Jan Gunnik Hope

Kan vi forberede oss på det uventede?

Masteroppgave i organisasjon og ledelse

Trondheim, august 2017

Norges teknisk-naturvitenskapelige universitet

Fakultet for samfunns- og utdanningsvitenskap

Institutt for sosiologi og statsvitenskap

INNHOLDSFORTEGNELSE

1 Innledning 1
1.1 Problemstilling 1
1.2 Avgrensinger 2
1.3 Disposisjon 3
1.4 Caset 4
2 Teori 6
2.1 Begrepene sikkerhet og risiko 6
2.1.1 Risiko 6
2.1.2 Sikkerhet som fravær av risiko 7
2.1.3 Sikkerhet som nærvær av organisatoriske egenskaper 7
2.1.4 Safety-I og Safety-II 8
2.1.5 Resilience Engineering 9
2.2 Strategier for å skape og ivareta god sikkerhet 9
2.2.1 Bow tie modellen 9
2.2.2 Swiss cheese modellen 10
2.2.3 Overlappende hendelser 10
2.3 Uventede hendelser 11
2.3.1 Uventede og ukjente hendelser 11
2.3.2 Unknown unknown 12
2.3.3 Klassifisering av trusler 13
3 Metode 14
3.1 Overordnet forskningsdesign 14
3.1.1 Kvalitativ metode 15
3.2 Datainnsamling 15
3.2.1 Formell godkjenning 15
3.2.2 Intervjuene 16
3.2.3 Informantene 17
3.2.4 Koding og kategorisering 18
3.3 Min rolle 18
3.4 Dataenes interne gyldighet 19
3.5 Ekstern gyldighet 19

4 Funn og analyse 20
4.1 Fakta om selskapet 20
4.2 Kjente feilsituasjoner 21
4.2.1 Tekniske fellesfeil 21
4.2.2 Ikke-tekniske situasjoner 23
4.3 Mottiltak – kjente feilsituasjoner 23
4.3.1 Tekniske mottiltak - nettverksfeil 23
4.3.2 Designmessige mottiltak – nettverksfeil 24
4.3.3 Mottiltak - kundemottak 24
4.3.4 Mottiltak – organisasjon 25
4.4 Mulige uventede og ukjente hendelser 25
4.4.1 Force Majeure – type hendelser 25
4.4.2 Mindre alvorlige natur-/miljøhendelser 26
4.4.3 Utro tjener 26
4.5 Mulige motttiltak – ukjente hendelser 26
4.5.1 Ledelse 26
4.5.2 Informasjon internt og eksternt 27
4.5.3 Samarbeid og rolleavklaring 27
4.5.4 Det praktiske 27
4.5.5 Bevisstgjøring 28
4.6 Hvor forberedt er selskapet? 28
5 Drøfting 29
5.1 Forskningsspørsmål 1 29
5.1.1 Det uventede 29
5.1.2 Endring i hva som er uventet 30
5.1.3 Om svarte svaner 31
5.1.4 Alvorlighetsgrad 32
5.1.5 Alvorlig og uventet for hvem 32
5.1.6 Hvordan kan informantenes hendelser klassifiseres? 34
5.1.7 Mulige framtidige hendelser i kategorien UkjentUkjent 35
5.1.8 Hendelse i forhold til konsekvens 35
5.1.9 Forskningsspørsmål 1 oppsummert 36
5.2 Forskningsspørsmål 2 36

5.2.1 Mitigere kjente feil 37
5.2.2 Kan man forberede seg på ukjente situasjoner? 37
5.2.3 Mitigere ukjente situasjoner 39
5.2.4 Forhindre uventede situasjoner / HRO perspektivet 40
5.2.5 Resilience engineering perspektivet, normativt ståsted 41
5.2.6 Uventet vs. kompleks 44
5.2.7 HRO / RE vs. kjente feil / hendelser 44
5.2.8 Forskningsspørsmål 2 oppsummert 45
5.3 Hvorfor er ikke alle organisasjoner HROer? 45
6 Konklusjon 48
6.1 Oppsummering 48
6.2 Personlige refleksjoner over problemstillingen 49
6.3 Personlige refleksjoner over oppgaven 49
6.4 Mulig videre forskning 50
Figurer 51
7 Referanser 52
Vedlegg A Tilbakemelding fra NSD 54
Vedlegg B Informasjonsskriv med samtykkeerklæring 57
Vedlegg C Intervjuguide 58

1 INNLEDNING

«Verden har blitt stadig mer uforutsigbar» er et uttrykk vi ofte kan høre. Til tross for bedre kommunikasjon enn noen gang, og mer kunnskap om omgivelsene våre enn noensinne før, så lar vi oss stadig overraske. Dette gjelder ikke minst i forhold til menneskeskapte hendelser. I løpet av 2016 opplevde vi «Brexit» og valget av Trump som president i USA, begge på tross av de fleste «eksperters» forventninger. Vi har blitt rammet av ulike former for terror[1] som har vært oppfinnsomme og dermed dessverre ikke blitt forutsett av myndighetene – og på den positive siden ser vi også innovasjon og framvekst av nye produkter[2], markeder og tjenester som har gått fra null til milliardindustri på få år.

I denne oppgaven ønsker jeg å utforske i hvilken grad det er mulig å forutse og kontrollere de uventede hendelsene som kan forstyrre tjenestene et moderne teleselskap leverer. Jeg lar begrepet «uventet» stå for *brå, plutselig, ikke planlagt* og deler det ytterligere opp i «kjent» og «ukjent». De kjente hendelsene har vært observert tidligere, og er noe man kan forvente å måtte håndtere fra tid til annen. De mer eller mindre ukjente hendelsene, har man gjerne ikke observert tidligere og har sannsynligvis ikke standardiserte responsmekanismer for. Det er disse ukjente hendelsene jeg finner mest spennende – kan man også forberede seg på det ukjente?

For å gjøre dette vil jeg først se på de tekniske og organisatoriske tiltakene som er tilstede, og vurdere i hvilken grad de fungerer for kjente hendelser. Deretter vil jeg bevege meg over i de ukjente hendelsene. I hvor stor grad det eksisterer ukjente hendelser som kan påvirke tjenesteproduksjonen, og dersom slike eksisterer, om de kan klassifiseres på noen måte. Derfra vil jeg vurdere mulige måter å håndtere de tilhørende uventede situasjonene på. Til det vil jeg spesielt se til *High Reliability Organizations (HRO)* og *Resilience Engineering (RE)* for å finne mulige måter å håndtere det tidligere ukjente. Jeg vil også se på hvordan ulike hendelser utvikler seg fra de første gang observeres til de har blitt «hverdagslige».

Jeg arbeider i teleselskapet som danner rammen for oppgaven. Når den skrives er jeg mellomleder i en mindre avdeling. Oppgaven er skrevet som siste ledd i en erfaringsbasert mastergrad i organisasjon og ledelse ved NTNU.

1.1 PROBLEMSTILLING

Som presentert i innledningen ønsker jeg å se på det uventede som kan oppstå og hvordan man best kan forberede seg på det. Min problemstilling blir dermed:

[1] 9/11 i USA og 22. juli i Norge er klassiske eksempler, i 2016 og 2017 var det også flere tilfeller der lastebiler ble tatt i bruk som «våpen» mot sivile.

[2] Twitter og Snapchat er gode eksempler på selskap i internett-sfæren, et noe mindre kjent eksempel er Nest Labs (www.nest.com) som ble stiftet i 2010. Da de ble kjøpt av Google for 2,3 Milliarder USD i januar 2014 hadde de kun to produkter klare for salg: Termostater og røykdetektorer som var laget for smarte hjem.

Kan det oppstå uventede hendelser av alvorlig karakter og hvordan kan selskapet eventuelt beskytte seg mot dem?

For å svare på det stiller jeg opp to forskningsspørsmål som blir sentrale i diskusjonen:

1. *Hva kjennetegner hendelser som er uventede og som kan ha en alvorlig eller katastrofal konsekvens for selskapet?*
2. *Hvordan kan selskapet forhindre at uventede hendelser oppstår og hvordan kan slike håndteres om de skulle oppstå?*

Uventede hendelser vil forekomme og bli håndtert i de fleste organisasjoner. Forskningsspørsmål 1 sin hensikt er å se på hvordan dette gjøres i selskapet i dag og om det eksisterer uventede hendelser som selskapet ikke er forberedt på. Dersom slike eksisterer er det interessant å finne ut hva som karakteriserer dem. Da kan de også klassifiseres, i forhold til type uventet hendelse og i forhold til alvorlighetsgrad for selskapet.

Forskningsspørsmål 2 tar opp hvordan selskapet kan forholde seg til det uventede, både det som er kjent og det som er ukjent. Jeg ønsker å se på hva som kan gjøres preventivt og hva som kan gjøres for å hindre / begrense skader. Spesielt vil jeg studere de ukjente hendelsene.

1.2 AVGRENSINGER

I et stort selskap er det mange ulike fagfelt. Min bakgrunn er i nettverkstjenester og tilhørende kundepåvirkning, og det er der jeg har valgt å fokusere. Det betyr ikke at det er bare der uventede hendelser kan oppstå. Andre innfallsvinkler som kunne vært vektlagt er for eksempel:

Økonomi - Hvordan kan selskapets inntektsstrømmer eller likviditetssituasjon bli forstyrret i alvorlig grad uten at administrasjonen klarer å se og håndtere det raskt nok?

Omdømme - Kan selskapet oppleve et så stort direkte tap i omdømme at det får alvorlige konsekvenser? Kan selskapet oppleve at kundene forlater selskapet som en «demonstrasjon»?

Organisasjon - Kan selskapet oppleve større hendelser som forhindrer organisasjonens normale evne til produksjon? Det er mulig å tenke seg både menneskeskapte (streik, konflikt osv.) og ufrivillige (sykdom) årsaker til at de ansatte ikke utfører sine arbeidsoppgaver.

Sabotasje - Kan selskapet motstå direkte ondsinnete handlinger fra enkeltpersoner eller organisasjoner? Jeg berører dette temaet noe, men da med enkeltpersoner som ønsker å skade selskapet. Dette kunne vært utvidet til å se på hva mer organiserte motparter kan tenkes å gjøre.

IT-systemer - I hvor stor grad har selskapet robuste IT-systemer? Dette kunne vært interessant å se på for hvert enkelt system – et moderne teleselskap har ganske mange –

men også hvordan de fungerer sammen i en stadig mer integrert portefølje av gamle og nye løsninger.

Kvalitet - Kan den generelle opplevde kvaliteten på selskapets tjenester forandre seg uventet så raskt at man ikke kan gjøre effektive mottiltak?

Produkter/tjenester - Kan selskapets produkter og tjenester plutselig bli irrelevante? Kan det komme disruptive hendelser som gjør selskapet til et moderne Kodak Company?[3]

Jeg velger som sagt å ikke ta disse perspektivene. Jeg tror at nettverkstjenester og kundeforholdet gir tilstrekkelig med eksempler og underlag til å diskutere mine to forskningsspørsmål på en relevant måte. Som jeg vil vise senere mener jeg at det gir bakteppe nok til å slå fast at det eksisterer ukjente hendelser av alvorlig karakter og at vi neppe er i stand til å forutse dem alle. Det gir også grunnlag nok til å diskutere mulige mottiltak for å håndtere ukjente hendelser.

Uventede hendelser er ikke nødvendigvis negative, gode ideer er gjerne også uventete. I denne oppgaven har jeg fokus på det som forstyrrer tjenester og er uønsket, og som derfor også kan omtales som trusler mot normalsituasjonen.

Selskapet har vært gjennom store endringer (fusjon, fisjon, bemanningsendringer og flytting av funksjoner) i løpet av de siste årene, men jeg lar ikke det være tema i oppgaven. Jeg forsøker å se forbi det og fokusere på oppgavens problemstilling som jeg mener er relevant for kunder, omgivelser og selskapet selv, uavhengig av de endringene selskapet til enhver tid gjør.

Jeg tror at problemstillingen kunne vært grundigere belyst ved å se på andre selskaper i samme bransje, for dermed å få et bedre empirisk grunnlag. Særlig i forhold til håndtering av ukjente hendelser kunne det også vært interessant å se hvordan andre organisasjoner håndterer dette – gjerne organisasjoner som har et tydeligere beredskapselement. Dette kunne vært offentlige (brann, politi, helse, strøm, vann), private (veidrift, transportselskaper) eller ideelle organisasjoner (Røde Kors, Norsk Folkehjelp). Ut i fra oppgavens størrelse og arbeidsomfang samt egen kapasitet har jeg likevel valgt å ikke gjøre dette.

1.3 DISPOSISJON

Etter denne innledningen er oppgaven delt inn i følgende deler:

Teori - For å se på håndtering av uventede, kjente hendelser tar jeg utgangspunkt i sikkerhetsbegrepet og ser på sikkerhet som fravær av risiko og som nærvær av organisatoriske egenskaper. Først ser jeg på klassiske tilnærminger til det å hindre uønskede

[3] Se f.eks. https://hbr.org/2016/07/kodaks-downfall-wasnt-about-technology Kodak dominerte lenge film- og fotografibransjen. Da digital film og fotografering tok over, ventet selskapet for lenge med å tilpasse seg. Det søkte konkursbeskyttelse i 2012. Selskapet overlevde så vidt, men er i dag mindre og med et mye smalere produktspekter.

hendelser og det å mitigere dem om de likevel skulle oppstå. Deretter på organisatoriske tilnærminger som High Reliability Organizations, Resilience Engineering og Safety-I vs. Safety-II.

Jeg går så over til de uventede, ukjente hendelsene, først ved å se på begrepet «svarte svaner» og hvordan vi kan utvide det vi anser som kjent. Jeg tar opp en modell for hvordan vi klassifiserer den kunnskapen vi har og en modell som viser hvordan trusler kan klassifiseres.

Metode - Jeg presenterer forskningsdesignet og hvorfor jeg har valgt kvalitativ metode for denne oppgaven. Jeg gjennomgår hvordan jeg praktisk har gjennomført intervjuene, inkludert for- og etterarbeid. Så vurderes dataenes gyldighet og min egen rolle.

Funn og analyse - Funnene jeg har gjort presenteres, og jeg forsøker både å trekke dem sammen og systematisere dem. Før jeg behandler ukjente situasjoner lister jeg opp hvordan organisasjonen er rigget for å håndtere de kjente situasjonene.

Drøfting - I drøftingen tar jeg konkret opp de to forskningsspørsmålene og ser på dem i lys av empirien. Først ser jeg på hvordan uønskede, uventede hendelser - trusler - kan klassifiseres på to ulike måter og setter dem i sammenheng. Så tar jeg opp hvordan trusler endrer karakter etter at de har blitt «oppdaget» - enten ved at de faktisk skjer eller ved at vi innser at de kan komme til å skje. Jeg ser på mine observasjoner i forhold til dette og plasserer dem i modellen.

Så går jeg over til forskningsspørsmål 2 og ser hvordan det er mulig å forberede seg på uventede hendelser og situasjoner. Jeg vurderer i hvor stor grad selskapet har egenskapene som HRO og RE framhever, og hva som eventuelt kunne være gjort annerledes. Jeg finner relativt lite overlapp mellom selskapet og HRO/RE og avslutningsvis i kapittelet diskuterer jeg mulige årsaker til det.

Konklusjon - I konklusjonen henter jeg opp igjen forskningsspørsmålet og oppsummerer hvordan jeg har gått fram for å samle data og hva jeg har funnet når jeg kombinerer det med teorien. Jeg ser på min egen forskerrolle og hva jeg har fått ut av oppgaven. Jeg forsøker å se på oppgaven som helhet og mulig videre forskning på området.

1.4 CASET

Selskapet som omhandles i oppgaven er et større norsk telekommunikasjonsselskap som leverer kommunikasjons- og innholdstjenester til private og bedrifter i Norge. Det er børsnotert og har en relevant posisjon i sine markeder, men er ikke størst i noen av dem.

Selskapet tilbyr tjenester innenfor telekommunikasjon til private og bedrifter. For privatmarkedet er vanlig internettforbindelse det viktigste produktet, levert over en fast linje til hjemmet. I bedriftsmarkedet er det i tillegg til internett også såkalte VPN-tjenester som lar bedriften kommunisere på sikker måte både internt og mot andre selskaper. I begge markedene tilbys også ulike taletjenester og andre verdiøkende tjenester.

Nettverkstjenestene har blitt allment tilgjengelig i samfunnet, og i løpet av selskapets levetid har de gått fra å være nyskapende til å bli alminneliggjort – de forventes å virke hele tiden. I likhet med basistjenester som strøm og vann så har nettverkene blitt noe vi tar som en selvfølge.

Informantene er hentet blant nåværende og tidligere ansatte i bedriften, og jeg har intervjuet dem enkeltvis med støtte i en intervjuguide som jeg har utviklet.

2 TEORI

Mitt forskningsspørsmål tar opp uventede hendelser og jeg ønsker spesielt å utforske de som også er ukjente. For at det skal gi mening begynner jeg med kjente hendelser og hvilken rolle de spiller i klassisk sikkerhetstenkning. I dette kapittelet vil jeg derfor først se på risikobegrepet og to ulike perspektiver på sikkerhet. Deretter presenterer jeg noen klassiske modeller som brukes for å diskutere håndteringen av uønskede hendelser.

Som teoretisk bakgrunn for det ukjente ser jeg på begrepet «svart svane» og en mer generell modell «UkjentUkjent» for å klassifisere det vi vet kontra det vi ikke vet. Jeg beskriver også en modell for å klassifisere trusler, som uønskede hendelser ofte er.

2.1 BEGREPENE SIKKERHET OG RISIKO

Hva er egentlig sikkerhet? Kongsvik (2013) skiller mellom to perspektiver på sikkerhet: *Sikkerhet som fravær av risiko* og *sikkerhet som nærvær av organisatoriske egenskaper*.

2.1.1 Risiko

En vanlig oppfatning av risiko er sannsynligheten for at noe uønsket skal skje multiplisert med konsekvensen av hendelsen (Rausand & Utne, 2009):

*Risiko = Sannsynlighet (uønsket hendelse) * Konsekvens (uønsket hendelse)*

For å oppnå lavest mulig risiko for uønskede hendelser kan vi altså

- Gjøre noe for å hindre at hendelsene oppstår.
- Redusere de skadelige konsekvensene.

Denne enkle definisjonen av risiko lar seg bruke matematisk. Dersom vi har et stort nok antall hendelser (for eksempel trafikkulykker) og kan relatere dem til et volumbegrep (antall kjørte kilometer), så kan vi mene noe om sannsynlighet for at en hendelse oppstår, målt i forhold til volumbegrepet (ulykke per kjørte kilometer). Hvis vi videre vet noe om konsekvensen av hendelsen (for eksempel målt i kroner) så kan vi sette måltall på risikoen (i kroner for hver kjørte kilometer).[4]

Dersom vi kjenner kostnaden på eventuelle risikoreduserende tiltak, kan vi vurdere om de isolert sett er lønnsomme og veie ulike risikoreduserende tiltak opp mot hverandre.

Desto oftere en hendelse skjer, jo bedre datagrunnlag vil vi ha for å anslå sannsynligheten for at den skal skje igjen. Tilsvarende vil vi som regel ha bedre grunnlag for å vite noe om konsekvensene når vi ser på hendelser som skjer ofte, enn hvis vi analyserer ting som skjer sjelden (eller ennå ikke har skjedd).[5] Dette vil jeg komme tilbake til senere.

[4] Forutsatt at det konsekvensen lar seg beregne. Å tallfeste «kostnaden» ved dødsfall er ikke uproblematisk.
[5] Sannsynligheten for at uønskede hendelser skal skje med utstyr kan også beregnes statistisk, med utgangspunkt i komponentenes MTBF (Mean Time Between Failures). Dette kan gjøres før hendelsen (utstyret feiler) noensinne har skjedd. Denne type «mekaniske» uønskede hendelser er ikke tema i denne oppgaven.

2.1.2 Sikkerhet som fravær av risiko

Sikkerhet som fravær av risiko betrakter dermed sikkerhet og risiko som inverse begreper – klarer vi å fjerne/minimere all risiko så vil vi også ha perfekt/maksimal sikkerhet.

I en ideell verden skulle man gjerne sett at man kunne hatt perfekt sikkerhet, dvs. null risiko, men i den virkelige verden er begrepet *As Low As Reasonably Possible* mye brukt: Vi aksepterer altså en viss risiko. Mengden av risiko som aksepteres er ofte avhengig av alternativet – dersom vi forbød all bilkjøring ville vi oppnå Statens Vegvesen sin nullvisjon[6] umiddelbart, men kostnaden ville være uakseptabel. Tilsvarende ville mange foretrukket atomkraft framfor fossile brensel eller vannkraftutbygginger hvis vi bare kunne eliminert muligheten for nedsmelting eller radioaktive stråleskader på omgivelsene – nå og for framtiden.

