 mennesker ble drept i terrorangrepet mot USA den 11. september 2001. Om morgenen 11. september 2001 ble fire passasjerfly kapret av 19 selvmordsaksjonister fra al-Qaida. To av flyene tok av fra Boston, ett fra Newark og ett fra Dulles i Virginia, like utenfor Washington D.C. To av flyene styrtet i hvert sitt tårn i World Trade Center i New York, og begge tårnene kollapset. Mer enn 400 brann- og politifolk som hadde rykket ut til åstedet, var blant de drepte. Det tredje flyet ble styrt ned i USAs forsvarsdepartementsbygning Pentagon, og det fjerde flyet styrtet i Pennsylvania før det nådde sitt mål (antakelig Det hvite hus eller Kongressen). En offentlig undersøkelseskommissjon konkluderte med at kaprerne

styrtet det fjerde flyet for å unngå at angripende passasjerer tok over kontrollen (Notaker, 2019). Hendelsen denne dagen demonstrerte en endring i terrorangrepets art, hvor intensjonen var å påføre maksimal skade. Angrepene hadde store konsekvenser på flere nivåer. Et av hovedfunnene fra 11. september kommisjonen var:

“The most important failure was one of imagination, underscoring the commission’s belief that the leaders of the U.S had not understood the gravity of the terrorist threat prior to 9/11 (National Commission on Terrorist Attacks Upon the United States, 2004, s. 9).

Videre uttalte kommisjonen at:

“The 9/11 attacks were a shock, but they should not have come as a surprise, since Islamic extremists had given several warnings that they aimed to indiscriminately harm Americans in large numbers” (National Commission on Terrorist Attacks Upon the United States, 2004).

Kommisjonen kritiserte det svake sikkerhetssystemet i luftfarten, og kom med flere anbefalinger for å styrke sikkerheten. Slike forbedringer kom fort på plass, og ingen andre hendelser har noen gang hatt så omfattende konsekvenser for organiseringen av sikkerheten.

The Christmas Day Bomber 2009:

Et av de nylige terrorforsøkene mot sivil luftfart er den skalte «Christmas Day bomber», også kjent som «the underwear bomber». Terrorforsøket fant sted på Northwest Airlines Flight 253 mellom Amsterdam og Detroit den 25. desember 2009. En nigeriansk 23 åring hadde fått med seg eksplosiver som var skult i undertøyet hans gjennom sikkerhetskontrollen. Han forsøkte å detonere bomben før flyet landet i Detroit, men klarte ikke å detonere sprengstoffene ordentlig og trakk oppmerksomhet fra passasjerer og mannskap før han kunne gjennomføre handlingen. Han ble overveldet av en passasjer, og det brennende sprengstoffet ble slukket av flyvertinnene. Al-Qaida kunngjorde senere at de sto bak angrepsforsøket. Dersom bomben hadde blitt detonert, ville de 290 personene ombord trolig ha omkommet. Til tross for at denne hendelsen ikke genererte noen direkte endringer i security regelverket, så demonstrerte hendelsen den vedvarende trusselen mot sivil luftfart (Olsvik, 2015, s. 18).

Kato-Air hendelsen 2004:

Den 29. oktober 2004, på ruten mellom Narvik og Bodø, ble et Dornier 228-fly operert av Kato-Air, utsatt for et forsøk på å styrte flyet. En av de sju passasjerene gikk inn i den åpne cockpiten og slo begge pilotene bevisstløse med en øks han hadde tatt med seg inn i flyet. Han tok kontroll over flyet og forsøkte å styrte det. Passasjerer var en flyktning fra Algerie som hadde fått avslag på sin asylsøknad i Norge, og skulle returneres til hjemlandet. To av passasjerene klarte til slutt å overmanne flyktningen, og 30 meter over bakken fikk pilotene tilbake kontrollen over flyet og landet trygt på Bodø lufthavn, mens mannen ble holdt nede av passasjerene i kabinen. Gjerningsmannen ble dømt til 15 års fengsel.

Denne hendelsen hadde omfattende konsekvenser for sikkerheten i norsk luftfart. Det var ingen form for sikkerhetskontroll ved de små lufthavnene i Norge før denne hendelsen, og på mange fly var cockpiten åpen. I etterkant av 9/11 angrepene ble det kun innført sikkerhetskontroll ved de største lufthavnene i Norge, mens etter Kato-Air hendelsen akselererte implementeringen av EU-regelverket for samtlige lufthavner. I løpet av 48 timer ble det implementert sikkerhetskontroll på de norske regionale (små) lufthavnene, som frem til da hadde vært fritatt for full implementering av EU-regelverket. Selv om Kato-Air hendelsen ikke ble definert som et terrorforsøk, var det et forsettlig angrep rettet mot å skade fly og passasjerer (Olsvik, 2015, s. 18-19).

2.2 Internasjonale aktører og organisering av security i sivil luftfart

I det følgende vil jeg presentere sentrale aktører og gjeldene regelverk innenfor security i den sivile luftfarten, både nasjonalt og overnasjonalt. Det er et omfattende samspill mellom flere nivåer av aktører, samt ulike forskrifter og regler som aktørene må forholde seg til i deres arbeid.

2.2.1 International Civil Aviation Organization (ICAO)

I 1944 opprettet et spesialorgan fra FN, kalt Konvensjonen om internasjonal sivil luftfart (også kjent som Chicago-konvensjonen) International Civil Aviation Organization (ICAO). Denne konvensjonen skulle være ansvarlig for regulering av internasjonal sivil luftfart. Den ble opprinnelig implementert i 1947 av 52 stater og har blitt revidert åtte ganger siden den gang. 192 stater har i dag sluttet seg til konvensjonen. Konvensjonen etablerte regler for luftrom, flyregistrering og sikkerhet og består av 18 vedlegg. Vedlegg 17 behandler security-spørsmål og inkluderer krav som den sivile luftfartssektoren må imøtekomme. Vedlegg 17 ble

innstiftet for å: *«prevent and suppress all acts of unlawful interference against civil aviation throughout the world»* (ICAO, 2021).

Konvensjonen var ikke juridisk bindende, men medlemslandene ble enige om å rapportere eventuelle avvik fra reglene. Norge ratifiserte konvensjonen i 1945, og det nasjonale regelverket er justert for å imøtekomme konvensjonens intensjoner. En stor del av dagens EU-regelverk er basert på vedlegg 17 fra ICAO-konvensjonen. Vedlegg 17 i ICAO konvensjonen gir veiledning og prosedyrer for hvordan man kan beskytte sivil luftfart mot ulovlige handlinger (ICAO, 2021).

2.2.2 European Civil Aviation Conference

European Civil Aviation Conference (ECAC) ble grunnlagt i 1955 av ICAO og Europarådet. ECAC har i dag 44 medlemsland, inkludert EUs 27 medlemmer. ECACs hovedoppgave er å fremme et trygt, effektivt og bærekraftig europeisk lufttransportsystem (ECAC, 2021). De viktigste strategiske prioriteringene er safety, security og miljø. ECAC var en viktig aktør i utviklingen av EUs reguleringsystem for security i luftfarten.

EUs forordning 2320/2002 for sivil luftfart ble utarbeidet som en direkte konsekvens av 9/11 angrepene, og var basert på European Civil Aviation Conference, Dokument 30, som igjen bygget på ICAOs vedlegg 17. Den største forskjellen mellom ICAO og EU-regelverket er at mens ICAO-konvensjonen baserte deres regulering på frivillig overholdelse, som antydte at medlemmene var forpliktet til å rapportere avvik fra anbefalte forskrifter, krevde EU at alle medlemsstatene skulle overholde kravene i regelverket. Hovedmålene med forordning 2320/2002 var å:

- Etablere og iverksette egnede fellesskapstiltak for å forhindre handlinger med ulovlig inngrep mot sivil luftfart.
- Gi grunnlag for en felles tolkning av de relaterte bestemmelsene i ICAO-konvensjonen, særlig dens vedlegg 17 (European Parliament & European Council, 2002).

Ved å sette felles standarder som medlemslandene var forpliktet til å følge, i stedet for anbefalinger som ikke var juridisk bindende, ville sikkerheten i Europa bli bedre og mer konsistent. "Nivået og kvaliteten på luftfartssikkerhet i Europa anses allment å ha forbedret

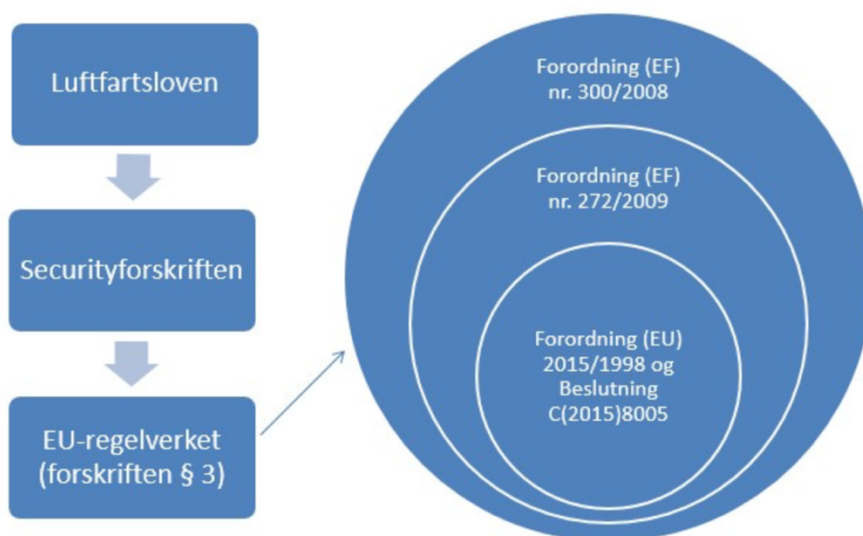
seg betydelig siden innføringen av forordning nr. 2320/2002 sammen med et system for juridisk bindende inspeksjoner" (Irish Aviation Authority & Aviasolution, 2004, s. 29).

I 2008 trådte en ny og oppdatert forordning i kraft, forordning 300/2008, med den hensikt å gjøre forordningen mer risikobasert, mer fleksibel og enklere å forholde seg til. Forordning 300/2008 er den gjeldende forordningen for security-arbeidet i dag. At forordningen skulle bli mer risikobasert, var et klart ønske fra bransjen. Som det fremgår av bransjekilder, er "erstatningen av forordning nr. 2320/2002 med nr. 300/2008 et skritt mot et mer fleksibelt og bedre harmonisert luftfartssikkerhetssystem i Europa" (Poole, 2008, s. 15).

2.3 Nasjonale aktører og organisering av security i sivil luftfart

I det følgende vil det kort redegjøres for de nasjonale security- bestemmelsene, samt en beskrivelse over de viktigste aktørenes ansvarsområder og mandater.

I Norge er security-regelverket i luftfarten i stor grad felleseuropeisk. I tillegg til de felleseuropeiske reglene, foreligger det nasjonale security-bestemmelser som kun gjelder for Norge. Disse er nedfelt i securityforskriften. Securityforskriften er hjemlet i luftfartsloven (Luftfartstilsynet, u.å). Det felleseuropeiske regelverket som er gjeldende for Norge er hjemlet i securityforskriften § 3. Det europeiske regelverket endres i takt med utviklingen på området, og dette kan skje flere ganger i året alt etter behov. Når en endring er tatt inn i securityforskriften § 3 gjelder den overfor norske aktører (Luftfartstilsynet, u.å). Security-regelverket er bygd opp på følgende måte:



Figur 1: Oppbygging av securityregelverk (Luftfartstilsynet, u.å).

Forordning 300/2008 er rammeforordningen som inneholder de grunnleggende standarder for sivil luftfart, mens forordning nr. 272/2009 utfyller rammeforordningen. Forordning 2015/1998 og beslutning C (2015) 8005 inneholder de detaljerte bestemmelsene på security-området (Luftfartstilsynet, u.å). Med andre ord er forordning 300/2008 grunnloven i security arbeidet i luftfarten. Det er primært punktene i denne forordningen som blir inspisert av Luftfartstilsynet på Avinors lufthavner, og denne studien vil derfor fokusere på denne forordningen.

2.3.1 Nasjonalt luftfartssystem

Luftfartsloven, etablert i norsk lov i 1993, administreres av Luftfartstilsynet. Luftfartstilsynet er ansvarlig for å presentere forskrifter, kalt BSL (Bestemmelser for Sivil Luftfart), som regulerer alle deler av norsk sivil luftfart. I denne loven er det fastlagte instruksjoner for hvordan man skal handle i henhold til EØS-avtalen; i første kapittel heter det at:

”For flytrafikk som omfattes av resolusjonen i EØS-avtalen, er regler for utfylling og gjennomføring av EØS-avtalen på luftfartsområdet gyldige fremfor andre lovers forskrifter” (Samferdselsdepartementet, 1993). Dette betyr i praksis at en forskrift som er gyldig for EØS-avtalen går foran de opprinnelige reglene i luftfartsloven.

Frem til år 2000 ledet Luftfartsverket alle områder knyttet til luftfart og flyplassdrift. I 2000 ble det besluttet å dele dette byrået inn i tre nye byråer, der Luftfartstilsynet skulle arbeide som en kontrollfunksjon, Havarikommisjonen ville fungere som et etterforskningsorgan mens Avinor, etablert i 2003, ville fungere som et statlig eid aksjeselskap og eier og operatør av flertallet av flyplassene i Norge. Ved å dele luftfartsmyndigheten skulle hver divisjon bli mer spesialisert på sine egne områder (Samferdselsdepartementet, 2017).

2.3.2 Samferdselsdepartementet

Samferdselsdepartementet er et av 16 departementer underlagt den norske regjeringen. Departementet er et politisk organ som utvikler og fremmer transportpolitikk i Norge. Det overordnede målet for transportpolitikken er å *”tilby et effektivt, tilgjengelig, trygt og miljømessig bærekraftig transportsystem som dekker samfunnets behov for transport i tillegg til regional utvikling”* (Samferdselsdepartementet, 2021). Forbindelsen mellom departementet og Luftfartstilsynet er at Luftfartstilsynet har hovedansvaret for tilsyn og inspeksjon av norsk luftfart. Som beskrevet av den norske regjeringen, skal Luftfartstilsynet være en aktiv

pådriver for en sikker og offentlig nyttig luftfart i henhold til overordnede mål for regjeringens transportpolitikk.

2.3.3 Luftfartstilsynet

I Norge er Luftfartstilsynet ansvarlig luftfartsmyndighet, og fører tilsyn og kontroll med at aktører i norsk luftfart samsvarer med EU-regelverket. Luftfartstilsynet har seks nøkkelområder, security seksjonen blant dem. Hovedmålet for securityseksjonen er å delta i å utvikle reglene nasjonalt og internasjonalt angående security i luftfarten og å utføre inspeksjoner av flyplasser, flyselskaper, lasteselskaper, flyplassleverandør, sikkerhetsvaktoppføringsfirmaer etc. Luftfartstilsynets arbeid er underlagt kontroll og inspeksjon av EUs overvåkningsorgan, EFTA Surveillance Authority (ESA). I praksis betyr dette at ESA utfører inspeksjoner av de forskjellige områdene som Luftfartstilsynet er ansvarlig for, og Luftfartstilsynet vil derfor holdes ansvarlig for alle eventuelle feil, mangler eller feilbehandlinger i disse områdene. Med andre ord inspiserer Luftfartstilsynet flyplassene og flyplassfirmaene og ESA inspiserer Luftfartstilsynet (Olsvik, 2015).

2.3.4 Avinor

Avinor er et heleid statlig aksjeselskap med ca. 3100 ansatte underlagt Samferdselsdepartementet og har ansvar for 43 statlig eide lufthavner og flysikringstjenesten for sivil og militær luftfart i Norge. I tillegg til de ansatte på de forskjellige flyplassene, har Avinor et hovedkontor i Oslo (Bjørsvika). Her planlegges og forberedes alt for flyplassene, samarbeidet med Luftfartstilsynet, Samferdselsdepartementet og internasjonale organisasjoner, komiteer og fora styres derfra. Security er et av selskapets fire divisjoner. Avinor er ansvarlig for å implementere og gjennomføre sikkerhetstiltak på alle flyplasser, noe som i praksis betyr at de er ansvarlige for at alle selskaper på flyplassen opererer i henhold til sikkerhetsforskriftene (Samferdselsdepartementet, 2017). Disse selskapene kan være alt fra selskaper som skaffer drivstoff til flyene til kafeteriaene i det sikkerhetsbegrensede området eller sikkerhetsselskapene som screener passasjerer, bagasje og last.

3. Teori

I dette kapittelet vil jeg presentere relevant teori, som skal anvendes for å belyse oppgavens empiri og besvare oppgavens problemstilling og forskningsspørsmål.

Kapittelet vil starte med en beskrivelse av *risiko- og usikkerhets* begrepet, og hvordan risiko kan forklares i en security sammenheng.

Videre vil jeg presentere sentrale kjennetegn ved *risikostyring og regulering*, med et særlig fokus på det reguleringsregime som norsk og europeisk luftfart er underlagt i dag.

Deretter vil jeg presentere og anvende «*High Reliability Organization*» teori, som et verktøy for å forstå det empiriske materialet og de rammene som Avinor opererer innenfor. HRO teorien vil gi en økt forståelse over organisasjoner som opererer i en risikofylt industri, og gi et rammeverk som kan fortelle noe om komponentene som skal være til stede for å være pålitelige.

Til slutt i kapittelet vil jeg kort presentere *James Reasons* teorier om *forsvar-i-dybden*, hvor hensikten er å illustrere hvordan forsvar- og barriere systemet i luftfarten er konstruert.

3.1 Risiko og usikkerhet

Risikobegrepet blir i dag brukt i flere forskjellige sammenhenger, med ulike og til dels uklare betydninger. Vår forståelse og oppfatning av risiko har implikasjoner for vår praksis når det kommer til å styre sikkerhet og risiko (Aven et al., 2004). Det er vanlig å forstå risiko som en kombinasjon av mulige konsekvenser med tilhørende sannsynligheter. På et mer generelt plan kan risiko oppfattes som et uttrykk for mulige konsekvenser og deres tilhørende usikkerhet (NOU: 2006:6, s. 35). Risiko viser til noe som kan eller kunne ha skjedd, hvordan hendelsene påvirker samfunnet vi lever i, og hvordan bestemte handlinger kan endre forløpet av en hendelse (Engen et al., 2016, s. 79).

Ulrich Beck deler utviklingen av risiko inn i tre faser i boken *risikosamfunnet* (1992): det førmoderne samfunnet, det moderne samfunnet og risikosamfunnet. Modernitet er forbundet med hvordan man organiserer seg med tanke på nye risikoer, altså hvordan samfunnet utvikler sosiale systemer, forvaltning og politikk knyttet til håndtering av risiko. I det moderne samfunnet blir risikoene beregnet ved matematiske og statistiske modeller, hvor risiko blir betegnet som et produkt av sannsynlighet og konsekvens. Samtidig skapes det også en forståelse over at det moderne samfunnet gjennom nye teknologier produserer nye og kvalitativt sett annerledes risikoer. Det er dette Giddens kaller «produserte usikkerheter». De

er bivirkninger av kapitalismens og industrialismens suksess, og det er vanskelig å gjøre noe med dem. Det er denne erkjennelsen både Beck og Giddens omtaler som «modernitetens refleksivitet» (Engen et al., 2016, s. 114). Til tross for at Beck og andre teoretikere er pessimistiske i troen på at moderne risikoer kan styres og kontrolleres, viser nedgangen i antall ulykker, katastrofer og tilsiktede hendelser at risiko til en viss grad kan holdes i sjakk. Økt kunnskap, gode risikostyringsmetoder og analyser bidrar til at risikofylte aktiviteter og industrier kan holdes på et akseptabelt nivå, fremfor at de må forbys helt (Engen et al., 2016).

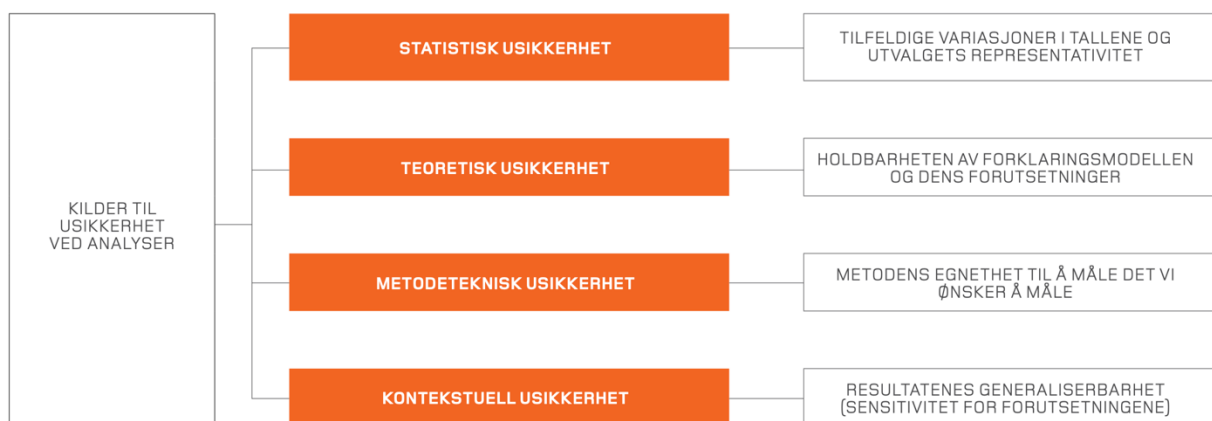
Aven og Renn (2010) knytter risiko opp imot usikkerhet, og forstår risiko som «*usikkerheten om og alvorligheten av hendelser og konsekvenser av en aktivitet med hensyn til det mennesker verdsetter*» (Aven & Renn, 2010). Usikkerheten er knyttet til realisering av hendelser, konsekvenser av en eventuell hendelse og alvorligheten av hendelsen og konsekvensene. Alvorlighetsgraden viser til intensitet, størrelse, utbredelse, omfang satt i sammenheng med forringelse av konkrete ting, sosiale forhold og verdier mennesker verdsetter- det være seg arbeid, status, hus, eiendom, miljø, menneskeliv (Aven & Renn, 2010). Aven og Renns hovedpoeng er at risikobegrepet må basere seg på usikkerheten utover en tallfestet sannsynlighet. Slik tallfesting av risiko kan være effektive verktøy, men det vil alltid være usikkerhet knyttet til de sannsynlighetene man regner seg frem til (Engen et al., 2016, s. 81). Samtidig er det slik at jo mer relevant informasjon man legger inn i beregningene, desto mer informativ blir risikoanalysen for beslutningstakeren. Utfordringen er at det finnes mange usikkerheter og verdivurderinger knyttet til ulike risikoer, og at risikoene har forskjellige karaktertrekk. Mange aktiviteter, hendelser og konsekvenser vet vi mye om og har mye data på. Andre vet vi knapt at eksisterer. Risikoanalyse og risikostyring handler derfor om å beskrive og systematisere hva slags type aktiviteter og risikofenomener vi har med å gjøre (Engen et al., 2016).

Uventede hendelser er ikke noe nytt i risikofaget, men konseptet «*unknown-unknowns*» og «*sorte svaner*» er først blitt tatt i bruk de siste årene. Aven (2014) referer til «sorte svaner» som «*en overraskende, ekstrem hendelse sett i forhold til ens kunnskap/tro*. I Avens definisjon er kunnskap kvalifisert som tro, og er vanligvis basert på data og informasjon. Ifølge Aven kan en «sort svane» hendelse være en overraskelse for noen, men ikke for andre, det er kunnskapsavhengig. «Black swans» hendelser kan i henhold til Aven og Krohn (2013) brytes ned i tre hovedkategorier:

- a.) **Unknown-unknowns** – hendelser som var helt ukjent for det vitenskapelige miljøet.

- b.) **Unknown-known** – farer som er kjent for noen, men ukjente for mange.
- c.) **Known events** – hendelser på listen over kjente hendelser i risikoanalysen, men er vurdert til å ha ubetydelig sannsynlighet for forekomst, og dermed ikke antas å forekomme.

De fleste risikoanalytikere er enige om at sannsynlighetsteoretiske tilnærminger som oftest er for enkle. I rapporten *Nasjonalt risikobilde* (DSB, 2014) legges følgende usikkerhetskilder til grunn når man skal beregne risiko.



Figur 2: Usikkerhetskilder knyttet til risikoanalyser (DSB, 2014)

Usikkerheten kan beskrives gjennom en vurdering av kunnskapsgrunnlaget for analysen og resultatenes sensitivitet for endringer i forutsetningene. Sensitive resultater er lite generaliserbare og følsomme for små endringer i scenarioer eller antakelsene som konklusjonene bygger på. For å vurdere styrken i kunnskapsgrunnlaget er det brukt tre indikatorer som foreslått av Flage & Aven (2009).

- * Tilgangen på relevante data.
- * Forståelsen av hendelsen/fenomenet som analyseres (hvor god er forklaringsmodellen).
- * Enighet blant ekspertene som deltar i risikoanalysen (DSB, 2014, s. 22).

Ulike metoder og kunnskapssyn anvendes for å estimere risiko og avgjøre om risikoen er akseptabel eller ikke. Risikoanalyser gjennomføres på mange fagfelt med ulike framgangsmåter og formål, som innenfor økonomi, matematikk, naturvitenskap, medisin og samfunnsfag. Derfor er det behov for å presisere hva man legger i sentrale begreper når man presenterer en risikoanalyse. På noen fagområder baseres risikoanalysene utelukkende på statistikk og modeller, mens andre fagområder har en bredere og mer prosessuell, kunnskaps

og konsensusbasert tilnærming. Dette fører til forskjeller i datainnsamling (tall, erfaringer, ekspertkunnskap), analyseprosess (hvem og hvor mange som involveres), presentasjon av resultatene (beregninger, verbale beskrivelser) og vurderinger av usikkerhet knyttet til disse (signifikans, validitet, kunnskapsmangel) (DSB, 2014, s. 19).

3.1.1 Risiko i et security perspektiv

Beskyttelse mot terrorisme eller andre forsettlige handlinger betegnes som security, mens safety innebærer beskyttelse mot utilsiktede handlinger. Når en høyrisikoindustri som flybransjen kan feire hundre dager uten ulykker, kan det forklares med gode prosedyrer, god opplæring og årvåkne ansatte. Innenfor security er dette derimot annerledes. Hundre dager uten hendelser kan selvsagt bety at security systemet har lyktes med å ikke la noen med ondsinnede intensjoner skade systemet, men det kan også bety at ingen har forsøkt. Dette illustrerer en av hovedforskjellene mellom safety og security.

Jore (2017) definerer security som: *“the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crises caused by peoples deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking”* (Jore, 2017, s. 169).

Definisjonen til Jore vektlegger hvordan security-relaterte hendelser oppstår som følge av at overtrederen har en ondsinnet hensikt og bevisst sikter på å forårsake skade. På bakgrunn av denne tilnærmingen kan risiko i en security kontekst omhandle en rekke farer og trusler som oppstår som følge av ulike kriminelle aktiviteter, herunder også terrorisme (Jore, 2017).

I denne studien betraktes risiko som forholdet mellom de verdier vi ønsker å verne om, de trusler som potensielt kan ramme disse verdiene, og sårbarhetene som verdiene har i relasjon til truslene (NOU: 2016, s. 19). Sikkerhetstilstanden er påvirket av den innsatsen vi legger i å sikre verdiene våre. Kunnskap om egne verdier og sårbarheter, samt en forståelse for at verdiene kan være attraktive for ulike trusselaktører, er således viktig for menneskers risikoerkjennelse. Formålet med virksomheters security-arbeid er følgelig å verne om sine verdier. I et større perspektiv er formålet å verne om sentrale og sårbare samfunnsverdier, og ivareta rikets selvstendighet og nasjonale sikkerhetsinteresser (NSM, 2017).

Den største security trusselen mot luftfarten er terrorisme, og historien har vist at terrorister både har hatt intensjon og kapasitet nok til å ramme luftfarten.

Selv om det ikke foreligger en allment akseptert definisjon av terrorisme i verden i dag, er det likevel nødvendig å trekke opp noen grenser for hva slags virksomhet som skal regnes som terrorisme. I sikkerhetsloven defineres terrorhandlinger som: «*ulovlig bruk av, eller trussel om bruk av, makt eller vold mot personer og eiendom, i et forsøk på å legge press på landets myndigheter eller befolkning eller samfunnet for øvrig for å oppnå politiske, religiøse eller ideologiske mål*» (Brynjar et al., 2017).

Terrorisme kjennetegnes for å være komplekst, flerkausalt og omgitt av usikkerhet og tvetydighet (Jore, 2019a), og kan videre defineres som:

“... a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity plays a significant role” (Weinberg et al., 2004, s. 786).

Terrorisme omtales som et «*wicked problem*», på grunn av det mangfoldet som er til stede i de forskjellige angrepsscenarioene som kan materialisere seg og den tilhørende usikkerheten i angrepets intensitet, der terroristen med relativt enkle verktøy kan utføre omfattende angrep med kaskadeeffekter og store politiske konsekvenser (Jore, 2019b). Terrortrusler er dynamiske i sin natur, da terrorangrep utføres av strategisk tenkende individer som kan tilpasse og endre sine mål. Det er nesten et uendelig antall mulige angrepsscenarioer, noe som gjør det vanskelig å vurdere effekten av å bruke avbøtende og beskyttende tiltak mot terrorisme. Terrorister kan slå til brått, uten advarsel, og for at et terrorangrep skal være effektivt, må terroristene holde lav profil; følgelig vil en terrortrussel være hemmelig av natur og derfor i stor grad ikke kjent av de som er ansvarlige for å sikre samfunnet eller en organisasjon (Jore, 2019b).

Et terrorangrep vil ofte føre til store konsekvenser. Målet til terroristene er ikke bare å forårsake skade, men også å gi en symbolsk og politisk signaleffekt. Siden gjerningsmennene er strategiske, har de ingen interesse av å avsløre sine planer før et angrep, noe som betyr at det, i motsetning til for mange safety-hendelser, ikke vil være mulig å oppdage tidlige faresignaler (Jore, 2019b). Siden terrorangrep er lavfrekvente hendelser, eksisterer det dessuten begrensede relevante tilgjengelige historiske data, som fører til en stor usikkerhet i risikovurderingene. De diversifiserte truslene som kan stamme fra interne eller eksterne gjerningsmenn, enkeltpersoner til statssponserte grupper, i tillegg til det brede spekteret av mulig forebyggende innsats, gjør security-arbeid krevende. Den uforutsigbare karakteren av

terrorangrep gjør det umulig for sikkerhetsbyråer og regjeringer å garantere for offentlig sikkerhet (Jore, 2019b).

3.1.2 Trussel, verdi og sårbarhet

Ifølge Norsk Standard (NS) 5830:2012 er en tilsiktet uønsket handling en hendelse som forårsakes av en aktør som handler med hensikt. Risikovurderinger knyttet til tilsiktede uønskede handlinger tar utgangspunkt i risiko definert som «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen» (trefaktormodellen) (Engen et al., 2016, s. 89). Risiko knyttet til tilsiktede uønskede handlinger kan endre seg fra år til år, avhengig av de trusselvurderinger som gjøres. Trusselvurderinger gir en indikasjon på muligheten for at en hendelse kan inntreffe. Trusselnivået indikerer derfor en form for sannsynlighet. En trussel kan kategoriseres ut fra stigende sannsynlighet eller trusselnivå. Når vi vurderer trusler, ser vi på risikoen for at noe kan skje i framtiden, men vurdering av trusler innebærer også usikkerhet. Ifølge Aven blir en risikovurdering basert på dimensjonene verdi, trussel og sårbarhet. Usikkerheten beskrives gjennom begrepene kapasitet, intensjon, sannsynlighet og kunnskapsstyrke. Avens hovedpoeng er at man må anvende begreper som i tilstrekkelig grad ivaretar usikkerhetsdimensjonene (Engen, et al, 2016, s. 89).

I vurderingen av trussel er det terroristens eller gjerningsmannens intensjon og kapasitet som vurderes (DSB, 2014, s. 8). Et terroranslag vil for eksempel være bestemt av terroristens intensjoner om å ramme en befolkning for på den måten å skape oppmerksomhet om en eller annen politisk sak. Et terroranslag som gjør stor skade og skaper store medieoppslag, er attraktivt for terroristene. Samtidig vil intensjonene være begrenset av hvilken kapasitet terroristen har til å gjennomføre handlingene. Ulike sikringstiltak (fysiske barrierer, sikkerhetskontroll, overvåkning etc) vil begrense handlingsrommet til eventuelle terrorister og i de aller fleste tilfeller forhindre at handlingene skjer. Terroristenes evner til å vurdere sikringstiltak og lage nye planer basert på ny informasjon er en av grunnene til at sikkerheten på flyplasser er underlagt en stor grad av hemmelighold. Alle vet at det er svært mange gjenstander som er forbudt å ta med seg om bord på flyet, men det er svært få som vet hvorfor. Hemmeligholdelsen av begrunnelsen for hva som er lov, og hva som ikke er lov, er nettopp fordi de som ønsker å ramme luftfarten, ikke skal få nye ideer til hvordan de kan gå fram dersom de ønsker å planlegge et angrep. Å vite begrunnelsen for sikringstiltakene kan

nettopp være den informasjonen terroristene trenger for å revurdere planer, forsere barrierene og dermed gjennomføre et angrep (Engen et al., 2016, s. 156).

Security risikoer reiser helt spesielle krav til risikovurderinger og risikoanalyser. Evnen til å innhente og bearbeide informasjon om terroristenes intensjoner og kapasiteter blir av avgjørende betydning (Engen et al., 2016).

3.2 Risikostyring- og regulering

Luftfart har vist seg å være en risikofylt aktivitet med potensielt katastrofale utfall, og er derfor underlagt et strengt reguleringsregime. Risikoregulering er en metode for risikostyring, en måte for myndigheter å håndtere en risikabel virksomhet i stedet for å forby den helt. Risikostyring dreier seg om balansen mellom å realisere det ønskede og unngå det uønskede (Lindøe et al., 2015). Internasjonal litteratur anvender gjerne begrepet «governance» om offentlig styring og kontroll. På norsk blir begrepet oversatt til samstyring, som kjennetegnes ved at det skjer en horisontal og en vertikal koordinering mellom ulike aktører. Horisontal koordinering kan skje mellom aktører innenfor næringsvirksomhet, som produsenter, leverandører, transportører, konsumenter og sivilsamfunn. Vertikal koordinering kan skje mellom ulike nivåer, som departementer, direktorater, kommuner og lokalsamfunn, virksomheter og interessegrupper (Engen et al., 2016, s. 236).

