Universitetet i Stavanger

Charlotte Hille og Charlotte Nordbø Myr

Security-kultur

Hva kan Marinen som organisasjon gjøre for å forbedre security-kulturen?

Masteroppgave 2016

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I

Risikostyring og sikkerhetsledelse

MASTEROPPGAVE

SEMESTER:

Vår og høstsemester 2016

FORFATTER:

Charlotte Hille og Charlotte Nordbø Myr

VEILEDER:

Riana Steen

TITTEL PÅ MASTEROPPGAVE:

Security-kultur

EMNEORD/STIKKORD:

Security, Security-kultur, cyber, trussel, risiko, usikkerhet, innsidetrussel,

---

SIDETALL: 96 (Eksklusiv tabeller, figurer, diagrammer og vedlegg)

BERGEN, 12. oktober 2016…….

Forord

Å skrive masteroppgaven har vært utrolig lærerikt og givende. Faglig har det gitt oss muligheten til å gå i dybden innenfor områder vi har egeninteresse av, i tillegg til å være jobbrelevant. Vi har fått en påminnelse om at selv om organisasjonen vår har sine utfordringer, er vi omgitt av kollegaer med store mengder kunnskap, erfaringer og vilje til å dele og støtte oss i vårt arbeid. Vårt interne samarbeid har gitt oss muligheten til drøfting og refleksjon med en person som er vel så neddykket i temaet som den andre, og bidratt til å forbedre prosessene underveis med å stille krav og kvalitetssikre hverandres bidrag.

Vi vil rette en stor takk til våre informanter som utelukkende stilte seg positive til å delta, og hadde et engasjement for vår problemstilling som motiverte til videre arbeid.

I tillegg ønsker vi å takke venner og kollegaer som har bistått.

Vi takker vår veileder Riana Steen for hennes entusiasme og engasjement gjennom hele prosessen. Din klare tale er ikke til å misforstå, men verdsettes stort! Tydelige tilbakemeldinger, konstruktiv kritikk og press ledet oss til målet.

Oslo/Bergen, Oktober 2016

Charlotte Hille, Charlotte Nordbø Myr

Vil rette en stor takk til min største støttespiller, min mann Jens- Erik Myr, som har vært en bauta i hjemmet med våre 3 barn, hund og katt. Du er meget dyktig, tusen takk.

Charlotte Myr.

Samarbeidsorganisasjoner i masteroppgaven

Nasjonal sikkerhetsmyndighet (NSM)

Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet (NSM, 2016). Direktoratet er nasjonal varslings- og koordineringsinstans for alvorlige dataangrep og andre IKT-sikkerhetshendelser. Direktoratet er administrativt underlagt Forsvarsdepartementet (FD), og rapporterer med faglig ansvarslinje til Justis- og beredskapsdepartementet (JD) for oppgaveløsning i sivil sektor, og til Forsvarsdepartementet for militær sektor.

Roar Thon er fagdirektør for sikkerhetskultur i NSM, og har blant annet jobbet med sikkerhetskulturbegrepet siden 2005. Thon har bakgrunn fra politiet og Forsvaret, og kom til NSM som yrkesoffiser fra militærpolitiet (MP). Gjennom Thons yrkeskarriere i Forsvaret og politiet har han drevet med etterforskning av mennesker og hendelser. Thon er teknologiinteressert, og selv om han jobber i en veldig teknologifokusert organisasjon er det mennesker, og i det perspektivet også organisasjon, han primært jobber med. I følge Thon er det samspillet, eller mangel på samspill, mellom mennesker og teknologi som er med på å påvirke sikkerhetstilstanden.

Forsvarets sikkerhetsavdeling (FSA)

FSA er fagmyndighet for sikkerhetstjenesten i Forsvaret på vegne av Forsvarssjefen. FSA ivaretar det overordnede ansvaret for utøvelsen av sikkerhetstjenesten i Forsvaret ved å sikre at virksomheten organiseres, utføres og revideres i samsvar med sikkerhetsloven. FSA holder oversikt over det sikkerhetsmessige risikobildet som omgir Forsvaret, samt norsk militær aktivitet både hjemme og ute. FSA har ansvaret for fagsiden «Sikkerhetstjeneste» som er autorativ for faget sikkerhetstjeneste (security) i Forsvaret. FSAs overordnede oppgave i Forsvarssjefens målsetting om en effektiv militær struktur, er å styrke og opprettholde en sikkerhetsmessig beskyttelse av Forsvarets operative evne og grunnlaget for denne. For å oppnå dette er det nødvendig å utvikle en tidsriktig sikkerhetskompetanse og kapasitet i linjen. Den forebyggende sikkerhetstjenesten skal være basert på kunnskap, holdninger og troverdighet. Kunnskaper opparbeides gjennom personlig og faglig utvikling. Initiativ og kreativitet skal stimuleres til det beste for Forsvaret, FSA og den enkelte medarbeider.

Kommandør Hans Kristian Herland har sittet som sjef FSA siden 2010. Kommandør Herland startet sin militære karriere ved befalsskolen for kystartilleriet, og har hatt en bred

tjenesteerfaring fra Sjøforsvaret. I 2002 valgte han en mer strategisk retning og har erfaring fra både FD og Forsvarsstaben (FST).

Cyberforsvaret (CYFOR)

CYFOR sin hovedoppgave er å understøtte Forsvarets virksomhet med sikre og effektive kommando og kontroll informasjonssystemer. CYFOR skal lede utviklingen mot et nettverksbasert forsvar. De skal støtte den teknologiske utviklingen av Forsvaret, og implementere ny teknologi og nye konsepter. CYFOR leder Forsvarets innovasjons- og eksperimenteringsvirksomhet og produserer spisskompetansen i form av militære telematikkingeniører og ledere.

Oberstløytnant (Oblt) Ivar Kjærem er sikkerhetsleder i Cyberforsvaret. Han har sin grunnutdanning fra Hærens samband. Oblt Kjærem har bachelorgrad i programutvikling og en mastergrad i informasjonssikkerhet. Han har i snart 20 år arbeidet med ulike aspekter innen sikkerhet i Forsvaret, først og fremst knyttet til informasjonssikkerhet og cyber forsvar.

Nytrøen (avdelingssjef i E-tjenesten)

Brigader (BG) Johannes Nytrøen var avdelingssjef i Etterretningstjenesten da intervjuet ble gjennomført. BG Nytrøen har bred tjenesteerfaring fra både kommando- og stabsstillinger. Etter å ha fullført Krigsskolen tjenestegjorde han i diverse hæravdelinger, og har videre gjennomført Stabsskolen 1 og 2. BG Nytrøen var prosjektleder for etableringen av Forsvarets fellesoperative hovedkvarter i Bodø. Brigaderen har deltatt i flere internasjonale operasjoner, og var den første sjefen for Etterretningsbataljonen (EBN).

Roer (CLTRe)

Kai Roer (Røer) er en norsk sikkerhetsekspert med fokus på security-kultur. Roer har utgitt flere bøker om ledelse og sikkerhet, forelest på universiteter og høyskoler i Europa og Asia, og er en mye benyttet foredragsholder på konferanser og seminarer om security rundt i verden. I 2013 ga han bort Rammeverk for Security-kultur (Security Culture Framework) til det globale sikkerhetsmiljøet. Roer fikk i 2015 prisen Ron Knode Service Award av Cloud Security Alliance (CSA) for sitt fremragende arbeid med å spre kunnskap og interesse om nettskysikkerhet. I det daglige leder Roer et norsk sikkerhetsforetak, CLTRe AS, som leverer tjenester innen måling av security-kultur.

Sammendrag

Forsvaret har hatt et stort fokus på safety i lengre tid, mens security ikke blir omtalt og håndtert i like stor grad i det daglige arbeidet. For å håndtere security må det ligge en security-fokusert kultur til grunn. Vi har valgt å fokusere på å kartlegge security-kulturen og hvordan den kan bidra til håndtering av trusler, spesifikt innsidetrussel.

Hensikten med forskningen er å kartlegge menneskelige, teknologiske og organisatoriske (MTO) faktorer som påvirker risikoen og organisasjonens evne til håndtering. Verdier, sårbarheter og trusler beskriver risikoen, og organisasjonens adferd og føringer påvirker det risikobildet som skapes. Følgende problemstilling innleder til videre forskningsarbeid:

«Hva kan Marinen som organisasjon gjøre for å forbedre security-kulturen?»

Gjennom første forskningsspørsmål, ved bruk av etterretningsbaserte rapporter og fagintervju, forsøker vi å vise et bilde av innsidetruslene som Marinen står ovenfor. Forskningsspørsmål to besvares gjennom observasjoner, fag-, ledelse- og hurtigintervjuer hvor vi ser på nåværende security-kultur i Marinen. Forskningsspørsmål tre besvares ved å se sammenhengen mellom forskningsspørsmål en og to, og trekke ut mulige tiltak for å forbedre security-kulturen i Marinen.

Analysen viser at innsidetrusselen er høy, og MTO-faktorene er sårbarheter som gjør oss utsatt for angrep. Funnene fra ledelse- og hurtigintervjuene viser manglende kompetanse og forståelse, ikke bare for trusselen, men også for egne verdier og sårbarheter. Dette kan ha en sammenheng med at det ikke er en rød tråd på security i Forsvarets utdanning- og opplæringssystem. I tillegg fremkommer det at prosedyrer og retningslinjer ikke er godt nok kjent. Uklar begrepsbruk, divergerende praksis mellom avdelingene, manglende ressurser og føringer på hva som kreves for å håndtere fagfeltet security, vanskeliggjør håndteringen av security på et gjennomgående nivå i organisasjonen. Intervjufunnene viser også at Marinen ikke har tilstrekkelig robust security organisasjon med delvis uklare ansvarsforhold, og til tross for manglende forståelse så tas det avgjørelsen av hva som er rapporteringsverdig på laveste nivå. I følge resultatene ville det kunne være et behov for et rapporteringssystem som er enkelt nok til å få alle til å rapportere, og at det sitter fagkompetente ansatte et nivå eller to høyere opp som tar vurderingen av hva som må rapporteres videre. Uten et fungerende rapporteringssystem vil ikke organisasjonen kunne ta lærdom av hendelsene, se behovene, eller gi et riktig bilde videre til politisk/strategisk nivå, og organisasjonen vil ikke få nødvendig kompetanse eller ressurser for å håndtere trusselen.

Liste over forkortelser

Forkortelser	Forklaring
ASL	Avdelingssikkerhetsleder
BG	Brigader (Militær grad)
CIA	Central Intelligence Agency
CLTRe	Culture
CSA	Cloud Security Alliance
CYFOR	Cyberforsvaret
DIF	Driftsenhet i Forsvaret
DSL	Datasikkerhetsleder
EBN	Etterretningsbataljonen
E-tj	Etterretningstjenesten
EU	European Union
FBI	Federal Bureau of Investigation
FD	Forsvarsdepartementet
FISBASIS	Forsvarets infrastruktur basis tjenester
FMA	Forsvarets materiell
FOKUS	E-tjenestens ugraderte trusselvurdering
FSA	Forsvarets sikkerhetsavdeling
FST	Forsvarsstaben
GIS	Generalinspektøren i Sjøforsvaret
GDS	Grunnlagsdokument sikkerhet
HRO	High Reliability Organization
IKT	Informasjons- og kommunikasjonsteknologi
IS	Islamske stat
JD	Justis- og beredskapsdepartementet
KE	Kysteskadren
KSL	Kryptosikkerhetsleder
LKM	Lokal koordinerende myndighet
MTO	Menneskelig, Teknologiske, Organisatoriske
MP	Militærpoliti
NATO	North Atlantic Treaty Organization
NorCERT	Norwegian Computer Emergency Response Team
NOU	Norges offentlige utredninger
NSM	Nasjonalt sikkerhetsmyndighet
Oblt	Oberstløytnant (Militær grad)
PST	Politiets sikkerhetstjeneste
SST	Sjøforsvarsstaben

Definisjoner og begreper

Listen inneholder definisjoner på de viktigste begrepene som er brukt i oppgaven. Terminologiforståelsen i punkt 3.1 viser hvordan vi har kommet frem til enkelte av begrepene vi bruker.

Cyberdomenet: består av fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedier og data (E-tj, 2013) (s.17)

Cybersikkerhet: handler om å beskytte «alt» som er sårbart fordi det er koblet til, eller på annen måte er avhengig av informasjons- og kommunikasjonsteknologi (FDs cyberretningslinjer 2014) (s.18)

Innsiderisiko: faren for at tilsiktede uønskede handlinger skal kunne utføres som følge av plassering eller utnyttelse av personell med adgang til en virksomhet, systemer, informasjon eller prosesser (NSM, 2015a) (s.19)

Risiko: Mulige konsekvenser ved tilsiktet uønsket hendelser med tilhørende usikkerhet. Disse uønskede hendelsene kan være i forhold til trusler mot verdier, og hvordan konsekvensene blir er avhengig av sårbarhetsgraden og kapasiteten til å møte truslene (s.11)

Safety: Operativ sikkerhet er i denne sammenheng alt systematisk arbeid med sikkerhets- og risikoforhold for å optimalisere yteevne og slagkraft, og derved redusere risiko for tap og uønskede hendelser i militære operasjoner og aktiviteter (Forsvaret, 2010) (tabell 2)

Security: Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet (Sikkerhetsloven, 1998) (s.17)

Security-kultur: Produktet av verdier, holdninger, kompetanse, normer og regler som kommer til uttrykk gjennom organisasjonens totale security-adferd for å redusere risiko som følge av sikkerhetstruende virksomhet (s.21)

Sikkerhet: evnen til å unngå skade på eller tap av mennesker, ytre miljø og materiell på grunn av akutte, utilsiktede hendelser (ulykker, uhell) eller kriminelle handlinger (Sjøforsvaret, 2016) (tabell 2)

Sikkerhetskultur: De aspektene av organisasjonskulturen som påvirker holdninger og adferd relatert til en økning eller senkning av risiko (Guldenmund, 2000) (s.21)

Trussel: Med en trussel forstås ethvert forhold eller enhver enhet med et potensial til å forårsake en uønsket hendelse (NOU 2000:24) (s.12)

Trusselbilde: Tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet (Norsk Olje og gass, 2003) (s.12)

Verdi: Ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressursen (NSM, 2014) (s.12)

Usikkerhet: Usikkerhet forstår vi som mangel av kunnskap om ukjente størrelser (Flage et al., 2009) (s.12)

Oversikt over Tabeller, diagrammer og figurer

Figurer

Diagram

Innhold

1. Innledning

1.1 Bakgrunn

Vårt dynamiske og komplekse samfunn gir store utfordringer til styring av sikkerheten i industrien og i samfunnet vårt generelt. På mange områder i samfunnet skjer det raske teknologiske endringer, dette innbefatter også den raske utviklingen innen informasjons- og kommunikasjonsteknologien. Vi har fått et mer åpent verdenssamfunn, hvor en raskere uavhengig av geografisk plassering, kan opprettholde kommunikasjon og samarbeid.

Denne raske utviklingen fører til stor grad av integrering og kobling mellom systemer, noe som også gir mer komplekse teknologiske systemer. Den store integrasjonen og gjensidige avhengigheten mellom viktige samfunnsfunksjoner kan bidra til at alvorlige forstyrrelser i en funksjon kan gi store ringvirkninger for andre funksjoner. De funksjonene som er absolutt nødvendige for samfunnsvirksomheten, også kalt «bærebjelker», er kraftforsyningen, telekommunikasjon, ledelse og informasjon og forsyning av rent vann og ernæring. Svikt i en av disse «bærebjelkene» kan medføre svikt i de fleste andre samfunnsfunksjoner (Aven et al., 2013 s.23). Direktør i Nasjonalt sikkerhetsmyndighet (NSM), Kjetil Nilsen, uttalte at «*Det er behov for en omfattende satsing på sikkerhet i Norge mot 2020. Risiko- og sårbarhetsbildet har blitt mer komplekst og vi må ta tak i det vi kan gjøre noe med for å kunne beskytte verdiene vi har i samfunnet*» (NSM, 2015b s.26).

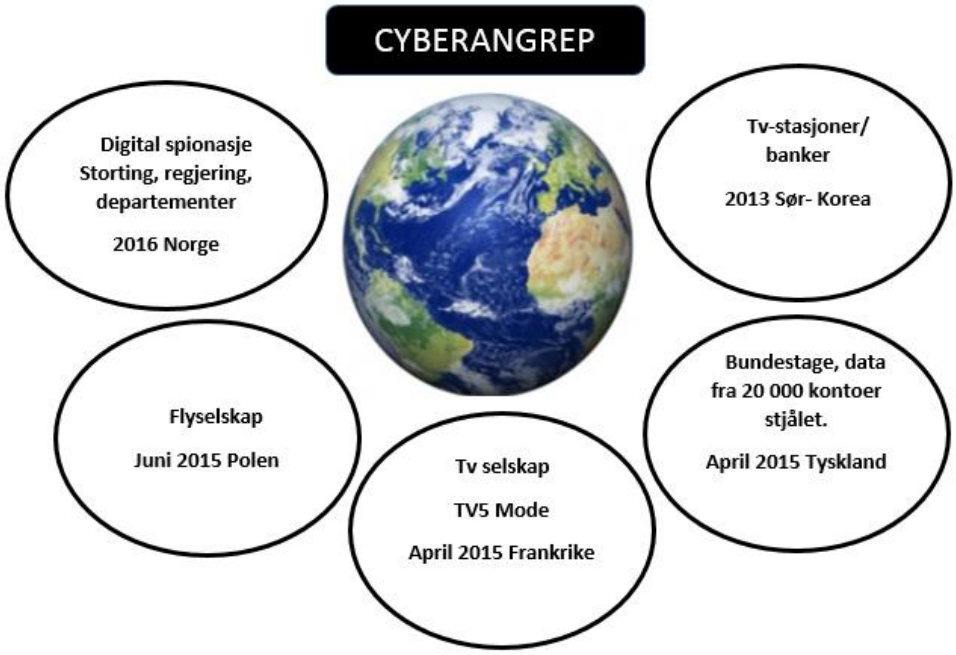
Samtidig vil det økende kostnads- og effektivitetspresset, et næringsliv i stadig raskere omstilling samt reduksjon i bemanning i mange virksomheter, kunne gi en økt sikkerhetsutfordring i samfunnet (Aven et al., 2013).

Norge forvalter i dag store verdier, som andre kan ha interesse av å tilegne seg for egen vinning eller for å gjøre skade. På flere områder er trusselen økende eller vedvarende høy (NSM, 2015b s.26). En lang rekke aktører kan tenkes å ha som målsetting å skaffe seg informasjon om stats- og forretningshemmeligheter, forskningsresultater, teknologiske nyvinninger eller strategier og planer (NSM, 2015a s.14). Nasjonal sikkerhetsmyndighet uttaler at de vet at etterretningstrusselen fra andre starter er høy, og at de stadig tar i bruk nye metoder som for eksempel cyberangrep (NSM, 2015b s.26).

For å imøtekomme utfordringer har sikkerhetsarbeidet endret karakter flere ganger de siste tiårene. Det er et skifte fra fokus på sikkerhet gjennom teknologiske løsninger til fokus på sikkerhet gjennom reduksjon av menneskelige feilhandlinger, videre til fokus på sikkerhet gjennom systemtiltak rettet mot organisasjonen og dens ledelse. I den epoken som vi er inne

i nå, hvor fokuset er på organisasjonen og ledelse, er det lagt større vekt på relasjoner og samspill mellom ulike faktorer i organisasjonen og samfunnet. En er opptatt av samspillet mellom teknologi, organisasjon og individet (Aven et al.2004 s.27).

Cyberangrep er avdekket mot norsk forsvars-, sikkerhets- og beredskapssektor, politiske prosesser og norsk kritisk infrastruktur (NSM, 2015a s.14). I 2013 var det mistanke om et cyberangrep mot tv-stasjoner banker i Sør-Korea (Dagbladet, 2013), mens det i april 2015 var et angrep mot det franske TV selskapet TV5 Mode, hvor hackere endret selskapets nettsider og sosiale medier og tok 11 tv-kanaler av luften. Disse hackerne hevdet at de hadde tilknytning til den islamske stat (IS). Samme måned rapporterte tyske medier at hackere hadde stjålet data fra 20 000 kontoer i Bundestag, Tyskland (NSM, 2015a s.15).

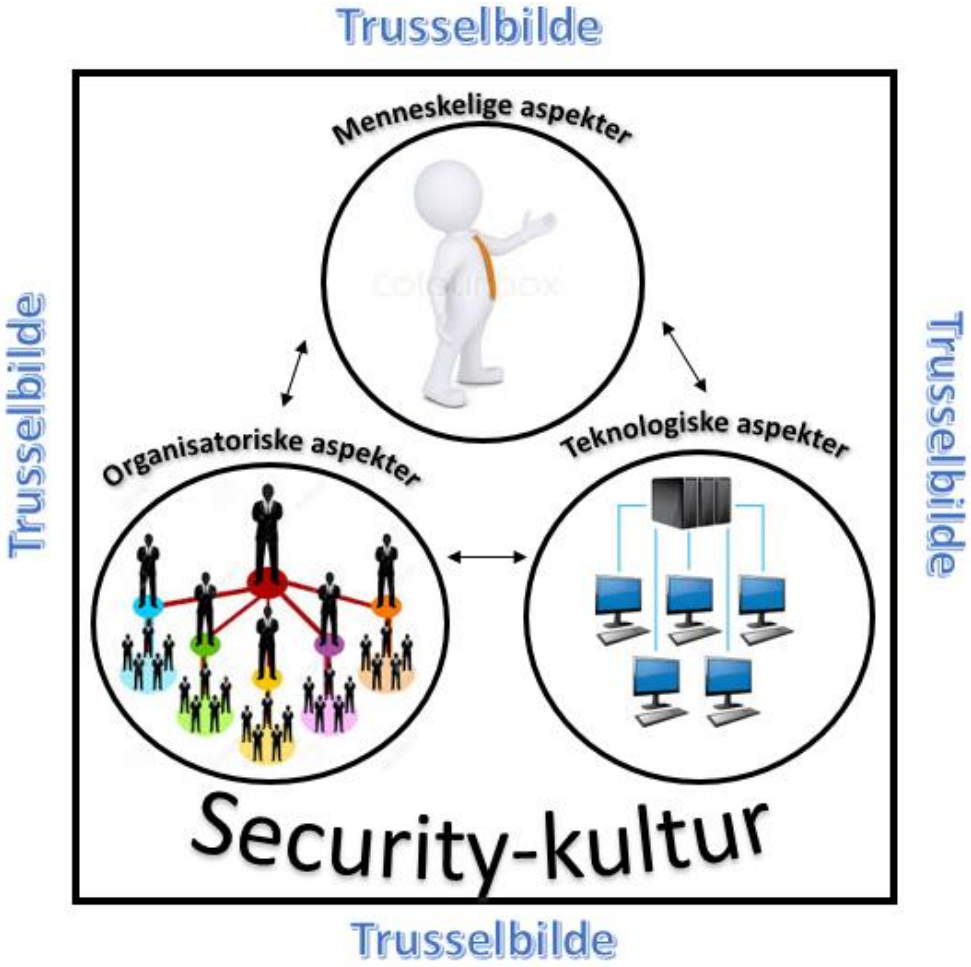


Figur 1: Visualisering av cyberangrep (Fritt utarbeidet)

I juni 2015 hadde et polsk flyselskap et cyber angrep som resulterte i at selskapet måtte innstille 10 flyavganger og utsette 12 (NSM, 2015a s.15). I februar 2016 uttalte PST-sjef Benedicte Bjørndal i et intervju at Storting, regjering og departementer har blitt utsatt for digital spionasje fra fremmede makter (TV2, 2016). Den digitale spionasjen utgjør en økende trussel mot Norge. Det er også alvorlige trusler rettet mot flere sentrale samfunnsområder (NSM, 2015a s.14). Innsidetrusselen i norske virksomheter, både i utland som innland, er reel høy (NSM, 2015b s.5). Et eksempel er fra 9. april 2016, da flere Høyrepolitikere fikk tilsendt hemmelige regjeringsnotater om Forsvarets langtidsplan fra en anonym avsender (Verdens Gang, VG, 2016). Både Politiets Sikkerhetstjeneste (PST), og Nasjonal

Sikkerhetsmyndighet (NSM), ble varslet umiddelbart og har forsøkt å spore avsenderen. Selv med flere hendelser rundt om i verden, er det i henhold til Nasjonal sikkerhetsmyndighet «Stuxnet», som er den mest kjente og ødeleggende nettverksoperasjonen hittil (NSM, 2015a s.15). I følge NSM (2015a) var den sannsynligvis rettet mot digitale styringssystemer anvendt i iransk kjernekraftindustri.

Grunnleggende mangler (eksempel manglende Cybersikkerhet) gjør det lettere for trusselaktørene å komme seg inn i norske IKT-systemer. Sikkerhetsmessige sårbarheter kan ha tekniske, menneskelige eller organisatoriske årsaker og trusselaktørene kan lett hente ut ønsket informasjon ved å utnytte disse sårbarhetene (NSM, 2015b s.15). Trussel fra innsiden av en organisasjon er et menneskelig aspekt påvirket av det organisatoriske og tekniske, noe som trusselaktører kan utnytte. Figur 2 visualiserer dette. Dette har vært en kilde til motivasjon for valg av problemstilling og forskningsspørsmål.



Figur 2: Visualisering av MTO, security-kultur og trusselbilde.

1.2 Problemstilling og formål

Sjøforsvaret, som en del av det norske Forsvaret, skal håndtere trusler og beskytte nasjonen og dens interesser. Det har vært fokus på land-, sjø- og luftdomenene, men i den senere tid har også cyberdomenet fått økt fokus. Cyberdomenets relevans for samfunnet har økt betraktelig i senere tid, og samfunnet, herunder Forsvaret, vil ikke kunne ignorere den trusselen dette domenet kan medføre. Vi har valgt å rette fokus mot cyberdomenet og den økte relevansen dette har for samfunnet, herunder Sjøforsvaret, og mer spesifikt innsidetrusselen. I et studie fra 2015 «Kultur for forebyggende sikkerhetstjeneste (security) i Sjøforsvaret», utdypet i punkt 5.2.1, viste resultatet at Sjøforsvaret har en vei å gå for å kunne tilfredsstille Sikkerhetslovens minimumskrav til forebyggende sikkerhet (security), og at det var behov for å iverksette tiltak for endring. For å forstå hva som må til for å håndtere en innsidetrussel har vi tatt utgangspunkt i de menneskelige-, teknologiske-, og organisatoriske faktorene som er med på å forme Sjøforsvaret og dens kultur. Med bakgrunn i overnevnte har vi utarbeidet følgende **problemstilling:**

«Hva kan Marinen som organisasjon gjøre for å forbedre security-kulturen?»

Vi har delt forskningen inn i to faser, hvor vi i første fase forsøker å danne et overordnet bilde av trusselsituasjonen, og hvordan Marinen imøtekommer truslene. Dette fokusområdet danner grunnlaget for første forskningsspørsmål som omhandler trusselbildet for Sjøforsvaret, og for det andre forskningsspørsmålet med hva som kjennetegner Marinens security-kultur. Etter at trusselbildet og security-kulturen i Marinen er beskrevet gjennom forskningsspørsmål en og to, vil vi med utvalgt teori belyse hvordan en forbedring av Marinens security-kultur kan forbedre evnen til håndtering av truslene. Dette tar oss over i fase to og danner fokusområdet for forskningsspørsmål tre, hvor vi ønsker å se sammenhengen mellom security-kultur og håndteringen av trusler. Vi velger primært å se på cyberdomenet og innsidetrusselen for å kartlegge forbedringsmuligheter ved security-kulturen. Følgende tre **forskningsspørsmål (FS)** ble utledet:

1. **Hva er trusselbildet fra cyberdomenet og innsidetrusselen mot Marinen?**
2. **Hva er kjennetegn ved Marinens security-kultur?**
3. **På hvilken måte kan security-kulturen i Marinen forbedres?**

Formålet med forskningsspørsmålene er å danne et bilde ved å belyse eksisterende security-kultur med det valgte teoretiske rammeverket, og drøfte Marinen sitt ståsted og mulige tiltak for forbedring av security-kulturen for å håndtere innsidetrusselen. Forskningen gikk bredt ut ved at den ble innledet med et større antall spørsmål fordelt på tre intervjuguider. Vi valgte å

fokusere bredt fremfor å gå i dybden da studien er gjort i en organisasjon som håndterer mye gradert informasjon, og det var essensielt at alt materialet ble holdt på et ugradert nivå. Vi valgte et større antall spørsmål for å forske på kulturen for å kunne danne et så korrekt bilde som mulig. I tillegg gav dette oss muligheten til seleksjon av datamaterialet for å holde forskningen ugradert. Sårbarheter er sensitivt, og vi kan ikke gå i dybden i denne studien. Punkt 4.5 fordeler og ulemper ved metoden, beskriver ytterligere utfordringen ved å holde oppgaven ugradert.

1.3 Avgrensning

Trusselbildet for Norge og Forsvaret er omfattende, og grunnet oppgavens omfang velger vi derfor å fokusere på innsidetrusselen i cyberdomenet. Cybertruslene er mange og Norge har statlige organer som er gitt ansvaret for kartlegging og håndtering av truslene. Vi legger til grunn overordnede organer, som NSM, FSA og CYFOR, sine føringer og definisjoner for cyberdomenet ettersom det er de og sikkerhetsloven som er styrende for Forsvaret. Vi har spesifikt valgt innsidetrusselen for å forske på forståelsen og security-kulturen på et mer gjennomgående nivå i Marinen, som er en underavdeling i Sjøforsvaret. Lengden på masteroppgaven er noe større en veiledningen til masteroppgave UIS skisserer. Bakgrunnen for dette er at vi har funnet mange viktige funn ved Marinens security- kultur, som er viktig for oss å belyse overfor Marinens ledelse.

Når det gjelder teoretisk grunnlag fokuserer vi hovedsakelig på Reasons (1997) teori om sikkerhetskultur, og ser nærmere på hvordan vi kan utvikle en security-kultur ved å presentere Roers rammeverk for å bygge en security-kultur. På bakgrunn av valgte organisasjon presenterer vi HRO teori, og tar for oss karakteristikker/aspekter som resilient, mindfulness, usikkerhet og sensemaking. For relevant akademisk teori har vi valgt Klein (2011) og Boins (2015) bruk av teori opp imot komplekse og uforutsigbare situasjoner, som vil bidra til å kartlegge mulige tiltak for å forbedre security-kulturen.

Det empiriske arbeidet ble avgrenset til Marinen, med tre underliggende avdelinger og deres fartøygrupper. Det ble gjennomført totalt 41 intervjuer på tre nivåer i organisasjonen, i tillegg til at vi gjennomførte fem fagintervjuer hos organisasjoner utenfor Marinen, men med tilknytning til cyber, security eller kultur. Vi bruker det teoretiske rammeverket for å belyse resultatet fra datainnsamlingen ved å se på eksisterende kultur, herunder MTO-faktorene, og videre behov og muligheter for endring for å utvikle security-kulturen.

Med referanse til Retningslinjer for masteroppgaven i erfaringsbasert master i risikostyring og sikkerhetsledelse (2013) punkt 4.2 Omfang, er oppgaven vår noe lenger enn størrelsesorden på 80 sider. Funnene viste at Marinen i et security aspekt ikke oppfølger beskrivelsen av en HRO, og grunnlaget for sensemaking er ikke tilstede. I tillegg viste funnene graverende mangler i utdanning, opplæring og kompetanse på security som vi ønsker å belyse for organisasjonen. Vi anser valgte teoretiske rammeverk som nødvendig grunnlag for videre forskning på security-kultur. Vi ønsker å gi et mest mulig helhetlig og transparent bilde av funnene våre ved Marinens security- kultur, for at andre kan kontrollere, replisere og bygge videre på arbeidet som er gjort. Formålet med oppgaven var å se på hvordan security-kulturen i Marinen kunne forbedres, og vi valgte derfor et utvidet teoretiske rammeverket og utvalg av data.

1.4 Struktur og oppbygning av masteroppgaven

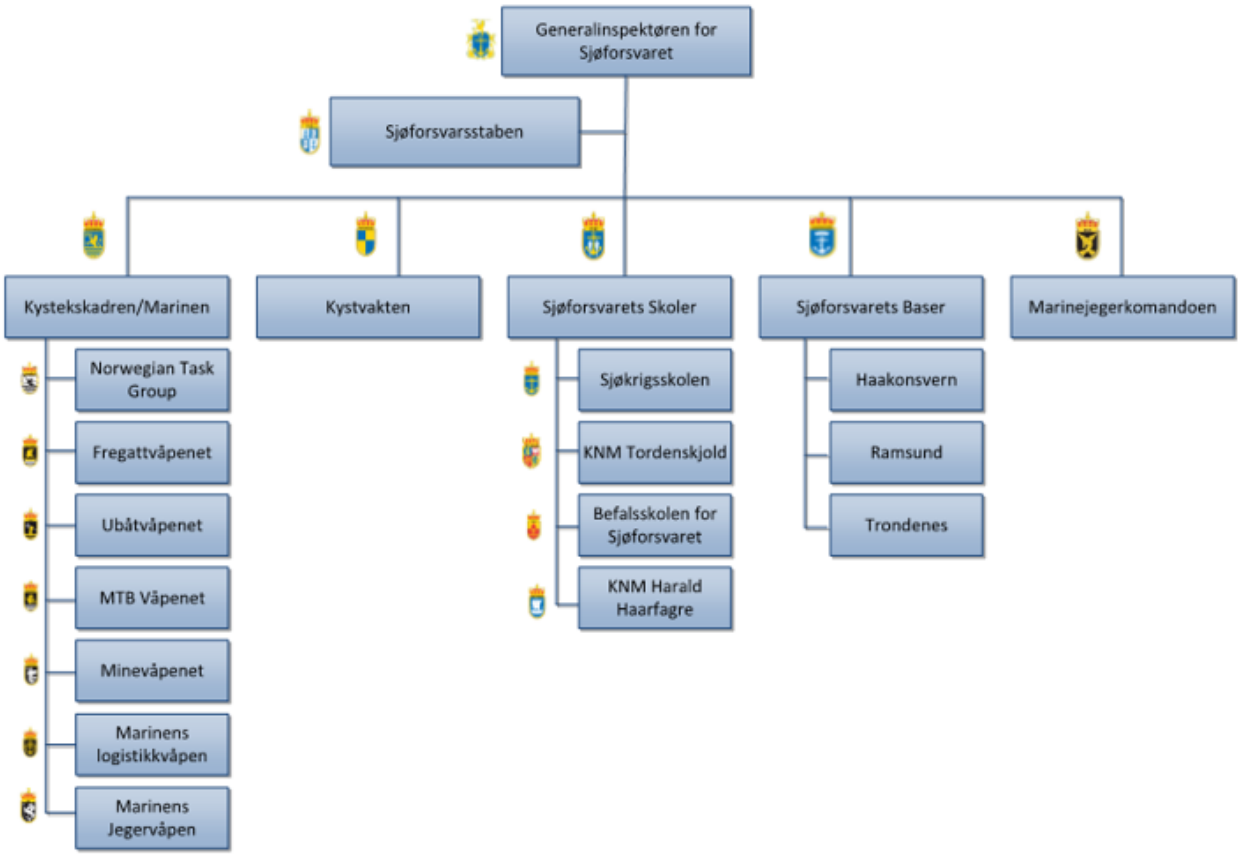
Tabell 1 skisserer og visualiserer oppbyggingen av masteroppgaven med kapittel og tilhørende fokusområde.