2.1.3 Sikkerhet som nærvær av organisatoriske egenskaper

Det virker intuitivt fornuftig å definere sikkerhet som fravær av risiko, men hvordan kan man finne, kvantifisere og deretter fjerne eller mitigere alle risikofaktorer i komplekse systemer? Dess mer komplisert og avhengig (tett koblet) et system er, dess verre er det å forutse og forhindre alle mulige årsaker som kan lede til ulykker. Perrow (1999) hevder at hvis systemet bare er komplisert nok, så vil ulykker «måtte» skje, vi får «Normal Accidents».

Som en motreaksjon på dette ble det pekt på at mange kompliserte systemer ikke opplevde disse «uunngåelige» ulykkene. Hangarskipsoperasjoner, flygeledelse i travelt luftrom og moderne kraftproduksjon ble brukt som eksempler på komplekse aktiviteter med høyt skadepotensiale, men der organisasjonene hadde lært å operere på en trygg måte – såkalte *High Reliability Organizations (HRO) (Weick, Sutcliffe, & Obstfeld, 2008).*

Weick, Sutcliffe og Obstfeld beskriver fem kjennetegn ved HROer:

Preoccupation with failure - Særlig oppmerksomhet på feil og uventede hendelser – HROene er klar over at de ikke «har råd til å feile» og at de derfor må være oppmerksom på uvanlige hendelser og reagere tidlig på dem. Dette innebærer en evig «mistenksomhet» til omgivelsene og hva som kan indikere at noe er i ferd med å gå galt. Eksempelvis vil effektive HROer oppmuntre feilrapportering og gjøre sitt beste for å lære av dem.

Reluctance to simplify interpretations - Effektive organisasjoner trenger å utvikle felles begrepsapparat og forståelse av situasjoner, med tilhørende reaksjonsmønster. Et kjennetegn ved HROer er at de likevel forsøker å være bevisst på de forenklingene som gjøres og hva man velger å ignorere. Dette gjør at det er lettere å være oppmerksom på variasjoner og lar organisasjonen ha en sunn skepsis til om man til enhver tid gjør de riktige valgene.

Sensitivity to operations - HROer ønsker å ha en sterk «tilstedeværelse» i situasjoner i den forstand at nøkkelpersoner klarer å ha en fullstendig helhetsforståelse av den situasjonen organisasjonen, med nok oppmerksomhet på detaljer. Det vil si at man er opptatt av om det

[6] Stortinget vedtok i forbindelse med behandlingen av Nasjonal transportplan for 2002–2011 "en visjon om et transportsystem som ikke fører til tap av liv eller varig skade" – Nullvisjonen. Se f.eks. http://www.vegvesen.no/fag/fokusomrader/Trafikksikkerhet/Nullvisjonen

man observerer er forenlig med det den situasjonen man til enhver tid er i. Dersom man observerer noe som avviker vil det raskt bli fanget opp og vurdert i forhold til om avviket kan forklares innenfor normal variasjon eller om det er et forvarsel for en feilsituasjon.

Commitment to resilience - HROer tilstreber å være robuste både for å forutse og hindre at en feil skal oppstå og for å mitigere den så snart den er i ferd med å utvikle seg. De «foretrekker» altså ikke den venstre eller høyre siden av bow tie modellen (nedenfor), men ønsker å mestre begge sider. En HRO vil søke å lære av tidligere erfaringer, men vil ikke være låst i handlingsmønsteret når en tilsvarende situasjon oppstår. Tvert imot vil man improvisere og tilpasse responsen etter som situasjonen utvikler seg.

Underspecification of structures - Ansvar og myndighet er sentralt i oppbyggingen i enhver organisasjon, men en HRO vil forsøke å være fleksibel og tilpasse seg situasjonen som oppstår – kritiske problemer skal løses nærmest mulig der de oppstår og av den som er best skikket til det, uten å forsinkes av behov for formelle beslutninger. Det er organisasjonen som fortløpende skal tilpasse seg problemet.

Intensjonen er altså å lære opp en organisasjon til å detektere og håndtere alvorlige hendelser fremfor å ha «pre-programmerte svar» på alle situasjoner som kan tenkes å oppstå. Til sammen skal disse fem prosessene gi en organisasjon en kollektiv bevissthet (*collective mindfulness)* i forhold til ønsket normaltilstand. HROer erkjenner altså at de ikke kan operere feilfritt, men tar sikte på å oppdage og korrigere feil raskest mulig.

2.1.4 Safety-I og Safety-II

I forlengelsen av forskningen rundt HROer har det vært hevdet (E. Hollnagel, 2014) at man i tillegg til å fokusere på alt som kan gå galt (Safety-I), også burde se hva som gjør at ting går bra (Safety-II). Det er jo svært mange flere tilfeller av flygninger og bilturer som går bra, enn det er flyulykker og trafikkulykker - *på tross av* at det stadig skjer uventede hendelser som kunne ført til en ulykke.

	Safety-I	Safety-II
Definisjon / mål	Minst mulig skal gå galt.	Mest mulig skal gå bra.
Sikkerhetstenking	Reaktivt.	Proaktivt.
Den menneskelige faktor	En risiko, som bør unngås og/eller overvåkes.	En viktig ressurs for å tilføre fleksibilitet.
Ulykkes-/hendelsesanalyse	Hendelser skyldes feil/avvik hos operatør eller i prosess. Fokus på å finne feilårsak.	Stort sett går ting bra. Fokus er å finne ut og forklare hvorfor det innimellom ikke går bra.
Risikovurderinger	Finne og identifisere årsaker og faktorer som kan «ødelegge» en fungerende prosess.	Fokus på å forstå hvilke tilstander og hendelser som kan bringe oss ut av den ønskede normaltilstanden.

Tabell 1 – Safety-I vs. Safety-II (Hollnagel, 2014)

Tabell 1 er hentet fra (E. Hollnagel, 2014) og noe forenklet.

Et skifte fra Safety-I til Safety-II innebærer mer proaktivitet, noe som kan være vanskelig i dagligdagse situasjoner. En mulig utfordring er at krav om effektivitet gjør at organisasjoner

blir mer reaktive (Safety-I) ved at man avvikshåndterer det som ikke «følger standarden», fremfor å bruke ressurser proaktivt.

2.1.5 Resilience Engineering

Resilience engineering (RE) perspektivet har utviklet seg med Safety-II som utgangspunkt, og forsøker å beskrive på en mer holistisk måte hvordan en organisasjon kan unngå uønskede hendelser. Dette inkluderer (Wreathall, 2006) (Kongsvik, 2013):

Engasjement og forpliktelse fra toppledelsen - Toppledelsen erkjenner (både i «festtaler» og i daglig praksis) at menneskene i organisasjonen er viktige og at deres bidrag er kritisk for gode resultater.

Rettferdig kultur - Hendelsesrapportering er oppmuntret og har ikke fokus på å finne syndebukker (med mindre det er gjort straffbare handlinger).

Læringskultur - Organisasjonen er oppriktig interessert i å lære av hendelser, heller enn å bortforklare, minimalisere eller fordele skyld.

Oppmerksomhet - Ledelsen er opptatt av kvaliteten på arbeidet i organisasjonen og vurderer dette i forhold til mulige problemer og tilhørende sikkerhetsbarrierer.

Beredskap - Organisasjonen streber etter å være pro-aktiv; forutse problemer og hindre at de oppstår eller eskalerer.

Fleksibilitet - Organisasjonen evner å tilpasse seg effektivt til nye eller komplekse problemer uten å stoppe opp. En viktig forutsetning er delegert myndighet til «frontlinjen» for raskt å ta nødvendige, operative avgjørelser.

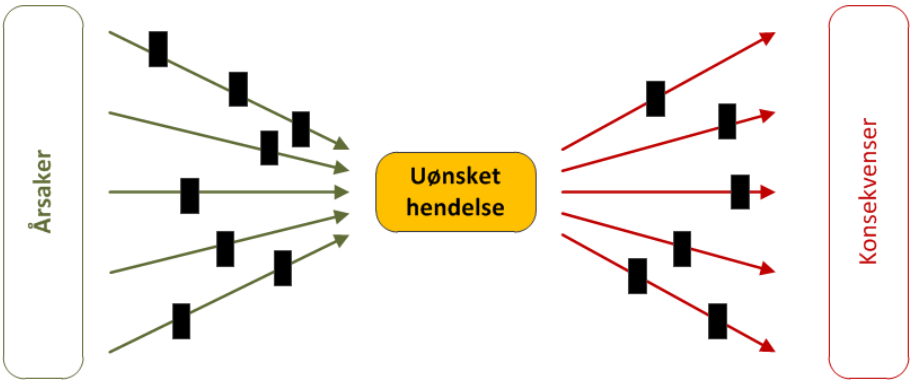
Grensebevissthet - Organisasjonen er klar over, og bevisst på, rammene for sikre operasjoner. Det fører til en risikoforståelse, også i forhold til de forsvarsmekanismene som eksisterer.

2.2 STRATEGIER FOR Å SKAPE OG IVARETA GOD SIKKERHET

Jeg vil kort presentere noen grunnleggende modeller innenfor klassisk sikkerhetstenking.

2.2.1 Bow tie modellen

God sikkerhet i betydningen «fravær av risiko» kan forstås som ingen negative hendelser, men en mer presis definisjon er å *forhindre en uønsket hendelse eller å minimere konsekvensene av den*. Det er det som er utgangspunktet for *bow tie modellen* (Figur 1), som adresserer årsakene og konsekvenser ved uønskede hendelser.

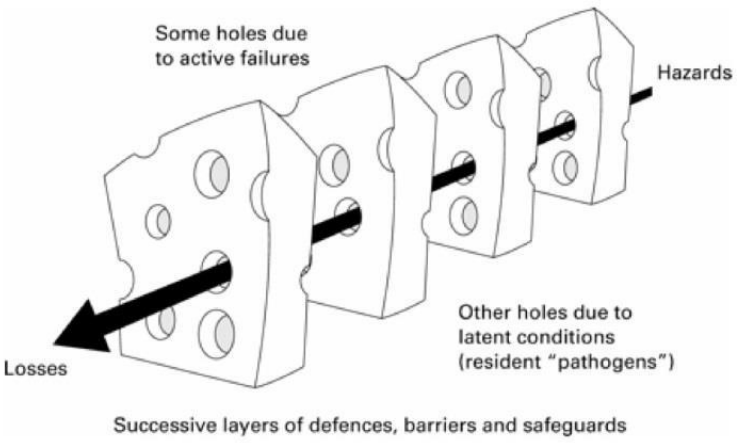


Figur 1 – Bow tie modellen

Man kan bygge barrierer for å hindre at årsakene leder til den ønskede hendelsen og man kan bygge barrierer som minimerer eller fjerner helt de uønskede konsekvensene av hendelsen (Haddon Jr, 1970, 1980). Haddon har en relativt konkret tilnærming og bruker fysiske barrierer som bilder, men modellen kan også brukes i mer virtuelle situasjoner, for eksempel IT-sikkerhet.

2.2.2 Swiss cheese modellen

Bow tie modellen viser at multiple sikkerhetsbarrierer både før og etter hendelsen kan forhindre uønskede hendelser eller uønskede konsekvenser av slike. Slike konsekvenser kan likevel oppstå. Figur 2: *Swiss cheese modellen* (Reason, 1997) forsøker å illustrere det ved å la hullene i osten symbolisere feiltilstander i barrierene som er etablert. Ingen barrierer er perfekte, og over tid vil normal variasjon kunne føre til at det ikke er noen fungerende barrierer – det er et sammenhengende hull tvers gjennom osten og vi har en uønsket hendelse.



Figur 2 - Swiss cheese modellen (Reason, 1997)

2.2.3 Overlappende hendelser

Grøtan og Albrechtsen (2017) påpeker at det også er viktig å se på effekten av samtidige hendelser. Dersom ulike hendelser oppstår samtidig vil det kunne gi:

Escalating effect - En hendelse vil kunne føre til at en annen hendelse får økt effekt.

Additive effects - Det at hendelsene skjer samtidig fører til at den totale effekten blir mer enn summen av de to.

Blocking effect - Fordi hendelsene skjer samtidig faller en funksjon ut, for eksempel to kommunikasjonssystemer som i utgangspunktet er backup for hverandre.

Ressurseffekter - Samtidige hendelser kan være problematiske fordi det er de samme ressursene (personell eller utstyr) som normalt brukes til å håndtere dem.

2.3 UVENTEDE HENDELSER

Verden er heldigvis ikke helt forutsigbar. Samme hvor mye vi forsøker å repetere noe som har skjedd før, så vil det som regel være noen variasjoner. Slike variasjoner fører til læring og vi utvikler vår forståelse av verden omkring oss. Til en viss grad kan vi også forutsi de mulige variasjonene og bruke dem i forhold til planlegging og forberedelser. Det er rimelig å anta at hvis det kommer mye vann i elvene hvert år når snøen smelter, så vil vannmengden variere med temperatur, snømengde, nedbør og lignende. Da er det fornuftig å planlegge for at det enkelte år skjer en opphopning av uheldige faktorer, og vi får usedvanlig store vannmengder, med flom og fare for skade på mennesker og eiendommer som resultat. Slike variasjoner kan vi kalle *uventede* – vi vet ikke når de skjer, men vi er innforstått med at med at de vil inntreffe fra tid til annen.

2.3.1 Uventede og ukjente hendelser

På den annen side overraskes vi fra tid til annen av fenomener som vi i ettertid erkjenner at var mulige, men som vi ikke anså som praktisk mulig før de skjedde. Et klassisk eksempel som også har blitt et begrep er «svarte svaner». Før vestlige mennesker dro til Australia var det en akseptert sannhet at svaner var hvite. Når det så viste seg at i Australia finnes det svarte svaner, rokket det ved definisjonen på en svane. Taleb (2007) lister tre egenskaper ved fenomenet svart svane:

- Det må være høyst uvanlig og uventet, en sjeldenhet («*outlier, rarity*»).
- Det må gjøre en stor innvirkning («*extreme impact*»).
- I retrospekt må det framstå som forklarbart og mulig («*explainable and predictable, after the fact*»).

Det er lett å finne mange eksempler blant menneskeskapte handlinger som passer med denne definisjonen, både 9/11 og 22. juli hendelsene er gode eksempler. Ikke-menneskeskapte hendelser som askeskyen som rammet Europa i 2010 kan også klassifiseres som svarte svaner, fordi omfanget og konsekvensene var så mye større enn ved tidligere utbrudd.[7]

[7] Vulkanutbrudd med tilhørende askesky skjer regelmessig; at det lammer flytrafikken i en hel verdensdel i flere dager var for de fleste svært uventet før det skjedde.

Begrepet svart svane blir av noen avfeid som ikke-vitenskapelig, men Aven (2013) argumenterer med at det er en relevant metafor og diskuterer hvorvidt konseptet svart svane bør knyttes til:

1. En sjelden hendelse med ekstreme konsekvenser.
   («a rare event with extreme consequences»).
2. En ekstrem, overraskende hendelse i forhold til den kunnskapen man besitter.
   («an extreme, surprising event relative to the present knowledge»).

Aven konkluderer med at begrepet svart svane er relevant og at det bør benyttes om situasjon 2 for å være nyttig og interessant. Han vektlegger dermed det at hendelsen er knyttet til vår kunnskap og evne til å forestille oss hva som kan skje, heller enn vår oppfatning om hva som er sannsynligheten for at noe kan skje.

2.3.2 Unknown unknown

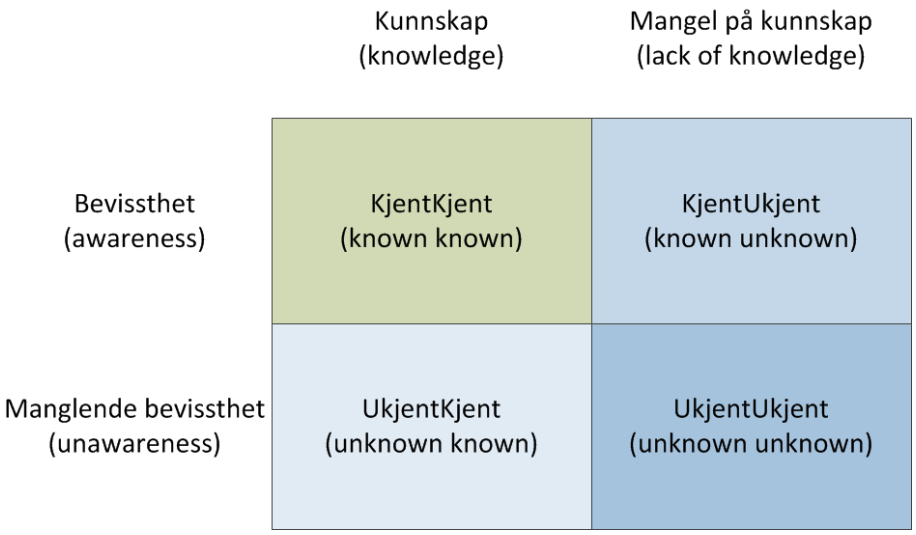
Tidligere forsvarsminister i USA - Donald Rumsfeld - kom i 2002 med en innfløkt[8] uttalelse (Rumsfeld, 2002):

> «T*here are things we know that we know. There are known unknowns. That is to say there are things that we now know we don't know. But there are also unknown unknowns. There are things we don't know we don't know. So when we do the best we can and we pull all this information together, and we then say well that's basically what we see as the situation, that is really only the known knowns and known unknowns. And each year, we discover a few more of those unknown unknowns.*»

Rumsfeld sin kommentar var i relasjon til terrorisme og masseødeleggelsesvåpen – han hevdet at det ikke var mulig å ha kjennskap til alle trusler – det er alltid et element av UkjentUkjent som vi ikke kjenner, men som likevel utgjør en trussel.

De mulige variantene kan tabuleres (Girard & Girard, 2009; Paltrinieri, Dechy, Salzano, Wardman, & Cozzani, 2012) og utforskes mer grundig enn Rumsfeld gjorde i sin korte tale. I fortsettelsen velger jeg likevel å tilegne UkjentUkjent begrepet til Rumsfeld. Figur 3 viser variantene med tilhørende kjennetegn.

[8] Uttalelsen er til dels også latterliggjort og kritisert som vanskelig formulert. Se for eksempel http://www.plainenglish.co.uk/campaigning/awards/2001-2010-awards/2003-awards/811-foot-in-mouth-award-2003.html



Figur 3 – De fire kombinasjonene av kjent og ukjent, oversatt fra Paltrinieri et al. (2012)

Det vi vanligvis kjenner til befinner seg altså i *KjentKjent: D*et er det vi forholder oss til i det daglige. Så er vi klar over at det finnes en del ting vi ikke vet noe om: *KjentUkjent*. Det eksisterer også fenomener vi kjenner til, men ikke er særlig bevisst på, gjerne fordi vi ikke ser dem som relevante lenger: *UkjentKjent*. Rumsfeld sitt poeng er altså at det også eksisterer ting vi ikke har forestilt oss enda: *UkjentUkjent* fenomener. Over tid vil hendelser som skjer gjøre at fenomener beveger seg ut fra UkjentUkjent og opp og mot venstre i matrisen.

2.3.3 Klassifisering av trusler

En mer lineær tilnærming til uønskede situasjoner finner vi hos Westrum (2006) som klassifiserer dem som tre typer trusler:

Regulære trusler *(regular threats)* - Det enkleste å forholde seg til er de regulære truslene, de forekommer ofte nok til at det er fornuftig å utvikle en standard responsmekanisme, og man kan lære av feil som gjøres og stadig forbedre oss. Det er disse truslene man er forberedt på å håndtere i det daglige. Her er det også mulig å si noe om matematisk sannsynlighet for at trusselen skal bli en realitet.

Irregulære trusler *(irregular threats)* - Disse truslene har mye lavere sannsynlighet for å oppstå, men kan ha stor, negativ effekt. De forekommer sjelden, og selv om man er i stand til å forestille seg at de kan skje, så er det for mange mulige scenarier til at det gir mening (mentalt eller praktisk) å forberede seg på alle. Sannsynligheten for at trusselen skal inntreffe blir i praksis gjort som en vurdering heller enn statistisk basert. Det utvikles sjelden standardiserte måter å reagere på, responsen vil sannsynligvis i stor grad være avhengig av håndterende organisasjons kvaliteter.