Renn (2008) hevder at alle konsepter om risiko har ett element til felles: *«forskjellen mellom mulige beslutningsalternativer og den valgte handlingen»*. Hvordan risiko skal håndteres er avhengig av dens karakteristikk. Ifølge Renn og «International Risk Government Council» (IRGC) er det mulig å skille mellom fire ulike risikokarakteristikker som krever ulik tilnærming for effektiv risikostyring:

1. Enkle risikoproblem
2. Risikoproblem preget av kompleksitet
3. Risikoproblem preget av usikkerhet
4. Risikoproblem preget av tvetydighet

Luftfarten består av en rekke organisasjoner som kan stå ovenfor flere ulike risikoproblemer. Risikoproblemene vil kunne variere fra enkle problemer, til mer komplekse, usikre og tvetydige problemer. Ifølge Renn (2008) kan enkle risikoproblemer ofte analyseres gjennom historiske sannsynlighetsdata og løses med bakgrunn i eksisterende retningslinjer eller lovpålagte føringer. Renn påpeker på den andre siden at de komplekse, usikre og tvetydige

risikoene krever eksterne eksperter og en frekvensbasert tilnærming til risikomodelleringen (Renn, 2008, s. 281). Sett i forhold til security-regimet i luftfarten, som i stor grad retter seg mot komplekse, usikre og tvetydige risikoer, vil det ifølge Renn (2008) være behov for et rammeverk for risikostyring som er fleksibelt med tanke på metode og samtidig egnet til å løse ulike typer risikoproblem. Ved medium til høy usikkerhet hevder Renn (2008) at ulike involverte interessenter må reflektere sammen med beslutningstaker for å dra normative konklusjoner vedrørende hva som er akseptabel risiko og hvilke tiltak som må iverksettes. I den virkelige verden vil det alltid være en rekke ukjente variabler som kan påvirke resultatene av en risikoanalyse, og slik usikkerhet er nødvendig å ta i betraktning, særlig i security arbeidet.

Flere forskere har diskutert og beskrevet to ulike regimer for regulering av risiko. Hopkins (2011) omtaler disse regimene som «regeloverholdelses- regime» og «risikostyringsregime». Skillet og balansen mellom disse regimene har blitt diskutert grundig, og de fleste reguleringsregimer bygger i dag på en blanding av regimene. Det har vært en tendens til at security risikoer er blitt styrt gjennom et regeloverholdelses- regime, noe security-regimet i luftfarten er et kjerneeksempel på (Jore, 2015). Historisk sett var regeloverholdelses- regime den dominerende tilnærmingen til å regulere farlige aktiviteter. Statlig regulering av risikofylte industrier i løpet av første del av det 20. århundre ble dominert av en «top-down» kommando og kontrollbasert reguleringsmodell preget av en forskriftsmessig regulering, som involverte detaljerte og tekniske krav. Innen de fleste bransjer, som atom, olje og gass, var risikostyring tradisjonelt basert på dette reguleringsregime der detaljerte krav til design og drift ble spesifisert (Lindøe et al., 2015). Selv om dette regime ofte omtales som et historisk regime, som i dag utfordres av risikostyringsregime, er regime fortsatt til stede i mange sektorer i dag, deriblant innen security i luftfarten.

I regeloverholdelsesregime har myndighetene fastsatt detaljerte krav og forskrifter for å styre retningen til virksomheter, og virksomhetene må samsvare med disse forskriftene for å kunne fortsette sin virksomhet. Regimet vil føre til en enhetlig implementering av sikkerhetstiltak, noe som betyr at hver enkelt virksomhet som er underlagt regimet, vil ha samme sikkerhetsnivå uavhengig av virksomhetenes egne oppfatninger av tilgjengelige ressurser, trusselbilde og tidligere erfaringer (Jore, 2015). Selv om trusselbilde og tidligere erfaring med tilsiktede hendelser er langt større i enkelte virksomheter, vil sikkerhetsnivået likevel være det samme i alle de virksomhetene som er underlagt kravene og forskriftene. Et slikt regimet vil

på mange måter føre til en enklere styringsprosess i en organisasjon, da myndighetene eller overnasjonale offisielle organer har satt reglene for når og hvordan man skal iverksette sikkerhetstiltak (Jore, 2015). Organisasjonene slipper å investere tid og ressurser i evalueringer av om det skal iverksettes sikkerhetstiltak eller ikke. En annen fordel med regimet er at det gjør arbeidet for kontroll og tilsynsmyndigheter lettere og mer presist. Tilsynsmyndigheten kan under inspeksjonene forholde seg til de samme kravene og kontrollpunktene, og undersøke hvorvidt det er samsvar med kravene eller ikke. Tilsynsmyndigheten har i lys av regimet ikke ansvar for å påse hvorvidt sikkerhetstiltakene er effektive og i tråd med trussellandskapet, noe som i stor grad ville vært preget av spekulasjoner og stor usikkerhet (Jore, 2015).

I en slik detaljert risikostyring, vil derimot fastsatte tiltak og løsninger ikke være kontinuerlig tilpasset et samfunn og et trussellandskap som er i stadig utvikling (Baldwin & Cave, 1999). Reglene vil stå i sentrum, ikke nødvendigvis hvordan man skal oppnå det optimale sikkerhetsnivået. Organisasjonene og tilsynsorganene som opererer innenfor regimet, vil i stor grad være opptatt av om reglene blir fulgt, fremfor hvordan man oppnår det optimale sikkerhetsnivået mot forsettlige handlinger (Jore, 2015). Et annet utfordrende aspekt er at når risikostyring er bygget på slike generelle regler fremfor spesifikke trussel- og sårbarhetsvurderinger for hver enkelt organisasjon, vil mange organisasjoner iverksette sikkerhetstiltak som er på et høyere nivå enn det som er nødvendig. Dette vil føre til unødvendig høye kostnader og ulemper for organisasjon og dets ansatte. En annen utfordring ved å bruke et slikt reguleringsregime i tilknytning til security risikoer, er at siden prosessen med å endre regulering tar tid, legger ikke dette sikkerhetsregime til rette for raske og effektive endringer i regelverket dersom trussellandskapet endres. Regimet kan derfor i noen situasjoner være reaktivt, og nye regler blir lagt til fordi avvik, forsøk på eller reelle terroranslag avdekker sårbarheter i dagens sikkerhetssystem (Jore, 2015).

På 1970-tallet dukket det opp et nytt reguleringsregime, og fokuset endret seg fra detaljert myndighetskontroll til et internkontrollregime (Lindøe, 2012). Innen de fleste bransjer ble regeloverholdelses-regimet erstattet med mer målrettede regimer. Målorientering og risikokarakterisering var to hovedkomponenter i dette nye regimet. Risikostyringsregime bygger på antagelsen om at organisasjoner har den nødvendige kompetansen for å vite hvilken type risiko organisasjonen kan møte i fremtiden, og hva som er passende midler og tiltak for å imøtekomme disse truslene (Jore, 2015). Forutsetningen er følgelig at

organisasjoner har evnen til å beskrive hva som kan skje i fremtiden, å vurdere tilhørende risiko og usikkerhet, og velge mellom relevante alternativer (Aven, 2013). Antagelsen er at risikovurderinger skal fungere som beslutningsstøtte i en beslutningsprosess for å ta ideelle beslutninger om hvordan man finner det optimale sikkerhetsnivået.

I et slikt regime er statens rolle ikke å tvinge selskaper til å følge detaljerte regler og forskrifter, men å tilrettelegge for og bistå selskapene med å finne det optimale sikkerhetsnivået (Jore, 2015). Dermed endres også rollen til kontroll og tilsynsorganene, som i dette regimet skal kontrollere at organisasjonene har gjennomført risikovurderinger og iverksatt tiltak i samsvar med risikovurderingen. Inspektørens rolle endres derfor fra å være en som pålegger organisasjonene bøter og sanksjoner, til å bli en rådgiver.

I risikostyringsregimet er kunnskapen som en organisasjon har om sine verdier, sårbarheter og tilhørende trusler i fokus. Dette gir organisasjonene en større grad av fleksibilitet i hvordan de skal organisere sikkerheten, og organisasjonen kan rette sikkerhetssystemet mot de truslene som anses for å være mest kritiske for organisasjonen. På den måten kan organisasjonen beskytte de eiendelene og verdiene som er vurdert som de mest verdifulle, og organisasjonen kan endre og tilpasse sikkerhetstiltak dersom trusselbildet endres (Jore, 2015).

Bak det risikostyringsregimet som ble innført i Norge, ligger sikkerhetsloven som krevde at eiere av kritiske gjenstander måtte praktisere risikostyringsregime (Forsvarsdepartementet, 2011). De ulike risikoanalyse standardene som er utviklet og som er under utvikling, kan anses som veiledninger som skal bistå bedrifter med å tolke og håndtere regulering av risiko, da organisasjoner fortsatt trenger regler og retningslinjer som skal veilede dem i sitt sikkerhetsarbeid. Fra et slikt synspunkt er risikostyringsregimet og regeloverholdelsesregimet flettet sammen og utfyllende strategier (Jore, 2015).

3.3 High Reliability Organizations (HRO)

HRO teorien står som det positive og optimistiske teoribidraget som hevder at uønskede hendelser i komplekse teknologiske systemer kan forebygges gjennom pålitelige systemer. Security innen den sivile luftfarten kan i følge Frederickson og LaPorte (2002) defineres som en High Reliability Organization (HRO): *“Commercial air passenger security is part of a unique class of institutional characteristics and decision-theoretic challenges that are*

collectively described as high-reliability organizations” (Frederickson & LaPorte, 2002, s. 34).

HRO er organisasjoner som opererer i et svært uforgivende miljø som i tilfelle feil kan ha katastrofale utfall med potensielt mange dødsfall. Pålitelighet kan defineres på flere måter, avhengig av disiplin og kontekst (Eede, 2009). Eede definerer pålitelighet som: “*Reliability is the system outcome that can be described as safe, effective and efficient, in terms of average and variance*” (Eede, 2009, s. 5). *Average* referer til en forventning om at et system fungerer mesteparten av tiden, mens *variance* refererer til forventede og upålitelige forekomster. For å komplimentere med definisjonen til Eede, definerer Weick og Sutcliffes (2001) pålitelighet som: «*what one can count upon not to fail in doing what is expected*» (Weick & Sutcliffe, 2001, s. 91). Denne definisjonen viser til en nulltoleranse for ulykker og katastrofer blant organisasjoner som opererer innenfor høyrisikoindustrier, fordi skadepotensialet er så høyt.

I organisasjoner med så stor usikkerhet at det kan være vanskelig å evaluere systemets faktiske suksess, gir HRO teorien en måte å evaluere hvorvidt organisasjonsprosessene i organisasjonen samsvarer med prosessene som fører til høy pålitelighet. Derfor vil teori som indikerer hvordan organisatorisk pålitelighet forbedres, være svært anvendelig i tilfeller som ellers er vanskelig å evaluere.

I etterkant av noen av historiens største organisatoriske katastrofer, som Three Mile Island i 1979 og Tsjernobyl i 1986, oppsto det en teoretisk utvikling i tilnærmingen til sikkerhet (safety) og pålitelighet i høyteknologiske systemer. Denne utviklingen var et resultat av erkjennelsen om at organisasjoner spilte en kritisk rolle i forståelsen og styringen av risikoer i moderne samfunn (Hutter, 2010). Dette førte til et fokus på å studere organisasjoner som kunne demonstrere pålitelighet under vanskelige forhold, som ble merket HRO-teori.

Til tross for at security innebærer annerledes typer risikoer enn de som HRO-teori og litteratur normalt har vært opptatt av, vil det likevel ha mindre betydning når formålet er å undersøke hvilke komponenter som gir pålitelige resultater i organisasjoner, uavhengig av om truslene er bevisst forårsaket (security) eller forårsaket ved et uhell (safety). Studier om security kan derfor innlemmes i litteraturen om organisatorisk sikkerhet og pålitelighet.

3.3.1 Bakgrunnen for HRO

I følge Eede (2009) kan utviklingen av HRO- teorien ses på som en tretrinnsprosess. Den første tilnærmingen til HRO ble opprettet av Morone og Woodhouse (1986), som studerte håndtering av giftige kjemikalier, kjernekraft og genteknologi og fant at sikkerhetsregistrene var overraskende gode. Gitt den utfordringen moderne teknologi fører med seg, slo forfatterne fast at historien hittil var overraskende god. Til tross for alvorlige advarsler, hadde ingen katastrofer skjedd i USA (Morone & Woodhouse, 1986). Denne gode sikkerheten var ifølge forfatterne «et systematisk produkt av menneskelig handlinger- resultatet av en bevisst prosess der risikoer overvåkes, vurderes og reduseres» (Morone & Woodhouse, 1986).

Den andre tilnærmingen var strategiene «anticipation» (forventning) og resiliens (mostandsdyktighet) i Wildavsky bok «Searching for Safety» fra 1988. Forventning beskriver en strategi for å forutsi og forhindre skade før den har skjedd. Resiliens er egenskapen et system har til å motstå og tilpasse seg forstyrrelser, og til å gjenopprette funksjonaliteten etter alvorlige påkjenninger. Wildavskys hovedfokus var å undersøke fordelene og ulempene med disse strategiene, og hevdet at all risikostyring ble optimal gjennom en blanding av forventning og resiliens (Wildavsky, 1988).

Den tredje tilnærmingen stammer fra Universitetet i California, den såkalte Berkeley gruppen. Grunnleggerne av gruppen, Roberts, LaPorte og Rochlin, baserte sin forskning på de to tilnærmingene som er beskrevet ovenfor. De utførte empiriske undersøkelser av tre organisasjoner som opererte innenfor høyrisikoindustrier: luftfart (flygeledere), gass og elektrisitet. Berkeley gruppen hevdet at disse organisasjonene var i stand til å utføre nærmest feilfrie operasjoner (Sagan, 1993). Gjennom sin forskning fastholdt de at: *«we have begun to discover the degree and character of effort necessary to overcome the inherent limitations to securing consistent, failure free operations in complex social organizations»* (LaPorte (1991) i Sagan, 1993, s. 15). Disse organisasjonene ble eksempler på hvordan andre organisasjoner innen høyrisikoindustrier skulle operere trygt og pålitelig.

Ifølge Sagan (1993) fokuserte disse tre tilnærmingene på hvordan organisasjoner som opererer innenfor høyrisikoindustrier fungerer, samt et sett med fire egenskaper som anses for å bidra til et høyt sikkerhetsnivå. Disse egenskapene er:

- Ledelsesmål: politiske eliter og organisasjonsledere prioriterer høy sikkerhet og pålitelighet.
- Behovet for redundans: betydelige nivåer av redundans, med overlappende enheter og flere tilgjengelige systemer som utfører samme type oppgave slik at funksjonen ivaretas dersom et eller flere systemer skulle falle bort.
- Desentralisering: der feil og avvik reduseres gjennom desentralisering av autoritet, sterk organisasjonskultur og kontinuerlig drift og opplæring.
- Organisatorisk læring: skjer gjennom en prøve-og-feile-prosess, supplert med forventning og simulering.

Disse fire faktorene utgjør i følge Sagan «en oppskrift eller strategi til ekstremt pålitelig drift selv med svært farlige teknologier» (Sagan, 1993, s. 17). Dette begrunnet han med at slike forhold har vært til stede i en rekke av de effektive HROene som er blitt forsket på. Tanken er derfor at dersom disse forholdene eksisterer i en organisasjon, vil det være mulig å forhindre alvorlige ulykker eller katastrofer. Riktig utformede og godt administrerte organisasjoner kan trygt betjene selv de aller farligste teknologiene (Sagan, 1993).

3.3.2 Hva er en HRO?

The Berkeley Group begynte å bruke begrepet «High Reliability Organizations» for å skille mellom ulike organisasjoner. HROer hadde ikke bare unngått ulykker og katastrofer på grunn av flaks, men de hadde aktivt klart å unngå feil i et miljø rikt på potensiale for feil. Det er flere måter å definere en HRO på, og Berkeley gruppen skildret flere egenskaper, indikatorer og kriterier som de fant i organisasjonene som de forsket på.

Rochlin (1993) definerer en HRO som: *“A highly reliable organization is often defined as one that has already been judged on empirical or observational grounds to provide a desirable activity, product, or service at a desired or demanded level of performance while maintaining a very low rate of error or accident”* (Rochlin, 1993, s. 16).

HRO forskning har vist at høy pålitelighet i høyrisikoteknologier er knyttet til strukturelle trekk, ledelse og kulturelle forhold som gjorde organisasjonene i stand til å håndtere utfordringer knyttet til kompleksitet og tette koplinger. Høy pålitelighet tar utgangspunkt i at den teknologien som organisasjonen opererer, må være godt forstått, og at rutinene er gjennomarbeidet. Disse organisasjonene utvikler ofte et utstrakt rammeverk av prosedyrer for å støtte opp om rutinene. Rutinene bygger på en felles forståelse av hvilke hendelser som ikke

kan få lov til å skje, sammen med grundige og gjennomgående analyser av hva som fører til disse hendelsene (Roe & Schulman, 2008). De søker å arbeide ut fra et bredt grunnlag av forventninger, gjennom variasjon i forhold til årvåkenhet, tillit, kollektiv meningsdannelse, kommunikasjon og samarbeid mellom medlemmene i organisasjonen. HRO-er bruker store ressurser på dette.

HRO-er har som mål å styre enhver tilpasning og redusere usikkerhet (Pettersen & Schulman, 2019). De er ekstremt vare overfor endringer, påvirkninger og hendelser som indikerer at noe kan gå galt, og vil unngå å operere når påliteligheten kan stå på spill. I tillegg til strategien om å redusere usikkerhet har de en årvåkenhet overfor at noe kan gå galt, og at prosedyrer kan være mangelfulle når man møter nye situasjoner eller er utsatt for et høyt arbeidstempo. I slike tilfeller vil organisasjonen anvende erfaringskunnskap, og beslutningsmyndigheten kan bli mer situasjonsbestemt og flyttes nedover i organisasjonen. Dette fører til en økt tilpasningsevne og robusthet i responsen. Samtidig vil ikke HRO-er løse opp i rutiner på en slik måte at resultatet bevisst bryter med ønskede mål og standarder. Egenskapene HRO-er har til tilpasning, har blitt beskrevet som resiliens.

3.3.3 Mindfulness i organisasjoner

For Weick, Sutcliffe og Obstfeld (1999) er det konseptet om «mindfulness» som skiller de gode HROene fra de dårlige. Weick et al (1999) brukte egenskapene i mindfulness til å teoretisere hvordan HROer oppnådde sin høye pålitelighet, sikkerhet og feilfrie operasjoner. Individuell mindfulness beskriver hovedsakelig individets bevissttilstand, preget av økt bevissthet og oppmerksomhet, med en følelse om å «være i øyeblikket» (Sutcliffe, Vogus & Dane, 2016). Kollektiv (eller organisatorisk) mindfulness er et sosialt fenomen og refererer til en tilstand av delt bevissthet og oppmerksomhet som kommer fra interaksjoner mellom flere aktører. Weick et al. hevder at særpreget til HROer ligger i hvordan ulike men stabile kognitive prosesser henger sammen for å kunne oppdage og korrigere feil (Weick et al., 1999). Denne evnen til oppdagelse og korrigerende er det Weick og hans kollegaer betegner som kollektiv mindfulness, og gjennom sin HRO forskning har de funnet fem prosesser som gir HROer denne evnen:

1. **Oppmerksomhet rundt feil og svikt.** Dette innebærer at i en organisasjon der muligheten for prøving og feiling er begrenset, er det allikevel en vilje til å lære av de få feilene som er tilgjengelige. Dette vil oppmuntre de ansatte til å rapportere inn feil

og avvik, på grunn av det læringspotensialet det bringer med seg. Effektive HROer oppmuntrer til rapportering av feil og de får mest mulig ut av de feilene som rapporteres (Weick et al., 1999).

2. **Motvilje mot å forenkle tolkninger.** Handler om å unngå selvtilfredshet og situasjoner der ansatte blir sosialisert til å ignorere de samme tingene. Tradisjonelle organisasjoner har en tendens til å overse spørsmålet om hva de ignorerer, mens effektive HROer respekterer dette spørsmålet og vet mer om hva de ikke vet. I tillegg implementeres ofte redundans i HROer for å bevare bevisstheten. Redundans innebærer kryssjekk, tvil om at forholdsregler er tilstrekkelige og varsomhet rundt påståtte nivåer av kompetanse. Selv om tillitt er en viktig faktor også i HROer, så foreligger det allikevel en tanke om at mennesket gjør feil, og at skepsis og en viss grad av mistro vil forbedre påliteligheten og sikkerheten (Weick et al., 1999).
3. **Følsomhet rundt operasjoner.** Handler om HROer sin situasjonsbevissthet, og at følsomhet rundt operasjoner skal forhindre at feil akkumuleres. Følsomhet for driften blir oppnådd gjennom en kombinasjon av felles mentale antakelser, kollektiv meningsdannelse, kontinuerlig oppdatering og kunnskapsformidling rundt operasjonen og god kjennskap om kompetanse rundt sammenkoplinger og parameterne for systemene. Dette bidrar til å produsere en oppmerksomhet og bevissthet i «øyeblikket» (Weick et al., 1999).
4. **Forpliktelse til resiliens.** Gjør at organisasjonen har kapasitet til å motstå og tilpasse seg forventede og uventede forstyrrelser, og til å gjenopprette funksjonaliteten etter alvorlige påkjenninger. De forbereder seg til utenkelige scenarioer og overraskelser, for å være bedre rustet til å takle slike hendelser. HROer anerkjenner at mennesker gjør feil og at teknologien kan være feilaktig. For å takle denne virkeligheten, tar HROer hensyn til at dette kan føre til feil og farlige situasjoner (Weick et al., 1999).
5. **Underspesifisering av strukturer.** Handler om tilfeller der det detaljerte og ordnede systemet forsterker feil. Dette er et paradoks, fordi de ordnede systemene som er utarbeidet for å unngå feil, noen ganger forårsaker feilene (Weick et al., 1999). En måte å forhindre dette på kan være å løsne på den hierarkiske beslutningsstrukturen og i større grad la beslutningene følge etter problemene. Dette vil bidra til at de ansatte blir mer oppmerksomme og proaktive og «lever i øyeblikket». En særegen egenskap ved effektive HROer, er den fleksible beslutningstakingen der beslutningsmyndigheten blir mer situasjonsbestemt og flyttes nedover i organisasjonen (Weick et al., 1999, s. 103).

Kollektiv mindfulness kan oppfattes som en nøkkelmekanisme der karakteristikken til HROer blir oversatt til evnen til å oppdage og reagere hensiktsmessig på uventede hendelser, og på den måten muliggjøre pålitelig drift under vanskelige forhold (Weick et al., 1999).

3.3.4 Sikkerhetskultur i HRO

Et sentralt element ved HRO-pålitelighetsstyring er lateral kommunikasjon, dvs utveksling, formidling og deling av informasjon, ideer eller følelser mellom menneskene i avdelingen, i organisasjonen, innenfor sektoren eller på et nasjonalt eller overnasjonalt nivå. Slik kommunikasjon er viktig for å opprettholde påliteligheten til systemene, samt for å forhindre desentraliserte og personlige handlinger som ikke tar hensyn til de bredere effektene. Et internt, eksternt og tverrfaglig samarbeid er viktig for å opprettholde et høyt pålitelighetsnivå (Schulman, 2020). HROer kjennetegnes for å ha en sterk sikkerhetskultur, der lateral kommunikasjon er en viktig faktor. En slik kultur er blant annet fleksibel, lærende og rettferdig. Disse kjennetegnene samsvarer med det Reason (1997) beskriver som en generativ organisasjonskultur.

3.4 Reason- forsvar-i-dybden

Reason (1997) sine teorier om «forsvar-i-dybden» illustrerer på mange måter hvordan security systemet på lufthavnene er konstruert, gjennom lag av ulike sikkerhetsbarrierer. Dersom en ulykke eller ondsinnet handling inntreffer, betyr det at disse barrierene er blitt brutt eller forbigått. Til tross for at Reason sine teorier i utgangspunktet er på organisatoriske ulykker (safety), vil imidlertid teorien kunne overføres til en security kontekst, da lag av sikkerhetsbarrierer anvendes i forebyggingen av både security trusler og safety trusler. Hensikten med lag av sikkerhetsbarrierene er å skille skadelige farer og trusler ifra sårbare mennesker, verdier eller eiendeler (Reason, 1997, s. 2). Reason trekker frem tre faktorer som kan føre til at trusselen trenger igjennom de ulike sikkerhetsbarrierene: menneskelige, tekniske eller organisatoriske.

Alle forsvar er designet for en eller flere av disse funksjonene (Reason, 1997, s. 7).

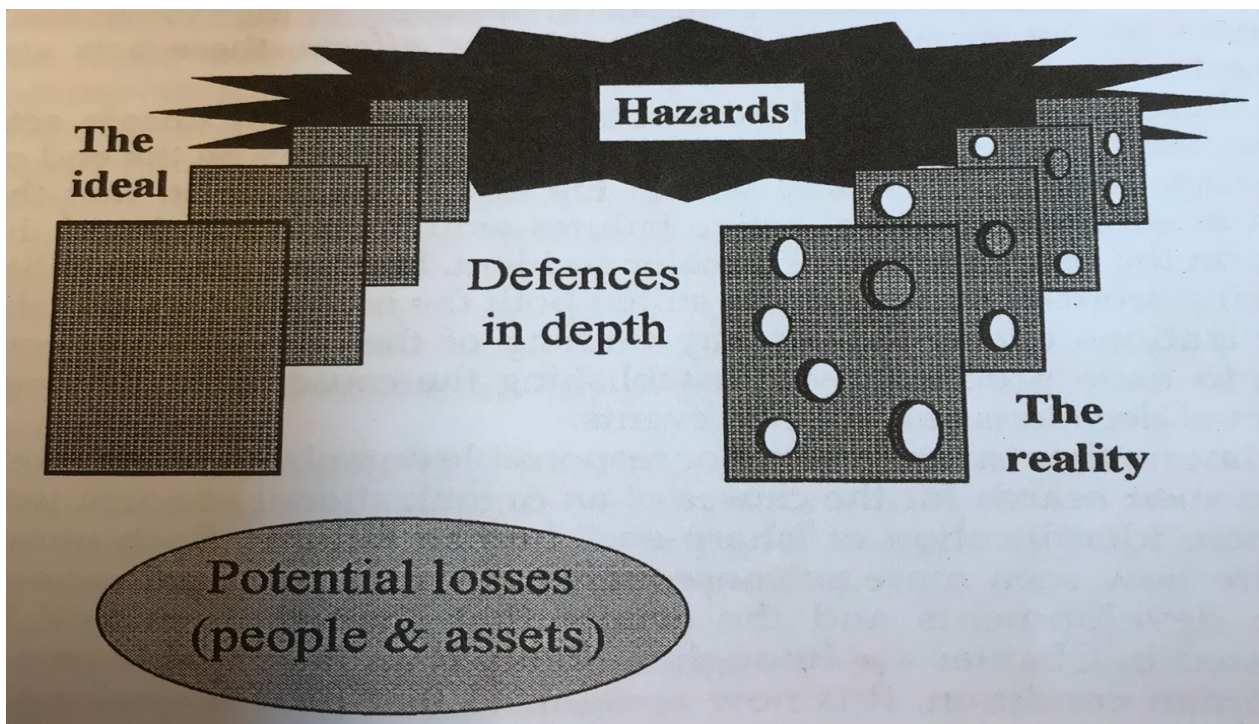
- Å skape en forståelse og bevissthet om de lokale farene.
- Å gi klare retningslinjer for hvordan man skal operere trygt.
- Å gi advarsler, gjerne i form av alarmer, når faren er nært forestående.
- Å gjenopprette systemet til en trygg tilstand i en unormal situasjon.

- Å plassere sikkerhetsbarrierer mellom farer og potensielle tap.
- Å begrense og eliminere farene dersom de unnslipper barrierene.
- Å sørge for fluktmuligheter og redning dersom en fare manifesterer seg.

Implisitt i rekkefølgen av denne listen er ideen om «forsvar-i-dybden»- suksessive lag av beskyttelse, ett lag bak ett annet. Hvert lag beskytter mot potensiell nedbryting av det foran. Når prosedyreveiledning, bevissthet og sikkerhetsforståelse ikke holder potensielle ofre borte fra farer, vil alarmer og advarsler varsle de ansatte om faren, og de kan gjenopprette systemet til en trygg tilstand. Hvis dette ikke er oppnåelig, er det fysiske barrierer mellom de potensielle tapene og farene. Andre forsvarsmekanismer har som hensikt å eliminere og begrense farene. Dersom alle disse forsvarerne mislykkes i å stoppe trusselen, blir flukt- og redningstiltak satt i kraft. Det er dette mangfoldet av et overlappende og gjensidig støttende forsvar som gjør at små feil av menneskelig eller teknisk art ikke resulterer i en ulykke eller katastrofe. Tilstedeværelsen av dette mangfoldet av forsvarsbarrierer, gjør at ulykker og uønskede hendelser skjer svært sjelden i dag (Reason, 1997).

De ulike forsvarsmekanismene er en blanding av det Reason (1997) omtaler som «harde» og «myke» forsvar. Det harde forsvaret inkluderer det fysiske forsvaret og barrierene. Tekniske enheter som automatiserte konstruerte sikkerhetsfunksjoner, fysiske barrierer, alarmer og varslingsystem, nøkler, ID-kort, personlig verneutstyr, forbedret systemdesign etc. Det myke forsvaret viser til en kombinasjon av papir og mennesker: lover, regulatorisk overvåkning, regler og prosedyrer, opplæring, trening og øvelser, orienteringer, administrative kontroller, lisensiering, sertifisering, tilsyn etc (Reason, 1997).

I en ideell verden ville alle lagene av forsvar vært intakte, og ikke tillate gjennomtrengning av ulike trusler, som vist på venstre side i figuren under. I den virkelige verden har imidlertid hvert lag av forsvar svakheter og hull i seg, som vist på høyre side i figuren. Reason (1997) har betegnet modellen som «The Swiss Cheese model», da hullene i forsvarslagene kan minne om en såkalt sveitserost.



Figur 3: Swiss cheese model (Reason, 1997)

Til tross for at figuren fremstiller de ulike forsvarslagene som faste og statiske, så er de i realiteten i konstant flyt og bevegelse. Figuren blir derfor best illustrert gjennom et bevegelig bilde, hvor hvert forsvarslag kommer inn og ut av rammen i samsvar med lokale forhold. Enkelte lag av forsvar kan fjernes bevisst under vedlikehold, kalibrering og testing, eller som et resultat av feil og brudd. På samme måte kan hullene i hvert lag bevege på seg, komme og gå, samt krympe og utvide seg som følge av operatørhandlinger eller lokale forhold. For å finne svar på hvordan disse hullene skapes, må skillet mellom aktive feil og latente forhold vurderes (Reason, 1997).

3.4.2 Aktive feil og latente forhold

Siden det er mennesker som designer, produserer, driver, vedlikeholder, overvåker og administrerer komplekse teknologiske systemer, er det ikke overraskende at menneskelige beslutninger og feilhandlinger kan føre til uønskede hendelser. Mennesker kan bidra til sammenbrudd av slike systemer på to måter. Mest tydelig blir det når feil blir gjort i den skarpe enden av systemet, for eksempel dersom en ansatt i sikkerhetskontrollen på en flyplass ikke oppdager en bombe i håndbagasjen til en gjerningsmann. Slike feil vil mest sannsynlig ha direkte innvirkning på sikkerheten, og på grunn av denne umiddelbare negative effekten blir slike feilhandlinger betegnet som aktive feil (Reason, 1997)

Det er nå anerkjent at mennesker som jobber i komplekse systemer gjør feil eller bryter med prosedyrer av grunner som generelt går utenfor omfanget av individuell psykologi. Slike årsaker betegnes som latente forhold. En utfordring med et forsvar-i-dybden, er at det gjør systemene mer komplekse. Det kan være utfordrende for menneskene som administrerer og overvåker systemene å ha den nødvendige forståelsen og innsikten i alle disse lagene av forsvar. Latente forhold kan være: dårlig design, svakt og ufullstendig tilsyn, uoppdagede produksjonsfeil eller vedlikeholds svikt, kompliserte prosedyrer, feilaktig automatisering, mangelfull opplæring og mangel på tilstrekkelig verktøy og utstyr. Slike latente forhold kan være til stede i flere år, før de kombineres med lokale forhold og aktive feil og bidrar til at trusselen klarer å trenge seg igjennom lagene med forsvar. Slike latente forhold stammer fra beslutninger som er tatt på det strategiske nivået, fra myndigheter, regulatorer, produsenter, designere og organisasjonsledere (Reason, 1997). Latente forhold er til stede i alle systemer, og er en uunngåelig del av organisasjonslivet. De kan øke sannsynligheten for at aktive feil begås, ved at de skaper lokale faktorer som kan fremme feil eller brudd.

Teorikapittelet har gitt en presentasjon av risiko og usikkerhetsbegrepene, hva som kjennetegner security risikoer og hvordan de skiller seg fra safety risikoer. Videre er rammene som Avinor arbeider innenfor blitt belyst, gjennom teori om risikostyring og regulering. Kjennetegn ved organisasjoner som opererer innenfor høyrisikoindustrier er blitt belyst gjennom HRO teori, hvor komponenter som fører til høy pålitelighet er blitt redegjort for. Til slutt ble Reason sine teorier om forsvar-i-dybden lagt frem for å belyse hvordan security systemet i luftfarten er konstruert for å forebygge terroranslag, og ulike faktorer som kan føre til uønskede hendelser.

4. Metode

I denne delen presenteres de ulike metodiske fremgangsmåtene som er blitt foretatt for å danne det empiriske grunnlaget for å besvare studiens problemstilling. Målsetningen har vært å skape sikre data som kan besvare de tre forskningsspørsmålene for å belyse problemstillingen. Innledningsvis presenteres forskningsdesign- og strategi, før en videre redegjørelse av hvordan dataene har blitt innsamlet og analysert blir foretatt. Videre vil jeg reflektere over studiens reliabilitet, validitet og etiske betraktninger. Avslutningsvis vises det til metodiske styrker og svakheter.