Kapittel	Fokusområde
1: Innledning	I innledningen vil bakgrunnen for oppgaven samt forskningsspørsmål og problemstilling synliggjøres. Videre settes avgrensningene på oppgaven.
2: Introduksjon av Sjøforsvaret og Kysteskadren/Marinen	Gjennom en innledning og figur 3 presenteres Sjøforsvarets organisasjon og sikkerhetsoppbygging.
3: Teoretisk grunnlag	Teoretisk grunnlag presenteres med fokus på terminologiforståelse, security-kultur, HRO og sensemaking.
4: Metode	Dette kapittelet viser hvilken metodisk tilnærming vi har benyttet gjennom å beskrive forskningsdesign, forskningsprosessen, utvalgsstrategi, intervjuguide, anonymitet og analyseprosessen. Videre tar vi for oss validitet, reliabilitet, etiske utfordringer og styrker/svakheter ved valgte metode.
5: Presentasjon av empiri	Empirikapittelet presenterer alt materialet som er samlet inn og analysert i fase 1. Her presenteres og fortolkes utvalgt data fra fire valgte hovedpilarer: I. Observatørrolle, kvalitativ, II. Intervjuer av typen semistrukturerte, åpne, III. Fag og IV. Rapporter.
6: Drøfting	Her drøftes de analyserte funnene presentert i empiridelen. Funnene sammenstilles med relevant teori som presenteres under tre kapitler inndelt eller forskningsspørsmålene. Trusselbildet og MTO-faktorene drøftes.
7: **Konklusjon**	Konklusjonen trekker frem hovedfunnene som besvarer problemstillingen og oppgavens forskningsspørsmål.
8: Referanser	En fremvisning av alle referanser benyttet i masteroppgaven.

Tabell 1: Oppgavens struktur og oppbygging

2. Introduksjon av Sjøforsvaret, herunder Kysteskadren/Marinen

Per dags dato (03.09.2016) består Forsvarets organisasjon av 15 driftsenheter med et vidt spekter av arbeidsoppgaver (Forsvaret, 2016a). Forsvaret er delt inn i fem nivåer hvor Forsvarssjefen med stab betegnes som nivå 1. Generalinspektøren for Sjøforsvaret med stab, betegnes som nivå 2, og er en av de 15 driftsenhetene. Under Sjøforsvaret er det etablert fire nivå 3- avdelinger: **Kysteskadren (KE - Marinen),** Kystvakten (KV), Sjøforsvarets skoler (SSK) og Sjøforsvarets baser (SB). Organisasjonskart mai 2016 fremgår i figur 3.



Figur 3: Organisasjonskart Sjøforsvaret, mai 2016 (Denk, Løberg 2015)

Kysteskadren (KE), heretter kalt Marinen, består av avdelinger/ våpen med hver sin våpensjef og tilhørende stab og treningssenter (Nivå 4). Avdelingene på nivå 4 består av et ulikt antall ansatte og antall seilende marinefartøy. Disse betegnes som nivå 5. I tillegg er det avdelinger med kystjegere, minedykkere og hurtiggående stridsbåter. Marinen teller i fredstid 1400 personer, inkludert vernepliktig personell (Forsvaret, 2016c).

Marinens primæroppgave er å stille maritime ressurser tilgjengelig for operative myndigheter i fred, krise og krig. Marinen har også ansvaret for styrkeproduksjonen av operative enheter i Sjøforsvaret, og skal sørge for at fartøyene og avdelingene er utstyrt med topp moderne utstyr og et trent og motivert personell (Forsvaret, 2016b).

Generalinspektøren i Sjøforsvaret (GIS) har delegert lokal koordinerende myndighet (LKM) for security til sjef Sjøforsvarets baser, herunder Haakonsvern sikkerhetsavdeling. På nivå 3, Marinen, er det en sikkerhetsleder i 100% stilling, mens det på nivå 4 og 5 skal være en avdelingssikkerhetsleder (ASL), en datasikkerhetsleder (DSL) og en Kryptosikkerhetsleder (KSL) i hver avdeling. Disse stillingene har rollen som ASL/DSL/KSL som en prosentandel av sin stilling.

Sjøforsvaret er i en omorganisering som trådte i kraft 1.august 2016 og organisasjons- og sikkerhetsstrukturen har blitt noe endret i forhold til figur 3. Noen av endringene er at Kysteskadren har endret navn til Marinen. Vi vil i denne masteroppgaven forholde oss til organisasjonen slik den var før 01.08.2016 da datainnsamlingen ble gjort. Vi vil derimot videre i masteroppgaven bruke navnet Marinen i stedet for Kysteskadren, da flere informanter og ledere også bruker Marinen. Vårt inntrykk er at ordet «*Marinen*» er mer kjent utenfor Sjøforsvaret og Forsvaret. Vi vil ikke navngi hvilke avdelinger i Marinen vi har valgt å gjennomføre datainnsamling i. Vi vil henvise til de tre avdelingene som avdeling 1, 2 og 3. Dette vil bli mer utdypet under punkt 4.3.5 anonymitet.

Sikkerhetsklarering og autorisasjon:

I henhold til sikkerhetsloven (1998) kapittel 6 Personellsikkerhet § 19, skal personer som skal gis tilgang til skjermingsverdig informasjon gradert konfidensielt eller høyere, autoriseres. Disse skal på forhånd sikkerhetsklareres. I henhold til § 21 vurderingsgrunnlag for sikkerhetsklarering; skal sikkerhetsklarering bare gis eller opprettholdes dersom det ikke foreligger rimelig tvil om vedkommendes sikkerhetsmessige skikkethet. Ved vurderingen av sikkerhetsmessig skikkethet skal det bare legges vekt på forhold som er relevante for å vurdere vedkommendes pålitelighet, lojalitet og sunne dømmekraft i forhold til behandling av skjermingsverdig informasjon. FSA utgir sikkerhetsklareringer mens det er lokal sjef sitt ansvar å autorisere personellet.

3. Teori

Cyberdomenet har, som nevnt, i senere tid fått et økt fokus både nasjonalt og internasjonalt. Det er innlemmet i lovverk, og ikke bare stater men også EU og NATO har utarbeidet strategier for informasjonssikkerhet. Hva betyr så cyberdomenet og trusselen for Sjøforsvaret? Hvordan bør cybertrusselen håndteres? Hvordan er man best i stand til å håndtere den i forhold til behov og forutsetninger som ligger til grunn? Hva slags kunnskap og forståelse er nødvendig for at Sjøforsvaret skal være i stand til å utnytte innehavende ressurser og kapasiteter for å håndtere trusselen? Vil en forbedret security-kultur bidra til Sjøforsvarets evne til å håndtere cybertrusselen? Spørsmålene nevnt ovenfor dannet grunnlaget for vårt valg av teori som vil være med på å svare på forskningsspørsmålene.

For å forstå hva som må til for å håndtere en cybertrussel har vi tatt utgangspunkt i de menneskelige, tekniske og organisatoriske (MTO) faktorene som er med på å forme Marinen. Først presenterer vi en terminologiforståelse som er med på å danne et felles utgangspunkt av begrepsbruk. En kort oppsummering av begreper som brukes gjennomgående i oppgaven er presentert innledningsvis på side VIII. Vi tar for oss Marinen og cybertrusselen hvor det ligger en del føringer fra nasjonalt nivå vi må forholde oss til.

Videre i kapittelet presenteres valgte teoretiske begrepsapparat og perspektiver som er utgangspunktet for drøftingen av det empiriske datamaterialet. Valgt teori utgjør et rammeverk og et verktøy for å belyse problemstillingen og forskningsspørsmål to og tre. Vi ønsker å se på hvordan en security-kultur kan utvikles for bedre å kunne håndtere innsidetrusselen. For å danne et bilde defineres først viktige begrep som risiko og risikoforståelse, sorte svane, sårbarhet, usikkerhet, safety, security, cyberdomenet og innsidetrussel. Vi beskriver hva som definerer en High Reliability Organization (HRO), ettersom elementene er med på å forme en security-kultur, og å gjøre Marinen i stand til effektiv utøvelse av militærmakt. Vi legger til grunn Reasons (1997) definisjon av en informert kultur som beskriver fire komponenter som er sentrale i å bygge kultur, i tillegg til Roer (2015) sin definisjon og rammeverk for å bygge en security-kultur. Vi fokuserer på security-kultur i et menneskelig, teknisk og organisatorisk (MTO) perspektiv, og nytter oss av utvalgte påstander fra Kleins bok *Streetlights and Shadows* (2011) sett i forhold til håndtering av tvetydige situasjoner (Shadows). Klein (2011) har tatt utgangspunkt i ti påstander tilpasset kontrollerte situasjoner (Streetlights), og videre forsket på prosesser i en verden av uklarheter (Shadows) for best mulig å tilpasse prinsippene til realiteten. Videre beskrives sensemaking av både Klein (2011) og Boin (2015) som et grunnleggende

perspektiv for å håndtere komplekse og uforutsigbare situasjoner, og vil i oppgaven knyttes til å se på hvordan security-kulturen kan forbedres.

3.1 Terminologiforståelse

Risiko og risikoforståelse

Risiko som begrep blir i det daglige ofte brukt i mange ulike sammenhenger, ulike fagområder og tradisjoner og ofte med forskjellige betydninger. Forståelsen av at det ikke bare er en måte å tenke på, har stor betydning når ulike fagområder skal samarbeide om problemstillinger vedrørende risiko (Aven et al., 2009 s.37).

Det opprinnelige begrepet risiko kommer fra det italienske ordet «*risicare*» og betyr å våge. Alt en gjør, både i privatlivet (for eksempel kjøre bil) eller aktivitet i jobbsammenheng, innebærer en eller annen form for risiko. Terje Aven et al. (2009 s.41) sin definisjon på risiko, beskrevet i boken *Risikostyring,* er denne:

«Risiko er en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet»

Når vi skal vurdere om det vil inntreffe uønskede hendelser det neste året, har vi en usikkerhet. En kan ikke med hundre prosent sikkerhet si at det ikke vil forekomme alvorlige hendelser i fremtiden. Det er denne usikkerheten som Aven (2009) innlemmer i risikobegrepet.

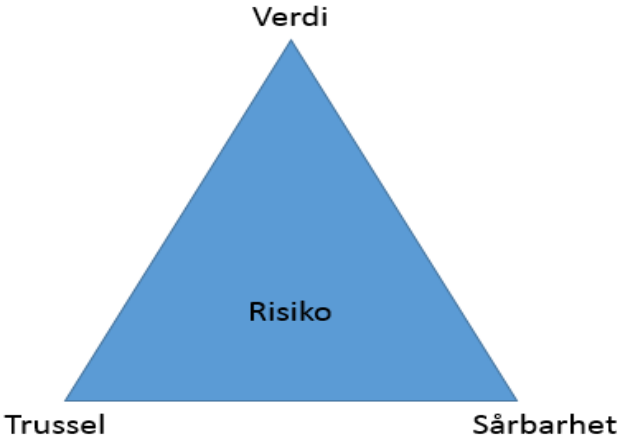
En annen definisjon på risiko er beskrevet i «Direktiv- krav til sikkerhetsstyring i Forsvaret» (2010) som:

«*Et uttrykk for kombinasjonen av sannsynlighet for og konsekvensen av en uønsket hendelse»*

Nasjonal sikkerhetsmyndighet (NSM, 2015a s.10) sier; «*For å vurdere risiko må det gjennomføres verdi-, trussel- og sårhetsvurderinger*». De definerer risiko som:

«Forholdet mellom faktorene verdier, trusler og sårbarheter.

Dette forholdet er ofte omtalt som risikotrekanten:



Figur 4: Risikotrekant- arealet i trekanten er et uttrykk for risiko (NSM, 2015a s.10)

Usikkerheter er et kjennetegn med tilsiktede uønskede hendelser der vi ikke kan si hvor, når og med hvilke metoder en trusselaktør slår til (NSM, 2015a s.10). Usikkerhet forstår vi som mangel av kunnskap om ukjente størrelser (Flage et al., 2009). Verdi defineres som en ressurs som hvis den blir utsatt for en uønsket påvirkning vil medføre en negativ konsekvens for den som forvalter eller drar fordel av ressursen (NSM, 2014). Med en trussel forstås ethvert forhold eller enhver enhet med et potensial til å forårsake en uønsket hendelse (NOU 2000:24). Et trusselbilde er en tidsavgrenset beskrivelse av identifiserte trusler mot en bestemt entitet (Norsk Olje og gass, 2003).

Vi ønsker å kombinere Aven et al. (2009) og NSM (2015a) sin definisjon av risiko, og sette dette i et security-perspektiv. Aven et al. (2009 s.42) sier at definisjon uten sannsynlighet, også har mening uten at usikkerhet kvantifiseres eller uttrykkes ved hjelp av sannsynligheter. Det er en risiko til stede, uavhengig av om en har uttrykt usikkerhetene ved hjelp av sannsynlighet (Aven et al., 2009 s.42). På bakgrunn av dette har vi ikke tatt med sannsynlighet i vår definisjon, slik «Direktiv- krav til sikkerhetsstyring i Forsvaret» (2010) har gjort. Vi bør ikke kun ta høyde for historiske data i vurderingen av hva vi kan møte av trusler og tilsiktede hendelser. Flere forfattere som Tablet (2010) og Aven (2014b) påpeker at fremtiden preges av stor usikkerhet og at man derfor ikke må legge for stor vekt på historiske data (ref punkt 3.1.2 Sorte svane). Vi har valgt å definere risiko i vår oppgave som:

«Mulige konsekvenser ved tilsiktet uønsket hendelser med tilhørende usikkerhet. Disse uønskede hendelsene kan være i forhold til trusler mot verdier, og hvordan konsekvensene blir er avhengig av sårbarhetsgraden og kapasiteten til å møte truslene».

Et relevant begrep til risiko er sikkerhet. Risiko handler om fremtiden (Aven et al., 2013 s. 37), mens begrepet sikkerhet ofte brukes om forebyggende tiltak med hensikt å redusere sannsynligheten for at noe skal skje, eller redusere konsekvensene av uønskede hendelser (Aven et al., 2013). Når nivået av risiko er lavt, er nivået av sikkerhet antatt å være høyt, og omvendt (Antonsen, 2009).

Risiko er «*noens risiko*». Risikopersepsjon er hvordan en opplever risiko og handler om hvordan mennesker flest forstår, opplever og håndterer risiko og farer (Aven et. al 2013). Douglas og Wildavsky (1982) mener at risiko er sosialt betinget og vil bli påvirket av sosiale prosesser og kulturelle mønstre. Som en konsekvens av dette vil oppfattelsen av risiko variere, og dermed også evalueringen og håndteringen av den (Antonsen, 2009).

Ved risikoanalyser samles informasjon og kunnskap på eksempel et anlegg eller et system som det gjennomføres en vurdering på. Likevel er dette en vurdering sett gjennom øynene til de som gjennomfører en slik risikoanalyse, andre kan vurdere usikkerheten annerledes. Det er ikke alltid like opplagt hva en velger å fokusere på. Risiko avhenger derfor av hvem som vurderer og hva som vurderes (Aven et al., 2009).

Selv om ekspertene beviser at noe er mindre risikofylt, kan mennesker allikevel se dette annerledes. Forskning sier at mennesker flest betrakter det som langt farligere å fly enn å kjøre bil, selv om dette ikke er i overensstemmelse med ekspertenes risikovurderinger. Når beslutningstakere på samfunns- og organisasjonsnivå skal forsøke å redusere risiko gjennom styring, bør de derfor også ta inn i vurderingene hvordan mennesker sosialt og kulturelt skaper sin egen risikoforståelse (Aven et al., 2013).

I styring av risiko og sikkerhet er det viktig å fokusere på tekniske og organisatoriske forhold, individuelle og mellommenneskelige relasjoner og forholdet mellom ansatte og ledelse. Alt henger sammen og vi kan alle påvirke og være med å styre sikkerheten gjennom våre handlinger og de valg vi gjør (Aven et al., 2013). En gjengs oppfatning er at uønskede hendelser ikke bare skjer, de forårsakes. Sikkerhet innebærer en form av handling og viser til våre evne til å eliminere faren (Antonsen, 2009).

Sorte svane (Black Swans)

Innen risikofaget er ikke uønskede hendelser noe nytt, men konseptet med sorte svaner og unknown- unknowns er tatt mye i bruk de siste årene. Sorte svaner er en metafor som er relativt forståelig, samtidig som den er utfyllende og beskriver en del hendelser på en god måte.

Det var den italienske poeten, Juvenal, som på 1600 tallet tok i bruk begrepet sorte svaner. Tidligere var det kun observert hvite svaner og det skulle ikke mer til enn én sort svane for å endre troen på at det bare eksisterte hvite svaner (Aven, 2014a). I samme tidsepoke ble den første sorte svane observert på Swan River i Australia av en nederlandsk oppdager ved navnet Wilem de Valmingh. En kunne ikke lenger karakterisere sorte svaner som umulige. Etter dette endret begrepet sorte svaner seg fra å være noe veldig sjeldent, til å bli mer umulig, men som seinere viste seg å eksistere og være sant (Aven, 2014a). Sorte svaner er derfor blitt en metafor på den feilaktige antakelsen at hvis man ikke har kunnskap om noe eller hvis man ikke vet, så eksisterer det ikke (Aven, 2014a).

Flere forfattere, deriblant Tablet (2010) og Aven (2014b), skriver om sjeldne hendelser som en ikke kan forutse. Fremtiden preges av stor usikkerhet og de mener derfor at en ikke må legge for stor vekt på historisk data. Videre uttrykker de at risiko ikke bør baseres på det man ser, men det man ikke ser, da det er der man finner de sorte svanene. Aven (2014b) og Tablet (2010) mener begge at usikkerhet er det motsatte av kunnskap og at usikkerhetsfaktorene befinner seg der de sorte svanene er. Aven (2014a s.84) referer til sorte svaner som «*en overraskende, ekstrem hendelse sett i forhold til ens kunnskap og tro*». Sorte svaner hendelser kan deles inn i tre hovedkategorier (Aven, 2014a):

- **Ukjente- ukjente** (Unknown- unknowns) er helt ukjente hendelser for det vitenskapelige miljøet. Disse hendelsene er utenkelige og uforutsigbare og bærer ekstreme konsekvenser når de oppstår. Eksempel en ny type virus.
- **Ukjente- kjente** (Unknown- known): er farer som er ukjent for mange, men kjent for noen. Slike hendelser er ikke identifisert i de aktuelle risikovurderinger, enten fordi en ikke har gjort grundige og tilstrekkelige vurdering eller fordi man ikke kjenner til de. På den ene siden er hendelsen som oppstår ikke forutsett, mens den på den andre siden kan være kjent av andre individer, grupper eller samfunn. Eksempel er angrepet på Twin Towers 11 september 2001.
- **Kjente hendelser** (Known events) er hendelser som er kartlagt i en risikoanalyse, men er blitt vurdert til å ha en ubetydelig sannsynlighet for å forekomme og dermed ikke antas å forekomme. Selv om disse vurderingene for forekomst er satt til ubetydelige kan hendelsen allikevel oppstå med ekstreme konsekvenser.

Det betyr ikke nødvendigvis at alle sorte svaner hendelser og situasjoner er knyttet til og resulterer i store eller ekstreme konsekvenser. Hendelser og situasjoner som ikke resulterer i store konsekvenser er kjent som «*nesten- sorte svaner*». Aven (2014a s.123) skriver at

«nesten-sorte svaner» betyr «*overraskelser i forhold til ens kunnskap og tro, men der hendelsen ikke førte til ekstreme konsekvenser; barrierer virket og vi unngikk de ekstreme utfallene*».

Sårbarhet

Sårbarhet er kombinasjonen av mulige konsekvenser og tilhørende usikkerhet, gitt en initierende hendelse. Dette uttrykkes blant annet ved at sannsynlighet for at en ønsket funksjon, ikke ivaretas, gitt en initierende hendelse (Aven et al., 2008).

Sårbarhetsbegrepet definert av sårbarhetsutvalget:

«*Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet*» (NOU, 2015:13 s31).

Sårbarhetene som gjør oss utsatt for angrep er enten menneskelige, teknologiske, eller organisatoriske og sårbarhetsvurderinger må gjennomføres sammen med verdivurdering og trusselvurdering for å kunne vurdere risiko (NSM, 2015a s.15).

Usikkerhet

Det forekommer aldri en situasjon uten risiko, og det vil alltid foreligge en viss usikkerhet for hva konsekvensene kan bli. Risiko uttrykker faren som uønskede hendelser representerer, og usikkerhet er knyttet til manglende kunnskap og viten (Aven, 2008b). Usikkerhet som skyldes mangel på nødvendig kunnskap kan reduseres ved å skaffe mer viten i form av nærmere undersøkelser, få frem sentrale avgjørelser eller dele problemet opp i mer håndterbare størrelser (Austeng et al., 2005). Risiko- og sårbarhetsanalyser gjør oss i stand til å måle størrelsen på truslene et system utsettes for, og evnen til å møte truslene, og er redskaper for å si noe om usikkerhet (Aven et al., 2013 s.98). MTO-faktorene vil kunne svikte og gjøre ulike feil, og vi kan ikke forutsi med rimelig sikkerhet hva som vil skje.

Aven et al. (2013) viser til Rasmussens (1982) kognitive adferdsmodell hvor opplæring må balanseres på en måte som gjør det mulig for personell å analysere situasjonen (kunnskapsbasert nivå) og å reagere raskt og automatisk (ferdighetsbasert nivå), gjerne på bakgrunn av et sett av regler (regelbasert nivå). Dette innebærer at aktøren ikke foretar en eksplisitt vurdering av risiko og usikkerhet. Det er nødvendig med vurderinger av risiko og usikkerhet for å utvikle regelen og ferdigheten, men når de er etablert erstatter de slike vurderinger. Det foreligger også liten konsensus for hvordan å tolke og presentere usikkerhet, på lik linje som for risiko.

Store Norske Leksikons definisjon av usikkerhet i en risikokontekst forstås som det å ikke vite sann verdi av en størrelse eller fremtidige konsekvenser av en aktivitet. Vi snakker også om en usikkerhet som følge av å ha ufullstendig eller upresis informasjon eller kunnskap om en hypotese, en størrelse eller opptreden av en hendelse. Lipshitz (1993) definerer usikkerhet som en følelse av tvil som blokkerer eller forsinker handlinger.

Lipshitz og Strauss (1997) gjennomførte en analyse for å se på hvordan ledere håndterer usikkerhet. De identifiserte usikkerhetsmomenter som manglende forståelse, udifferensierte alternativer, og manglende informasjon. Resultatene samsvarer med påstanden om at beslutningstaking er drevet av situasjonsvurderinger (Lipshitz, 1993; March, 1981). De identifiserte også fem vide strategier for å håndtere usikkerhet; redusering, forhindre/vanskeliggjøre, resonnement basert på antagelser, veie argumenter for og imot, og undertrykkelse. Lederne brukte forskjellige strategier for å håndtere de forskjellige usikkerhetene; manglende forståelse – redusering, manglende informasjon – resonnement basert på antagelser, konflikt mellom valgmuligheter/alternativer – veie argumenter for og imot, forhindre – reservestrategi ved alle former for usikkerhet, undertrykkelse – minst sannsynlig brukt ved alle former.

Safety og security

Vi tar for oss generelle definisjoner av begrepene for så å se på lovens definisjoner, og videre hva Forsvaret og statlige organer bruker (tabell 2). Når dette sees i sammenheng med forskjellige direktiver og hva som blir brukt i praksis, skaper variasjonen i begrepsdefinisjoner og bruk stor forvirring. Til slutt oppsummerer vi med hvilke definisjoner vi velger å bruke videre i oppgaven.

Kilde	Begrep	Definisjoner
Oxford dictionary	Safety	Som tilstanden av å være beskyttet fra eller ikke i stand til å påføre fare, risiko eller skade.
	Security	Som ideer, adferd, holdninger til mennesker eller en gruppe som hjelper dem til å være fri fra trusler og fare.
Bartnes et al. 2006	Safety	Omhandler utilsiktede hendelser i forbindelser med andre farer og feil.
	Security	Bevisste, ondsinnede handlinger eller hendelser knyttet til trusler og hendelser.
Sikkerhetsloven 1998	Forebyggende sikkerhetstjeneste	Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.
NSM 2006	Sikkerhet (security)	Som tilstand av fravær av uønskede hendelser, frykt eller fare.
	Security-kultur	Er summen av de ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.
Sjøforsvarets sikkerhetshåndbok 2016	Sikkerhet (Safety)	Som evnen til å unngå skade på eller tap av mennesker, ytre miljø og materiell på grunn av akutte, utilsiktede hendelser (ulykker, uhell) eller kriminelle handlinger
	Operativ sikkerhet	Menes at man gjennom god risikohåndtering skal optimalisere yteevne og slagkraft. Man skal altså lykkes i oppdragsløsning fordi man mestrer å håndtere risiko.
	Forebyggende sikkerhetstjeneste	Som planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.
Direktiv-Krav til sikkerhetsstyring i Forsvaret 2010	Sikkerhet	Som fravær av forhold som kan føre til uønskede hendelser.
	Operativ sikkerhet	Er i denne sammenhengen alt systematisk arbeid med sikkerhets- og risikoforhold for å optimalisere yteevne og slagkraft, og derved redusere risiko for tap og uønskede hendelser i militære operasjoner og aktiviteter.
	Forebyggende sikkerhetstjeneste	Som planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet.
Forsvarets fellesoperative doktrine 2014	Styrkebeskyttelse	Deles inn i de fire følgende koordineringsområdene; Forebyggende sikkerhet, aktive tiltak, passive tiltak og skadereperasjon/skadebehandling.
	Forebyggende sikkerhet	Til å omfatte alle fysiske, prosedyremessige og tekniske systemer og tiltak for å vedlikeholde sikkerheten og redusere mulighetene for angrep på personell, informasjonssystemer, materiell og installasjoner.
Kai Roer 2015	Security-kultur	Ideene, holdninger og sosial adferd til spesifikke mennesker eller grupper som hjelper dem til å være fri fra trussel og fare.

Tabell 2: Terminologi forståelse

NSM bruker sikkerhet i betydningen security. Forsvarets definisjon av sikkerhet omhandler både safety, beskrevet under operativ sikkerhet, og security, beskrevet som forebyggende sikkerhetstjeneste. En ting som kan skape forvirring er at NSM bruker både begrepet sikkerhet og forebyggende sikkerhet, men kun i betydningen security. Forsvaret omtaler forebyggende sikkerhet som et delelement i styrkebeskyttelse hvor det beskriver fysisk

sikring av installasjoner, personellsikkerhet, operasjonssikkerhet og informasjonssikkerhet, miljøsikkerhet, trafikksikkerhet og helsemessige preventive tiltak. Forsvarets fellesoperative doktrine (2014) definerer operasjonssikkerhet som den systematiske beskyttelsen av egne operasjoner gjennom aktive og passive tiltak, i den hensikt å frata motstandere muligheten til å oppnå uventede fordeler.

På grunn av uklarheter i direktivene velger vi i oppgaven å nytte oss av begrepet security definert slik sikkerhetsloven definerer forebyggende sikkerhetstjeneste; *«Planlegging, tilrettelegging, gjennomføring og kontroll av forebyggende sikkerhetstiltak som søker å fjerne eller redusere risiko som følge av sikkerhetstruende virksomhet»*. Gjennom egen erfaring fra Forsvaret og intervjuene i forbindelse med oppgaven opplever vi variert begrepsbruk som grunnlag for misforståelser for hva man egentlig snakker om. Security fremkommer som begrepet med størst felles forståelse blant ansatte i Marinen.

Cyberdomenet

Cyberdomenet ble første gang i Norge beskrevet som det femte krigføringsdomenet i langtidsplanen «Et forsvar for vår tid» (2013-2016). Cyberdomenet er et uavhengig nettverk av informasjonsteknologi infrastruktur, og inkluderer internett, telekommunikasjonsnettverk, datasystemer og innebygde prosessorer og kontrollere i kritisk industri (egen oversettelse, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011).

Etterretningsdoktrinen (2013 s.15) definerer cyberdomenet slik: [Cyberdomenet] *består av fysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, medier og data.*

Det blir ofte benyttet ulike begreper om det digitale sikkerhetsarbeidet, blant annet IKT-sikkerhet, informasjonssikkerhet og cybersikkerhet. I de siste årene i Norge er begrepene brukt mye om hverandre. Informasjonssikkerhet blir brukt i den nasjonale strategien utgitt i 2012. I kongelige resolusjon av 2013 er begrepet IKT- sikkerhet benyttet, mens cybersikkerhet blir benyttet i Forsvarsdepartementets cyberretningslinjer fra 2014 (NOU, 2015:13 s.34).

Internasjonalt brukes ofte cybersikkerhet, der cyber henviser til alt cyberdomenet består av: «*datasystemer og kommunikasjonsinfrastruktur, i tillegg til informasjonen som lagres og overføres. Cybersikkerhet handler derfor om å beskytte «alt» som er sårbart fordi det er koblet til, eller på andre måter er avhengig av informasjon- og kommunikasjonsteknologi».*

Sårbarhetsutvalget legger også til grunn at IKT- sikkerhet er synonymt med cybersikkerhet. (NOU, 2015:13 s.34).

Vi vil i denne masteroppgaven benytte oss av cybersikkerhet da dette begrepet er i bruk i Forsvaret. Forsvarsdepartementet benytter begrepet i sine cyberretningslinjer noe som har bidratt til forankring nedover i organisasjonen.

Innsidetrussel

Norsk sjømakt beskytter, ivaretar og fremmer norske interesser i Nordområdene blant annet gjennom å håndheve norsk jurisdiksjon og suverenitet og avskrekke potensielle motparter fra bruk av militærmakt (Børresen og Helseth, 2011:13-15). Teknologien, som i fremtiden vil bli brukt på å ivareta disse interessene, kan en sofistikert motpart søke å manipulere gjennom cyberdomenet. Opprettelsen av CYFOR, NSM, NorCERT og flere sektorvise sentre skal bidra til å håndtere cyberhendelser og angrep, men også militære ledere må forstå hva cyberdomenet er, og ikke minst erkjenne at den raskt voksende trusselen mot våre datasystemer er en av de alvorligste trusler mot vår nasjonale sikkerhet i årene fremover (Generalmajor Roar Sundseth, Sjef Cyberforsvaret, foredrag Oslo Militære Samfunn mandag 18. februar 2013). Generalmajor Sundseth påpekte også at hele Forsvarets organisasjon, ned til den enkelte ansatte, må flette dette perspektivet inn i sin daglige aktivitet og virke, ellers kan konsekvensene bli store. CYFOR skal være i stand til å håndtere truslene når og hvor de måtte oppstå i Forsvarets systemer, men Sundseth understreker at det fortsatt er den enkelte ansatte i Forsvarets som er førstelinjes forsvar mot både de sivile og militære truslene som eksisterer der ute. NSM og FSA uttaler seg om den enkelte forsvarsansatte sitt ansvar og behovet for kartlegging av mulige tiltak på lavere nivå. Vi valgte å fokusere på innsidetrusselen ettersom den bør og kan håndteres på et gjennomgående nivå i organisasjonen.

Searchseurity.techtarget.com definerer en innsidetrussel som en ondsinnet hacker, som kan være en ansatt eller leder av en bedrift, institusjon eller byrå. Begrepet kan også omfatte en fra utsiden som utgir seg for å være en ansatt eller leder ved å skaffe seg falsk legitimasjon, og så utfører handlinger ment å skade bedriften (egen oversettelse).

Den amerikanske CERTen definerer innsidetrussel generelt som en nåværende eller tidligere ansatt, kontraktør, eller annen virksomhetspartner som har eller hadde autorisert tilgang til en organisasjons nettverk, system eller data og har med intensjon misbrukt tilgangen til negativt å påvirke konfidensialiteten, integriteten og tilgjengeligheten til organisasjonens informasjon

eller informasjonssystem. Innsidere handler ikke alltid alene, og er ikke nødvendigvis klar over at de hjelper en trusselaktør, det vil si utilsiktet innsidetrussel (egen oversettelse).

NSM er vårt statlige organ, underlagt FD, med ansvaret for forebyggende sikkerhet (security) i både militær og sivil sektor i henhold til sikkerhetsloven. NSM støtter Sjøforsvaret blant annet ved brifer og informasjon om cybertrussel, og vi velger videre i oppgaven å bruke deres definisjon av innsidetrussel. Ved innsiderisiko menes «*faren for at tilsiktede uønskede handlinger skal kunne utføres som følger av plassering eller utnyttelse av personell med adgang til en virksomhet, systemer, informasjon eller prosesser*». Innsidere vil kunne ha et stort spekter av angrepsmål for å tjene målsettingene til den opprinnelige oppdragsgiveren. Dette ved å tilstrebe å komme i posisjoner hvor en kan påvirke beslutninger, innhente sensitiv informasjon, gi feilaktig informasjon eller skape ødeleggelser og skader (NSM, 2015a s.16).

Det kan være mange aktører som står bak forsøk på å utnytte mulighetene for en innsider. Det kan, som tidligere nevnt, blant annet være andre staters etterretnings- og sikkerhetstjenester. Innsidetrusselen i norske virksomheter, både i Norge og i utlandet, er i henhold til NSM høyst reell (NSM, 2015b s.5). PST skriver i sin trusselvurdering for 2015 at det har vært hendelser hvor PST-ansatte har blitt forsøkt rekruttert av utenlandske etterretningstjenester og flere personer prøvd å få seg arbeid i den norske sikkerhetstjenesten (NSM, 2015a s.17). Innsidere kan deles inn i følgende tre kategorier (NSM, 2015a s.17):

- **Infiltratøren:** Vedkommende arbeider i utgangspunktet for en trusselaktør og blir forsøkt innplassert i et ansettelses- eller tilknytningsforhold for å utøve eller bistå i utøvelsen av tilsiktede uønskede hendelser.
- **Den vervede:** Vedkommende står i utgangspunktet i et ansettelses- eller tilknytningsforhold, men av forskjellige grunner, frivillig eller etter manipulering, påvirkning eller press, lar vedkommende seg overtale til å utøve eller bistå i utøvelsen av tilsiktede uønskede hendelser, eller av egen fri vilje endrer den lojalitet og utøver eller bistår i utøvelsen av slike hendelser.
- **Den utnyttede**: Vedkommende har manglende kunnskap og sikkerhetsbevissthet eller generelt manglende dømmekraft, og av den grunn indirekte bidrar den til at en trusselaktør kan utøve tilsiktede uønskede hendelser.

Ved å kartlegge kompetanse og forståelse om innsidetrussel i Marinen vil vi også få et innblikk i security-kulturen. Ved å relatere den nåværende situasjon i Marinen til teori om sikkerhetskultur og security-kultur vil vi forsøke å besvare oppgavens forskningsspørsmål.

3.2 Security-kultur

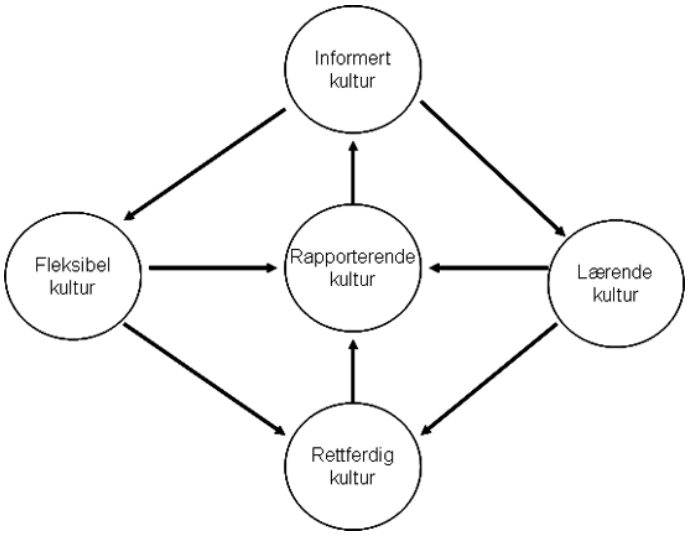
Forsvaret bruker ordet sikkerhetskultur i deres sikkerhetspolicy og direktiv - krav til sikkerhetsstyring (2010), hvor de blant annet referer til Reason (1997) sine fire delkomponenter. De enkelte avdelinger arver dette og bruker det i avdelingenes spesifikke instrukser. Det fremkommer ingen definisjon av begrepet sikkerhetskultur, og security-kultur blir ikke brukt. Vi har tatt utgangspunkt i NSMs (2006) definisjon av sikkerhetskultur (security-kultur) (tabell 2) sett opp imot definisjoner av kultur og security, og formulerte følgende definisjon som brukes i oppgaven:

«Produktet av verdier, holdninger, kompetanse, normer og regler som kommer til uttrykk gjennom organisasjonens totale security-adferd for å redusere risiko som følge av sikkerhetstruende virksomhet».