Helt nye trusler *(unexampled events)* - De helt nye truslene kjennetegnes av at de er så «fantastiske» at man egentlig ikke er i stand til å forestille oss at de kan skje før de virkelig har skjedd. Vår eksisterende mentale referanseramme er ikke lenger gyldig og det må derfor etablere helt ny forståelse *idet hendelsen skjer* (Westrum, 2006).

Trusseltypen er lokalt tolket, regulære trusler i et miljø kan være irregulære i andre miljø.

3 METODE

Jeg vil i dette kapitelet presentere forskningsdesignet og hvordan jeg har samlet inn og deretter strukturert empirien. Jeg vil også se på min forskerrolle og dataenes interne og eksterne gyldighet.

3.1 OVERORDNET FORSKNINGSDESIGN

Mitt mål med oppgaven er å utforske mulige uventede hendelser og eventuelle måter å håndtere slike på i det selskapet jeg er ansatt i. Da jeg planla arbeidet ønsket jeg en eksplorerende tilnærming – jeg ville stille åpne spørsmål og forsøke å ikke være forutinntatt i forhold til informantenes mening om emnet. Jeg hadde ingen spesiell hypotese jeg ønsket å vurdere, men var spesielt opptatt av det vi ikke har sett tidligere – det ukjente.

For å konkretisere arbeidet har jeg utformet en problemstilling:

> *Kan det oppstå uventede hendelser av alvorlig karakter og hvordan kan selskapet eventuelt beskytte seg mot dem?*

Problemstillingen er så brutt ned til to forskningsspørsmål:

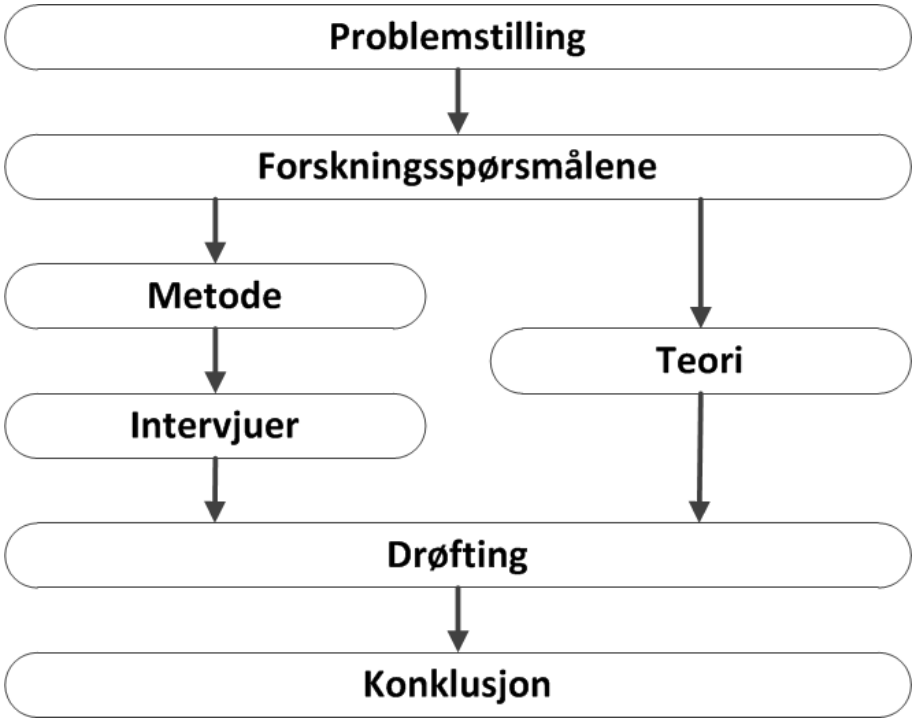
1. *Hva kjennetegner hendelser som er uventede og som kan ha en alvorlig eller katastrofal konsekvens for selskapet?*
2. *Hvordan kan selskapet forhindre at uventede hendelser oppstår og hvordan kan slike håndteres om de skulle oppstå?*

Derfra har jeg utledet en intervjuguide og gjennomført et antall enkeltintervjuer. Intervjuene har jeg så systematisert og forsøkt å finne fellestrekk.

I drøftingen kobler jeg mine funn opp mot teoriene for klassifisering av ukjente hendelser og opp mot beskrivelser av organisasjoner som har vist seg å være robuste.

I konklusjonen tar jeg et tilbakeblikk og ser overordnet på hele oppgaven. Til slutt peker jeg på mulig videre forskning.

Figur 4 viser hvordan det hele henger sammen.



Figur 4 - Visualisering av forskningsdesignet

3.1.1 Kvalitativ metode

For å undersøke min problemstilling har jeg som nevnt valgt kvalitativ metode. Jeg ønsker å utforske det ukjente og ha en åpen datainnsamling om fenomener som er ukjente. Da finner jeg at den kvalitative tilnærmingen er best, fordi jeg som forsker kan sette rammene og lytte til informantenes synspunkt i fri form. Dette gir den fleksibiliteten som jeg tror er ønskelig og nødvendig.

Dersom jeg skulle brukt en kvantitativ tilnærming tror jeg at jeg i mye større grad ville satt premissene for hva som er ukjente hendelser og dermed «låst svarene inne». Et spørsmålsskjema med fastsatte alternativ gir liten mulighet for den som besvarer det til å svare fritt, og det kan være krevende å tolke eventuelle frie kommentarfelt i ettertid og uten informantene til stede. Jeg hadde heller ingen spesiell hypotese jeg ønsket å teste ut og måle informantenes erfaringer opp mot.

En kvalitativ datainnsamling stiller større krav til etterarbeidet i form av systematisering, analyse og aggregeringen av dataene. Samtidig er det nettopp denne friheten jeg ønsket å ha i arbeidet med oppgaven.

3.2 DATAINNSAMLING

3.2.1 Formell godkjenning

Jeg har søkt Norsk senter for forskningsdata (NSD) om tillatelse til å gjennomføre intervjuene, og tillatelse er gitt den 05/12-2016 på prosjektnummer 50864 (Vedlegg A). Jeg har utarbeidet et informasjonsskriv (Vedlegg B) til informantene, som også lå ved søknaden.

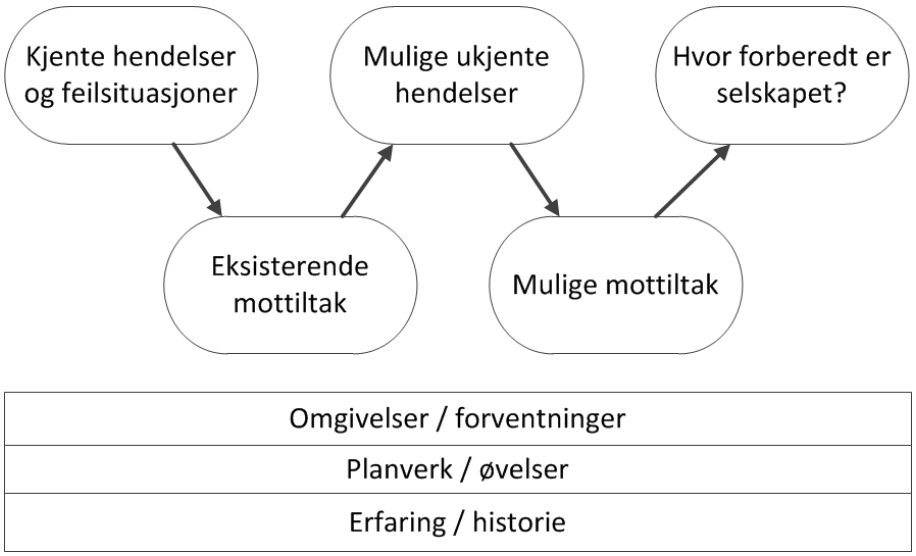
NSD har gitt tillatelse til å ta opp lydfiler under intervjuene, gitt at de behandles forsvarlig under arbeidet med oppgaven og slettes etterpå.

3.2.2 Intervjuene

Jeg har brukt enkeltintervjuer for å samle data, fordi jeg har ønsket en «tett» intervjusituasjon, der jeg har kunnet gå i dybden med en og en person for å utforske emnet. Når man skal diskutere ukjente fenomener synes jeg det er viktig å ha tid til å reflektere over det som kommer fram og forfølge og forstå det det informantene forbinder med emnet.

Som et alternativ vurderte jeg å bruke gruppeintervjuer, men jeg har tidligere erfart at det da kan være vanskelig å få fram all kunnskap informantene har. Slike situasjoner blir gjerne dominert av enkelte deltakere. Dette tror jeg ville blitt forsterket av at informantene ikke utgjør en homogen gruppe og dermed ikke har samme utgangspunkt og meninger.

For å støtte meg i intervjusituasjonen har jeg utarbeidet en intervjuguide (Vedlegg C). Den har fungert mer som en mal enn som en fast agenda. Jeg har brukt den for å sikre at det har vært en skikkelig start og slutt og at alle tema har vært dekket. Figur 5 illustrerer min tilnærming til intervjutemaene.



Figur 5 - Intervjustruktur

Jeg har forsøkt å ha en rød tråd tilsvarende Westrum (2006) sin tilnærming fra regulære til irregulære til helt nye trusler, med mest fokus på de to siste. Samtidig ønsket jeg at noen tema, som for eksempel omgivelsenes påvirkning, ble ivaretatt i alle scenarioene. Intervjuguiden ble laget med utgangspunkt i forskningsspørsmålene og teoriene jeg har inkludert. Jeg vurderte underveis om den burde endres, men fant at det ikke var nødvendig.

Intervjuguiden vektlegger det ukjente og har mange spørsmål knyttet til det – det viste seg å være fornuftig, informantene var mest «selvgående» i forhold til kjente feilsituasjoner og måtte utfordres mer på de ukjente situasjonene.

Selve intervjuene ble gjennomført i møterom for å være på nøytral grunn og ha nødvendig ro. Stort sett har de vært gjennomført mot slutten av, eller etter normal arbeidstid.

Jeg tok opp samtalen på PC og tok i tillegg notater på papir fortløpende. I starten gjentok jeg kort innholdet i informasjonsskrivet og brukte deretter intervjuguiden til løst å styre innholdet. I praksis fungerte den mest som en sjekkliste for meg underveis og som et hjelpemiddel når det var nødvendig med nye vinklinger på temaene. Intervjuene hadde karakter av samtaler, men der jeg forsøkte å være spørrende, nysgjerrig og utfordrende.

De fleste intervjuene tok i overkant av en time. Til slutt presiserte jeg at informasjonen som var gitt ville bli anonymisert og systematisert før den ble brukt i oppgaven.

3.2.3 Informantene

Informantene har blitt forespurt en og en om de vil delta i undersøkelsen, først muntlig og så formelt på epost. I eposten la jeg også ved informasjonsskrivet. Dette inneholdt også samtykkeerklæring som jeg ba om å få signert i retur.

Jeg har valgt ut intervjuobjektene blant nåværende og tidligere kolleger på arbeidsplassen. Jeg har forsøkt å velge personer med litt ulike perspektiver. Det er personer med og uten lederansvar, og blant dem med lederansvar er det både mellomledere og representanter for toppledelsen (Executive) i selskapet. Det er både representanter for Teknologiavdelingen og for Kundeservice/leveranse. Jeg har fokusert på disse to avdelingene siden det er de som har primæransvar for tjenestene og kundenes opplevelse av dem. Dermed vil de også være sentrale for å håndtere ukjente og uventede hendelser som påvirker tjenesteproduksjonen.

Til sammen ni personer ble intervjuet i perioden desember 2016 – januar 2017. I utgangspunktet hadde jeg en lenger liste over mulige informanter[9]. Min intensjon var å intervjue «mange nok» til at temaet var tilstrekkelig belyst. Jeg lagde ikke utgangskriterium og stoppkriterium som beskrevet i Jacobsen (2015), men opplevde i de siste intervjuene at lite nytt kom fram, selv om jeg selvsagt fikk litt ulike vinklinger på de samme temaene. Jeg mener derfor at *metning av informasjon* er oppnådd i tilstrekkelig grad.

Jeg har bevisst valgt mange ledere blant informantene fordi jeg har ønsket personer som i kraft av sin stilling ikke bare må forholde seg til de daglige oppgavene, men som også har et ansvar for å tenke framover – hva kan oppstå i morgen, hvilke utfordringer kan selskapet måtte håndtere. Jeg tror det er spesielt viktig å forstå lederes perspektiv for å kunne mene noe om organisasjoners reaksjoner i ukjente situasjoner.

Det er min intensjon at alle intervjuobjekter skal være anonyme. Jeg har med noen direkte sitater, uten at de skal være mulig å bringe tilbake til enkeltpersoner. Alle informantene er orientert om at det også etter intervjuet har vært mulig å trekke seg og kreve opplysningene slettet, men ingen har benyttet seg av det.

Jeg har møtt stor velvilje blant de som har latt seg intervjue, og det har vært interessante samtaler. Som regel har vi gått ut over avsatt tid, da vi begge har funnet det spennende å diskutere.

[9] Jeg bruker for det meste begrepet «informant» om de jeg har intervjuet for å vise at de er direkte bidragsytere til forskningen og at intervjuet har hatt preg av en samtale. Alternativt kunne «respondent» vært brukt, men for meg har det mer preg av en som besvarer et (kvantitativt) skjema.

3.2.4 Koding og kategorisering

Etter intervjuene har jeg transkribert lydfilene og sammenstilt dem med de notatene jeg gjorde på papir. Deretter har jeg forsøkt trekke sammen og systematisere de funn og observasjoner som finnes ved å samle alle punkt som ligner hverandre. Denne listen er så brukt som disposisjon for kapittel 4.

Det ville vært interessant om en annen person hadde analysert rådataene og systematisert dem, for så å sammenligne med min analyse. Dessverre er det ikke mulig innenfor rammene av denne oppgaven.

Hver enkelt informant har bare blitt intervjuet én gang. Jeg kunne ha gjennomført en oppfølgingssamtale med hver enkelt. Da ville det vært interessant å høre om vedkommende hadde reflektert over temaene og kommet opp med nye vinklinger eller synspunkt på andres innspill. Det kunne også vært mulig å tatt en gjennomgang av det som ble transkribert for å se om det var riktig oppfattet. Dessverre har det ikke vært mulig, både av hensyn til egen tid og ikke minst belastningen for informantene. Det har av samme grunn heller ikke vært gjennomført annen ekstern validering – for eksempel intervjuer i et annet selskap.

3.3 MIN ROLLE

Jeg skriver oppgaven som ledd i videreutdanning, der dokumenterte utgifter er refundert av arbeidsgiver. Det har ikke fulgt med noen føringer i forhold til hvilket tema oppgaven skal handle om, hvilke eventuelle hypoteser som skal undersøkes eller hvilket case som skal behandles.

Jeg har valgt å skrive oppgaven med utgangspunkt i eget selskap. Der har jeg erfaring fra flere avdelinger og jeg har hatt ulike roller, både med og uten lederansvar. Informantene er personer jeg kjenner som kollegaer og noen også som venner. I en slik situasjon er det naivt å tro at jeg kan være en helt nøytral forsker og ikke ta med meg holdninger, meninger og tidligere erfaringer inn i den nye rollen. Dette har jeg forsøkt å være bevisst på under hele prosessen.

Jeg har valgt kvalitativ metode for å kunne ha en åpen datainnsamling. Under intervjuene har jeg presisert at vi møtes i en nøytral intervjusituasjon og på nøytral grunn. Jeg har for tiden har ikke personalansvar for noen av informantene. Det er mulig at jeg har utviklet «blinde flekker» (Jacobsen, 2015) i forhold til egen organisasjon, men jeg har forsøkt å være bevisst på situasjonen og lydhør overfor alt som har kommet fram i intervjuene.

På den annen side har jeg opplevd en del fordeler med det å forske på egen organisasjon. Det har vært enkelt å få tilgang på gode informanter som velvillig har ønsket å bidra. Fordi jeg har god kjennskap til organisasjonen tror jeg også jeg har klart å finne et godt utvalg av informanter, inkludert noen som nylig har gått videre til andre arbeidsgivere. Interne forkortelser og «stammespråk» - spesielt i eksempler på tekniske feilsituasjoner - har heller

ikke vært noe problem. Det har dermed ikke vært nødvendig å bruke mye tid på å avklare begreper.

For at oppgaven skal være spennende, ønsker jeg at den ikke bare skal være beskrivende om hva informantene tror og mener at situasjonen er, men at jeg også behandler hva selskapet kan gjøre. I overgangen fra det deskriptive til det normative har jeg forsøkt å ta forskerens drøftende perspektiv og være bevisst på *ikke* å ta mitt perspektiv som mellomleder i selskapet.

3.4 DATAENES INTERNE GYLDIGHET

I intervjusituasjonen opplevde jeg informantene som åpne og ærlige. Jeg tror ikke de bevisst holdt tilbake noe informasjon, tvert imot framsto de som interesserte og engasjerte og som nevnt gikk flere intervjuer utover tiltenkt tid. Jeg opplevde også som beskrevet ovenfor at *metning* oppsto. Det er selvsagt ingen garanti for at ikke nye perspektiver ville kommet fram om jeg hadde gjennomført flere intervjuer, men jeg opplever at dataene godt representerer tilstanden i selskapet på det aktuelle tidspunktet, og at de er et riktig utgangspunkt for analysen i kapittel 5, både i forhold til reliabilitet og validitet.

3.5 EKSTERN GYLDIGHET

Ekstern gyldighet dreier seg om i hvilken grad funnene fra en undersøkelse kan *generaliseres til andre enn dem man faktisk har undersøkt* (Jacobsen, 2015).

I oppgaven og datainnsamlingen har jeg vært særlig opptatt av nettverkstjenester og kundepåvirkning, men som nevnt i kapittel 1.2 er det mange andre interne forhold som kunne vært analysert i forhold til mulige årsaker til uventede hendelser. Det er også mulig å se til andre selskaper og organisasjoner for å undersøke om de kan oppleve uventede hendelser.

Jeg tror at funnene kan generaliseres til å gjelde andre områder – både internt og eksternt. Det uventede vil kunne oppstå andre steder og det virker rimelig at en tilsvarende klassifisering og analyse vil være meningsfull også i andre omgivelser. Uventede hendelser er en generell utfordring for de fleste organisasjoner, og jeg tror tiltakene jeg beskriver kan være gyldige også i andre bransjer og virksomheter.

4 FUNN OG ANALYSE

Jeg vil først se kort på selskapets situasjon og organisasjon. Deretter presenterer jeg funnene og følger da samme struktur brukt i intervjuene (Figur 5).

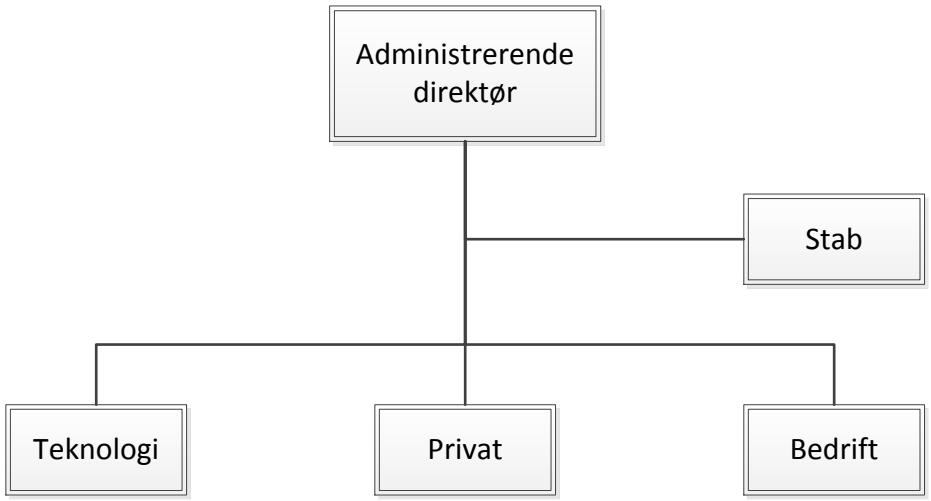
4.1 FAKTA OM SELSKAPET

Jeg fokuserer på et selskap som har sin virksomhet i Norge. Det er et av flere selskap i et holdingselskap som også eier andre virksomheter både innenlands og i utlandet.

Noen fakta for 2016:

- Bruttoomsetning på drøyt 1,1 milliarder NOK.
- Tilbyr internett, mobiltelefoni, IP-telefoni og IPTV,[10] samt private nett for bedrifter.
- Betjener både privat- og bedriftskunder, omtrentlig fordelt på hhv. 3/4 og 1/4 av omsetningen.
- Totalt 160 000 bredbåndstilknytninger.
- Holdingsselskapet (morselskapet) er notert på Oslo Børs.