4.1 Problemstilling og forskningsspørsmål

Blaikie (2019) anser formuleringen av forskningsspørsmål som en av de viktigste delene av et forskningsdesign. Etableringen av forskningsspørsmål gjør det mulig å velge forskningsstrategi, metode for datainnsamling og en analyse basert på tillit.

Forskningsspørsmål kan grupperes i tre hovedtyper; hva, hvorfor og hvordan-spørsmål. Hva spørsmålet kommer gjerne før hvorfor spørsmålet, og hvorfor spørsmålet kommer før hvordan spørsmålet. Man må forstå hva som skjer før man kan forklare det, og man må vite hvorfor et fenomen oppfører seg slik det gjør, før vi kan komme frem til en praktisk løsning for å forandre det. I forbindelse med valg av forskningsspørsmål, er det avgjørende å velge spørsmål som passer til forskerens motivasjon og ønsker, men også de eksternt gitte rammene som tilgang på data, lokalisering, forskningens relevans og tidsrammer (Blaikie, 2019, s. 68).

Hva spørsmålet i denne studien innebærer en beskrivelse av karakteristikkene ved dagens security-regimet, og hvilke følger det får for security-arbeidet i norsk luftfart. Videre retter hvorfor spørsmålet seg mot bakgrunnen for at KPIene anvendes for å definere sikkerhetsnivået, og hvilke variabler som kan påvirke påliteligheten til KPIene. Til slutt vil hvordan spørsmålet belyse hvordan security-regimet kan bli mer risikobasert og proaktivt i møte med trusselen for terrorisme. Forskningsspørsmål handler om hvilken kunnskap forskeren ønsker å produsere. Et forskningsprosjekt kan ta utgangspunkt i flere av disse, men kun en om gangen. Det vil si at en studie kan begynne med å beskrive, og fortsette med å forklare eller forandre (Blaikie, 2019).

Formålet med oppgaven har gjennomgående vært å undersøke hvordan Avinor arbeider for å forhindre anslag mot norsk luftfart. Problemstillingen og forskningsspørsmålene er blitt

justert og presisert underveis. Etter hvert som jeg fikk mer forståelse rundt temaet, fikk jeg økt kunnskap om hvilke faktorer det var relevant å kartlegge. På bakgrunn av dette utarbeidet jeg i samarbeid med Avinor en interessant problemstilling, samt forskningsspørsmål som kunne fange opp relevante faktorer som kunne belyse problemstillingen.

4.2 Forskningsdesign og strategi

Bestemmelser knyttet til datainnsamling vil variere i forhold til hvilken forskningsstrategi som anvendes. I et forskningsdesign gjør forskeren rede for planen med forskningsprosjektet, samt tydeliggjør valgene som ble tatt i prosessen. Blaikie (2019) mener at et forskningsdesign refererer til prosessen som kopler sammen forskningsspørsmål, empiriske data og forskningskonklusjoner.

I følge Blaikie (2019, s. 16) må følgende tre spørsmål besvares i et forskningsdesign. Med utgangspunkt i min problemstilling blir det som følger;

1. *Hva skal studeres* (hvordan security-regimet i luftfarten er konstruert for å forebygge terroranslag, hvilke aktører og regler som inngår i regimet og hvor sikre KPIene er for å kunne definere sikkerhetsnivået på bakgrunn av dem).
2. *Hvorfor skal det studeres* (det er kritisk at sikkerhetsnivået på lufthavnene blir definert på et pålitelig grunnlag, for å ivareta flysikkerheten. Å stille spørsmål ved slike etablerte sannheter vil kunne føre til økt bevissthet på området).
3. *Hvordan skal det studeres* (kvalitativ metode- semistrukturerte intervjuer og dokumentanalyse) og analyse av Avinors datamaterialet. Dette spørsmålet kan igjen deles inn i; hvilken forskningsstrategi skal brukes, hvor kommer data fra og hvordan skal datainnsamling og analyse foregå, samt definering av hvert forskningsstadium).

4.2.1 Retroduktiv forskningsstrategi

Studien bygger på en retroduktiv forskningsstrategi, ettersom data fra intervjuene og dokumentanalysene baserer seg på en rekke rutiner, forskrifter, lover og regler. Informantenes adferd kan derfor i stor grad forklares ut ifra retningslinjer og rammeverk de har å forholde seg til. Samtidig vil de ha egne tanker om hvordan dette fungerer i praksis og eventuelle konsekvenser av reguleringen. Retroduksjon er en metode som er forbundet med kritisk realisme og som forsøker å kombinere både induksjon og deduksjon (Blaikie, 2019, s. 97). Forskningsprosessen og retroduksjon hjelper forskeren til å videreutvikle kunnskapen om

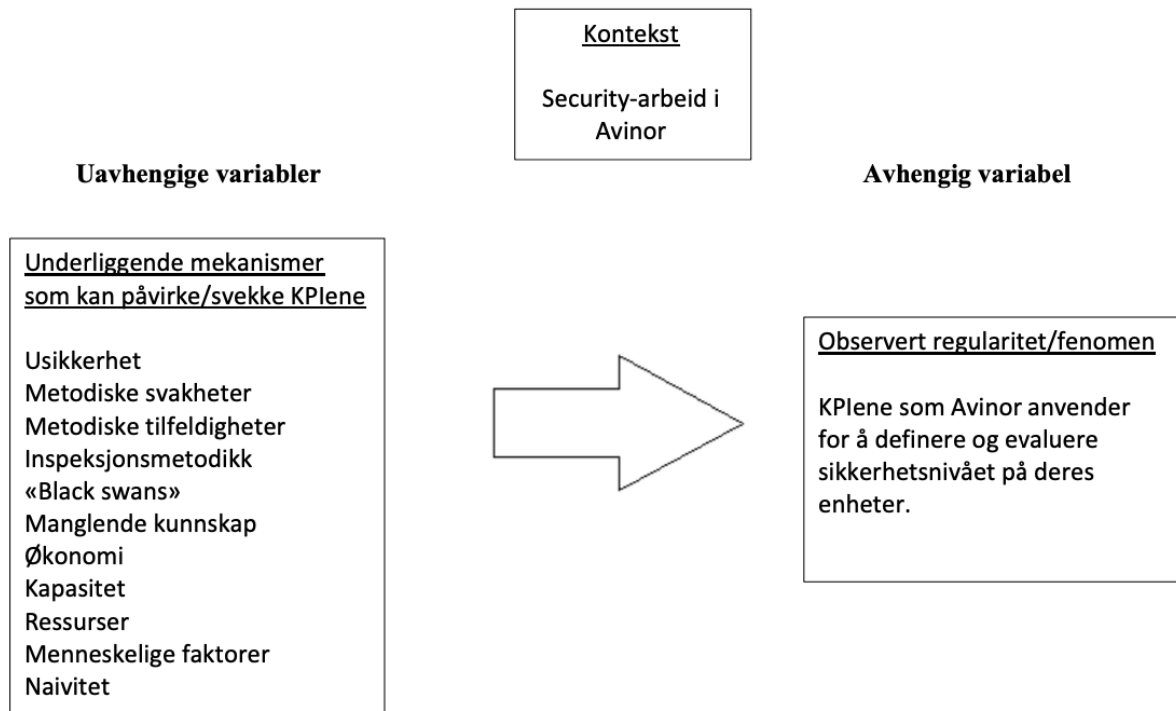
sosiale fenomener og hvordan vi forstår virkeligheten. Hensikten med å benytte seg av en retroduktiv forskningsstrategi er et ønske om å kartlegge underliggende mekanismer i en bestemt kontekst, som bidrar til å forklare en eller flere observerte regulariteter og/eller fenomener. Dette innebærer at man tar utgangspunkt i å arbeide seg tilbake fra data og frem mot en mulig forklaring (Blaikie, 2019, s. 97).

Den første fasen i et forskningsarbeid basert på en retroduktiv forskningsstrategi, er å utarbeide og formulere en god beskrivelse av den observerte regulariteten som oppgaven har til hensikt å undersøke. Videre bør man konstruere en hypotetisk modell som viser til den observerte regulariteten, samtidig som modellen sier noe om hvilke underliggende mekanismer man ønsker å forklare regulariteten opp imot (Blaikie, 2019, s. 98). I dette tilfellet fastslår oppgaven at Avinor definerer deres sikkerhetsnivå på bakgrunn av ulike KPIer, og at dette er den observerte regulariteten som man ønsker å forklare gjennom valgte underliggende mekanismer. At KPIene kan være upålitelige, reaktive eller lite risikobaserte i møte med et usikkert og komplekst trusselbilde, samt at KPIene kan inneholde usikkerhet og metodiske svakheter og tilfeldigheter, er fastsatt som oppgavens hypotetiske underliggende mekanismer.

I korte trekk kan man oppsummere og forklare den retroduktive forskningsstrategien ut ifra fem punkter;

1. Utarbeidelsen og en beskrivelse av de underliggende mekanismene som oppgaven ønsker å undersøke i forhold til den observerte regulariteten, hvor man så
2. Konstruerer en modell med plasseringen av den observerte regulariteten/fenomenet og plasserer det inn i en sosial kontekst/sammenheng.
3. Dersom modellen er korrekt representerer den mekanismen(e) og sammenhengen som forklarer regulariteten.
4. Deretter skal modellen testes som en hypotetisk beskrivelse av den faktisk observerte regulariteten/fenomenet og deres relasjoner. Min oppgave som forsker er å teste modellen for å undersøke hvorvidt det foreligger en sammenheng mellom mekanismene og regulariteten/fenomenet.
5. Dersom disse testene viser vellykkede resultater, gir dette grunn til å trekke konklusjoner om at det finnes en faktisk sammenheng.
(Blaikie, 2019, s. 98-99).

På bakgrunn av argumentasjonen redegjort for ovenfor tar denne studien utgangspunkt i en hypotetisk modell som illustreres nedenfor.



Figur 4: Hypotetisk modell av uavhengige og avhengige variabler (Babbie, 2010)

Modellen har som hensikt å søke forklaringer på den avhengige variabelen, den observerte regulariteten/fenomenet, ved å identifisere uavhengige variabler som i denne sammenhengen beskrives som underliggende mekanismer (Babbie, 2010, s. 94).

4.3 Triangulering av metoder

Min metode bygger på kvalitative forskningsmetoder, med en kombinasjon av semistrukturerte intervjuer og dokumentanalyse. Gjennom anvendelse og kombinasjon av forskningsmetodene kan samme fenomen belyses for å unngå iboende svakheter i studien. Poenget med å kombinere metoder er for å teste resultatenes validitet som fremtrer fra metodene. På den måten kan dataene og undersøkelsen få en høyere troverdighet (Bryman, 2006). Forskeren kan dermed oppnå et mer helhetlig bilde av fenomenet som studeres, fordi ulike data gir en komplimenterende tilnærming til fenomenene. Videre er det et argument at triangulering av metoder kan bidra til utvikling i selve forskningsprosjektet. Blaikie (2019) argumenterer for at bruk av enkeltmetoder vanligvis er forbundet med smale forskningstemaer med ett forskningsspørsmål. Slik forskning gir begrensede muligheter for å

fremme kunnskap. Derfor vil en kombinasjon av flere metoder være hensiktsmessig dersom målet er å fremme kunnskap og belyse problemstillingen fra flere ulike sider (Blaikie, 2019, s. 219).

I tillegg til de kvalitative metodene, har jeg fått tilgang til data fra Avinors interne analysesystem. Dataene fremstiller sikkerhetsnivået ved alle Avinors lufthavner, på bakgrunn av resultatene fra Luftfartstilsynets inspeksjoner. Jeg har ikke innhentet dataene selv, eller foretatt egne kvantitative analyser av datamaterialet. Bakgrunnen for det, er at jeg anser det som utfordrende å belyse problemstillingen gjennom kvantitative analyser av datamaterialet. I analysedelen anvendes materialet som et supplerende aspekt for å belyse problemstillingen og for å illustrere hvordan Avinor definerer og evaluerer deres sikkerhetsnivå, og hvordan utviklingen i sikkerhetsnivået på de ulike lufthavnene har vært de senere årene. Intervjuene og dokumentanalysene har på den andre siden hensikt i å gå direkte inn for å besvare problemstillingen. Avinor anvender analyseverktøyet Microsoft Power BI for å definere og evaluere sikkerhetsnivået på lufthavnene. Jeg har fått tilgang til samme plattform for å foreta egne refleksjoner og analyser. Analyseverktøyet gir mulighet for å studere og fremstille dataen gjennom ulike diagrammer. Siden datamaterialet er underlagt taushetsplikt, vil jeg ikke presentere detaljerte og sårbare opplysninger, noe jeg begrunner mer grundig senere i kapitlet.

Studiens metode er delvis innenfor rammene til det som omtales som «mixed-methods» (kombinasjon av kvalitativ og kvantitativ forskningsmetode). Metoden anses likevel for å være innenfor en kvalitativ tilnærming, da primærdata innhentes gjennom intervjuer mens den kvantitative dataen er sekundærdata som er innhentet av Avinor og anvendes som supplerende empiri. Tilsynsrapportene som analyseres gjennom dokumentanalysene, er også sekundærdata, men jeg foretar egne analyser av rapportene. Ved å ta i bruk primærdata vil jeg få en nærhet til datakildene som samles inn, og jeg vil selv ha deltatt i innsamlingen av dem (Halvorsen, 2008).

4.3.1 Semistrukturerte intervjuer

For å oppnå en dypere innsikt i studiens komplekse problemstilling, anså jeg det som nødvendig å foreta intervjuer med relevante aktører innenfor security regimet i norsk luftfart. Jeg valgte intervju fordi det kunne tilføye en ekstra dimensjon til studien, og fordi problemstillingen kunne bli sett fra involverte aktørers perspektiv forut for vitenskapelige

forklaringer (Kvale & Brinkmann, 2012). Samtidig er intervju en fleksibel metode, og ga meg mulighet til å utarbeide spørsmål direkte knyttet til problemstillingen i tillegg til at jeg kunne stille oppfølgingsspørsmål og oppdage uforutsette forhold (Grønmo, 2004). Intervjuene førte til at temaet ble belyst fra ulike sider, da aktører fra ulike virksomheter og ulike nivåer ble intervjuet. I et forskningsintervju produseres kunnskap sosialt, gjennom interaksjon mellom forsker og informant. Kvaliteten på data fra et intervju avhenger av kvaliteten på intervjuerens ferdigheter og kunnskaper om temaet (Kvale & Brinkmann, 2012, s. 99). I forkant av alle intervjuer hadde jeg derfor fokus på å utarbeide relevante og treffende spørsmål til de ulike informantene, i tillegg til at jeg satte meg godt inn i deres fagområder og roller. Fordelen med semistrukturerte intervjuer er at det kan minne om en dagligdags samtale, noe som fører til at informantene i større grad kan uttrykke seg mer åpent og fritt. Intervjuet utføres i overensstemmelse med en intervjuguide som sirkler inn bestemte temaer, og som kan inneholde forslag til spørsmål (Kvale & Brinkmann, 2012, s. 47). Det betyr at det verken er en åpen samtale eller at det blir benyttet et spørreskjema.

4.3.2 Utvalg av informanter

I startfasen av studien opprettet jeg først kontakt med security avdelingen i Avinor, og i den anledning hadde jeg en uformell samtale via Microsoft Teams med en informant fra avdelingen. Under samtalen ble ulike temaer og problemstillinger diskutert, og vi ble enige om studiens tematikk og problemstilling. Videre ga informanten meg en innføring i hvordan Avinor arbeider med security, hvilke krav de er pålagt å følge, hvordan de blir inspisert, hvilke verktøy og styringsindikatorer de bruker for å overvåke sikkerhetsnivået etc. Ett par uker senere hadde vi en ny digital samtale, før vi møttes på Stavanger lufthavn noen uker etter det igjen. Informanten ga en detaljert innføring i verktøyene som Avinor anvender i deres security-arbeid, samtidig som relevant informasjon knyttet til problemstillingen ble formidlet. Videre signerte jeg på en taushetserklæring, og fikk tilgang til tilsynsrapportene fra Luftfartstilsynet og analyseprogrammer og verktøy som Avinor anvender i deres risikostyring. Under de tre samtalene ble relevant informasjon og refleksjoner knyttet til temaet og problemstillingen formidlet av informanten. Informasjonen vil derfor behandles som om den ble innhentet gjennom et ordinært intervju.

Det videre utvalget av informanter er basert på strategisk utvelging, da jeg underveis i prosessen fikk økt innsikt i hvilke aktører det ville være strategisk relevant å inkludere i utvalget (Grønmo, 2004, s. 98). Utvalget består av totalt fire informanter:

Informant 1 er ovennevnte informant fra security avdelingen i Avinor. Informant 2 er en lufthavnsjef fra Avinor, stasjonert på en mellomstor lufthavn i Norge. Informant 3 arbeider i securityseksjonen i Luftfartstilsynet. Informant 4 arbeider i Samferdselsdepartementet, avdeling for luftfart-, post- og kjøp, seksjon for regulatoriske og internasjonale saker. Informantene vil av hensyn til anonymitet refereres til som:

Informant 1 Avinor, informant 2 Avinor, informant Luftfartstilsynet, informant SD.

Det ble utført semistrukturerte intervjuer med alle informantene, med unntak av *informant 1 Avinor*, hvor informasjon ble innhentet gjennom uformelle samtaler. Formålet med å intervjuer aktører fra ulike virksomheter, var for å belyse problemstillingen fra ulike perspektiver og nivåer innad i security-regimet. Security i luftfarten er omfattende og komplekst, med mange involverte aktører på ulike nivåer. Et utvalg av informanter på ulike nivåer var derfor hensiktsmessig.

4.3.3 Forberedelse og gjennomføring av intervju

Intervjuene ble utført digitalt, som følge av Covid-19 restriksjoner og store geografiske avstander til informantene. Intervjuene med *informant 2 Avinor* og *informant Luftfartstilsynet* foregikk via Microsoft Teams, mens intervjuet med *informant SD* foregikk via telefon. I forkant av intervjuene fikk informantene tilsendt intervjuguider, slik at de var forberedt og dermed kunne gi mer utfyllende og reflekterende svar. Ulempen med å sende intervjuguiden i forkant, er at man kan gå glipp av den spontane responsen på spørsmålene. Det ble utarbeidet egne intervjuguider for hver informant, slik at spørsmålene var relevante og samsvarte med deres ansvarsområder, roller og kompetanse. Samtidig inneholdt intervjuguidene mange av de samme spørsmålene, for å få innsikt i hvordan ansatte i ulike virksomheter og på ulike nivåer i systemet reflekterte rundt de samme spørsmålene. Informantene fikk også i forkant av intervjuene tilsendt bakgrunnsinformasjon om studiet og en samtykkeerklæring.

Under intervjuene ble intervjuguiden benyttet for å føre samtalen i ønsket retning, men intervjuene var samtalebaserte og fleksible. Flexibilitet i intervjusituasjonen førte til at informantene kunne komme med tilleggsinformasjon og eksempler (Grønmo, 2004, s. 159-162). Underveis i intervjuene tok jeg lydopptak og stilte oppfølgingsspørsmål etter behov. Det ga meg mulighet til å reflektere underveis og aktivt stille presise oppfølgingsspørsmål for å oppnå mer detaljert kunnskap. I etterkant av intervjuene og etter at intervju transkripsjonene

var blitt foretatt, kunne intervjuene betraktes som grunnleggende empiriske data i mitt prosjekt. Når intervjumaterialet struktureres i tekstform blir det lettere å få oversikt over det, og struktureringen er i seg selv en begynnelse på analysen (Kvale & Brinkmann, 2012, s. 188). Data fra intervjuene ble først bearbeidet gjennom åpen koding for å registrere gjennomgående sentrale empiriske funn. Deretter gjennomførte jeg en mer systematisk koding der jeg hentet ut og registrerte informasjon som var relevant for problemstillingen og de tre forskningsspørsmålene. På bakgrunn av dette utviklet jeg kategorier med fellestrekk og liknende egenskaper fra informasjonen fra de ulike informantene. Disse kategoriene vil utgjøre strukturen i presentasjonen av resultatene fra intervjuene i empiridelen.

4.3.4 Dokumentanalyse

I dokumentanalysen har jeg systematisk gjennomgått innholdet i utvalgte tilsynsrapporter fra perioden 2015-2020 som Avinor har mottatt fra Luftfartstilsynet i etterkant av inspeksjoner. Grønmo (2004) hevder at hovedkjennetegnet ved denne formen for analyse er en systematisk gjennomgang av dokumenter med sikte på å kategorisere innholdet, og registrering av data som er relevant for problemstillingen. Hensikten med analysen av rapportene har vært å avdekke og registrere relevant informasjon knyttet til samspillet mellom tilsynsmyndigheten og tilsynsobjektet, og videre hvilke styrker og svakheter som foreligger ved en slik form for tilsynsvirksomhet. Tilsynsrapportene er unntatt offentligheten, og informasjon fra rapportene vil derfor fremlegges med varsomhet. Utvelgelsen av rapportene har foregått underveis i studien og blitt tilpasset etter hvert som problemstillingen og forskningsspørsmålene ble bedre belyst. I det følgende vil jeg redegjøre for hvordan utvalg av dokumenter og informasjon foregikk.

4.3.5 Utvalg av dokumenter

Luftfartstilsynets tilsynsaktivitet og tilsynsrapporter er en sentral del av security-arbeidet i luftfarten. Forskningsspørsmålene ga føringer for hvilken type informasjon det var relevant å studere og registrere fra rapportene. Dette var informasjon knyttet til rapportenes innhold og utforming, hvilket grunnlag de baserer sine inspeksjoner på, hvordan inspeksjonene foregår i praksis, hvordan tilsynsaktiviteten og rapportene kan bidra med å avdekke og utbedre avvik og på den måten styrke sikkerheten og eventuelle svakheter med rapportene eller tilsynsaktiviteten.

Luftfartstilsynet har foretatt 171 inspeksjoner av Avinors lufthavner i perioden 2015-2020, som er den avgrensede perioden denne studien vil basere analysene på. Jeg har tilgang til alle rapportene fra disse inspeksjonene, og det var nødvendig å foreta en avgrensing med tanke på hvilke rapporter som skulle utgjøre grunnlaget for dokumentanalysen. Utvelgelsen av rapportene er blitt foretatt med hensyn til ulike faktorer: størrelse på lufthavnene, geografisk lokasjon, tidspunkt for inspeksjon og ulike typer avvik. Utvelgelsen og systematiseringen utgjorde et grunnlag for å kunne sammenlikne data fra de ulike dokumentene, som presenteres i empiridelen av oppgaven.

4.4 Reliabilitet og validitet

Reliabilitet retter seg mot studiens pålitelighet og knytter seg til spørsmålet om en kritisk vurdering av studien gir inntrykk av at forskningen er utført på en tillitsvekkende måte (Thagaard, 2018, s. 201). En studie kan sies å ha høy reliabilitet dersom en annen forsker har mulighet til å komme frem til de samme resultatene ved å gjenta undersøkelsen og anvende den samme metoden. Studien bærer preg av en retroduktiv forskningsstrategi, og mulighetene for en reproduksjon av studien ved hjelp av en retroduktiv forskningsstrategi vil være større sammenliknet med bruk av andre forskningsstrategier. Informantenes utsagn og standpunkter er i stor grad basert på de prosedyrer og regler de må forholde seg til. Reliabiliteten vil imidlertid kunne svekkes ved at presentasjonen av resultatene er i lys av mine tolkninger og i lys av den konteksten informasjonen ble innhentet i. Andre kunne ha tolket de samme dataene annerledes.

I et forsøk på å øke reliabiliteten har jeg benyttet en semistrukturert intervjuguide. Hensikten var å skape en noenlunde tilsvarende intervjusituasjon for alle informantene. Underveis i intervjuene avklarte vi informasjon for å bekrefte at uttalelsene var blitt forstått riktig. Videre vil det være mulig å analysere de samme tilsynsrapportene på liknende vis, da rapportene ikke vil endres som følge av at de baserer seg på allerede utførte inspeksjoner. Andre forskere vil imidlertid kunne tolke data fra rapportene annerledes.

Gjennom intervjuene fikk jeg ikke inntrykk av at informantene utelot sentral informasjon som kunne virke negativt på security- regimet eller deres respektive virksomheter (Grønmo, 2004, s. 165). Mitt inntrykk var at informantene ønsket å bidra til studien og forsøkte å besvare spørsmålene så utfyllende og korrekt som mulig. Grønmo (2004, s. 165) viser samtidig til at ukorrekte opplysninger kan avdekkes ved å tolke informantenes svar opp mot hverandre. Jeg

sammenliknet informantenes beskrivelser, og avdekket at det foreligger samsvar mellom de fleste beskrivelsene. Det bidrar til å styrke reliabiliteten.

For å kunne bedømme hvorvidt forskningen har gitt et korrekt svar på problemstillingen, må intern og ekstern gyldighet (validitet) vurderes (Jacobsen, 2000). Førstnevnte innebærer hvorvidt resultatene kan oppfattes som «sanne», i den grad et fenomen er befestet med en objektiv sannhet. I empiridelen er utsagnene fra informantene i tråd med det som kom frem av intervjuene. Videre bekreftet jeg gyldigheten til data fra intervjuene ved å sammenlikne informasjonen med ulike dokumenter. Dokumentanalysen og analysen av Avinors data bidro til at jeg oppnådde oversikt over gjeldende regelverk og hvordan kontroll- og tilsynspraksisen foregår, noe som styrker validiteten.

Knyttet til den eksterne gyldigheten presiserer Jacobsen (2000) at formålet med kvalitative metoder vanligvis ikke er «å generalisere fra utvalget av enheter til en stor gruppe enheter». Utvalget av informanter og dokumenter kan i den sammenhengen anses for å være lite i forhold til studiens vide og komplekse problemstilling. Tanker og refleksjoner knyttet til hvor sikre KPIene er, vil variere mellom EU stater, lufthavner, sikkerhetsekspertene, politikere, politi, ansatte på ulike nivåer på lufthavnene etc. Samtidig har utvalget av informantene høy kompetanse på området, og tilsynsrapportene er utarbeidet på et sterkt faglig grunnlag.

4.5 Etiske betraktninger

Mye av security-arbeidet i luftfarten er underlagt strengt hemmelighold. Med hensyn til de kravene som foreligger, har sensitiv informasjon i denne studien blitt behandlet med varsomhet. Denne begrensningen har tilsynelatende vært styrende for hvilken informasjon informantene kunne formidle i intervjuene, samt hvilken informasjon jeg kunne presentere og analysere på bakgrunn av tilsynsrapportene og Avinors datamateriale.

I denne studien er det særlig vektlagt at alle opplysninger blir behandlet konfidensielt. Hensikten er at ingen skal kunne gjenkjenne personene som er blitt intervjuet, eller at statistikk, avvik og informasjon kan spores tilbake til enkelte lufthavner. Materialet som blir brukt, skal ikke være til skade eller ulempe for informantene eller virksomhetene. Etter skriftlig samtykke fra informantene kan imidlertid informasjon benyttes i den grad av vedkommende ikke blir gjenkjent, eller informasjon knyttet til sårbarheter i systemet eller på enkelte lufthavner. Studien er meldt inn og godkjent av Norsk senter for forskningsdata (NSD).

Lydopptak som er gjort i forbindelse med intervjuene, er kun beregnet for denne masteroppgaven. Disse vil bli slettet etter at sensur er falt.

4.6 Styrker og svakheter ved metodevalg

En utfordring i denne studien har vært å finne frem til data som direkte besvarer studiens komplekse problemstilling. Det er utfordrende å besvare en slik problemstilling med to streker under svaret. Å avgjøre hvilke KPIer eller hvilket reguleringsregime som bør være gjeldene i luftfarten, vil i stor grad bygge på spekulasjoner fordi usikkerheten og kompleksiteten er stor. Likevel har formålet med studien vært å finne frem til empiri og koble den opp imot relevant teori, da dette vil gi økt kunnskap og bevissthet rundt problemstillingen.

Det er utfordrende å gi en fullstendig presentasjon av hele security-regimet i luftfarten, da flere områder er underlagt strengt hemmelighold. Flere usynlige tiltak og barrierer foreligger i systemet, noe denne studien ikke kan ta i betraktning. Sikkerhetssystemet er derfor mer omfattende og komplekst enn det denne studien gir uttrykk for. Studien fokuserer kun på de områdene av security-arbeidet som er tilgjengelig for offentligheten, noe som svekker studiens forutsetning for å belyse alle elementene som inngår i systemet. Studien involverer imidlertid flere sentrale og viktige aspekter ved security-regimet, og vil derfor ha en sterk relevans for industrien.

Videre ville deltakende observasjon på lufthavnene vært hensiktsmessig å ha gjennomført. På den måten kunne studien gitt en dypere innsikt i hvordan ansatte på lufthavnene utfører security-arbeidet og hvilken grad de anser regelverket for å være tilpasset norske forhold. Grunnet studiens tidsramme og restriksjoner knyttet til Covid-19 ble dette ikke gjennomført. Jeg vurderte det som hensiktsmessig å avgrense studien til å studere problemstillingen fra et mer sentralisert og overordnet nivå.

Styrkene ved metodevalgene er at empirien bygger på uttalelser og informasjon formidlet av kompetente og relevante informanter, som har bidratt til god innsikt i studiens tematikk og problemstilling. I tillegg bygger studien på dokumenter som detaljert fremstiller hvordan reguleringsregimet i luftfarten fungerer i praksis. Studien bygger også på reell statistikk fra Avinors lufthavner, som viser hvordan Avinor definerer og evaluerer sikkerhetsnivået på deres lufthavner.

5. Empiri

I dette kapittelet vil jeg starte med å gi en detaljert illustrasjon over hvordan Avinor anvender resultatene fra Luftfartstilsynets inspeksjoner som styringsindikator for å definere og evaluere sikkerhetsnivået på deres enheter. Videre vil jeg presentere funn fra dokumentanalysene og intervjuene, som er primærdata som skal besvare problemstillingen.

5.1 Avinors risikostyring

Avinor definerer og evaluerer deres sikkerhetsnivå på bakgrunn av 73 målepunkter/KPI. Luftfartstilsynet foretar hyppige og grundige inspeksjoner av norske lufthavner, for å kontrollere at Avinor som lufthavnoperatør samsvarer med de ulike sikkerhetskravene. I etterkant av alle inspeksjoner får Avinor tilsynsrapporter, hvor Luftfartstilsynet informerer om hvilke punkter som ble kontrollert, graden av samsvar med kravene og en nærmere beskrivelse av eventuelle avvik. Graden av samsvar blir fremstilt i form av en karakter (1-5).

1	Alvorlige avvik som truer flysikkerheten.
2	Avvik som kan true flysikkerheten.
3	Samsvar med krav, men med kommentar om ønsket forbedring.
4	Samsvar med krav.
5	Bedre enn samsvar med krav.

Figur 5: Samsvarsoversikt i henhold til forordning 300/2008

De ulike KPIene er delt inn i kapitler, og inkluderer blant annet: screening av passasjerer og håndbagasje for å stoppe forbudte gjenstander, som våpen og eksplosiver, kontroll av den innsjekkede bagasjen, sikring av flyplassområdet (f.eks. kontroll av tilgang til sikkerhetsbegrensede områder på flyplasser, screening av personell og kontroll av kjøretøy, overvåking og patruljering for å forhindre at uvedkommende kommer inn i disse områdene), beskyttelse av fly og søk før avreise for å sikre at ingen forbudte gjenstander er om bord; kontroll av last og post før de lastes på fly; kontroll av flyplassforsyninger (dvs. varer som selges i butikker og restauranter på flyplassen) og forsyninger under flyging (f.eks. mat og drikke til passasjerer); rekruttering og opplæring av ansatte; sikkerhetsutstyrets ytelse (dvs. utstyr som brukes til screening og tilgangskontroll oppfyller definerte spesifikasjoner og er i stand til å utføre de aktuelle sikkerhetskontrollene).

Alle punktene i forordning 300/2008 er offentlig tilgjengelig, og ligger vedlagt i appendiks med mine oversettelser.

5.1.1 Avgrensning av datamaterialet

Datamaterialet som Avinor anvender som styringsindikator, og som inneholder alle resultatene fra Luftfartstilsynets inspeksjoner, er klassifiserte data. Det har derfor vært behov for å foreta en rekke avgrensinger, for ikke å avsløre sensitiv informasjon.

Jeg har gruppert inn Avinors lufthavner i kategoriene A, B og C, etter størrelse på lufthavnene. Bakgrunnen for dette er at informasjon fra datamaterialet ikke skal kunne spores tilbake til spesifikke lufthavner, da slik informasjon kan misbrukes. Kategori A består av landets åtte største lufthavner, kategori B består av 15 mellomstore lufthavner mens kategori C består av de 19 minste lufthavnene. Lufthavnenes størrelse er blitt indikert på bakgrunn av to variabler: antall passasjerer og antall flybevegelser, i kalenderåret 2019. Flybevegelser gjelder all flygning, herunder rute, charter, frakt, ambulanseflyging, skoleflyging etc. 2019 var et normalår for luftfarten, og tallene er derfor valide for å kunne avgjøre lufthavnenes størrelse. En gruppering av lufthavnene vil i tillegg føre til en systematikk, og likheter og ulikheter mellom lufthavnkategoriene kan avdekkes.

Tabell 1: Antall passasjerer i kalenderåret 2019 (Avinor, 2021)

	<i>Kategori A</i>	<i>Kategori B</i>	<i>Kategori C</i>	Total
Gjennomsnitt	6 280 669	231 279	40 106	1 246 398
Median	3 340 144	148 787	28 154	103 189

Tabell 2: Antall flybevegelser i kalenderåret 2019 (Avinor, 2021)

	<i>Kategori A</i>	<i>Kategori B</i>	<i>Kategori C</i>	Total
Gjennomsnitt	75 461	7872	2681	17 897
Median	50 303	7245	2442	5841

Lufthavnkategori A

I lufthavnkategori A finner vi landets åtte største lufthavner: *Oslo, Bergen, Trondheim, Stavanger, Kristiansand, Bodø, Tromsø og Ålesund.*

Oslo Lufthavn Gardermoen skiller seg klart ut i forhold til de andre lufthavnene med tanke på størrelse. I 2019 var det *28 592 619 passasjerer* som benyttet seg av Gardermoen, mens det var *254 659 flybevegelser* til og fra flyplassen. Til sammenligning er Kjevik Lufthavn i Kristiansand den minste lufthavnen i denne kategorien, med *1 064 387 passasjerer* og *20 113 flybevegelser* i 2019.