I litteraturgjennomgangen ser vi at security-kultur fortsatt fremstår som et relativt nytt begrep uten en entydig definisjon og har i liten grad vært forsket på i motsetning til safety-kultur (Malcolmson, 2009). Reasons (1997) beskrivelse av en god sikkerhetskultur er sett i lys av safety, vi mener derimot at denne teorien også er gjeldene for å bygge en god security-kultur. I tillegg ser vi på Roers teori som fokuserer kun på security-kultur.

3.2.1 God sikkerhetskultur

Guldemund (2000) definerer sikkerhetskultur som de aspektene av organisasjonskulturen som påvirker holdninger og adferd relatert til en økning eller senkning av risiko. Videre beskrives Reasons (1997) sitt perspektiv, hvor en god sikkerhetskultur innbefatter fire delkomponenter; rapporterende kultur, rettferdig kultur, fleksibel kultur og lærende kultur. Disse omtaler Reason samlet som en informert kultur (Reason, 1997 s.196) (figur 5).



Figur 5: Komponentene i informert kultur Reason (1997)

En informert kultur har kunnskap om alle faktorer som har betydning for sikkerheten og bruker denne proaktivt ved å finne tiltak for å forhindre uønskede hendelser i fremtiden. Organisasjonen søker informasjon om både menneskelige, teknologiske og organisatoriske faktorer som kan ha en betydning på sikkerheten. Det handler om å opprette et sikkerhetsinformasjonssystem hvor en får inn, analyserer og formidler informasjon om uønskede hendelser, og videre at det gjennomføres proaktiv kontroll av tilstanden i organisasjonen. Ledelsen gjennomfører revisjoner og justeringer av blant annet prosedyrer og arbeidspraksis for å ivareta sikkerheten på en best mulig måte for organisasjonen. Målet med dette er at både ledere og de ansatte har den siste gyldige kunnskapen om tekniske, organisatoriske, menneskelige og miljømessige faktorer som i sin helhet kan virke inn på sikkerheten i et system. (Reason, 1997).

En rapporterende kultur motiverer personellet til å rapportere feil og hendelser. Velvillig deltagelse fra de ansatte er meget viktig i et sikkerhetsinformasjonssystem, og for å oppnå dette er det nødvendig å utvikle en rapporterende kultur. Dette fordrer at de ansatte er villige til å rapportere feil, hendelser og avvik (Reason, 1997). I følge Reason (1997) er det ledelsens ansvar å legge til rette for en rapporterende kultur. Det kan være en utfordrende oppgave å få personell i en organisasjon til å rapportere hendelser, spesielt når det kommer til å rapportere egne feil. Menneskets reaksjon på å gjøre feil kan variere, og ærlige tilståelser kommer ikke alltid øverst på listen. Det kan være flere årsaker til dette; «er det verd det ekstra arbeidet det tar å skrive en rapport når en ikke er sikker på utfallet?» Selv om en organisasjons ledelse oppfordrer til rapportering, kan det være at personellet har en mistillit til ledelsen og ikke stoler på dem. Videre kan frykten for represalier hindre rapportering. «Vil jeg få min kollega i problemer? Vil jeg selv havne i problemer?» Fokuset må dermed være på å avdekke hendelser som kan bidra til å fremme et trygt og sikkerhet arbeidsmiljø, og ikke ha et fokus på straff og skyld (Reason, 1997).

Reason (1997 s.197) sier i sin bok at det er fem faktorer som er viktig ved en rapporterende kultur. Dette er både faktorer som omhandler det å skape en sikkerhetskultur og klima med tillit, men også faktorer som innbefatter det å motivere personell til å rapportere uønskede hendelser. Disse faktorene er: **1:** Personellet er sikret mot disiplinære reaksjoner, så langt det lar seg gjøre. **2:** At det er konfidensialitet ved rapportering. **3:** At en skiller enheter som samler inn, analyserer og rapporterer, og de enheter som sanksjonerer. **4:** At tilbakemeldingene er raske, nyttige, tilgjengelige samt forståelige for de rapporterende. **5:** At det er lett å lage rapporter på uønskede hendelser.

Med organisatorisk fleksibilitet menes det å inneha en kultur som er i stand til å tilpasse seg effektivt de endringer som kreves. Dette innbefatter også akutte hendelser.
En fleksibel kultur går fra byråkrati til kollegial autoritet, og formell rang har mindre betydning. Den med best kompetanse for oppgaven avgjør handlingen når dette er nødvendig. Sikkerhet skapes gjennom kommunikasjon og en finner løsninger ved å gjennomføre samtale i grupper, en form for profesjonalisering av teamsamarbeid.

Iverksetting av tiltak for å unngå tidligere feil forutsetter ofte nye krav til personellet, materiellet og organiseringen. Evnen til å raskt kunne implementere tiltak krever en fleksibilitet hos organisasjonen men også hos den enkelte medarbeider (Stikholmen, 2012). Effektive team, kapable til å operere autonomt når situasjonen krever det, trenger også høyt kvalifiserte ledere. Dette krever også at organisasjonen investerer mye i kvalitet, motivasjon og erfaring hos sine ledere i førstelinje (Reason, 1997).

Av alle «subkulturer» er en lærende kultur mest sannsynlig det letteste å skape, men det vanskeligste å få til å virke. En lærende kultur omhandler informasjonshåndtering gjennom observasjoner (følge med og legge merke til), refleksjon (analysere og tolke), å skape (planlegge, designe) og handling (implementere, gjennomføre og teste). I henhold til Reason (1997) er de tre første ikke så vanskelig, men det er handling som mest sannsynlig kan skape utfordringer for en organisasjon. Det er organisasjonens kompetanse og vilje til å trekke de riktige konklusjoner på hendelser som er rapportert i et sikkerhetsinformasjonssystem som også bidrar til en lærende kultur. Det handler om å ha et kritisk syn på eksisterende praksis og vilje til å implementere endringer, tiltak eller reformer som kan være nødvendig med bakgrunn i sikkerhetsinformasjonssystemet (Reason, 1997).

Det bør være stor takhøyde i en lærende organisasjon, og dette forutsetter en kultur hvor det er «lov å gjøre feil», og der det er en åpenhet og et reaksjonsmønster som gir operativt personell trygghet til å rapportere egne feil (Tinmannsvik, 2008). Samtidig kan det være avvik som får så alvorlige konsekvenser at en arbeidsgiver må gripe inn med disiplinære tiltak. Dette kan være utfordrende: Hvor går grensen mellom avvik vi kan lære noe av, og de avvik som krever en disiplinær reaksjon? (Reason, 1997).

En helt rettferdig kultur mener Reason (1997) er nesten et uoppnåelig ideal. En forutsetning for å skape en rettferdig kultur et at det er enighet i organisasjonen hvor linjen mellom akseptable og uakseptable handlinger er satt. Det vil på ene siden være uakseptabelt å straffe alle feilhandlinger som blir gjort uavhengig av deres opprinnelse og omstendigheter, mens

det på den andre siden bør være uakseptabelt å gi full «immunitet» fra straff på alle handlinger som kunne ha /har bidratt til uønskede hendelser. Det må legges til rette for en atmosfære der de ansatte blir oppmuntret til å dele viktig sikkerhetsrelatert informasjon uten at dette kan ende med sanksjoner. Dette vil kunne bidra til at personellet sier ifra om farlige aktiviteter gjennom rapportering. (Reason, 1997).

Organisasjoner som har en positiv sikkerhetskultur er kjennetegnet ved «*en kommunikasjon bygget på gjensidig tillit, felles oppfatning om betydningen av sikkerhet og med tiltro til at organisasjonens sikkerhetsmål fungerer effektivt*» (Reason, 1997 s.194). Reason (1997) snakker videre om at sikkerhetskulturen handler om den kollektive forståelsen av hva som er farlig, hvordan en klarer å redusere farene, og at dette ofte blir spørsmål om en prioritering både på tid og økonomi.

3.2.2 Hvordan å bygge en security-kultur

Kai Roer (2015) utviklet «The Security Culture Framework» gjennom å ha sett security bevisstgjørings/bevissthets (awareness) treningsprogrammer i en årrekke bli gjennomført uten kontroll, mulighet for måling eller nødvendig planlegging. Roers (2015) konsept er et holistisk rammeverk som skal bidra til å bygge og opprettholde en security-kultur.

Definisjoner, byggesteiner, påvirkning og security bevissthet (awareness) er elementer som er nødvendig for å endre kultur og adferd. Vi må vite hvem som bygger kultur. Interaksjon påvirker muligheten for forbedring av security-kultur. Hvorfor skal vi måle? Og hvordan?

Roer (2015 s.10) setter kultur i et security-perspektiv ved å kombinere definisjonene til Oxford English Dictionary av henholdsvis kultur og security:

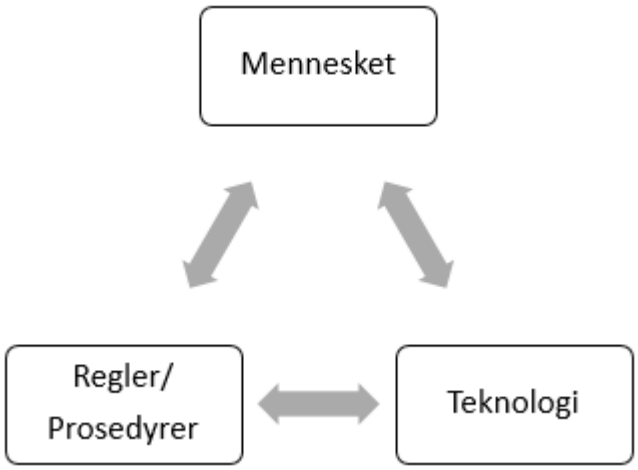
Culture: *"The ideas, customs and social behaviors of a particular people or group"*

Security: *"The state of being free from danger or threat"*

Roer (2015) sin definisjon av Security culture: «Ideene, holdninger og sosial adferd til spesifikke mennesker eller grupper som hjelper dem til å være fri fra trussel og fare»

Til grunn for definisjonen av kultur legger Roer (2015 s.7) at menneskers evne til å leve sammen i små eller store grupper er en biologisk utviklet evne, og at vi er ment til å danne grupper og finne måter å leve sammen på. I følge Roer (2015 s.9) er vår evne til gjenkjenning, av for eksempel en påstand, kulturelt, det vil si at det er en lært adferd. Hvis vi tar for oss en arbeidsplass så består kultur av mange grupper av mennesker som har hver sin kultur bestående av deres ideer, holdninger og sosiale adferd, og videre undergrupper og

kulturer, men sammen danner disse undergruppene organisasjonens kultur. Hver av gruppene følger de tre elementer mennesker, regler/prosedyrer (skrevne/uskrevne) og teknologi, som sammen former og endrer kulturen. (Roer, 2015 s.9-10).



Figur 6: Roers trekant: Endring av et hjørne vil endre security-kulturen. (2015, s 26)

Endring av et hjørne i figur 6 vil føre til endring av kulturen, er det også viktig å vurdere hvordan den endringen vil påvirke de to andre elementene. Det vil også være fornuftig å ta utgangspunkt i å bruke alle tre elementene hvor man for eksempel implementerer en ny prosedyre, sørger for å lære ansatte i organisasjonen å forstå endringene og hvorfor, og bruker teknologien for å innføre endringen. Under «Menneske» i figur 6 ligger også security bevisstgjøring (awareness), som er et begrep uten en klar felles forståelse av hva som ligger i det. (Roer, 2015 s.26-27). I følge Roer (2015 s.35) er rett kompetanse og evnen til å anvende gitt kompetansen i en spesifikk situasjon det som beskriver bevisstgjøring, og det som hjelper folk å kjenne til og være klar over hvilke security forhold de trener i.

Roer (2015 s.12) beskriver at måten organisasjonen behandler passord, hvordan ansatte oppdager og håndterer fremmende i bygningene er en del av security-kulturen, og også hvordan reglementer, innføringen av dem og opplæring av ansatte påvirker security-kulturen. I tillegg er omgivelsene viktige faktorer å vurdere når vi jobber med security-kultur (Roer, 2015 s. 26).

Å kun vite noe er ikke det samme som å endre adferd, men bare et av stegene mot å oppnå endret adferd (Roer, 2015 s.35). I følge Roer (2015 s.38) bør all vår innsats ligge i å identifisere ideene, holdningene og adferden fra security definisjonen i dagens organisasjon, og så gjøre en vurdering av hva vi ønsker de skal utgjøre i organisasjonen. Dette er ikke en enmanns jobb, og det er flere som bør involveres når man jobber med security-kultur. I

tillegg kommer den psykologiske forståelsen av hvordan mennesker påvirkes av andre, og det finnes taktikker som kan nyttes for å skape den støtten du trenger for å bygge og opprettholde sikkerhetskulturen i organisasjonen (Roer, 2015 s.50). I følge Roer (2015 s.69) er det mulig å måle kultur som vil vise adferden i egne systemer. Målet med Security Culture Framework er å støtte organisasjonen i å utvikle og opprettholde en god security-kultur, hvor Roers erfaring tilsier at en strukturert angrepsvinkel gir større sannsynlighet for suksess. Bygge og opprettholde en kultur er en pågående, uendelig prosess, en tilbakemeldings sløyfe som skaper en gjensidig endrings-syklus (Roer, 2015 s.102).

3.3 High Reliability Organisation

High Reliability Organization (HRO: Høypålitelige organisasjoner), ble utviklet av en gruppe forskere ved University of California, Berkley[1]. Teorien om HRO tar utgangspunkt i at ulykker i høyteknologiske systemer kan forebygges. Det fokuseres på organisasjonsdesign og forutsetter at det er mulig å utvikle pålitelige systemer basert på upålitelige enkeltkomponenter (Aven et al, 2013). Organisasjonens fokus må hele tiden være på sikkerhet og pålitelighet gjennom desentralisert styring, planlegging, redundans, kontinuerlig læring og en sterk organisasjonskultur. Robuste (resilient) organisasjoner har skapt en bevissthetskultur (awareness) hvor alle ansatte vurdere sikkerhet i alle aspekter av hva de gjør. De forventer at en hendelse vil inntreffe. En sterk desentralisering vil styrke de ansattes tro på egen intuisjon og melde oppover når de mistenker at noe ikke er som det skal, men det forventes ikke å stole på intuisjon alene (Boin et al., 2015 s.36).

LaPorte og Consolini (1991) påviste ved sin forskning at mange høypålitelige organisasjoner har evnen til spontant å omstrukturere seg i spesielle situasjoner. Kunnskap om organisatorisk redundans og organisasjonens evne til spontan strukturendring som tilpasning til kriser og plutselige belastningstopper, var viktige resultater fra forskningen på HRO.

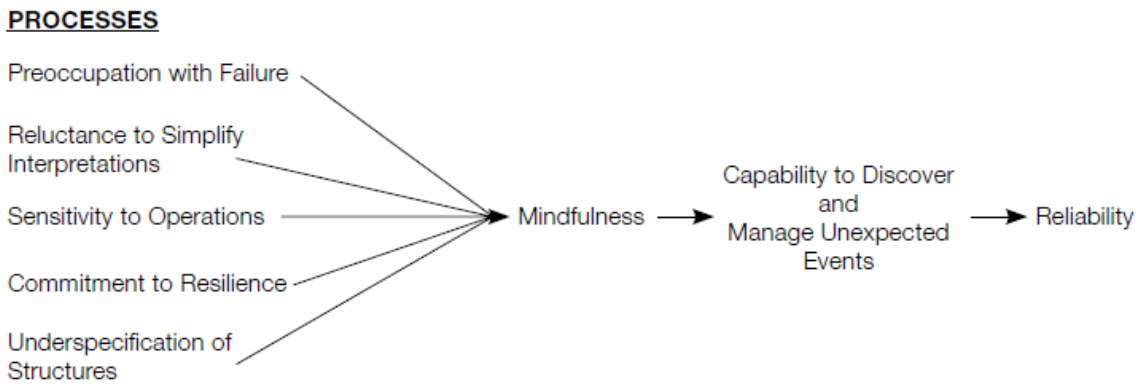
Reservesystemer, duplikasjoner og overlapp er nødvendig for å kompensere for eventuelle feil og kan gi pålitelige systemer av upålitelige komponenter. En sterk organisasjonskultur som setter pålitelighet høyt, vil øke sikkerheten ved at alle på lavt nivå oppmuntres til å reagere likt og riktig på unormale situasjoner. Kontinuerlig øving, trening og simulering gir høy pålitelighet (Aven et al., 2013 s.59).

[1] Sentrale personer var: Geoffery Gosling, Todd R. La Porte, Karlene H. Roberts, Gene I. Rochlin, Paul Schulman og Karl Weick.

Westrum (1992, 1997) viser til en «generativ» organisasjon der nye ideer er velkomne, informasjon søkes aktivt og feil fører til undersøkelser. Dette refererer Westrum til som en "lisens til å tenke" (Westrum, 1992 s.405). Organisasjoner som er villig til å handle på bestemte farer, er også villig til å se truslene og vurdere dem, fremfor å ignorere og avvise dem. Evnen til å oppdage og rette feil er en del av egenarten i HRO (Westrum, 1993).

Weick og Sutcliffe (2007) benytter begrepet «mindfulness» (oppmerksomhet/årvåkenhet) som en betydningsfull karakteristikk for HRO. Dette innebærer å kontinuerlig overvåke situasjoner ut fra eksplisitte forventninger og antagelser og oppdatere disse ut fra erfaring. Ikke minst vil en HRO ha en evne til å hele tiden å skape nye forventninger og antagelser utfra endringer i indre og ytre forhold.

Weick et al. (1999) påpeker at kognitive prosesser er viktig i høy pålitelige organisasjoner og uttrykker at en tilstand av oppmerksomhet/årvåkenhet (mindfulness) ser ut til å være skapt av minst fem prosesser; fokus på feil, unngår å forenkle tolkninger, årvåken ved operasjoner, jobber mot robusthet (resilience) og overordnet struktur. Figur 7 illustrerer hvordan de kognitive prosessene bidrar til å skape oppmerksomhet/årvåkenhet (mindfulness). Dette skal øke evnen til å oppdage og håndtere uventede hendelser som igjen vil gi økt pålitelighet i organisasjonen.



Figur 7: A mindful infrastructure for High reliability (Weick et al., 1999, s. 37)

En del forskere utpeker HROer til å ha en proaktiv kultur når det kommer til «å se etter problemer» i miljøet deres, og har klart å utvikle en kapasitet for grundig, men hurtig informasjonsprosessering under stressforhold (Boin et al., 2015 s.35). Boin et al. (2015 s.36) viser til at militæret er en organisasjon som ofte jobber i ekstreme miljø med raskt tempo og potensielt dødelig utfall. Det krever tilpasning, kontinuerlig sondering av vurderingene og identifisering av indikatorer som betyr endring.

3.4 Sensemaking

Sensemaking (meningsdannelse) defineres ifølge Weick (1995) som den kognitive prosess som foregår når vi forsøker å skape mening av det som skjer i våre omgivelser. Sensemaking handler om å skape mening i situasjoner som fremstår som tvetydige eller meningsløse. Dette gjøres ved å sette subjektive inntrykk i en forståelsesramme, og videre konstruere en midlertidig fortolkning av situasjonen. Sensemaking vil bidra til å håndtere fortløpende kompleksitet og usikkerhet ved en uønsket hendelse.

3.4.1 Fra kontrollerte situasjoner til uklare og komplekse situasjoner

Klein (2011 s.10) har identifisert ti påstander han har omformulert til å fungere i gråsoner, tvetydige, komplekse og uforutsigbare situasjoner. Vi har valgt ut fem av Kleins (2011) ti påstander, som vi ønsker å knytte til bygging av security-kultur. Vi vil drøfter relevansen av påstandene opp imot empirien i kapittel 6. Tabell 3 viser hvordan påstandene er gjeldene i kontrollerte situasjoner, men viser også til andre faktorer som påvirker påstandene i komplekse situasjoner og hvordan påstandene kan endres til å ta høyde for dette. Nummerering i tabell 3 stemmer ikke overens med Klein (2011) sin bok.

Nr	Kontrollerte situasjoner:	Uklare og tvetydige situasjoner:
1	Å lære folk prosedyrer hjelper dem å utføre oppgaver med dyktighet.	I komplekse situasjoner vil folk trenge dømmekraft for å kunne prosedyrene effektivt og handle utover dem når nødvendig.
2	For å få folk til å lære, gi dem tilbakemelding på konsekvensene av deres handlinger.	Vi kan ikke bare gi tilbakemeldinger; vi må finne måter å gjøre dem forståelig på.
3	For å forstå en situasjon trekker vi slutninger fra data.	Vi skaper mening fra dataene ved å plassere de i historier og andre rammer, men det motsatte forekommer også; våre rammer avgjør hvilken data som er gjeldene.
4	Planene våre vil lykkes oftere hvis vi identifiserer de største risikoene og finner måter å eliminere dem på.	Vi burde håndtere risiko i komplekse situasjoner ved å stole på resiliense engineering fremfor å forsøke å identifisere og forhindre risiko.
5	Ledere kan etablere et felles utgangspunkt ved å tildele roller og etablere basis regler i forkant.	Alle team medlemmer er ansvarlige for å kontinuerlig monitorere den felles plattformen/felles utgangspunktet for å oppdage feil og fikse feilene når nødvendig.

Tabell 3: Påstander fra kontrollerte til uklare og komplekse situasjoner (Klein, 2011)

Første påstand omhandler viktigheten av prosedyrer. Dette er fremtredende i Marinen hvor det er prosedyrer for nesten all aktivitet. Prosedyrer bidrar til å evaluere utførelse, om personellet kjenner prosedyrene og følger dem, men prosedyrer er vanskelig å holde oppdatert og er ofte utgått på grunn av at arbeidspraksisen utvikler seg (Klein, 2011 s.16/21). I følge Klein (2011) kan prosedyrer villede oss og føre til at personellet blir passive og følger

stegene i prosedyrene uten å tenke over hva de egentlig gjør, som igjen fører til at vi ikke forsøker å utvikle evnene våre. Personell som har lært å forstå systemet utvikler ifølge Sauer, Hockey og Wastell (2000) mer utviklede mentale modeller enn personell som kun er lært å følge prosedyrer (Klein, 2011). Klein (2011) viser også til styrkene ved å ha prosedyrer; de er treningsverktøy, støtte til hukommelsen, kan forhindre forstyrrelser, redusere arbeidsmengde, men utfordringen er at de ikke er sensitive til kontekst. Tinmannsvik (2008) påpeker at problemet med prosedyrer ikke er at de er ufullstendige, men at de ikke kan inneholde alle mulige eventualiteter. Regler og prosedyrer må justeres og re-designes for å kunne håndtere uforutsette situasjoner på en effektiv måte.

Produksjon av prosedyrer forsøker å fange opp hva ekspertene gjør, men prosedyrer og manualer kan ikke forklare taus kunnskap som folk har opparbeidet seg over tiår med erfaring (Klein, 2011 s.29). Personell bryter ikke regler fordi de synes det er morsomt, men fordi de ikke har noe annet valg (Tinmannsvik, 2008). Dette tilsvarer det Reason (1997) kaller «*necessary violation*». Dette viser betydningen av å finne en balansegang mellom det å være regulert gjennom regler og prosedyrer, og samtidig opprettholde evnen til kunnskapsbasert problemløsning (Tinmannsvik, 2008). Hovedbudskapet til Klein (2011) er ikke å forkaste prosedyrer, men hva som må gjøres i tillegg for å gjøre et bedre arbeid. Ved å lære personellet prosedyrer i en scenario-setting vil de se nytten av prosedyrene, forstå begrensningene og det vil hjelpe dem å tilegne seg noe av den tause kunnskapen nødvendig for effektivt å ta i bruk prosedyrer (Klein, 2011 s.31). Påstand en skaper et dilemma om å gjøre jobben korrekt eller å holde seg til prosedyrene, hvor det å ikke holde seg til prosedyrene kan føre til straff, og det å holde seg til prosedyrene men ikke få gjort jobben også kan medføre straff.

I **Påstand to** argumenterer Klein (2011) mot at tilbakemelding i seg selv ikke er tilstrekkelig. Tilbakemelding på utfallet av et arbeid/handling hjelper oss ikke til å forstå hvordan det kan bli bedre, vi trenger også tilbakemelding på prosessen, og ikke minst må tilbakemeldingen gi mening (Klein, 2011 s.166). En tilbakemelding må settes i kontekst, men ved uklare utfall er det vanskelig å se årsaks effekten av relasjoner knyttet til initiativ og pålitelighet, og i komplekse situasjoner vil du aldri finne ut av alt som foregår (Klein, 2011 s.167). I komplekse situasjoner må vi lære å tolke tilbakemeldingene, knytte handlingene til konsekvenser, sortere ut relevante og tilfeldige årsakssammenhenger. Sensemaking er kjernen til å lære kognitive ferdigheter ifølge Klein, ettersom vi ikke bare tilegner oss ny kunnskap, men endrer måten vi ser og tenker om ting – vi gir mening til motstridende og forvirrende data. Sensemaking, som innebærer å se hva som førte til hendelsene som foregår

og kunne forutse hvordan våre handlinger sannsynligvis vil påvirke fremtidige hendelser, er essensielt for å lære av tilbakemeldinger (Klein, 2011 s.173).

Påstand tre omhandler å trekke slutninger fra dataen for å skape forståelse av en situasjon. Sensemaking er som tidligere nevnt et forsøk på å forstå hendelser som har funnet sted og å forutse hva som kan skje videre. Å forstå en situasjon handler ikke bare om å se sammenhengen mellom elementer (dots), men å se dem i et historisk perspektiv som knytter dem sammen. Endrer historien seg, endrer elementene seg også. Intuisjon vil ifølge Klein (2011) hjelpe oss å gjenkjenne hvilke elementer som er verd å koble, og minne oss på hvilke elementer vi trenger for å skape et fullstendig bilde (Klein, 2011 s.185). Vi bruker ekspertise for å se mønster i dataene, definere hva som er gjeldene data og stille spørsmål til historier som ikke virker mulige (Klein, 2011 s.193). Sensemaking handler ikke bare om å motta data og slutninger, men å vite hvordan å bruke systemet for å finne hva vi leter etter. Vi skaper mening av hint og data ved å organisere de inn i rammer som historier, skript, kart og strategier, samtidig som også rammene kan bestemme hva vi skal bruke som data. Vekselvirkningen mellom data og rammer er kjernen i sensemaking (Klein, 2011 s.196).

Påstand fire sier at våre planer vil lykkes oftere hvis vi identifiserer de største risikoene og så finner måter å eliminere dem. Risiko avhenger av perspektiv og hvor vi står (Klein, 2011 s.233). Planlegging alene vil nødvendigvis ikke redusere risiko. For velorganiserte og strukturerte situasjoner fungerer prioritere-og-redusere risiko samt beregne-og-bestemme tilnærmingen seg, i motsetning til vurdere-og-tilpasse seg perspektivet som passer til komplekse, uklare og uforutsigbare situasjoner (Klein, 2011 s.245). High-reliability kultur foretrekker å lære av nesten-hendelser fremfor å vente på å lære fra ulykker, og kulturen forventer at arbeiderne er på vakt for eventuelle uregelmessigheter (Klein, 2011 s.247). Forskjellen i mentalitet gir ifølge Klein (2011) dem en økt evne til å forvente, unngå og håndtere risiko. Woods og Hollnagel (2006) og andre har beskrevet resilience engineering som en måte å utvikle prosjekt, organisasjoner og systemer til å være i stand til å tilpasse seg og stå imot uforutsigbare risiko (Klein, 2011 s.247). Resilience engineering forbereder ledere på å forvente å møte ubehagelige overraskelser fremfor å forsøke å forutse og kontrollere uforutsigbare risiko (Klein, 2011 s.248).

I følge **påstand fem** kan ledere skape en felles plattform ved å tildele roller og etablere grunnregler i forkant. Felles forståelse er essensielt, og team som har opparbeidet et felles utgangspunkt vil i større grad lykkes. I følge Klein (2011) er en felles plattform aldri perfekt og vil kontinuerlig brytes ned, og vi må derfor kontinuerlig monitorere og reparere den

underveis. Studier av HROer viser at gode team oppdager potensielle forvirringer og fikser dem, samtidig som de benytter seg av nede-tider til å re-kalibrere den felles plattformen ettersom erfaring tilsier at midt i en krise vil det kunne være for sent (Klein, 2011 s.266). I følge Forsvarets sikkerhetspolicy (2015) synliggjøres suksess når prosedyrer og praksis forenes. Forsvarets sikkerhetspolicy har fokus på at Forsvaret hele tiden må tilpasse seg ikke bare endringer, men teknologisk utvikling og økt kompleksitet i utførelsen av oppdrag. I følge policyen skal sikkerhetsarbeid påvirke tankesett og evne til å forvente og å håndtere det uventede. Dette skal oppnås ved å forene prosedyrer og praksis. Policyen innleder med at sikkerhetskulturen i Forsvaret skal skapes av ledere og ansatte gjennom gjensidig tillit, men hva Forsvaret legger i begrepet sikkerhetskultur er usikkert. I direktivet «Krav til sikkerhetsstyring» nevnes at avdelingene skal arbeide for å utvikle en sikkerhetskultur, men heller ikke her definerer Forsvaret hva de legger i begrepet.

Tankesettet Klein (2011) ønsker å fremme er å forvente å møte på problemer og forberede oss på å komme seg, altså være resilient. Når rutinene bryter sammen er det ifølge Klein (2011) de med et resilient tankesett som «skifter gir».

3.4.2 Sensemaking i komplekse og uforutsigbare situasjoner

Boin et al. (2015) fokuserer på krisehåndtering i det politiske systemet, men forståelsen og evnen til håndtering av kriser er overførbar til enhver organisasjon hvor det utøves ledelse. For å forstå at en situasjon er i emning må vi se betydningen av svake, usikre og motstridende signaler på at noe utenom det normale er i emning – sensemaking av situasjonen og informasjonen som er tilgjengelig. Lederen må drive sensemaking for å kunne vurdere trusselen, hvem/hva hendelsen vil berøre og videre utvikling av hendelsen. En krise defineres henholdsvis som en situasjon og en hendelse, med utvidet beskrivelse av begrepene. Vi ønsker å holde tråden i oppgaven hvor vi snakker om komplekse og uforutsigbare situasjoner knyttet til tilsiktede uønskede hendelser. Videre i teorien og oppgaven brukes derfor komplekse og uforutsigbare situasjoner, situasjoner eller hendelser fremfor krise.

Det er lett å være etterpåklok i etterkant av kriser og hendelser, men hendelseshåndtering på tynt grunnlag i de mest komplekse situasjoner kan håndteres bedre når man klarer å trekke mening av informasjon og tegn som er tilstede. Sensemaking ifølge Boin er å håndtere hendelser som de utvikler seg (Boin et al., 2015 s.18). I følge Boin et al. (2015 s.19) er det nesten umulig å forutsi med noen form for presisjon når og hvor en uønsket hendelse vil oppstå, og derfor nødvendig å evne å håndtere hendelsen når den inntreffer. Boin et al. (2015

s.38) påpeker også at ledere må bestemme hvilke signaler å ense, hvilke de vil ignorere og hvordan de skal forstå en trussel som allerede har materialisert seg. Forskning viser til at mange av ledetrådene vi trenger for å detektere en kompleks situasjon i emning er tilgjengelig i organisasjonen (Turner & Pidgeon 1997), men aktører i organisasjonsledelsen klarer ikke å samle ledetrådene før det er for sent (Boin et al., 2015 s.21). Eksempel: FBI satt i forkant av 9/11 på informasjon som alene ikke gav mening, men som sammen med CIAs informasjon kunne ha advart myndighetene før det var for sent.

Det er vanskelig i en organisasjon å få samlet data til en sammenhengende historie fordi personellet sjelden er enige om hva dataene forteller dem eller hvilken betydning det har for organisasjonen (Boin et al., 2015 s.22). I tillegg uthever Boin et al. (2015) at mangel på god etterretning om forestående hendelse, og deretter håndteringsgrunnlaget, kommer av fraværet på mekanismer som legger til rette for hurtig sensemaking. Oppfattelsen av en trussel er subjektiv og før man kan snakke om en kompleks og uforutsigbar situasjon må det være et betydelig antall aktører som er enige om at en trussel eksisterer og må håndteres snarest (Bovens & t'Hart, 1996 s.25).

Boin et al. (2015 s.118) beskriver et pessimistisk perspektiv hvor det er usannsynlig at ledere som frykter for sin posisjon vil oppmuntre andre til å gjennomføre en grundig undersøkelse av hva som nøyaktig gikk galt før og under en hendelse. En underliggende utfordring er at organisasjoner ikke kan kommunisere ordentlig og misforstår informasjon, de mislykkes med å samle tilstrekkelig relevant data. De som har lykkes med hendelseshåndtering sørger for å integrere erfaringen i regler og rutiner for å guide de ansatte. Utfordringen er at ingen hendelser er like, og læringen fra fortiden vil sannsynligvis bli morgendagens «blind corners». På samme måte vil en mislykket håndtering kunne føre til drastiske endringer av organisasjonens eksisterende regler som eksisterte før hendelsen inntraff, noe som er grunnleggende risikabelt, ettersom fremtiden ikke er en repetisjon av fortiden. I tillegg vil politikken rundt å holde folk ansvarlig, drive «blame-game», underbygge evnen til læring.

I et optimistisk perspektiv vil ifølge Boin et al. (2015 s.120) en forsterket og hensiktsmessig læring være mulig. Faktorer som påvirker til læring er en overbevisende vurdering av problemene koblet sammen med fornuftige løsninger for å få til endringer. Tid er også en faktor for å få til endringer etter en hendelse, hvor det er større mulighet for å få støtte og ressurser til implementering fra læring rett i etterkant av hendelsen. Forskning på HRO understøtter disse konklusjonene, og viser at organisasjonsledere kan bygge og opprettholde sikkerhetskulturer i organisasjoner som fasiliteter effektiv læring.

Tilsiktede uønskede hendelser kan komme overraskende, hvor ingen så i riktig retning da den inntraff. Løsningen kan være at ledere forsøker å forhindre slike «blind spots», og har fokus på hva de ikke blir fortalt og hva de kanskje ikke ser i omstendighetene (Boin et al., 2015 s.141). En annen grunn er at man ikke klarer å sette sammen puslebrikkene i tide. Dette krever deling av informasjon og felles situasjonsbevissthet, men å evne dette påvirkes av elementer som maktkamp, penger, prestisje, oppmerksomhet. Ledere må aktivt motivere og stimulere til å dele og sammenligne informasjon. En annen utfordring er når indre sirkel er opptatt av å fortelle lederen hva vedkommende vil høre, og unngår å nevne noe kontroversielt eller bekymringsfullt. Ledere må ikke bare etterspør informasjon, inkludert «worst-case scenarios», men også vise verdsettelse av de som frembringer dårlig nyheter eller argumenterer for upopulære synspunkt. Sensemaking av en kompleks og uforutsigbar situasjon krever i tillegg robuste systemer for datainnsamling og verifisering av informasjon, men også en organisering av informasjonsflyten og håndtering av rykter. Stressfaktoren må håndteres av en leder, og hans evne til å se egne begrensninger vil påvirke evnen til sensemaking i en kompleks situasjon (Boin et al., 2015).

3.5 Sammendrag av teorier

Studiet forsker på Marinens security-kultur og ser på relevansen MTO-faktorene har for å forbedre kulturen. MTO-faktorene gjør oss sårbare for trusler, men sammen med forståelsen av sårbarhetene og verdiene vil de bidra til bygging og håndtering av risikobildet.