Ved årsskiftet 2016/2017 er selskapet organisert i to markedsrettede divisjoner: Privat og Bedrift som hver har resultatansvar og kontroll over sine respektive verdikjeder, inklusive leveranse og kundestøtte. Utvikling og teknisk drift er organisert i Teknologidivisjonen. Til slutt er det også en stabs-/støttedivisjon som inneholder økonomi, HR, innkjøp og lignende. Figur 6 illustrerer dette.



Figur 6 - Selskapets organisering

Toppledelsen (Executive) utgjøres av administrerende direktør og direktørene for Privat, Bedrift, Teknologi.

[10] IP-telefoni og IPTV er hhv. telefoni og fjernsyn levert over internett, altså via IP-pakker over bredbånd. Tjenestene har gjerne ekstratilbud som for eksempel filmleie og webgrensesnitt. Den største fordelen – og ulempen – er at alle tjenestene leveres over samme kabel. Dette gjør det rimeligere, men gjør også at feil på kabel eller utstyr gir større konsekvens.

Selskapets hovedkontor er i Oslo med et avdelingskontor i Bergen. Deler av selskapets ledelse og noen tekniske ressurser samt noen salgsressurser befinner seg i Oslo. Størstedelen av de ansatte er samlet i Bergen, herunder store funksjoner som kundeservice, leveranse og mesteparten av teknologi og stab.

Kundene møtes og betjenes hovedsakelig i tre akser:

- Salg.
- Leveranse.
- Kundeservice.

Alle tre aksene eksisterer både i Privat og Bedrift. Det er altså Kundeservice som har ansvaret for tradisjonell feilhåndtering mot sluttkunder.

Den tekniske driftsorganisasjonen tilhører som nevnt Teknologi. Der overvåkes nett og tjenester både i forhold til feil og ytelse i avdelingen Nettdrift. Personellet der har fokus på fellesfunksjoner og fellesfeil i motsetning til kundeservice som mer har fokus på enkeltkunder og enkeltfeil.

4.2 KJENTE FEILSITUASJONER

Mange av feilsituasjonene som sluttkundene opplever er knyttet til feil i hjemmet eller i den lokale bedriften. Det kan være feil på den kundes linje eller tilhørende kundeutstyr. Slike lokale feil ser jeg bort fra, siden de ikke har den ikke har høy nok alvorlighetsgrad.[11]

4.2.1 Tekniske fellesfeil

De feilsituasjonene som alle informantene nevner som «vanlige feilsituasjoner» er det som kalles tekniske fellesfeil. Datakommunikasjon er selskapets hovedprodukt i seg selv og er en viktig transporttjeneste for de andre tilleggstjenestene. Enhver feil som går ut over nettverkets stabilitet er derfor potensielt alvorlig. Vanlige tekniske fellesfeil omfatter:

- Brudd i fiber- eller andre transportsamband.
- Brudd i strømtilførsler.
- Feil i maskinvare.

Dette er relativt vanlige feil som Nettdrift håndterer rutinemessig. Alle informantene gir uttrykk for at selskapet er gode på å håndtere slike feil i den forstand at:

- Informasjon om feil blir raskt spredd internt.
- Det eksisterer en eskaleringsmatrise i forhold til informasjon ved feil av ulikt omfang.
- Teknologi vet hvordan tekniske feil av denne typen skal løses, og det gjøres raskt og effektivt.

[11] For kunden det gjelder kan tjenesteavbruddet selvsagt være alvorlig, men med mindre det er en systematisk feil (dårlig kvalitet, tjenesteangrep) som gjelder mange tjenester, så er det for selskapet en lokal, avgrenset hendelse.

Et fellestrekk ved disse situasjonene er at de som regel oppstår uten at noen har ønsket det. Det kan være en menneskelig handling som utløser det – en uheldig gravemaskinfører som graver over en fiberkabel – men det er sjelden det er gjort med hensikt.

Menneskelige feil i nettverksutstyret forekommer også. De kan være direkte, ved at en tekniker utfører en manuell oppgave som feiler eller får utilsiktede konsekvenser. Selskapet har hatt eksempler på at den type feil har gjort tjenesten utilgjengelig for deler av kundemassen i kortere tid, men det har så langt ikke forårsaket massive utfall over lengre tid. Det er mange regler og prosedyrer på plass for å hindre og minimere denne typen feil, slik som:

- Kompetansekrav.
- Tilgangsbegrensning til utstyr i forhold til kompetanse og arbeidsoppgaver.
- Krav om «fire øyne» på enkelte operasjoner.
- Noen operasjoner tillates bare i forhåndsvarslede servicevinduer.
- Kontinuerlig automatisk logg av alle manuelle kommandoer på utstyr.
- Regelmessige sikkerhetskopier av alle konfigurasjoner.

Det kan også forekomme feil i ulike typer programvare, både den som direkte styrer utstyret og diverse støtteprogramvare for provisjonering / endring. Eksempler på tiltak i forhold til dette er:

- Konservativ oppgraderingsmetodikk, ikke «bleeding edge».
- Testing og verifisering i labmiljø av nye funksjoner.

Både for manuelle konfigurasjonsendringer og programvareendringer praktiseres det et «frysregime» ved det at man unngår å gjøre endringer like før perioder med lavere bemanning (helg, høytid) og at man unngår dem i størst mulig grad i ferieperioder. Avhengig av størrelse og antatt risiko på endringene som gjøres kan det også finnes formelle gjennomføringsplaner inkludert plan for gjenoppretting (tilbakerulling) av tjenesten om endringen skulle feile eller få utilsiktede konsekvenser.

De senere årene har det blitt stadig vanligere med en type angrep over Internett kalt DDoS[12]. I korthet går det ut på å sende så store mengder trafikk til en mottaker at den blir overveldet – legitim trafikk blir fullstendig blokkert. Det eksisterer illegale nettverk der man billig kan kjøpe slike angrep. Angrepet blir da styrt fra et sted, men trafikken kommer fra mange ulike punkter, typisk maskiner som tidligere har fått virus og dermed blitt «tatt over». Slike angrep kan rettes mot enkeltpersoner, mot selskap eller mot nettverksoperatørene. Det er vanskelig å forhindre dem, men de er relativt grei å bekjempe med de rette verktøyene og god kontakt med omkringliggende nettverksoperatører.

[12] DDoS: Distributed Denial of Service. Se f.eks. http://nordic.businessinsider.com/amazon-spotify-twitter-github-and-etsy-down-in-apparent-dns-attack-2016-10 eller http://variety.com/2016/digital/news/twitter-netflix-amazon-spotify-down-internet-outage-ddos-attack-1201896595/ som omhandler et DDoS angrep mot en DNS leverandør, som gjorde at brukere hadde problemer med å nå Amazon, Twitter, Spotify m.fl.

4.2.2 Ikke-tekniske situasjoner

Informantene har i liten grad erfart situasjoner som berører hele eller store deler av selskapet eller kundemassen, men som ikke er av teknisk karakter. Det nevnes bare to situasjoner, en opplevd og en teoretisk.

For kunder i Bergensområdet er det mulig å møte fysisk opp i selskapets lokaler for å betale utestående regninger (for å få gjenopprettet en stengt tjeneste), for å bytte ødelagt utstyr eller på annen måte få bistand. Det oppleves som positivt for kundene at de kan henvende seg til «ekte» mennesker og få assistanse, og i noen tilfeller går det også raskere, spesielt om det må byttes noe utstyr. I dette kundemottaket har det vært noen eksempler på kunder som har oppført seg ubehagelig og truende. Dette har ført til politianmeldelser, i de tilfellene hvor kundebehandlerne har blitt fysisk truet. Det har også vært truet med å sette fyr på eller bombe lokalene. En mulig videre konsekvens av dette vil være evakuering av lokalene, med tilhørende full stans i kundeservice, samt pågående leveranse og drift.

En mulig, ikke-opplevd trussel er brann. En brann i lokalene vil særlig være problematisk i forhold til to dimensjoner:

- Teknisk utstyr, servere og data.
- Organisasjonens evne til normal produksjon.

Det er særlig kundeservice som vil være nødt til å re-etablere seg raskt på en alternativ lokasjon dersom egne lokaler ikke lenger lar seg benytte. Ingen av informantene kjente til at det nå finnes håndfaste planer for dette. Tidligere har det eksistert en ordning med mulighet for å sette opp et midlertidig kundesenter basert på mobiltelefoner og bærbare PCer på en skole, men dette har ikke blitt videreført – uvisst av hvilken grunn.

4.3 MOTTILTAK – KJENTE FEILSITUASJONER

I forhold til de vanlige – kjente – feilene har selskapet mange mottiltak, både av preventiv og avbøtende karakter.

4.3.1 Tekniske mottiltak - nettverksfeil

Mange av de tekniske feilene regnes som uunngåelige, og det legges vekt på å hindre skadevirkningene heller enn å unngå selve feilen. Eksempler på dette er:

- Feil i strømforsyning: Doble strømforsyninger.
- Brudd i nettverk til viktige komponenter: Doble linjer som tilførsel, helst med adskilt føringsvei.
- Feil på kort i utstyr: Koble tilførselslinjene til ulike kort.

Det å bygge redundans på denne måten for å begrense / hindre negativ effekt er svært vanlig i nettverksbransjen. Det gjøres i leverandørens eget nettverk, og selges også som egne løsninger til kunder med høye krav til oppetid[13].

4.3.2 Designmessige mottiltak – nettverksfeil

I selskapets tydeligste vekstfase, fra oppstarten i 2000 og fram til ca. 2006, gikk utbyggingen av nettet og tjenestene til tider svært raskt. Som et resultat av dette ble ikke all utbygging gjort like konsistent. I tillegg var teknologien i en rivende utvikling. Dette førte til en del alvorlige feil som ble opplevd som vanskelig å løse fordi det var vanskelig å se hvordan «det var ment å virke». Dette er et ikke ukjent teknisk fenomen; når et teknisk komplisert system har fått utvikle seg over tid uten en grunnleggende plan så blir det ofte vanskelig å forstå helheten og interaksjonene mellom de ulike delsystemene. Flere av informantene trekker fram nettopp *god design* som et viktig element for å unngå feil, men også for raskt å reetablere tjenester ved feil som krever manuell innsats (i motsetning til automatisk reruting[14]).

En egenskap ved god design som framheves er *enkelhet*. Dersom det eksisterer to alternative design for en oppgave, foretrekker de designansvarlige den som oppfattes som enklest i kontekst av kompetansen hos avdelingene for design og drift av nettet.

En annen egenskap som vektlegges ved god design er *gjentagelse*. Samme utfordring skal løses på samme måte alle steder. Der man tidligere kunne oppleve at noen telesentraler var tilkoblet resten av nettverket på en forunderlig måte, har man i dag standardisert «arbeidstegningene» og gjenbrukt designet over alt. I forlengelsen av det har det også vært vist vilje og evne til å ta kostnadene med å oppgradere og gjennomføre endringene over alt når det har vært fornuftig å endre grunndesignet.

En informant brukte følgende bilde for å illustrere dette punktet:

> *«Når du sitter helt alene midt på natten og må håndtere en alvorlig nettverksfeil så skal det ikke være nødvendig å hente fram dokumentasjon og lese deg fram til hvordan ting skal være. Du skal huske de viktige elementene i designet og det skal være logisk. Kreftene skal brukes på problemløsning!»*

4.3.3 Mottiltak - kundemottak

I forhold til kundemottak og truende kunder er det innført en rutine med skjult alarmknapp med varsling til kundeservice og en tilhørende rutine som sier noe om hvordan man skal oppføre seg ved truende kunder – både i forhold til den som føler seg truet og i forhold til de som blir varslet og som skal bistå. Dette er et lokalt tiltak som er kjent i avdelingen som

[13] Oppetid regnes i prosent tilgjengelighet av tjenesten over en periode, som regel pr. måned. Typiske oppetidsmål er «bedre enn» 99,95% – 99,99%. For å nå 99,99% oppetid på en måned kan tjenesten maksimalt være utilgjengelig drøyt fire minutter.

[14] Moderne datanettverk har som regel automatisk reetablering av tjenester i flere lag. De forutsetter selvsagt at det eksisterer eller er mulig raskt å etablere alternative veier ved brudd eller kvalitetsforringelse i primærveien. Slik automatisk reruting skjer som regel i løpet av noen titalls millisekunder ved moderne protokoller, opp til noen sekunder ved alvorlige feil.

bemanner kundemottaket, men det eksisterer ikke en tilsvarende generell rutine for hvordan man skal håndtere en større truende situasjon rettet mot alle i bygningen.

4.3.4 Mottiltak – organisasjon

Ved større tekniske feil med ukjent årsak hadde alle informantene en klar mening om at det skulle etableres en midlertidig kriseorganisasjon for å løse det tekniske problemet. Imidlertid var det stor variasjon i meningene om hvordan dette skulle gjøres. Noen refererte til planer som skulle eksistere, men som de ikke var sikker på hvor var, andre til at «det er slik vi pleier å gjøre det». Enkelte visste om at det er klargjort et møterom med blant annet nødstrøm, andre var ukjent med det. En klar forventning fra mange av informantene på teknisk side var at etableringen av et slikt «war room» ville bidra til at de fikk «jobbe i fred», altså fokusere all innsats på problemforståelse og –løsning. Historisk har leder for Nettdrift eller leder for Teknologi vært den som har bestemt at «war room» skal etableres og hvem som skal delta. Vedkommende leder er da også den som har håndtert ekstern informasjon og oppdatert resten av organisasjonen.

Tidligere fantes det rutiner for å etablere en tilsvarende krisestab på selskapsnivå, der selskapets ledelse skulle samles når det oppsto feil som ble vurdert som så alvorlige at det kunne gå betydelig ut over selskapets omdømme eller økonomi. Flere informanter savnet denne type krisestab på nylige hendelser og situasjoner, og en av dem oppsummerte det slik:

> *«Når vi ikke tar nesten-situasjoner på alvor – hvordan skal vi da kunne håndtere den store smellen? De har bedre rutiner for dette i en vanlig barnehage enn her hos oss!»*

4.4 MULIGE UVENTEDE OG UKJENTE HENDELSER

Informantene forteller i liten grad uoppfordret om mulige ukjente hendelser. På mer direkte, utforskende, spørsmål kommer det likevel opp noen eksempler på slike.

4.4.1 Force Majeure – type hendelser

Store hendelser som krig og naturkatastrofe nevnes som mulige, men lite realistiske hendelser. De fleste informantene mener det er mulig at en slik situasjon kan oppstå, men anser at da er samfunnet og omgivelsene mye mer forståelsesfulle i forhold til selskapets forpliktelser:

> *«Ingen forventer at vi har beredskap for å takle den type situasjoner uten kundepåvirkning.»*

4.4.2 Mindre alvorlige natur-/miljøhendelser

Det er mulig at lokalene kan brenne opp eller at fly kan styrte i nærheten. Mer sannsynlig er kanskje det som man har opplevd andre steder, at hele områder har måttet evakueres i perioder på grunn av eksplosjonsfare.[15]

4.4.3 Utro tjener

Flere av informantene fra teknisk side mente at en ansatt med tilstrekkelige adgangsprivilegier kan utgjøre en alvorlig trussel. Det ble vurdert som lite sannsynlig, og ikke noe man hadde opplevd fra ansatte i Teknologiavdelingen. Skadepotensialet ved en «utro tjener» med de rette tilgangene og tilstrekkelig kompetanse ble ansett som meget stort. Bare det å hindre andre teknikere (kollegaer) tilgang til nettverksutstyret ville være svært alvorlig (noe som faktisk har skjedd hos andre[16]). Enda mer ødeleggende ville det være med en systematisk sletting av konfigurasjoner og påfølgende omstart av utstyret. I verste fall må det da personell fysisk ut på hvert eneste sted for å gjenopprette tjenestene. Dette vil ta lang tid.

Gitt at man først har en situasjon med en utro tjener som utfører slike handlinger, så risikerer man også at vedkommende ikke «gir seg til kjenne» umiddelbart. Dermed vil vedkommende høyst sannsynlig også bli involvert i analyse av situasjonen og forsøk på å utbedre den – noe som igjen kan benyttes til ytterligere å forverre ting og forsinke gjenopprettingen av normal tjeneste. Spesielt et par av informantene med lederansvar dvelte mye ved den ledelsesutfordringen det ville være å få mistanke om en slik situasjon og hvordan man skal opptre dersom mistankene eventuelt blir bekreftet.

4.5 MULIGE MOTTTILTAK – UKJENTE HENDELSER

Flertallet av informantene var først tvilende til om det var mulig å forberede seg på ukjente hendelser, men ved nærmere refleksjon kom det likevel opp mange forslag.

4.5.1 Ledelse

Det at lederne er forberedt på at de skal opptre annerledes i uventede situasjoner ble nevnt. Det var både en forventning og et ønske om at ledere skulle opptre mer autoritært og styrende, for å prioritere og fokusere innsatsen. Tilsvarende at den enkelte medarbeider måtte være forberedt på å bli ledet på en annen måte.

---

[15] Se f.eks. http://nrbr.no/om-oss/nrbrs-avdelinger/operativ-avdeling/propanbrannen-pa-lillestrom-stasjon/ Propanbrannen på Lillestrøm stasjon i april 2000 førte til at 2000 mennesker ble evakuert og luftrommet over Lillestrøm stengt. Situasjonen vedvarte i mer enn fire og et halvt døgn.

[16] Terry Childs ble i 2008 fengslet fordi han ikke ville oppgi passordene han hadde konfigurert i utstyret tilhørende San Francisco sitt kommunale fibernettverk. Dette førte til at ingen andre enn han selv kunne gjøre endringer eller rette feil. Han var av mange oppfattet som den mest erfarne ansatte i avdelingen som administrerte nettverket, og oppga at han ikke stolte nok på ledelsen og kollegaene til å la dem «slippe til» i nettverket. Se f.eks. http://www.sfgate.com/bayarea/article/S-F-officials-locked-out-of-computer-network-3205200.php

4.5.2 Informasjon internt og eksternt

Det eksisterer allerede et godt system for å varsle internt ved større og mindre hendelser. Systemet er basert på interne websider, SMS og epost, og det er åpent i den forstand at det er enkelt å legge til hendelser og enkelt å melde seg på varsling i den kategorien man ønsker. De fleste lederne abonnerer på slike driftsmeldinger og blir dermed automatisk holdt løpende oppdatert på feil over en viss størrelse.

På feil av et visst omfang eller en viss alvorlighetsgrad blir det også vurdert om man skal varsle kunder. For noen typer feil skjer dette nesten automatisk – det er bare en operatør som må godkjenne at meldingen sendes. For noen tjenester kreves det mer manuelt arbeid, for eksempel i forhold til å vite hvilke kunder som er berørt. Når det gjøres kundevarsling av uvanlige feil er det kundeservice som har ansvaret for å formulere en melding som er presis og informativ nok, uten å gå for mye i detaljer. Kundeinformasjon anses som et tveegget sverd – for lite eller for mye informasjon fører til uønsket oppmerksomhet og påtrykk fra kunder og media. Det eksisterer også en viss frykt for å være for åpen, i forhold til konkurrenter og omdømme.

4.5.3 Samarbeid og rolleavklaring

Som nevnt håndteres «vanlige» og kjente feil bra og med forutsigbar løsningstid. Dersom man har «uvanlige» feil er ofte årsak, løsning (eventuelt «workaround») og løsningstid ukjente. Det samarbeidet som må oppstå når mange teknikere med ulike kompetanse, arbeidsfelt og oppgaver skal settes sammen, nevnes som noe selskapet godt kunne øvet mer på. En slik øvelse forventes da å fokusere på samarbeid, organisering/rolleavklaring og problemløsningsprosessen, slik at man etterpå kan se hva som fungerte bra og hva som bør justeres.

Spesielt nevnes bedre samarbeid og samhandling i aksene Teknisk–Kundeservice og Ledelse–Omgivelser som et øvingstema. Flere av informantene var bekymret fordi dagens ledelse ikke hadde måttet håndtere store, pågående feil.[17]

4.5.4 Det praktiske

Dersom en uventet, alvorlig feil oppstår i arbeidstiden har de fleste en forventning om at det praktiske «ordner seg». Folk er tilgjengelige og kan om nødvendig hentes ut av møter eller omprioriteres på annen måte. Det er tilgjengelig ressurser for å utføre manuelle varslingsoppgaver, hente inn flere medarbeidere, kontakte leverandører og så videre.