Lufthavnkategori B

I lufthavnkategori B finner vi landets mellomstore lufthavner: *Alta, Brønnøysund, Florø, Førde, Hammerfest, Harstad/Narvik, Kirkenes, Kristiansund, Leknes, Mo i Rana, Molde, Stokmarknes, Svalbard, Vadsø og Ørsta Volda.*

Den største lufthavnen i denne kategorien er Harstad/Narvik med *767 812 passasjerer*, og *11 625 flybevegelser* i 2019. Den minste lufthavnen er Førde med *83 306 passasjerer* og *6380 flybevegelser*.

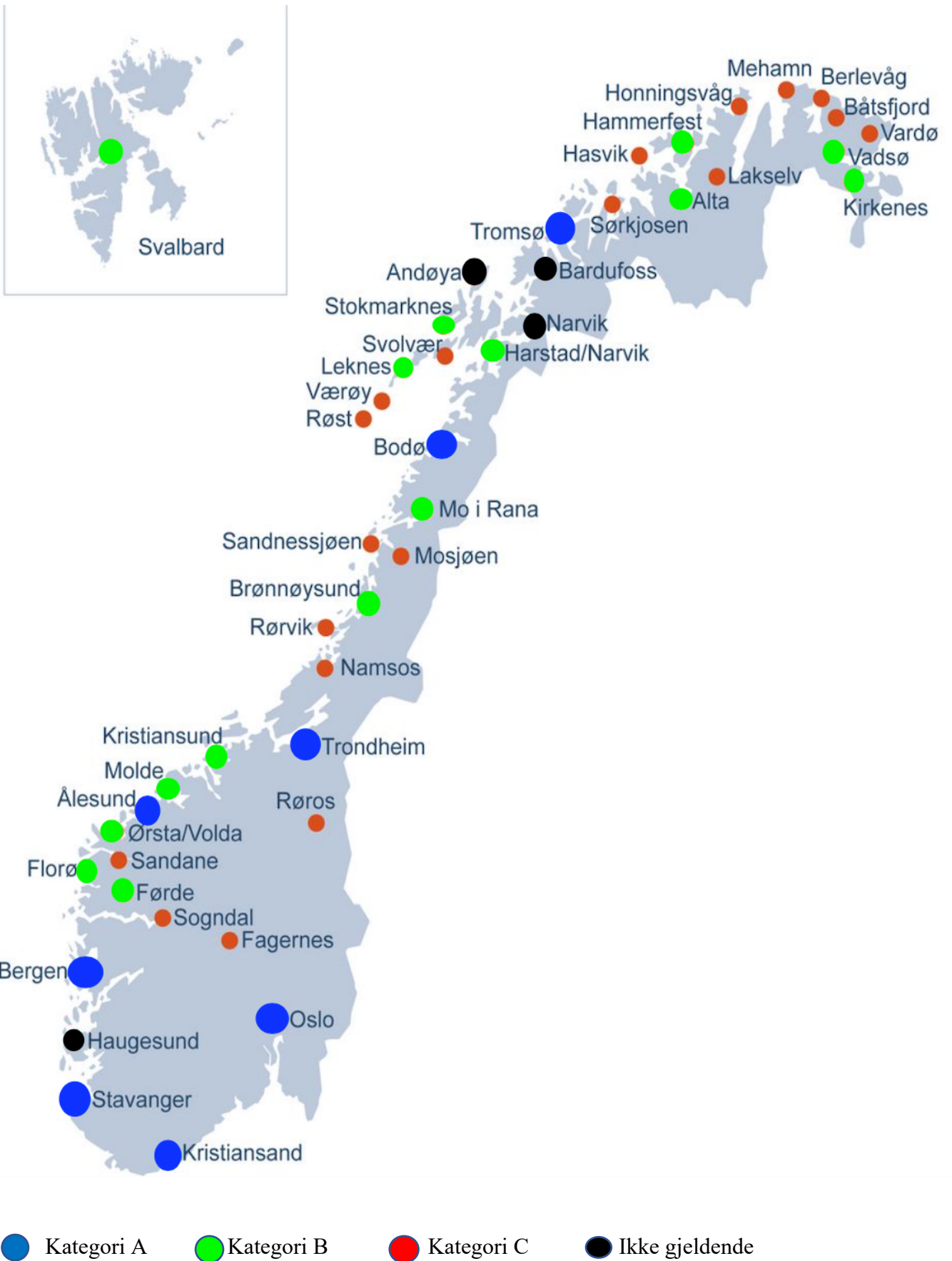
Lufthavnkategori C

De fleste lufthavnene i kategori C er del av det såkalte kortbanenettet på Nord-Vest landet og i Nord-Norge: *Berlevåg, Båtsfjord, Fagernes, Hasvik, Honningsvåg, Lakselv, Mehamn, Mosjøen, Namsos, Røros, Rørvik, Røst, Sandane, Sandnessjøen, Sogndal, Svolvær, Sørkjosen, Vardø og Værøy.*

Svolvær lufthavn hadde mest trafikk i 2019, med *94 498 passasjerer* og *4603 flybevegelser*. Værøy lufthavn hadde minst trafikk, med *8372 passasjerer* og *1216 flybevegelser*.

Lufthavner som ikke er gjelde for analysen

På kartet under vises et kart over alle Avinors lufthavner, inndelt i kategoriene A, B og C. *Haugesund, Bardufoss, Andøya og Narvik* er markert som ikke gjeldene for analysen. Avinor er ikke lufthavnoperatør ved disse lufthavnene i dag, og det er derfor mangelfulle data.

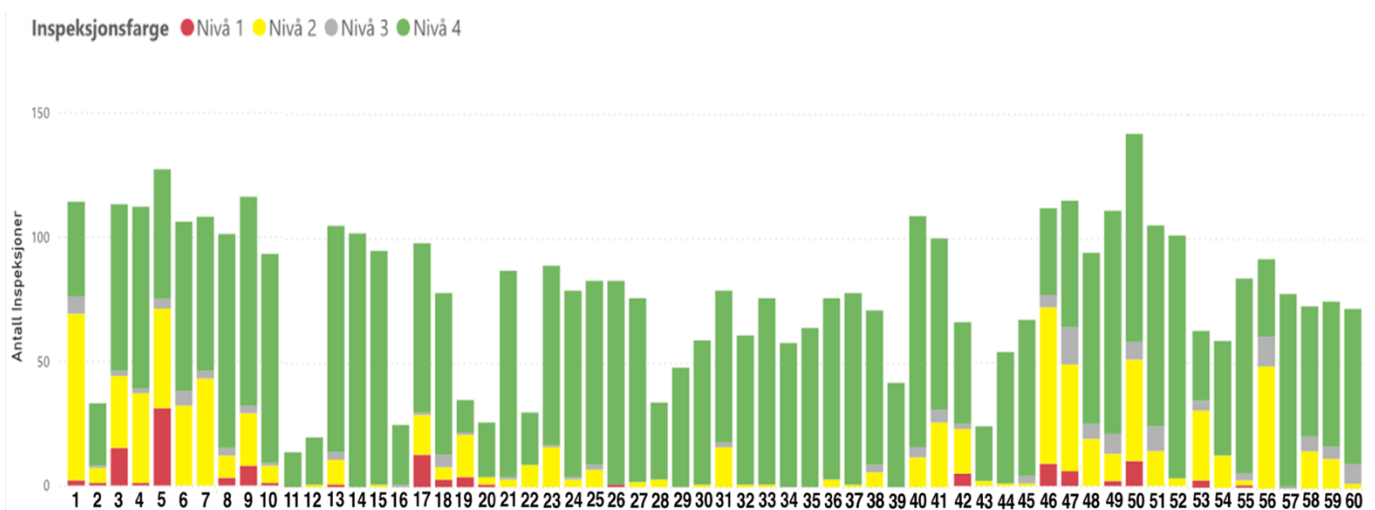


Figur 6: Kart over Avinors lufthavner

Spesifikk informasjon om KPIene i regelverket vil også bli behandlet konfidensielt. Figuren som fremstilles under illustrerer ett av verktøyene som Avinor bruker for å overvåke sikkerhetsnivået på deres lufthavner. Det er et sammenstillings diagram, som viser sikkerhetsnivået på de ulike KPIene og lufthavnene, gjennom søyler. For å fremstille det samme diagrammet med varsomhet, er punktenes identifikasjon/navn blitt tatt bort, for ikke å avsløre detaljerte sårbarheter knyttet til dem. I tillegg er målepunktene søyler blitt plassert i en tilfeldig rekkefølge i figuren, for å sikre at KPIene ikke kan avsløres på bakgrunn av kapitellinndelingen i forordning 300/2008. Hver enkelt søyle har blitt markert med et tall, for å kunne henviser til dem og foreta sammenlikninger. Tallene har ingen sammenheng med KPIene eller kapitellinndelingen i forordning 300/2008.

Figuren viser statistikken for samtlige inspeksjoner foretatt av Luftfartstilsynet på Avinors lufthavner, i tidsrommet 01.01.2015 til 01.03.2020. Datamaterialet fra perioden etter mars 2020 er mangelfullt, da flytrafikken ble kraftig redusert som følge av Covid-19. Samtidig vil nylig avdekkede avvik kunne være under behandling, og slik informasjon er derfor sårbar. Datamaterialet før 2015 er også mangelfullt, og blir derfor ikke involvert i analysen. Figuren viser til resultatene på 60 KPIer. For lufthavnene i kategori A, har Luftfartstilsynet inspisert 69 av de totalt 73 KPIene i forordningen. For lufthavnene i kategori B og C har Luftfartstilsynet kontrollert 60 KPIer. For å kunne sammenlikne sikkerhetsnivået på KPIene mellom de ulike lufthavnene, vil analysen derfor studere de 60 KPIene. KPIene er listet opp i samme rekkefølge i de ulike figurene for lufthavnkategoriene, slik at sammenlikninger kan foretas.

5.1.2 Samlet statistikk for alle lufthavner i Avinor



Figur 7: Samlet statistikk for Avinor 01.01.2015-01.03.2020

Figuren illustrerer hvordan Avinor anvender resultatene på KPIene i deres risikostyring. I etterkant av hvert tilsyn legger Avinor inn resultatene i analyseprogrammet, og kan studere sikkerhetsnivået og utviklingen på hver KPI og hver lufthavn. Det er primært på dette grunnlaget at Avinor definerer sikkerhetsnivået, og det er direkte måling opp imot EU-regelverket. Den røde søylen viser til alvorlige avvik (1), den gule til avvik (2), den grå til samsvar med krav, men med kommentar om ønsket forbedring (3), og den grønne til samsvar med krav (4). Avinor har ikke fått karakter 5 på noen av inspeksjonene i det aktuelle tidsrommet.

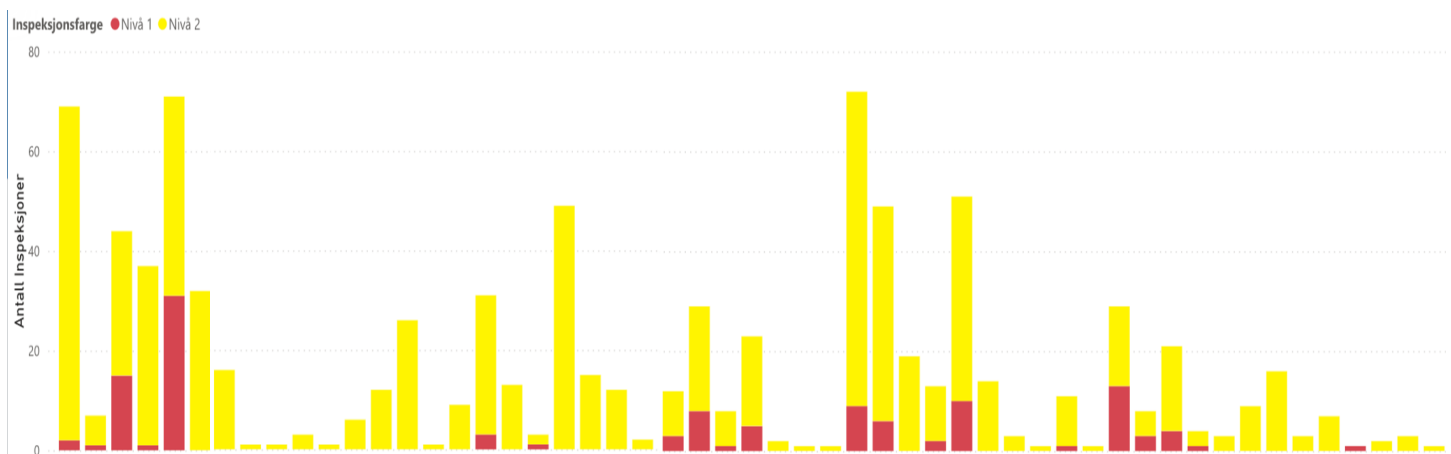
Figuren viser at det er blitt foretatt i gjennomsnitt 100 inspeksjoner av de ulike KPIene. De fleste punktene er blitt inspisert omtrent likt antall ganger, mens inspeksjon av enkelte punkter har nærmest vært fraværende. Dette gjenspeiles også gjennom å studere tilsynsrapportene, som viser at det ofte er de samme punktene som blir kontrollert under inspeksjonene. Dette viser at Luftfartstilsynet anser enkelte punkter i forordningen for å være mer kritiske enn andre. Figuren viser at det er de grønne søylene som dominerer, til tross for at det også er blitt avdekket en relativt stor andel avvik. Figuren viser en klar sammenheng mellom punktene som er blitt kontrollert flest ganger, og høye avvikstall. Sannsynligheten for å avdekke avvik vil økes proporsjonalt med antall inspeksjoner, men Luftfartstilsynet vil også ha et større fokus på å inspisere de punktene hvor det tidligere er blitt avdekket avvik. De mest kritiske avvikene er dem som fremstilles i form av den røde søylen, som er avvik som anses som truende for flysikkerheten. Punkt 5 i figuren viser at alvorlige avvik utgjør omtrent 20-25% av det totale antallet inspeksjoner i perioden 2015-2020. Punkt 5 er blitt inspisert nest flest ganger, som viser at tilsynet har stort fokus på punktet. Etter at alvorlige avvik er blitt avdekket, stiller Luftfartstilsynet strenge krav om at tiltak må iverksettes for å utbedre avviket. En antakelse er derfor at punktene med høye avvikstall har hatt en nedgang i andelen avvik i denne perioden. Utviklingen i avviksnivået på punkt 5 viser imidlertid at en slik antakelse ikke stemmer.

01.01.2015 til 01.03.2020=	24% alvorlige avvik
01.01.2016 til 01.03.2020=	20% alvorlige avvik
01.01.2017 til 01.03.2020=	19% alvorlige avvik
01.01.2018 til 01.03.2020=	18% alvorlige avvik
01.01.2019 til 01.03.2020=	24% alvorlige avvik
Utvikling:	0%

Statistikken hadde en positiv utvikling mellom 2015 og 2019, før kurven igjen fikk en negativ utvikling mellom 2019 og 2020.

Et annet interessant funn fra figur 7 er at inspektørene fra Luftfartstilsynet i svært liten grad anvender karakter 3. Karakter 3 innebærer at tilsynet fremlegger anbefalinger om tiltak som bør iverksettes, og at det i stor grad er opp til Avinor å bestemme hvorvidt anbefalingen skal følges eller ikke. Inspektørene kan derfor ha mindre terskel for å gi karakter 2 fremfor 3, for å sikre at Avinor pålegges å iverksette nødvendige tiltak og utbedringer innen en gitt tidsfrist. Det er en effektiv måte for Luftfartstilsynet å påse at tiltak blir iverksatt, men det fører til mindre grad av selvbestemmelse og desentraliserte beslutninger i Avinor.

Informant 1 Avinor uttrykte det som positivt for sikkerhetsarbeidet og sikkerhetskulturen i Avinor, da EU i 2014 besluttet at tilsynsmyndighetene skulle informere om alle punktene som ble inspisert under tilsynene, også dem hvor det var samsvar med kravene. Før 2014 informerte Luftfartstilsynet kun om de punktene hvor det ble avdekket avvik. Den samme figuren som er presentert ovenfor, ville derfor sett slik ut før 2014:



Figur 8: Fremstilling av avvik

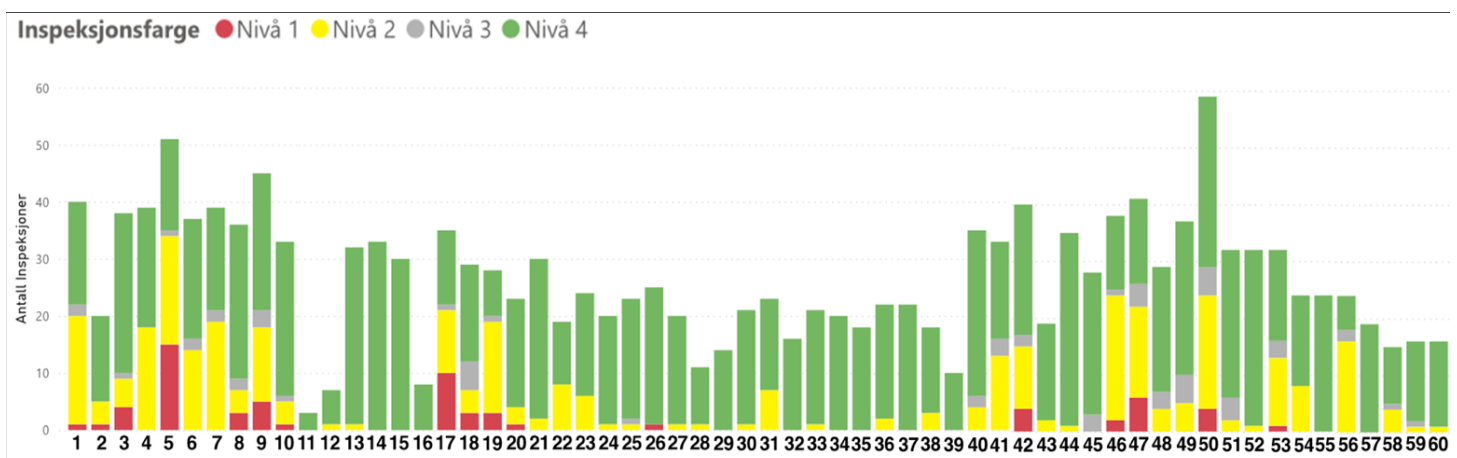
En slik fremstilling av statistikken er ufullstendig å benytte i risikostyringen, da den ikke gir noe kunnskap eller indikasjon på den totale sikkerhetssituasjonen i organisasjonen. På søylene med høye avvikstakk, kan avvikene likevel bare utgjøre en liten andel av det totale inspeksjonsantallet. Uten kunnskap om det totale sikkerhetsbildet, var det utfordrende for Avinor å ha kunnskap om hvilke områder sikkerhetssituasjonen var mest kritisk.

Beslutningsgrunnlaget var derfor mangelfullt når tiltak skulle iverksettes. Samtidig er det primært på bakgrunn av avvikrappoteringer at Avinor og Luftfartstilsynet kan gå direkte inn

for å tette hull i sikkerhetssystemet og dermed styrke sikkerheten. De grønne søylene har derfor mindre betydning sammenliknet med avvikssøylene, men en totaloversikt over sikkerhetssituasjonen vil likevel føre til et mer pålitelig security-arbeid.

I det følgende vil jeg fremstille statistikken for hver lufthavnkategori, med den hensikt å studere forskjeller mellom antallet inspeksjoner og avviksnivå. Figurene inneholder de samme KPIene som i figur 7, i den samme rekkefølgen slik at punktene kan sammenliknes. Figurene viser til alle inspeksjoner foretatt i tidsrommet 01.01.2015 til 01.03.2020.

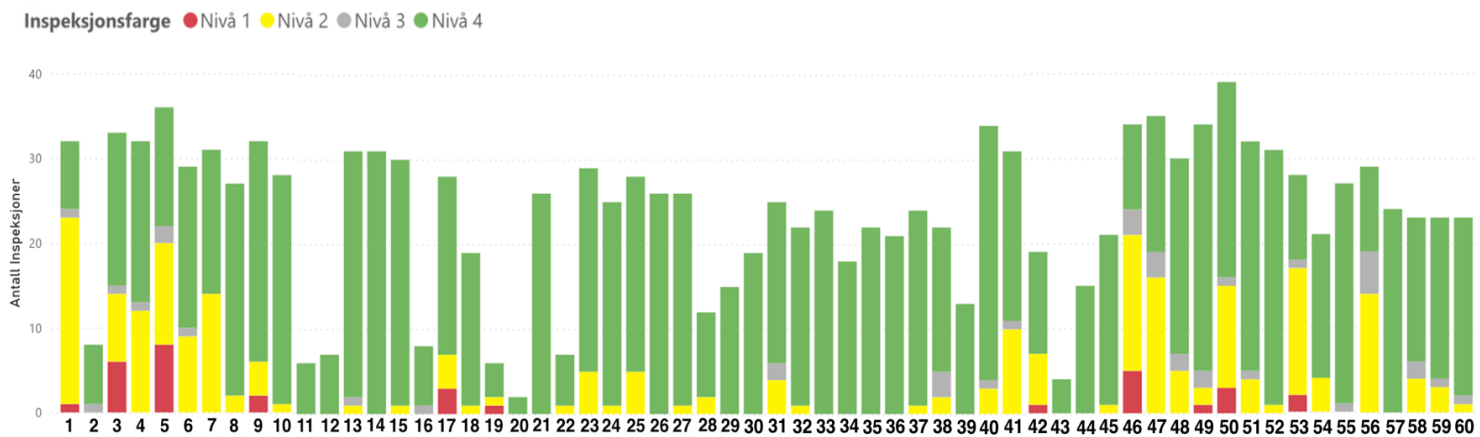
Lufthavnkategori A



Figur 9: Statistikk for lufthavnkategori A

Figuren viser til flere likheter med figur 7. Det er i gjennomsnitt blitt foretatt mellom 30 og 40 inspeksjoner på KPIene ved de største lufthavnene. Figuren viser at det er blitt avdekket en relativt høy andel avvik under inspeksjonene. Andelen alvorlige avvik og avvik er betydelig høyt på punkt 5 for de største lufthavnene, og avvik utgjør omtrent to tredjedeler av alle inspeksjonene som er blitt foretatt.

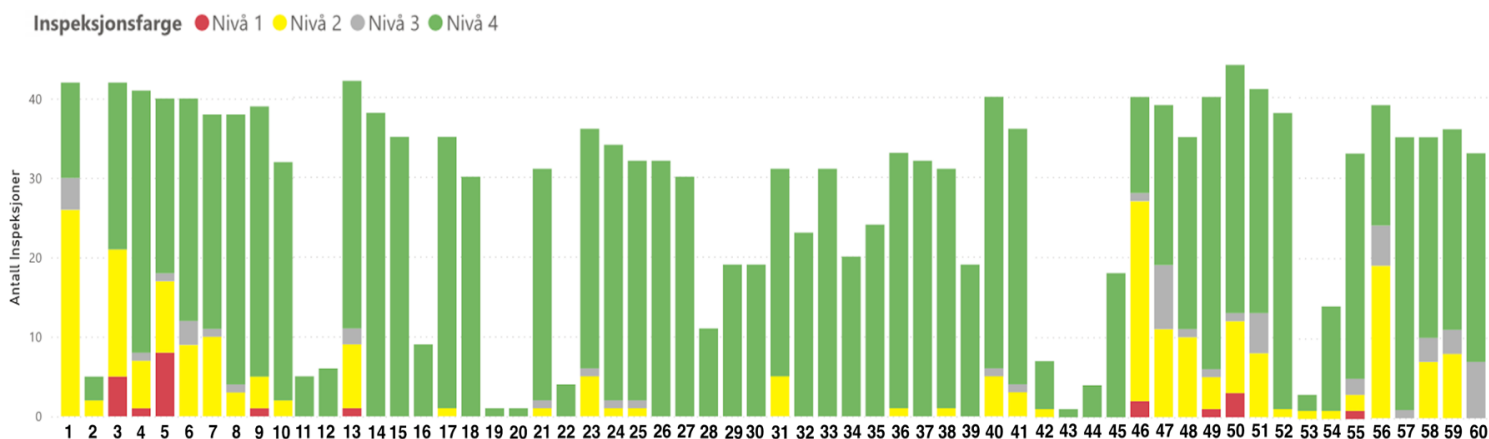
Lufthavnskategori B



Figur 10: Statistikk for lufthavnskategori B

Figuren for de mellomstore lufthavnene viser at Luftfartstilsynet har gjennomført omtrent 30 inspeksjoner av de fleste punktene. De fleste inspeksjonene har avdekket samsvar med kravene, men figuren viser samtidig at det foreligger en høy andel avvik på enkelte KPIer. Punkt 5 har også flest avvik på de mellomstore lufthavnene. Til tross for at lufthavnskategori B består av dobbelt så mange lufthavner som kategori A, er det likevel blitt gjennomført færre inspeksjoner. Det viser at Luftfartstilsynet har et større fokus på å inspisere de største lufthavnene.

Kategori C



Figur 11: Statistikk for lufthavnskategori C

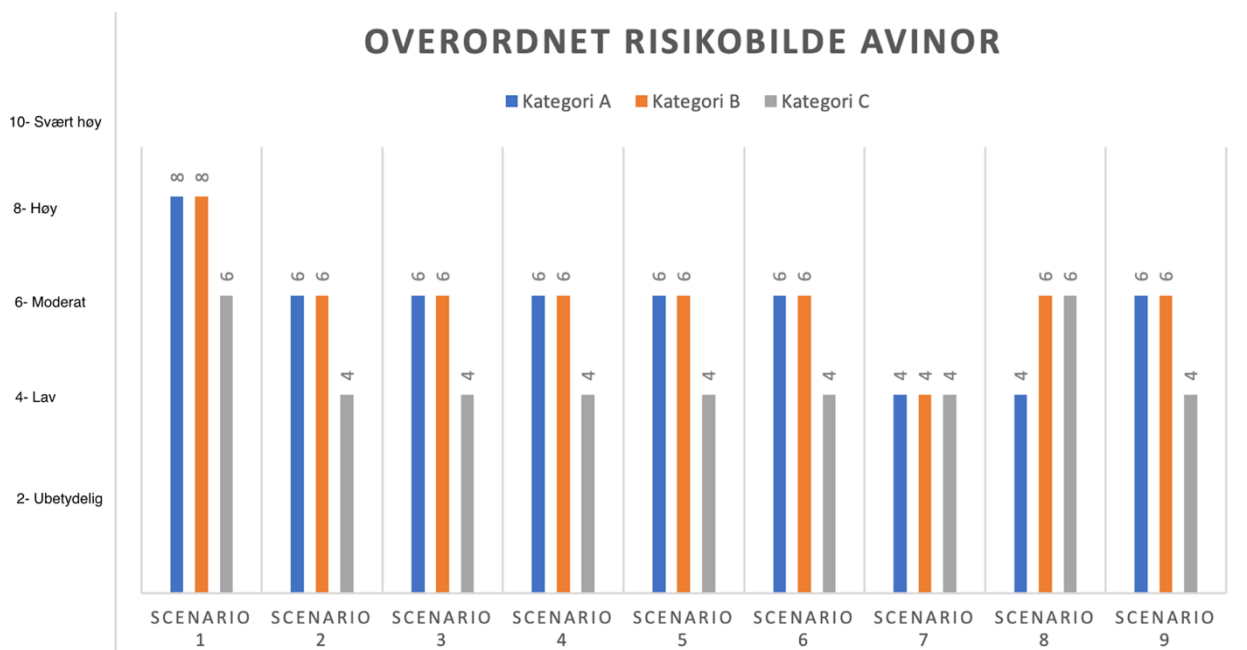
For lufthavnene i kategori C, viser figuren at andelen avvik er betydelig lavere sammenliknet med kategori A og B. Gjennomsnittet for antall inspeksjoner på KPIene er omtrent 30 inspeksjoner. Figuren viser at det er blitt avdekket noen alvorlige avvik på punkt 5, men langt

færre sammenliknet med de andre lufthavnene. Til tross for at denne kategorien består av 19 lufthavner, er det blitt gjennomført færre inspeksjoner sammenliknet med kategori A som består av åtte lufthavner. Det viser at de små lufthavnene i Norge har sjeldnere besøk av Luftfartstilsynets inspektører.

Formålet med å fremstille figurene har vært å illustrere hvordan Avinor anvender resultatene fra inspeksjonene for å overvåke sikkerhetsnivået. Denne studien har imidlertid som hensikt i å belyse påliteligheten ved å definere sikkerheten på dette grunnlaget.

5.1.3 Overordnet risikobilde Avinor

Avinor har utarbeidet et internt risikobilde med bakteppe i scenarioer som Avinor har funnet relevante i forhold til dagens trusselbilde for tilskitete handlinger, og den aktiviteten Avinor bedriver. Risikobilde baserer seg på en overordnet verdi, trussel og sårbarhetsvurdering for Avinor. Risikobilde gjennomgås årlig og ved behov, eller når hendelser eller nye trusselvurderinger fører til endringer i trusselbilde. Rapporten inneholder 9 scenarioer hvor søylene indikerer hvor stor risiko det enkelte scenario utgjør for den enkelte lufthavnkategori. Lufthavnkategoriene er tilsvarende de kategoriene som er presentert ovenfor.



Figur 12: Overordnet risikobilde Avinor

Scenario 1: Håndvåpenangrep i terminal

Scenario 2: Eksplosiver på landside i terminal

Scenario 3: Terroranslag med bruk av kjøretøy (terminal)

Scenario 4: Eksplosiver i kjøretøy utenfor terminal

Scenario 5: Eksplosiver i varemottak

Scenario 6: Sabotasje mot tårn og sikringsbygg

Scenario 7: Sabotasje mot IKT og el-forsyning

Scenario 8: Sabotasje mot adgangskontrollsystem (terminal)

Scenario 9: Innføring av gjenstander til CP fra landside

Risikobilde viser at Avinor anser risikoen for å være generelt høyere ved lufthavnene i kategori A og B, sammenliknet med lufthavnene i kategori C. På scenario 7 anses derimot risikoen som lav ved alle lufthavnene. På scenario 8 anses risikoen som moderat ved kategori B og C, mens den anses som lav ved kategori A. Det eneste scenarioet hvor risikoen anses som høy, er på scenario 1 som omhandler håndvåpenangrep i terminal. Slike typer angrep har funnet sted ved flere lufthavner rundt om i Europa de senere årene. Risikoen på de resterende scenarioene anses som moderat, som betyr at det er like sannsynlig som usannsynlig at et angrep finner sted.

5.2 Dokumentanalyse av Luftfartstilsynets tilsynsrapporter

I det følgende vil funn fra dokumentanalysene bli presentert, hvor et utvalg av tilsynsrapportene har lagt grunnlaget for analysen. I perioden 01.01.2015 til 01.03.2020 foretok Luftfartstilsynet totalt 171 inspeksjoner av Avinors lufthavner. 82 av inspeksjonene var på landets åtte største lufthavner (kategori A), 43 på landets mellomstore lufthavner (kategori B) mens 46 var på landets minste lufthavner (kategori C). Dette viser at inspeksjonshyppigheten øker etter lufthavnens størrelse. Risikobildet er et annet ved de større lufthavnene, grunnet internasjonale flyforbindelser og en generell større symbolsk betydning (Tønnessen, 2008).

Tilsynsrapportene fra Luftfartstilsynet innledes med en kort beskrivelse av formålet med tilsynet. Her beskriver Luftfartstilsynet at de «gjennomfører virksomhetstilsyn i henhold til forskrift om sikkerheten i luftfarten mv. (BSL Sec 1-1) med tilhørende forordninger og bestemmelser». Inspeksjonen har som formål å verifisere at virksomhetens operasjoner er i samsvar med et utvalg av myndighetskrav. Rapporten beskriver Luftfartstilsynets vurdering med hensyn til grad av samsvar med regelverket. Gradering av samsvar er i henhold til EUs klassifisering- ref (EU) 18/2010 vedlegg 2.

I tilsynsrapportene blir eventuelle funn av avvik listet opp, med tilhørende beskrivelser om bakgrunnen for avviket samt krav om iverksettelse av tiltak for å lukke avviket. Punktene med samsvarsnivå 3 (samsvar med krav, med kommentar om ønsket forbedring) blir også beskrevet i rapportene med en anbefaling om ønsket forbedring. Punktene som samsvarer med kravene (nivå 4 eller 5) beskrives ikke ytterligere og er kun til informasjon.

I beskrivelsen informerer Luftfartstilsynet om hvilke KPIer som ble inspisert, hvilken inspeksjonsmetode som ble anvendt, klokkeslett og dato for inspeksjonen samt funn og årsaker som førte til avvik eller anbefaling om forbedring. Beskrivelsen er grundig og detaljert, med den hensikt at lufthavnoperatøren skal få god nok kunnskap til å kunne iverksette treffende tiltak for å lukke avviket og operere i tråd med regelverket. I beskrivelsen informerer Luftfartstilsynet også om hvilke tiltak som må eller bør iverksettes, og det settes en frist for når tiltakene må være implementert. Luftfartstilsynet fortar ofte nye inspeksjoner på et senere tidspunkt, for å kontrollere at tiltaket er på plass og at det har ønsket effekt. Det legges også et ansvar om kvalitetskontroll på Avinor. Virksomheten skal følge opp de korrigerende tiltakene, samt sikre at tiltakene har hatt ønsket effekt. Virksomheten skal sende en beskrivelse av de korrigerende tiltakene, samt resultatene av den interne kvalitetsoppfølgingen, til Luftfartstilsynet. Det settes en frist på når dette skal være innsendt.

Informant 2 Avinor påpeker at det er vanlig med et møte med inspektørene i etterkant av inspeksjonene, slik at ulike funn og problemstillinger kan diskuteres og inspektørene kan gi mer grundige forklaringer. Informanten gav uttrykk for at tilsynsrapportene isolert sett kan være vanskelige å forholde seg til, og at et møte med inspektørene er svært formålstjenlig. Inspektørene fra security seksjonen i Luftfartstilsynet er ifølge *informant Luftfartstilsynet* de fremste ekspertene på området, og behovet for en pedagogisk fremleggelse av funn og tiltak er derfor essensielt for at deres funn skal ha en reell virkning på sikkerheten.