Det teoretiske rammeverket innledes med en definering av risiko og risikoforståelse hvor en tilsiktet uønsket hendelse med tilhørende usikkerhet må sees i sammenheng med truslene man står ovenfor og en forståelse for verdier og sårbarheter. Organisasjonene må gjennom risikostyringen ta høyde for hvordan mennesker sosialt og kulturelt skaper sin egen risikoforståelse. Alt henger sammen, og i styringen av risiko og sikkerhet er det viktig å fokusere på MTO-forholdene og forstå koblingene (Aven et al., 2013).

Usikkerhetsfaktoren ved tilsiktede uønskede hendelser er stor ettersom kartleggingen av mulige trusler er vanskelig og krever store ressurser. Begrepet sorte svane beskriver en overraskende, ekstrem hendelse sett i forhold til ens kunnskap og tro (Aven, 2014a s.84), hvor usikkerhet er fraværet av kunnskap. En god security-kultur beskrives som en adferd hvor det er kompetanse til å håndtere tilsiktede uønskede handlinger, og det tas høyde for verdier, sårbarheter og usikkerhet. Begrepsavklaring vil skape en felles plattform og utgangspunkt for felles forståelse og evne til å håndtere trusler. Forsvarets uklare begrepsbruk vil skape forvirring, påvirke kompetansebygging og læring.

I cyberdomenet, som det femte krigføringsdomenet, handler cybersikkerhet om å beskytte «alt» som er sårbart fordi det er koblet til, eller på andre måter er avhengig av informasjon- og kommunikasjonsteknologi (NOU, 2015:13). Skal en organisasjon bygge en security-kultur må det ligge til grunn forståelse for trusselen man står ovenfor og hvilke sårbarheter og risiko dette fører med seg. Studien legger til grunn Reasons (1997) definisjon på en god sikkerhetskultur ettersom komponentene også er gjeldende for å skape en god security-kultur. Det største skille mellom security- og sikkerhetskultur ligger i vurderingene som gjøres for å beskytte seg mot trusler og tilsiktede uønskede hendelser vs. tilfeldige hendelser. I tillegg er usikkerhetene rundt trussel-håndtering større ved tilsiktede uønskede hendelser.

Fokuset til en HRO må hele tiden være på sikkerhet og pålitelighet gjennom desentralisert styring, planlegging, redundans, kontinuerlig læring og en sterk organisasjonskultur, som security-kulturen er en del av. Mindfulness er en karakteristikk av HRO hvor kompetanse og erfaring nyttes til å oppdage og håndtere uønskede hendelser, og som bygger pålitelighet i organisasjonen. Boin et al. (2015) viser til at militæret er en organisasjon som ofte jobber i ekstreme miljø med raskt tempo og potensielt dødelig utfall, hvor det kreves tilpasning, kontinuerlig sondering av vurderingene og identifisering av indikatorer som betyr endring. Slike resilience (robuste) organisasjoner karakteriseres ved sikkerhetsbevissthet (awareness), desentralisering og trening, som er faktorer i en HRO. I tillegg vil begrepet sensemaking, som handler om å skape mening i en situasjon som fremstår som tvetydig og meningsløs, bidra til fortløpende å håndtere kompleksitet og usikkerhet ved en tilsiktet uønsket hendelse.

Trusler og tilsiktede uønskede hendelser skaper uklare og komplekse situasjoner som Marinen må håndtere. Vi forsøker å relatere Reasons (1997) elementer, som beskriver en god sikkerhetskultur, til Kleins (2011) påstander som tar høyde for kompleksitet og tvetydighet i situasjoner. Klein (2011) beskriver blant annet viktigheten av prosedyrer som treningsverktøy, støtte til hukommelsen, kan forhindre forstyrrelser, redusere arbeidsmengde, men også utfordringer som at de ikke er sensitive til kontekst og vanskelige å holde oppdatert. I tillegg til prosedyrer må personellet forstå systemene og opparbeide fleksibilitet til å håndtere det uventede. Læring er et av Reasons (1997) elementer i en god sikkerhetskultur, og ifølge Klein (2011) vil tilbakemelding gi læring, men er i seg selv ikke tilstrekkelig. I komplekse situasjoner må vi tolke tilbakemeldingene, knytte handlingene til konsekvenser, sortere ut relevante og tilfeldige årsakssammenhenger. Sensemaking, som innebærer å se hva som førte til hendelsene og kunne forutse hvordan våre handlinger vil påvirke fremtidige hendelser, er essensielt for å lære av tilbakemeldinger (Klein, 2011). Videre som en del av sensemaking understreker Klein (2011) at intuisjon og ekspertise vil

bidra til å gjenkjenne relevante elementer og bruke systemet til å finne det vi leter etter i komplekse og uklare situasjoner.

Risikohåndtering i et security-aspekt hvor trusler skal håndteres, har et større usikkerhetsmoment enn i et safety-aspekt, og planlegging vil nødvendigvis ikke redusere risiko. Mentaliteten i en HRO-kultur, som foretrekker å lære av nesten-hendelser fremfor å vente på å lære fra ulykker, og en kultur som forventer at arbeiderne er på vakt for eventuelle uregelmessigheter, gir dem økt evne til å forvente, unngå og håndtere risiko. Slik vil også resilience engineering forberede ledere på å forvente å møte ubehagelige overraskelser fremfor å forsøke å forutse og kontrollere uforutsigbare risiko. Felles forståelse er essensielt, og en team med en felles plattform vil i større grad lykkes, men en felles plattform må kontinuerlig monitorere og repareres underveis. (Klein, 2011).

Boin et al. (2015) fokuserer på å håndtere situasjoner som de utvikler seg, og sensemaking er noe lederne må ta i bruk for å håndtere hendelsen når den inntreffer. Utfordringen er at mange ledetråder for å detektere trusler som er i ferd med å materialisere seg befinner seg i organisasjonen, men ledelsen klarer ikke å samle dem. I tillegg er de ansattes uenighet om dataenes betydning en utfordring for å bygge et sammenhengende bilde av situasjonen. Dette sammen med manglende etterretning om trusselbildet, og derav håndteringsgrunnlaget, kommer på grunn av fraværet av mekanismer som legger til rette for hurtig sensemaking. (Boin et al., 2015).

4. Metode

Dette kapittelet presenterer oppgavens forskningsdesign, herunder på hvilken måte datainnsamlingen er gjennomført for å kunne gi svar på problemstillingen og forskningsspørsmålene. Gjennom dette kapittelet forsøker vi å vise at forskningsprosessen på best mulig måte søker å oppfylle krav til relevante teoriperspektiver, utvalg av informanter, tilstrekkelig observasjon og data. I tillegg til at metodiske og etiske krav er blitt oppfylt gjennom datainnsamlingen.

4.1 Forskningsdesign

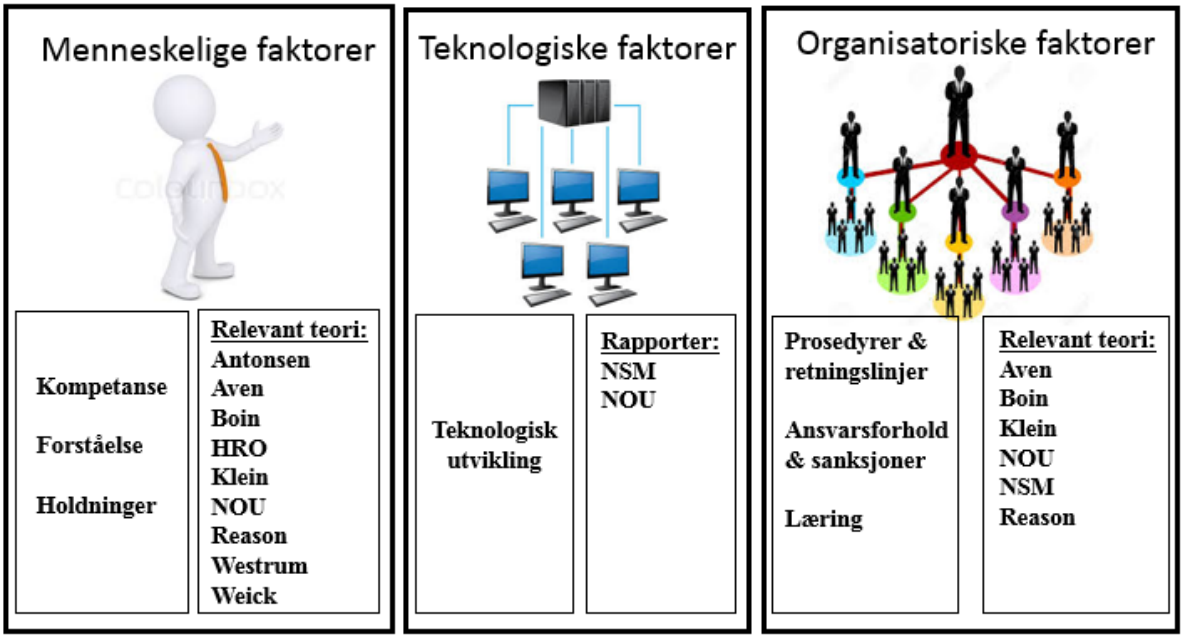
Vi har valgt å gjennomføre oppgaven som en litteraturstudie bygd opp på fire hovedpilarer; I. Observatørrolle (forfatterne), kvalitative, II. Semistrukturert- og åpne-intervjuer, III. Fag intervjuer og IV. Rapporter. Bakgrunnen for dette er at vi ønsket å få mer utfyllende svar på våre spørsmål for å få en bedre forståelse av virkeligheten Marinen står ovenfor og trusselen organisasjonen må håndtere.

Det vi ville se på gjennom forskningen var security-kulturen i en organisasjon som må håndtere uklarheter, kompleksitet, usikkerhet og mangel på kontroll, ergo de kravene stilles til oss som offiserer. I innledende fase valgte vi et bredt spekter av informanter, tre intervjuguider med et større antall spørsmål som gav oss store datamengder, noe vi ønsket for å best mulig kunne beskrive kulturen i organisasjonen.

Svært forenklet kan vi i den samfunnsvitenskapelige metodelæren si at kvantitativ metode forholder seg til data i form av kategoriserte fenomener og legger vekt på opptelling og utbredelse av fenomenene (Johannessen et al., 2009 s.36/101). Kvalitative data derimot, består av kortere eller lengre tekster som bearbeides ved å få frem meningsinnholdet og dataene foreligger som skrevne tekster, lyd eller bilder (Johannessen et al., 2009 s.351). To grunnleggende måter å samle inn egne kvalitative data på er gjennom observasjoner, der dataene bygger på forskerens sanseinntrykk av handlinger og samhandlinger i konkretet situasjoner. Eller gjennom intervjuer der dataene bygger på det informantene sier i samtaler med forsker. Vi har valgt å benyttet oss av begge de grunnleggende måtene når vi samlet inn data.

Vi ønskte å skape en tillit til deltakerne av studien for å få mest mulige oppriktige og ærlige svar. Kvalitative metoder vil ifølge Blaikie (2014 s.214) tillate en forsker å bli en «insider», og oppdage aktørenes kultur og verdenssyn.

Figur 8 viser vår hovedtilnærming til plan og struktur på relevant teori og empiri i oppbygging av oppgaven. Dette er fordelt under overskriftene menneskelige, teknologiske og organisatoriske aspekter (MTO).



Figur 8: Plan og struktur på relevant teori og empiri

4.2 Forskningsprosessen

Vi startet arbeidet med diskutere oss frem til et felles tema vi begge ønsket å skrive om. Det ble utarbeidet en prosjektskisse som ble oversendt Sjøforsvarsstaben (SST) for godkjenning for så å bli oversendt Universitet i Stavanger (UIS) i januar 2016. Alt arbeidet vi har gjort har vi hatt på et delt område i Dropbox, som gjorde at begge til enhver tid kunne se siste versjon av alle dokumentene. Denne måten å organisere oss på mener vi har fungert på en meget god måte, tross de geografiske utfordringene som kan oppstå. Vi brukte meget hyppig Skype, telefonkonferanser og fysiske samlinger for å opprettholde en god kommunikasjon og et godt samarbeid. Det ble også laget en tentativ fremdriftsplan med tilhørende dreiebok for å styre prosessen frem mot leveranse. Dreieboken ble oppdatert forløpende gjennom hele prosessen.

I februar 2016 fikk vi tildelt veileder som vi raskt gjennomførte et møte med. Problemstilling og forskningsspørsmål ble her justert, og vi startet arbeidet med å skrive teori. I tilnærmet samme periode valgte vi metode og startet arbeidet med spørsmål til intervjuguidene. Vi var deltagere på sikkerhetskonferansen i mars 2016 i regi av NSM. Vi har også deltatt på foredrag om «Etterretningstrussel mot Norge og Haakonsvern» gjennomført av PST og foredrag om «Sikkerhet & personvern i den digitale tidsalder» arrangert av

sikkerhetsutvalget. Sistnevnte hadde som mål å skape debatt rundt sentrale tema for utvalgets arbeid, slik at relevante perspektiver og innspill blir ivaretatt i utredningen. Dette for å få enda flere innspill og en bedre forståelse for temaet. Vi valgte også observerende deltaker og tilstedeværende observatør rolle i tillegg til intervjuer i data innsamlingen, for å få direkte tilgang til samhandling, handlinger og adferd. Vi valgte observasjon hvor kunnskap om den sosiale verden best tilegnes ved å delta og erfare naturlige settinger (Johannessen et al., 2009 s.118).

Observasjon er ifølge Johannessen et al (2009 s.118) den best egnede metoden for å få tak i dybde, kompleksitet, bredde og flerdimensjonalitet ved den sosiale virkeligheten, og det er ikke sikkert det vi sier er det vi faktisk gjør. På bakgrunn av dette har en av oppgavens medlemmer seilt med to av Marinens enheter både som observerende deltaker og tilstedeværende observatør for å få innblikk og forståelse i hverdagen ombord. I løpet av et forskningsprosjekt kan forskeren i en del tilfeller velge å ha ulike roller, spesielt når observasjonen foregår åpent (Johannessen et al., 2009 s.127). Den andre av oppgavens medlemmer har sitt daglig virke i dette miljøet, og gjennomførte også en åpen feltrolle som både observerende deltaker og tilstedeværende observatør.

I samme periode fikk vi muntlig godkjenning av tre avdelingssjefer på nivå 4 (ref. punkt 2: organisasjons- og sikkerhetsstruktur) til å starte kartleggingen og kontakte mulige informanter nedover i avdelingene. Det ble ikke overfor avdelingssjefene informert om hvem som ville bli kontaktet, dette vil bli mer utdypet under punkt 4.3.5 anonymitet. Vi startet samtaler med personell på nivå 3- 4 og 5 for å rekruttere de som informanter, både til semistrukturerte hurtigintervju men også til ustrukturerte/åpne leder intervju. Vi kontaktet også faginstanser og personell som FSA, NSM, CYFOR, Roer (CLTRe) og Nytrøen (E-tj) til fagintervjuene. Samtlige vi har vært i kontakt med, syntes oppgaven og problemstillingen var interessant og var villig til å bidra som informanter og fageksperter. Organisasjonens og informanters positivitet til oppgaven var en ekstra motivasjon for oss i vårt videre arbeid med oppgaven.

Tid og gjennomføring av intervjuer ble avtalt direkte med hver enkelt informant og vi satte av to uker til praktisk gjennomføring. Grunnet enkelte kansellering ble intervjuene gjennomført i løpet av en fire ukers periode. Det ble laget en detaljert gjennomføringsplan, som var utfordrende og tidkrevende, noe som blir mer utdypet under punkt 4.3.4 gjennomføring intervjuer. Etter at datainnsamlingen var gjennomført startet vi det store arbeidet med å analysere, se punkt 4.3.6 analyseprosessen. Når arbeidet med å analysere var

gjennomført startet vi prosessen med drøftingen av teori og empiri, for deretter å utarbeide konklusjon og vise til forbedringsmuligheter.

4.3 Innsamling av data

4.3.1 Primær og sekundærdata

Primærdata

Som beskrevet i punkt 4.1 forskningsdesign er studien bygget opp på fire hovedpilarer. Primærdata er i denne studien; I. Observatørrolle (forfatterne), kvalitative, II. Intervjuer av typen semistrukturert-, åpne- og III. Fag intervjuer. Datainnsamlingsmetodene er utarbeidet og gjennomført for besvare studiens problemstilling.

Primærdata ble samlet inn gjennom 36 semistrukturerte hurtigintervjuer med ansatte, samt fem ustrukturerte/åpne intervjuer med ledere, i tre anonyme avdelinger på nivå 3, 4 og 5 i Marinen. Nivå 3 er Marinens ledelse og stabselement, nivå 4 er avdelingsledelse med tilhørende treningssentre og nivå 5 er fartøyene og deres besetning. Utvalg av informanter utdypes mer under punkt 4.3.3 Utvalgsstrategi.

Vi har også gjennomført fem åpne ekspert intervjuer med FSA, NSM, CYFOR, Roer (CLTRe) og BG Nytrøen (E-tj), hvor de har godkjent bruk av navn og avdeling. Videre har oppgavens medlemmer hatt observerende deltager og tilstedeværende observatørrolle i miljøet, ref punk 4.2 Forskningsprosessen. Hensikten ved observatørrollen var å få tilgang til samhandling, handlinger og adferd. Observatørenes erfaring: I løpet av 15 år i Forsvaret har Hille gjennomført Befalsskolen for Marinen og Sjøkrigsskolen. Hille har tjenestegjort ved Dykker- og froskemannsskolen, på Minejaktfartøy og ved Minevåpenets treningssenter, vært skipssjef i to år på Stridsbåt 90 (hurtiggående fartøy på 50 fot), har et års erfaring fra internasjonale operasjoner og jobber i dag som stabsoffiser (seks år). Myr har i løpet av 16 år i Forsvaret, blant annet gjennomført Befalsskolen for Marinen og kvalifiseringskurs på Sjøkrigsskolen. Myr har tjenestegjort på Minejaktfartøy, Hauk klasse MTB, Sjøforsvarets sikkerhetssenter og vært skipssjef Stridsbåt 90. Myr har vært fem år som sikkerhetskoordinator for MTB Våpenet og jobber i dag som sikkerhetskoordinator i Sjøforsvarsstaben.

Resultatene fra fagintervjuene vil fremkomme i FS1 hvor det blir trukket frem hva fag-informantene legger vekt på i beskrivelsen av trusselbildet og innsidetrusselen. Deler av resultatene fra fag-intervjuene vil også sammen med resultatene fra resterende intervju og observatørroller bli presentert som primærdata under FS2. Primærdata ble valgt for å kunne

danne en forståelse for trusselbilde (FS1) og en kartlegging av hva som beskriver Marinens security-kultur i dag (FS2). Knyttet til teori vil FS1 og 2 bli sett i sammenheng for å kartlegge muligheter for å forbedre security-kulturen i Marinen (FS3).

Sekundærdata

Sekundærdataen i denne studien ble ikke utarbeidet for å besvare problemstillingen eller forskningsspørsmålene. Valgte sekundærdata ble brukt til å understøtte valg av tema og problemstilling, og videre som grunnlag for utarbeidelsen av intervjuguidene. Trusselbildet er i kontinuerlig endring og kan ikke beskrives gjennom eksisterende teori. Etterretningstjenesten og politiets sikkerhetstjeneste er statlige organer som utarbeider trusselvurderinger. NSM og NOU rapportene støtter seg blant annet på disse vurderingene i tillegg til annen data for å sette informasjonen i en samfunnsrelatert kontekst slik at det dannes et grunnlag for å gjøre vurderinger for håndtering av truslene. Studien la rapportene fra E-tjenesten, NSM og NOU til grunn for å kunne gi et bilde av trusselen Marinen står ovenfor for å kunne belyse hvilken relevans en security-kultur har for organisasjonen.

4.3.2 Intervjuguider

Da vi hadde kartlagt og skrevet store deler av teorien og i samråd med veileder valgt metode, begynte vi å utarbeide informasjonsskriv til informanter og intervjuguider. Det ble laget tre informasjonsskriv (vedlegg A, B og C) og intervjuguider basert på gruppene vi anså nødvendige å dekke for å svare på forskningsspørsmålene og problemstillingen. Valg av informanter vil bli mer utdypet under punkt 4.3.3 utvalgsstrategi. Informasjonsskriv til informantene inneholdt kort informasjon om oppgavens medlemmer, overordnet tema, problemstilling og forskningsspørsmål samt anonymitet. Informantene fikk også oversendt et skjema for samtykke, som ble signert ved oppmøte til intervjuet.

Den første intervjuguiden (vedlegg A) var semistrukturert og ble gjennomført som hurtig intervjuer på rundt 15-20 minutter. Vi hadde på forhånd fastlagt tema og spørsmålsformuleringer. Dette bidro til at vi til en viss grad sikret oss lik kontekst under intervjuene, men at vi samtidig kunne variere spørsmålsrekkefølgen i forhold til hvordan samtalen utløp seg (Johannessen et al., 2006 s.137). De informantene som var sikkerhetsledere under dette intervjuet fikk flere spørsmål enn de som ikke hadde en slik rolle. Dette fremkommer i intervjuguiden. Intervjuguiden til hurtigintervjuene inneholdt 21 spørsmål til informantene, som inkluderer de ekstra spørsmålene som kun sikkerhetslederne fikk. Med bakgrunn i vår innsikt og erfaring fra miljøet, samt gjennomføring av to

testintervjuer, fant vi det hensiktsmessig å gjennomføre intervjuene med 21 spørsmål for å få et helhetlig inntrykk av MTO faktorene.

Den andre intervjuguiden (vedlegg B) ble gjennomført som ustrukturerte/åpne intervjuer med ledere på nivå 3-5 og ble gjennomført på 30-40 minutter. Denne formen for intervju er mer uformelt med åpne spørsmål der vi på forhånd hadde gitt et tema, men spørsmålene ble tilpasset den enkelte intervjusituasjon (Johannessen et al., 2006 s.137). Dette intervjuet bar preg av en samtale.

Den tredje intervjuguiden (vedlegg C) ble utarbeidet for å intervjue fageksperter på området, og ble gjennomført på rundt en time avhengig av hvor mye de ønsket å si. Det var flere organisasjoner som ble intervjuet med tilnærmet like spørsmål, men tilpasset organisasjonens utgangspunkt. Her ble intervjuene gjennomført som åpne, hvor samtalen gikk forholdsvis fritt. Den ene organisasjonen hadde ingen tilknytning til Forsvaret generelt, men ble intervjuet som fagekspert på temaet security-kultur.

4.3.3 Utvalgsstrategi

Det avhenger av forskningsspørsmålene hvem og hvor mange informanter som velges ut. Utvelgelsen av informantene er viktig i all forskning fordi prosessen har stor innflytelse på analysen av dataene (Johannessen et al., 2009 s.106). I samarbeid med ledelsen i Marinen valgte vi ut tre tilgjengelige avdelinger på nivå 4. Disse er blitt anonymisert i oppgaven, noe som blir mer utdypet under punkt 4.3.5 anonymitet.

Ved hurtigintervjuene (vedlegg A) ble det intervjuet 30 informanter samt seks informanter som innehar rollen som sikkerhetsledere. I følge Johannessen et al. (2009 s.111) kan valg av informanter deles inn i spesielle, ulike, feltbestemte og på forhånd bestemte utvalg (Shakir, 2002). For å besvare problemstillingen var «ulike tilfeller» relevant, og utvalgskriterier er avhengig av forskningsspørsmålene og hva som er praktisk og hensiktsmessig å gjennomføre (Johannessen et al., 2009 s.111). Oppgavens medlemmer satte følgende kriterier på hvilke informanter vi ønsket på dette nivået:

- Likt antall informanter fra tre ulike avdelinger innad i Marinen (nivå 4 og 5).
- Lavere og høyere grad (Menig – Orlogskaptein)
- Erfarne og uerfarne
- Både land- og sjøpersonell
- Seks informanter som innehar rollen som sikkerhetsleder

Begrunnelse for valg av kriterier er ønsket om spredning på hvilke type informanter vi intervjuet. Både på grads- og erfaringsnivå, land- og sjøpersonell. Videre ønsket vi å også å kartlegge forståelse og kjennskap hos personell som i kraft av sin rolle har bedre innsikt i utfordringer og forbedringsforslag rundt oppgavens tema.

Ved intervjuform ustrukturert /åpen intervju (vedlegg B) ønsket vi å intervjue ledere på nivå 3, 4 og 5. Kriteriene her var noe kortere og innbefattet at de måtte ha en lederrolle innad i en av de tre nivåene i Marinen.

Ved ekspertintervjuene ønsket vi å intervjue personer som hadde kompetanse innenfor fagfeltet security, kultur og cyber, og som jobbet i en av organisasjonene som støtter Forsvaret i håndteringen av cybertrusselen. FSA, NSM, CYFOR, Roer (CLTRe) og BG Nytrøen (E-tj) var organisasjoner og personer som utpekte seg.

4.3.4 Gjennomføring intervjuer

Det ble gjennomført to prøve hurtigintervjuer på nivå 4 og 5 for å kartlegge om spørsmålene og planlagt tidsbruk per intervju var i henhold til plan. Dette viste seg svært nyttig da vi fikk verifisert at vi kunne fortsette som planlagt men med noen små endringer i spørsmålsformuleringen.

Etter samtaler med potensielle informanter på nivå 3, 4 og 5 laget vi en detaljert gjennomføringsplan for intervjuene. Informantene fikk velge et tidspunkt som passet de best. Gjennomføringsplanen bidro sannsynligvis til at gjennomføringen gikk overraskende bra, selv med det store antallet informanter. Vi hadde to møterom disponible til intervjuene som var på et «nøytralt område» for begge parter. Videre gjennomførte vi også noen intervjuer om bord hos informanter, ved ønske, og behov for å ta minst mulig av deres tid i en travel hverdag. Det ble da benyttet et egnet lukket rom slik at vi ikke ble forstyrret. Vi som intervjuere valgte å ikke stille i uniform under intervjuene, slik at ikke vår grad skulle være en faktor som påvirket svarene deres.

Vi startet hvert intervju med å presentere oss, og informanten fikk anledning til å fortelle litt om sin jobb. Hensikten med dette var å skape en relasjon og åpen atmosfære før intervjuet startet (Johannessen et al., 2009 s.137). Videre repeterte vi informasjonsskrivet informantene hadde fått tilsendt, og informanten fikk anledning til å stille eventuelle spørsmål. Vi avsluttet innledningsfasen ved at informanten signerte samtykke-skjema.

Vi valgte å sette av 10-15 minutter mellom hvert intervju til å notere tanker, observasjoner og fordeler/ ulemper med hvert intervju. Dette viste seg å være fordelaktig når vi skulle gjennomføre mange intervjuer på en dag og gav støtte til seinere analyser av data.

De første hurtigintervjuene på nivå 4 og 5 ble gjennomført med begge oppgavens medlemmer til stede. Dette for å få en enda mer lik kontekst når resten av intervjuene skulle gjennomføres. Etter dette delte vi oss for å kunne klare å komme gjennom flere intervjuer i tidsperioden vi hadde tilgjengelig. Under intervjuene av lederne var begge oppgavens medlemmer tilstede.

Det ble tidlig tatt kontakt med organisasjoner som Sjøforsvarets har som samarbeidspartnere innenfor fagområdet cyber/security. Det ble koordinert tid og sted for gjennomføring av intervjuer med personene i organisasjonene som ønsket å støtte oss i vårt arbeid. Det ble benyttet flere uker på å koordinere i forkant og gjennomfør fagintervjuene. Samtlige som ble kontaktet stilte seg positive til forespørselen.

Vi sendte ut *«Informasjonsskriv til informanter fageksperter»* i god tid før møtene og tok kontakt noen dager i forveien for å forsikre oss om at avtalen fortsatt var gjennomførbar. Intervjuene med CYFOR ble gjennomført på Lillehammer, mens intervjuet med FSA ble gjennomført i Oslo samme uken. Begge oppgavens medlemmer deltok i dette arbeidet. Intervjuet med NSM, Roer og BG Nytrøen ble også gjennomført i Oslo. Disse ble gjennomført av kun en av oppgavens medlemmer. Avtalt båndopptak gjorde at begge fikk anledning til høre alle intervjuene i etterkant. Gjennomføringen av fagintervjuene ble gjort på et egnet sted for begge parter.

4.3.5 Anonymitet

Da tillatelsen for å gjennomføre intervjuer innad i Marinen ble muntlig innhentet hos tre nivå 4 sjefer, ble det ikke utdypet hvilke enheter på nivå 5 vi kom til å kontakte i deres avdeling. Heller ikke hvilke informanter vi kom til å kontakte. Nivå 4 sjefene vet kun om egen avdeling og vet ikke hvilke to andre avdelinger som deltar. I oppgaven blir disse tre avdelingene anonymisert. Kun oppgavens medlemmer vet hvilke avdelinger som er en, to og tre. Dette ble gjort for å anonymisere informantene ytterligere.

Det ble til alle informanter innad i Marinen sendt ut «*Informasjonsskriv til informanter*», hvor det ble presisert at intervjuene var anonyme. Dette ble også repetert før intervjuet startet. Informantene fikk også muntlig informasjon om at de kunne trekke seg som informanter hvis de ønsket det, helt frem til oppgaven leveres. Ved å forsikre informanten

anonymitet ønsket vi å redusere eventuelle feilaktig og manipulerte svar. Informantens kjønn, navn, grad, stilling eller avdeling er ikke benyttet i denne oppgaven for å ivareta informantens anonymitet. Det fremkommer henvisning til sikkerhetsledere og ledere, men med antallet sikkerhetsledere og ledere i Marinen på nivå 3, 4 og 5, vurderer vi det til at anonymiteten er ivaretatt. Det ble innhentet godkjenning for forskningen av Norsk senter for forskningsdata (NSD) (Se vedlegg D). Det henvises til informant ved nummer og avdelingsnummer, for eksempel informant 13 avdeling to ble informant nummer 132. I empirikapitelet blir det satt informantnummer i parentes bak utsagnene. Oversikten over informanter og informantnummer ble lagret på et gradert område som kun en av oppgavens medlemmer har hatt tilgang til. Da listen ble lastet over på ugradert pc for å kunne transkribere intervjuene og analysere dataen, var det kun informant- og avdelingsnummer som ble tatt med over. Samtlige anonyme informanter signerte samtykkeskjema. Disse blir oppbevart på et skjermet sted og makuleres når oppgavens sensur foreligger.

I forkant av fagintervjuene avklarte vi muligheten for å referere til intervjuet ved bruk av både person- og organisasjonsnavn. Grunnet sine posisjoner i organisasjonen de tilhørte var det ikke et behov for anonymitet fra deres side. Samtlige signerte samtykke til å delta i prosjektet samt at det kunne refereres til stillingsnavn, person og organisasjon i masteroppgaven. Det ble avtalt at vi sendte ferdigarbeidet tekst, hvor vi henviste til deres uttalelser, for godkjenning i god tid før masteroppgaven ble levert.

Det ble tatt opptak under intervjuene med godkjenning av informantene. For å også her ivareta anonymiteten ble det ikke nevnt navn, stilling eller avdeling i lydopptakene. Det var heller ikke tillat å snakke om noe som er gradert og dette ble informanten informert om før opptak. Hvis informanten ønsket å komme med eksempler som var gradert ble lydopptakene stoppet og mobilene tatt ut av rommet. Denne informasjonen ble ikke brukt i oppgaven, men for å bidra til økt forståelse for oss som intervjuere. Lydopptakene ble ikke delt med andre og ble kun benyttet til denne masteroppgaven. Lydopptakene slettes når masteroppgavens sensur foreligger.

4.3.6 Analyseprosessen

Etter at intervjuene var gjennomført startet arbeidet med transkripsjon, noe som er det første steget i analyseprosessen. Uten god kvalitet på transkripsjoner kan kvaliteten på arbeidet lide. Det er viktig å ha en viss føling med materialet, og det anbefales derfor i faglitteraturen at intervjuerne selv gjennomfører dette arbeidet (Landridge, 2006 s.261). Vi delte derfor arbeidet med å høre gjennom opptakene på nytt og gjennomføre transkripsjon av rådata.

Vi benyttet en fenomenologisk fremgangsmåte ved at vi beskrev transkripsjonen i form av hvem som sa hva i kronologisk rekkefølge (Landridge, 2006 s.258). Vi utarbeidet en egnet oversikt i et XL ark (figur 9) hvor vi skrev inn alle svarene.

	INTERVJU SVAR NIVÅ 4- 5 hurtig intervju	
Informant NR:	**SPØRSMÅL:**	
	1.Hva mener du er innsidetrussel, og tror du det er en reel trussel du kan møte? Utdyp gjerne. (Alle, SL)	**2.På hvilket nivå må innsidetrusselen håndteres? Utdyp gjerne (Alle, SL)**
111	Kronologisk tekst	Kronologisk tekst
302	Kronologisk tekst	Kronologisk tekst

Figur 9: Utdrag av arbeidsdokument ved fenomenologisk fremgangsmåte

Spørsmålene ble lagt i rader mens informantenes nummer og svar ble lagt i egne kolonner under hvert spørsmål. Dette gjorde at vi fort kunne se hva hver enkelt informant svarte på samme spørsmål. Underveis i dette arbeidet laget vi notater, også kalt memoer, med refleksjoner om dataene (Landridge, 2006 s.261). Disse notatene nyttet vi oss av i vårt videre arbeid med analysen. Deretter organiserte vi datamaterialet i kategorier (Johannessen et al., 2006 s.162) vist i tabell 4. Vi sorterte kategoriene for å avdekke liknende utsagn, mønstre, sammenhenger, fellestrekk eller forskjeller.

Vi tok utgangspunkt i MTO-perspektivet som en åpen koding med underkategorier til M og O faktorene (Blaikie, 2014 s.211). Videre delte vi M inn i *kompetanse, forståelse* og *holdninger*, og O inn i *prosedyrer & retningslinjer, ansvarsforhold & sanksjoner* og *læring.* Hensikten var å kunne knytte koblinger mellom kategoriene senere i analysen (Blaikie, 2014 s. 212). Vi ønsket også å kategorisere materialet for å strukturert kunne fremlegge funnene i empiri kapitelet. Kodingen av datamaterialet var den mest tidkrevende prosessen grunnet den store mengden data og at det ikke er et klart skille mellom MTO faktorene.

Resultatene fra hurtigintervjuene gav oss en mulighet til å gi en numerisk fremstilling av enkelte elementer til støtte av helhetsbildet. I følge Blaikie (2014) kan kvalitative studier produsere enkle tabeller med frekvens og prosenter for å oppsummere noen av funksjonene i ikke-numeriske data. Slik telling i kvalitativ forskning kan gi støtte til visse elementer i en sosial gruppe eller kategori (Blaikie, 2014 s.215). Når vi analyserte teksten kom vi i flere av spørsmålene frem til tolkninger som gjorde at vi kunne lage diagram av svarene til informantene. Diagrammene er presentert i kapittel 5 empiri.

Vi tok bort mest mulig irrelevant informasjon og fortsatte med den informasjonen som var sentral for våre forskningsspørsmål.

4.4 Validitet, reliabilitet og etiske utfordringer

For å beskrive kvaliteten på en oppgave brukes begrepene reliabilitet og ulike validitetsformer innfor kvantitativ forskning. Johannessen et al. (2009 s.98) mener det ved kvalitative studier ikke er snakk om enten eller, men både og. Reliabilitet omhandler hvilken data som brukes, måten de samles inn på og hvordan de bearbeides i undersøkelsen. Slike krav om reliabilitet er lite hensiktsmessig innenfor kvalitativ forskning ettersom strukturerte datainnsamlingsteknikker ikke benyttes, observasjoner er klart verdiladede og kontekstavhengige, og man som forsker bruker seg selv som instrument (Johannessen et al., 2009 s.199). Johannessen et al. (2009 s.199) påpeker at forskeren kan styrke påliteligheten ved å gi en inngående beskrivelse av konteksten og en åpen og detaljert framstilling av framgangsmåten under hele forskningsprosessen. Ved detaljert beskrivelse av hele forskningsprosessen anser vi påliteligheten for å være tilstrekkelig for valgte metode.