Derimot uttrykkes det mye større uro i forhold til det praktiske når noe skjer utenfor kjernetiden. Et eksempel som trekkes fram er en større nettverksfeil på Sørlandet som skjedde på en søndag morgen. Teknisk sett var det en «lettforståelig» situasjon: To redundante linjer inn til et større område på Sørlandet hadde sviktet, dermed var flere tusen kunder uten internett. Noen av dem har IPTV og manglet dermed også fjernsyn. Hadde det skjedd i arbeidstiden ville det vært naturlig å informere via SMS, epost og informasjon på sosiale medier (primært facebook). Selskapet har etablert tekniske vaktordninger som sikrer

[17] Merk at det ikke betyr at det ikke har vært store feil under dagens ledelse. De feilene som har vært har blitt håndtert av linjeorganisasjonen og «ad hoc», uten at krisestab har vært etablert, eller toppledelsen (utover linjen) har vært involvert.

at det å detektere, finne og rette feil er en 24/7 operasjon, men det mangler tilsvarende løsninger på kundeservice. Dermed ble det en «best effort» innsats i forhold til å skulle informere kundene og holde dem løpende informert. Det var bare en mellomleder tilgjengelig fra kundeservice. Vedkommende løste situasjonen etter beste evne, men fikk ikke mobilisert flere ressurser hverken fra ledelsen eller kundeservice.

I forlengelsen av dette påpekes det også at man tenke seg betydelig større problemer dersom selskapets lokaler eller mobilnett[18] var rammet.

> *«Hvis ikke vi får tak i ressurser på en såpass liten feil en søndags morgen, hva da hvis vi har en alvorlig feil som også rammer oss selv på et enda mer ugunstig tidspunkt?»*

4.5.5 Bevisstgjøring

> *«Vi har blitt så flinke til å unngå vanskelige feil at jeg tror vi har blitt mindre flink til å håndtere dem».*

Sitatet er fra en av de tekniske informantene, og kommer til uttrykk hos flere. Det at det er brukt betydelige ressurser på å bygge redundans og benytte standard designmaler ved utbygging, har som forventet ført til at antallet feil har gått ned og færre «uforståelige» feil har oppstått. Påstanden er at dette også kan virke negativt – en organisasjon som sjelden må håndtere vanskelige situasjoner *og* som ikke har fokus på å forberede seg / øve blir dårligere «når det gjelder».

4.6 HVOR FORBEREDT ER SELSKAPET?

I forrige kapittel pekte informantene på ulike tiltak som kunne hjelpe selskapet til å gjenopprette normalsituasjon dersom en tidligere ukjent hendelse skulle oppstå. Oppsummert virker den enkelte å ha tro på egen evne til å løse hendelser som påvirker egen avdeling, forutsatt at det er noe som er observert tidligere eller ligner noe som har skjedd før, spesielt hvis det skjer i eller i nærheten av normal arbeidstid.

Derimot er det mer usikkerhet knyttet til hvordan selskapet vil håndtere store hendelser, både de som bør være mulig å forutse og de som er nye. Både i forhold til samhandling og ledelse virker det å være ulik oppfatning av hvem som skal gjøre hva og ansvarsområdet til hver enkelt.

[18] Selskapet er virtuell mobiloperatør – såkalt MVNO – og alle selskapets mobiltelefoner unntatt noen dedikerte tekniske vaktmobiler er meldt inn i selskapets nett. Dersom (MVNO) mobilnettet faller ut, mister man dermed også muligheten til å kommunisere med ansatte via tjenestemobil.

5 DRØFTING

I drøftingen vil jeg vende tilbake til problemstillingen ved å diskutere og forsøke å besvare de to forskningsspørsmålene.

5.1 FORSKNINGSSPØRSMÅL 1

> *Hva kjennetegner hendelser som er uventede og som kan ha en alvorlig eller katastrofal konsekvens for selskapet?*

Jeg tar utgangspunkt i to nøkkelord i denne setningen; «uventet» og «alvorlig».

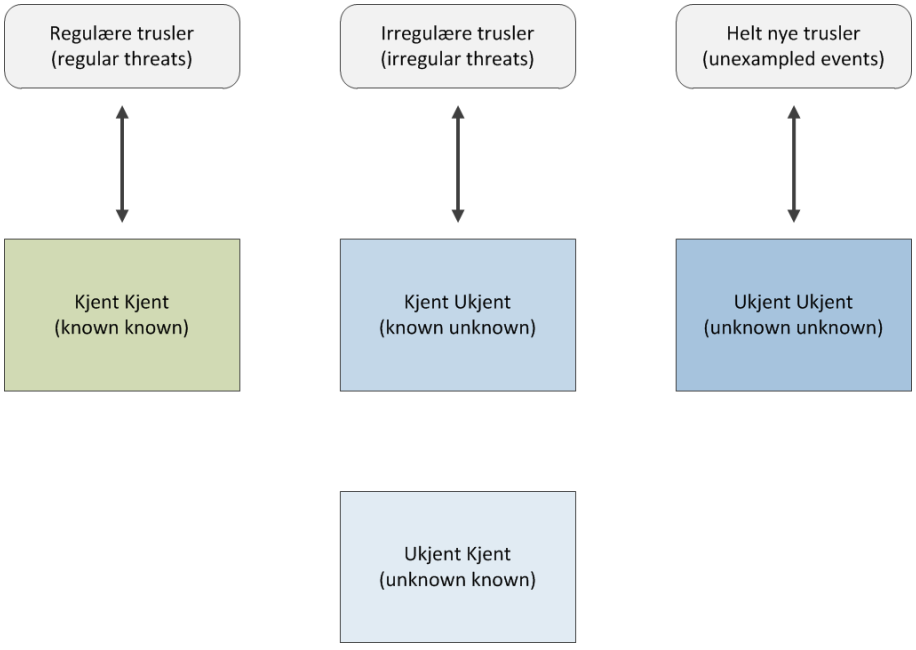
5.1.1 Det uventede

I denne sammenhengen er det de uønskede hendelsene jeg utforsker, og det uventede blir dermed en trussel mot en stabil, normal situasjon.

Slike uventede trusler kan deles videre opp i to kategorier, de kjente og de ukjente. De kjente truslene har organisasjoner et forhold til og som regel mer eller mindre formelle responsmekanismer for å håndtere.

De ukjente truslene deles ytterligere opp av Westrum (2006) i irregulære og helt nye trusler. Rumsfeld (2002) ser ikke direkte på trusler men på den kunnskapen vi besitter og vårt forhold til det vi vet og det vi ikke vet.

Jeg ser paralleller mellom Westrum og Rumsfeld sine beskrivelser og mener de kan tabuleres som vist i Figur 7. Selv om Westrum bruker trusselbegrepet, så er essensen det samme: Det vi vet og forholder oss til, påvirker hvordan vi kan forberede oss.



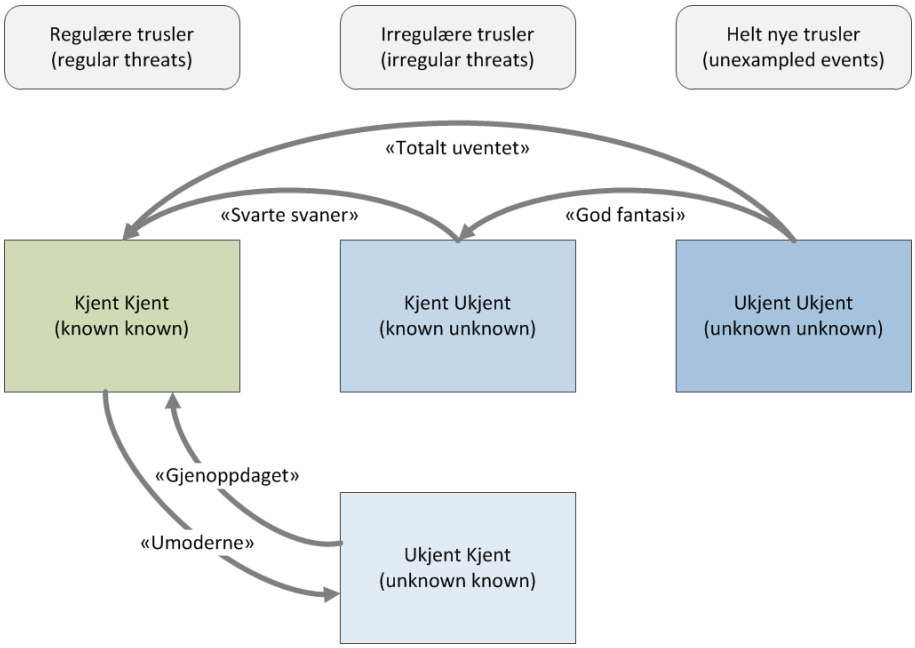
Figur 7 - Mapping mellom Westrum og Rumsfeld

Jeg klassifiserer både KjentUkjent og UkjentKjent som irregulære trusler. KjentUkjent er irregulære trusler vi ikke har forholdt oss til, mens UkjentKjent er trusler man tidligere var oppmerksomme på, men som over tid har mistet aktualiteten. Dette kan ha skjedd bevisst eller ubevisst. Et eksempel kan være stabiliteten i strømnettet. Vi har blitt så vant til å ha stabil tilgang på strøm, at mange i dag ikke har gode alternativer til å varme opp boligen ved lange strømutfall.

Rumsfeld sin oppdeling er mer granulær, og jeg bruker i hovedsak den i fortsettelsen.

5.1.2 Endring i hva som er uventet

Vår kunnskap utvikler seg over tid, det som var utenkelig i går kan være dagligdags i morgen. Den kunnskap vi besitter og er bevisst på, befinner seg altså i KjentKjent. For å illustrere hvordan kunnskap kan utvikle seg har jeg beskrevet noen overganger i Figur 8.



Figur 8 - Overganger mellom ulike trusler

Den eneste overgangen i denne modellen som beveger seg i retning bort fra KjentKjent er «Umoderne». Den viser at når kunnskap ikke lenger er i vår bevissthet så blir den umoderne og ikke tatt med i betraktningen når vi skal gjøre vurderinger. Overført til trusler og risikovurderinger så kan det være fenomener vi har sett tidligere men som ikke lenger blir vurdert som relevante. Det kan være fordi de forekommer så sjelden eller fordi utvikling har gjort at vi bevisst eller ubevisst velger å se bort fra dem.

Overgangene mot KjentKjent kommer fra det jeg til nå har omtalt som uventede og ukjente hendelser. En ukjent hendelse vil før den skjer tilhøre en av de tre andre kategoriene:

UkjentKjent - Hendelsen har blitt observert tidligere, men er ikke lenger forventet.

KjentUkjent - Vi kan forestille oss hendelsen, men regner den ikke som forventet.

UkjentUkjent - Hendelsen er helt uventet. Før den skjer vil bare de med god fantasi forsøke å tabulere den som KjentUkjent.

Dermed får vi også tre tilhørende overganger når en hendelse først skjer. Jeg har forsøkt å gi dem beskrivende navn:

Gjenoppdaget - Hendelsen fører til at vi erkjenner at noe som har skjedd før virkelig kan skje igjen.

Svart svane - Hendelsen fører til at vi erkjenner at faktagrunnlaget eller risikovurderingen var feil – vi kunne/burde vurdert annerledes (etterpåklokskap).

Totalt uventet - Hendelsen fører til at vi erkjenner at vi hadde for dårlig fantasi, men også til muligheter for helt ny læring.

Jeg har valgt å kalle den fjerde overgangen fra UkjentUkjent til KjentUkjent for «god fantasi» fordi den illustrerer at man kan forsøke å forestille seg mulige scenarier ved å teoretisere om dem, selv om de ikke har blitt observert. Får man aksept for at hendelsen kan skje så er den dermed flyttet til ny kategori.

Ved å fokusere på overgangene kommer det også tydelig fram at klassifiseringen av så vel mulige som opplevde hendelser i stor grad kommer an på den eller de som gjør analysen. Hvor noe klassifiseres vil være avhengig av så vel erfaring som teoretisk og praktisk kunnskap. Det medfører at risikoanalyser med fordel kan utføres av personer med ulik bakgrunn og erfaring for å få flest mulig hendelser vurdert. Det er rimelig å tro at med god historisk kunnskap og med bred erfaringsbakgrunn og informasjon om hendelser andre steder, så vil flere hendelser bli klassifisert a priori som KjentKjent, i stedet for å «dukke opp» i UkjentKjent eller KjentUkjent dersom de skulle skje.

5.1.3 Om svarte svaner

Figur 8 med sine fire klassifiseringer av kunnskap om hendelser og tilhørende overganger er ganske granulær. Aven (2013) diskuterer begrepet svarte svaner og har en mer binær tilnærming – enten er noe svart svane eller så er det ikke det. Han diskuterer hvorvidt det i det hele tatt eksisterer fenomener som ikke er mulig å sannsynlighetsberegne, og konkluderer med at de finnes, og at de karakteriseres ved at de er ekstreme og overraskende *relativt til kunnskapen man har.* Dette er ikke helt overlappende med Taleb (2007) sin definisjon som har en mer universell «ikke noensinne sett tidligere» definisjon. Haugen og Vinnem (2015) tar opp denne ulikheten og drøfter hvorvidt svarte svaner bør klassifiseres som:

- UkjentUkjent.
- Vurdert som umulig.
- Vurdert som svært usannsynlig.

Haugen og Vinnem konkluderer med at er mest hensiktsmessig å reservere svart svane begrepet for de hendelsene som er *UkjentUkjent*, mens min tolkning heller mot *vurdert som umulig*. Jeg mener det er en forskjell på det vi kunne ha forutsett og det som virkelig er UkjentUkjent og videre at svart svane begrepet bør reserveres for det vi kunne ha forutsett.

5.1.4 Alvorlighetsgrad

Hvor alvorlig en hendelse er, kan vurderes ut fra ulike perspektiv. For eksempel kan man se på:

- Skade på liv og helse.
- Skade på eiendom, gjenstander.
- Manglende tjenesteyting.
- Skadet omdømme.

Videre kan man måle alvorlighetsgraden med ulike parametre.

- Personskade kan måles i antall timer fravær fra arbeidsplassen, liggetid på sykehus, antall døde.
- Skader på eiendom og gjenstander kan måles i kroner.
- Manglende tjenesteyting kan måles i timer, gradert i redusert eller ingen tjeneste.
- Omdømme måles gjerne i form av en indeks[19], der man ser selskap i relasjon til andre i samme bransje og generelt.

I forhold til et børsnotert selskap vektlegges gjerne det økonomiske perspektivet. Enhver aktivitet eller potensiell hendelse kan vurderes ut fra mulige inntekter og kostnader. Risikovurderinger kan da bli å balansere risikoen for direkte kostnader inkludert erstatninger mot kostnaden ved å mitigere risikoen. Det å operere i utkanten av etablert praksis kan være det som gir et selskap en konkurransefordel (Rasmussen, 1997).

Likevel er det også viktig å vurdere omdømmet. Et selskap som opererer i et modent marked kan forvente at kunder vil se på omdømme som en viktig faktor når man skal kjøpe tjenester. Dermed vil en hendelse som gir synkende omdømme kunne føre til lavere framtidig inntjening, selv om den konkrete hendelsen ikke medfører direkte kostnader.

Eksempelvis eksisterer det for selskapets bedriftskunder mulighet for å tegne SLA-avtaler[20] med høyere oppetidsgaranti enn standard. Dette forankres teknisk i bedre løsninger og bedre prioritet ved feilretting. Dersom garantert tilgjengelighet likevel ikke oppnås gir det grunnlag for refusjon tilbake til kunden. Den reelle trusselen i bedriftsmarkedet er likevel ikke å måtte yte kompensasjon, men at kunden over tid mister tilliten og velger å bytte leverandør.

Jeg fokuserer primært på økonomi når jeg vurderer hvor alvorlig en hendelse er.

5.1.5 Alvorlig og uventet for hvem

En og samme hendelse kan ha ulik alvorlighetsgrad for ulike parter. Et linjebrudd for en enkeltkunde framstår for selskapet som en dagligdags hendelse, men kan for den aktuelle kunden være svært alvorlig. Flere av informantene pekte nettopp på det at kundene er blitt stadig mer avhengig av operative nettverkstjenester hele døgnet. Selv om det er mulig å

[19] Se f.eks. http://www.epsi-norway.org/. EPSI kundetilfredshetsmålinger gjøres på en skala fra 0-100, og selskap med høy score regnes å ha et godt omdømme og god kundebinding. Det er store variasjoner mellom ulike bransjer.

[20] SLA: Service Level Agreement. Avtale som regulerer minimum forventet tilgjengelighet til tjenesten. Inkluderer som regel kompensasjonsmekanismer ved brudd og bedre tilgang til teknisk bistand ved behov.

bestille redundante linjer i forkant, er det få som velger å gjøre det før man har opplevd uheldige situasjoner.

Tilsvarende kan det også tenkes at det selskapet opplever som regulære feil – at en linje blir nede i mange dager på grunn av feilretting – for kundene oppleves som helt irregulært. Det er ikke nødvendigvis det at man ikke innser at feil kan skje og at bortfall av linjetjenester er mulig, men over tid har man gjerne bygget komplekse systemer som har avhengigheter man ikke skjønner før situasjonen oppstår.

En bedriftskunde sentraliserte for noen år siden lagerstyringen for sine regionale lager, og genererte optimaliserte plukklister for truckene. Uten slike plukklister er i praksis lageret helt lammet for utkjøring av varer. For å minimere risiko bestilte de redundante linjer i separate traseer, og anså risikoen for å miste begge som neglisjerbar.

Likevel opplevde de totalt utfall til et av lagrene, med tilhørende lammet produksjon der. Etter noe tid valgte de å skrive ut plukklister sentralt og fakse dem til lageret, så de fikk plukket og levert varene, om enn ganske forsinket. Det som var en helt regulær hendelse for nettverksleverandøren (linjebrudd) ble for kunden en trussel de hadde sett men valgt å ikke tro kunne skje – en KjentUkjent trussel som de klarte å håndtere. Etter hendelsen er det naturlig å tro at kunden endret synet på det å miste begge linjene til et lager, den ble «gjenoppdaget».

Interessant nok kan trusselen hvis den ikke skjer igjen med det første bevege seg bort igjen fra KjentKjent til UkjentKjent. De fleste selskap avvikler eller har avviklet alle faksløsninger. Noen velger å beholde en løsning på hovedkontoret, men tar besparelsen i alle andre avdelinger. Dersom denne kunden fjerner faksløsningen på avdelingskontoret uten å tenke på alternativer ved doble linjebrudd så vil de kunne «gjenoppdage» hendelsen en gang i framtiden.

Internt i selskapet kan også samtidige hendelser bli alvorlige. Påtrykket på kundeservice varierer i forhold til mange faktorer. Det er spørsmål om faktura, problemer med å koble seg trådløst til internett, kundeutstyr som går i stykker og mye annet. Noen av disse er til en viss grad forutsigbare, som at fakturautsendelser fører til fakturaspørsmål og at lyn og torden vil føre til en del ødelagt kundeutstyr. En viss variasjon i påtrykket håndteres vanligvis ved at det eksisterer fleksibilitet både i forhold til bemanning og oppgaver som kan omprioriteres. Det er mulig å tenke seg at flere av disse faktorene forekommer samtidig og at de sammenfaller med ytre faktorer slik at man til sammen opplever en «perfect storm». Som påpekt i (Grøtan, 2017) kan man da oppleve både forsterkende og forhindrende effekter, og eventuelt også ressurskonflikter samtidig. Selv om delelementene var KjentKjent ville situasjonen før den oppsto kanskje ikke vært vurdert som KjentKjent.

5.1.6 Hvordan kan informantenes hendelser klassifiseres?

Jeg har tabulert de ulike hendelsene som informantene har nevnt i Tabell 2.

1: Regulære trusler	2: Irregulære trusler	3: Helt nye trusler
KjentKjent • Brudd i samband • Brudd i strømtilførsel • Feil i maskinvare • Brann/ødeleggelse teknisk rom • Brann arbeidslokaler • DDoS mot kunder	**KjentUkjent** • Alvorlige samtidige feil • DDoS mot selskapet • Force Majeure / ytre miljø / natur • Utro tjener **UkjentKjent** • Utilgjengelige arbeidslokaler	**UkjentUkjent**

Tabell 2 - klassifisering hendelser

Som kolonne 1 viser er det mange alvorlige hendelser som regnes som «dagligdagse» i den forstand at man er forberedt på dem og har planverk, formelt eller uformelt. Noe forekommer så sjelden at det gjennomføres regelmessige øvelser (brann), mens mye skjer såpass ofte at teknikere forventes å håndtere det uten at man må øve på forhånd.