Tilsynsrapportene avsluttes med en tabell/oversikt over alle observasjoner som ble gjort under inspeksjonen, med tilhørende klassifisering (1-5). Gjennom en slik oversikt får Avinor kunnskap om samtlige punkter som ble inspisert. I tabellen under vises et eksempel på en slik oversiktstabell, hentet fra en tilsynsrapport av en norsk lufthavn.

Implementing Rule	Title	NA	NR	Finding Level				
				1	2	3	4	5
Security 1.2.1	Innpassering til flyside						x	
Security 1.2.2	Innpassering til sikkerhetsbegrenset område SRA/CSRA						x	
Security 1.3.1	Gjennom søkning av andre personer enn passasjerer og av gjenstander de bringer med seg						x	
Security 1.4.1	Sikkerhetskontroll av kjøretøy - CSRA				x			
Security 1.5	Overvåking, patruljering og andre former for fysisk kontroll						x	
Security 4.1.1	Gjennom søkning av passasjerer				x			
Security 4.1.2	Gjennom søkning av håndbagasje						x	
Security 4.1.3	Sikkerhetskontroll av LAGs						x	
Security 5.1	Gjennom søking av innsjekket bagasje						x	
Security 9.1.1	Sikkerhetskontroll av forsyninger til lufthavnen – generelle bestemmelser			x				
Security 9.1.2	Gjennom søkning						x	
Security 11.3	Sertifisering eller godkjenning		x					
Security 12.0	Generelle bestemmelser						x	

Tabell 3: Oversiktstabell fra tilsynsrapport

Tabellen viser at den aktuelle inspeksjonen avdekket ett alvorlig avvik (1), og to avvik (2). Resten av punktene som ble inspisert, samsvarte med kravene og ble derfor ikke beskrevet ytterligere i tilsynsrapporten.

5.2.1 Inspeksjonsmetoder

Inspektørene fra Luftfartstilsynet anvender ulike inspeksjonsmetoder for å kontrollere at aktørene i luftfarten opererer innenfor kravene i security-regelverket. I tillegg til fysiske inspeksjoner på lufthavnene foretar Luftfartstilsynet revisjoner av Avinor, med en totalgjennomgang av all dokumentasjon. Under inspeksjonene blir metodene *observasjon*, *testing* og *intervju* brukt.

Observasjon foregår ved at inspektørene står og observerer at aktørene på lufthavnene utfører sitt arbeid i henhold til kravene, for eksempel at sikkerhetskrollørene er fokuserte og utfører sitt arbeid i tråd med reglene. Observasjon av at ulike tiltak og løsninger på lufthavnen er i tråd med reglene er også en sentral del av tilsynsaktiviteten. Det er i stor grad opp til hver enkelt lufthavnoperatør å bestemme hvilke løsninger som skal være gjeldende for at kravene i regelverket skal være oppfylt, for eksempel hvordan overvåkningssystemet av det sikkerhetsbegrensede område skal innrettes. Lufthavnoperatørene bestemmer hvordan overvåkingen skal skje, hvor mange kamera som skal brukes etc. Tiltak og løsninger kan derfor variere mellom lufthavnene, men alle krav i regelverket skal være oppfylt uavhengig av hvilke løsninger som anvendes. Luftfartstilsynets observasjoner er derfor viktige for å kontrollere hvorvidt tiltakene er innenfor rammene til regelverket.

Et eksempel fra en tilsynsrapport hvor inspektørene benyttet seg av observasjon som inspeksjonsmetode, er følgende:

Punkt 1.1.1 (Grenser)

Vest for tårnet var lufthavngjerdet som skiller flyside fra landside ikke egnet til å hindre uautorisert innpassering på grunn av en (1) helt usikret åpning under. Ellers langs gjerdet var en del utbedringer i underkant av gjerdet iverksatt, men steinene plassert under gjerdet vil på flere steder være enkle å fjerne fra yttersiden.

Under denne inspeksjonen har inspektørene tatt en fysisk runde rundt hele lufthavnen, for å observere om gjerdet er robust nok til å hindre uautorisert tilgang til lufthavnen. Inspeksjonsmetoden er effektiv og enkel å utføre. Inspektørene går aktivt inn for å finne hull i barrierene, og dersom hull identifiseres får Avinor tilbakemelding om funnet og eventuelle tiltak blir iverksatt. I dette tilfellet ble avviket utbedret umiddelbart.

Et ytterligere eksempel på observasjon som metode, er følgende:

Punkt 1.1.3 (CP-områder)

Luftfartstilsynets inspektør observerte oppgradering av kritisk del av sikkerhetsbegrenset område (CP) utendørs. Oppgraderingen var ikke i henhold til regelverkskrav, da følgende områder ikke ble gjennomført: innhold i sandkasse, presenning, et hull i bakken ved fuel-skap og el-skap, kasse bak fuel-skap, grøft til kanal og avløpsrenne. Luftfartstilsynets inspektør anså oppgraderingen for å ikke være gjennomført i henhold til regelverkskravene og ga et pålegg om øyeblikkelig korrigerende tiltak. Vedtaket ble først viderefremmet muntlig, og ettersendt til fagansvarlig for security skriftlig.

Luftfartstilsynets inspektør ble pålagt å korrigere avvikene innen 24 timer fra vedtak om umiddelbar korrigerende tiltak ble mottatt på e-post. Beskrivelse av kompensierende tiltak ble mottatt av Luftfartstilsynet 1 døgn senere. Tilsvar ble akseptert av Luftfartstilsynet samme dag.

Kritisk del av sikkerhetsbegrenset område (CP- Critical point) skal etableres på hver flyplass i den tiden det er aktivitet der. Før et område kan oppgraderes til CP, må det utføres et grundig sikkerhetssøk for å kontrollere at det ikke finnes forbudte gjenstander i området. Flyplasser med begrenset trafikk kan bruke fleksibel-CP, som betyr at CP-område kun etableres når fly ankommer flyplassen. I avviket som er beskrevet over, ble sikkerhetssøket ikke utført i henhold til kravene. Avviket ble korrigert umiddelbart.

Testing er en annen inspeksjonsmetode som brukes av inspektørene fra Luftfartstilsynet. Testing skjer ved at inspektørene fysisk tester de ulike sikkerhetssystemene, for eksempel ved at de bringer med seg ulovlige gjenstander i håndbagasjen og tester om screening maskinen og de ansatte oppdager gjenstanden eller ikke.

To eksempler hvor testing ble brukt som inspeksjonsmetode, er følgende:

Punkt 1.2.2 (Tilgang til CP)

Det ble gjennomført en test av innpassering til sikkerhetsbegrenset område i sikkerhetskontrollpunkt for ansatte i terminalbygg venstre løp ved at security-inspektører benyttet Avinors ID-kort. Testen viste at det ikke var mulig å innpassere uten bruk av gyldig ID-kort og pin-kode. Test bestått.

Punkt 1.3.1 (Sikkerhetskontroll av andre enn passasjerer)

Inspektører fra Luftfartstilsynet gjennomførte tre (3) tester med testobjekt (IED) plassert i sekk. Testene ble gjennomført i sikkerhetskontrollpunkt for ansatte i terminalbygg. Test bestått.

Testing som metode er effektiv og gir et klart svar på hvorvidt sikkerhetssystemene og de ansatte er operative og årvåkne.

Intervju som inspeksjonsmetode vil også gi et klart svar på om de ansatte har nok kunnskap om kravene i regelverket. Tilsynsrapportene viser at lufthavnsjefen blir intervjuet ved de fleste inspeksjoner, men øvrige ansatte på lufthavnen kan også bli utsatt for intervju. Kombinasjon av inspeksjonsmetoder blir også brukt under tilsynene. Dersom en test viser at ansatte avviker fra kravene, kan inspektørene følge opp med et intervju for å avdekke hvorvidt avviket kom som følge av en feil eller som følge av manglende kompetanse eller motivasjon.

5.2.2 Menneskelige feil og avvik

Funn fra dokumentanalysene har vist at det stadig avdekkes avvik på bakgrunn av ansattes manglende kompetanse knyttet til kravene og prosedyrene i regelverket. Funn har også vist at dette kan være gjeldene for lufthavnsjefer. Et sentralt kjennetegn på organisasjoner som opererer deres systemer med høy pålitelighet, er at de ansatte har høy kompetanse og ferdigheter knyttet til systemene og prosedyrene som opereres. Det er lufthavnoperatøren sitt ansvar å ansette egnede personer som kan utføre security-arbeidet på en pålitelig måte, samt å sørge for god opplæring og oppfølging. Funn fra dokumentanalysene har også vist at ansatte har valgt å trosse prosedyrene bevisst. Under fremstilles tre eksempler på ansattes manglende kompetanse eller bevissthet i forbindelse med kravene i regelverket:

Punkt 9.1.1 (Sikkerhetskontroll av forsyninger til lufthavnen)

Intervju med ansatte i vaktelskapet som betjente overgangspunkter mellom landside og sikkerhetsbegrenset område (CP) avdekket at flere typer forsyninger til lufthavnen ikke ble gjenstand for sikkerhetskontroll ved innpassering.

Punkt 1.6 (Forbudte gjenstander)

Gjennom intervju fremkom det at en sikkerhetskontrollør var noe usikker angående forskjell på forbudte gjenstander.

Punkt 1.3.1 (Sikkerhetskontroll av andre enn passasjerer)

Inspeksjonsteamet observerte at 3 sikkerhetskontrollører med noen minutters mellomrom gikk fra landside og inn på CP via dør inn til bagasjehall ankomst innland uten at de ble sikkerhetskontrollert. Intervju med ansatte sikkerhetskontrollører avdekket at dette ble gjort regelmessig. Det fremkom gjennom intervju at personene skulle bistå i bagasjehall og at det var en omvei å gå via etablert sikkerhetskontroll.

Funnene viser at ansatte i disse tilfellene har manglet tilstrekkelig kunnskap, at de har gjort feil eller valgt å trosse prosedyrene bevisst. Ansatte kan velge å trosse prosedyrene for å spare tid, eller fordi de anser det som krevende og belastende å til enhver tid operere innenfor kravene. Luftfartstilsynet og Avinor har en kritisk rolle i å avdekke slike avvik.

Gjennomgangen av tilsynsrapportene har vist at tilsynsvirksomheten har en kritisk funksjon i security-arbeidet i norsk luftfart. Tilsynene avdekker både på menneskelige, tekniske og organisatoriske avvik og svakheter. Luftfartstilsynet stiller krav om at alle avvik må utbedres, noe som direkte bidrar til å styrke «compliance» nivået. I bransjen er dette synonymt med at sikkerhetsnivået styrkes. Funn fra dokumentanalysene har vist at hyppigheten av inspeksjoner øker etter lufthavnenes størrelse. Ved de største lufthavnene er det en generell større pågang av passasjerer, bagasje, frakt etc. Det fører til at de ansatte har flere faktorer å forholde seg til. Det foreligger også mer teknologiske løsninger ved de største lufthavnene, som for eksempel tekniske overvåkningssystemer knyttet til CP området. Ved de minste lufthavnene foregår slik overvåkning i større grad gjennom fysisk overvåkning fra de ansatte. Likevel har rapportene ikke påvist noen åpenbare forskjeller i tilsynsaktiviteten mellom de ulike lufthavnkategoriene. Dokumentanalysene har heller ikke avdekket noen åpenbare forskjeller knyttet til geografisk lokasjon av lufthavnene. Lufthavner av samme størrelse har blitt inspisert omtrent likt antall ganger, og det er i stor grad de samme KPIene som inspiseres. Analysen har ikke avdekket at det har forekommet store endringer i utførelsen av inspeksjonene med årene. Rapportene viser imidlertid at det er blitt tatt i bruk flere teknologiske løsninger ved lufthavnene de senere årene.

5.3 Funn fra intervjuene

I dette underkapittelet vil funn fra intervjuene fremlegges. Underkapittelet er strukturert etter studiens forskningsspørsmål. Det vil først redegjøres for hva som karakteriserer security-regimet i luftfarten, hvilke roller og ansvarsområder informantenes virksomheter har og hvordan Avinor må innrette seg etter regelverket. Deretter vil styrkene og svakhetene med å definere sikkerheten på bakgrunn av KPIene redegjøres for. Til slutt vil det redegjøres for om security-regimet kan anses som risikobasert, fleksibelt og proaktivt i møte med terrortrusler.

5.3.1 Karakteristikk for security-regime, og konsekvenser for norsk luftfart

Informanten fra Luftfartstilsynet definerer security-regimet i luftfarten som et strengt reguleringsregime, og at et slikt reguleringsregime fører til et pålitelig og robust sikkerhetsnivå i norsk luftfart. Informanten sier at security-regimet er utformet på en slik måte at ansvarlige aktører regelmessig blir inspisert av en høyere myndighet. I 2005 startet EFTA Surveillance Authority (ESA) å føre tilsyn med at EU statene overholdt kravene i security-regelverket. Frem til 2021 har ESA gjennomført om lag 50 inspeksjoner/revisjoner av Norge. ESA inspiserer all dokumentasjon, metodene som Luftfartstilsynet anvender og sikrer at tilsynet utfører deres lovpålagte arbeidsoppgaver på en måte som samsvarer med EU kravene. *Informant SD* sier at Samferdselsdepartementet har jevnlig møter med både Luftfartstilsynet og Avinor. I møtene med Luftfartstilsynet legger tilsynet frem en situasjonsrapport, hvor funn av avvik, bekymringer, hva tilsynet gjør for å håndtere situasjonen og eventuelle anmodninger om ressurser blir lagt frem. I departementets møter med Avinor videreformidler departementet bekymringene som ble lagt frem av Luftfartstilsynet. Luftfartstilsynet utfører på sin side jevnlig revisjoner og inspeksjoner av Avinor og andre aktører i luftfarten, for å sikre at EU-kravene etterlevs. *Informant I Avinor* sier at security-avdelingen i Avinor også foretar inspeksjoner av lufthavnene, og at avdelingen har det overordnede ansvaret for security internt i virksomheten. Informanten fra Luftfartstilsynet anser at kontroll- og tilsynsregime som råder i luftfarten er svært hensiktsmessig, da det alltid vil være en høyere myndighet som kontrollerer at arbeidet utføres i henhold til regler og prosedyrer. Det fører til at EU sitter med en totaloversikt over sikkerhetssituasjonen på hele kontinentet, og kan iverksette tiltak og beslutninger på et bredt og informativt beslutningsgrunnlag.

I en slik tilsyn og kontroll praksis, er det kritisk at de som utfører tilsyn har nok ekspertise, kompetanse og ressurser til å foreta hyppige og pålitelige tilsyn. Funn fra intervjuet med Luftfartstilsynet tilsier at Luftfartstilsynet har den nødvendige kompetansen og de nødvendige

ressursene for å sikre at Avinor trygt kan definere og evaluere sikkerheten på bakgrunn av deres inspeksjoner. Informanten påpeker likevel at Avinor også har et ansvar om internkontroll, hvor de skal kontrollere at de samsvarer med alle krav. Informanten trekker frem at inspektørene i Luftfartstilsynet har svært høy kompetanse, og at det stilles en rekke krav til kompetanse og autorisasjoner til alle inspektørene i tilsynet. Informanten påpeker at dersom Luftfartstilsynet hadde manglet ressurser, kompetanse eller utført et upålitelig arbeid, ville dette ha blitt avdekket av ESA sine mange tilsyn og revisjoner.

På spørsmålet om hvorfor norsk luftfart er underlagt et regelverk som Norge ikke har stemmerett over, påpeker informantene fra SD og Luftfartstilsynet at Norge har talerett og god anledning til å fremme synspunkter og bidra med å påvirke regelverket. Informantene presiserer at det er langt mer ønskelig enn ikke ønskelig fra EU sin side at Norge tar ordet og deltar aktivt i utformingen og endringene i regelverket. Når endringene skal stemmes over, blir imidlertid Norges representanter sendt ut på gangen. Til tross for det anser informantene at norske interesser og synspunkter i stor grad tas i betraktning, og at de norske synspunktene ofte samsvarer med de andre EU- statene og dermed blir innlemmet i regelverket.

Informantene uttrykker at det innad i bransjen har vært diskutert muligheter for å utvikle et alternativt regelverk for de minste lufthavnene i Norge. Informantene uttrykker derimot at et alternativt regelverk ville gått på bekostning av flere positive faktorer med dagens security-regime. *Informant SD* trekker frem bekymringen om at terrorister kan utnytte små lufthavner som inngangsporter til det europeiske luftfartssystemet, dersom sikkerhetsnivået hadde blitt redusert. Et alternativt regelverk ville også ha havnet i konflikt med EU sine sikkerhetskrav om å være del av One-Stop-Security regimet. EU krever at det skal være likt sikkerhetsnivå på alle lufthavnene som er del av systemet, for å ivareta en robust flysikkerhet på hele kontinentet. Informantene anser derfor at det vil være svært u hensiktsmessig å gjennomføre en politikk som resulterer i at enkelte flyplasser i Norge blir utelatt fra systemet. Informantene fra Luftfartstilsynet og SD trekker også frem at et mindre strengt regelverk på de minste lufthavnene, ville ført til misnøye og skepsis blant passasjerene som benytter seg av lufthavnene. Dersom ulike sikkerhetstiltak hadde blitt fjernet ved Båtsfjord lufthavn, hadde passasjerene, lokalbefolkningen og media stilt spørsmålet: «er de reisende til og fra Båtsfjord ikke like mye verdt som dem på Gardermoen eller på Flesland»?

Informant 2 Avinor, som er lufthavnsjef på en mellomstor lufthavn, kunne ikke vise til noen ulemper eller negative effekter ved å praktisere EU-regelverket på lufthavnen. Informanten anser reglene for å være fornuftige, robuste og i tråd med trusselbilde, og trekker frem mulighetene for å kunne utveksle erfaringer med andre lufthavner som er underlagt de samme kravene. Informanten var derfor utelukkende positiv til at EU-regelverket skal være førende og bindende for norsk luftfart.

Informantene fra Luftfartstilsynet og SD er også utelukkende positive til at alle lufthavner i Norge praktiserer det samme regelverket, både fordi det ivaretar flysikkerheten på en robust måte, men også fordi det fører til at den norske luftfarten får være del av det europeiske og internasjonale luftfartssamarbeidet. I en globalisert industri som luftfarten er et slikt samarbeid helt avgjørende. Informanten fra Luftfartstilsynet trekker frem styrkene med et slikt likhetsprinsipp, da det både fører til samme nivå av sikkerhet, at erfaringer og kunnskap mellom lufthavnene kan utveksles og at tilsynsvirksomheten blir mer pålitelig. Informanten bruker samme argumenter på spørsmålet om et alternativt regelverk kunne blitt praktisert på innenriksflyginger mellom små lufthavner i Norge. Informanten trekker frem Kato Air hendelsen. Ingen hadde forestilt seg at et lite propellfly med sju passasjerer på flygningen mellom Narvik og Bodø skulle bli kapret og forsøkt styrtet. Informanten påpeker at terrorister er uforutsigbare og nådeløse, og at sikkerheten derfor ikke må tukles med. Security-regelverket er derfor essensielt, både på de største, de mellomstore og de minste lufthavnene.

Videre påpeker *informant Luftfartstilsynet* at det er opp til Avinor å sørge for at organiseringen og konstruksjonen av lufthavnene bidrar til at regelverket oppfattes som effektivt for de ansatte og passasjerer å forholde seg til, samt at tiltakene oppleves som meningsfulle og fornuftige. Regelverket inneholder en rekke krav om ulike tiltak og barrierer, men det er i stor grad opp til Avinor og hver lufthavn å bestemme hvordan tiltakene skal etterleves og fungere i praksis. *Informant 2 Avinor* trekker frem at de har et kontinuerlig fokus på å finne praktiske løsninger som fører til at security-tiltakene blir oppfattet som fornuftige. *Informant Luftfartstilsynet* trekker frem et eksempel fra da regelverket ble innført i Norge på 2000-tallet, da det var stor misnøye blant piloter og kabinansatte med de nye security-bestemmelsene. Organiseringen av flere lufthavner var utformet på en ineffektiv og dårlig måte, og fasiliteter som kantine, toalett og møterom lå utenfor det sikkerhetsbegrensede område. Det førte til at crewet måtte igjennom ny sikkerhetskontroll for hver gang de beveget seg ut av området. Crewet kunne derfor bli screenet opp imot 12-13 ganger i løpet av en

arbeidsdag. Pilotene anså dette som krenkende mot deres autoritet, da det tross alt er pilotene som har det øverste ansvaret for flysikkerheten. Dette førte til mye frustrasjon og sinne blant pilotene, noe som til tider gikk utover konsentrasjonsevnen og dermed også flysikkerheten. Security-systemet virket på den måten mot sin hensikt. I dag er denne organiseringen langt bedre, og slike fasiliteter er plassert innenfor det sikkerhetsbegrensede område. Dermed blir security-tiltakene oppfattet som mer givende og fornuftige å forholde seg til, noe som er en viktig forutsetning for security-arbeidet. *Informant Luftfartstilsynet* understreker at slik organisering er Avinor sitt ansvar.

5.3.2 Hvor sikre er KPIene, og i hvilken grad er regimet risikobasert og proaktivt?

Funn fra intervjuene med Luftfartstilsynet og Samferdselsdepartementet slår fast at dagens KPIer i EU-regelverket er grundig utarbeidet på bakgrunn av en rekke risiko og trusselvurderinger, i samarbeid mellom flere nasjoner, ekspertgrupper, politi og etterretning, forsvar etc. I etterkant av 11. september 2001 angrepene, da forordning 2320/2002 trådte i kraft i Europa, var regelverket i større grad hendelsesbasert. KPIene var i større grad utviklet som en respons på historiske hendelser, velkjente angrepsmetoder og scenarioer. Ifølge informantene var det lite rom for å diskutere innholdet i forordningen, og regelverket ble betraktet som mer detaljert og reaktivt sammenliknet med dagens regelverk. Regelverket på den tiden bygget i mindre grad på risiko og trusselvurderinger, og sannsynligheten for at ondsinnede individer kunne lykkes med å gjennomføre angrep ved bruk av ukjente metoder, var langt større sammenliknet med i dag. Informantene påpeker at flere av dagens regler også er innført som en respons på reelle hendelser og velkjente angrepsmetoder. *Informant SD* påpeker likevel at det skjer flere regelverksendringer i dag uten at det nødvendigvis har vært noen konkret hendelse i forkant. Informanten anerkjenner at det vil være utfordrende å ha oversikt og kunnskap over alle mulige angrepsmetoder som terrorister kan benytte seg av, men informantens inntrykk er likevel at det arbeides proaktivt og risikobasert gjennom å kartlegge alle mulige risikoer. *Informant Luftfartstilsynet* understreker at bakgrunnen for at flere av sikkerhetstiltakene på lufthavnene er underlagt hemmelighold, er fordi flere tiltak og barrierer retter seg mot metoder som ikke er blitt brukt av terrorister tidligere. Sikkerhetssystemet i luftfarten ligger derfor på mange områder et steg foran terroristene, men dersom terroristene får kunnskap om begrunnelsen for ulike tiltak og forsvarsbarrierer, kan de utnytte den kunnskapen for å planlegge og utføre angrep. Informanten fra Luftfartstilsynet sier at security-systemet i luftfarten er bygd opp på en måte som i stor grad samsvarer med det Reason (1997) omtaler som et forsvar-i-dybden, bestående av flere lag av forsvar og barrierer

som sammen skal stenge ute en trussel. Dersom en person kommer seg over gjerdet på flyplassen, er de neste barrierene overvåkning, patruljering, fysiske hindringer etc. Informanten påpeker at det ikke er mange aktører som har den totale oversikten over det totale barrieresystemet, og at det også er slik det skal være.

Funn fra intervjuene viser at det foregår et bredt samarbeid mellom flere aktører i arbeidet med trusselvurderingene for luftfarten, både overnasjonalt, nasjonalt og lokalt. Informantene fra Luftfartstilsynet og SD viser til at EU har stor tilgang på trusselinformasjon og etterretning, og et eget organ i EU innhenter all relevant trusselinformasjon fra de ulike nasjonene og andre relevante aktører. Alle permanente og midlertidige endringer som blir gjort i EU-regelverket i dag, er derfor på grunnlag av et grundig etterretningsarbeid.

Informant Luftfartstilsynet dro frem et aktuelt eksempel, om innside trusselen som foreligger i luftfarten i dag. I flere av de planlagte terroraksjonene mot luftfarten de senere årene, skal ansatte ha blitt infiltrert eller forsøkt infiltrert og bistått terroristene i planene. Av den grunn arbeides det grundig med personkontroll av de ansatte, noe som i stor grad kommer som følge av den trusselinformasjonen som EU sitter på. Det kommer også stadig nye krav til teknologi på lufthavnene. Screening maskinene må for eksempel stadig utvikles for å kunne oppdage nye typer av sprengstoff. EU stiller med andre ord en rekke krav til medlemstatene, på bakgrunn av den risiko og trusselinformasjonen de innhenter.

Informant SD viser også til det nasjonale sikkerhetsrådet for luftfarten, som ledes av Luftfartstilsynet. Ulike departementer, Avinor, PST, NSM og andre relevante aktører er deltakere i sikkerhetsrådet, hvor det foretas risiko og trusselvurderinger for å sikre at flysikkerheten er ivaretatt. *Informant SD* slår også fast at aktører innen luftfarten er i kontinuerlig dialog med politi og etterretning. *Informant 2 Avinor* deler dette synet om at det foreligger et tett samarbeid. Representanter fra informantens lufthavn er i jevnlig møter med lokalt politi for å vurdere trusselbilde, samtidig som PST og etterretningsvirksomheter avholder jevnlig møter og seminarer. Dersom ny trusselinformasjon blir avdekket, får alle lufthavner rask informasjon om dette.

Videre kommer det frem av intervjuene at KPIene i forordning 300/2008 kun er en minimumsstandard for sikkerheten i luftfarten. Ytterligere tiltak utover forordning 300/2008 som anses som nødvendige ut ifra trusselvurderinger, kan iverksettes nasjonalt og lokalt og innlemmes i den norske securityforskriften. Securityforskriften inneholder alle EU-kravene,

samt en rekke tilleggsbestemmelser som ikke fremgår av EU regelverket. Informantene sier at det kan foretas justeringer og styrke sikkerheten nasjonalt, regionalt og lokalt, gjennom å anvende securityforskriften. *Informant Luftfartstilsynet* presiserer at alle punktene i EU-regelverket fremdeles må være oppfylt, da disse kravene er minimumsstandarden. Informantene argumenterer for at dette gjør at security arbeidet i luftfarten er fleksibelt, effektiv og proaktivt. Luftfartstilsynet sitter på en lang liste over tiltak som kan iverksettes på kort tid, for å gjøre regelverket strengere for å imøtekomme en konkret trussel. Slike tiltak kan innføres lokalt, regionalt eller nasjonalt. Dersom det oppstår en konkret trussel mot Stavanger lufthavn Sola, kan det innføres strengere tiltak der uten at de samme tiltakene må iverksettes andre steder. Påstanden om at dagens security-regelverk er lite fleksibelt og effektivt, er derfor noe *informant Luftfartstilsynet* og *informant SD* er uenig i. Informantene anser at etterlevelse av KPIene i EU-regelverket langt på vei vil føre til et robust sikkerhetsnivå, men at det gir en ekstra dimensjon å ha muligheten for å styrke sikkerheten ytterligere gjennom nasjonal og lokal beslutningstaking.

Alle informantene påpeker at trusselvurderinger er noe Luftfartstilsynet og Avinor også arbeider med hver dag. Trusselinformasjon hentes ikke bare fra EU organet, men også nasjonalt arbeides det kontinuerlig og systematisk med risiko og trusselinformasjon. Informasjon fra PST, NSM, Forsvarets etterretning og flere andre aktører settes sammen til en nasjonal trusselvurdering. I denne nasjonale trusselvurderingen inngår også informasjon fra EU og andre samarbeidstater. Samtidig blir også lokale trusselvurderinger utarbeidet, da trusler kan rette seg mot lokale lufthavner eller områder. Internasjonale, nasjonale, regionale og lokale forhold spiller derfor inn på den totale risikovurderingen. Denne vurderingen er unntatt offentligheten, og *informant Luftfartstilsynet* understreker at det kun er noen få aktører som har innsyn og kunnskap om denne vurderingen.

Funn fra intervjuene har vist at KPIene i seg selv er robuste og proaktive forsvarsmekanismer som gjør det svært utfordrende for terrorister å overliste security-systemet. KPIene er samtidig bare en del av det totale security-systemet. Ifølge *informant Luftfartstilsynet* foreligger det en rekke andre usynlige og hemmeligholdte barrierer, samtidig som det foregår en kontinuerlig og systematisk overvåkning og vurdering av trusselbilde mot luftfarten. Informantene fra Avinor påpeker også at det foreligger en rekke tilleggskrav og bestemmelser internt i Avinor. *Informant 2 Avinor* har en oppfatning om at Avinor ønsker å dobbelsikre sikkerheten, noe informantene anser som positivt, men også som tid og ressurskrevende. Alt av

security arbeid som utføres må grundig dokumenteres, og til tider anså informanten at det blir avholdt møter kun for å ha møter. Informanten ser likevel fordelene ved at Avinor ønsker å styrke sikkerheten utover EU-kravene, men at det stadig legges til flere regler og bestemmelser internt i Avinor og at dette er tid og ressurskrevende.

6. Drøfting

I dette kapittelet vil oppgavens tre forskningsspørsmål diskuteres med sikte på å besvare problemstillingen; *Er det sammenheng mellom de KPIene som Avinor benytter for å definere deres sikkerhetsnivå, og hvordan disse KPIene faktisk påvirker sikkerhetsnivået?* Funn som er presentert i empirikapittelet vil diskuteres i lys av oppgavens teoretiske rammeverk. Formålet med studien er å belyse hvor sikre og pålitelige dagens KPIer er. Det første forskningsspørsmålet tar for seg hva som er karakteristisk for dagens security-regime og aktørene i luftfarten. Det andre forskningsspørsmålet har til hensikt å diskutere bakgrunnen for at de 73 KPIene benyttes som indikatorer på om sikkerhetsnivået er akseptabelt eller ikke, og hvilke variabler som kan påvirke påliteligheten til KPIene. Det tredje forskningsspørsmålet vil belyse hvordan security-regimet eventuelt kan bli mer risikobasert og proaktivt.

6.1 Hva karakteriserer regimet og aktørene som driver med security-arbeid i luftfarten?

Luftfarten er et eksempel på en høyrisikoindustri som er underlagt en rekke reguleringer, med det formål at industrien skal holdes på et akseptabelt risikonivå fremfor at den må forbys. Beck (1992) forklarer at samfunnet har utviklet sosiale systemer, forvaltning og politikk for å håndtere slike risikoer. Trusselen for terroranslag mot luftfarten er reell, både i Norge og i Europa, til tross for det omfattende sikkerhetssystem som finnes på lufthavnene. Terrorisme anses som en kompleks, tvetydig og usikker risiko, med potensiale for katastrofale utfall. Ifølge Renn (2008) er det behov for å involvere flere ulike eksperter i arbeidet med å forebygge og håndtere slike risikoer. Empiri fra intervjuene med Luftfartstilsynet og SD viser at det foreligger et bredt samarbeid mellom flere aktører i security-arbeidet. Det gjelder både sentralt i EU der regelverkbeslutninger blir tatt, men også nasjonalt og lokalt i Norge. Ifølge *informant SD* innhenter EU store mengder data og involverer ulike aktører fra alle medlemslandene i EU, for å sikre at utarbeidelsen og utviklingen av regelverket er i tråd med et kunnskapsbasert og oppdatert trusselbilde. Med tanke på antallet nasjoner og aktører som er underlagt regimet, gir det et stort potensial for å utveksle kunnskap og erfaringer. Det gir rom for at ulike involverte interessenter kan reflektere sammen med beslutningstakerne i EU, for å dra normative konklusjoner vedrørende hva som er akseptabel risiko og hvilke tiltak som må iverksettes. Empirien viser likevel at det er begrenset hvor mange aktører som får delta i selve beslutningsprosessene i EU. Ifølge *informant SD* blir det satt sammen en komité med et begrenset antall aktører, som sammen diskuterer, utarbeider og stemmer over endringer eller utarbeidelse av nye forordninger og regler. Informanten uttrykker at hemmeligholdet rundt

security-arbeidet i luftfarten gjør at et deliberativt demokrati der avgjørelser blir fattet på grunnlag av en bred, offentlig debatt fremfor stemmegiving alene (Renn, 2008), er utfordrende i luftfarten. Internasjonal terrorisme er et komplekst og usikkert fenomen, noe som gjør åpenhet, tilgjengelighet og involvering av flere interessenter uforsvarlig. Mye av arbeidet med security i luftfarten er derfor klassifisert, slik at terrorister ikke skal få kunnskap om systemet.

Norske myndigheter og virksomheter har derfor mindre innflytelse og påvirkningskraft i security-arbeidet i dag, sammenliknet med før 9/11 da norsk luftfart ble regulert av nasjonal lovgivning. *Informant SD og Luftfartstilsynet* anser likevel at norske myndigheter har anledning til å bidra i påvirkningen og utviklingen av EU-regelverket, til tross for at Norge ikke har stemmerett. Informantenes syn er at Norge er svært aktive i å fremme synspunkter, både i EU og i ICAO. Skifte fra en nasjonal regulering til en overnasjonal regulering, har likevel ført til mer hemmelighet og mindre deltakelse og innflytelse fra nasjonale og lokale aktører i Norge. Security-regime samsvarer delvis med Renn (2008) sine teorier om involvering av et bredt utvalg av ulike interessenter og eksperter, da komiteene som etableres består av aktører med ulik bakgrunn og kompetanse. I tillegg innhenter EU relevant informasjon fra en rekke ulike hold, og tar informasjonen i betraktning når beslutninger skal foretas. Utvalget av aktører er derimot begrenset i de avgjørende beslutningssituasjonene, og beslutningsprosessene skal foregå så effektivt som mulig for å respondere på utviklingen i trussellandskapet. De iboende kjennetegnene ved terrorisme gjør derfor at et deliberativt demokrati er vanskelig å gjennomføre i security-beslutningene i luftfarten.