Begrepsvaliditet, «måler vi det vi tror vi måler», er en vanlig definisjon av validitet innenfor kvantitative undersøkelser, mens kvalitative studier/undersøkelser vil ikke være valide etter det begrepet fordi de ikke kan kvantifiseres (måles) (Johannessen et al., 2009 s.199). I følge Johannessen et al. (2009 s.199) vil validitet i kvalitative undersøkelser dreie seg om i hvilken grad forskerens funn på en riktig måte reflekterer formålet med studien og representerer virkeligheten. To teknikker som øker sannsynligheten for at forskningen frembringer troverdige resultater er ifølge Guba og Lincoln (1985) vedvarende observasjon og triangulering (Johannessen et al., 2009 s.199);

> *Vedvarende observasjon* innebærer å investere nok tid til å bli godt kjent med felten, slik at man kan skille mellom relevant og ikke relevant informasjon og bygge opp tillit. Det er vanskelig å forstå et fenomen uten å kjenne til konteksten.
>
> *Metodetriangulering* vil si at forskeren under feltarbeidet bruker ulike metoder – for eksempel både observasjon og intervju. Det kan også bety at forskeren ikke bare tar utgangspunkt i en setting som for eksempel en skoleklasse, men tar utgangspunkt i flere skoleklasser hvis han ønsker å studere elevers samarbeidsevner i en klasse.

Vedvarende observasjon mener vi ivaretas tilstrekkelig ved henholdsvis 15 og 16 års erfaring i organisasjonen, og flere års samarbeid med ansatte fordelt på alle avdelingene for å sikre validiteten til oppgaven. Dette styrkes ytterlige ved at vi nyttet oss av metodetriangulering

ved å gjennomførte åpne- og semistrukturerte-intervju, observasjon og rapporter. Hvorvidt forskningens resultater er pålitelige handler om hvor pålitelige forskningens empiri er samt i hvor stor grad datamaterialet er troverdig (Jacobsen, 2005 s.225). Oppgavens skriftlige kilder anses i all hovedsak å være representative og pålitelige kilder.

Etiske problemstillinger ble meget relevant ved valg av kvalitativ metode hvor vi gjennom intervjuer og observasjon kom direkte i berøring med mennesker (Johannessen et al., 2009 s.91). Vi har tatt høyde for de etiske utfordringene ved å få intervjuguidene godkjent av Norsk senter for forskningsdata. I tillegg har vi hentet tillatelse fra Sjøforsvarsstaben for å gjennomføre intervjuene i Marinen. Vi valgte også å anonymisere informantene på nivå 3, 4 og 5 for å unngå interne konflikter i etterkant basert på uttalelser. Informasjon om hvorfor vi gjennomførte intervjuene ble gitt i forkant, og informantene kunne stille spørsmål før intervjuet startet. Observatørrollene, observerende deltaker og tilstedeværende observatør, ble også valgt slik at alle ansatte involvert var klar over rollen vår og forskningsprosjektet.

4.5 Fordeler og ulemper ved metoden

Vi ser i etterkant at antatt spissing av problemstillingen og valg av metode for datainnsamling gav rom for forskning til flere masteroppgaver. Problemstillingen tar for seg tre store fagfelt; cyber, security og kultur.

Oppgaven spenner ganske bredt med spørsmålsmengden i intervjuguidene, noe som påvirker analysens dybde. Dette var et bevisst valg i forhold til at valgte organisasjon består av og håndterer store mengder gradert materiale. Ved å velge bredde holdt vi oss på et ugradert nivå, og vår formening er at oppgaven gir en konstruktiv innsikt i utfordringene ved organisasjonen security-kultur. Videre forskning på et gradert nivå vil gi organisasjonen muligheten til å fordype seg ytterlige på gitte områder.

Under intervjuene vi gjennomførte med informantene så vi tydelig fordelen kvalitativ metode gav ved at det ble lagt få begrensninger på svarene informanten gav. Selv om vi benyttet semi-strukturerte intervjuer på mange av informantene kom de med utdypende/utfyllende svar. Det var både likheter i svarene deres men også mange ulike svar. Ved å åpne intervjuet med å fortelle litt om hvem vi som intervjuere var, og la informantene fortelle om sin jobb, åpnet det opp for en lettere dialog gjennom intervjuene.

Selv om vi hadde laget hovedtemaer og spørsmål, lot vi samtalen flyte ganske fritt og informanten fikk si det vedkommende hadde på «hjertet», noe vi følte fungerte godt. Et

sentralt stikkord her er åpenhet, som betyr at den som intervjuer i mindre grad på forhånd har bestemt seg for hvilken informasjon vi får inn.

Når vi som intervjuere ble usikker på hva vedkommende mente fulgte vi opp med oppfølgings spørsmål og vi fikk derved umiddelbart frem den «riktige» forståelsen av en situasjon. Det er informanten som i stor grad definerer hva som er den «korrekte» forståelsen og dermed får frem sine tolkninger og sine meninger (Jacobsen, 2012).

Det å kunne gi «nærhet» mellom intervjuer og informant kan bidra til en god atmosfære og gjøre at informanten sier det de faktisk ønsker å formidle. Vi som intervjuere merket at vi kom litt «under huden» på informantene gjennom samtalene. Det er en fordel at metoden er fleksibel, ved at en kan endre problemstillingen og datainnsamlingsmetoden etter hvert som en får vite mer av informantene.

Vi fikk også erfare noen av ulempene med denne metoden. Først måtte vi få kontakt med informantene og avtale tid og sted. Videre måtte vi gjennomføre intervjuene tidlig i prosessen grunnet annen aktivitet i Marinen, som gjorde informantene utilgjengelig på et senere tidspunkt. Alle intervjuene og etterarbeidet etter fullførte intervjuer tok tid og var ressurskrevende. Det at vi kun rakk over et mindre antall informanter, i motsetning til hva en kvantitativ metode ville gitt rom for, gjør at vi kan få en utfordring med representativiteten ved det vi spør om. Altså den eksterne gyldigheten (Jacobsen, 2012). En annen ulempe ved denne metoden vil være at informasjonen vi får inn kan være vanskelig å tolke på bakgrunn av sin nyanserikdom. Vi oppdaget i ettertid at vi har fått inn utrolig mye data på de ustrukturerte/ åpne intervjuene og det kan være utfordrende å få noe fornuftig av slike mengder data (Johannesen et al., 2009). Dette har gjort at vi ikke har kunnet benytte all dataen vi har fått inn grunnet begrensninger i oppgavens størrelse. Et intervju på ca en time under de ustrukturerte intervjuene gav oss utrolig mange ord, og i tillegg var dataene ustrukturerte. Etterarbeidet var derfor mer krevende enn selve intervjuet. Dette gjorde håndteringen av dataene svært omfattende. Blaikies (2014 s.215) beskrivelse av innsamling av kvalitativ data som rotete og uforutsigbar, og ser ut til å kreve forskere som kan tolerere uklarheter, kompleksitet, usikkerhet og mangel på kontroll.

Videre var det essensielt at vi holdt oppgaven på et ugradert nivå. Dataene innsamlet var ugradert men vi måtte hele tiden vurdere om den totale sammensetningen også ble ugradert. Noen av funnen ble tatt bort fra studien, selv om de i utgangspunktet var ugradert, men når den drøftes kunne vi nærme oss en sårbarhet som vi ikke vil synliggjøre i oppgaven.

Videre vil nærhet, som er nevnt som en fordel, også kunne være en ulempe. I noen situasjoner kan nærheten bli for tett. Dette kan skje når en studerer en gruppe over lengre tid og en ender opp med å bli «en av gjengen». I vår situasjon, hvor vi begge har tilhørighet til Sjøforsvaret, var vi allerede kjent med noen av informantene. Dette var noe vi var observant på, da det kan gi uønskede effekter ved at en mister evnen til kritisk refleksjon. Vi prøvde derfor å tilstrebe at den som kjente informanten minst gjennomførte dette intervjuet.

Fleksibiliteten kan også skape problemer ved at en føler at en aldri blir ferdig med intervjuet da det hele tiden dukker opp ny informasjon (Jacobsen, 2012), noe som var meget forskjellig fra informant til informant i vårt tilfelle. De med mer erfaring brukte mer tid da de hadde mer å komme med. Vi opplevde derimot at tidsbruken var god, og vi brukte verken for kort eller for lang tid. Ved de åpne fagintervjuene ble tiden noe overskredet, men informantene gav uttrykk for at dette ikke var noe problem og at det var avsatt god tid fra vedkommende sin side.

5. Presentasjon av empiri

I empiridelen av oppgaven vil vi presentere utvalg av data som er samlet inn og analysert i fase en. Vi vil presentere og fortolke utvalgt data fra fire valgte hovedpilarer; I. Observatørrolle (forfatterne), kvalitative, II. Semistrukturerte- og åpne-intervjuer, III. Fagintervjuer og IV. Rapporter. Vi innledet med følgende problemstilling:

«Hva kan Marinen som organisasjon gjøre for å forbedre security-kulturen?»

Empirikapittelet deles inn i forskningsspørsmål (FS) 1 *«Hva er trusselbildet fra cyberdomenet og innsidetrusselen mot Sjøforsvaret?» og* FS2 *«Hva er kjennetegn ved Marinens security-kultur?»*. Empirien fra FS1 og 2 nyttes for å besvare FS3, og blir drøftet i punkt 6.3 i lys av valgte teoretiske rammeverk.

Presentasjonen av data bærer preg av valgte metode, hvor vi ønsker å belyse FS1, 2 og problemstillingen med intervju resultatene og valgte teori. FS1 og 2 er delt inn under overskriftene: Menneskelige, Teknologiske og Organisatoriske faktorer (MTO) med tilhørende under områder, se tabell 4. MTO-faktorene påvirker hverandre, og empiriresultatene viser at det ikke er et klart skille. Deler av dataen fra intervjuene kunne vært plassert under flere av faktorene, men vi har valgt å kun legge empiriresultatene under en av faktorene for å unngå å gjengi materialet. Vi ønsker å påpeke at denne masteroppgaven blir skrevet på et ugradert nivå og vi kan derfor, under både empiri og drøfting, ikke gå i detaljer på sårbarheter og verdier til organisasjonen.

Faktorer		Beskrivelse	Relevans for FS	Hurtigintervju spm nr:	
M	Kompetanse Forståelse Holdninger	**Først forsøker vi å kartlegge trusselbildet. Videre ønsket vi å undersøke hvilken opplæring de ansatte har fått på security, samt hvilken forståelse de har av innsidetrussel og sårbarheter gjennom å kartlegge security-kulturen.**	1,2,3	1,3,7,8,11, 12,13,14	Leder-, Fagintervjuer og observasjon
T	Teknologi	**Her ønsker vi å se nærmere på den raske teknologiske utviklingen og hvordan den påvirker håndtering av innsidetrussel.**	1	Fagintervju	
O	Prosedyrer Retningslinjer	**Vi ønsker her å undersøke om de ansatte er kjent med prosedyrer og retningslinjer som er blitt gitt og om disse følges.**	1,2,3	5,10,11,16	
	Ansvarsforhold Sanksjoner	**Her ønsker vi å undersøke ansvarsforhold og rollefordelinger. Videre vil vi se nærmere på om det er en rettferdig kultur.**	1,2,3	2,6,9,14	
	Læring	**Her ønsker vi å undersøke lærings- og rapporteringskulturen i Marinen. Hva motiverer eller hindrer rapportering. Blir hendelser rapportert, fulgt opp og tiltak iverksatt.**	1,2,3	15, 18,19,20,21	

Tabell 4: Viser sammenhengen mellom MTO faktorer og spørsmål til informanter opp mot relevant forskningsspørsmål

5.1 FS1: Hva er trusselbildet fra cyberdomenet og innsidetrusselen mot Marinen?

For å besvare forskningsspørsmål en har vi analysert dokumenter som blant annet har støttet seg på Etterretningstjenesten og PSTs trusselvurderinger. I tillegg til E-tjenestens doktrine (2013) og ugradert trusselvurdering (FOKUS, 2015), bidrar NSM og NOU rapportene til å sette trusselen i en samfunnsrelatert kontekst. Resultatene fra dokumentene blir presentert i tabell 4 i punkt 5.1.1, og intervjuene presenteres i tekst i punkt 5.1.2, begge delt inn under MTO som vist i tabell 4.

5.1.1 Rapport analyse

Trusselbildet er i konstant endring og hensikten med dokumentanalysen er å presentere et så oppdatert bilde som mulig av dagens trussel innenfor cyberdomenet, og hva vi står opp imot når det kommer til innsidetrussel. Grunnet oppgavens omfang går vi ikke i detaljer på cybertrusler, men viser til trusselvurderinger og utfordringer den teknologisk utvikling fører med seg for å potensielt se hva vi står ovenfor og hvilke sårbarheter dette gir. Innsidetrussel beskrives i punkt 3.1 s.17.

Etterretningsdoktrinen (2013) innledes av daværende Forsvarssjef General Harald Sunde med at den økende aktiviteten i det digitale rom er et eksempel på at vi står overfor nye utfordringer og trusler. Trusselbildet er i konstant endring og for å presentere et så oppdatert bilde som mulig støtter vi oss på rapporter fra Etterretningstjenesten, som eneste statlige organ som utarbeider trusselvurderinger i tillegg til PST. Etterretningstjenesten gir ut sin årlige ugraderte vurdering de kaller FOKUS. I FOKUS (2015) uttaler de innledningsvis at nettverksbaserte etterretningsoperasjoner blir stadig mer målrettede, og teknisk avanserte, og fremmed etterretning angriper nå daglig norsk infrastruktur. En av FOKUS (2015) sine hoved overskrifter er «trusler i det digitale rom» hvor de innleder med at nettverkbaserte etterretningsoperasjoner er en betydelig trussel mot norske interesser. Den ugraderte vurderingen av videre utvikling i årene som kommer, er at nettverksbaserte etterretningsoperasjoner i all hovedsak vil være knytte til skjult innsamling av informasjon om politiske, militære og økonomiske forhold. Trusselen vil være i form av nettverks-operasjoner og utro tjenere inne i bedriftene (FOKUS, 2015).

NSM har fått i oppgave av Forsvarsministeren å blant annet foreslå sikkerhetstiltak innen deres fagområde frem mot 2020 på bakgrunn av at trussel aktørene benytter mer avanserte metoder enn tidligere, og risiko- og sårbarhetsbildet er blitt mer komplekst. Det gjør at det stilles større krav til forebygging, gjennom både redusering av sårbarheter og

hendelseshåndtering. Dette innebærer blant annet tiltak for å reduserer risikoen for innsidere (NSM, 2015a s.7).

Aktørene vi står ovenfor strekker seg fra overbeviste aktivister og terrorister til organiserte kriminelle, konkurrenter og andre starter, hvor Russland og Kina står bak den mest alvorlige trusselen (NSM, 2015b). Dette uttaler også politiets sikkerhetstjeneste (PST) i sin årlige trusselvurdering for 2015. For det norske Forsvar, herunder Sjøforsvaret, vil angrep som ikke blir stanset kunne i alvorlig grad ramme Forsvarets operative evne både i fred, krise og krig (NSM, 2015b, s21).

Som nevnt i innledningen er sårbarhetene som gjør oss utsatt for angrep enten menneskelige, tekniske eller organisatoriske. Vi har delt inn tabell 5 i MTO og trukket ut av NSM og NOU sine rapporter elementer som beskriver trusselbildet.

	Dok	Argumenter
Menneskelig	NSM 2015b	• Nettverksoperasjoner blir mer og mer målrettet og teknologisk avanserte • Aktørene strekker seg fra overbeviste aktivister og terrorister til organiserte kriminelle, konkurrenter og andre starter, hvor Russland og Kina står bak den mest alvorlige trusselen • Angrep som ikke blir stanset kan i alvorlig grad ramme Forsvarets operative evne både i fred, krise og krig • Menneskets evne til å la seg lure er en sårbarhet som kan utnyttes aktivt gjennom sosial manipulasjon
	NOU 2015:13	• «mennesket er det svakeste ledd», og mennesker gjør feil selv med de beste intensjoner • Menneskelig svikt kan oppstå på grunn av lav brukervennlighet i sikkerhetstiltak og manglende sikkerhetskunnskap • Utfordringer med å følge komplekse rutiner, særlig når de ikke forstår hvordan systemet virker • Sikkerhetsrutiner kan også være vanskelig å følge i praksis • Enkeltindividets holdninger til sikkerhetsarbeidet og sikkerhetskulturen i miljøet vil påvirke sikkerhetsnivået • Konflikter mellom det å prioritere sikkerhetsrutiner og det å få oppgaver gjort tidsnok • Ansatte være tillagt stort ansvar for sikkerhetsnivået. Man bør derfor spørre seg om det alltid er riktig å skylde på menneskelig svikt.
Teknologiske	NOU 2015:13	• Hurtige teknologisk utvikling og digitalisering forenkler hverdagen til enkelt individet, og sørger for en effektivisering slik at samarbeid kan utføres av færre • Den forandrer også måten vi styrer prosesser på, og bidrar til sentralisert kontroll • Utfordringer; Sentrale tjenester for samfunnet, eks telefoni, utfordres av internasjonale aktører som leverer tjenester i Norge uten at norske myndigheter har rettslig kontroll over dem • Videre er vår evne til å holde informasjon konfidensiell utfordret • Etterspørselen etter kunnskap vil øke kraftig og den teknologiske utviklingen vil fortsette i sitt raske tempo • Mennesker har naturlig en viss forståelse av hvordan vi sikrer informasjon i manuelle, papirbaserte løsninger • Digitaliseringen fremmedgjør sikring av informasjon og vi mister oversikt over sårbarhetsbildet • Design og implementasjonsfeil hvor produkter installeres og brukes utgjør en stor sikkerhetsrisiko • Initiale sårbarheter i maskinvaren, applikasjonen eller operativsystemet økes ytterligere ved manglende logging av trafikk og manglende tiltak for å oppdage irregulær bruk og aktivitet • UD: *«Internett er blitt en generator for sosial utvikling og økonomisk vekst, men håndtering av sikkerhetsutfordringene i det digitale rom er en forutsetning for at dette skal skje»* •Økning i antall gjenstander koblet til internett bidrar til å forsterke eksisterende sårbarheter knyttet til informasjonssikkerhet • Andre gjenstander og apparater som er koblet til internett er også sårbare for angrep fra inntrengere uten rettmessig tilgang til systemet • Når gjenstander er sammenkoblet i nettverk blir de sårbare for sikkerhetssvakheter andre steder i nettverket. • De siste årene har datachips og sensorer blitt billigere, bedre og så små at de kan plasseres i smykker, briller, klær eller andre gjenstander som digitale klokker - «wearable» eller kroppsnær teknologi, som gir økt lagring av informasjon og forsterker sårbarheten • Bruken av privat teknologi i jobbsammenheng øker kraftig. • Sikkerhetspolicyer i virksomheter er ofte rettet mot utstyr som de selv eier og/eller har kontroll over • Flere virksomheter har imidlertid utarbeidet sikkerhetspolicyer som omfatter bruk av privat utstyr tilknyttet deres IKT systemer og nettverk
Organisatoriske	NOU 2015:13	• Organisatoriske sårbarheter omhandler manglende forankring og styring av sikkerhetsarbeid i ledelsen •Mangel på bevisstgjøring og tydelig ansvarfordeling kan gjøre sikkerhetsarbeidet ytterligere komplisert •Det er dokumentert at svak lederforankring, organisatoriske forhold samt menneskelige feilhandlinger og ubevissthet, er årsaker til mangelfull sikkerhetsarbeid og uønskede hendelser i IKT systemer

Tabell 5: Empiri forskningsspørsmål 1

5.1.2 Resultat fag-intervjuer

Resultatene fra fag-intervjuene presenteres under MTO-faktorer både på FS1 og 2. Vi har i denne delen av oppgaven trukket frem hva fag-informantene legger vekt på i beskrivelsen av innsidetrusselen fordelt under Menneskelige-, Teknologiske- og Organisatoriske faktorer ref. tabell 4. Det ble innhentet godkjenning fra fageksperter til å bruke person- og organisasjonsnavn i oppgaven, beskrevet i punkt 4.3.5 Anonymitet. Fagintervjuer er gjennomført med:

- Sjef FSA Kommandør Hans Kristian Herland
- Fagdirektør for sikkerhetskultur i Nasjonal sikkerhetsmyndighet Roar Thon
- Sikkerhetsleder i Cyberforsvaret Oberstløytnant Ivar Kjærem
- Avdelingssjef Etterretningstjenesten Brigader Johannes Nytrøen
- Kai Roer, norsk sikkerhetsekspert med fokus på security-kultur

Videre i oppgaven refererer vi til Sjef FSA som FSA, fagdirektør NSM som NSM, sikkerhetsleder CYFOR som CYFOR, og Nytrøen og Røer ved navn. Analysen av datainnsamlingen fra de åpne intervjuene ble gjennomført ved koding med hovedinndeling av informasjonen under MTO faktorene. Ettersom intervjuene var åpne referer vi ikke til konkrete spørsmål, men trekker frem informasjon som besvarer faktorene og deres underpunkter; **Menneskelige**; *Kompetanse, forståelse, holdninger,* **Teknologiske** og **Organisatoriske**; *Prosedyrer & retningslinjer, ansvarsforhold & sanksjoner og læring*.

Menneskelige faktorer:

Kompetanse:

I det åpne intervjuet med NSM fremheves det at kompetanse er bare et element i kultur bygging, men essensielt. NSM peker til at det eksisterer en rekke sikkerhetstiltak av teknologisk og fysisk art, men du er fortsatt avhengig av ansatte som forstår hvordan å ta det i bruk i praksis. *«For eksempel kan vi gi statsministeren den sikreste mobilen, men vi er fortsatt avhengig av at hun forstår at hun ikke kan sitte på Gardermoen og føre en sensitiv samtale så tjue andre kan høre den samtalen»* (NSM).

I intervjuet med CYFOR fremkommer det endring i håndteringen av sårbarheter i informasjonssystemene da det ble iverksatt et arbeid med operasjonssikkerhetsvurderinger, 2003/2004, og kunnskapen ble spredt til flere avdelinger. CYFOR stiller spørsmålet hvis du ikke kan se sårbarheten, eller har kunnskapen om hvordan det kan utnyttes, har du da kontroll på det? *«Hvis du har god kompetanse, da vet du hvordan det fungerer, og da kan du*

kanskje si du har kontroll. Sikkerhetselementene blir kanskje oversett i enkelte tilfeller fordi vi ikke har kunnskap om dem» (CYFOR). CYFOR underbygger at kompetanse bare er et element i security-kulturen.

Forståelse:

I de åpne intervjuene ble forståelse gjennomgående trukket frem av informantene, og fremkom klart som et av premissene for å håndtere innsidetrussel. NSM opplever at forståelsen rundt begrepet security er at det skal håndteres av noen få, at det er noe sært, noe som er på siden, men påpeker at sikkerhet er noe enhver offiser og leder skal ha i bakhodet. Det er de små, daglige dryppene som er viktig. Det er viktigere med ledere, mellomledere som er fokusert på sikkerhet i den daglige virksomheten enn å ha fått en masse penger for å gjennomføre en sikkerhetskampanje er NSMs erfaring. *«Jeg synes Forsvaret har vært flinkere til å snakke om lederutdanningen sin enn å utøve den. Ikke lett å finne en helhetlig kultur, du vil ha så mange forskjellige kulturer basert nettopp på utførelse av lederskap, og jeg tror veldig på det at du kan endre kulturer. Det tar tid, men samtidig kan du endre kulturer veldig raskt avhengig av hvordan lederen opptrer og hvor bevisst lederen er på det. Så det med eksemplets makt ved å adressere og ta opp ting folk kjenner seg igjen i, og være både motiverende og støttende er viktig».*

Forsvaret skal ikke bare beskytte organisasjonen verdier, men evne å forvare og beskytte nasjonen. *«Så jo mer man greier, når man snakker om sikkerhetskultur, i hvert fall i organisasjons perspektiv, å skape forståelsen for at man evner å beskytte de verdiene»* (NSM). Forsvaret er en unik organisasjon når det kommer til samhold og det at man trener for krig. For å løse et oppdrag kreves en forståelse av hva man står opp imot.

«Kunnskap om trusselen mot digitale systemer er viktigste faktor til at vi ikke bruker tid og penger på å beskytte det. Handler om å beskytte systemer også, ikke bare kommunikasjonen. Forståelse av trussel for å kunne beskytte seg» (Nytrøen). Nytrøen mener mangel på oppfattelse av trussel er Sjøforsvarets største utfordring, og det handler om fraværet av den type erfaring. Både NSM og FSA viser til militære styrker som har opplevd trusselen på nært hold, hvor Sjøforsvaret ikke har tilsvarende erfaringer med opplevelser av fare for egen sikkerhet i like stor grad. *«Vi er generelt for dårlig på security i Forsvaret»* (Nytrøen).

Holdninger:

Det fremkom klart fra de åpne intervjuene at de ansattes holdninger i utgangspunktet ikke er av en ødeleggende karakter for organisasjonen, men påvirkes av miljøet, og ikke minst av

hvordan de blir behandlet. I følge FSA er det generelt sagt en vilje til å lekke, å gi fra seg gradert informasjon. *«Det er da de mest betrodde individene vi har, de som i ihvertfall ikke skulle lekke lekker, da har vi en utfordring»* (FSA). Følgende eksempler kan søkes opp på internett: E14 saken med E-tj – stay behind tematikk. Arkiv saken på Langkaia. E-bataljonen saken for to år siden – lekkasje. I følge FSA viser det jo at når man føler *«min»* sak er under trussel, så er de fleste villig til å gå veldig langt. «*Det ikke fordi de i og for seg vil Forsvaret noe vondt, men de kjemper for sin sak. Vi ser det også i forbindelse med lokaliseringssaker, når baser skal ligge der eller der. Viljen er der»* (FSA).

Ved bruk av eksempler viser NSM til hvordan historien forsterker betydningen av å ivareta ansatte for å redusere risiko. *«Eksempel med amerikanernes liste tilbake til 1945 over personer som har vært dømt for spionasje. Hvis man ser på årsaken til at de har endt opp med å gjøre det de har gjort, så er det ikke ideologi, ikke penger, det er hevn og misnøye. Hevn fordi de føler seg forbigått, ikke sett, eller ikke ivaretatt, misnøye i forhold til det. Så har det etter hvert for noen blitt en faktor at de også har fått penger, så det blir bare en ytterlige faktor. Ideologi kommer ekstremt langt nede på lista. Glade og fornøyde medarbeidere, så satser du på arbeidsmiljøet, en god kultur på arbeidsplassen så reduserer du sannsynligheten for innsidetrusselen»* (NSM).

Også ifølge CYFOR kan lekkasjer oppstå på bakgrunn av misfornøyde ansatte. *«Og det er i hvert fall viktig å fange opp dersom det er noe som glipper for slike misfornøyde ansatte, vi vil jo ha fornøyde ansatte, er de fornøyde er det også mer sannsynlig at de følger reglene, og ergo kan det bli mindre lekkasjer. For å se de ansatte og ivareta de ansatte, det er klart at det er en viktig del av sikkerhetsarbeidet det også sett opp mot innsideproblematikken»* (CYFOR). Roer understøtter trusselen misfornøyde ansatte utgjør når det kommer til innsidetrussel; «*Disgruntled workers" har større sannsynlighet for å utøve misnøye mot sjefen – da ved sabotasje, manipulasjon/endring av informasjon, trojanske bomber (går av et år senere)."* Innsidetrusselen er en av truslene som må håndteres og forstås på alle nivåer». «*Vil aldri kunne fjerne innsidetrusselen – men å begynne å skape dem selv må vi håndtere»*. (Roer).

Teknologiske faktorer:

Resultatene fra de åpne fagintervjuene belyser både utfordringer og muligheter det teknologiske aspektet gir, samtidig som informantene fremhever utfordringene med ressurser, forståelse for behov og beslutninger på høyeste hold for å implementere endringer. I forhold til FSAs syn på data og cybersikkerhet, mener de at verktøyet de bruker til vanlig er

ganske godt beskyttet ettersom det ikke er direkte oppheng i internett. *«Men det er helt umulig å verne seg mot cybertrusler så lenge du har vilje, og kamera»* (FSA). Enkelte elementer som utgjør en risiko er enklere å iverksette tiltak rundt enn andre. *«Vi har gjort en del grep når det kommer til minnepinner, som har virket. Neste steg må i så fall være å umuliggjøre bruk av minnepinner. Det er teknisk sett ikke så vanskelig å gjøre i Forsvaret. Vi har jo eksempler på at folk har brukt minnepinner feil, mindre nå enn før, men det er ubevisst, og ikke gjort med forsett. At du må trykke kode, og det bare er den minnepinnen som går, gjør jo at folk er mer bevisst bruken av minnepinner, som egentlig er den store utfordringen i praksis»* (FSA). FSA påpeker også utfordringen med Googles «kontroll» over oss, og hvordan telefonen kan fungere som en opptaker. Et annet eksempel FSA viser til er radar-systemene på fregattene; *«Når det kommer en ny programvare fra et eller annet sted på kloden, og inn skal det, hva det gjør, vet ikke vi»* (FSA).

Den teknologiske utviklingen fører ikke bare med seg sårbarheter og nye trussel aspekter, men som nevnt også muligheter. Utfordringen her er ressurser og forståelsen for hva som er behovet for å håndtere truslene. *«Tilgangen til informasjonen blir større, og ikke minst muligheten til å påvirke. Med totalnettverksbaseringen av Forsvaret øker sårbarheten for utnyttelsen ved at flere personer får tilgang»* (CYFOR). Det vil alltid være løsninger, utfordringen er som sagt ressurser, men også at løsningene ikke blir et hinder for Forsvaret operative evne. «*Vi har ikke implementert seksjonering og styring av tilganger noe vi kan gjøre, men det krever ressurser. Fokus har vært på funksjonalitet og tilgjengelighet. Teknologiske løsninger er på vei, men med en gjennomsnittlig utviklingstid på et IKT-system i Forsvaret på 8 år, vil du få 8 år gamle krav. Vi må lage krav som kan utvikles underveis»* (CYFOR).

Roer har utviklet et måleverktøy basert på rammeverk for security-kultur. Det handler blant annet om å akseptere at trusselen er tilstede for å kunne skape en kultur rundt det. *«Det er viktig å ikke ta integriteten i systemene for gitt, man må forstå svakhetene i teknologien og akseptere at det ikke er noen garanti for at uvedkommende kommer inn i systemene»* (Roer).

I følge Nytrøen er digitale systemer, som ikke har sikkerhet rundt seg, en direkte trussel mot oppdraget og videre norske liv og virksomhet som kan medføre tap av liv og helse. Nytrøen nevner at generelt sett har Snowden avsløringene gitt verden innsikt i de digitale sårbarhetene og ført til økt fokus på å beskytte digitale systemer. *«Forsvaret er fremtredende på krypto»*, sier Nytrøen, *«men vestlige land har hatt fortrinn på å lage og knekke krypto. Det et tidsspørsmål før kryptert informasjon er tilgjengelig – kulturbegrepet er altomfattende*

i en slik sammenheng. Industriene ut av eget kommersielle behov utvikler krypto som gjør det nødvendig med store ressurser for å klare å forsere beskytta informasjon på digitale systemer». Den teknologiske utviklingen er en faktor som Forsvaret ikke kommer utenom. *«Vår oppgave er også å få informasjon som søkes holdes skjult (ergo er det andre som er interessert i vår info). Digitaliseringen er nær ved å bli total, derfor er cyber en av de viktigste måtene å få tak i informasjon. Erkjennelse av at informasjonen du har en verdi for andre (eks våpen som mener de ikke har noe å skjule). Hvis ikke klarer du ikke bygge opp en beskyttelseskultur som vil gjøre deg i stand til å beskytte deg mot trusler utenfra»* (Nytrøen).

Både NSM og egen observasjon viser at Forsvaret i enkelte sammenhenger mangler systemer til å håndtere gradert kommunikasjon. *«GIS er ansvarlig for å sette sikkerhetskravene til systemene – har økonomiske konsekvenser – fører til reduksjon i sikkerhetskrav for å få produktet – indikator på at man ikke har forstått risikoen. Sikkerhet kan ikke ha ligget som et bærende krav når man ikke kan kommunisere på tvers av forsvarsgrener»* (Nytrøen).

Organisatoriske faktorer:

Prosedyrer og retningslinjer:

Det fremkom av de åpne fagintervjuene et dilemma rundt prosedyrer og retningslinjer for å håndtere innsidetrusselen. Er det tilstrekkelig å sørge for at eksisterende prosedyrer blir innført eller er det behov for implementering av nye? FSA tar utgangspunkt i at Sjøforsvaret har et form for regelsett rundt praksisen ved mobil-/pc-/internettbruk. På bakgrunn av intervjuene i Marinen fremlegger vi funnet om ulike måter/praksiser å gjøre ting på. Dette påpeker FSA at er viktig å få frem. *«Det er ganske klare regelsett rundt det med radiosender som egentlig er det vi snakker om, og kamera»* (FSA). FSA mener også at det må lages et fornuftig regelsett for praksisen, og dette må følges opp. I følge FSA er ikke nødvendigvis løsningen strengere krav, ettersom det kan fremkomme at eksisterende krav ikke blir praktisert, og tror det er utfordrende nok å forklare de som er. *«Hadde vi klart å praktisere de slik de er hadde vi kommet langt. Skal alt være forbudt, nei, men de må forstå hvorfor de skal ta det av og hvorfor det er forbudt. Ja, det er forståelsen, at de tenker på det selv og folk hjelper hverandre og minner hverandre på det»* (FSA).

I følge CYFOR bør vi definitivt stille høyere krav i forhold til bruk av mobil, pc, internett og lignende. I tillegg mener CYFOR at eksterne leverandører er en utfordring når det kommer til innsidetrussel, og selv med egne regimer for å håndtere risikoen tror CYFOR at mye av kontrollregimet blir for skjematisk, *«og hvis vi ikke klarer å se mennesker bak skjema,*

hvordan klarer vi å se på hvordan et menneske kan være en innsidetrussel eller ikke» (CYFOR).

Ansvarsforhold og sanksjoner:

Informasjonen fra fagintervjuene understreker viktigheten av klare ansvarsforhold og et internt regime som kan bidra til å redusere risikoen for innsidetrussel. FSA påpeker at det er viktig å vite hvem vi har blant oss, og det er en utfordring at vi med utviklingen introduserer sivile strukturer som gir økt og flere risikoer for Forsvaret. FSA tror ikke det er en vei utenom, men vi må bare finne en eller annen måte å håndtere det på. *«Det er en kjempe utfordring for Sjøforsvarets base selv om de er ganske flinke til å ha en kommando linje i organisasjonen for håndtering av dette»* (FSA).

FSA jobber mot Forsvaret som en blokk og har en del aktivitet mot Sjøforsvaret når fartøyene skal utenlands. Spesielt når de skal østover informerer FSA om hva de må være forberedt på å møte, hva en opponent kan finne på å gjøre å ikke gjøre, både mens de er der og i etterkant. FSA gir også ut ukesbriefer, ikke så ofte som de skulle ønske lenger, hvor de tar opp ulike temaer som blir sent sikkerhetsorganisasjonen. I følge FSA må vi jo forvente, og derfor ha som en arbeidshypotese, at vi har noen på innsiden. *«Det er derfor viktig å bruke klareringsinstituttet, og stresse sjefenes ansvar, dette er et sjefsansvar, og autorisasjon skal de gjennomføre. Der har jo Forsvaret vært ganske dårlig, men blir sakte men sikkert bedre. Den samtalen håper vi på sikt blir skarpere og skarpere og ikke en sånn koseprat alene»* (FSA).