I kolonne 2 finner vi hendelser som informantene mener kan skje, men som selskapet så langt ikke har opplevd i alvorlig omfang. Interessant nok er det en hendelse jeg mener passer i kategorien UkjentKjent: *Utilgjengelige arbeidslokaler.* Informantene beskriver dette som en hendelse man tidligere var oppmerksom på og hadde beredskap i forhold til. Med tiden har oppmerksomheten blitt borte og det eksisterer ikke lenger aktive planer og rutiner for å reetablere seg i alternative lokaler.

Det virker å være et misforhold mellom det informantene tror omgivelsenes (kunder, myndigheter, aksjonærer) forventninger til selskapet er, kontra hva man faktisk har planer for og «kontroll på». I etterpåklokskapens lys vil sannsynligvis en eventuell hendelse i kolonne 2 framstå som noe man burde forutsett og gardert seg mot – altså en svart svane. En av informantene hadde følgende hjertesukk i forhold til hva man planla for kontra hva som kunne komme til å skje:

> *«De fleste av planene våre handler om å vinne den forrige krigen, vi burde heller forsøke å forestille oss hvordan den neste krigen vil bli.»*

I kolonne 2 (og sannsynligvis i kolonne 3) finner vi også hendelsene med størst potensiale for å skade selskapet. Alle hendelsene under KjentUkjent vurderes av informantene som store nok til potensielt å kunne true bedriftens eksistens. Dersom kundene opplever for lang periode uten tjenester forventes det at mange vil se seg om etter alternative leverandører. I et etablert marked med standardiserte tjenester er det enkelt for kundene å velge bort den som oppfattes som utilstrekkelig.

Informantene kom ikke opp med noen trusler / hendelser som hører hjemme i kolonne 3 – helt nye trusler. Det er i seg selv ikke så bemerkelsesverdig – det er nettopp noe av egenskapen til den type hendelser – vi ser dem ikke for oss før de virkelig har skjedd. I

retrospekt kan vi kanskje si at noen av hendelsene bransjen har opplevd hører hjemme i den kategorien, men informantene hadde ingen historiske eksempler på totalt uventede hendelser som de selv hadde opplevd.

5.1.7 Mulige framtidige hendelser i kategorien UkjentUkjent

For å spekulere i mulige framtidige hendelser i kategorien UkjentUkjent kan det være nyttig å se på hendelser som har – eller ryktes å ha - forekommet.

Avanserte angrep fra statlig aktør - Viruset *Stuxnet* [21]angriper industrielle styringssystemer, og gjorde stor skade på Irans atomvåpenprogram. Det ryktes at det er utviklet av USA og Israel i samarbeid, ene og alene for det formålet. Det finnes også andre eksempler der andre stater holdes ansvarlig. I framtiden kan det godt tenkes at det å utvikle skadelig programvare blir en mer vanlig måte å ramme motstandere på, og at det også kan bli brukt mot selskaper eller for å ramme en spesiell sektor i et land.

Mulighet for å «bricke» utstyr - I USA har det vært stor frykt for at spesielt Kina legger inn mulighet for å kunne sende kommandoer som ødelegger nettverksutstyr på en slik måte at det ikke kan repareres – det må byttes ut. Av denne grunn er det ikke tillatt med kinesiskprodusert utstyr i offentlige nett i USA[22]. Dersom slike kapabiliteter virkelig eksisterer kan man tenke seg at de blir brukt, enten av aktøren som har laget det, men også av andre som har klart å få tilgang til å utløse det.

Kunstig intelligens på avveie - Tidligere har det stort sett vært et tema i underholdningsfilmer og -litteratur, men det er en økende bekymring for at kunstig intelligens – AI – kan utvikle seg i en retning der vi ikke lenger klarer å kontrollere det.[23] I nettverksbransjen er alle enheter per definisjon knyttet sammen. Dette i sammenheng med høye krav til lønnsomhet og automatisering kan det bety at man er spesielt utsatt.

Felles for disse scenariene er at de er beskrevet og diskutert. De kan altså ikke klassifiseres som UkjentUkjent, men heller i kategorien KjentUkjent. Men for relativt kort tid siden var de UkjentUkjent, og jeg tror det er sannsynlig at vi i framtiden vil oppleve eller få beskrevet hendelser som slekter på disse og som vi i dag ikke klarer å forestille oss.

5.1.8 Hendelse i forhold til konsekvens

Jeg har i kapitlet ovenfor fokusert på selve trusselen / hendelsen og funnet at de lar seg klassifisere. Det å klassifisere og forstå hendelsen gir et godt utgangspunkt for å forstå de mulige resultatene / konsekvensene av hendelsene. Men er det også mulig at det finnes kjente hendelser som gir ukjente resultater?

Selskapet har flere ganger opplevd at manuelle endringsoperasjoner har gitt uventede, alvorlige konsekvenser. Det som av operatøren har blitt oppfattet som rutinemessige

[21] Se f.eks. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[22] Se f.eks. https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf
[23] Se f.eks. http://www.telegraph.co.uk/technology/2017/07/17/ai-biggest-risk-face-civilisation-elon-musk-says/

oppgaver (fjerning av ubrukt konfigurasjon, forbedring av tjenesten) har ødelagt tjenesten.[24] Dette ligner på det Perrow (1999) beskriver: et system som er så komplekst at man ikke har full oversikt og ser konsekvensene av handlinger og feil, og man kan få en forventning om «Normal Accidents».

5.1.9 Forskningsspørsmål 1 oppsummert

Hva kjennetegner hendelser som er uventede og som kan ha en alvorlig eller katastrofal konsekvens for selskapet?

Jeg mener empirien som diskutert ovenfor viser at det eksisterer uventede hendelser som kan få alvorlig konsekvens for selskapet. Noen av disse har virksomheten en forventning til at vil skje, enten basert på tidligere erfaringer eller på risikoanalyser. Andre er ukjente i den forstand at selskapet ikke har en felles forventning om at de vil kunne oppstå før de virkelig forekommer

De mest alvorlige er etter min vurdering de ukjente fordi det er vanskelig å forutse hvordan selskapet vil respondere på disse. Informantene er trygge på at kjente hendelser blir håndtert på en adekvat måte, og den nære historien viser også at selskapet har kontroll i slike situasjoner.

Informantene peker spesielt på de ukjente hendelsene i forhold til mulig skadelig konsekvens. Både i forhold til det man kunne/burde planlagt for og i forhold til de totalt uventede hendelsene, så oppfattes kombinasjonen av stort skadepotensiale og usikkerhet i forhold til håndtering som truende og alvorlig.

Jeg tror det kan ha verdi å bruke oppdelingen i KjentUkjent, UkjentKjent og UkjentUkjent for å klassifisere de ukjente truslene. En slik tilnærming skaper en «bredere» bevissthet rundt fenomenet ukjente hendelser og strukturer problemet. Dette er også nyttig i håndteringen av de truslene som er tema i neste kapittel.

5.2 Forskningsspørsmål 2

Hvordan kan selskapet forhindre at uventede hendelser oppstår og hvordan kan slike håndteres om de skulle oppstå?

I forrige delkapittel så jeg på hvorvidt det kan forekomme uventede hendelser som kan ha alvorlig/katastrofal konsekvens for selskapet, og hva som kjennetegnet disse. Jeg konkluderte med at slike eksisterer og at skadepotensialet sannsynligvis er størst når vi beveger oss over i det ukjente, klassifisert som irregulære/helt nye trusler Westrum (2006) eller i en av de tre kvadrantene som ikke er KjentKjent i Figur 3 / Rumsfeld (2002).

[24] Både «black holes»: Det at kundenes trafikk forkastes og «routing loops»: Det at kundenes trafikk går i ring før den til slutt forkastes, er noe som har forekommet. De fleste nettverksteknikere har opplevd dette når man setter opp nye nettverk, før all konfigurasjon er på plass. Det er selvsagt mer alvorlig dersom slike feil introduseres i et produksjonsnettverk.

I drøftingen vil jeg ta utgangspunkt i de kjente hendelsene og så bevege meg over til de ukjente.

5.2.1 Mitigere kjente feil

Bow tie modellen (Haddon Jr, 1970) setter den uønskede hendelsen i fokus og deler tiltak i to kategorier: De som gjøres for å hindre den uønskede hendelsen i å oppstå og de som begrenser skadeeffekten dersom den likevel oppstår.

Dette er et tankesett som mange av informantene kjenner seg igjen i. For nettverkstjenestene har det historisk vært driftsavbrudd som har vært kostbare og ubehagelige og som man har ønsket å unngå for framtiden. Dette har blitt gjort ved:

- Preventive tiltak:
    - Tydelige designregler.
    - Enkle design (enkelt å forstå, enkelt å feilsøke).
    - Redundans så mye som økonomisk og praktisk mulig.
    - Kompetansekrav.
- Responsive tiltak:
    - Overvåkning, rask alarm.
    - Vaktplaner, god opplæring.
    - Reservedelslager, avtaler med underleverandører.

Jeg synes informantene har en god tilnærming til det å mitigere kjente feil. Man erkjenner at det er nesten umulig å hindre at det oppstår brudd i den fysiske infrastrukturen. Men det er ikke av interesse for kundene – de er opptatt av hvorvidt tjenesten virker. Ved å sette «brudd i kundens tjeneste» som den uheldige hendelsen heller enn «brudd i fysisk infrastruktur» så settes fokus på det man skal unngå. Da blir redundans den (proaktive bow tie) barrieren som hindrer at en uønsket hendelse utvikles.

En konsekvens av dette er at det sjelden oppstår uønskede, alvorlige hendelser på «kundenivå». Det er selvfølgelig bra, men kan ha noen uheldige bivirkninger. Dette trekkes også fram av informantene, og de to viktigste som nevnes er:

- Organisasjonen blir mindre vant til å håndtere uønskede hendelser.
- Ledelsen blir mindre opptatt av uønskede hendelser.

5.2.2 Kan man forberede seg på ukjente situasjoner?

Når vi beveger oss bort fra kjente feil og over i ukjente feil er det på sin plass å diskutere hvorvidt man prinsipielt kan forberede seg på ukjente situasjoner. Som nevnt har verden åpenbart stor variasjon og alle vil fra tid til annen komme opp i *for dem* ukjente situasjoner. Fordi situasjoner sjelden er helt nye går mye opplæring ut på nettopp å dele erfaringer fra tidligere situasjoner og forklare hva som er riktig respons. Det gjelder enten det er generell oppdragelse av barn eller mer skole-/yrkesrettet. Målet er å kunne gjenkjenne en situasjon og vite hvilke muligheter man har, og fortrinnsvis velge «den riktige».

I organisatorisk perspektiv finner vi dette i Mintzberg (1979) sin maskinbyråkratimodell. To sentrale kjennetegn (av 7) er ifølge Jacobsen & Thorsvik (1997):

> *2) Ustrakt bruk av regler som angir hva som skal gjøres i ulike tilfeller.*
>
> *4) Et hierarki der det er klart definert hvem som er henholdsvis overordnet og underordnet innen de ulike kompetanseområdene.*

I et maskinbyråkrati er det altså en klar forventning om at man a priori kan forutse de situasjoner som kan oppstå, og definere riktig måte å håndtere dem på. Organisasjonen vet altså «beste måte» å håndtere alle situasjoner på, og institusjonaliserer dette ved å hjelp av regler og hierarki. Organisasjonen *standardiserer adferd* (Jacobsen & Thorsvik, 1997).

Slike organisasjoner oppfattes ofte som «trege å tilpasse seg» og dermed lite egnet til å håndtere ukjente situasjoner. På den annen side er det gjerne nettopp det som er hensikten med å organisere seg slik – det skal være regelstyrt og ikke avhengig av saksbehandler eller hvem saken gjelder. Offentlig forvaltning tilstreber forutsigbar saksbehandling, og anser byråkratiet som en hensiktsmessig organisering.

En mulig måte å forberede seg på ukjente situasjoner er å forsøke å gjøre dem kjente. Det vil si å finne alle de mulige «svarte svanene» og forberede en mulig respons. I praksis er dette vanskelig, av flere grunner. Det eksisterer svært mange teoretisk mulige hendelser som hver har svært lav sannsynlighet[25], og det vil kreve uforholdsmessig mye ressurser å forberede seg på alle tenkelige hendelser. Man vil også ha usikkerheten om man virkelig har funnet alle mulige hendelser og om planlagt respons virkelig er adekvat.

Der samfunnet har behov for å håndtere ukjente situasjoner foretrekkes sjelden den byråkratiske modellen. Nødetatene, som i det daglige utgjøres av brann, politi og helse[26], opplever stor variasjon i arbeidsdagene. De må tilpasse seg det som til enhver tid skjer, selv om de selvsagt har utviklet planverk for mange situasjoner.

Politiet sine innsatsstyrker for de skarpeste aksjonene er sjelden i aktivitet, men de har et stort ansvar i det at samfunnet forventer at de alltid skal kunne klare å løse sine oppgaver på så god måte som mulig. De er på mange måter «siste skanse» for befolkningens trygghet i fredstid. De siste årene har det stadig kommet nye og ukjente situasjoner[27] som har gjort at politiet har måttet tilpasse seg. Bechky & Okhuysen (2011) beskriver hvordan et SWAT-team[28] i en storby i USA forbereder seg på ukjente situasjoner ved å:

- Ha et lite, dedikert team der deltakerne har lang fartstid.
- Bruke mye tid på trening.
- Kjenne hverandres roller godt:

[25] Som nevnt tidligere lar slik sannsynlighet seg vanskelig beregne matematisk, den vil bare bli oppfattet som svært lav.
[26] Forsvaret er også en organisasjon som må være forberedt på å håndtere ukjente hendelser, men de må (heldigvis) relativt sjelden gjøre det i praksis.
[27] Selvmordsbombere, skoleskytinger, kjøretøy inn i folkemengder for å nevne noen.
[28] SWAT: Special Weapons And Tactics. Innsatsstyrke i politiet har ekstra trening, utstyr og kompetanse for å håndtere skarpe situasjoner.

    - For å erstatte hverandre ved behov.
    - For å kunne forutse hverandres reaksjoner/handlemåter.
- Aktivt dele/hente erfaringer fra andre tilsvarende team.

Det å bygge dedikerte team med høy grad av trening er også noe vi kjenner fra Forsvarets spesialstyrker og andre organisasjoner som «ikke kan mislykkes», altså der det kan rettferdiggjøres å bruke mye ressurser på forberedelser kontra innsats. De har regler og forventet handlingsmøte, men er forberedt på å bryte dem og tilpasse seg når situasjonen krever det.

For mange organisasjoner er det ikke praktisk eller realistisk å ha dedikerte spesialister som skal håndtere de vanskeligste situasjonene – hele organisasjonen må kunne tilpasse seg vanskelige – eller ukjente situasjoner. Det er det som både HRO og RE forsøker å underbygge.

I forhold til UkjentUkjent situasjonene blir det nesten en filosofisk diskusjon hvorvidt det er mulig å forberede seg på det personlige plan. En vanlig antakelse er at om man har tenkt gjennom mange scenarier og mulige løsninger så er man bedre i stand til å opptre fornuftig, men det er vanskelig å etterprøve hvorvidt det virkelig stemmer. Haugen og Vinnem (2015) skriver at det å forhindre UkjentUkjent hendelser ikke er mulig («(...) preventing this from happening is not really an option since we do not know what can happen…»), og fokuserer på å hindre skadevirkningene («(…) limiting the consequences of failures»). Det virker defensivt i forhold til det å detektere og stanse et forløp, noe som er sentralt i HRO og RE som diskuteres nedenfor.

5.2.3 Mitigere ukjente situasjoner

Som vist ovenfor så er det et antall irregulære trusler som kan oppstå. Det kan være alvorlige enkelthendelser, men også uheldige kombinasjoner av samtidige hendelser (Grøtan, 2017).

Bow tie modellen er i sin natur ikke så egnet til å håndtere ukjente hendelser, med mindre de «oppfører seg» som kjente feil. Eksempelvis forekommer det en sjelden gang sabotasje mot linjer. Det er gjerne «guttestreker», der en datalinje inn til et boligområde kuttes opp, brennes over eller skades på annen måte. Selv om det er sjelden og ikke noe som er særskilt planlagt for, så omtales det ikke på noen måte som en irregulær trussel. Det er bare enda en hendelse som medfører midlertidig tap av en linje, og som må håndteres på vanlig måte.

Som nevnt i kapittel 4.5 framkommer det mange tiltak som etter informantenes mening vil gjøre selskapet bedre i stand til å håndtere uventede hendelser:

- Forberedt ledelse.
- Gode informasjonsrutiner internt og eksternt.
- Godt samarbeid og tydelige rolleavklaringer.
- Avklarte praktiske forhold.
- Bevisstgjøring.

Felles for disse tiltakene er at de er uavhengige av den konkrete situasjonen som kan oppstå. I stedet forbereder de organisasjonen på å en ekstraordinær innsats utover det

daglige. Når informantene peker på dette som relevante tiltak ligger det også en forutsetning på at man ikke oppfatter seg som «god nok» i dag. Det kommer klart til uttrykk at det er store forbedringer å hente på alle disse feltene.

Det oppfattes som relativt enkelt å bli bedre innenfor alle disse tiltakene. For det meste handler det om å bruke tid på å avklare rutiner, roller og forventede handlingsmønstre internt, og deretter øve på dem. Det framkom enkelteksempler på at det tidligere hadde vært gjennomført øvelser og flere av informantene konkluderte med at de burde øve mer for å være bedre forberedt. Det omfattet både «problemløsningsøvelser» på teknisk nivå, men mest «samhandlingsøvelser» der ulike avdelinger burde øve på å samarbeide og takle uvante situasjoner.

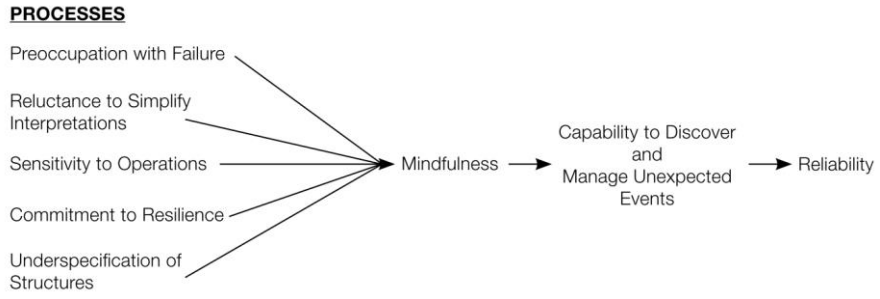
Det uttrykkes ønske om å øve mer, både på kjente og ukjente situasjoner.

5.2.4 Forhindre uventede situasjoner / HRO perspektivet

Et fellestrekk ved tiltakene i forrige kapittel er at de ikke forsøker å forhindre at situasjonen skal oppstå – de er rettet mot å håndtere den best mulig *når den har inntruffet*. Det å håndtere at ukjente situasjoner har oppstått kan sammenlignes med det å operere komplekse systemer feilfritt. Det er vanskelig å forutse alt som kan gå galt og detaljplanlegge for det, men man kan likevel fokusere på så trygge operasjoner som mulig. Dette er idealet til High Reliability Organizations (HROer).

Kan det være en «falsk utrygghet» når informantene i kapittelet ovenfor mener at det er nødvendig med flere tiltak og mer øving – oppfører organisasjonen seg allerede som en HRO? Og er i så fall ønskene om mer øving bare et uttrykk for «mindfullness» som HROene iflg Weick et al. (2008) er så bevisst på?

Figur 9 lister opp prosessene som skal føre til økt «mindfullness», og jeg vil vurdere hver av disse i forhold til selskapet.



Figur 9 - HRO principles (Weick et al, 2008)

Preoccupation with failure – Fokus på mindre feil er viktig for å hindre at de får utvikle seg. Både fordi mindre feil kan utvikle seg til å bli større, men også fordi de kan interagere med andre feil og omgivelser og gi uforutsette konsekvenser. Her finner jeg at selskapet har lite fokus på mindre feil – tvert imot uttrykkes det at man tidligere hadde mer kapasitet til å drive aktiv feilsøking og preventiv feilretting.

Reluctance to simplify interpretations – Det å unngå å forenkle fordi man da kan miste viktig informasjon om hendelser som er under utvikling. Kan unngås ved å la medarbeidere samhandle aktivt for å dele informasjon og drøfte situasjoner som har oppstått. Jeg finner lite av denne «tilstedeværelsen» i situasjonen – det er heller det motsatte; at så snart en situasjon passer inn i et mønster man mener å kjenne igjen, så blir det forklaringsmodellen, og tilhørende løsning/handlingsmønster er dermed gitt.