Det foreligger også strukturelle trekk ved security-regime som hindrer aktørene i luftfarten til å operere innenfor rammene til HRO teorien. Det til tross for at Frederickson og LaPorte (2002) definerer security systemet i luftfarten som en HRO. Et av de viktigste tankesettene i HRO-teorien er at kompetanse og beslutningsmyndigheten flyttes ned til de lavere nivåene i systemet, dersom en krise oppstår eller trusselnivået økes. Antakelsen er at desentralisering vil føre til en økt tilpasningsevne og robusthet i responsen. Empirien viser imidlertid at det er lite rom for lokale tiltak, beslutninger og desentraliserte tolkninger av selve EU-regelverket i en normaltilstand på lufthavnene. De ansatte ved Avinors lufthavner er forpliktet til å følge kravene i EU-regelverket slavisk, da antakelsen er at det vil føre til et robust sikkerhetsnivå. På bakgrunn av det må de ansatte følge arbeidsoppgaver som er forhåndsbestemt og detaljert beskrevet, noe som kan gå på bekostning av lokalt engasjement, innovative løsninger og

individuell og kollektiv «mindfulness». De ansattes «mindfulness» hvor deres følelse om å «være i øyeblikket» gjennom bevissthet, oppmerksomhet og menneskelig dømmekraft, kan bli redusert til fordel for et kontinuerlig fokus etter å operere innenfor kravene i regelverket.

Når regelverket ikke åpner opp for menneskelig dømmekraft og rasjonell tolkning av prosedyrene i forhold til ulike situasjoner, betyr det at regelverket må beskrive alle mulige situasjoner som ansatte kan havne i. Ifølge *informant 1 Avinor* kan det anses som en utopi, da faktum er at det er mennesker som opererer de mekaniserte systemene. Informanten setter spørsmålsteget ved hvorfor regelverket ikke åpner opp for at mennesker i større grad kan bidra med sin dømmekraft og erfaring for å styrke sikkerheten ytterligere. *Informant Luftfartstilsynet* trekker frem at det skal foreligge et likhetsprinsipp mellom passasjerene, og at det kan føre til diskriminering dersom de ansatte ved lufthavnene skal bestemme hvem som skal kontrolleres grundigere. Informanten påpeker at de ansatte ikke har kompetanse til å foreta slik profilering, men utelukker ikke at det foregår en viss form for profilering ved norske lufthavner til tross for at dette ikke er regulert av regelverket. Samtlige ansatte har et ansvar om å være oppmerksomme på mistenkelig aktivitet og oppførsel. Ifølge informanten vil det derfor være rom for å bruke en viss grad av sunn fornuft i security-arbeidet, men i utgangspunktet så er det regelverket som skal beskrive hvordan ulike situasjoner skal løses.

Videre viser empirien at det er rom for en viss grad av nasjonal og lokal risikostyring, og at beslutningsmyndigheten kan flyttes nedover i systemet. Dette er et sentralt kjennetegn ved en HRO. Dersom en hendelse oppstår eller at trusselbilde tilsier at det er behov for å styrke sikkerheten utover de tiltakene som fremkommer av EU-regelverket, kan Luftfartstilsynet iverksette en rekke ulike tiltak. Det åpner opp for at Luftfartstilsynet kan foreta en viss form for nasjonal og lokal risikostyring under krevende forhold. *Informant 2 Avinor* påpeker også at det foreligger en rekke interne security-bestemmelser i Avinor som skal bidra til å øke sikkerhetsnivået utover EU-kravene. Det viser at det også er rom for å foreta lokale beslutninger under en normaltilstand. Det er et minimumskrav at alle EU-reglene til enhver tid skal være oppfylt, men utover dette kan nasjonale og lokale tilleggsbestemmelser iverksettes på bakgrunn av egne vurderinger.

Innføringen av security-regime i etterkant av 9/11 angrepene har ført til en nedgang i antallet terroranslag mot luftfarten. Det viser at security-regime har hatt ønsket effekt, og at industrien reguleres på en slik måte at risikoen holdes på et akseptabelt nivå. Security-systemet

samsvarer derfor på mange måter med Morone og Woodhouse (1986) sitt utsagn om HROer: «den gode sikkerheten er et systematisk produkt av menneskelige handlinger- resultatet av en bevisst prosess der risikoer overvåkes, vurderes og reduseres». Empirien viser at det foregår et kontinuerlig arbeid med å redusere risikoen for terroranslag mot luftfarten, gjennom barrierer, bevissthet, samarbeid, etterretning, politisk engasjement, økonomi etc. Luftfarten er et eksempel på en høyrisikoindustri som er eksponert for terrorisme, men som holdes på et akseptabelt sikkerhetsnivå gjennom pålitelige systemer. I organisasjoner med så stor usikkerhet at det kan være vanskelig å evaluere systemets faktiske suksess, gir HRO teorien et bilde på at pålitelige komponenter i stor grad fører til systemets suksess.

Det er likevel tendenser ved security-regimet som tilsier at suksessen ikke bare er som følge av pålitelighet, men at flaks, tilfeldigheter og fravær av terrorplaner mot luftfarten også er faktorer som har ført til suksessen. Empirien viser at Luftfartstilsynet stadig vekker avdekket nye hull i barrierene ved norske lufthavner. Dersom inspektørene klarer å finne hull, vil også terrorister kunne klare det. *Informant 1 Avinor* påpeker imidlertid at det må foreligge en erkjennelse om at 100% samsvar med KPIene i regelverket vil være umulig å oppnå til enhver tid. Når det er mennesker som opererer de fleste systemene, så vil det alltid bli begått feil. En slik erkjennelse og en tanke om at barrierene og de ansatte kan svikte, er avgjørende i det daglige sikkerhetsarbeidet og vil bidra til å styrke påliteligheten og sikkerheten. En kombinasjon av strategiene forventning og resiliens vil bidra til at de ansatte opererer med mer bevissthet og oppmerksomhet knyttet til en slik erkjennelse. Forventning om at terrorister kan komme seg usett gjennom en barriere, vil styrke robustheten til de andre barrierene. Dersom de ansatte som overvåker det sikkerhetsbegrensede område har en innstilling om at sikkerhetskontrollen har garantert for at ingen har fått med seg ulovlige gjenstander, vil overvåkning som barriere være bortkastet. De ansatte må ha en kontinuerlig forventning og innstilling om at systemer og mennesker kan svikte, og at de skal være den neste barrieren som skal fange opp trusselen. En innstilling om at det ikke er spørsmål om et angrep vil skje, men når det vil skje, vil føre til større bevissthet og pålitelighet i security-arbeidet. Resiliens er også en viktig egenskap å bygge inn i systemet, slik at systemet kan justere sine funksjoner i forkant av, under, eller etter uønskede hendelser. På den måten kan nødvendige funksjoner opprettholdes under både forventede og uventede forhold. Slike egenskaper er sentrale kjennetegn for organisasjoner med høy pålitelighet.

Videre viser empirien til en side ved security-regimet som svekker inntrykket av at systemet innehar en stor grad av pålitelighet. En viktig forutsetning for at en organisasjon skal være pålitelig, er at teknologien og prosedyrene må være godt forstått av de ansatte og at rutinene er gjennomarbeidet. Tilsynsrapportene viser flere eksempler på at ansatte gjør åpenbare feil eller bevisst velger å trosse regelverket. Dersom ansatte hadde valgt å ignorere regelverket til fordel for innovative løsninger som ble ansett som mer treffende og risikobaserte, ville det ifølge HRO teorien vært en faktor som hadde styrket påliteligheten. Flere avvik fra tilsynsrapportene viser derimot at ansatte har trosset regelverket for å spare tid, krefter eller som følge av manglende kunnskap om prosedyrene eller manglende bevissthet knyttet til terrortrusselen. *Informant 2 Avinor* understreker at det er et kontinuerlig fokus på god utdanning, opplæring og oppfølging av alle ansatte for å forhindre slike tendenser. Informanten trekker frem at uvarslede inspeksjoner vil bidra til å opprettholde fokuset blant de ansatte, noe som vil redusere sannsynligheten for at slike negative tendenser oppstår. Informanten trekker også frem viktigheten av lateral kommunikasjon, hvor utveksling og formidling av informasjon, ideer eller følelser mellom menneskene på lufthavnene vil føre til et større samhold og dermed mer bevissthet rundt security-arbeidet. Informanten trekker også frem at det foregår en løpende dialog mellom lufthavnene i Norge, særlig lufthavnene i samme geografiske områder, for å kunne utveksle erfaringer. Lateral kommunikasjon er et sentralt element i HRO teorien, og er en sentral forutsetning for å kunne utvikle en kollektiv bevissthet. Weick et al (1999) hevder at særpreget til HROer ligger i hvordan ulike men stabile kognitive prosesser henger sammen for å kunne oppdage og korrigere feil. Denne evnen til oppdagelse og korrigerende er det Weick et al (1999) betegner som kollektiv bevissthet, og de anser fem prosesser for å gi HROer denne evnen:

1. *Oppmerksomhet rundt feil og svikt.* Empirien viser at det foregår et kontinuerlig søk etter feil og svikt på lufthavnene, både under Luftfartstilsynets inspeksjoner, internt i Avinor og fra et europeisk hold gjennom EFTA sine revisjoner og inspeksjoner. *Informant 2 Avinor* understreker at det også foregår et kontinuerlig søk blant de ansatte på lufthavnene etter feil og svakheter i systemene. Når mulighetene for prøving og feiling er begrenset, så vil inspeksjoner og egen rapporterte avvik bidra til et stort læringspotensial. Empirien viser at Luftfartstilsynets inspeksjoner fører til læring, i den forstand at feil og svikt i systemene avdekkes og tiltak iverksettes. Likevel viser empirien at tilsynet ofte avdekker nye avvik på de samme punktene som

tidligere har hatt avvik, noe som svekker antakelsen om at inspeksjonene fører til en direkte styrking av sikkerheten.

2. *Motvilje mot å forenkle tolkninger.* Effektive HROer forsøker å unngå selvtilfredshet og situasjoner der ansatte blir sosialisert til å ignorere de samme tingene. Empirien viste at Luftfartstilsynet avdekket at ansatte på en lufthavn regelmessig beveget seg fra landside til sikkerhetsbegrenset område uten å først bli kontrollert i sikkerhetskontrollen. Dette er et eksempel på at ansatte kan bli sosialisert til å foreta kollektive handlinger som avviker fra regelverket, og tilsynet reagerer sterkt på slike avvik for å opprettholde påliteligheten og bevisstheten blant de ansatte.

I tillegg implementeres ofte redundans i HROer for å ivareta bevisstheten. Det innebærer kryssjekk, tvil om at forhåndsbestemte regler er tilstrekkelige og varsomhet rundt påståtte nivåer av kompetanse. Slike kjennetegn er på bakgrunn av empirien fraværende i security-systemet, da det gis lite rom for å stille spørsmål ved regelverket og foreta egne refleksjoner og handlinger som avviker fra regelverket. De ansatte skal ha full tiltro til regelverket og utføre sitt arbeid i samsvar med instruksene. I HRO teorien står skepsis og en viss grad av mistro til reglene sentralt for å opprettholde påliteligheten og sikkerheten. Slike kjennetegn samsvarer derfor ikke med empirien. Intervjuene fra empirikapittelet viser at det er rom for dialog og innspill fra de ansatte vedrørende svakheter i systemene, og at slik kommunikasjon er viktig for å opprettholde et høyt sikkerhetsnivå. Likevel er det beslutningstakerne i EU som skal foreta justeringer i regelverket, og de ansatte må utelukkende arbeide systematisk etter prosedyrene.

3. *Følsomhet rundt operasjoner.* Handler om HROer sin situasjonsbevissthet, og at følsomhet, kollektiv bevissthet og kunnskap rundt operasjoner og tekniske systemer skal forhindre at feil akkumuleres. Empirien viser at aktørene i luftfarten arbeider aktivt for å sikre at operasjoner og handlinger er i tråd med regelverket. De fleste inspeksjonene fra Luftfartstilsynet konkluderer med at det er samsvar med reglene. *Informant 2 Avinor* har ett inntrykk av at menneskene som arbeider med security-relaterte oppgaver er kompetente, bevisste og oppmerksomme, og at de samarbeider tett for å oppnå en kollektiv meningsdannelse, kunnskapsformidling og utveksle kontinuerlige oppdateringer rundt det arbeidet som foretas.

På den andre siden viser empirien at det stadig avdekkes avvik i forbindelse med security-arbeid. Luftfartstilsynet avdekker jevnlig at ansatte mangler kunnskap om systemene eller om innholdet i regelverket, noe som svekker organisasjonenes evne til å operere pålitelig. I et slikt komplekst og omfattende sikkerhetssystem er det avgjørende at de ansatte har nok kunnskap om komponentene og sammenkoplingene i systemene.

4. *Forpliktelse til resiliens.* Handler om at organisasjonen har kapasitet til å motstå og tilpasse seg forventede og uventede forstyrrelser, og at de forbereder seg til utenkelige scenarioer og overraskelser for å være bedre rustet til å takle slike hendelser.

Informantene fra Luftfartstilsynet og SD påpeker at det foregår et kontinuerlig arbeid med å overvåke og evaluere trusselen mot luftfarten, for på den måten å kunne respondere på uventede hendelser. Ressurser og tiltak kan iverksettes umiddelbart dersom slike hendelser oppstår. Samtidig viser empirien at de statiske punktene i regelverket kan være reaktive i møte med utenkelige scenarioer og overraskelser. Dersom et angrep avviker mye fra tidligere hendelser, vil det kunne føre til at regelverket ikke beskriver hvordan situasjonen skal håndteres. Samtidig foreligger det en tanke om at samsvar med reglene vil gjøre at trusler blir identifisert og stanset. Security-regime tar derfor i liten grad hensyn til at mennesker gjør feil og at teknologien kan være feilaktig. En slik forventning knyttet til at systemet kan svikte, er sentralt for å kunne bygge inn resiliens i sikkerhetssystemet.

5. *Underspesifisering av strukturer.* Handler om tilfeller der det detaljerte og ordnede systemet forsterker feil. En måte å forhindre dette på kan være å løsne på den hierarkiske beslutningsstrukturen og i større grad la beslutningene følge problemene. En særegen egenskap ved effektive HROer, er den fleksible beslutningstakingen der beslutningsmyndigheten blir mer situasjonsbestemt og flyttes nedover i organisasjonen. Empirien viser at det daglige security-arbeidet på lufthavnene i liten grad samsvarer med slike egenskaper. Det fører til at lufthavnene i mindre grad kan være proaktive gjennom egne handlinger og beslutninger. Tanken er at de sentraliserte beslutningstakerne i EU har utviklet robuste KPIer på bakgrunn av bred kunnskap om risikobilde, og at de ansatte skal fungere som komponenter for å sikre at KPIene

etterleves. Tilliten til lokal kunnskap og bevissthet er derfor mangelfull i regimet, noe som kan gå på bekostning av et mer situasjonsbestemt sikkerhetsarbeid.

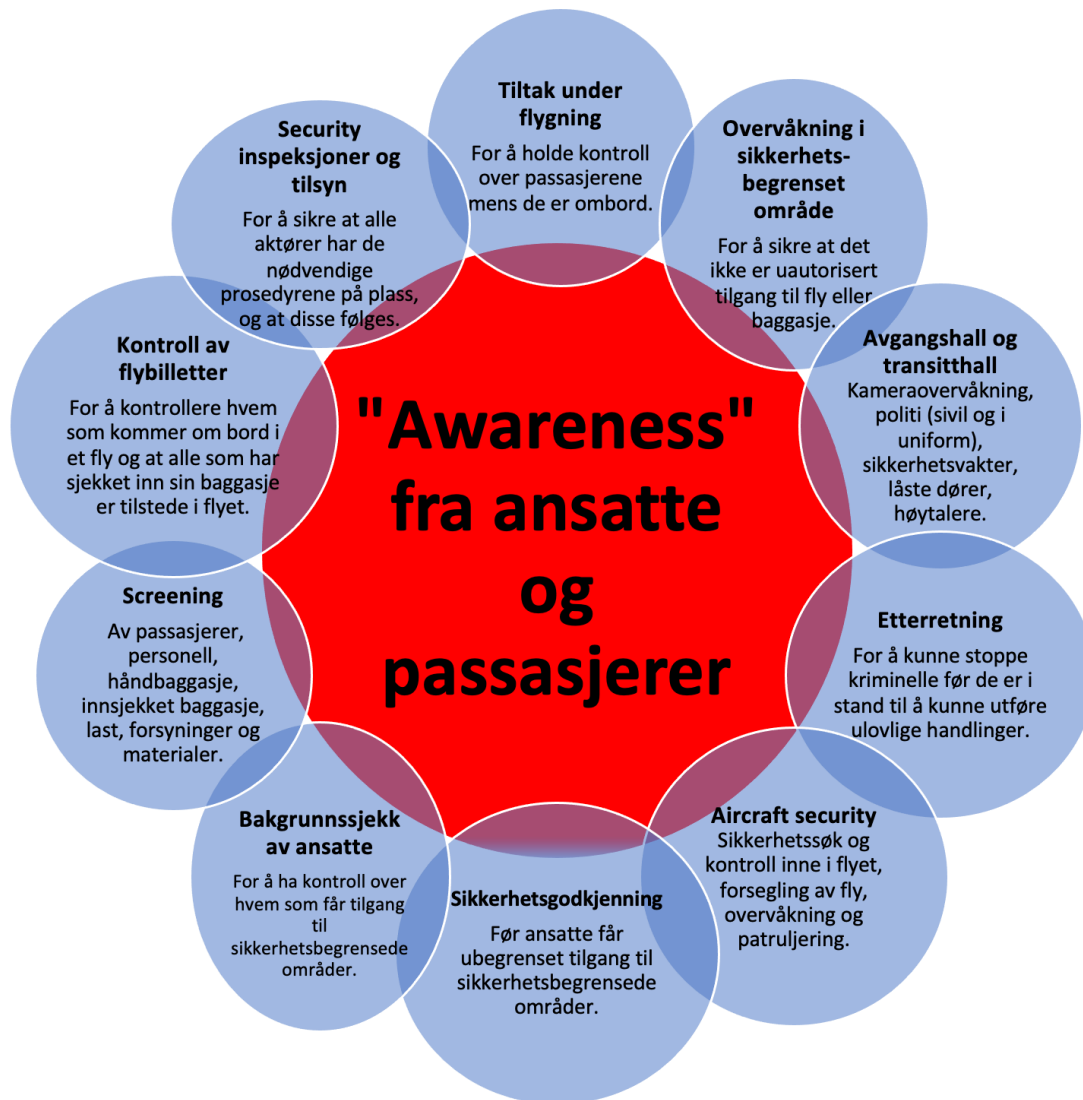
Den uforutsigbare karakteren av terrorangrep gjør det umulig for myndigheter, industrier og organisasjoner å garantere for offentlig sikkerhet. Etterlevelse av sentrale komponenter i HRO teorien vil likevel føre til at organisasjoner vil operere med høyere pålitelighet, noe som igjen vil redusere risikoen for terroranslag. Empirien har vist at security-regime i luftfarten etterlever enkelte punkter i HRO teorien, men at det også foreligger strukturelle trekk ved regimet som gjør slik etterlevelse vanskelig for de aktørene som er underlagt regimet. For at security-regimet skal være i stand til å forhindre terrorangrep i fremtiden, vil et økt fokus på å operere med høy pålitelighet være en robust strategi. Det vil bidra til at sikkerhetsarbeidet i større grad er tilpasset det mangfoldet av angrepsscenarioer som kan ramme luftfarten, fremfor at det foreligger et ensidig fokus på å samsvare med punktene i regelverket. En erkjennelse av at KPIene ikke monitorerer alle mulige angrepsscenarioer, og en bevissthet knyttet til at barrierene, systemene og menneskene kan gjøre feil, vil bidra til økt pålitelighet og sikkerhet ved norske og europeiske lufthavner.

6.2 Hvor sikre er dagens KPIer, og hvilke variabler kan påvirke deres pålitelighet?

Dagens KPIer i forordning 300/2008 er utviklet for å gjøre flysikkerheten så trygg som mulig. KPIene er i stor grad hendelsesbaserte, og er blitt utviklet som respons på historiske hendelser. Informantene fra Luftfartstilsynet og SD understreker likevel at dagens KPIer i langt større grad enn tidligere, er kunnskapsbaserte og utviklet på bakgrunn av grundige risiko og trusselvurderinger. Informantene anser derfor at KPIene er proaktive og risikobaserte nok til å kunne avverge terrorangrep som baserer seg på nye og ukjente metoder.

Den eneste måten å oppnå 100% sikkerhet på er å holde alle fly på bakken til enhver tid. Når dette ikke er en ønskelig løsning, er det behov for et sett med sikkerhetsbarrierer som kan holde sivil luftfart så trygg som mulig. Sikkerhetsbarrierene er organisert som lag på lag. Hver barriere er ikke individuelt 100%, men må sees i sammenheng med de andre barrierene. Regelverket samsvarer i stor grad med Reason (1997) sine teorier om ulike lag av barrierer og et forsvar-i-dybden. Barrierene består av menneskelige, tekniske og organisatoriske faktorer. Menneskelig bevissthet, kompetanse og konsentrasjon, tekniske apparater som overvåkningskameraer, screeningmaskiner og alarmer og organisatorisk struktur og retningslinjer for hvordan ansatte skal operere, er eksempler på barrierer som sammen skal

hindre terrorister i å angripe luftfarten. Det er dette mangfoldet av overlappende og gjensidig støttende forsvaret som gjør at små feil av menneskelig eller teknisk art ikke behøver å resultere i at et angrep blir vellykket. Figuren under viser til en rekke forsvarsmekanismer og sikkerhetsbarrierer som sammen skal oppdage eller stanse ondsinnede individer fra å gjennomføre angrep mot luftfarten.



Figur 13: Forsvarsmekanismer og barrierer i luftfarten

Det mest effektive tiltaket mot terrorisme er å stanse terroristene i forebyggingsfasen, gjennom et godt etterretningsarbeid. Det vil foreligge en viss risiko for at terrorister vil kunne lykkes i å overliste sikkerhetssystemet på en lufthavn dersom de har den nødvendige kapasiteten og intensjonen. Terroristene kan anvende kreative metoder som ikke fanges opp av sikkerhetssystemet, eller så kan de ha flaks ved at barrierene, systemene og de ansatte svikter.

Etterretningsarbeid er derfor kritisk for å oppdage og stanse terrorister før de møter opp på en lufthavn med intensjoner om å ramme industrien. Dersom terroristene likevel klarer å holde seg under radaren til etterretningsvirksomhetene og ikke avsløre deres planer, så foreligger det en rekke barrierer på lufthavnene som mest sannsynlig vil oppdage og stanse dem. En av de viktigste egenskapene for å oppdage terrorister, er bevissthet fra de ansatte og passasjerene. *Informant 2 Avinor* påpeker at security-arbeidet er en felles innsats, hvor alle ansatte må være oppmerksomme og årvåkne ovenfor personer eller gjenstander som kan være en trussel. Dette gjelder alle fra piloter, ansatte i sikkerhetskontrollen til de ansatte på kafeene. I tillegg har passasjerene et ansvar om å melde ifra om avvikende og mistenksom oppførsel eller gjenstander. En bevissthet og forventning om at terrorister kan angripe når som helst og hvor som helst, er en viktig forutsetning for å kunne oppdage og stanse dem. De andre barrierene og mekanismene som fremstilles i figuren, er KPIer fra regelverket. *Informant Luftfartstilsynet* mener at et fullstendig samsvar med KPIene i stor grad vil sørge for et robust forsvarssystem, da KPIene monitorerer de fleste inngangsporter og metoder som terrorister kan anvende. Det må likevel foreligge en erkjennelse om at KPIene ikke overvåker alt.

Ifølge *informant 1 Avinor* vil det å definere sikkerhetsnivået på bakgrunn av KPIene, kunne føre til en feil og misvisende fremstilling av det faktiske sikkerhetsnivået. Informanten anser en slik «compliance» fokusert vurdering for å være mekanisk, fordi den avdekker samsvarsnivet med regelverket og ikke nødvendigvis det reelle sikkerhetsnivået. En slik metode forutsetter at regelverket monitorerer alle mulige trusler mot luftfarten, men historien har vist at terrorister stadig har funnet nye metoder for å gå rundt de gjeldende tiltakene og barrierene. Til tross for at empirien slår fast at dagens KPIer er utarbeidet og justeres på bakgrunn av grundige risiko og trusselvurderinger, ligger det i terroristenes natur å utvikle nye metoder som vil kunne overløse sikkerhetstiltakene. En bevissthet knyttet til dette er avgjørende å ta i betraktning i security-arbeidet. Selv om det foreligger fullstendig samsvar med regelverket, betyr det ikke at det reelle sikkerhetsnivået er hundre prosent. En tanke om at systemets suksess kan feires dersom Luftfartstilsynet ikke avdekker noen avvik, kan føre til en falsk trygghet og være direkte truende for flysikkerheten.

Informant SD understreker at det vil være utfordrende å ha en total oversikt og kunnskap over alle mulige angrepsscenarioer og metoder som terrorister kan benytte seg av. Informanten understreker derfor at EU har en kritisk rolle med å avdekke nye typer risikoer, og utvikle KPIer som sørger for at disse risikoene overvåkes. Samtidig påpeker informanten at security-ansatte aldri kan si seg ferdig eller fornøyd med sitt arbeid, fordi trussellandskapet er i

kontinuerlig endring. Informanten understreker derfor at KPIene isolert sett kan være mangelfulle i møte med et slikt trussellandskap.

Et annet aspekt som kan svekke påliteligheten ved en slik «compliance» fokusert tilnærming som råder i luftfarten i dag, er at en rekke ulike faktorer kan påvirke og svekke troverdigheten til KPIene som brukes som indikatorer for å bedømme sikkerhetsnivået. Slike faktorer kan føre til at sikkerhetsnivået blir kartlagt på et feilaktig grunnlag. En slik faktor er usikkerhet.

6.2.1 Usikkerhet

Usikkerhet er et sentralt begrep i all risikostyring, men særlig i forbindelse med security-arbeid. *Informant 1 Avinor* uttrykker at det er viktig å ta usikkerhet i betraktning i alt security-arbeid. Hva terrorister vil forsøke å angripe neste gang, hvilke metoder de vil anvende, hvor mange de vil være og når og hvor de vil forsøke seg. Usikkerhet kan knyttes opp imot en rekke spørsmål. Aven og Renn (2010) slår også fast at usikkerhet er viktig å ta i betraktning, men at jo mer relevant informasjon man legger inn i beregningene, desto mer informativt blir det generelle sikkerhetsarbeidet.

Ifølge *informant 1 Avinor* er det kritisk å ta stilling til at ulike usikkerhetsfaktorer kan ha innvirkning på inspeksjonene som utføres av Luftfartstilsynet, og at det derfor vil foreligge en viss grad av usikkerhet i de resultatene som Avinor mottar i etterkant av inspeksjonene. Luftfartstilsynet informerer ikke om den usikkerheten som foreligger i deres tilsynsaktivitet. Et eksempel på en slik usikkerhetsfaktor er antall passasjerer som er til stede under inspeksjonen. Informasjon om hvor mange passasjerer som inngår i observasjonsgrunnlaget når tilsynet utfører inspeksjonen, blir ikke fremstilt i tilsynsrapporten. En stor pågang av passasjerer og andre stressende faktorer vil kunne gi utslag i resultatene. Dersom inspektørene gjennomfører observasjon som inspeksjonsmetode, og kontrollerer om de ansatte i sikkerhetskontrollen opererer i tråd med regelverket, så vil sannsynligheten for avvik øke proporsjonalt med et økt antall passasjerer som skal screenes. Et større observasjonsgrunnlag vil gi større sannsynlighet for avvik. Dersom det er lite trafikk og lite stressende faktorer som kan påvirke de ansattes kapasitet og konsentrasjon, vil sannsynligheten for avvik reduseres. Informanten anser derfor at det vil være en større prestasjon å unngå avvik på en lufthavn hvor pågangen av passasjerer er stor og stressnivået er høyt, sammenliknet med en lufthavn hvor pågangen er mindre. Slike faktorer kan bidra til å forklare hvorfor avviksnivået er generelt høyere på lufthavnene i kategori A. I 2019 hadde Oslo lufthavn 28 592 619 reisende,

mens Værøy lufthavn hadde 8372. Det vil si at observasjonsgrunnlaget har vært langt større på Gardermoen sammenliknet med Værøy når tilsynet har utført inspeksjoner. Likevel vil et avvik ha nøyaktig samme betydning, uavhengig av hvor mange passasjerer som inngikk i observasjonsgrunnlaget. Dersom sikkerhetskontrollørene på Gardermoen screener 10 000 passasjerer i det tidsrommet Luftfartstilsynet har inspeksjon, så vil ett enkeltstående avvik fra regelverket resultere i at sikkerhetsnivået anses som lavt. Avviket blir ikke sett i sammenheng med helheten, og det kan stilles spørsmålstegn ved om en slik metode er hensiktsmessig å anvende for å definere sikkerhetsnivået i luftfarten. Isolert sett vil ett avvik i et så stort observasjonsgrunnlag være et tegn på at sikkerhetsnivået er relativt høyt. I dette tilfellet ville Avinor ha mottatt en tilsynsrapport med informasjon om at sikkerhetsnivået ikke anses som akseptabelt, fordi det ble avdekket avvik under kontrollen.

Informant 1 Avinor trekker også frem at menneskelig prestasjon i hverdagen kan ha påvirkning på inspeksjonene. De ansatte på lufthavnen som blir underlagt kontroll, eller inspektørene fra Luftfartstilsynet, vil ha gode og dårlige dager. Inspektørene kan overse feil som blir begått, eller stille svært kompliserte spørsmål under intervjuene som fører til avvik. De ansatte kan bli usikre og begå feil fordi de ser at Luftfartstilsynet har inspeksjon. Eller motsatt, at de opererer fullstendig i tråd med regelverket under inspeksjonen, mens de vanligvis tar noen snarveier. *Informant Luftfartstilsynet* trekker frem at inspeksjonene vanligvis foregår gjennom uvarslede inspeksjoner hvor inspektørene er sivilt kledd, for å unngå at slike faktorer påvirker inspeksjonen. Dette er likevel eksempler på at menneskelige faktorer kan ha innvirkning på resultatene av inspeksjonene. Slike faktorer er derimot vanskelige å ta stilling til i en tilsynspraksis, og det vil alltid foreligge en viss grad av usikkerhet og tilfeldigheter som kan ha påvirkning. Alle mennesker vil kunne gjøre feil og være skyld i at det ble avdekket avvik. Dersom avvik er gjentakende blant ansatte, vil inspeksjonene kunne avdekke dette og videre tiltak kan iverksettes. Inspeksjonene vil også kunne avdekke dersom ansatte bevisst velger å trosse reglene eller innehar en generell negativ holdning til security-arbeidet. Det er derfor essensielt at tilsynet utfører uvarslede inspeksjoner for å kunne avdekke slike tendenser.

Til tross for at tilsynsaktiviteten primært retter seg mot å avdekke avvik og svakheter slik at hull kan tettes, er det ifølge *informant 2 Avinor* også viktig å fokusere på de punktene hvor det sjelden eller aldri avdekkes avvik. *Informant Luftfartstilsynet* trakk også frem dette, og påpekte at mange stiller spørsmålstegn ved hvorfor tilsynet inspiserer punkter hvor det aldri er avvik. Informanten påpekte at EU har bestemt at det skal være slik, fordi sikkerhetsnivået på

de ulike punktene kan forandre seg fra dag til dag. *Informant 2 Avinor* understreker at samsvar med kravene som regel skyldes et systematisk og pålitelig security-arbeid utført av dyktige og årvåkne ansatte, men at det også kan forekomme en grad av tilfeldigheter og flaks som førte til at inspektørene ikke avdekket avvik. Til tross for at et punkt besto Luftfartstilsynet sin inspeksjon den ene dagen, kan virkeligheten være en annen dagen etterpå. Informanten trekker derfor frem at tilsynsaktiviteten i noen tilfeller kan ha en negativ effekt, gjennom at de ansatte senker fokuset og bevisstheten knyttet til security-arbeidet etter at tilsynet har informert om at alle punkter samsvarer med kravene. Dette kan være en forklaring på hvorfor Luftfartstilsynet aldri har gitt karakteren 5 i etterkant av deres tilsyn. Karakter 5 betyr bedre enn samsvar med krav, og en slik karakter vil kunne føre til at sikkerhetssystemets suksess blir feiret og at bevisstheten og fokuset blant de ansatte reduseres. Informanten trekker frem at avvik fra tilsynet ofte fører til et skjerpet fokus knyttet til security, og en påminnelse om at et kontinuerlig fokus og arbeid må finne sted. Punktene som besto inspeksjonen, kan kort tid etterpå inneholde hull samtidig som regelverket ikke dekker alle trusler mot luftfarten. I tillegg kan inspeksjonene inneholde metodiske svakheter, og tilfeldigheter og usikkerhet kan ha ført til at resultatene ikke gjenspeiler virkeligheten.

Informant 2 Avinor trekker derfor frem viktigheten av å aldri si seg fornøyd og feire sikkerhetssystemets suksess, fordi trussellandskapet er dynamisk og endrer seg kontinuerlig. Dette kan ses i sammenheng med Reason (1997) sin teori om at de ulike forsvarslagene er i konstant flyt og bevegelse. Enkelte lag av forsvar kan fjernes bevisst under vedlikehold, kalibrering eller testing, eller som et resultat av feil og brudd. Hullene i hvert forsvarslag kan også bevege seg, komme og gå, samt krympe og utvide seg som følge av operatørhandlinger eller lokale forhold. Når forsvarsbarrierene på lufthavnene blir inspisert av Luftfartstilsynet eller av Avinor selv, kan hullene være helt tette, mens de noen timer etterpå kan inneholde hull. Inspeksjonene vil derfor kun avdekke «ett øyeblikks» sikkerhetsnivå. Tilsynsrapportene viser i tillegg at det kan gå år mellom hver gang enkelte lufthavner blir inspisert av Luftfartstilsynet. *Informant 2 Avinor* trekker derfor frem viktigheten av å gjennomføre interne inspeksjoner, da inspeksjonene fra Luftfartstilsynet ikke er tilstrekkelig nok for å avdekke svakheter i systemet. Av den grunn er det avgjørende å erkjenne at sikkerhetsnivået ikke kan defineres utelukkende på Luftfartstilsynet sine inspeksjoner. Det er viktig å reflektere over at ulike variabler kan påvirke resultatene på KPIene, i tillegg til at KPIene ikke monitorerer alle mulige trusler mot luftfarten.