NSM legger igjen trykk på viktigheten av begrep og forståelse for prosessene i risikohåndteringen. *«Det beste virkemiddel mot innsidetrussel, da må man definere hvem som er innsidetrussel, hvis jeg skulle starte med å snakke om sikkerhetsklarering og hele den prosessen der, så handler den om å redusere risiko. Den prosessen er ikke der for å hindre allerede eksisterende mennesker som jobber for andre lands etterretning. Sikkerhetsklareringsprosessen skal redusere risiko på enkelte elementer, på mennesker som har en for høy grad av manglende lojalitet og dømmekraft i enkelte situasjoner som kan utnyttes av en aktør"* (NSM).

CYFOR trekker frem at klarerings og autorisasjonsregimet blir for skjematisk, og det ligger til grunn en ganske enkel opplæring for de som står for det arbeidet. *«Min påstand er at du må ha veldig lang erfaring innen dette for å kunne begynne å se noe som dette, hva som pågår. Vi er ikke der hvor vi har et godt bilde enda».* (CYFOR).

Nytrøens har et operativt fokus, og viser til viktigheten av security for en organisasjon som Forsvaret. *«Har vi ikke cyber sikkerhet kan vi i dagens samfunn ikke påregne sikkerhet for eget oppdrag. Risikoen er uendelig mye større når vi er i internasjonale operasjoner. Cyber sikkerhet som security aspekt handler om å lykkes med oppdraget og spare norske liv. Safety/HMS har samme formål å redusere risikoen for menneske og materiell»* (Nytrøen).

Læring:

Faginformantene er enige om at det eksisterer uklarheter og en blanding av begrepsbruken safety/security, i tillegg til at security ikke har fått nødvendig fokus og prioritet. Dette skaper en utfordring for organisasjonens evne til læring, og å kunne utvikle en robusthet mot innsidetrusselen. «*Vi ønsker å komme dit hvor security-miljøet gjør handlinger på bakgrunn av en vurdering rundt sårbarheter og risiko. Det vi skal få til er å bidra til å sikre operativ evne, og at vi har tilgang til ressursene vi skal når det gjelder, lykkes vi ikke nå kan det fort være kjørt»* (FSA).

CYFOR viser til at skifte med økt internasjonal aktivitet sammen med den teknologiske utviklingen skapte et fokus på funksjonalitet og å få ting til å fungere, og førte nok til at security-kulturen har lidd de senere årene. *«Med et sånt fokus på funksjonalitet, så er det større mulighet for ufrivillig innsidetrussel, som i og for seg ikke er den farligste innsidetrusselen, men potensialet for at du kan lekke mye informasjon er tilstede»* (CYFOR). Nytrøen hevder også at uklarhetene rundt begrepene lager mer forvirring, og vanskeliggjør håndteringen av innsidetrusselen.

I følge Roer handler sikkerhetskultur om virksomheten og personene sin forståelse, og forståelsen for de svake sidene ved teknologien. *«Det er folk som er en trussel, og det handler om å lære folk å finne/kjenne dem igjen»* (Roer). I følge Roer er det kritisk å bygge kompetanse på security, og det må være noen som kan forstå teknologien for å gjøre vurderingene. Det må et gjennomgående fokus på security i all utdanning, for å ha en kompetanse og forståelse til kontinuerlig organisatorisk læring.

5.1.3 Oppsummering hovedfunn forskningsspørsmål 1

Hovedfunn i empiri FS1
• Innsidetrusselen fra eksterne aktører, som for eksempel Russland og Kina, er høy • Marinens manglende kunnskap og forståelse øker de menneskelige sårbarhetene for innsidetrussel • De mest betrodde individene lekker informasjon • Lekkasjer kan oppstå på bakgrunn av misfornøyde ansatte • Teknologisk utvlklingen skaper muligheter for en trusselaktør, hvor Forsvaret også kan benytte seg av muligheten denne utviklingen gir til å forsvare seg • I enkelte situasjoner mangler Forsvaret systemer for å håndtere gradert kommunikasjon • Ulik praksis av føringer og prosedyrer kan skape forvirring ved en tilsikted uønsket hendelse • Forsvaret har insidere, men ledernes manglende forståelse undergraver ansvaret for autorisasjonsarbeidet

Tabell 6: Oppsummering hovedfunn FS1

5.2 FS2: Hva er kjennetegn ved Marinens security-kultur?

FS2 er delt inn i følgende to deler: En kort del hvor vi har trukket frem en tidligere rapport på Sjøforsvarets security-kultur, punkt 5.2.1, og den andre delene som presenterer utvalgt empiri fra datainnsamlingen, punkt 5.2.2.

5.2.1 Rapport analyse

Det er skrevet en del rapporter/masteroppgaver som omhandler både Forsvaret og Cyberdomenet, men på et mer overordnet, strategisk og politisk nivå. Vi har kun trukket frem en rapport, hvor de forsker på security-kulturen i Sjøforsvaret og konkluderer med tiltak. Funnene i studiet gav oss et utgangspunkt for å se nærmere på security-kulturen i Sjøforsvaret.

Det ble i 2015 skrevet en studie om «Kultur for forebyggende sikkerhetstjeneste i Sjøforsvaret» (J.Marøy, S.Warholm 2015) som omhandlet i hvilken grad kulturen for forebyggende sikkerhetstjeneste påvirkes av endringer i den sikkerhetspolitiske situasjonen. Studien har sett på hvordan kulturen arter seg i organisasjonen, og om endringene i den sikkerhetspolitiske situasjonen har påvirket dette. Studien bestod av en spørreundersøkelse hvor resultatet viser at Sjøforsvaret har en vei å gå for å kunne tilfredsstille sikkerhetslovens minimumskrav til forebyggende sikkerhet, og det er et behov for å iverksette tiltak for endring. Studien tok for seg den høyre delen av Kaufmann & Kaufmann (2009) sin modell om utvikling av kultur hvor man ser på hvordan det ytre miljøet påvirker medarbeiderne og

kulturen. Oppgaven foreslår videre forskning på modellens venstre del hvor man fokusere på hvordan ledernes kunnskaper og holdninger påvirker medarbeiderne og kulturen.

Et av funnene deres var at tilliten til organisasjonens evne til å beskytte seg mot sikkerhetstruende virksomhet var lite tilfredsstillende. Derimot hadde den sikkerhetspolitiske utviklingen påvirket kulturen og medført en vesentlig økning i sikkerhetsbevisstheten og rapporteringsviljen hos ansatte. Resultatene viste også at det var lite forskjell mellom ulike avdelinger og tjenesteområder, men de største forskjellene var mellom ulike militære utdanningsnivåer. Erfaringen til forfatterne av oppgaven var at det i teorien innenfor sikkerhet er mer passende for safety enn security. Forfatterne referer til kultur som et komplekst fenomen som krever en kombinasjon av flere sekvensielle tiltak over tid for å oppnå ønsket effekt og konkluderer med følgende tiltak:

- Holdningsskapende tiltak i organisasjonen
    - Informasjonskampanjer vedrørende riktig bruk av minnepinner, mobiltelefoner, dokumentsikkerhet og sosiale medier
- Få forebyggende sikkerhetstjeneste inn på fagplanen, i alle utdanningsnivåer
- Utarbeide e-læringskurs om forebyggende sikkerhet, som supplement til autorisasjonssamtalen.

5.2.2 Resultat intervjuer

I denne delen av empiripresentasjonen fortsetter vi med fase en, og fremlegger resultatene på FS2 fra 36 hurtig intervjuer, fem lederintervjuer og utvalgte deler av fem fagintervju. Videre vil observasjoner fra observatørene fremkomme her. Resultatene er inndelt i MTO ref tabell 4. Beskrevet under punkt 4.3.6 analyseprosessen, kan kvalitative studier produsere enkle tabeller med frekvens og prosent for å oppsummere noen av funksjonene i ikke- numerisk data (Blaikie, 2014). Noen av spørsmålene under hurtigintervjuene var lukkede spørsmål hvor informanten kunne gi korte svare som eksempel ja, nei eller vet ikke. Informantene ble allikevel oppfordret til å utdype svarene sine. Basert på besvarelsene under hurtig intervjuene (36 stykker), fremstiller vi deler av resultatene i form av statistiske diagrammer.

Menneskelige faktorer:

Under menneskelige faktorer har vi valgt å se nærmere hvilken opplæring de ansatte har fått på security og innsidetrussel, samt hvilken forståelse og holdninger de har til security og innsidetrussel i forhold til trusselbildet. Menneskelige faktorer er delt inn i; Kompetanse, forståelse og holdninger (ref tabell 4).

Kompetanse:

På spørsmålet om hva informantene mener er innsidetrussel var det flere varierende svar (Spørsmål 1). Mange informanter fra alle tre avdelingene uttaler at innsidetrussel er de ansatte i avdelingene som sprer informasjon, både bevisst og ubevisst. Det trekkes frem press fra utsiden og salg av informasjon, uærlighet blant ansatte og spion virksomhet (91,141, 177, 353, 433,393). Andre informanter trekker frem at systemet ikke er godt nok (111), noe som kan gjøre at ansatte eller systemet gjør feil, mens andre trekker frem viktigheten av å ikke lekke informasjon muntlig eller i sosiale media (383,423).

NSM peker på utfordringen ved at begrepene brukes uten å vite hva man egentlig snakker om. NSM ønsker fokus på adferds delen av kulturbegrepet, «*hva ønsker vi å få ut av å jobbe med sikkerhetskultur*» (NSM). Kompetanse er bare et element i kultur bygging, men essensielt. *«Det er mye kunnskap som må til for å vite hvordan vi får de menneskene til å ha den adferden. Det er mangel på kunnskap som gjør at folk tror det er sikkert å snakke på telefonen, og enda sikrere hvis det er en tjenestetelefon. Mobil, internett handler mer om kunnskap. Handler om å finne den gylne middelvei, og forklare de enkelte situasjonene.* V*åre forsøk handler om å få opp oppmerksomheten ved å bruke eksempler*» (NSM). Det er viktig å kunne forklare hvorfor, og NSM bruker mye eksemplets makt til å få folk til å forstå at det er mennesker der ute som vil legge puslespillet bestående av brikker den enkelte ansatte legger ut. NSM påpeker også at det er nødt til å være en rød tråd i sikkerhetskulturen. *«Du kan ha så god adferd du bare vil, men hvis du løper rundt med en geotag du ikke vet om er du ute å kjører»* (NSM). Vi viser til uttalelse fra hurtigintervjuene hvor det blir sagt i en avdeling at de ikke har noe å skjule; *«Eneste verre kommentaren enn det, har jeg hørt fra norske byråkrater som sier at vi forvalter ikke noe av verdi»* (NSM).

FSA liker dårlig blandingen av safety og security, det skaper forvirring. FSA ser at ute på avdeling blir han som skulle drevet med security ofte spist opp av safety-miljøet og alt mulig annet. FSA ønsker at security skal gå mer over i et operativt domene bort fra ren forvaltning og kun regelfokus. *«Forsvaret er nødt til å fokusere på at vi har en trussel, at vi har en risiko, og se på hva det betyr for oss, hva må vi gjøre nå, hva må ansatte som skipssjef gjøre med den trusselen. For eksempel en vurdering som: Skal jeg gå til den kaien der, nei jeg skal ikke gå til den kaien, jeg skal gå dit fordi «begrunnelse».*

CYFOR mener Sjøforsvaret har gjort et stort arbeid knyttet til sikkerhetsledelse og sikkerhetsstyring, men tror det å blande safety og security slik de har gjort i sikkerhetsstyringen er feil. *«Det er selve direktivet – Krav til sikkerhetsstyring i Forsvaret*

som blander. Risikovurderinger i et safety perspektiv kan bli noe helt annet enn risikovurdering i et security perspektiv. I et safety perspektiv skal du ivareta liv og helse, i et sec perspektiv så skal du ivareta faren for kompromittering, det er noe som gjør at du i et safety perspektiv vil du låse opp døra, men i et security perspektiv vil du låse døra, og holde den låst. Det er viktig at safety og security prater sammen» (CYFOR) Direktiv- krav til sikkerhetsstyring i Forsvaret (2010) er nå oppe til revidering med antatt ferdigstilling i 2017. *«Vi har på mange måter ikke innført sikkerhetsstyring slik direktivet fastsetter det, vi kommer til å jobbe ganske hardt etter safety/security søylene i Forsvaret, ellers kommer vi til å ha en samordning på tvers på de ulike nivåene. Men vi mener skille mellom safety og security er viktig i så måte, men som jeg sier er dialogen imellom også viktig»* (CYFOR).

Roer mener også det trengs en opprydning i begrepsapparatet, og han skiller safety med HMS/uhell, ulykker, mens security handler om abstrakte verdier, informasjonssikkerhet, ondsinnede handlinger. I følge Roer handler sikkerhetskultur om virksomheten og personene sin forståelse, og forståelsen for de svake sidene ved teknologien. *«Det er folk som er en trussel, og det handler om å lære folk å finne/kjenne dem igjen»* (Roer).

En leder (37) uttrykker at trusselen er høyere avhengig av geografisk plassering og antall personer ombord. *«Det er å mye flere mennesker ombord på våre enheter enn det var for bare få år siden»*. Lederen (37) påpeker spesifikk «*outsourcing*» som en faktor. «*Fordi samfunnet har blitt som det har blitt og fordi organisasjonen er blitt mye mindre*». *«Vi er mer sårbare»*. En annen leder (8) uttrykker også at eksternt personell og leverandører er en «*kjempe utfordring*», men «*jobbes med kontinuerlig*».

Forsvarssjefen utgir en sikkerhetspolicy som skal være kjent i organisasjonen. Sikkerhetspolicyen skal være en del av opplæringen til de militære ansatte og den skal være oppslått på veggen i samtlige avdelinger. På nivå 5 kontrolleres dette under internrevisjon sikkerhetsstyring. I 2015 hadde Sjøforsvaret en egen policy som bygget på forsvarssjefens policy, men med mer konkrete målsettinger. I 2016 valgte Sjøforsvaret å benytte Forsvarssjefens policy. På spørsmålet om hva er Forsvarets/Sjøforsvarets sikkerhetspolicy svarte 89% vet ikke, mens 11% hadde noe mer utfyllende svar (diagram 1). Disse 11% tilhørte avdeling 1 og 3, noe som tyder på at policyen er noe mer kjent i disse avdelingene enn i avdeling 2. Sitater som «*årvåkenhet og monitorering*» (111) og «*skal rapporteres til ASL*» (161) ble uttalt. En informant (333) uttaler at «*Sjøforsvarets policy er det samme som Forsvarets policy*». Videre sier vedkommende at: «*Mitt inntrykk er at veldig mye av det vi snakker om og det som står, det blir ikke overholdt om du er admiral eller menig. Det spiller*

liten til ingen rolle, vi har like liten forståelse og etterlevelse av sikkerhetskulturen vår, og alle synder».

Diagram 1: Resultat spørsmål nummer 7 hurtig intervju.

Vi spurte informantene om de har fått opplæring i innsidetrussel og hvor ofte de har fått denne opplæringen. 44% svarer nei, 25% sier ja mens 31% hadde andre svar (diagram 2).

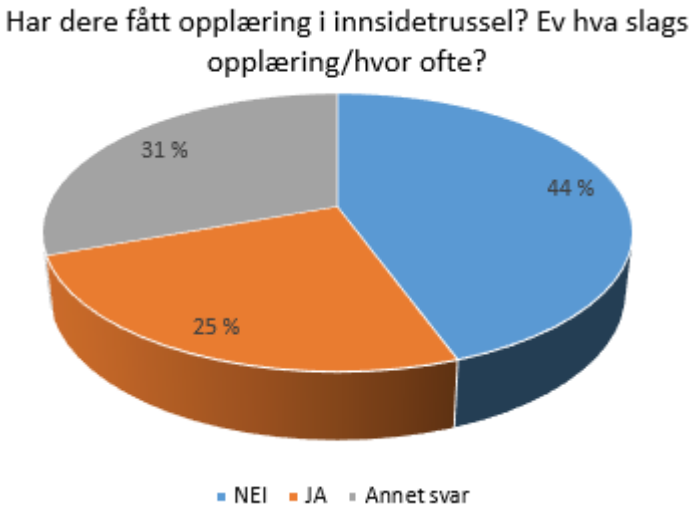


Diagram 2: Resultat spørsmål nummer 8 hurtig intervju.

Svarene fra informantene gir et bilde av at det tilsynelatende er litt tilfeldig når og hvor de får tilført kunnskap rundt temaet security og innsidetrussel. Av de 25 % (JA) og 31% (andre svar) er det mange som sier at opplæringen ofte omhandler føringer på bruk av mobil, internett og sosiale medier. Det er alt fra brief på avdeling, brief om innsidetrussel fra PST, månedlig brief fra LKM, bransjespesifikke kurs på avdeling, autorisasjonssamtaler og GDS. Sikkerhetslederne henviser til ASL/DSL kurs og uttrykker at det omhandler «*sikkerhetsloven, lite om trussel (121)*». Det uttales også at langt fra alle sikkerhetsledere har ASL/DSL kurs, men at denne kompetansen sitter på land i noen avdelinger. Leder (19)

uttrykker at det «*har vært tilstrekkelig, du har «kunnskapshubben» din som du henter kunnskap til enhver tid og det satser vi å videreføre. Men det krever også at de følger opp enhetene ute og bygger kompetanse*». Informant 252 frem at det «*må større kunnskap over hele linja, heve kunnskapen om faren og det nytter ikke å sende én person på kurs*».

FSA kjører kurs for personell som har en sikkerhetsrolle og for de som jobber i sikkerhetsorganisasjonen. FSA jobber veldig mye med toppsjefene, tilsvarende General Inspektøren for Sjøforsvaret (GIS), for å få de til å ta jobben og ansvaret sitt rundt sikkerhetsstyring. Det vil ifølge FSA gjøre det mulig å få til, selv om FSA er klar over at de har en kjempe utfordring på mellomnivået av sjefer. FSA ser helst at security blir en naturlig del av utdanninger/ øvelser i Forsvaret og at alle Forsvarets utdanningsinstitusjoner legger dette inn i fagplanene sine. Dette kan bidra til at elevene helt naturlig tenker igjennom temaet. «*Det må ikke bli et særskilt emne, det skal være et helt naturlig emne. Vi er i ferd med å prøve å se hvordan vi formelt kan få det inn i fagplanene. Men vi er ikke så mange, så er litt begrenset hva vi får til, men vi utdanner mange på disse kursene vår*». FSA forsøker å opptre i ulike sammenhenger hvor de treffer folk og selger det glade budskap.

CYFOR uttaler også viktigheten ved bruk av eksemplets makt. I følge CYFOR så må det være en rød tråd for å sikre ivaretakelse av security aspektet gjennom hele utdannelsen. *«Hvis alle har en basis kunnskap de har fått refresha opp gjennom hele utdannelsen og tjenesten, så skaper det en felles forståelse* (CYFOR).

CYFOR ønsker på lik linje med FSA at security blir en del av en gjennomgående utdanning. *«Hvor er den gjennomgående sikkerhetsutdanningen? Er det noen sikkerhetstankegang på hvor Forsvarets personell skal utdannes innenfor sikkerhet? Nei, det er ikke det. Det er ingen helhetstankegang bak det. Det er ikke en rød tråd gjennom dette her for å sikre at vi har en god ivaretakelse gjennom hele utdannelsen. Det handler om hvordan forstår vi hverandre når vi snakker om dette»* (CYFOR). Den røde tråden må ikke være gjennomgående bare i organisasjonsstrukturen, men i utdanningsløpet og kulturen. *«Den røde tråden gjennom det hele er viktig for å skape en god sikkerhetstjeneste og sikkerhetskultur, for det hele bygger jo på kompetanse. Den kompetansen må tilføres gjennom hele utdanningsløpet. 100% stillinger vil bidra til forbedring, og et fokus utover kontrollfunksjonen hvor det dannes et bilde på tilstanden, og ikke minst det mellommenneskelige. Sikkerhetskulturen er essensiell for måloppnåelse. Det er nok ressurser, men utfordringen er å vite hvor man skal fokusere, hvor læringen skal være og prioritering av ressursene»* (CYFOR).

I følge Nytrøen har det vært manglende undervisning på Krigsskole og Stabsskole når det kommer til trussel og security på bakgrunn av at vi har hatt 70 år med fravær av noe vi oppfatter som en trussel. Nytrøen mener det er en indikator på manglende risikoforståelse. *«Mentale tenkningen over tid. Fravær av opplevd trussel gjør noe med sikkerhetskulturen, og at det ikke prioriteres ressurser til å beskytte oss»* (Nytrøen).

Forståelse:

Før vi stilte informantene spørsmålet; tror du innsidetrussel er en reell trussel du kan møte? leste vi kort opp NSM sin definisjon og forklaring på innsidere ref punkt 3.1 Terminologiforståelse: Innsidetrussel. 61 % svarte JA om det er en reel trussel de kan møte, mens 8 % NEI, og 31 % var usikker (Diagram 3 venstre side). På spørsmålet om Sjøforsvaret er sårbare for innsidetrussel svarte 94% kontant JA, 0% svarte NEI, mens 6 % var usikker, disse tilhørte avdeling 2. (Diagram 3 høyre side)

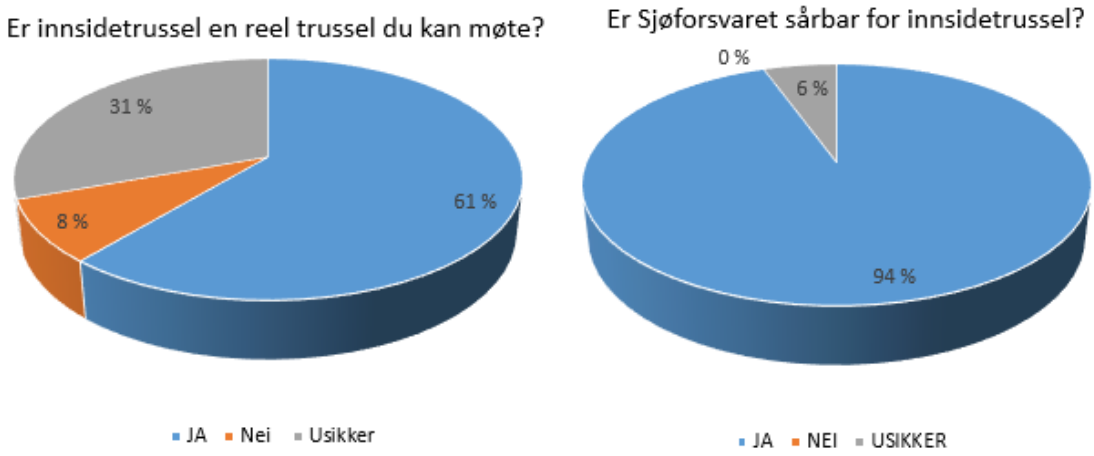


Diagram 3: Resultat spørsmål nummer 1del 2 og 3 hurtig intervju

Det er langt flere (94%) som mener at Sjøforsvaret er sårbar for innsidetrussel enn de som mener at det er en reell trussel de selv kan møte (61%). Noen av svarene tyder på at enkelte informanter ikke tror de er personlig sårbare for trusselen, samtidig som de uttrykker at de har vært kontaktet av russisktalende på Facebook. Andre er overbevist om at det er en trussel og at forsvarets lavgraderte systemer blir tappet for viktig informasjon, og at dette lekkes. En informant (212) sier *«vi har ikke mye kompromitterende utstyr her hos oss, utenom i radio, så om de får vite noe om annet utstyr så er ikke det så kritisk»*. En annen (262) sier at: *«Ja det er en trussel, det handler mye om tillit, gjensidig tillit, det er mye man håndterer som menig, matros, befal. Tenker det er viktig å bli opplyst om de forskjellige farene ved det, hvilket ansvar en har i de forskjellige tingene»*. Noen informanter trekker frem at forsvaret er like sårbar som andre i samfunnet på cyberangrep og trekker frem sårbarhetene ved at forsvaret er på Facebook, internett og Twitter. De mener også at de mangler informasjon på

hvor viktig temaet security er. «*Lite kunnskap om det og lite folk til å håndtere det. Så det blir tatt mye raske løsninger» (393).*

Leder (18) trekker frem tilfeller «*hvor ansatte har vært løsslupne opp mot media*», og *«at en ubevisst sier litt for mye, fordi det er en del av vanlig tale hos oss og tenker ikke over hva som er gradert og ugradert»*.

FSA forsøker å vise tilstedeværelse rundt om i avdelinger, og *«opplever at folk skjønner hvorfor, helt til de har litt dårlig tid, så blir det litt plunder og heft og så gjør de det litt enklere»* (FSA). FSA har en opplevelse av at Kystvakten er litt bedre enn resten av Sjøforsvaret på bakgrunn av at de har eldre ansatte. *«Vi er litt opptatt av at de som driver med sikkerhet ikke skal være de yngste, men eldre befal, og tror det er helt nødvendig for å få gjennomslag at alderen er høyere»* (FSA). FSA satser, som NSM, på å vise eksempler fra virkeligheten. *«Vi opplever at det virker best når mennesker selv ser hva som skjer og reflekterer over det, og synes det er gale så har de et rammeverk i hvert fall til å mene at det skal i hvert fall ikke skje hos meg. Sånn regelpiskning er vanskelig, det er et langsiktig gnagerarbeid»* (FSA).

«I en militær sammenheng handler det jo vel så mye om å skape den kulturen for at, Forsvaret er jo bygd opp på det, du er jo sammen med noen som du må legge livet ditt i hendene på. Du er avhengig av at den tillitsrekka eksisterer for at man ikke er der så mye for å løse oppdraget, men for å slåss med den andre personen som står ved siden av deg. Så å finne de faktorene som faktisk fungerer, både grunnleggende i kulturen, men også situasjonsbestemt – hva man skal spille på, det tror jeg er viktig. Og da er jeg veldig på åpen og ærlighet, at man skal være ærlig i situasjonene» (NSM).

Hvis ikke organisasjonens ansatte forstår trusselen, er det vanskelig å beskytte seg mot den. Roer sier at vi må forstå innsidetrusselen. *«Det hjelper ikke å stramme inn hvis man ikke vet hvorfor, ikke har forståelse. Forstå teknologien først før man regulerer bruk og utarbeider policy»* (Roer). Nytrøen fokuserer også på viktigheten av forståelse når vi snakker om security. *«Folk må forstå trusselen for å kunne sette av ressurser og tid. Handler om å beskytte oppdraget»*.

Holdninger:

Resultatene etter de neste to spørsmålene sier noe om holdninger hos de ansatte, men også noe om oppfølging av retningslinjer og rapporteringskulturen. Holdninger vil bli drøftet under menneskelige faktorer, mens retningslinjer og rapporteringen vil bli drøftet under det

organisatoriske. Vi stilte informantene spørsmålene om de har erfart at de selv eller andre har valgt å ignorere sikkerhetstiltak/føringer (spørsmål 11) eller latt være å rapportere brudd på sikkerhetstiltak/ føringer (spørsmål 12). 58% av informantene svarer JA på spørsmål 11, mens 42% svarer NEI. Avdeling 1, 2 og 3 har akkurat like mange informanter på ja og nei siden (Diagram 4 venstre side). 61% svarer JA på spørsmål 12, mens 39% svarer NEI. Avdeling 2 og 3 er noe mer representert på ja siden enn avdeling 1 (Diagram 4 høyre side).

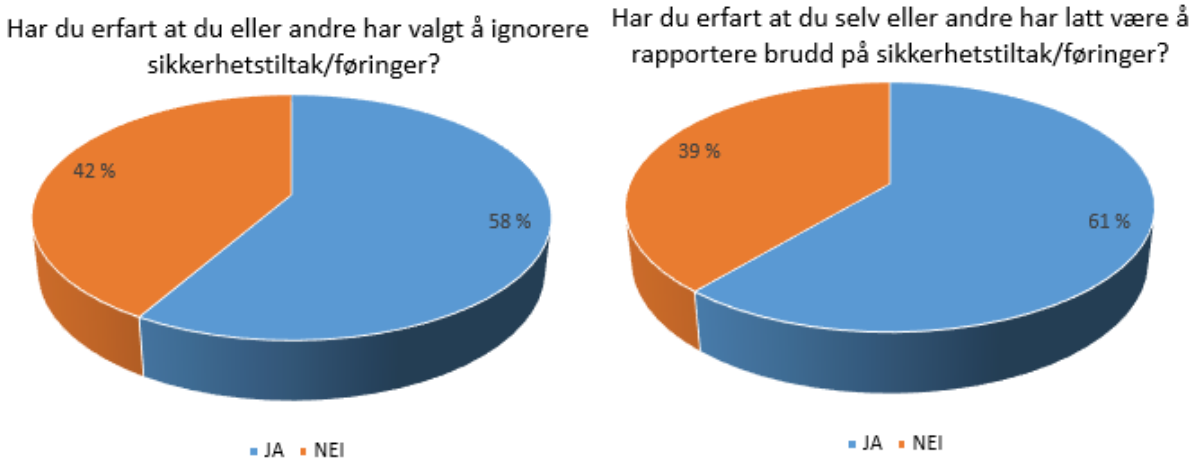


Diagram 4: Resultat spørsmål nummer 11 og 12 hurtig intervju.

Informanter uttrykker at det oftest er med uhell at føringer ikke blir fulgt, men at noen velger å ikke høre på føringer. Flere trekker frem at mobiler i graderte rom forekommer og uttrykker at deler av personellet «*nesten nekter å gi fra seg mobilen*» (212). Det fremkommer at det er ulike praksis av føringer på fartøyene når det kommer til mobilbruk, og flere informanter uttrykker frustrasjon når befalet bruker mobil når de selv ikke får lov. I en avdeling kom det frem at det var lett å slå av flight mode når en var for seg selv, selv om det var gitt føringer på at denne skulle være på.

I svarene til informantene fremkommer det at veldig mange vurderer selv om sikkerhetsbruddet er alvorlig nok til at det trengs å rapporteres. Dette gjelder helt fra laveste nivå (menige) og oppover. Utsagn som: *«bruddene blir tatt oss imellom, og som regel ikke tatt opp i et «høyere organ», før det blir så alvorlig at det kreves at en sier ifra. Hvis det skal tas opp helt til «toppen», blir det som regel jævlig dårlig stemning. Miljøet er veldig viktig her» (423),* og «*Det er ikke alltid poeng å rapportere det hvis en kan håndtere det der og da. Når en snakker om å rapportere sikkerhetsbrudd, da tenker jeg at det er noe alvorlig. Så føler en at dette kan få noe konsekvens og vil ikke at det skal få en konsekvens for andre som egentlig ikke er alvorlig» (161).* CYFOR påpeker at det *«er ikke alltid like lett å rapportere når man selv har gjort. Hva er alvorlig nok til at du skal rapportere – det kan være en*

utfordring». En annen informant trekker frem «*Det er del sikkerhetstiltak som man velger å ignorere for det lar seg nesten ikke gjøre*» (424).

NSM viser også til gode eksempler for å forklare at det trengs mer enn en bevisstgjøring og kunnskap for å skape en kultur. *«Grunnleggende så mener jeg at vi mennesker ikke går rundt og ønsker å gjøre negative ting, vi er stolt av arbeidsplassen. Jeg mener bevissthet, awareness, ikke er nok. Kunnskap og bevissthet skaper ikke automatisk en adferd.* NSM uttaler at det er lettere å få personellet til å forstå bruk av eksempel hjelm, da dette kan være en direkte fysisk trussel som kan påvirke de ansattes sikkerhet. *Det å bruke de samme virkemidlene på en byråkrat som sitter i Oslo, og få han til å passe på en informasjon som i en sånn abstrakt situasjon er verdifull og som på sikt kan føre til akkurat samme konsekvenser dersom noen agerer på det, det er betydelig mer vanskelig å nå frem. Fordi vedkommende ikke føler noe trussel eller risiko ved det overhodet»* (NSM).

Flere informanter prater om bekvemmelighets hensyn, tidspress og operativ kapasitet som årsak til at en ikke rapporterer og en sier «*en kan velge å ta en snarvei eller en kan velge at det ikke blir gjort» (393)*. Informant 272 uttaler at «*vi må bli vant til at det kommer noe godt ut av rapportering»*, mens informant 222 sier at *«det blir nok tatt der og da, men det blir nok ikke rapportert»*. En informant (91) sier at *«rapportering er grunnlaget, læring er nøkkelen, ikke straff»*, mens en annen ønsker «*mer kunnskap om rapporteringsverktøy - oppleves som tung grodd (252)»*. Videre uttrykker vedkommende at det *«blir ikke skilt mellom små eller store brudd. Ikke kunnskap om konsekvens og gir mer papirarbeid*». En sikkerhetsleder sier *«Ahh, det med mobiler inn i graderte områder, jeg ser ikke det som et stort brudd. Så det rapporteres ikke»*

NSM uttrykker at security ivaretas ikke og innlemmes ikke i kulturen med mindre lederne tar sitt ansvar og setter det på dagsordenen for hele organisasjonen og forstår sitt ansvar ovenfor de ansatte. «*Daglig sikkerhet er kanskje det mest kulturbringende, at du har en leder som fokuserer på sikkerhet i det daglige. Det krever litt av en leder å få endret kulturen, ettersom du i noen tilfeller skal følge gitte prosedyrer, men av og til må det gjøres en vurdering om at du ikke skal følge prosedyren. Sannsynligvis den beste forsikringen mot innsidetrussel er å ha glade og fornøyde ansatte som føler en stolthet og lojalitet mot arbeidsplassen sin og som føler de blir verdsatt og ivaretatt og tenkt på»* (NSM).

Vi spurte informantene om arbeidsmiljøet har påvirket deres håndtering av sikkerheten? (Spørsmål 13). 61% svarte NEI, 31% svarte JA, mens 8% hadde andre svar (Diagram 5

venstre side). Har dårlig personellforvaltning fra lokal og høyere ledelse påvirket deg til å begå sikkerhetsbrudd, eventuelt påvirket deg til å la være å rapportere? 89% svarte NEI, 0% svarte JA, mens 11% vet ikke (Diagram 5 høyre side). Alle under svaret «vet ikke» tilhører avdeling 2. Resultatene kan tyde på at flere blir påvirket av arbeidsmiljøet i form av kollega, enn av dårlig personellforvaltning av ledelsen.

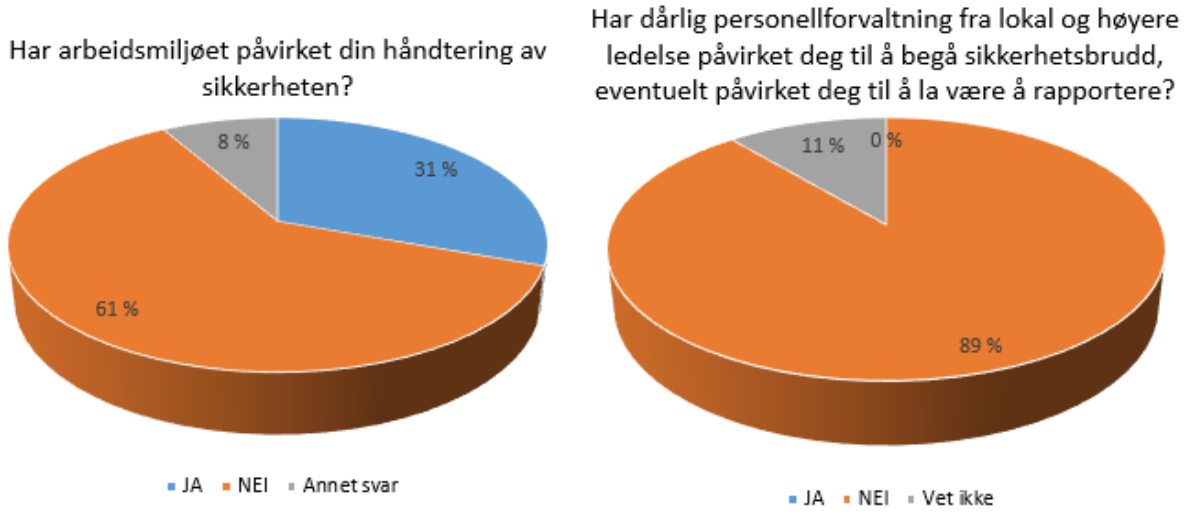


Diagram 5: Resultat spørsmål nummer 13 og 14 hurtig intervju.