Sensitivity to operations – Ved å være aktivt involvert i det operative arbeidet, villig til å stille spørsmål og korrigere underveis vil en HRO ha en bevisst holdning til kontinuerlig opprettholde kvaliteten. Dette fordrer aktiv deltakelse fra medarbeidere og ledere, noe som nok er lettere å observere på et hangarskipsdekk enn i et driftssenter. Det er lite som underbygger at dette er en tydelig egenskap i selskapet. Saker og situasjoner håndteres så langt mulig av enkeltpersoner, med til dels betydelig arbeidspress. Dersom «sensivity to operations» var tilstede ville jeg for eksempel forventet en mer gruppebasert tilnærming til oppgaver og jevnlige statusoppdateringer i løpet av arbeidsdagen. Involvering fra toppledelsen er det lite spor av – rapportering skjer langs to hovedakser: statistikk og informasjon om alvorlige enkelthendelser.

Commitment to resilience – Erkjennelse av at feil og uheldige situasjoner vil kunne oppstå, fører til- at HROer er opptatt av å ha motstandsdyktighet under press. Det kan være organisatorisk så vel som utstyrsmessig. Teknisk finner jeg mye de samme holdningene i selskapet – det er viktig å sikre robusthet i installasjoner, slik at feil ikke får negativ konsekvens for kunder og omgivelser. Organisatorisk er det til dels slik – kunnskap spres planmessig mellom personer og avdelinger, og man har også organisert seg med egen avdeling for langsiktighet som ikke påvirkes av daglig driftsutfordringer. Likevel er det en stor mangel i forhold til tilgjengelig kapasitet – i det daglige er det få personer som står for driften og som nevnt er det krevende å mobilisere når noe skjer utenfor normalarbeidstid.

Underspecification of structures – I alvorlige situasjoner vil en HRO la den med best kvalifikasjoner ta de kritiske avgjørelsene heller enn den som har formell myndighet. Dette korrelerer bra med hvordan teknikerne i selskapet tenker – det er en forventning i alvorlige situasjoner om at alle med kvalifikasjoner skal bidra til å feilsøke og foreslå løsninger. Selv om formelle beslutninger vil bli «kvittert ut» av lederen så er det som et resultat av en åpen prosess der stillingstittel er av liten betydning. Det er likevel en del tvil om det også vil gjelde toppledelsen, dersom den blir involvert i virkelig alvorlige situasjoner.

I sum finner jeg lite overlapp mellom de egenskapene Weick et al. (2008) tillegger en HRO og det informantene forteller at de virkelig gjør i det daglige. De grunnleggende kjennetegnene er ikke tilstede i tilstrekkelig grad og selskapet kan ikke sies å være en HRO.

5.2.5 Resilience engineering perspektivet, normativt ståsted

Resilience engineering (RE) perspektivet har i mine øyne stor overlapp med HRO perspektivet. De er begge opptatt av å være proaktive og ser mennesker som en ressurs som kan og bør aktivt bidra til å kontrollere prosesser. Litteraturen rundt HRO er mer observerende, mens RE framstår mer normativ. Hopkins (2014) mener sågar at de ikke kan skilles fra hverandre: *«A resilient organization (…), seems indistinguishable from a high*

reliability organization (…)». I teoridelen listet jeg opp egenskaper for de to perspektivene. Disse har jeg forsøkt å vurdere mot hverandre i Figur 10 og finner at de er svært sammenfallende.

High Reliability Organizations \ Resilience Engineering	Engasjement og forpliktelse fra toppledelsen	Rettferdig kultur	Læringskultur	Oppmerksomhet	Beredskap	Fleksibilitet	Grensebevissthet
Preoccupation with failure	x	x	x		x		x
Reluctance to simplify interpretations		x	x	x	x		
Sensivity to operations	x	x	x	x	x	x	x
Commitment to resilience	x	x	x		x	x	x
Underspecification of structures	x			x		x	

Figur 10 - HRO vs. RE

Eksempelvis søker man i HRO perspektivet *underspecification of structures,* mens man i RE tilstreber *fleksibilitet.* Begge er etter mitt syn uttrykk for det samme: Organisasjonen skal på lavest mulig nivå tilpasse seg uventede eller uheldige hendelser. Man skal være tilpasningsdyktig til situasjonen uten at det oppfattes som å bryte med formell ledelse og autoritet.

Med utgangspunkt i at det er stor overlapp mellom HRO og RE, og min vurdering ovenfor om at organisasjonen i dag ikke framstår som en HRO, ønsker jeg å bruke de sju RE temaene normativt. Jeg vil beskrive hvordan jeg mener selskapet kunne konkretisert og operasjonalisert hvert tema, basert på hva informantene mente var mulige forbedringspunkter.

Engasjement og forpliktelse fra toppledelsen - I et selskap med flere hundre ansatte vil den enkelte ansatte sjelden se eller bli sett av toppledelsen – ledelse utøves gjennom mellomledere. Dersom toppledelsen ønsker å fokusere på de ansatte som en viktig ressurs så kan dette gjøres ved:

- Regelmessige allmøter med relevant informasjon.
- «Storytelling», der ansatte løftes fram.
- Synlig ledelse, som aktivt bruker tid på å møte ansatte også utenfor formelle møter.
- God personalpolitikk, som viser at selskapet verdsetter sine ansatte og tar vare på dem. Lønn er et element, men vel så viktig for mange er følelsen av at selskapet i alle situasjoner opptrer ryddig, rettferdig og realt.

Rettferdig kultur - Et selskap med oppriktig interesse i forbedringskultur vil vise det gjennom å:

- Lete etter forbedringer, ikke syndebukker, når hendelser gjennomgås.

- Ha ordninger for å rapportere «nestenulykker» tilsvarende det man ser i andre industrier. Slike ordninger fungerer best dersom de er ikke-anonyme fordi man da får mest mulig informasjon rett fra kilden. Dersom slike ordninger skal være ikke-anonyme forutsetter det stor tillit fra den som rapporterer til hvordan mottaker håndterer informasjonen.

Læringskultur – En lærende kultur i et selskap vil komme til uttrykk i hvordan man behandler faktiske hendelser, som nevnt ovenfor. Men det vil også kunne sees gjennom at:

- Selskapet anser seg ikke tilbake i normaltilstand før uønskede hendelser er evaluert med tanke på hva om kunne vært gjort annerledes.
- Opplæringsmateriell og instrukser revideres jevnlig, etter en plan.

Oppmerksomhet – Selskapet ved ledelsen har også ikke-økonomiske måleparametre, som bare indirekte relaterer seg til økte kostander eller tapt fortjeneste. Tiltak iverksettes dersom slike parameterne utvikler seg uheldig:

- Sykefravær.
- Medarbeidertilfredshet.
- Kompetansenivå.
- Nesten-hendelser.

Beredskap – Selskapet søker å ha beredskap både for kjente og ukjente situasjoner som kan oppstå, ved å:

- Avholde øvelser, med tilhørende evalueringer og diskusjoner.
- Utveksle faglig informasjon med andre selskap i samme eller sammenlignbare bransjer.
- Videreutdanne ansatte, både i forhold til den enkeltes ønsker og planmessig i forhold til selskapets behov.
- Delta på bransjesamlinger.

Fleksibilitet – Et selskap med god fleksibilitet oppfordrer aktivt de ansatte til å ta ansvar og løse akutte problemer raskt, innenfor det som er lovlig og ansvarlig. Dette kan oppnås ved at:

- De ansatte får tillit og støtte, også når situasjoner ikke utviklet seg som ønsket.
- Det er kultur for at «det er lov å gjøre ting feil én gang» - men også for at man skal lære og unngå å gjenta feil.
- Ledere aksepterer at de ikke trenger å ha alle svar selv, men skal bruke ansatte til å løse situasjoner.

Grensebevissthet – Selskapet tar fram risikoindikatorer og monitorerer disse aktivt, både enkeltvis og i forhold til hverandre. Eksempelvis vil man:

- Koble pågående drift og planlagt arbeid, inkludert ha vilje til å utsette planlagt arbeid når det er feilsituasjoner som gjør risikoen høyere enn forventet.
- Være oppmerksom på omgivelsene. Dersom uvanlige situasjoner oppstår (stormvarsel, massivt nedbør) så vurderes risiko og eventuelle tiltak fortløpende.

- Vurdere personalsituasjonen kontinuerlig. Ferie, fravær og arbeidspress blir passet på for å sikre at det alltid er kapasitet igjen til å håndtere plutselige eller uventede situasjoner.

Når jeg ser på hvordan jeg ville operasjonalisert RE perspektivet i forhold til virksomheten finner jeg at det er stor overlapp med det informantene ser som mulige måter å forberede seg på uventede hendelser. Mange av tiltakene bygger organisasjonen og utvikler kompetanse og selvtillit hos medarbeiderne – nettopp det som er grunntanken til RE: mennesket er en ressurs som kan og bør brukes for å hindre at uheldige situasjoner får utvikle seg. Få av punktene oppleves som fremmede for informantene – de er tilstede i selskapet i dag, men blir lett nedprioritert i travle dager med for få ressurser.

5.2.6 Uventet vs. kompleks

Både i HRO og RE blir det argumentert for at det er kompleksiteten i oppgaven (hangarskipsoperasjoner, flykontroll) eller «maskinen» (atomkraftverk) som gjør at klassisk sikkerhetstenking er utilstrekkelig:

> *«According to this paradigm, 'error' was something that could be categorized and counted» (E. W. Hollnagel, David D.; Leveson, Nancy (2012))*

Det blir vanskelig å forutse mulige hendelser på grunn av at årsakssammenhengene og utviklingen i hendelsene ikke lenger er enkle å forstå. Dette gjør at man ikke klarer å kartlegge og kontrollere alle utfall.

Ovenfor argumenterer jeg for at både HRO og RE i stor grad kan anvendes for å forberede en organisasjon på uventede hendelser. Men jeg sier derimot *ikke* at alle uventede hendelser skyldes økt kompleksitet i oppgave eller teknologi. En potensiell uventet hendelse som er beskrevet er en utro tjener som bevisst velger å sabotere nettverket og tjenestene. Dette mener jeg i ettertid vil bli beskrevet som *uventet*, men neppe som særlig *komplekst*.

5.2.7 HRO / RE vs. kjente feil / hendelser

I sin natur er både HRO og RE velegnet til å håndtere kjente hendelser. De forsøker å utvikle de egenskapene som gjør organisasjonen oppmerksom på hva som er normal operasjon og vil gjenopprette normaloperasjon så tidlig som mulig i et potensielt ulykkesforløp.

Også Safety-II perspektivet vektlegger at det i mange situasjoner utfyller – ikke erstatter – Safety-I (E. Hollnagel, 2014). Samtidig er det grunnleggende forskjellig å se på sikkerhet som fravær av feil kontra fokus på hva som går bra. En HRO kan se mange rapporterte hendelser som positivt fordi det gir mulighet til å justere organisasjon og oppførsel. En klassisk organisasjon ser gjerne mange rapporterte hendelser som et uttrykk for dårlig sikkerhet.

Tradisjonelle organisasjoner har ifølge (Weick et al., 2008) en tendens til å fokusere på *enten* forebygging *eller* mitigering, mens effektive HROer er god på begge deler. Dette samsvarer med flere av observasjonene på teknisk side, man har over tid utviklet god evne til å unngå uønskede hendelser, men frykter at evnen til å håndtere alvorlige og uventede hendelser har blitt dårligere.

5.2.8 Forskningsspørsmål 2 oppsummert

Hvordan kan selskapet forhindre at uventede hendelser oppstår og hvordan kan slike håndteres om de skulle oppstå?

Med utgangspunkt i at uventede hendelser kan oppstå, har jeg vurdert mulige måter virksomheten kan forberede seg på. For de kjente hendelsene framstår selskapet som godt forberedt og kompetent. Dette vises som høy selvtillit blant informantene i forhold til «vanlige» feilsituasjoner. Det eksisterer formelle planer og rutiner, og sammen med en felles forståelse for hvordan vanlige feil skal håndteres, så gjenopprettes normalsituasjonen greit. De utfordringene som nevnes er stort sett knyttet til for lite ressurser eller samarbeid mellom avdelinger. Selskapet har, spesielt på teknisk side, lagt stor vekt på det preventive – det er ønskelig å unngå alvorlige situasjoner, heller enn å være dyktig i krisehåndtering.

For de uventede og ukjente hendelsene utrykker informantene større usikkerhet i hvordan de tror selskapet vil opptre. Samtidig anses skadepotensialet som større.

Fordi det er vanskelig å utelukke muligheten for uventede og ukjente hendelser, har jeg fokusert på hva som kan gjøres dersom de oppstår. Jeg har sett på HRO og RE som perspektiver, og mener at de er svært beslektet og godt egnet til også å håndtere det uventede. Begge postulerer at robuste organisasjoner med høy kompetanse, god selvtillit og høy «tilstedeværelse» (mindfulness) er godt rustet til å håndtere komplekse operasjoner med lav risiko for hendelser med alvorlige konsekvenser. Begge perspektivene framhever at det er viktig å fokusere på det som går bra og bygge videre på det, heller enn å forsøke å forutse og deretter forhindre alle mulig måter noe kan gå galt på.

Etter min mening oppfører selskapet seg ikke som en HRO i dag. Informantene peker på ulike tiltak som ville passet inn i en «HRO-organisering» av selskapet, men de er i liten grad tilstede og operative. Når jeg gjør en vurdering av hvordan selskapet kunne benyttet prinsippene fra RE så finner jeg det samme; fragmenter er tilstede, men det blir ikke riktig å hevde at de er førende for hvordan selskapet er organisert og drevet.

Jeg mener at HRO og RE som idealer vil kunne gjøre virksomheten bedre i stand til å håndtere ukjente hendelser og jeg benyttet RE som utgangspunkt for å konkretiser noen mulige forbedringer.

5.3 HVORFOR ER IKKE ALLE ORGANISASJONER HROER?

I mine to forskningsspørsmål så jeg på hva som kjennetegner uventede hendelser og om det var mulig å forberede seg på slike. Jeg fant at hendelsene kunne inntreffe, og at spesielt de tidligere ukjente kunne vært katastrofale for virksomheten. Det er også pekt på mulige tiltak for å bedre organisasjonens reaksjon på slike ukjente hendelser.

Gitt at uventede hendelser som diskutert her også er uønskede hendelser – hvorfor søker ikke selskapet å tilnærme seg tankesettet i HRO og RE i større grad? Selv om det ligger litt på siden av problemstillingen er det naturlig å knytte noen tanker til det.

Alle bedrifter er i praksis i en konkurransesituasjon og må balansere mange ulike hensyn for å kunne fortsette sin virksomhet. Man må drive innenfor eksisterende lover og regler, man må ha medarbeidere som yter nok, man må ha varer eller tjenester som har riktig pris og kvalitet, og man må framstå som attraktiv å gjøre forretning med. For et børsnotert selskap blir dette særlig tydelig; som regel er det kvartalsvise framlegginger av resultat, hvorpå selskapet blir sammenlignet med andre i samme bransje. Man blir også vurdert i forhold til andre steder aksjonærene kan velge å satse sine midler, og blir man ikke vurdert som attraktiv nok, så får man umiddelbar og konkret tilbakemelding fra aksjemarkedet i form av kursendringer og aktivitet i aksjen.

Dette medfører at mange avgjørelser blir en avveining mellom økt lønnsomhet kontra økt risiko, beskrevet av Reason (1997) som en båtreise mellom to farlige ytterpunkt: Katastrofe og konkurs. For mye vekt på verdiskapning vil kunne føre til for dårlig beskyttelse mot katastrofer, mens for mye vekt på beskyttelse mot katastrofer vil gi for dårlig verdiskapning og lede til konkurs. «The unrocked boat» billedliggjør faren med ikke å oppleve små hendelser som gjør at kursen korrigeres tilbake «inn i den trygge leden» før det er for sent. "The unrocked boat" passer etter min mening bedre i klassisk sikkerhetstenkning, enn i situasjoner med ukjente hendelser – de kjennetegnes jo av at de er vanskelig eller umulig å forutse. Likevel blir utfordringen for et selskap den samme – man må navigere mellom høy lønnsomhet og høy risiko. Dette vanskeliggjøres ved at man får svar på lønnsomheten med jevne mellomrom, mens risikoen er en teoretisk faktor som innimellom viser seg ved uønskede hendelser som kan måles kostnadsmessig.

Både HRO og RE forutsetter en viss *organisatorisk redundans* (Rosness, Håkonsen, Steiro, & Tinmannsvik, 2000), altså at det er overlapp i blant annet kompetanse, arbeidsoppgaver og ansvar. Fra et kortsiktig økonomisk perspektiv kan dette synes negativt – det brukes mer ressurser enn nødvendig for å løse en oppgave.

Rasmussen (1997) anser at selskapers handlingsrom ligger i rommet mellom tre avgrensninger: Økonomi, arbeidsbelastning og sikker produksjon. Alle disse tre kan til en viss grad påvirkes av selskapet selv, men påvirkes også av omgivelsene. En mulig konsekvens av økt press på økonomi blir derved at man nærmer seg grensene for arbeidsbelastning og sikker produksjon: Fokus på lønnsomhet tar for mye tid og oppmerksomhet.

På noen områder har selskaper i Norge kunnet spekulere i om kostnaden ved lovovertredelse ikke er høy nok til rettferdiggjøre etterlevelse. Dette i motsetning til USA der domstolene ofte tilkjenner det vi oppfatter som ekstremt høye bøter og erstatninger for å «statuere eksempler». Det ser vi nå at brer om seg i EU – og dermed i praksis også i Norge. Et aktuelt eksempel er EUs personvernforordning (GDPR[29]) som forventes implementert i norsk rett i mai 2018. Ved brudd på dagens personopplysningslov kan Datatilsynet gi bøter på inntil ca. 925 000 NOK. Når GDPR er innført heves bøtegrensene til 20 000 000 EURO / 4% av selskapets globale omsetning. Intensjonen til EU med GDPR er at selskaper skal beskytte personvern via veldefinerte systemer og rutiner («privacy by design») og man vil tvinge selskapene til etterlevelse.

[29] The EU General Data Protection Regulation, se http://www.eugdpr.org/

Ved slik å gi dramatisk økt konsekvens av uønskede hendelser, tvinges selskapene til å håndtere personvernproblemetikken. Risikoen blir for stor ved å la være, og man kan ikke lenger ignorere uventede hendelser som man antar har lav sannsynlighet.

Et annet viktig element i det moderne forretningslivet at det stadig skjer endringer på selskapsnivå. Outsourcing, privatisering og andre selskapsendringer virker i motsatt retning av idealene for en HRO. I stedet for en robust organisasjon med mulighet for samvirke på tvers av ulike fagområder, ser vi stadig oftere at deler av verdikjedene håndteres i andre selskaper. Eksempelvis kan man se stor kontrast mellom det tidligere «Televerket»[30] og de moderne aktørene. Televerket hadde et enormt spenn i virksomheten sin, med eiendomsforvaltning, anleggsvirksomhet, montører og teknisk installasjon og drift av et utall systemer. Dagens selskaper er mye mer spesialiserte, og mange ulike underleverandører er involvert i verdikjedene. Dette gjør det vanskelig å håndtere uventede situasjoner, det er få som har god oversikt, og det er tungt å omstille til krisehåndtering.

Oppsummert er det naturlig å se på hvor HROer først ble beskrevet: Hangarskip, kjernekraftverk og senter for flykontroll. De kjennetegnes både av at det er svært kostbart om de feiler, men også av at de i praksis har liten konkurranse. Økonomistyring er ikke uvesentlig, men de risikerer i liten grad å bli utkonkurrert av en billigere tilbyder.[31]

[30] Det statlige Televerket ble skilt ut som aksjeselskap 1. november 1994. Etter det har det vært gjennom mange omorganiseringer og kjernevirksomheten - Telenor - framstår i dag som et helkommersielt selskap, om enn med en stor statlig eierandel. Fra i praksis å være nasjonal monopolist på teletjenester har det i dag storparten av virksomheten i utlandet.

[31] Kanskje kan HROer litt spøkefullt betegnes som «en ingeniørs drøm, men en økonoms mareritt»?

6 KONKLUSJON

Her gjør jeg først en oppsummering av oppgaven. Så ser jeg litt overordnet på selve problemstillingen og mitt arbeid med oppgaven, før jeg avslutter med noen betraktninger rundt mulig videre forskning.