Det vil også kunne foreligge latente forhold i security-regime, som ifølge Reason (1997) er til stede i alle systemer. Systemet i luftfarten er konstruert etter et forsvar-i-dybden-prinsipp, noe som gjør systemet mer komplekst. Det kan være utfordrende for de som administrerer og overvåker systemene å ha den nødvendige forståelsen og innsikten i alle disse lagene av forsvar. Slike latente forhold stammer ifølge Reason (1997) fra beslutninger som er tatt på det strategiske nivået. Dårlig design, kompliserte prosedyrer og svakt og ufullstendig tilsyn er eksempler på slike latente forhold, som kan øke sannsynligheten for at aktive feil begås, ved at de skaper lokale faktorer som kan fremme feil eller brudd. Empirien har vist at de ansatte stadig avviker fra prosedyrene, som ifølge Reason (1997) delvis kan forklares med prosedyrenes kompleksitet og et regelverk som er dårlig designet. Tidligere forskning har også vist at EU-regelverket er konstruert for de store europeiske lufthavnene, og at utfordringene var store da regelverket ble implementert ved små norske lufthavner (Olsvik, 2015). Avviksstatistikken i empirikapittelet viser imidlertid at de minste lufthavnene i Norge har den laveste andelen avvik. Det svekker påstanden om at regelverket ikke er konstruert for de minste lufthavnene. Samtidig kan faktorer som lave passasjertall, lite stress og sjeldne tilsyn fra Luftfartstilsynet på de minste lufthavnene, forklare noe av bakgrunnen for de lave avvikstallene. God opplæring og oppfølging av de ansatte slik at deres forståelse og kunnskap knyttet til prosedyrene og innholdet i regelverket, vil redusere risikoen for at feil begås på bakgrunn av slike latente forhold. I tillegg har EU en viktig rolle i å utvikle prosedyrer som er tilpasset lokale forhold og som er forståelige for dem som skal håndheve reglene.

6.2.2 «Black swans»

Til tross for at KPIene monitorerer de fleste tenkelige scenarier som terrorister kan ta i bruk for å ramme luftfarten, vil uventede hendelser kunne oppstå. Slike hendelser refereres ofte til som «sorte svaner», og Aven (2014) definerer slike hendelser som «*overraskende, ekstreme hendelser sett i forhold til ens kunnskap/tro*». Security-eksperter må derfor bruke kreativitet og reflektere over hvilke metoder terrorister kan komme til å bruke neste gang. *Informant Luftfartstilsynet* sier at hele bransjen forsøker å tenke kreativt og utvikle KPIer som monitorerer nye angrepsscenarioer. På den måten vil security-systemet fremstå som mer proaktivt. Det er hovedsakelig opp til beslutningstakerne i EU å tenke kritisk og kreativt, for å kunne utvikle et slikt proaktivt regelverk. Samtidig er EU avhengig av innspill fra relevante aktører, deriblant Luftfartstilsynet og Avinor. Enkelte scenarier kan derimot anses som så usannsynlige at tiltak ikke blir iverksatt. Teorien om «unknown-unknowns» bidrar til å svekke påliteligheten ved dagens KPIer. Hendelser som er helt ukjente for det vitenskapelige

miljøet, vil ikke dekkes av dagens KPIer og kan føre til at det ikke finnes tiltak og barrierer rettet mot slike hendelser. Imidlertid er det ikke mulig å ta stilling til alle slags scenarioer man kan tenke seg frem til. Det hadde ført til et enda mer komplekst sikkerhetssystem, og sikkerhetssystemet kunne blitt ansett som meningsløst. I tillegg ville spørsmålene om kostnadseffektivitet blitt mer aktuelt. Det er derfor en strategisk metode å utvikle KPIer som retter seg mot de mest sannsynlige angrepsscenarioene, men likevel ha en sterk bevissthet knyttet til at hendelser som ikke omfattes av KPIene kan inntreffe.

6.2.3 Økonomi

Økonomi er også et aspekt som kan føre til at det ikke er samsvar mellom security-arbeidet og den reelle sikkerheten. Dersom nødvendige tiltak og løsninger ikke implementeres som følge av høye kostnader, så er det ifølge *informant 1 Avinor* lite samsvar mellom det som regelverket er rettet mot, og det som faktisk har noe med security å gjøre. Økonomiske aspekter som kan påvirke sikkerheten, kan også dreie seg om de ressursene som Avinor og Luftfartstilsynet besitter, i form av personell, kapasitet etc. Det er kritisk at Luftfartstilsynet har nok ressurser og kapasitet til å foreta hyppige og grundige inspeksjoner av lufthavnene, da Avinor primært definerer sikkerhetsnivået på bakgrunn av disse inspeksjonene. *Informant Luftfartstilsynet* slår fast at Luftfartstilsynet har gode økonomiske rammer, og nok kapasitet og ressurser til å foreta jevnlig og grundige inspeksjoner. Informanten understreker at EFTA sine revisjoner og tilsyn av Norge, aldri har avdekket at de økonomiske rammene eller kapasiteten til Luftfartstilsynet har vært dårlig. I tillegg må Avinor påse at det foreligger gode økonomiske rammer og kapasitet ved alle lufthavnene, for å sikre at security-arbeidet blir ivaretatt. Tilsynsrapportene viser enkelte eksempler på at dårlig bemanning har ført til avvik, for eksempel ved at et område ikke har blitt tilstrekkelig overvåket.

Dette delkapittelet har vist at en rekke variabler kan påvirke resultatene som Avinor mottar fra Luftfartstilsynets inspeksjoner. Til tross for at resultatene fra inspeksjonene forteller mye om sikkerhetssituasjonen på lufthavnene, forteller de ikke alt. Det er derfor behov for en usikkerhetsvurdering. En beskrivelse og erkjennelse av det foreligger usikkerhet utover de tallene som definerer sikkerhetsnivået. Tallene belyser «compliance» nivået med forordning 300/2008, men det tilsvarer ikke nødvendigvis det reelle sikkerhetsnivået.

6.3 Hvordan kan security-arbeidet bli mer proaktivt og risikobasert?

For å kunne være i forkant av terrorister og avsløre deres planer før de gjennomfører et angrep, vil det være behov for et proaktivt, fleksibelt og risikobasert sikkerhetssystem. Security-regimet i luftfarten har blitt kritisert for å være det motsatte. Forhåndsdefinerte og detaljerte regler vil kunne oppfattes som reaktive og lite i tråd med et usikkert og dynamisk trusselbilde, og terrorister kan legge deres planer utenom disse statiske tiltakene og barrierene. Nye regler blir lagt til i regelverket som følge av avvik, forsøk på eller reelle terroranslag som avdekker sårbarheter i dagens sikkerhetssystem. Det er kritisk at slike svakheter blir avdekket av sikkerhetspersonell, og ikke av terrorister. Likevel gir dagens security-regimet i luftfarten lite rom for at områder utenfor punktene i regelverket kan kontrolleres. Luftfartstilsynet og Avinor har i lys av dette slikt regime ikke ansvar for å påse hvorvidt sikkerhetstiltakene på lufthavnene er effektive og i tråd med trussellandskapet. Regimet bygger på en forutsetning om at aktørene i europeisk luftfart skal ha en tillit til at beslutningstakerne i EU har gjennomarbeidet en liste over punkter som vil føre til en robust og pålitelig sikkerhet. En slik praksis forutsetter derfor at beslutningstakerne i EU kontinuerlig oppdaterer denne listen, for å sørge for at reglene er tilpasset et samfunn og trussellandskap i stadig utvikling. En utfordring er likevel at siden prosessen med å endre regulering tar tid, legger ikke et slikt regime til rette for raske og effektive endringer i regelverket dersom trussellandskapet endres.

Informant SD er enig i at endringer i regelverket ofte kan ta tid. Det må forberedes et konkret forslag av EU kommisjonen før det legges frem, så må det diskuteres blant de involverte aktørene før det kan vedtas. Informanten påpeker at prosessen avhenger av hvor mye det haster og hvor stor regelverksendring det omhandler, men at det er utfordrende å fatte effektive beslutninger i EU organet. Det er derfor behov for å anvende andre fremgangsmåter når effektive og fleksible beslutninger skal tas. Informantene fra Luftfartstilsynet og SD trekker frem muligheten for å anvende den norske securityforskriften for å kunne foreta slike fleksible og effektive beslutninger. KPIene i EU-regelverket er minstestandarden, og en rekke andre tiltak kan iverksettes for å gjøre regelverket strengere for å møte en trussel.

Teoribidragene knyttet til kjennetegn ved terrorisme tilsier likevel at en slik tankegang kan føre til en slags falsk trygghet. Kunnskap og informasjon om en konkret trussel eller et generelt økt trusselbilde må foreligge, før Luftfartstilsynet, Avinor og politiet eventuelt iverksetter ekstra strenge tiltak utover KPIene i regelverket. Et sentralt kjennetegn ved terrorisme er derimot at terrorister kan slå til brått uten noen form for advarsler. Det kan derfor være vanskelig å oppdage tidlige faresignaler fra terrorister, noe som kan føre til at de

ekstra strenge tiltakene ikke rekker å bli iverksatt før et angrep finner sted. Av den grunn er det kritisk at de grunnleggende KPIene i regelverket som til enhver tid er gjeldende, er robuste nok til å stanse og oppdage eventuelle terrorister.

Et risikostyringsregime, definert av Hopkins (2011), vil kunne føre til at reglene i større grad er tilpasset et trusselbilde i kontinuerlig endring. Et slikt regime bygger på antakelsen om at organisasjonene selv har den beste forutsetningen for å identifisere og håndtere risiko, og at slik desentralisert styring kan føre til et mer risikobasert, fleksibelt og proaktivt security-arbeid. En utfordring med et slikt regimet er derimot at det ikke vil gi klare retningslinjer for hva som er et passende sikkerhetsnivå, eller noen referanseverdier for når en lufthavn har oppnådd det «riktige» sikkerhetsnivået. Det vil være vanskelig for lufthavnene å avgjøre hvor alvorlig trusselen for tilsiktede handlinger faktisk er. Det vil derfor være utfordrende for hver enkelt lufthavn å tilpasse deres egen sikkerhet i et slikt trussellandskap som er preget av en stor grad av usikkerhet. Et slikt regime vil dermed ikke gi en generell god veiledning til dem som står overfor disse beslutningene, og det vil være vanskelig å avgjøre om risikoen er akseptabel eller ikke. I tillegg vil utveksling av security informasjon mellom lufthavnene være vanskelig, da slik informasjon i stor grad er klassifisert. Dette vil også svekke lufthavnenes evner til å foreta beslutninger på et godt grunnlag.

I tillegg vil det være svært utfordrende for lufthavner å ha den nødvendige oversikten over trusselbilde i en globalisert og kompleks industri som luftfarten. Slike risikoer må ifølge informanten fra Luftfartstilsynet håndteres gjennom et utstrakt samarbeid mellom ulike nivåer av aktører, for på den måten å ha nok kunnskap og oppdatert informasjon om trusselbilde. Et europeisk samarbeid hvor flere aktører deltar i kunnskapsutvekslingen og bidrar med informasjon og innspill, for å utvikle tiltak og løsninger, anses derfor som en pålitelig form for risikostyring. Risikostyringsregimet vil derfor være utfordrende for luftfarten.

7. Konklusjon

I denne studien har security-arbeidet i sivil luftfart stått i sentrum. Formålet har vært å undersøke sammenhengen mellom de KPIene som Avinor benytter for å definere sikkerhetsnivået på deres lufthavner, og hvordan disse KPIene faktisk påvirker sikkerhetsnivået. Min tolkning og mine funn viser at det foreligger en delvis sammenheng, men at sammenhengen er ufullstendig og ikke sterk nok til at sikkerhetsnivået utelukkende kan defineres på dette grunnlaget. Dagens KPIer i forordning 300/2008 er utarbeidet på bakgrunn av historiske hendelser, grundige risiko og trusselvurderinger, etterretning og enighet blant eksperter og beslutningstakere. KPIene er derfor robuste kilder som retter seg mot de fleste angrepsscenarioer som truer dagens flysikkerhet. En slik «compliance» fokusert fremgangsmåte forutsetter imidlertid at regelverket monitorerer og beskriver alle mulige angrepsscenarioer og risikoer som foreligger mot luftfarten. Historien har vist at terrorister gjentatte ganger har vært i stand til å overliste de etablerte sikkerhetstiltakene i luftfarten. Til tross for at dagens KPIer i større grad enn tidligere er utviklet på bakgrunn av risiko og trusselvurderinger, så ligger det i terroristenes natur å utvikle og eksperimentere med nye metoder som kan overliste ethvert sikkerhetssystem. Det er derfor sannsynlig at terrorister også i fremtiden vil kunne klare å finne hull og veier rundt sikkerhetsbarrierene på lufthavnene.

På det grunnlaget vil det derfor være upålitelig og feilaktig å utelukkende definere sikkerhetsnivået i luftfarten på bakgrunn av samsvar med regelverket. Usikkerhet, tilfeldigheter og metodiske svakheter kan også påvirke Luftfartstilsynets inspeksjoner, noe som igjen kan føre til at resultatene av inspeksjonene gir feilaktige indikasjoner på det reelle sikkerhetsnivået. En usikkerhetsvurdering og erkjennelse av at det foreligger usikkerhet utover de tallene som definerer sikkerhetsnivået, er derfor helt avgjørende. Det vil bidra til en økt bevissthet rundt at de resultatene som Luftfartstilsynet gir i etterkant av deres inspeksjoner, ikke nødvendigvis er absolutte sannheter på det faktiske sikkerhetsnivået. I tillegg er det avgjørende å ta stilling til at latente forhold kan ha påvirkning på security-arbeidet og sikkerhetsnivået på lufthavnene. Dårlig design av regelverket, svakt og ufullstendig tilsyn, uoppdagede produksjonsfeil, kompliserte prosedyrer og mangelfull opplæring er eksempler på slike latente forhold som kan svekke sikkerhetsnivået. Slike forhold kan være til stede over lang tid, og vil være usynlige mekanismer som svekker det

reelle sikkerhetsnivået. Slike mekanismer vil ikke nødvendigvis bli avdekket under tilsynene, noe som illustrerer forskjellen mellom «compliance» nivå og sikkerhetsnivå.

På bakgrunn av denne studiens funn, kan det derfor slås fast at det er forskjell mellom «compliance» nivå og sikkerhetsnivå. Ukjente variabler kan påvirke påliteligheten til KPIene, i tillegg til at ulike trusler ikke monitoreres av de gjeldene KPIene. Det kan derfor være direkte misvisende å basere sikkerhetsnivået i luftfarten på bakgrunn av samsvarsgraden med regelverket. En måte å redusere en slik usikkerhet som foreligger utover de resultatene som Luftfartstilsynet formidler, er å fokusere på organisasjonsprosesser som gir høy pålitelighet. Individuell og kollektiv «mindfulness» vil føre til at security-arbeidet vil inneholde en større grad av bevissthet rundt at regelverket ikke dekker alt, at barrierene og tiltakene kan inneholde hull og at security-arbeidet er en kontinuerlig prosess som aldri blir fullført. På den måten vil security-systemet på lufthavnene være mer forberedt, bevisste og tilpasningsdyktige ovenfor uventede situasjoner og hendelser som ikke dekkes av KPIene i forordning 300/2008.

7.1 Videre forskning

Konklusjonen fra denne studien viser at det europeiske security-regimet i luftfarten innebærer en «compliance» fokuset tilnærming hvor sikkerhetsnivået på europeiske lufthavner defineres på bakgrunn av samsvar med regelverket. Denne studien er derfor generaliserbar for det europeiske luftfartssystemet. I en større studie ville en nærmere undersøkelse av hvordan KPIene samsvarer med faktiske forhold vært interessant, og hvorvidt et risikostyringsregime kunne ha ført til et mer proaktivt og risikobasert security-arbeid. I tillegg ville det ha vært interessant å ha studert forskjellene mellom EU-statene, og hvordan security-regime har ulike implikasjoner for ulike stater og lufthavner. Det er EU sitt ansvar å utvikle et regelverk som i størst mulig grad samsvarer med det reelle trusselbilde mot luftfarten. En studie knyttet opp imot hvordan EU arbeider for å utvikle og justere regler og prosedyrer, hadde vært en opplysende og viktig studie. En studie knyttet til hvordan pålitelighet i større grad kan bygges inn i systemet, og hvilke følger det ville ført med seg, hadde også vært interessant.

Litteraturliste

- Aven, T., Boyesen, M., Njå, O., Olsen, K. H. & Sandve, K. (2004). *Samfunnssikkerhet*. Oslo: Universitetsforlaget
- Aven, T. & Renn, O. (2010). *Risk Management and Governance. Concepts, Guidelines and Applications*. London: Springer
- Aven, T. (2013). *Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts*. Reliability Engineering & System Safety, 119 (0), 229-234.
- Aven, T. & B.S. Krohn (2013). *A new perspective on how to understand, assess and manage risk and the unforeseen*. Reliability Engineering and System Safety. **121**: s. 1-10.
- Aven, T. (2014). *Risk, surprises and black swans. Fundamental ideas and concepts in risk assessment and risk management*. London: Routledge.
- Avinor. (2020, 28. oktober). *Plan for virksomheten 2020-2021*.
https://avinor.no/globalassets/_konsern/om-oss/samfunnsoppdraget/avinors-10-plan-2020-2021.pdf
- Avinor. (2021). *Trafikkstatistikk*. <https://avinor.no/konsern/om-oss/trafikkstatistikk/arkiv>
- Babbie, E. (2010). *The Practice of Social Research*, 12. utgave. Wadsworth, Cengage Learning.
- Baldwin, R. & Cave. M. (1999). *Understanding regulation: theory, strategy, and practice*. Oxford: Oxford University Press.
- Beck, U. (1992). *Risk society. Towards a new modernity*. London: Sage.
- Blaikie, N. (2019). *Designing social research* (3. utg.). Cambridge: Polity Press.
- Bryman, A. (2006). *Mixed Methods Research*. Volume 1. SAGE Publications, London.
- Brynjar, L., Berg, J. K., Leraand, D. & Stenersen, A. (2017). *Terrorisme*. Store norske leksikon. <https://snl.no/terrorisme>
- DSB. (2014). *Nasjonalt risikobilde 2014*. Tønsberg: Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/nrb_2014.pdf

- ECAC. (2021, 26. februar). *History*. European civil aviation conference. <https://www.ecac-ceac.org/about-ecac/history>
- Eede, G. V. D. (2009). *Two Cases in High Reliability Organizing: a Hermeneutic Reconceptualization*. Universiteit Van Tilburg.
- Engen, O. A., & Olsvik, E. A. (2010). *Security in civil aviation post 9/11* (S. 2323-2329). Boca Raton, Fla.: CRC Press.
- Engen, O. A., Kruke, B. I., Olsen, O. E., Olsen, K. H., Lindøe, P. & Pettersen, K. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm.
- European Parliament & European Council. (2002). *Establishing common rules in the field of civil aviation security*. (EC) No 2320/2002. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:355:0001:0 021:EN:PDF>
- Flage R. & Aven T. (2009). *Expressing and communicating uncertainty in relation to quantitative risk analysis*. R&RATA # 2(13) part 1 (Vol. 2).
- Forsvarsdepartementet. (2011) *Forskrift om objektsikkerhet* (2011). LOV-1998-03-20-10-§17.
- Frederickson, H. G., & LaPorte, T. R. (2002). *Airport security, high reliability, and the problem of rationality*. Public Administration Review, 62, 33-43.
- Gillen, D. D., & Morrison, D. W. G. (2014). *Economic of Aviation Security: Design, Governance, Performance, Financing and Policy*. Journal of Air Transport Management.
- Grønmo, S. (2004). *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget.
- Halvorsen, K. (2008). *Å forske på samfunnet- En innføring i samfunnsvitenskapelig metode*. Cappelen Damm Akademisk.
- Hopkins, A. (2011). *Risk-management and rule-compliance: Decision-making in hazardous industries*. Safety Science, 49(2), 110-120.
<http://dx.doi.org/10.1016/j.ssci.2010.07.014>.
- Hutter, B. (2010). *Anticipating risks and organising risk regulation*. Cambridge: Cambridge University Press.
- ICAO. (2021, 21. februar). *Annex 17*. Security and facilitation.
<http://www.icao.int/Security/SFP/Pages/Annex17.aspx>
- IRGC. (2017). *Introduction to the IRGC Risk Governance Framework, revised version*. Lausanne: EPFL International Risk Governance Center.

- Irish Aviation Authority & Aviasolution. (2004). *Study on Civil Aviation Security Financing*. Report requested by the European Parliament and Council. Study No: TREN/F3/51-2002.
https://ec.europa.eu/transport/sites/default/files/themes/security/studies/doc/2004_09_study_financing_aviation_security_en.pdf
- Jacobsen, D. I. (2000) *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. Kristiansand. Høyskoleforlaget.
- Jore, S. H. (2015). *Challengers of Building Societal Resilience through Organizational Security Risk Management, Working on Safety 2015*, Portugal.
- Jore, S. H. (2017). *The conceptual and scientific demarcation of security in contrast to safety*. European Journal of Security Science.
<https://link.springer.com/content/pdf/10.1007/s41125-017-0021-9.pdf>
- Jore, S. H. (2019a). *Standardization of Terrorism Risk Analysis -A Means or an Obstacle to Achieve Security?* I Olsen, O.E., Juhl, K.V., Lindøe, P. and Engen, O.A. (eds). *Standardization and Risk Governance: A Multi-Disciplinary Approach*. Routledge.
<https://www.taylorfrancis.com/books/e/9780429290817>
- Jore, S. H. (2019b). *The Multifaceted Aspect of Uncertainty – the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism*. Proceedings of the 29th European Safety and Reliability Conference. Edited by Michael Beer and Enrico Zio Copyright c 2019 European Safety and Reliability Association. Research Publishing, Singapore. DOI: 10.3850/978-981-11-2724-3_0622-cd
- Kvale, S., & Brinkmann, S. (2012). *Det kvalitative forskningsintervju* (2. utg.). Oslo: Gyldendal Norsk Forlag.
- Lindøe, P. (2012). *Risikoforståelse og myndighetskontroll: Risiko og Tilsyn*. Oslo: Universitetsforlaget AS.
- Lindøe, P. H., Kringen, J. & Braut, G. S (2015). *Risiko og tilsyn*. Oslo: Universitetsforlaget.
- Luftfartstilsynet. (2017, 5. juli). *Forberedt på terror*. <https://luftfartstilsynet.no/om-oss/nyheter/nyheter-2017/forberedt-pa-terror/>
- Luftfartstilsynet. (u.å). *Regelverksoppbygging securityregelverket*. Hentet 21. februar 2021 fra <https://luftfartstilsynet.no/aktorer/security/regelverk-security/>
- Morone, J. G., & Woodhouse, E. J. (1986). *Averting catastrophe: Strategies for regulating risky technologies*. Berkeley: University of California Press.

- Nasjonal sikkerhetsmyndighet. (2017). *Risiko 2017. Risiko og sårbarheter i en ny tid*.
https://nsm.no/getfile.php/133726-1592915950/Demo/Dokumenter/Rapporter/nsm_risiko_2017_lr_0404_enkelts_v3.pdf
- National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. <https://govinfo.library.unt.edu/911/report/911Report.pdf>
- NOU 2006: 6. (2006). *Når sikkerheten er viktigst- beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Justis- og beredskapsdepartementet.
<https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf>
- NOU 2016: 19. (2016). *Samhandling for sikkerhet - beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid*. Forsvarsdepartementet.
<https://www.regjeringen.no/contentassets/816d557c6ab24493a1101837cc2e1cf8/nou-2016-19-samhandling-for-sikkerhet.pdf>
- Nordstoga, A. (2009, 8. september). *Historien om hvorfor det ble forbudt å ta med væsker på fly*. Aftenposten. <https://www.aftenposten.no/verden/i/11dzG/historien-om-hvorfor-det-ble-forbudt-aa-ta-med-vaesker-paa-fly>
- Notaker, H. (2019, 31. juli). Terrorangrepet 11. september 2001. Store norske leksikon.
https://snl.no/Terrorangrepet_11._september_2001
- Official Journal of the European Union. (2015). *Regulation 300/2008*. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1998&from=EN>
- Olsvik, E. A. (2015). *Challenges of Aviation Security regulation in Norway post 9/11*. (Doktorgradsavhandling, Universitetet i Stavanger). UiS Brage.
https://uis.brage.unit.no/uis-xmlui/bitstream/handle/11250/2360216/Elise_Anonby_Olsvik.pdf?sequence=1&isAllowed=y
- Petterson, K. & Schulman, P. (2019). *Drift, adaption, resilience and reliability. Toward clarifying some important organizational concepts*. Safety Science.
<http://dx.doi.org/10.1016/j.ssci.2016.03.004>
- Poole, R. (2008). *Toward Risk-Based Aviation Security Policy*. OECD/ITF Round Table of 11-12 December 2008 on Security, Risk Perception and Cost-Benefit Analysis.
<https://www.itf-oecd.org/sites/default/files/docs/dp200823.pdf>
- PST. (2021). *Nasjonal trusselvurdering 2021*. Politiets sikkerhetstjeneste.
https://www.pst.no/globalassets/artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/ntv_2021_final_web_1802-1.pdf

- Reason, J. (1997). *Managing the Risk of Organizational Accidents*. United Kingdom: Taylor & Francis Ltd.
- Renn, O. (2008). *Risk Governance Coping with Uncertainty in a Complex World*. London/New York: Routledge.
- Rochlin, G. (1993). *Defining "High Reliability" Organisations*. In K. H. Roberts (Ed.), *New challenges to understanding organizations* (s. 22). New York: Macmillan.
- Roe, E. & Schulman, P. (2008). *High reliability management*. Stanford, California: Stanford University Press.
- Sagan, S. D. (1993). *The Origins of Accidents The limits of safety: organizations, accidents, and nuclear weapons* (s. 11-52). Princeton, N.J.: Princeton University Press.
- Samferdselsdepartementet. (1993). *Lov om luftfart (Luftfartsloven)*.
<http://www.lovdatabasen.no/all/nl-19930611-101.html>
- Samferdselsdepartementet. (2017). *Verksemda til Avinor AS* (Meld. St. 30 (2016-2017)).
<https://www.regjeringen.no/no/dokumenter/meld.-st.-30-20162017/id2548200/?ch=2>
- Samferdselsdepartementet. (2021, 8. mars). Om samferdselsdepartementet. Regjeringen.
<https://www.regjeringen.no/no/dep/sd/org/id815/>
- Schulman, P. R. (2020). *Safety and security: Managerial Tensions and Synergies*. I C. Bieder & K. G. Pettersen (Red.), *The Coupling of Safety and Security: Exploring Interrelations in Theory and Practice* (s. 87-95). Springer Open.
- Sutcliffe, K. M., Vogus, T. J. & Dane, E. (2016). *Mindfulness in Organizations: A Cross-Level Review*. Vanderbilt University.
- Thagaard, T. (2018). *Systematikk og innlevelse: En innføring i kvalitative metoder* (5. utg). Oslo: Fagbokforlaget.
- Tønnessen, T. H. (2008). *Luftfarten som terrormål*. Forsvarets forskningsinstitutt (FFI).
<https://publications.ffi.no/nb/item/asset/dspace:3408/08-00157.pdf>
- Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). *Organizing for High Reliability: Processes of Collective Mindfulness*. *Research in Organizational Behavior*, 21, 81-123.
- Weick, K. E., & Sutcliffe, K. M. (2001). *Managing the unexpected: assuring high performance in an age of complexity*. San Francisco, California.: Jossey-Bass.

Weinberg, L., Pedahzur, A. & Hirsch-Hoefler, S. (2004). *The Challenges of Conceptualizing Terrorism, Terrorism and Political Violence*, 16:4, 777-794, DOI: 10.1080/095465590899768

Wildavsky, A. (1988). *Searching for safety*. New Brunswick, N.J.: Transaction Books.

Vedlegg 1: Intervjuguide Luftfartstilsynet

Jeg skriver for tiden min masteroppgave i samfunnssikkerhet ved UiS, hvor jeg samarbeider med security avdelingen i Avinor. Tema for oppgaven handler om hvordan Avinor arbeider med å forhindre anslag mot luftfarten, og videre hvordan Avinor definerer og evaluerer sitt eget sikkerhetsnivå. Avinor definerer primært sitt sikkerhetsnivået på bakgrunn av de inspeksjonene som blir gjort av Luftfartstilsynet, hvor Luftfartstilsynet fører tilsyn ved at Avinor samsvarer med EU-regelverket for security. De resultatene og tilbakemeldingene som Avinor får i etterkant av inspeksjonene, bruker de som styringsindikatorer for å studere trender, utviklinger og svakheter i eget sikkerhetssystem, og det er på bakgrunn av disse data/KPI at de definerer om deres sikkerhet er god eller ikke.

På bakgrunn av dette, er følgende problemstilling utarbeidet:

Er det en sammenheng mellom de KPI som Avinor benytter for å definere deres sikkerhetsnivå, og hvordan disse KPIene faktisk påvirker sikkerhetsnivået?

Ifølge Avinor, så er det kun en antakelse at det finnes en slik sammenheng, men det er aldri bevist.

Formålet med oppgaven er derfor å undersøke fordeler og ulemper ved å definere sikkerheten på bakgrunn av compliance med regelverk. Kan en slik tilnærming anses som reaktiv og lite risikobasert, da historien har vist at regelverket i luftfarten ofte er blitt endret i etterkant av avvik, forsøk på angrep eller reelle terroranslag. Bør det i større grad tas hensyn til at terrorister kan finne hull i regelverket, og at sikkerhetssystemet derfor bør være mer fleksibelt og i tråd med et endret trusselbilde, for på den måten å være i forkant av eventuelle terrorister. Bør nasjonale og lokale trusselvurderinger, lokal kunnskap og desentralisert styring få en økt rolle i security arbeidet i luftfarten, slik man har sett i andre sektorer som for eksempel innen petroleumsbransjen med internkontroll ol?

1. Hva er Luftfartstilsynet sin rolle og ansvarsområder i forbindelse med security arbeid i norsk luftfart?
2. Hvilke inspeksjonsmetoder anvender Luftfartstilsynet for å kontrollere at Avinor samsvarer med EU-regelverket?
3. Når Luftfartstilsynet foretar inspeksjoner av Avinors lufthavner, er det kun punktene i EU-regelverket som blir inspisert, eller er det også andre lover og regler som inspiseres, som for eks nasjonale bestemmelser?
4. Hvilket forhold og påvirkningskraft har Luftfartstilsynet og andre norske aktører til beslutningstakerne innen aviation security i EU?
5. Er det forordning nr. 300/2008 som er det gjeldende EU-regelverket for security i luftfarten i dag, eller er det et mer oppdatert regelverk som gjelder?
6. I etterkant av inspeksjonene på Avinors lufthavner, gir Luftfartstilsynet i tilsynsrapportene en karakter på graden av samsvar med regelverket (score 1-5). Tidligere ga Luftfartstilsynet kun tilbakemelding om avvik, mens nå kommuniseres

samtligge av de punktene som ble inspisert, også de punktene hvor det var samsvar med krav. Hva er bakgrunnen for dette?

7. Luftfartstilsynets arbeid er underlagt kontroll og inspeksjon av EFTA Surveillance Authority (ESA). Hvordan foregår denne inspeksjonen, og omtrent hvor ofte blir Luftfartstilsynet inspisert?
8. Hva er Luftfartstilsynets ståsted rundt påstanden om at EU-regelverket kan oppfattes som reaktivt og lite risikobasert, da regelverket ofte endres i etterkant av uønskede hendelser?
9. I hvilken grad anser Luftfartstilsynet at regelverket er fleksibelt og proaktivt nok til å være i forkant av eventuelle terrorister? Tar det lang tid før endringer i regelverket kan tre i kraft, og er det vanskelig å påvirke og få gjennomslag for endringer i regelverket? Kan regelverket anses for å være et levende dokument?
10. Hvordan inkorporeres trusselvurderinger fra politi, etterretning og andre aktører i det gjeldende securityregelverket? Vil nasjonale eller lokale trusselvurderinger kunne føre til midlertidige endringer i securityarbeidet, eller er det slik at regelverket uansett skal følges slavisk?
11. Anser Luftfartstilsynet at samsvar med regelverket vil føre til en robust og pålitelig sikkerhet ved norske lufthavner?
12. Norge bruker om lag 1,2 milliarder kroner hvert år på å screene passasjerer og bagasje, til tross for et relativt lavt trusselbilde. Blir kostnadseffektiviteten rundt security arbeidet i luftfarten vurdert og evaluert, eller foreligger det en felles enighet om at «security arbeidet i luftfarten kan koste hva det vil, så lenge det fører til at vi samsvarer med EU-regelverket og dermed forblir en del av One-Stop Security regime»?
13. Hva er Luftfartstilsynets tanker rundt påstanden: «EU-regelverket er konstruert for store internasjonale flyplasser, og utfordringene var store da samme regelverk ble innført på små flyplasser i Norge»?
14. En av de viktigste sikkerhetsventilene vi har, er våkne operatører som ser meningen med jobben sin. Tidligere forskning på området har vist at flere informanter som jobber på små flyplasser i Norge, har uttrykt at jobben til tider oppleves som meningsløs og at reglene er lite tilpasset de lokale forholdene. Reglene kan også til tider virke malplassert. Hvordan stiller Luftfartstilsynet seg til slike uttalelser?
15. Har det vært diskutert innad i bransjen om det bør utvikles et annet regelverk for de små lufthavnene i Norge og i EU, for på den måten å sørge for at regelverket i større grad samsvarer med lokale forhold (lavt antall ansatte, lite flybevegelser ol).
16. Mens man i andre bransjer jobber mot mindre detaljstyring der tiltakenes effektivitet skal dokumenteres, mener noen at securityregimet i luftfarten er gammeldags og utdatert. Kan sikkerhetsregimet anses som overdrevet og for detaljstyrt, og hvor effektivt er det egentlig i en norsk sammenheng?