Flere informanter som har svart ja på spørsmål 13 (Diagram 5 venstre side) sier at arbeidsmiljøet har mye å si, og at en kan bli påvirket av andre på både låsing av dører og mobilbruk. Også her trekkes det frem befal som bruker mobil når reglene er der. Noen som svarer nei på spørsmålet, trekker allikevel frem at «*en kan bli små slapp av og til» (282),* mens en annen sier *«en tar det kanskje ikke like seriøst alltid, blir litt halvhjertet. Orker ikke følge opp andre hele tiden. Vanskelig å være den som strammer inn» (171).* Informant 262 trekker frem at arbeidsmiljøet og påvirkningen avhenger av «*hvor mye opplæring som har vært*» mens informant 393 sier at det er forskjellig fokus og holdninger noe som *«gjør det lettere å slippe opp selv»*. Samtidig trekker vedkommende frem at en påvirkes av kunnskap, dagligbruk og forståelse og mener at det er «*ingen fokus i det daglige*». På spørsmålet 14 (Diagram 5 høyre side, om dårlig personellforvaltning har påvirket rapportering) trekker flere frem at de har en god ledelse som fungerer bra og uttrykker at det er mer «*passive holdninger til føringene*» (443) hos de ansatte.

I følge Roer har alle et bredt spekter av adferd, og når man er sammen med andre bruker man fra spekteret og tilpasser seg. Roer understøtter trusselen misfornøyde ansatte utgjør når det kommer til innsidetrussel. «*Disgruntled workers» har større sannsynlighet for å utøve misnøye mot sjefen – da ved sabotasje, manipulasjon/endring av informasjon, trojanske bomber (går av et år senere)"* (Roer). Innsidetrusselen er en av truslene som må håndteres

og forstås på alle nivåer. *«Vil aldri kunne fjerne innsidetrusselen – men å begynne å skape dem selv må vi håndtere»* (Roer).

Teknologiske faktorer:

Her ønsker vi å se nærmere på den raske teknologiske utviklingen og hvordan den påvirker håndtering av innsidetrussel. Flere ledere utdyper at det har vært fokus på teknologisk utvikling, og at det er føringer på bruk av teknologiske enheter som mobil og trådløst internett. En leder (18) sier derimot at det «*er nok ikke så mange som tenker på Apple watch og alt mulig annet. Er ikke det samme fokuset.*» Leder uttrykker fokuset mot mobil har gjort at dette har blitt beskrevet i prosedyrene, men eksempel «*pulsklokker med blåtann og GPS står det ikke noe om»*. Noen av lederne sier at informasjon om ny teknologi blir informert om via LKM. «*Jeg har sikret at den informasjonen som er vesentlig for oss har blitt videresendt nedover i avdelingene»*. *Jeg tror den største utfordringen er å håndtere private elektroniske medier i en operativ setting*.» (Leder 19).

Leder (37) uttrykker at PCer som står i nettverk gjør oss sårbare og «*det oppleves at vi er veldig åpne for innsidetrussel*. *De som sitter i bestemmende posisjoner, er den eldre garde. De kan ikke så mye og vil ikke vite så mye om data i nettverk*». Informant 171 prater om teknologi under avslutningen av intervjuet og sier: *«Jeg tenker mest på: Hva kunne fienden funnet ut selv om vi har rutiner? Hva kan andre klare på tross av våre rutiner. Teknologikunnskapen i Forsvaret er lav»*.

Forsvaret har en del muligheter, men er avhengig av tydelige avsatte ressurser og krav til hva som skal iverksettes. «*Ved å være egen tjenesteleverandør kan du innskrenke hva du kan installere, kanskje det ikke var så nyttig som du ønsket, men så er spørsmålet, hva kommer først, ditt behov, eller Forsvarets behov for sikkerhet. Det finnes sikkerhetsløsninger slik at du unngår at tjeneste mobil kan avlyttes for eksempel. Og du har mange studier som går på sikkerhet ved produksjonskjeden, som viser at de fleste datamaskiner blir i dag produsert i Østen, i Kina. Hvordan kan vi være sikre på at det vi får er det vi ønsker. Finnes løsninger hvor de kan koble seg til fra egne kontorer»* (CYFOR). Det er også en utfordring å tillegge nye krav, spesielt hvis det medfører å ta vekk noe som ansees som en gode. *«Mange av sikkerhetsmekanismene vil jo føle som om vi tar bort funksjonalitet fordi vi har lagt oss til en vane. Da er det viktig å kommunisere forståelsen for hvorfor vi gjør dette, hva tjener den enkelte og hva tjener forsvaret på at vi gjør dette» (CYFOR).*

Organisatoriske faktorer:

Vi var interessert i å danne oss et bilde om hvordan organisatoriske faktorer i Marinen er i forhold til security-kultur. Vi har valgt å se nærmere på følgende; *Prosedyrer & retningslinjer, ansvarsforhold & sanksjoner og læring* (ref tabell 4).

Prosedyrer og retningslinjer:

Under dette punktet ønsker vi å undersøke om de ansatte vet hvilke prosedyrer eller føringer/retningslinjer som er gitt og om disse følges.

Flere ledere snakket om sikkerhetsloven, prosedyrer og retningslinjer innenfor security. Leder (18) sier at «*security organisasjonen er veldig firkantet innenfor lov og forskrifter. Der er det sagt at en skal ha en ASL, KSL, DSL. Det har vi i hele organisasjonen, på land ned til nederste nivå*». Leder (19) sier at «*vi har en rekke sikkerhetsregler som beskriver forholdet til sikkerhet på nett, bruk av mobiltelefoner, smartbrett, trådløse nett*».

Vi spurte sikkerhetslederne om det finnes pålagt sikkerhetsdokumentasjon for håndtering av cybertrussel? Ev hvilke? (Spørsmål 5). Fire av sikkerhetslederne, fordelt på avdeling 1, 2 og 3, pratet om sikkerhetsloven, interne prosedyrer og manualer herunder grunnlags dokument sikkerhet (GDS). Videre nevnte de rapporteringsverktøy som sikkerhetsweb, føringer på bruk av graderte systemer og prat i offentlig rom. De to resterende sikkerhetslederne uttalte *«Ja det gjør det sikkert, men ikke meg bekjent» og «vet ikke»*. Disse tilhørte avdeling 1 og 2. Årsaken til svarene deres kan enten være at de faktisk ikke vet, eller at de ikke har forstått spørsmålet de ble stilt. Det fremkommer fra mange informanter at det er ulike føringer, praksis/ gjennomføring i avdelingene. Årsaken til dette mener leder (19) er «*ulike kunnskap gir ofte ulik policy*». En annen leder (18) sier at «*det er nok ikke det eneste området hvor det er ulike føringer*». *«Men på en annen side så er det innen security veldig firkantet, av de fagområdene det burde vært mest likhet. Vi er uenig, forskjellig tilnærming. Det er en felles policy fra Marinens sin side, så er det opp til hver enkelt skipssjef å være strengere hvis de ønsker det. Og det ønsker vi jo»*.

Som observatører i miljøet kommer det tydelig frem at det er ulik praktisering av GDSene. To av avdelingene benytter tilnærmet like matriser på retningslinjer på hva som er lov og ikke, men de praktiserer matrisen ulikt.

Resultatet fra hurtigintervjuene og egne observasjoner viser at praksisen om bord varierer, ikke bare mellom avdelingen, men mellom de enkelte fartøyene. *«Det er store forskjeller i praksis på fartøyene, og det forekommer kommunikasjon av gradert informasjon på ugradert samband ettersom man mangler systemer. Utfordringen er perspektivet på at kommunikasjonsutstyr skal kunne beskyttes 30 år frem i tid, hvor man da ender opp med*

tiltak som fører til at brukervennligheten på det man har ikke nødvendigvis blir veldig bra. Info som sendes kan ha en ganske kort levetid, men det må da gjøres en vurdering av noen som forstår risikoen de tar ved å si ting i klartekst på et ugradert nettverk, for det kan ha betydning utover rikets sikkerhet» (NSM).

Lederne påpeker at det er utarbeidet GDSer i avdelingene, men at de ikke tror at det er gjort noen sårbarhets- eller risikoanalyser på det. Leder (18): *«Ikke i nærheten av noen slike vurdering er nok ikke gjort. Ikke på organisasjons- eller fartøys nivå»*. Leder (19) *«jeg er ikke kjent med at vi har noe tungt arbeid på det. LKM følger opp dette og er gode rådgivere til Marinen på de områdene de er gode på»*. En annen leder (37) sier også i sitt intervju at sårbarhetsanalyser «*det tror jeg aldri noen har gjort. Ikke som jeg kjenner til i alle fall*». Lederen bruker da eksempelet med enheter/fartøyer som skal til oppgradering/vedlikehold.

Ved nytt utstyr skal det gjennomføres en sårbarhetsvurdering og sikkerhetsgodkjenning, og ifølge FSA skal det ved endringer gjennomføres på ny. «Du skal ta høyde for den trusselen i utgangspunktet. Sjøforsvaret må eie risikoen selv, og vurdere om risikoen er verdt gevinsten. Med tanke på Sjøforsvarets plattformer må vi over til logikk, og si at dette er det beste vi kan få til, sånn må det bare være, men dette skal dokumenteres. Det vi forsøker å si til de ulike strukturene i Forsvaret er at de i større grad forsøker å kjøre standardiserte løp. Så ikke hele tiden lage nye komplekse løsninger som skaper enorme mengder arbeid. Hvis en avdeling x ser sånn ut i fred, kan den ikke se sånn ut hele tiden? Vi ønsker mest mulig «train as you fight» (FSA). CYFOR understøtter føringer om sårbarhetsvurdering og sikkerhetsgodkjenning, og påpeker i tillegg at «sjefen på fartøyet har den initielle risikovurderingen fra FMA og så har han sin egen kunnskap om plassering, initiering og rutiner og kontekst, som gjør at det er sjefen ombord som må gjennomføre og risikovurderingen» (CYFOR). Det observeres at svært få ledere på lavere nivå vet så mye om sårbarhetsvurderinger som er gjort og hvilket ansvar de har for å tilføre denne lokal kunnskap.

Nytrøen viser til den samme linjen som FSA og CYFOR for krav og godkjenninger til systemene, men stiller spørsmålet om det er noen som tenker krig i den prosessen. *«Økes ved å redusere kravene ved å få et antall systemer vs. sikre systemer. I ethvert prosjekt blir kravene til sikkerhet neglisjert for å holde budsjett. Hva vil være trusselen mot plattformene, og hvordan skal den beskyttes? Kravfastsettelse til utstyr må settes i forhold til reell bruk»* (Nytrøen).

Flere informanter uttrykker sin bekymring for hvor åpen dokumentasjonen er selv på et begrenset nettverk (Fisbasis), et nettverk hvor mange har tilgang. Dette uttaler også noen ledere (18,19,37). «*Vi har ikke kontroll på hvem som har tilgang på det begrensede nettverket. Alt for mange brukere. Autorisering av personell og tilgang til nettet er ikke godt nok kontrollert» (19)*. Samme leder (19) uttrykker videre: «*Det er en utfordring når en ser på fisbasis, som er vårt arbeidsverktøy i hverdagen som håndterer informasjon opp til og med begrenset. Så er det mange som tenker på at all info som en utveksler der er helt greit å snakke om, begrenset på nett, uten at en merker det som begrenset. Du skriver ikke nødvendigvis på at det er begrenset og henviser til paragrafer. Skriver bare det du mener, det tenkes ikke over, og det videresendes og distribueres og legges ved kalendere. Så er det alt for mange som har tilgang til systemet, en har da ikke kontroll på informasjonen»*. Informant 333 sier «V*i bli flinkere til å skille mellom forskjellige graderingsnivå, hva er begrenset, hva er konfidensielt, hva er unntatt offentligheten. Vi trenger mye mer opplæring, vi må bli flinkere»*. CYFOR har også registrert at Forsvaret ikke er flinke på internkontroll i forhold til tilganger på systemene og understreker at dette må tas inn som en del av rutinene og internkontrollen. Informant 333 snakker om personell som arbeider i landavdelinger: «*Det bør være mye større begrensninger til andres kontorer»*. Gjennom både observasjon og intervjuer ser vi at bygg er godt beskyttet med regulerte tilganger, men kontorer står ofte åpen og det er ikke alltid at personell låser ned pc når de forlater kontoret.

Vi spurte informantene hvilke føringer er lagt for rapportering av cyber/security-hendelser? (Spørsmål 16) 33% svarte at de skal rapportere til sikkerhetsleder i avdelingen, 27% sier at de vil rapportere hendelsen tjenestevei, 25% vet ikke hvordan de skal rapportere mens 17% hadde andre svar (Diagram 6). Avdeling 1 har flertallet av svarene under «sikkerhetsleder», avdeling 2 på «tjeneste vei», mens avdeling 3 på «vet ikke», etterfulgt av «sikkerhetsleder».

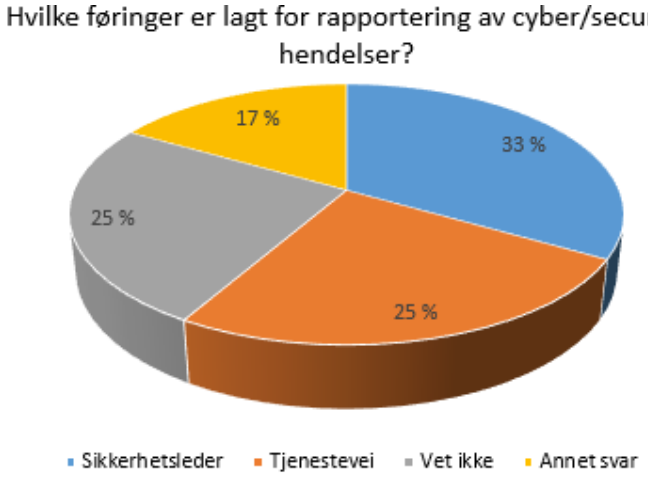


Diagram 6: Resultat spørsmål nummer 16 hurtig intervju.

Resultatene kan tyde på at personellet i avdeling 1 har en bedre forståelse for føringene og sikkerhetsorganisasjonen enn de andre to avdelingene. Ulikheter i svarene til avdelingene kan også tyde på at organisasjonen ikke har klart å få tydelig frem føringer på rapportering av security-hendelser. I forhold til rapportering påpeker FSA at det er viktig å følge kommandolinjen ved rapportering i utgangspunktet, ettersom FSA ikke har kapasitet til å ta den initielle vurderingen av sakenes alvorlighetsgrad. *«Sjøforsvaret må snakke om temaet, og oppfordre til rapportering»* (FSA). FSA ber Driftsenhetene i Forsvaret (DIF), GIS og tilsvarende, om å melde inn en årsrapport/tilstandsrapport innenfor security. FSA tror også ressurser kan være en utfordring, og ser i spennet fra fred til krig at, ettersom security inngår som en prosentandel av stillinger, vil den prosentdelen gå til hovedfunksjonen i det spennet. FSA ønsker i den grad det er mulig å søke mot større prosent security-innhold i stillingene, og mener det generelt kunne vært satt mer ressurser til security.

Når informantene fikk spørsmålet: Ville du godtatt strengere føringer på bruk av mobil/Pad/pc/internett/minnepinne/privat bruk av media for å bidra til å redusere Sjøforsvarets sårbarheter for fiendtlige handlinger? Svarte 84% JA, 8% svarte NEI mens 8% hadde andre svar (Diagram 7).

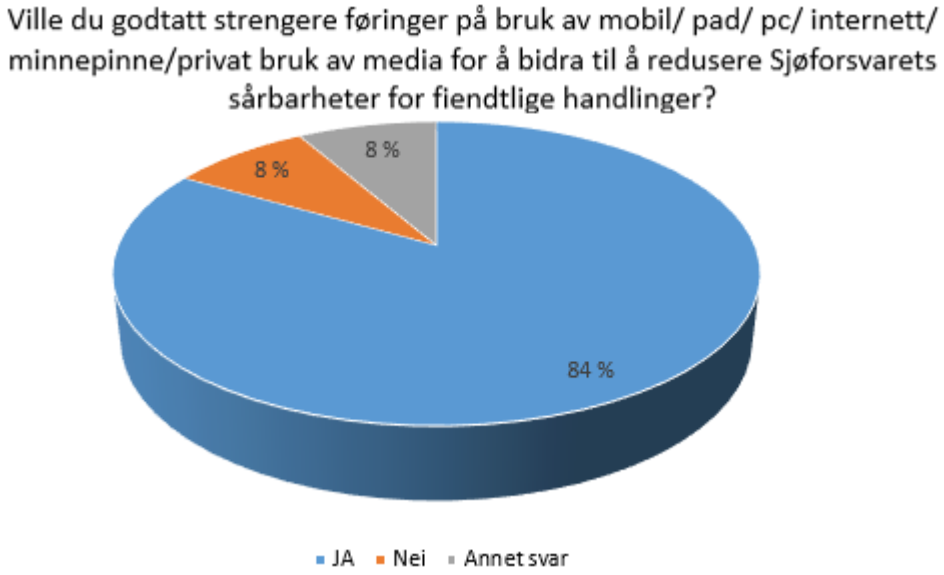


Diagram 7: Resultat spørsmål nummer 10 hurtig intervju.

De fleste informantene som sa JA på spørsmålet hadde også tilleggskommentarer. Informant 171 uttaler at *«noen tiltak er iverksatt»* (eks restriksjoner på bruk av mobil) og mener at de er *«unødvendige og ikke hensiktsmessige. Bedre forståelse vil gjøre at tiltakene blir bedre. De som lager tiltakene må ha kunnskap og forståelse for å få gode tiltak»*. Informant 161 sier at *«jeg tror ikke problemet er hva vi gjør på fartøyene alltid, det er like mye hva Forsvaret går*

ut med selv også». Vedkommende referer da til Forsvarets egne sider på for eksempel facebook og forsvaret.no.

Utsagn som «*Ja. En del føringer allerede (mobil). Lettere når de forklarer hvorfor»* (272), *«Ja. Men må gi mening og gjelde ALLE»* (232, 302), *«det er viktig å skape holdningene og bevissthet*» (413). Flere prater om mobil bruk og en informant uttaler temaet blir mye diskutert på avdelingen. *«Det er en kjempe sak for en tar fra folk velferden når en bare skal seile og ingen får ta med mobil*» (212). En leder (19) er ikke overrasket over resultatet vist i diagram 7, «*man begynner å skjønne det*». Samme leder påpeker at det da må være tilgjengelig alternative muligheter for å få kontakt med familien, dette finnes.

Ansvarsforhold og sanksjoner:

Under dette punktet ønsker vi å undersøke ansvarsforhold og rollefordeling, samt vil vi se nærmere på om det er en rettferdig kultur. Leder (19) sier at «*security har vært godt styrt fra Marinen, og det har vært et nettverk med sikkerhetsoffiserer som jeg oppfatter som dyktig. Det var ikke noe robust organisasjon, var noen borte satt du egentlig med et betydelig hull selv om en hadde en assisterende stedfortreder. Så man svekkes ganske fort hvis noen er borte*». Det er også noe vi har observert i organisasjonen. Videre observeres frustrasjon hos enkelte ansatte på lavere nivå når støtten fra nivå 3 ikke er robust nok.

På hvilket nivå må/bør innsidetrusselen håndteres? (Spørsmål 2, Diagram 8) 47% svarer at det bør håndtere på alle nivåer, 36% sier på laveste mulig nivå og oppover i organisasjonen, 9% mener det må håndteres på ledelsesnivå og 8% sier at dette må håndteres fra topp i organisasjonen og nedover (Diagram 8). Avdeling 1 og 3 har flertallet informanter under alle nivåer, mens avdeling 2 i gruppen fra bunn i organisasjonen og oppover. Funnet kan tyde på at det er ulik oppfatning i avdelingene på hvilket nivå innsidetrusselen bør håndteres.

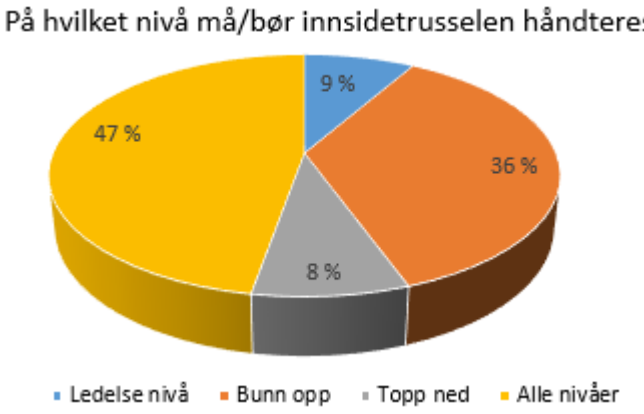


Diagram 8: Resultat spørsmål nummer 2 hurtig intervju

En informant uttrykker: *«Alle nivåer, men folk må gjøres oppmerksom på at den* (trusselen) *er der og at den er reel» (333)*. Informant 393 uttrykker at *«avhengig av bransje er folk litt forskjellig, har forskjellig nivå av interesse. Ikke samme forståelse i alle bransjer»*. Informant 161 sier at *«det er forskjellig måter å håndtere det på, på de forskjellige båtene i de forskjellige våpnene»*. Mens informant 423 sier at en bør *«starte på lavere nivå, men det skeier jo også ut mye høyere opp, folk slutter litt å bry seg. Og slik en ofte bør gjøre det er å ha gode eksempler oven fra og ned. Der må det starte på toppen, for hvis sjefen ikke bryr seg så bryr ikke jeg meg.* En leder (18) uttrykker at skal security håndteres «*må det tas grep over hele linjen*» og flere ledere trekker frem viktigheten i forankring i ledelsen på alle nivåer.

Roer kommer med en påstand litt utover det som er blitt uttalt tidligere. Han mener at arbeidet med å forbedre security-kulturen ikke nødvendigvis må starte fra ledelsen. Roer bruker ordet grasrotbevegelse – begynne med å dokumentere tiltak på lavere nivå for å vise ledelsen resultater. *«Strukturen (i Forsvaret) er en støttestruktur, har ikke til hensikt å stoppe gode endringer. Utfordring: må gjøre ting riktig for å forsøke å få til endringer. Struktur – en mulighet – lett å identifisere maktsenter, mulige ambassadører for saken. Trenger en som driver det – initiativ takere – men de vil ikke klare det alene. Aksepter at det tar tid*» (Roer).

Informant 91 trekker frem forskjellen på fokus på safety og security i Sjøforsvaret. *«Ledere blir målt på safety, det har vært prioritert*». «*Safety har 100% stillinger mens på security er det en bi jobb*». Flere ledere uttrykker utfordringer med prosentandel innenfor security i stillinger på nivå 4 og 5. Prosentdelen er «*veldig liten*» (Leder 19). Vedkommende stiller også spørsmålet: «*er det godt nok?*» «*Fordi kravet til kunnskap har økt noe voldsomt den siste tiden og det har vært helt nødvendig, det er så mye kunnskap som må til for å håndtere det ordentlig og være proaktiv og det å klare å lære opp alle andre på hvordan de skal bruke kunnskapen aktivt i handlingsmønsteret i hverdagen»*. Lederen (19) påpeker viktigheten av støtte fra spesialistene på land.

Det har «*vært veldig fokus fra øverste ledelse på å bygge opp enn safety sikkerhetskultur. Skal vi få til det på security så må en gjøre det på samme måte og få fokus på det, bygge opp en topp-Down oppbygging på en sikkerhetsorganisasjon. Slik som det er nå er det bortom-up og de på dørken som kjenner regelverket og skriker etter ressurser for å gjøre det som står i regelverket. Hvis dette hadde vært topp styrt hadde det kanskje vært mulig*» (Leder 18). Leder (19) utdyper at *«Du kan ikke gå rundt som leder å være spesialisten. Du* (lederen) *må bare sørge for at spesialistene får et arbeidsrom, at noen faktisk hører på spesialisten.*

Vi spurte sikkerhetslederne hvem har ansvaret for å ivareta håndteringen av innsidetrussel? Og hvem samarbeider dere med om cybertrusselen? (Spørsmål 6 hurtigintervju). Svarene fra sikkerhetslederne er ikke i særlig grad lik og det er ulik oppfatning av hvem som har ansvaret, men alle sikkerhetslederne nevner CYFOR. To sikkerhetsledere nevner LKM, mens to andre sier at det er sikkerhetsorganet på avdeling som håndterer internt (ASL/DSL). En nevner sikkerhetsleder på nivå 3 og Forsvarets Materiell (FMA: godkjenning utstyr). Utsagn fra flere sikkerhetsledere: *«Har hørt om CYFOR, men vet ikke om andre»*, *«det er enhver sitt ansvar å følge det opp, om man mistenker at det er aktivitet på et nettverk som gjør at det skjer noe som ikke burde skje eller noen roter bort noe»*, *«LKM koordinerer alt internt ut mot FSA. FSA holder kurs for ASL/DSL og kommer med jevnlige sikkerhetsmeldinger. Dette kunne blitt bedre»*

Alle lederne trekker frem LKM som samarbeidspartnere i forbindelse med security. «*LKM er sentral i Sjøforsvaret for å koordinere all den virksomheten her»* (18). Leder (8) sier at «*jeg tror at mye av det security baserte rapporteres til FSA direkte fra fartøyet, men ute av Sjøforsvarets håndtering. Jeg vet ikke så mye hva FSA gjør med det etterpå*». Noen ledere nevner også NSM, FSA og CYFOR, men ut ifra svarene til lederne er det noe uklart hvem som har ansvar for hva. Flere ledere er også usikker på om avdelingene har direkte kontakt med disse enhetene eller om dette kun går via LKM.

Alle informantene under hurtigintervju fikk spørsmålet: Hvilket ansvar har du for å sikre arbeidsplassen mot innsidetrusselen? (Spørsmål 9) Informantene prater om «*årvåkenhet»* (51,11,282), «*være oppmerksom»* (353), «*begrense hvem som vet hva»* (111,171,172) *«opprettholde regelverk»* (141,413,262), *«ikke legge ut sensitiv informasjon og bli en innsidetrussel»* (312,322, 343, 382) Noen informanter uttaler at en må passe på hva man selv gjør og deler (382, 382, 292, 393), mens andre sier at en må håndtere det på de måter en har fått beskjed om å gjøre det på (161, 413). Det ble trukket frem at en må påse at *«bestilt utstyr er i henhold til regler*» (121), Kun 19,4% av informantene ved hurtig intervju trekker frem det å rapportere som deres ansvar (91, 171, 242, 262, 292, 403, 443). Disse er fordelt tilnærmet likt på alle 3 avdelingene.

Flere informanter prater om frykt for personlige negative konsekvenser (121, 343) og negative sanksjoner, som eksempel å «*bli forflyttet til annet tjenestested»* (433), *«frykt for å ikke få opprykk»* (171), *«redd for å bli hengt ut og miste tilliten fra ledelsen»* (212) eller «*at det kommer på papiret»* (363). Informant 312 er usikker på konsekvensene og henviser til trussel om å bli rapportert til MP hvis en lekker informasjon på sosiale media, mens

informant 363 uttalte «*bryter man security blir man anmeldt etter norsk lov*», «*do'erne får på pukkelen, mens toppledelsen blir skjermet*». Det er viktig at lederne støtter seg på det apparatet som eksistere og bruker blant annet militærpolitiet, MP, som rådgivere, og ikke nødvendigvis for å straffe. Det er behov for rapportering for å skape et bilde av situasjonen (CYFOR). *«Jeg mener at man må innføre positiv rapporteringskultur så det ikke blir sanksjonert mot brudd. Så må vi bare erkjenne at det ligger straffebestemmelser i sikkerhetsloven som gjør at det kan sanksjoneres»* (CYFOR).

Leder (19) «*En ting er at en ønsker åpenhet for å håndtere det riktig, men på den andre siden har en gjort noe galt som krever en straffeforfølgelse eller administrativ oppfølging i vårt system, så kan en ikke unnlate det, det er en evig balansegang. En må skjønne at det ikke er noe problem å komme med saker, men det må gjøres på riktig måte, da får det ikke noe konsekvenser for jobben din»*. Lederen (19) sier at det går på opplæring, føringene ligger på det interne nettverket, «*men hvem leser det? En blir redd, en får angst, ingen som oppdaget det- jeg sier ingen ting»*.

Vi stilte informantene på hurtigintervjuet et oppfølgingsspørsmål til spørsmål 15: Er risikoen for å miste sikkerhetsklareringen en faktor som hindrer i å rapportere sikkerhetsbrudd? På dette spørsmålet svarte 42% NEI, 22 % svarte JA, mens 36 % gav ikke et direkte svar (diagram 9).

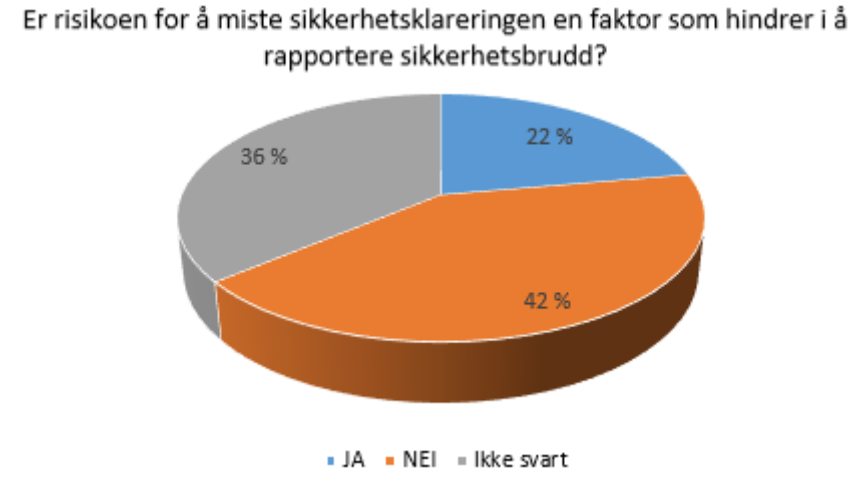


Diagram 9: Resultat oppfølgingsspørsmål under spørsmål nummer 15 hurtig intervju

Alle (minus en informant), som svarte JA på spørsmål 15 tilhørte avdeling 3. Resultatene kan også tyde på at 58% av informantene ved avdeling 3 kan frykte straff etter rapportering av sikkerhetsbrudd. Mister en sikkerhetsklareringen vil det i praksis si at en ikke kan arbeide på et som håndterer gradert informasjon. Dette resultatet kan tyde på at det er forskjeller i hvordan avdelingene kommuniserer konsekvenser for den enkelte ved sikkerhetsbrudd.

Læring:

Her ønsker vi å undersøke lærings- og rapporteringskulturen i Marinen. Hva motiverer til rapportering eller hindrer rapportering. Blir hendelser rapportert, fulgt opp og tiltak iverksatt. Vi stilte informantene spørsmålet: Hva hindrer eller motiverer deg i å rapportere sikkerhetsbrudd? (Spørsmål 15).

Når det kommer til hva kan gjøres for å motivere til rapportering trekker flere informanter frem fokuset på læring og ikke straff (91, 121,312, 363), mens noen trekker frem viktigheten av å forstå hvorfor tiltakene er der, hvor ille det kan gå (konsekvenser) og at det gjelder vår egen sikkerhet (141, 171, 282, 292, 383, 312, 353). Mens noen ønsker mer fokus på at det er positivt å rapportere (121, 343, 413) Andre uttrykker at «*begrensninger er en plage*» (292) og «*folk blir irritert*» (302). Informant 302 uttrykker også at en bør «*lette på regler når det er øvelser, skjønner at det er viktig når det er en skarp situasjon. Måtte levere inn telefonen i en uke på øvelse, det er ikke nødvendig. Det er ikke noe øvelsesmoment i det*».

CYFOR har påpekt til FSA at rapporteringssystemet må forenkles, ettersom de tror det vil senke terskelen for å rapportere. «*Jeg er av den formening at sikkerhetstilstanden ikke er så grei. Det er de små tingene tenker jeg hvor du kan se trendene, hvor vi kan se hvor vi må sette inn tiltakene og ressursene for å forebygge. Vi har jo ikke ubegrenset ressurser. Vi må komme dit at vi har en kultur hvor det er positivt å rapportere. Vil ha et enkelt system på Fisbasis (*gradert nettverk*) hvor man kan rapportere, og FSA vil da ha full oversikt. Hvis man hadde fått en ordning hvor CYFOR kunne registrert hendelser med 3-4 linjer og satt opp hvem som hadde ansvaret, så er hendelsen registrert hos FSA, sporbart hvor den kom fra, og hvem som har ansvaret*» (CYFOR).

Noen informanter trekker frem at nærhet til kollega og venner kan hindret dem i å rapportere (111, 322, 242) mens andre trekker frem egenvurdering av alvorlighetsgraden på bruddet (393). Sitater som: «*ikke vits å rapportere hvis det er et lite brudd*» (453), «*Ser ikke på bruddet som noe spesielt alvorlig*» (443), «*ingen ting hindrer meg i å rapportere hendelsen, jeg har bare ikke lyst å rapportere de som jeg ikke anser som alvorlig*» (161) og «*vet at det ikke er skjedd noen skade, og velger på egen vurdering å ikke rapportere*» (413). En informant trekker frem bagatellisering av sikkerhetsbruddet som et hinder til å rapportere det (232). Andre informanter sier «*troverdigheten til behovet for den strenge sikkerheten*» (423), «*manglende kjennskap til følgende av eller konsekvensene av at informasjon blir spredd*» og «*manglende respekt for graderingsnivåer*» (333). Det observeres at mange sikkerhetsbrudd blir tatt internt i avdelingene og at flere brudd ikke blir løftet videre. Det observeres også at

ledere tar tak i bruddene internt, hvor de tas opp på interne møter der de ansatte deltar, men bruddene blir ikke nødvendigvis tatt videre.

Det trekkes frem *«tidspress»* (51,91), *«tung grodd system»* (121), *«dårlig stemning»* (11, 302) og *«høyere ledere gjør det samme»* (292) som hinder for å rapportere sikkerhetsbrudd. Videre nevnes at *«rapportering nedprioriteres hvis en ikke får tilbakemeldinger»* (91), *«bryet med å måtte gjøre det, hvis du ikke ser viktigheten i å måtte ta det opp»* (403) og *«usikkerheter på hvor reglene går»* (363), hvor vedkommende henviser til usikkerhet rundt hva som er brudd og ikke. Andre henviser til at *«det er ingen vits å rapportere når det ikke blir håndtert»* (353) og *«latskap og neglisjering av viktigheten av sikkerhetsbruddene»* (212). Informant 212 henviser til episoder hvor sikkerhetsbrudd ikke er blitt rapportert, og prosedyrene for håndtering av situasjonen burde vært endret. Prosedyrene samsvarer ikke med praksis, men når de ikke rapporterer kan ingen fange opp at prosedyrene bør endres. Det observeres at det høye tempoet, tilgjengelige ressurser og oppdrag i enkelte avdelinger, til tider kan komme i konflikt med fokuset på security. Dette skaper en utfordrende balansegang for de ansatte på lavere nivå med tanke på hvordan de skal forholde seg til føringer og praksis. Leder (18) sier at *«det er enklere å rapportere innenfor safety, mens innenfor security skal det være mer formelt»*, en mulig grunn til at det ikke rapporteres er at «*da blir det armer og bein med en gang. Da skal det telles og rapportere og undersøkes*» (18). Mens leder (37) sier *«som regel så er det brudd på en sikkerhetsregel og det får egentlig ikke konsekvenser. Det er sjelden at det skjer noe endring»*

Vi spurte informantene om de opplever at rapportering blir fulgt opp (Spørsmål 18, Diagram 10 venstre side). 56% svarte JA, 0% svarte NEI, 5% svarte av og til, mens 39% vet ikke. På spørsmål 19: Blir tiltak iverksatt og endringer utført for å gjøre det mulig å gjennomføre i praksis (diagram 10 høyre side). 36% svarte JA, 9% svarte NEI, 8% svarte av og til, mens 25% vet ikke. De resterende 22 % hadde andre svar.