6.1 OPPSUMMERING

Jeg har tatt opp det generelle spørsmålet om det er mulig å forberede seg på det ukjente, ved konkret å se på hvordan et telekommunikasjonsselskap håndterer driften av nettverket og leveranse av sine tjenester. For å behandle problemstillingen *«Kan det oppstå uventede hendelser av alvorlig karakter og hvordan kan selskapet eventuelt beskytte seg mot dem?»* har jeg utformet to forskningsspørsmål:

1. *Hva kjennetegner hendelser som er uventede og som kan ha en alvorlig eller katastrofal konsekvens for selskapet?*
2. *Hvordan kan selskapet forhindre at uventede hendelser oppstår og hvordan kan slike håndteres om de skulle oppstå?*

Jeg finner at det eksisterer mulige hendelser som er uventede og at disse igjen kan deles i to kategorier. De kjente hendelsene har selskapet planer for og som regel erfaring med; de ukjente vil selskapet møte på en mer «ad hoc» måte. De ukjente hendelsene ser ut til å kunne være mer truende og alvorlig og jeg har diskutert hvordan disse kan klassifiseres ytterligere.

For å hindre og håndtere uønskede hendelser finner jeg at selskapet i stor grad bruker klassisk sikkerhetstenkning. Det gjøres ved å klassifisere og kvantifisere mulige trusler, for deretter å finne proaktive og reaktive mottiltak. Dette ser ut til å fungere svært bra for kjente hendelser men det er usikkert hvordan det vil fungere for ukjente hendelser. Sannsynligvis vil det i mye større grad bli påvirket av situasjon og personell til stede enn av planverk og rutiner.

For å håndtere ukjente trusler synes en mer moderne tilnærming å være nødvendig, og jeg har diskutert Safety-II, Resilience Engineering og High Reliability Organizations. Disse virker svært lovende da de er mer sensitiv i forhold til pågående operasjoner og mer villig til å tilpasse seg endringer for å bringe tilbake normaltilstanden. Med bakgrunn i dette har jeg sett på mulige forbedringer for selskapet.

Ulempene ved HRO og RE er også tatt opp. Det er vanskelig å beregne «businesscaset» for ukjente trusler, de fleste selskap opplever dem sjelden eller aldri. Dermed er det lett å ignorere den økonomiske trusselen slike kan utgjøre. Moderne selskap endrer seg også raskt, ofte nettopp med det som mål å effektivisere og fjerne det som oppfattes som ikke direkte lønnsomt.

Dette gjør at spesielt HROer ser mer ut til å være egnet for situasjoner der «failure is not an option». Nettopp erkjennelsen om at man ikke har råd til å feile, vil etter min mening være

første skritt til å unngå å gjøre det. Myndighetene kan bruke bøter som mekanisme for å framtvinge dette (ref. GDPR), men selskaper kan også på eget grunnlag velge å bli mer robuste.

Mine funn bekrefter tankesettet som ligger til grunn for Safety-II, HRO og RE. Jeg finner også at eksisterende litteratur om sikkerhet, og ikke minst klassifisering av ukjente trusler, har vært relevant og nyttig som utgangspunkt for drøftingen.

6.2 PERSONLIGE REFLEKSJONER OVER PROBLEMSTILLINGEN

Gjennom arbeidet med oppgaven har jeg reflektert mye over hvordan man kan forberede seg på det uventede. Jeg misunner på et vis de organisasjonene som har evne og vilje til å bygge den robustheten som gjør at man er i stand til å håndtere det ukjente. Slik robusthet er ikke binær i den forstand at enten har man det eller så har man det ikke. I den grad det kan måles, så er det mer en lineær verdi. Ofte er man er villig til redusere på robustheten når man er under press. Jeg ser et tydelig skille mellom hva man skulle ønske man gjorde (proaktivt og reaktivt) i selskapet, kontra hva man virkelig gjør.

Mot et slikt bakteppe er sannsynligvis den nye personvernlovgivningen fra EU et korrekt virkemiddel for å få nok oppmerksomhet i aktuelle selskap. Dersom konsekvensene av å feile blir store nok, så må systemer og organisasjoner designes, bygges og drives på en slik måte at de ikke kan feile. Kommersielle virksomheter veier i praksis ethvert tiltak i forhold til økt inntjening eller risiko for økt kostnad. Så er ikke sikkerhet en isolert prosess i noe selskap, økt satsning på sikkerhet vil sannsynligvis også kunne gi positive sideeffekter, eksempelvis innenfor kvalitet og kultur.

Samtidig synes jeg det er et paradoks at det sannsynligvis ikke nødvendigvis er så store kostnader involvert i å forbedre håndteringen av det ukjente. Bare det å gi temaet oppmerksomhet og tid i ulike fora vil sannsynligvis øke sjansene for god håndtering neste gang det uventede inntreffer. Kanskje kan slik oppmerksomhet i noen situasjoner føre til at det uventede ikke oppstår – ville verden i 2017 fått «Brexit» og president Trump i USA dersom de som stemte anså det som et reelt utfall?

6.3 PERSONLIGE REFLEKSJONER OVER OPPGAVEN

Ved å bruke kvalitativ metode har jeg fått anledning til å lytte til kompetente informanters meninger om problemstillingen. Det har gitt meg god anledning til å se ulike sider og høre mange gode synspunkt. Det har også gitt gode ordvekslinger om et tema som fenger og engasjerer. Samtidig erkjenner både jeg og informantene de begrensningene som omgivelsene gir. Man kan ønske seg mer tid til forberedelser før hendelser og mer ressurser og kompetanse til å håndtere hendelser, men til syvende og sist er også dette undergitt samme rammebetingelser som annen virksomhet – det må oppfattes å være riktig i et kost/nytte perspektiv. Jeg håper at oppgaven i alle fall kan belyse problemstillingen.

For min egen del har arbeidet med oppgaven gitt meg økt forståelse for fagfeltet og hvilket mulighetsrom man har når man skal håndtere det ukjente. Jeg tror jeg i dag har en bedre helhetsforståelse og oversikt, men er samtidig ydmyk i forhold til at er et stort fagfelt som kunne vært utforsket mye mer.

Jeg har forsøkt å være bevisst på min egen rolle. Som avdelingsleder i selskapet har jeg som andre mellomledere lenge hatt et ansvar for å håndtere uønskede situasjoner – enten de er kjente eller ukjente. Jeg har forsøkt så godt som mulig å holde egne meninger i bakgrunnen under intervjuene og la informantene forme intervjuene. Det har vært min intensjon å la funnene komme til uttrykk mest mulig slik de har framkommet, og heller la mine tolkninger og tillegg komme i drøftingen.

6.4 MULIG VIDERE FORSKNING

Jeg har sett mye på Safety-II, HRO og RE i oppgaven. Disse perspektivene har fokus på det som går bra, på årvåkenhet og på tidlig håndtering av uønskede hendelser. Dette fungerer fint i forhold til ukjente hendelser, der det kan være vanskelig å se for seg preventive tiltak. På den annen side er det som regel alltid bedre å forebygge enn å reparere i etterkant.

Nå lever vi i en tid der vi for første gang kan få tilgang på all eksisterende informasjon om et emne. Samtidig beskriver to av de tre «ukjent» kategoriene ovenfor hendelser som er kjent for noen, men som lokalt framstår som «svarte svaner» eller noe vi eventuelt må «gjenoppdage». Det ukjente ved dem er kanskje i bunn og grunn et informasjonsproblem.

Det ville derfor vært spennende om dette ble utfordret i framtidig forskning. Hvordan kan man bli mer bevisst på hvilke ukjente hendelser som kan inntreffe og hvordan de kan ramme? Kan moderne teknologi bidra til å gjøre mengden av ukjente hendelser mindre?

FIGURER

Figur 1 – Bow tie modellen 10
Figur 2 - Swiss cheese modellen (Reason, 1997) 10
Figur 3 – De fire kombinasjonene av kjent og ukjent, oversatt fra Paltrinieri et al. (2012) 13
Figur 4 - Visualisering av forskningsdesignet 15
Figur 5 - Intervjustruktur 16
Figur 6 - Selskapets organisering 20
Figur 7 - Mapping mellom Westrum og Rumsfeld 29
Figur 8 - Overganger mellom ulike trusler 30
Figur 9 - HRO principles (Weick et al, 2008) 40
Figur 10 - HRO vs. RE 42

7 REFERANSER

Aven, T. (2013). On the meaning of a black swan in a risk context. *Safety Science, 57*, 44-51. doi:http://dx.doi.org/10.1016/j.ssci.2013.01.016

Bechky, B. A., & Okhuysen, G. A. (2011). Expecting the unexpected? How SWAT officers and film crews handle surprises. *Academy of Management Journal, 54*(2), 239-261.

Girard, J. P., & Girard, J. L. (2009). *A Leader's Guide to Knowledge Management*: Business Expert Press, LLC, New York.

Grøtan, T. O. A., Eirik. (2017, 11/03-2017). *A methodology for identification of hidden, dynamic and emerging threats related to SCADA integration – experiences from a methodologically oriented workshop*. Arlington.

Haddon Jr, W. (1970). On the escape of tigers: an ecologic note. *American Journal of Public Health and the Nations Health, 60*(12), 2229-2234.

Haddon Jr, W. (1980). Advances in the epidemiology of injuries as a basis for public policy. *Public health reports, 95*(5), 411.

Haugen, S. V., Jan Erik. (2015). Perspectives on risk and the unforeseen. *Reliability Engineering & System Safety, 137*, 1-5.

Hollnagel, E. (2014). *Safety-I and Safety-II : The Past and Future of Safety Management*. Farnham: Ashgate Publishing Ltd.

Hollnagel, E. W., David D.; Leveson, Nancy. (2012). *Resilience Engineering: Concepts and Precepts*. In. Retrieved from https://www.amazon.com/gp/product/B009KNDF64

Hopkins, A. (2014). Issues in safety science. *Safety Science, 67*, 6-14. doi:http://dx.doi.org/10.1016/j.ssci.2013.01.007

Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser?* (3. utgave ed.). Oslo: Cappelen Damm.

Jacobsen, D. I., & Thorsvik, J. (1997). *Hvordan organisasjoner fungerer: innføring i organisasjon og ledelse*: Fagbokforlaget.

Kongsvik, T. (2013). Sikkerhet i organisasjoner. *Akademika forlag*.

Mintzberg, H. (1979). Patterns in strategy formation. *International Studies of Management & Organization, 9*(3), 67-86.

Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M., & Cozzani, V. (2012). Lessons learned from Toulouse and Buncefield disasters: from risk analysis failures to the identification of atypical scenarios through a better knowledge management. *Risk Analysis, 32*(8), 1404-1419. doi:10.1111/j.1539-6924.2011.01749.x

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies*. Princeton: Princeton University Press.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science, 27*(2), 183-213.

Rausand, M., & Utne, I. B. (2009). *Risikoanalyse - teori og metoder*.

Reason, J. (1997). Managing the risks of organizational accidents. *Hampshire (England): Ashgate Publishing*.

Rosness, R., Håkonsen, G., Steiro, T., & Tinmannsvik, R. (2000). *The vulnerable robustness of High Reliability Organisations: A case study report from an offshore oil production platform.* Paper presented at the 18th ESReDA seminar Risk Management and Human Reliability i Social Context, Karlstad, Sweden.

Rumsfeld, D. (2002). Nato HQ Speech and Press Conference. Retrieved from http://www.nato.int/docu/speech/2002/s020606g.htm

Taleb, N. N. (2007). *The Black swan: The Impact of the Highly Improbable (Incerto)*: Random House.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2008). Organizing for high reliability: Processes of collective mindfulness. *Crisis management, 3*(1), 81-123.

Westrum, R. (2006). *Resilience Engineering*. In D. R. W. Erik Hollnagel, Nancy Leveson (Ed.), *Concepts and Precepts (Kindle edition)*.

Wreathall, J. (2006). Properties of resilient organizations: an initial view. *Resilience engineering: Concepts and precepts*, 275-285.

Vedlegg A TILBAKEMELDING FRA NSD

Eirik Albrechtsen
Institutt for sosiologi og statsvitenskap NTNU
Dragvoll
7491 TRONDHEIM

Vår dato: 05.12.2016 Vår ref: 50864 / 3 / AMS Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 01.11.2016. Meldingen gjelder prosjektet:

50864	*Kan det oppstå totalt uventede/uforutsigbare hendelser - og hvordan kan i tilfelle selskapet beskytte seg mot disse? (I kontekst av et selskap innenfor IT/Telekom)*
Behandlingsansvarlig	*NTNU, ved institusjonens øverste leder*
Daglig ansvarlig	*Eirik Albrechtsen*
Student	*Jan Gunnik Hope*

Personvernombudet har vurdert prosjektet og finner at behandlingen av personopplysninger er meldepliktig i henhold til personopplysningsloven § 31. Behandlingen tilfredsstiller kravene i personopplysningsloven.

Personvernombudets vurdering forutsetter at prosjektet gjennomføres i tråd med opplysningene gitt i meldeskjemaet, korrespondanse med ombudet, ombudets kommentarer samt personopplysningsloven og helseregisterloven med forskrifter. Behandlingen av personopplysninger kan settes i gang.

Det gjøres oppmerksom på at det skal gis ny melding dersom behandlingen endres i forhold til de opplysninger som ligger til grunn for personvernombudets vurdering. Endringsmeldinger gis via et eget skjema, http://www.nsd.uib.no/personvern/meldeplikt/skjema.html. Det skal også gis melding etter tre år dersom prosjektet fortsatt pågår. Meldinger skal skje skriftlig til ombudet.

Personvernombudet har lagt ut opplysninger om prosjektet i en offentlig database, http://pvo.nsd.no/prosjekt.

Personvernombudet vil ved prosjektets avslutning, 01.09.2017, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Anne-Mette Somby

Dokumentet er elektronisk produsert og godkjent ved NSDs rutiner for elektronisk godkjenning.

NSD Norsk senter for forskningsdata AS Harald Hårfagres gate 29 Tel: +47-55 58 21 17 nsd@nsd.no Org.nr. 985 321 884
NSD – Norwegian Centre for Research Data NO-5007 Bergen, NORWAY Faks: +47-55 58 96 50 www.nsd.no

Personvernombudet for forskning

Prosjektvurdering - Kommentar

Prosjektnr: 50864

Utvalget skal informeres skriftlig og muntlig om prosjektet og samtykker til deltakelse. Informasjonsskrivet er godt utformet.

Personvernombudet legger til grunn at forskere og studenter følger NTNU sine rutiner for datasikkerhet. Dersom personopplysninger skal sendes elektronisk eller lagres på privat pc/mobile enheter, bør opplysningene krypteres.

Forventet prosjektslutt er 01.09.2017. Ifølge prosjektmeldingen skal innsamlede opplysninger da anonymiseres. Anonymisering innebærer å bearbeide datamaterialet slik at ingen enkeltpersoner kan gjenkjennes. Det gjøres ved å:

- slette direkte personopplysninger (som navn/koblingsnøkkel)
- slette/omskrive indirekte personopplysninger (identifiserende sammenstilling av bakgrunnsopplysninger som f.eks. bosted/arbeidssted, alder og kjønn)
- slette digitale lydopptak

Kontaktperson: Anne-Mette Somby tlf: 55 58 24 10
Vedlegg: Prosjektvurdering
Kopi: Jan Gunnik Hope jgh@nextgentel.no

Vedlegg B INFORMASJONSSKRIV MED SAMTYKKEERKLÆRING

Forespørsel om deltakelse i forskningsprosjektet

Kan vi forberede oss på det totalt uventede?

Jan Gunnik Hope - 2016

Bakgrunn og formål
Jeg holder på med en mastergrad ved NTNU der jeg ønsker å *se om det kan oppstå uventede / uforutsigbare hendelser* i NextGenTel og hvordan det *eventuelt er mulig å forberede seg på slike*. For å belyse emnet ønsker jeg å intervjue en del nåværende og tidligere ansatte.
Jeg har på eget grunnlag valgt ut de personene jeg ønsker å spørre. Utvalget er gjort med tanke på å få litt spredning / variasjon i bakgrunn, erfaring, stilling og tilnærming til problemstillingen. Det er mulig antallet som intervjues utvides underveis.

Hva innebærer deltakelse i studien?
Dersom du sier ja til å delta vil det innebære et en-til-en intervju med meg med en estimert varighet på en time / halvannen. Du trenger ikke forberede deg noe spesielt, men tenk gjerne litt over problemstillingen som skissert over.
Jeg ønsker for enkelhets skyld å ta samtalen opp på en lydfil og transkribere den etterpå. Dersom du ønsker det, kan du reservere deg mot at jeg gjør lydopptak.

Hva skjer med informasjonen om deg?
Alle personopplysninger vil bli behandlet konfidensielt.
Jeg vil ha tilgang til egne notater og eventuelt lydopptak. Veileder vil få tilgang til notatene i den grad det er nødvendig – sannsynligvis bare som sitater / bakgrunnseksempler. Veileder vil ikke få tilgang til å vite hvem som har sagt hva.
I endelig publikasjon vil sitater kunne bli brukt og eksempler gjengitt. Ingen av de som intervjues skal da kunne gjenkjennes.
Prosjektet skal etter planen avsluttes 1. september 2017. Etter prosjektslutt vil lydfilene og intervjunotatene slettes.

Frivillig deltakelse
Det er frivillig å delta i studien, og du kan når som helst trekke ditt samtykke uten å oppgi noen grunn. Det vil ikke ha noen innvirkning på vårt kollega-/arbeidsforhold om du velger å delta, eller avstår fra det.
Dersom du trekker deg, vil alle opplysninger om deg bli anonymisert.

Dersom du ønsker å delta eller har spørsmål til studien, ta kontakt med Jan G. Hope, mobil 48082210, jgh@nextgentel.no

Studien er meldt til Personvernombudet for forskning, NSD - Norsk senter for forskningsdata AS.

Samtykke til deltakelse i studien

Jeg har mottatt informasjon om studien, og er villig til å delta.

---------- ----------
Dato Navn

Vedlegg C INTERVJUGUIDE

Intervjuguide

Jan G. Hope – Masteroppgave 2016

Ingress

- Velkommen
- Takk
- Gjenta nøkkelinfo fra informasjonsskrivet
    - Bakgrunn (Masteroppgave)
    - Presisere at intervjuet er «uavhengig» av jobbrelasjon mellom oss
    - Anonymitet, mulighet til å trekke seg når som helst
- Problemstillingen
    - Problemstillingen i litt detalj
    - Eksempler: Svart svane, 9/11

Spørsmål

Bakgrunn

1. Kan du kort beskrive din stilling i bedriften?
    a. Stilling
    b. Erfaring
    c. Hvilken rolle har du i vakt-/beredskaps-/feilrettings-situasjoner?

Kjente situasjoner

2. Kan du beskrive feilsituasjoner vi opplever?
    a. Hvordan har vi forberedt oss til å håndtere disse?
    b. Hvor godt synes du vi håndterer dem? Hvorfor?
3. Kan du beskrive feilsituasjoner vi har planlagt for som du ikke har opplevd / hørt om?

Uventede situasjoner

4. Er totalt uventede / uforutsigbare hendelser en mulighet på hos oss?
    a. Teoretiske eksempler? (mest for å få praten / tankene i gang)
    b. Har du hørt om tilsvarende hendelser i vår bransje?
5. Gitt at slike hendelser kan inntreffe:
    a. Hva vil konsekvensen være for
        i. Selskap
        ii. Kunder
        iii. Tredjepart/omgivelser
    b. Gir det verdi å klassifisere slike hendelser?
        i. Hvorfor gir det evt. verdi?
        ii. Hvordan vil du klassifisere dem?
            1. Ondsinnede vs. uventede?
            2. Førstegangshendelser «globalt» vs. «Aldri skjedd hos oss»?

6. Hvordan tror du vi vil reagere i en slik situasjon?
    a. Hvorfor det? Utdyp
7. Hvordan kan selskapet
    a. Beskytte seg mot / forberede seg på slike hendelser
    b. Håndtere slike hendelser dersom de oppstår
    c. Gjør vi disse tingene? Hvorfor / hvorfor ikke?

Omgivelsene

8. Hva er forventningene til selskapets håndtering av slike hendelser fra
    a. Aksjonærer
    b. Ansatte
    c. Kunder
    d. Tredjepart/omgivelser

Egress

9. Avslutningsvis, hva tenker du generelt om temaet?
    a. Er temaet relevant?
    b. Har vi dekket det som er verdt å si?
    c. Andre sluttkommentarer?

Takk for praten!