17. Avinor definerer primært sitt eget sikkerhetsnivå på bakgrunn av de tilbakemeldingene de får fra Luftfartstilsynets inspeksjoner. Dermed legges det et stort ansvar på at Luftfartstilsynet foretar pålitelige, hyppige og grundige inspeksjoner av Avinor. Har Luftfartstilsynet nok kapasitet til å foreta hyppige og grundige tilsyn? Har det blitt vurdert å legge et større ansvar om internkontroll på Avinor sine skuldre, slik at også Avinor fører tilsyn på deres egne enheter?
18. Kan regelverket være til hinder for rasjonell menneskelig dømmekraft, for eksempel i sikkerhetskontrollen hvor profilering ikke er lov? Hvis en mistenkelig og stresset person blir screenet i sikkerhetskontrollen, men kontrollen ikke gir utslag for noen ulovlige gjenstander eller andre brudd på regelverket, så har de ansatte ikke myndighet til å avhøre eller undersøke personen ytterligere. Bør det være en prosedyre som sier det at ved avvikende oppførsel, så skal det gjennomføres en skjønnsmessig vurdering? Bør det være rom for at sunn fornuft og rasjonelle løsninger bør gå foran de detaljerte bestemmelsene i regelverket?

Vedlegg 2: Intervjuguide informant 2 Avinor

1. Kan du kort si noe om din rolle og dine ansvarsområder som lufthavnoperatør/sjef?
2. Omtrent hvor mange ansatte arbeider med security relaterte oppgaver på lufthavnen?
3. Hvor ofte blir lufthavnen inspisert av Luftfartstilsynet?
4. Hvor ofte foretar Avinor egne security inspeksjoner på lufthavnen?
5. Dersom Luftfartstilsynet avdekker avvik under inspeksjonen(e), hvordan arbeider du/dere med avviket? Blir det iverksatt tiltak umiddelbart for å lukke avviket?
6. I hvilken grad har lufthavnen rom for å foreta egne beslutninger og innføre egne tiltak knyttet til security? Må alt være 100% i tråd med EU regelverket (forordning 300/2008)?
7. Anser du dagens EU regelverk for security for å være egnet og treffende for de lokale forholdene på lufthavnen? Eller anser du regelverket for å være for omfattende for lufthavner på størrelse med din lufthavn?
8. Hvordan vil du si at kommunikasjonen og samarbeidet med Luftfartstilsynet er? Er tilsynsrapportene og tilbakemeldingene tydelige og enkle å forstå og rette seg etter?
9. Er det noen lokale faktorer på lufthavnen som øker risikoen for terroranslag?
10. Anser du Luftfartstilsynets inspeksjonsmetodikk for å være god? Er det noe ved metodikken som kunne blitt gjort annerledes eller bedre?

11. Synes du at tilsynsaktivitet og kontroll av samsvar med et detaljert regelverk er den beste måten å arbeide med security i luftfarten på? Kunne dette blitt gjort på en annen og bedre måte?

12. En av de viktigste sikkerhetsventilene vi har, er våkne operatører som ser meningen med jobben sin. Tidligere forskning på området har vist at flere informanter som jobber på små flyplasser i Norge, har uttrykt at jobben til tider oppleves som meningsløs og at reglene er lite tilpasset de lokale forholdene. Reglene kan også til tider virkemalplassert. Hvordan stiller du deg til slike uttalelser, og hvordan sørger dere for at operatørene er årvåkne?

13. Hva er ditt ståsted rundt påstanden om at EU-regelverket kan oppfattes som reaktivt og lite risikobasert, da regelverket ofte endres i etterkant av uønskede hendelser?

14. Hvordan inkorporeres trusselvurderinger fra politi, etterretning og andre aktører i det gjeldende security regelverket? Vil nasjonale eller lokale trusselvurderinger kunne føre til midlertidige endringer i securityarbeidet, eller er det slik at regelverket uansett skal følges slavisk?

15. Hva er dine tanker rundt påstanden: «EU-regelverket er konstruert for store internasjonale flyplasser, og utfordringene var store da samme regelverk ble innført på små flyplasser i Norge»?

16. Har det vært diskutert innad i bransjen om det bør utvikles et annet regelverk for de små og mellomstore lufthavnene i Norge, for på den måten å sørge for at regelverket i større grad samsvarer med lokale forhold (lavt antall ansatte, lite flybevegelser ol).

Vedlegg 3: Intervjuguide Samferdselsdepartementet

1. Hvordan arbeider Samferdselsdepartementet for å sikre at norsk luftfart ikke skal bli rammet av forsettlig og ondsinnede angrep som et terrorangrep?
2. Luftfartstilsynet har en kritisk rolle i tilsyn og inspeksjon av norsk luftfart. Hvordan sikrer departementet at Luftfartstilsynet har de nødvendige midlene og kompetansen for å utføre pålitelige og hyppige inspeksjoner av luftfarten (i forbindelse med security)?
3. Security innen norsk luftfart er underlagt et strengt og detaljert felleseuropeisk regelverk. Som et ikke EU-medlemsland, hva er bakgrunnen for at også Norge følger dette regelverket?
4. Hvilken påvirkningskraft og rolle har Norge i utviklingen av dette regelverket?

5. Hva er Samferdselsdepartementet sitt ståsted rundt påstanden om at EU-regelverket kan oppfattes som reaktivt og lite risikobasert, da regelverket ofte endres i etterkant av uønskede hendelser?
6. I hvilken grad anser departementet at regelverket er fleksibelt og proaktivt nok til å være i forkant av eventuelle terrorister? Tar det lang tid før endringer i regelverket kan tre i kraft, og er det vanskelig å påvirke og få gjennomslag for endringer i regelverket? Kan regelverket anses for å være et levende dokument?
7. Hvordan inkorporeres trusselvurderinger fra politi, etterretning og andre aktører i det gjeldende security regelverket? Vil nasjonale eller lokale trusselvurderinger kunne føre til midlertidige endringer i securityarbeidet, eller er det slik at regelverket uansett skal følges slavisk?
8. Norge bruker om lag 1,2 milliarder kroner hvert år på å screene passasjerer og bagasje, til tross for et relativt lavt trusselbilde. Blir kostnadseffektiviteten rundt security arbeidet i luftfarten vurdert og evaluert, eller foreligger det en felles enighet om at «security arbeidet i luftfarten kan koste hva det vil, så lenge det fører til at vi samsvarer med EU-regelverket og dermed forblir en del av One-Stop Security regime»?
9. Hva er departementets tanker rundt påstanden: «EU-regelverket er konstruert for store internasjonale flyplasser, og utfordringene var store da samme regelverk ble innført på små flyplasser i Norge»?
10. En av de viktigste sikkerhetsventilene vi har, er årvåkne operatører som ser meningen med jobben sin. Tidligere forskning på området har vist at flere informanter som jobber på små flyplasser i Norge, har uttrykt at jobben til tider oppleves som meningsløs og at reglene er lite tilpasset de lokale forholdene. Reglene kan også til tider virke malplassert. Hvordan stiller Samferdselsdepartementet seg til slike uttalelser?
11. Har det vært diskutert om det bør utvikles et annet regelverk for de små lufthavnene i Norge og i EU, for på den måten å sørge for at regelverket i større grad samsvarer med lokale forhold (lavt antall ansatte, lite flybevegelser ol).
12. Mens man i andre bransjer jobber mot mindre detaljstyring der tiltakenes effektivitet skal dokumenteres, mener noen at securityregimet i luftfarten er gammeldags og utdatert. Kan sikkerhetsregimet anses som overdrevet og for detaljstyrt, og hvor effektivt er det egentlig i en norsk sammenheng?
13. Hvordan samarbeider Norge med EU og andre stater knyttet til trusselinformasjon, etterretning etc i forbindelse med security i luftfarten?
14. Har det blitt diskutert i departementet om det bør legges mer ansvar om internkontroll på Avinor som operatør av norske lufthavner, for på denne måten å oppnå en mer desentralisert styring?

Vedlegg 4: Forordning 300/2008

- 1.1.1 **Grenser.** Grenser mellom landside, flyside, sikkerhetsbegrensede områder og kritiske deler. Avgrensede områder skal være tydelig identifiserbare på hver flyplass for å muliggjøre passende sikkerhetstiltak i hvert av disse områdene. Det skal være fysisk hindring mellom landside og flyside, som nekter en person uautorisert tilgang.
- 1.1.2 **SRA områder (security restricted areas).** Området på flyplassen hvor det kun er screenede passasjerer som skal ut å fly som har tilgang. I SRA området skal all bagasje og alle gjenstander vært gjennomsoekt og kontrollert i sikkerhetskontrollen. Dersom uvedkommende har hatt tilgang til SRA området, skal det umiddelbart foretas et sikkerhetssøk for å gjennomsoeke området for forbudte gjenstander. Dette gjelder ogsa for fly som står parkert i området.
- 1.1.3 **CP områder (critical parts of security restricted areas).** Slike kritiske deler skal etableres på flyplasser der mer enn 40 personer har ett lufthavn ID-kort som gir tilgang til security restricted areas. Kritiske deler er alle deler av en flyplass hvor bare screenede passasjerer og bagasje har tilgang.
- 1.2.1 **Tilgang til flyside.** Tilgang til flyside skal bare godkjennes hvis personer eller kjøretøy har en legitim grunn til å være der. Flyside viser til hele området hvor flyene står parkert. For å ha tilgang skal personer ha gyldig autorisasjon. Kjøretøy må ha gyldig bevis.
- 1.2.2 **Tilgang til CP.** Tilgang til CP områder skal bare gis personer og kjøretøy som har en legitim grunn til å være der. For å få tilgang til området, skal en person kunne fremvise en av følgende autorisasjoner: et gyldig boardingkort, et gyldig besetnings ID kort, et gyldig lufthavnansatt ID kort, et gyldig nasjonalt myndighetskort eller et gyldig myndighetskort fra en annen nasjon som er godkjent av den aktuelle nasjonale myndigheten. Kjøretøy skal ogsa ha gyldig bevis.
- 1.2.3-5 **ID kort for lufthavn.** Et besetningsidentifikasjonskort til en som er ansatt av et flyselskap, og ett lufthavn ansatt ID kort skal bare utstedes til personer som har et operativt behov og som har blitt bakgrunnsjekket. Identifikasjonskortene skal utstedes for en periode som ikke overstiger fem år. Identifikasjonskortet skal umiddelbart returneres til den utstedende enheten på: forespørsel fra den utstedende enheten, ved avslutning av ansettelsen, ved arbeidsbytte, ved endring av behovet for å ha tilgang til områder som det er gitt autorisasjon til, ved utløp av kortet.
- 1.2.4 **Tilleggskrav ID kort for besetningsmedlemmer.** ID-kortet skal inneholde innehaverens navn og fotografi, navnet på flyselskapet, ordet «crew» og utløpsdato.
- 1.2.5 **Tilleggskrav ID kort lufthavn ansatte.** ID kortet skal inneholde innehaverens navn og fotografi, navn på arbeidsgiver, navn på den utstedende enheten eller lufthavnen, områdene som innehaveren har tilgang til og utløpsdato. For å forhindre misbruk ID-kort skal det være et system som skal sikre at forsøk på bruk av kort som er stjålet, tapt eller som ikke er blitt returnert blir oppdaget.
- 1.2.6 **Innkjøringsbevis for kjøretøy.** Et kjøretøy bevis skal bare utstedes der det er etablert et operativt behov. Beviset skal være spesifikt for kjøretøyet, og vise: områdene det er autorisert til å ha tilgang til og utløpsdato.
- 1.2.7 **Eskortering/ledsagning.** Besetningen fra et flyselskap, bortsett fra de som har ett gyldig lufthavn ID-kort, skal til enhver tid ledsages når de er i SRA områder, unntatt: områder der passasjerer kan være tilstede, områder i umiddelbar nærhet av flyet de har ankommet fra eller skal ha avgang fra, og områder som er utpekt for besetningsmannskap. En ledsager skal ha et gyldig ID kort, være autorisert til å eskortere i SRA områder, ha den eller de eskorterte

- personene i direkte synsvidde til enhver tid og sikre med rimelighet at ingen sikkerhetsbrudd begås av personen(e) som blir eskortert.
- 1.3.1 **Sikkerhetskontroll av andre enn passasjerer.** Screening av andre enn passasjerer skal utføres på samme måte som for henholdsvis passasjerer og håndbagasje. Gjenstander som er oppført og godkjent skal slippes igjennom sikkerhetskontrollen for å utføre oppgaver som er essensielle for drift av flyplassanlegg eller fly.
 - 1.3.2 **Særlig fremgangsmåte og unntak for sikkerhetskontroll.** Vedkommende myndighet kan av objektive grunner tillate at andre enn passasjerer blir unntatt fra screening, eller blir utsatt for spesielle screeningsprosedyrer, forutsatt at de ledsages av en person som er autorisert til å eskortere i samsvar med punkt 1.2.7. Screenede personer utenom passasjerer som midlertidig forlater SRA området kan få fritak fra screening ved retur, forutsatt at de har vært under konstant observasjon av autorisert personell som med rimelighet kan sikre at de ikke innfører forbudte gjenstander i kritisk del av flyplassen.
 - 1.4.1 **Undersøkelse av kjøretøy til CP.** Alle kjøretøy skal undersøkes før de kommer inn til CP. Føreren og passasjerer i kjøretøyet skal ikke være tilstede under søket. Personlige eiendeler må tas ut av kjøretøyet for screening. Det skal være definerte metoder for å sikre tilfeldighet i valg av områdene som undersøkes.
 - 1.4.2 **Undersøkelse av kjøretøy til andre sikkerhetsbegrensede områder.** Alle kjøretøy skal undersøkes før de kommer inn i andre sikkerhetsbegrensede områder, utenom hvis de kommer fra CP. Føreren og passasjerer i kjøretøyet skal ikke være tilstede under søket. Personlige eiendeler må tas ut av kjøretøyet for screening. Det skal være definerte metoder for å sikre tilfeldighet i valg av områdene som undersøkes.
 - 1.4.3 **Undersøkelsesmetoder.** Et håndstøk skal bestå av en grundig manuell kontroll av de utvalgte områder, for å med rimelighet sikre at de ikke inneholder forbudte gjenstander. Følgende metoder kan brukes som et supplerende undersøkelsesmiddel: deteksjonshunder av eksplosiver, eksplosivt sporingsdeteksjonsutstyr (ETD).
 - 1.4.4 **Særlige fremgangsmåter og unntak for undersøkelse av kjøretøy.** Vedkommende myndighet kan av objektive grunner tillate at kjøretøy er unntatt fra undersøkelse, eller blir utsatt for spesielle undersøkelsesprosedyrer, forutsatt at de ledsages av en person som er autorisert til å eskortere i samsvar med punkt 1.2.7.
 - 1.5 **Overvåkning, patruljering og andre former for fysisk kontroll.** Overvåkning og patruljering skal gjennomføres for å overvåke: grensene mellom landside, flyside, SRA områder og CP områder, områder i nærheten av terminalen som er tilgjengelige for publikum, inkludert parkeringsområder og bilveier, kontrollere ID kort til ansatte i andre sikkerhetsbegrensede områder enn der passasjerene er til stede, kontrollere kjøretøy bevis, ha kontroll over bagasje, last og post i CP området som venter på å bli lastet ombord i flyet. Hyppigheten, omfanget og virkemidlene for overvåkning og patruljering skal være basert på en lokal risikovurdering foretatt av vedkommende myndighet, på bakgrunn av: lufthavnens størrelse, antall operasjoner, utformingen av flyplassen, mulighetene og begrensningene for å gjennomføre overvåkning og patruljering. Overvåkning og patruljering skal ikke følge et forutsigbart mønster, og ID kort skal kontrolleres tilfeldig.
 - 4.1.1 **Gjennom søkning av passasjerer.** Før screening skal jakker tas av og screenes sammen med håndbagasjen. Passasjerer skal screenes gjennom et håndstøk, eller walk-through metal detector (WTMD). Hvis screeneren ikke kan avgjøre om passasjerer har med seg forbudte gjenstander eller ikke, skal passasjerer nektes tilgang til SRA eller screenes på nytt til screenerens tilfredshet. Når et håndstøk utføres, skal det utføres for å med rimelighet sikre at personen ikke bærer forbudte gjenstander. Når WTMD maskinen gjør utslag, skal årsaken til

- alarmen løses. Håndholdt metalldeteksjonsutstyr (HHMD) kan kun brukes som en tilleggsmetode for screening. Det skal ikke erstatte kravene til et håndsøk.
- 4.1.2 **Gjennom søking av håndbagasje.** Før screening skal store elektriske gjenstander og alt flytende tas ut av bagasjen og screenes separat. Hvis screening maskinen er i stand til å screene flytende væsker, er det ikke nødvendig at det screenes separat. Alt flytende skal være i separate beholdere med en kapasitet på maks 100 ml. Håndbagasjen skal screenes av et håndsøk, av røntgenutstyr eller av eksplosivt deteksjonssystem (EDS) -utstyr. Hvis screeneren ikke kan avgjøre om håndbagasjen inneholder forbudte gjenstander eller ikke, skal den avises eller screenes på nytt. Der det brukes røntgen utstyr skal hvert bilde vises av screeneren. Hvis screeneren gjør utslag, skal håndbagasjen kontrolleres for å være sikker på at ingen forbudte gjenstander tas med til SRA eller inn i flyet. Deteksjonshunder og eksplosiv sporingsdeteksjons utstyr skal bare brukes som en tilleggs metode for screening.
- 4.1.3 **Gjennom søking av flytende.** Flytende væsker skal screenes av enten: røntgenutstyr, eksplosivt deteksjonssystem, eksplosivt deteksjonsutstyr, teststrimler for kjemiske reaksjoner eller væskeskannere i form av flasker. Smaking eller testing på huden kan brukes som et supplement til screening.
- 4.2 **Beskyttelse av passasjerer og håndbagasje.** Beskyttelse av passasjerer og håndbagasje skal være underlagt bestemmelsene i eget kommisjonsvedtak.
- 4.3 **Mulig forstyrrende passasjerer.** Flyselskaper skal underrettes skriftlig på forhånd av vedkommende myndighet om potensiell(e) forstyrrende passasjerer som skal fly. Meldingen skal inneholde følgende: personens identitet og kjønn, grunn til transport, ledsagerens navn og tittel, risikovurdering gjort av vedkommende myndighet. Myndigheten skal sikre at personer som er i varetekt alltid blir eskortert.
- 4.4 **Forbudte gjenstander.** Passasjerer har ikke lov til å frakte følgende gjenstander inn til SRA eller ombord i flyet: alle former for skytevåpen, herunder også falske skytevåpen som kan forveksles med ekte våpen, inhabiliserende kjemikalier som pepperspray, tåregass ol, gjenstander med skarp spiss eller kant, arbeidsverktøy som kan utføre personskade, stumpe gjenstander som kan utføre personskade som balltre ol, eksplosiver og brannfarlige stoffer.
- 5.1 **Gjennom søkning av innsjekket bagasje.** Følgende metoder, enten hver for seg eller i kombinasjon, skal brukes for å screene innsjekket bagasje: et håndsøk, røntgenutstyr, eksplosivt deteksjonssystem, eksplosivt sporingsdeteksjonsutstyr. Hvis screeneren ikke kan avgjøre om bagasjen inneholder forbudte gjenstander eller ikke, skal den avises eller screenes på nytt til screenerens tilfredshet.
- 5.2 **Beskyttelse av innsjekket bagasje.** Passasjerer skal ikke ha tilgang til screenet bagasje, med mindre det er deres egen bagasje og de er under oppsyn for å sikre at: ingen forbudte gjenstander blir lagt i bagasjen, eller at gjenstander som er forbudt i SRA blir tatt ut av innsjekket bagasje og tatt med inn i SRA eller i fly. Innsjekket bagasje som ikke er beskyttet mot uautorisert forstyrrelse, skal screenes på nytt.
- 5.3 **Gjenforening av bagasje.** Flyselskapet skal under ombordstigningen sørge for at passasjerene fremviser gyldig boardingkort i samsvar med den innsjekkede bagasjen. Flyselskapet skal identifisere passasjerer som ikke gikk ombord eller som forlot flyet før avgang. Hvis passasjerer ikke er ombord i flyet, skal passasjerens innsjekkede bagasje tas ut av flyet. Bagasje som sendes uten at eieren er ombord, skal tydelig merkes som godkjent for lufttransport, og det skal registreres hvorfor bagasjen sendes uten eier ombord.
- 5.4 **Forbudte gjenstander.** Passasjerer har ikke lov til å ha med følgende gjenstander i den innsjekkede bagasjen: eksplosiver og ildfaste materialer, inkludert ammunisjon, sprengnings hetter, detonatorer og sikringer, granater, fyrverkeri, røykgenererende beholdere, dynamitt, krutt og plasteksplosiver.

- 9.1.1 **Sikkerhetskontroll av forsyninger til lufthavn.** Forsyninger til flyplassen skal screenes før de slippes inn i sikkerhetsbegrensede området, med mindre forsyningene er blitt screenet tidligere av kjent leverandør og forsyningene har blitt beskyttet mot uautorisert forstyrrelse. Enhver forsyning fra kjent leverandør som viser tegn på at den kan ha blitt tuklet med, eller hvor det er grunn til å tro at den ikke har blitt beskyttet mot uautorisert forstyrrelse, skal screenes.
- 9.1.2 **Metode for sikkerhetskontroll av forsyninger til lufthavn.** Ved screening av forsyninger til lufthavnen, må metoden ta hensyn til leveransens art og være av en standard som er tilstrekkelig til å med rimelighet sikre at ingen forbudte gjenstander blir skjult i leveransen.
- 9.1.3 **Godkjenning av kjent leverandør.** For å bli utpekt som en kjent leverandør, skal foretaket sende inn en «erklæring om forpliktelse»- kjent leverandør av flyplassforsyninger til flyplassoperatøren.
- 9.1.4 **Sikkerhetskontroll som skal gjennomføres av kjente leverandører eller lufthavnoperatør.** En kjent leverandør av flyplassforsyninger skal: utnevne en person som er ansvarlig for sikkerheten i selskapet, sørge for at personer med tilgang til flyplassforsyninger får opplæring i sikkerhetsbevissthet før de får tilgang til disse forsyningene, forhindre uautorisert tilgang til sine lokaler og forsyninger, med rimelighet sikre at ingen forbudte gjenstander blir skjult blant forsyningene og bruke forseglinger på, eller fysisk beskytte alle kjøretøyer og/eller containere som transporterer forsyningene.
- 9.2 **Beskyttelse av forsyninger til lufthavnen.** Detaljerte bestemmelser for beskyttelse av flyplassforsyninger er fastlagt i eget kommisjonsvedtak.
- 9.3 **Ytterligere sikkerhetstiltak for forsyninger av væsker, aerosoler, geleer og forseglingsposer.**
- 11.0 **Ansettelse og opplæring av personell.** Myndighetene, flyplassoperatøren eller flyselskapet som setter inn personer som iverksetter eller er ansvarlige for å iverksette tiltak i samsvar med regelverket for sivil luftfart, skal sørge for at disse personene oppfyller standardene i dette kapittelet.
- I dette kapittelet betyr sertifisering en formell evaluering og bekreftelse av eller på vegne av den rette myndighet som indikerer at personen har fullført den aktuelle opplæringen, og at personen har den nødvendige kompetansen for å utføre tildelte funksjoner på et akseptabelt nivå.
- I dette kapittelet skal en bostedsstat være ethvert land der personen har vært bosatt kontinuerlig i 6 måneder eller mer.
- Kompetanse som er anskaffet av personer gjennom erfaring før ansettelse, kan tas i betraktning når man vurderer opplæringsbehov i henhold til denne seksjonen.
- 11.1 **Ansettelse.** Personer som rekrutteres for å være ansvarlige for gjennomføring av screening, tilgangskontroll eller annen sikkerhetskontroll i et sikkerhetsbegrenset område, skal ha vært utsatt for en bakgrunnsjekk. En bakgrunnsjekk skal: kontrollere personens identitet på grunnlag av dokumentasjon, kontrollere kriminelt rulleblad i alle bostedsstater i minst de fem foregående årene og dekke sysselsetting, utdanning og eventuelle hull i minst de fem foregående årene. Bakgrunnskontroll før ansettelse skal gjennomføres før personen gjennomgår sikkerhetsopplæring som innebærer tilgang til informasjon som ikke er offentlig tilgjengelig. Personer som blir rekruttert til å gjennomføre sikkerhetskontroller, skal ha de mentale og fysiske evnene som kreves for å utføre sine tildelte oppgaver effektivt, og personen skal gjøres oppmerksom på de kravene som foreligger i begynnelsen av rekrutteringsprosessen. Disse evnene skal vurderes under rekrutteringsprosessen og før prøvetiden er fullført. Rekrutteringsjournaler, inkludert resultater fra evalueringsprøver, skal oppbevares for alle personer som rekrutteres.

- 11.2.1 **Alminnelige opplæringskrav.** Personer skal ha fullført relevant opplæring før de får fullmakt til å gjennomføre sikkerhetskontroll uten tilsyn. Opplæringen skal omfatte teoretiske og praktiske opplæringselementer. Innholdet i kursene skal spesifiseres eller godkjennes av vedkommende myndighet før en instruktør kan gi opplæring i henhold til forordning nr 300/2008.
- 11.2.2 **Grunnopplæring.** Grunnleggende opplæring av personer som skal utføre security relaterte oppgaver skal gi følgende kompetanse: kunnskap om tidligere anslag mot sivil luftfart, terrorhandlinger og aktuelle trusler, kunnskap om de juridiske rammene for luftfart security, kunnskap om mål og organisering av luftfart security inkludert forpliktelser og ansvar for personer som arbeider i sikkerhetskontrollen, kunnskap for prosedyrer for tilgangskontroll, kunnskap om ID kort systemer som brukes på lufthavnen, kunnskap om prosedyrer for utfordrende personer og omstendigheter der personer skal håndteres eller rapporteres, kunnskap om rapporteringsprosedyrer, evne til å identifisere forbudte gjenstander, evne til å respondere godt på sikkerhetsrelaterte hendelser, kunnskap om hvordan menneskelig atferd kan påvirke sikkerhetsytelsen og evne til å kommunisere tydelig.
- 11.2.3.1 **Særskilt opplæring av personer som gjennomfører sikkerhetskontroll.**
- 11.2.3.3 **Opplæring av personer som utfører gjennom søkning av luftfartsselskapers frakt og post, forsyninger til flygning eller lufthavn.**
- 11.2.3.4 **Opplæring av personer som utfører gjennom søkning av kjøretøy.**
- 11.2.3.5 **Opplæring av personer som utfører patruljering, overvåkning og innpasseringskontroll.**
- 11.2.3.10 **Opplæring av personer som utfører annen gjennom søkning av luftfartsselskapers frakt og post, forsyninger til flygning eller lufthavn.**
- 11.2.4 **Særskilt opplæring av personer som fører direkte tilsyn med personer som utfører sikkerhetskontroll.**
- 11.2.5 **Særskilt opplæring av personer med allment ansvar på nasjonalt eller lokalt plan for å sikre at et sikkerhetsprogram og gjennomføring av dette overholder alle gjeldende rettslige bestemmelser (security manager).**
- 11.2.6 **Opplæring av personer som ikke er passasjerer og som må gis adgang til sikkerhetsbegrenset området uten følge.**
- 11.2.7 **Opplæring av personer med behov for generell sikkerhetsopplæring.**
- 11.3 **Sertifisering eller godkjenning.** Personer som utfører oppgaver som nevnt i punkt 11.2.3.1 til 11.2.3.5 skal være underlagt: en første sertifiserings eller godkjenningsprosess, og personer som bruker røntgen eller EDS-utstyr skal resertifiseres minst hvert tredje år, samt bestå en standardisert bildetolkningstest. Alle andre personer skal resertifiseres minst hvert femte år.
- 11.4.1 **Opplæring av personer som betjener røntgen eller EDS- utstyr.**
- 11.4.2 **Opplæring av personer som betjener security scanners.**
- 11.5 **Kvalifikasjon instruktører.** Vedkommende myndighet skal opprettholde eller ha tilgang til lister over sertifiserte instruktører. Instruktører skal ha gjennomført en bakgrunnsjekk og fremlegge relevante kvalifikasjoner og kompetanse. For å bli sertifisert som instruktør skal personen ha kvalifikasjoner og kompetanse innen følgende områder: instruksjonsteknikker, kvalitetskontroll og sikkerhetslementer som skal læres videre. Vedkommende myndighet skal sørge for at instruktører får regelmessig opplæring og informasjon om utviklingen innen de aktuelle feltene. Hvis myndigheten ikke lenger er overbevist over opplæringen som blir gitt av en kvalifisert instruktør, skal myndigheten enten trekke tilbake godkjenningen av det aktuelle kurset eller fjerne instruktøren.
- 12.0 **Sikkerhetsutstyr.** Operatøren som bruker utstyr for gjennomføring av security tiltak som den er ansvarlig for, skal sikre at utstyret oppfyller standardene i dette kapittelet. Det skal være rutinemessig testing av alt sikkerhetsutstyr.

- 12.1 **WTMD-utstyr.** Walk-through metal detector skal være i stand til å oppdage metall gjenstander ved at alarmeren går av. Deteksjonen skal være uavhengig av objektets posisjon og retning. Maskinen skal være godt festet til en solid base, og skal ha en visuell indikator som viser at utstyret er i drift. Det skal være beskyttelse mot å justere på deteksjonsinnstillingene, og slik justering skal kun være tilgjengelig for autoriserte personer. Alarmeren skal både være visuell og gi lyd, og den skal være merkbar i en rekkevidde på 2 meter. Den visuelle alarmeren skal gi en indikasjon på signalstyrken som oppdages av maskinen, og maskinen skal plasseres slik at den ikke påvirkes av forstyrrelseskilder.
- 12.1.2 **Standard for WTMD-utstyret.**
- 12.2 **Håndholdt metalldetektor.** Skal oppdage metallgjenstander, og gi utslag i form av alarm. Alarmeren skal være merkbar i en rekkevidde på 1 meter. Skal ikke påvirkes av forstyrrelseskilder.
- 12.3 **Røntgen utstyr.**
- 12.4 **EDS-utstyr for påvisning av sprengstoff.**
- 12.4.1 **Generelle krav til EDS.** Utstyr for påvisning av sprengstoff skal oppdage eksplosivt materiale i bagasje eller andre sendinger. EDS skal gi alarm hvis den oppdager eksplosivt materiale, hvis den oppdager tilstedeværelsen av en gjenstand som forhindrer at eksplosivt materiale blir oppdaget, eller hvis innholdet i en bagasje er for tett til å analyseres.
- 12.4.2 **Standarder for EDS.**
- 12.4.3 **Krav til bilde kvalitet for EDS.**
- 12.5 **Bildeprojeksjon (TIP- Threat image protection).** Skal fremstille virtuelle bilder av ulovlige gjenstander i røntgenbilde av bagasje som blir screenet.
- 12.5.2 **TIP- systemets sammensetning.**
- 12.6 **Utstyr til sporpåvisning (ETD- explosive trace detection).**
- 12.7 **Utstyr til gjennom søking av væsker, aerosoler, geleer.**
- 12.9 **Bombehunder.**
- 12.10 **Metal detection equipment (MDE).**
- 12.11. **Securityscannere.**
- 12.12 **Skoskanner.**
- 12.13 **Autoklarering (ACS).**

300/2008 art 12. Lufthavners sikkerhetsprogram.

Alle lufthavnselskaper skal utarbeide, anvende og opprettholde et sikkerhetsprogram for lufthavnen. Dette programmet skal beskrive de metoder og fremgangsmåter som skal følges av lufthavnselskapet for å overholde både forordning 300/2008 og det nasjonale sikkerhetsprogrammet for sivil luftfart i den medlemsstaten der lufthavnen befinner seg. Programmet skal omfatte bestemmelser om intern kvalitetskontroll som beskriver hvordan overholdelse av disse metodene og fremgangsmåtene skal kontrolleres av lufthavnselskapet. Lufthavnens sikkerhetsprogram skal oversendes til vedkommende myndighet, som kan treffe ytterligere tiltak dersom dette er hensiktsmessig.

BSL sec 1-1 §10. **Ansvarshavende sikkerhet (security manager).** Alle virksomheter som skal gjennomføre de felles bestemmelser om sikkerhet i sivil luftfart, skal utpeke en ansvarshavende for sikkerhet.

BSL sec 1-1 §11. Beredskapsplaner og øvelser som omfatter anslag mot luftfarten.

Lufthavnoperatører, luftfartsselskaper, fraktleverandører og postleverandører skal i samråd

med stedlig politi utarbeide og vedlikeholde beredskapsplaner, samt gjennomføre beredskapsøvelser. Beredskapsøvelsene som omfatter anslag mot sikkerheten i luftfarten, skal avholdes minst annet hvert år. Lufthavnoperatøren skal vurdere om andre aktører skal delta i beredskapsarbeidet.

BSL sec 1-1 §12. Sikkerhetsutvalg lokalt BSU.

Lufthavnoperatøren skal etablere et sikkerhetsutvalg ved lufthavnen. Sikkerhetsutvalget skal sørge for planlegging, samordning og evaluering av sikkerhetstiltak ved lufthavnen og delta aktivt i planlegging og gjennomføring av beredskapsøvelser. Sikkerhetsutvalget skal bestå av stedlig politi, lufthavnoperatør og representanter for øvrige aktører på lufthavnen. Representant for stedlig politi eller lufthavnoperatørens representant skal lede sikkerhetsutvalget.

BSL sec 1-1 §14. Ytterligere sikkerhetstiltak.

Luftfartstilsynet kan i særlige tilfeller treffe vedtak om ytterligere sikkerhetstiltak utover det som følger av forskriften. Sikkerhetsrådet for luftfarten, opprettet ved regjeringens resolusjon 4. juli 1991, skal så langt mulig konsulteres før vedtak treffes. Politi eller lufthavnoperatør kan iverksette ytterligere sikkerhetstiltak når særlige forhold ikke gjør det mulig å forelegge saken for Luftfartstilsynet. Slike tiltak skal uten unødig opphold meldes til Luftfartstilsynet.

Official Journal of the European Union. (2015).