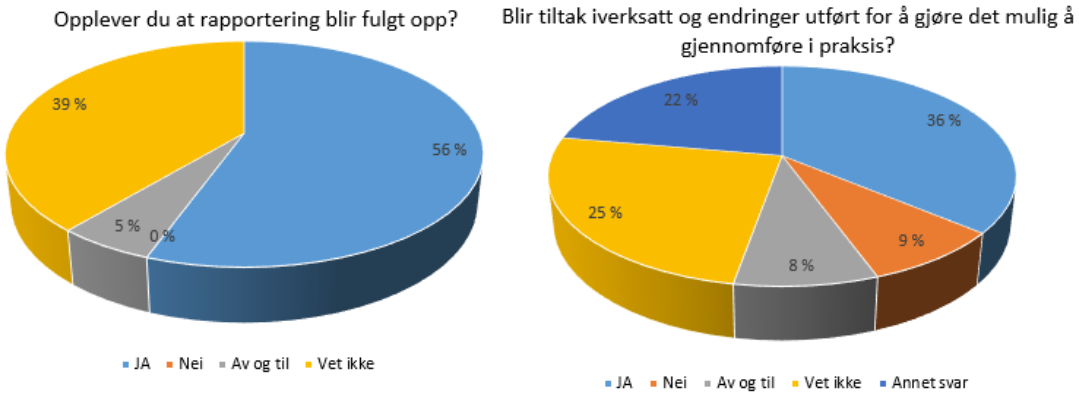


Diagram 10: Resultat spørsmål nummer 18 og 19 hurtig intervju

En informant under andre svar uttaler *«NSM må sette seg inn i hva et fartøy er for å forstå utfordringene, praktisk kjennskap. NSM kommer med føringer som ikke er gjennomførbare og de må ha grunnlag for å gi matnyttige tilbakemeldinger»* (343*).* En leder (37) uttrykker at oppfølging og fokus *«avhenger av avdelingens ASL sin kunnskap og initiativ»*.

Vi spurte sikkerhetslederne som de mener det blir gjort vurderinger av tiltak og nødvendige endringer av nye tiltak (Spørsmål 20). Samtlige sikkerhetsledere svarer JA på dette spørsmålet og utdyper dette videre med tilhørende eksempler. Sikkerhetsledere i avdeling 1 snakker om at det blir gjort endringer og justering på tiltak, hvor det eksempel blir gjort tilpasninger som skal opprettholde security, men samtidig ivareta safety ved for eksempel brann. Dette er et punkt som flere ledere trekker frem som utfordrende i praksis. I avdeling 2 trekkes det frem at tiltak tas opp på nytt og nye vurderinger gjøres hvis noe «sklir ut». Dette er det sikkerhetsleder som følger opp. I avdeling 3 uttaler en sikkerhetsleder at det på fartøyene blir gjort endringer og tilpasninger, men at det er «*mye interne føringer, men mangler kommunikasjon mellom fartøy og LKM*». Videre uttaler vedkommende at *«folk ønsker ikke å ta inn over seg sitt ansvar»*.

Vi stilte videre sikkerhetslederne (SL) spørsmålet: Hvordan håndteres rapportering av sikkerhetshendelser knyttet til innsidetrussel? SL i avdeling 1 trekker alle frem at hendelser rapporteres i sikkerhetsweben, og at dette går videre til sikkerhetsleder i Marinen (nivå 3) for så å bli sendt til FSA. SL uttaler videre at *«så får en sikkert et litt ullent svar tilbake»*. I avdeling 2 er svarene mer usikker og svarer *«vet ikke»*. I avdeling 3 påpekes det at hendelser med innsidetrussel blir tatt *«tilsvarende vanlige hendelser»* og tas direkte på rapport til sjef og håndteres av sikkerhetsleder som har mulighet å støtte seg på FSA.

5.2.3 Oppsummering hovedfunn forskningsspørsmål 2

	Hoved funn i empiri FS2
M	• Manglende kunnskap og forståelse for trusselbildet, security og innsidetrussel • Manglende holdninger til rapportering, med bakgrunn i manglende forståelse som kommer av manglende kunnskap og innføring fra ledelsen
T	• Organisasjonen klarer ikke å tilpasse prosedyrer og retningslinjer til den hurtige teknologiske utviklingen • Det eksisterer teknologiske løsninger som vil kunne redusere risikoen for lekkasjer • Forenkling av rapporteringssystemet vil kunne bidra til forbedret risikohåndtering
O	• Ulik praktisering av prosedyrer og retningslinjer på tvers og innad i avdelingene • Prodsedyrer og regler er ikke tilstrekkelig for å håndtere usikkerheten ved trusler • Secuirty organisasjonen i Marinen er ikke robust nok (i form av personell og tid) til å ivareta security på en tilstrekkelig måte •Manglende kompetanse, forståelse og holdninger som fører til mangelfull rapportering ødelegger muligheten for læring. •Manglende fagopplæring gjennomgående innenfor security vanskeligjør læring for organisasjonen, og det opparbeides heller ikke erfaring, kompetanse, intuisjon og det som muligjgjør sensemaking, awareness, resilience og mindfullness

Tabell 7: Oppsummering hovedfunn empiri FS 2

6. Drøfting

I dette kapittelet vil vi drøfte de analyserte funnene presentert i empiridelen. Vi sammenstiller funnene belyst med relevant teori som presenteres under tre kapitler inndelt etter forskningsspørsmålene. Under punkt 6.1 presenteres først trusselbildet, før empiri og teori drøftes opp mot FS1 under MTO inndelingen. I punkt 6.2 drøftes FS2 under M og O inndelingen, og videre i punkt 6.3 drøftes FS3 som et resultat av FS1 og FS2 belyst av valgte teoretiske rammeverk.

6.1 FS1: Hva er trusselbildet fra cyberdomenet og innsidetrusselen mot Sjøforsvaret?

Vi innleder med en beskrivelse av trusselbildet basert på rapporter og trusselvurderinger. Hensikten er å ha et felles bilde som utgangspunkt for videre drøfting av forskningsspørsmålene. Under FS1 drøftes teori opp mot empirien fra fagintervjuene, hvor resultatene fra de åpne intervjuene er fordelt under M; *Kompetanse, forståelse, holdninger,* T, O; *Prosedyrer & retningslinjer, ansvarsforhold & sanksjoner, læring*.

Trusselbildet

I følge E-tjenesten er nettverksbaserte etterretningsoperasjoner i form av utro tjenere inne i bedriften en betydelig trussel, og Russland og Kina fremstår som de mest aktive aktørene (Fokus, 2015). Mer avanserte metoder, mer komplekst risiko- og sårbarhetsbilde fører til større krav til forebygging ved blant annet tiltak for å redusere risikoen for innsidere (NSM 2015a s.7). I følge NSM (2015a) vil angrep kunne ramme Forsvarets operative ene både i fred, krise og krig. Innsidetrusselen er ikke bare reell, men utgjør en betydelig trussel som må håndteres for å ivareta Marinens operative evne. Teknologien som i fremtiden vil bli brukt for å ivareta norske interesser, kan en sofistikert motpart søke å manipulere gjennom cyberdomenet. Den raskt voksende trusselen mot våre datasystemer er en av de alvorligste trusler mot vår nasjonale sikkerhet i årene fremover (Generalmajor Roar Sundseth, tidligere sjef CYFOR).

Trusselbildet har mange aspekter, men vi har valgt å fokusere på MTO-faktorene som gjør oss sårbare (NSM, 2015a). De menneskelige faktorene er knyttet til blant annet kompetanse, ikke bare om trusselen, men verdier, sårbarheter og organisasjonens virke. I tillegg må de ansatte ha en forståelse for hvordan å ta i bruk kompetansen for å evne å håndtere tilsiktede uønskede hendelser. Den menneskelige faktoren holdninger farges blant annet av hva den ansatte tar med seg inn i organisasjonen. Denne vil kunne endres og påvirkes av de

forskjellige kulturene som eksisterer i en organisasjon, og vil kunne utgjøre en sårbarhet for innsidetrusselen. De teknologiske faktorene er et utsatt element i trusselbildet, og utviklingen av cyberdomenet gir store muligheter for en trusselaktør som har onde hensikter mot en organisasjon som Marinen. De organisatoriske faktorene som prosedyrer & retningslinjer gir et utgangspunkt for å håndtere truslene, men er ikke tilstrekkelig alene. Ansvarsforhold & sanksjoner vil vise hvem som har ansvar for å implementere nødvendige tiltak, opplæring, oppfølging og bidra til rapportering for å være bedre rustet til å møte truslene. Læring er nærmest en oppsummering av de overnevnte, og binder alt sammen for å muliggjør en utvikling av evnen til å håndtere trusler og bygge en security-kultur (Roer, 2015).

Menneskelige faktorer

Kompetanse

I følge Aven et al. (2013) handler risikopersepsjon om hvordan en opplever risiko, og hvordan mennesker flest forstår, opplever og håndtere risiko og farer. Den menneskelige faktoren er en sårbarhet når det kommer til innsidetrussel, hvor manglende kunnskap om trusselen vil påvirke evnen til å håndtere den. *«Hvis du har god kompetanse, da vet du hvordan det fungerer, og da kan du kanskje si du har kontroll. Sikkerhetselementene blir kanskje oversett i enkelte tilfeller fordi vi ikke har kunnskap om dem»* (CYFOR). I følge NSM eksisterer det en rekke sikkerhetstiltak av teknologisk og fysisk art for å håndtere en trussel, men for at de skal fungere er man avhengig av at menneske har kunnskap om hvordan de fungerer.

Når menneske ikke har kunnskap om trusselen den står ovenfor blir det en sårbarhet i forhold til at en trusselaktør kan utnytte personens uvitenhet. I tillegg vil en trusselaktør kunne utnytte et menneske ved bruk av pressmidler eller trusler. Dette er innside kategorien «den utnyttede» (NSM, 2015a s.17). Menneske er også en sårbarhet i forhold til kunnskapen om systemene de bruker. Her kan utviklere og sikkerhetsledere gjøre et arbeid ved å tilpasse systemer og sikkerhetsrutiner slik at det blir lett å bruke systemene sikkert og riktig, men det fordrer uansett utdanning og opplæring. Manglende kunnskap øker usikkerheten, og selv om det alltid vil være «sorte svaner» /sjeldne hendelser som en ikke kan forutse ifølge Tablet (2010) og Aven (2014b), vil kunnskap kombinert med ferdigheter og evnen til å ta det i bruk bidra til å redusere risikoen.

Nødvendig kompetanse for å ivareta sikkerheten innebærer ikke bare kunnskap om trusler, sårbarheter og verdier, men evnen til faktisk håndtering av en uønsket hendelse. I punkt 4.8 i D*irektivet – Krav til sikkerhetsstyring i Forsvaret* (2010) står det at avdelingen skal ha

nødvendig kompetanse for å ivareta sikkerheten, og krav til kompetanse for forskjellige stillinger skal være definert og beskrevet. Resultatene fra de åpne intervjuene peker på at security må innlemmes gjennomgående i utdannelsen, og det må være en rød tråd i utdannelse og praksis. Det fremkommer fra de åpne intervjuene og egne observasjoner at utdannelse og opplæring innenfor security i Forsvaret er mangelfull. I følge Reason (1997) har en informert kultur kunnskap om alle faktorer som har betydning for sikkerheten, og organisasjonen må proaktivt søke informasjon om MTO faktorene som kan ha betydning for sikkerheten. Uten gjennomgående kompetanse på faget security i organisasjonen vil dette være vanskelig. Hvis personellet ikke har kompetanse på fagområdet, hvordan skal de da vite hva de må være oppmerksomme på, vise årvåkenhet for? Mindfulness er ifølge Weick og Sutcliffe (2007) en betydelig karakteristikk for HRO. På bakgrunn av de åpne intervjuene og observasjon viser dette at manglende kompetanse i Marinen på security vil kunne redusere evnen til mindfulness.

Forståelse

Når beslutningstakere på samfunns- og organisasjonsnivå skal forsøke å redusere risiko gjennom styring, bør de derfor også ta inn i vurderingene hvordan mennesker sosialt og kulturelt skaper sin egen risikoforståelse (Aven et al., 2013). Hvis ikke menneske forstår trusselen vil det være vanskelig å forstå valg av styring fra organisasjonen, i tillegg til at menneske vil kunne velge bort prosedyrer mot effektivitet fordi de ikke forstod risikoen. I følge NSM har Forsvaret vært flinkere til å snakke om lederutdanningen sin enn å utøve den, og har mange forskjellige kulturer basert nettopp på utførelse av lederskap. For å skape økt forståelse bør ledere ifølge NSM se sitt ansvar i forbindelse med kulturendring, ta i bruk eksemplets makt og være en motiverende og støttende faktor i risikostyringen. Roer (2015) peker også på at det ikke er nok å implementere nye prosedyrer og teknologi uten å gi de ansatte forståelsen for hvorfor dette implementeres og hvordan det skal håndteres.

Risikobegrepet blir ofte brukt i ulike sammenhenger, med ofte forskjellig og uklar betydning, som vil påvirke risikoforståelsen. Når ulike fagområder skal samarbeide om problemstillinger vedrørende risiko er det viktig med forståelsen for at det ikke bare er en måte å tenke på når det kommer til risiko (Aven et al. 2009 s.37). NSM opplever at forståelsen rundt begrepet security er at det skal håndteres av noen få, at det er noe sært, noe som er på siden, men påpeker at sikkerhet er noe enhver offiser og leder skal ha i bakhodet. Både intervjuene og observatørrollen belyste utfordringen rundt uklar begrepsbruk, og at det gjør det vanskelig å forstå hva som egentlig formidles fra ledelsen. Reason (1997) snakker også om at sikkerheten handler om den kollektive forståelsen av hva som er farlig og

hvordan en klarer å redusere farene. Han legger også til at det ofte blir et spørsmål om prioritering både på tid og økonomi.

Holdninger

I styring av risiko og sikkerhet er det viktig å fokusere på MTO forhold og relasjoner, ettersom alt henger sammen og menneske vil kunne påvirke og være med på styre sikkerheten gjennom handlinger og valg (Aven et al., 2013). NOU (2015:13 s.53) påpeker at enkeltindividets holdninger til sikkerhetsarbeidet og sikkerhetskulturen vil påvirke sikkerhetsnivået. I følge Reason (1997) er det ledelsens ansvar å legge til rette for en rapporterende kultur, hvor de blant annet må bygge tillitt og oppfordre til rapportering for å skape positive holdninger blant ansatte til rapporteringssystemet. På lik linje må lederne forsøke å skape et positivt og sterk arbeidsmiljø for å unngå misfornøyde ansatte. FSA, NSM og CYFOR trekker frem misfornøyde ansatte som den største årsaken for lekkasjer. I følge FSA er det generelt en vilje til å lekke, og det er de mest betrodde individene som lekker, hvor misnøye kan være en årsak. Sikkerhet innebærer en form av handling og viser til våre evne til å eliminere faren (Antonsen, 2009), og i et security-perspektiv vil det også innebærer å inneha de rette holdningene til å bidra til å redusere trusselen og den påfølgende risikoen.

Teknologiske faktorer

Den teknologiske utviklingen og digitaliseringen fører med seg muligheter og risikoer, men det krever en god security-kultur for å evne å se og håndtere begge sider. Generalmajor Roar Sundseth, tidligere sjef CYFOR, (2013) beskrev cybersikkerhet som å bevare integriteten til IKT-baserte systemer som bærer og lagrer data og informasjon, og bevare integriteten til de funksjonene og prosessene som styres gjennom cyberdomenet. For å bevare integriteten vil også menneskelige og organisatoriske faktorer spille inn, slik Roer (2015) beskriver i sin MTO trekant, ref figur 6. I NOU rapporten (2015:13 s.34) uttales det også at cybersikkerhet handler om å beskytte alt som er sårbart fordi det er koblet til, eller på andre måter er avhengig av informasjon- og kommunikasjonsteknologi. I følge resultatene fra lederintervjuene påpekes det at datamaskinene som står i nettverk gjør oss sårbare, og gir en opplevelse av at vi er veldig åpne for innsidetrussel. FSA mener verktøyene vi bruker er ganske godt beskyttet, men påpeker at det er helt umulig å verne seg mot cybertrusler så lenge du har vilje og kamera. I tillegg eksisterer det mange teknologiske muligheter ifølge CYFOR, men det vil alltid være et spørsmål om ressurser, og en forståelse på politisk nivå for hvilken trussel vi står ovenfor. Nytrøen peker på de økonomiske konsekvensene hvor man reduserer på sikkerhetskravene for å få utstyret, som indikerer at man ikke har forstått

risikoen. Både NSM og egen observasjon viser at Forsvaret i enkelte tilfeller ikke har tilgjengelig nødvendige systemer for å håndtere gradert kommunikasjon, som kan skyldes ressurser. En annen side er forståelsen slik Nytrøen påpeker at sikkerhet ikke kan ha ligget som et bærende krav når man ikke kan kommunisere på tvers av forsvarsgrener i komplekse situasjoner.

I følge NOU rapporten (2015:13 s.44) kan IKT-produkter inneholde design- og implementasjonsfeil hvor produktet konfigureres, installeres og brukes på måter som utgjør en stor sikkerhetsrisiko. Videre sier rapporten at sårbarheter i maskinvaren, applikasjonen eller operativsystemet vil ved manglende logging av trafikk og tiltak for å oppdage irregulær bruk og aktivitet gir ytterlige sårbarheter. Det fremkommer av intervjuene at det eksisterer en del mulige tiltak, men det er et ressursspørsmål. En annen side er den hurtige teknologiske utviklingen hvor prosedyrer og instrukser ikke utvikles parallelt. Resultatene fra lederintervjuene påpeker dette ved å vise til at føringer for mobil er lagt inn, men ikke pulsklokker med blåtann og GPS. Tinmannsvik (2008) påpeker at prosedyrer ikke kan inneholde alle mulige eventualiteter, og må justeres for å tilpasse uforutsette situasjoner på en effektiv måte (prosedyrer drøftes mer i dybden under FS2: *Organisatoriske faktorer: Prosedyrer & retningslinjer).*

Organisatoriske faktorer

Prosedyrer og retningslinjer

FSA peker på at det er ganske klare regelsett rundt radiosendere og kamera, og at det er ganske graverende at resultatene fra hurtigintervjuene og observasjon viser store forskjeller i praktisering av føringene. Årsakene til resultatene kan komme av uklare føringer, føringer som ikke er implementert, manglende forståelse, kunnskap og feil holdninger. Feil holdninger trenger ikke være fordi det er dårlige mennesker, men kan skyldes manglende kompetanse og at ledelsen ikke legger forholdene til rette og følger opp. Reglementer, innføringen av dem og opplæring av ansatte vil påvirke security-kulturen (Roer, 2015 s.12). Hvis ikke prosedyrer og retningslinjer innføres slik at ansatte får en forståelse for hensikten, vil det kunne føre til at de ikke blir fulgt, og bidra til en økt risiko.

Prosedyrer og retningslinjer vil ikke bidra til en god security-kultur uten forankring i ledelsen ifølge Reason (1997). Det er dokumentert at svak lederforankring, organisatoriske forhold samt menneskelige feilhandlinger og ubevissthet, er årsaker til mangelfullt sikkerhetsarbeid og uønskede hendelser i IKT-systemer (NOU, 2015:13 s.53). Disse manglende fremkommer av intervjuer og observasjon. På den andre siden er prosedyrer

vanskelig å holde oppdatert og er ofte utgått på grunn av at arbeidspraksisen utvikler seg (Klein, 2011 s.16/21). Blir vi for bundet til prosedyrer kan det vanskeliggjør håndteringen av hendelser i forbindelse med trusler. I følge Klein (2011) kan prosedyrer villede oss og føre til at personellet blir passive og følger stegene i prosedyrene uten å tenke over hva de egentlig gjør, som igjen fører til at vi ikke forsøker å utvikle evnen vår. I følge FSA er ikke nødvendigvis løsningen strengere krav, ettersom det fremkommer at eksisterende krav ikke blir praktisert. Det må skapes en forståelse for hvorfor man implementerer prosedyrene. CYFOR derimot mener det definitivt bør stilles høyere krav i forhold til bruk av mobil, pc, internett og lignende. CYFOR peker i tillegg på utfordringen med eksterne leverandører hvor prosedyrer og kontrollregimer kan bli for skjematiske i forhold til å se menneskene bak skjemaene og gjøre en vurdering rundt hvordan et menneske kan være en innsidetrussel eller ikke. Prosedyrer vil bli ytterligere drøftet under FS2; *organisatoriske faktorer: prosedyrer &retningslinjer*.

Ansvarsforhold og sanksjonering

CYFOR har et ansvar for å håndtere trusler som oppstår i Forsvarets systemer, men Generalmajor Sundseth (2013) understreker at det fortsatt er den enkelte ansatte i Forsvaret som er førstelinjes forsvar mot truslene som eksistere der ute – både militære og sivile trusler. Hvis ikke Forsvarets ansatte forstår trusselen, vil det kunne føre til økt sårbarhet for organisasjonen. Dette kan forplante seg til mangelfull rapportering, som igjen vil gi øverste ledelse et mangelfullt risikobilde og grunnlag for å tildele nødvendige ressurser. Forståelse drøftes videre under FS2; *Menneskelige faktorer: Forståelse.*

Reason (1997) mener det er et lederansvar å legge til rette for en rapporterende kultur, og frykt for represalier kan hindre rapportering. Tinmannsvik (2008) peker også på at det må være stor tak høyde, det er «lov å gjøre feil», og forsøke å gi personellet en trygghet til å rapportere feil. Samtidig kan det være avvik som kan få så alvorlige konsekvenser at arbeidsgiver må gripe inn med disiplinære tiltak. Organisasjonen må ha en klar linje og lederne må forstå sitt ansvar i håndteringen av rapporterte saker for å skape tillit blant ansatte og oppfordre til rapportering. Reduksjon av risiko vanskeliggjøres ved at ledere ikke oppfordrer til rapportering og at det ikke bygges et bilde ut fra rapporterte trusselrelaterte hendelser. Velvillig deltakelse fra ansatte er meget viktig i et sikkerhetsinformasjonssystem, og for å oppnå dette er det nødvendig å utvikle en rapporterende kultur som har utspring fra ledelsen (Reason, 1997).

FSA mener at vi kan forvente å ha noen på innsiden og derfor bør ha dette som en arbeidshypotese. Dette fordrer at ledelsen også her tar ansvar for gjennomføring av autorisasjonssamtaler, og forstår hvorfor dette er viktig. I tillegg har vi sikkerhetsklareringsprosessen som handler om å redusere risiko på enkelte elementer på mennesker som kan ha en for høy grad av manglende lojalitet og dømmekraft i enkelte situasjoner som kan utnyttes av en aktør (NSM).

Læring

HRO-teorien tar utgangspunkt i at organisasjonens fokus hele tiden må være på sikkerhet og pålitelighet gjennom blant annet læring. Den hurtige teknologiske utviklingen og medfølgende trusler og risiko krever også en organisasjon som lærer og utvikler seg parallelt, eller må man akseptere at organisasjonen ikke klarer å følger utviklingen? Organisasjonens evne til å trekke riktige konklusjoner av hendelser rapporter i et sikkerhetsinformasjonssystem bidrar til en lærende kultur. I følge Reason (1997) handler det om å ha et kritisk syn på eksisterende praksis og vilje til å implementere endringer, tiltak eller reformer som kan være nødvendig med bakgrunn i sikkerhetsinformasjonssystemet. CYFOR mener at security-kulturen lider under fokuset på funksjonalitet og få ting til å fungere fremfor et fokus på sikkerhet og pålitelighet gjennom blant annet læring (HRO). De åpne fagintervjuene pekte også på begrepsforvirringen, som vanskeliggjør læring når det ikke er forståelse for at security-aspektet må ivaretas.

6.2 FS2: Hva er kjennetegn ved Marinens security-kultur?

I fase en av forskningsprosessen fokuserte vi på kjennetegn ved Marinens security-kultur i tillegg til trusselbildet for Marinen. Under punkt 6.2 drøftes de analyserte funnene fra empirien til FS2 belyst av det teoretiske rammeverket for oppgaven.

Menneskelige faktorer

Kompetanse

Douglas og Wildavsky (1982) mener at risiko er sosialt betinget og vil bli påvirket av sosiale prosesser og kulturelle mønstre, og som en konsekvens vil oppfattelsen av risiko variere, og dermed også evaluering og håndteringen (Antonsen, 2009). Vi stilte spørsmål til informantene om hva de mener innsidetrussel er. Resultatene var veldig forskjellige, og ingen gav en fullstendig beskrivelse av trusselen. I følge Aven et al. (2009) avhenger risiko av hvem som vurderer og hva som vurderes. Det innebærer kunnskap om hva begrepene betyr, kjennskap til utstyr og materiell og ikke minst kunnskap om sårbarheter og trusler. Kompetanse er bare et element i kultur bygging, men essensielt. I følge NSM er det mangel

på kunnskap som gjør at folk tror det er trygt å snakke på telefonen og ikke forstår at det de legger ut på nettet er for andre puslebrikker i et større bilde.

FSA mener blandingen av safety og security-begrepene skaper forvirring. Hvis direktiver, prosedyrer og regler ikke er tydelige på definisjonene av begrepene, vil det være vanskelig på et lavere nivå i organisasjonen å formidle kunnskap om håndteringen av security. I følge Reason (1997) vil en informert kultur ha kunnskap om alle faktorer som har betydning for sikkerheten, som nyttes proaktivt til å finne tiltak for å forhindre uønskede hendelser i fremtiden. Forsvaret bør ikke bare etablere klare begrepsdefinisjoner, men sørge for at dette blir implementert i utdanning og praksis for å være i stand til å bygge en security-kultur.

Forsvaret må som helhet fokusere på at vi har en trussel, at vi har en risiko, se på hva det betyr og hvordan organisasjonen skal håndtere den, uttaler FSA. Tablet (2010) og Aven (2014b) mener at fremtiden preges av stor usikkerhet og at en derfor ikke må legge for stor vekt på historisk data. Det vil bare være en utfordring for utdanningssystemet å skape et kunnskapsnivå innenfor security uten klare definisjoner, men også for de som bli satt til å håndtere security i praksis. CYFOR underbygger forvirringen rundt begrepene og viser til at de blander safety og security i *«Direktivet – krav til sikkerhetsstyring i Forsvaret»*. CYFOR understreker viktigheten at fagfeltene safety og security kommuniserer sammen, samtidig som risikovurderingene sett et security-perspektiv vil innebære noe helt annet en i et safety-perspektiv. Roer (2015) mener også det trengs en opprydding i begrepsapparatet og skiller klart mellom safety som uhell, ulykker og security til å handle om abstrakte verdier, informasjonssikkerhet, ondsinnet handlinger. Samtidig viser Talbot og Jakeman (2009) til at teorien som beskriver begrepet security-kultur er forholdsvis lik med beskrivelsen av safety kultur hvor elementer for å forme adferd, holdninger og tillit er med å bygge enhver kultur.

Sorte svaner har blitt en metafor på den feilaktige antakelsen at hvis man ikke har kunnskap om noe eller hvis man ikke vet, så eksisterer det ikke (Aven, 2014b). Håndtering av uønskede hendelser i et security-aspekt innebærer en mye større usikkerhetsfaktor, og sannsynligheten for at en militær avdeling møter ukjente trusler er mye større enn i andre organisasjoner. Aven (2014a s.84) refererer til sorte svaner som «en overraskende, ekstrem hendelse sett i forhold til ens kunnskap og tro». Aven (2014b) og Tablet (2010) mener begge at usikkerhet er det motsatte av kunnskap og at usikkerhetsfaktorene befinner seg der de sorte svanene er. Usikkerhetsfaktorene vil alltid være der, men kunnskap og kompetanse kan bygges til å bedre håndtere dem. I følge Klein (2011 s.173) er ikke kunnskap nok, men forklarer sensemaking som kjernen til å lære kognitive ferdigheter ettersom vi ikke bare

tilegner oss ny kunnskap, men endrer måten vi ser og tenker om ting. Sensemaking innebærer å se hva som førte til hendelsene som foregår og kunne forutse hvordan våre handlinger sannsynligvis vil påvirke fremtidige hendelser. Dette fremhever Klein (2011 s.173) som essensielt for å lære av tilbakemeldinger, og vi kommer tilbake til det under det organisatoriske perspektivet og læring.

I forhold til spørsmålet om Sjøforsvaret sikkerhetspolicy fremkom det klart fra hurtigintervjuene at 89% ikke hadde noe forhold til policyen. I D*irektivet – krav til sikkerhetsstyring i Forsvaret* (2010) punkt 4.2 er det kun føring til utarbeidelse av en policy for sikkerhet. Det kan virke som enkelte er kjent med den, men at det er kulturen i praksis som er gjeldene og vil kunne beskrive hva i policyen som etterleves. Policyen fremstår i dag «ullen», og lite håndfast. At den er vanskelig å konkretisere kan være det som gjør at den ikke blir brukt. Hvis de heller ikke ser sammenhengen med den og det faktiske arbeidet, hvorfor skal de bruke tid på å gå igjennom den? Videre i forhold til opplæring i innsidetrussel svarer 44% at de ikke har fått noen opplæring, 25% at de har fått opplæring, mens 35% hadde andre svar. Det fremkommer at opplæringen er litt tilfeldig og den består primært av brifer fra forskjellige internt i avdeling, internt i Sjøforsvaret eller fra NSM og PST. I det teoretiske rammeverket beskrives sensemaking av Weick (1995) som den kognitive prosess som foregår når vi forsøker å skape mening av det som skjer i våre omgivelser. Det er større krav til håndtering av trusler av en militær organisasjon som Marinen sammenlignet med sivile organisasjoner, og sensemaking vil bidra til å håndtere fortløpende kompleksitet og usikkerhet ved en tilsiktet uønsket hendelse. Resultatene fra fag-, leder-, hurtig-intervju og observatørene viser at Marinens utdanning og opplæring innenfor security ikke er gjennomgående eller har en rød tråd. I følge Klein (2011) er sensemaking kjernen til å lære kognitive ferdigheter ettersom vi ikke bare tilegner oss ny kunnskap, men endrer måten vi ser og tenker om ting – gir mening til motstridende og forvirrende data. Sensemaking for Marinens ansatte, uten grunnleggende kunnskap, vil være vanskelig.

FSA gjennomfører mye kurs, men primært for personell med en sikkerhetsrolle eller som en del av sikkerhetsorganisasjonen, og toppledelsen for at de skal kunne bringe det inn i sin del av organisasjonen. En utfordring her er den uklare begrepsbruken, og klare føringer for hva som kreves av stillinger, arbeid, ressurser og tid ikke bare for å etablere en security-organisasjon, men også å implementere security-kultur og gjøre organisasjonen i stand til å ivareta arbeidet. NSM, FSA og CYFOR belyser behovet for den røde tråden, og at security blir innlemmet i hele utdanningsløpet for Forsvaret. Nytrøen påpeker også den manglende undervisningen når det kommer til trussel og security på bakgrunn av 70 år med fravær av

noe vi oppfatter som en trussel. Dette er ifølge Nytrøen en indikator på manglende risikoforståelse, og at fravær av opplevd trussel gjør noe med sikkerhetskulturen, og at det ikke prioriteres ressurser til å beskytte oss. Sensemaking innebærer å forstå hendelser som har funnet sted for å forutse hva som kan skje videre, ikke bare se sammenhengen mellom elementer, men se det i et historisk perspektiv som knyter dem sammen (Klein, 2011). Sensemaking handler om kunnskap, ekspertise, erfaring for å operere i gitte rammer og evne å nytte seg av data tilgjengelig. Resultatene fra intervjuene viser til manglende kunnskap for trusler og hele security-aspektet organisasjonen må håndtere, som vil kunne påvirke evnen til å håndtere trusler.

Forståelse

Personellet i en organisasjon er sjelden enig om hva dataene forteller dem eller hvilken betydning det har for organisasjonen, noe som vanskeliggjør å få samlet dataene til en sammenhengende historie (Boin et al., 2015 s.22). Hvis ikke personellet forstår egne sårbarheter, verdier og trusler de kan stå ovenfor vil det kunne føre til splittelse i håndtering av situasjoner og at hva de står ovenfor oppdages for sent til å beskytte seg. Hurtigintervjuene viste at 61% mener innsidetrussel er noe de kan bli utsatt for, og 94% mente Sjøforsvaret er sårbar for innsidetrussel. Divergensen her kan skyldes manglende forståelse for hva en innsidetrussel er, og mangel på opplevd trussel. De antar at Sjøforsvaret er sårbar, men tror ikke nødvendigvis det er noe som treffer dem. Dette understrekes av Nytrøen og NSM som viser til Marinens manglende reelle erfaring med trussel hvis man ser på oppdrag i senere tid.

Resultatene fra hurtigintervjuene viser en delvis forståelse ovenfor trusselen, men samtidig manglende forståelse for egne sårbarheter: *«vi har ikke så mye kompromitterende utstyr her hos oss». «Vi har ingenting å skjule». «Det er jo bare en øvelse».* I følge Bovens og t'Hart (1996 s.25) er oppfattelsen av en trussel subjektiv, og før man kan snakke om en krise, må det være et betydelig antall aktører som er enige om at en trussel eksisterer og må håndteres snarest. Sensemaking innebærer å forsøke å forstå hendelser som har funnet sted og å forutse hva som kan skje videre, og baseres på erfaring og kunnskap (Klein, 2011 s.172). Resultatene fra intervjuene og observasjoner viser Forsvarets manglende begrepsavklaring, manglende føringer for hva security organisasjonen skal bestå av/utføre av arbeid og manglende ressurser viser til et mangelfullt grunnlag for sensemaking og evne hendelseshåndtering.

For Marinens ansatte er det også en utfordring at de hver eneste dag snakker og håndtere gradert informasjon delvis åpent på arbeidsplassen. Det krever en større bevisstgjøring for å klare å skille mellom gradert og ugradert i forhold til hvem som befinner seg i nærheten, om det er besøk, andre arbeidere, andre ansatte som ikke trenger å være kjent med den informasjonen, om de selv befinner seg utenfor arbeidsplassen, med samarbeidspartnere, med familie og lignende. Roer (2015) peker på at det ikke hjelper å stramme inn uten å ha forståelse for innsidetrusselen, og at det også må være en forståelse for teknologien for å kunne utarbeide hensiktsmessige prosedyrer og regler. Marinen må også håndtere begrensede ressurser både med tanke på personell og materiell. Det påvirker utfordringer som pålagt seiling, hvor det er lite tid, det mangler utstyr, personell, men ordren er at fartøyet skal forlate kai til en gitt tid. Selv om det da eksisterer forståelse av behovet for ivaretakelse av security-perspektivet, er dette noe som vil bli skjøvet til siden. Årsaker kan være manglende opplevelse av en trussel som gjør at det kreves tiltak, eller at security-rollen bare er en prosentandel av en annen stilling og at man tidsmessig ikke får håndtert det. Det fremkommer ikke innarbeidet i kulturen, da det ikke er en del av det daglige fokuset. Dette vanskeliggjør en kontinuerlig overvåking av situasjoner basert på forventninger og antagelser, oppdatering ut ifra erfaring slik Weick og Sutcliffe (2007) beskriver mindfulness som en del av HRO. Hvis Marinen ikke har kunnskap og forståelse, vil en antagelse være at de også mangler erfaring med security og innsidetrusselen. Nytrøen understreker viktigheten av å forstå trusselen, en forståelse han mener ikke er god nok i Forsvaret, for å kunne sette av ressurser og tid, og at det til slutt handler om å beskytte oppdraget.

Holdninger

Reason (1997) beskriver at en informert kultur har kunnskap om alle faktorer som har betydning for sikkerheten og bruker denne pro-aktivt ved å finne tiltak for å forhindre uønskede hendelser i fremtiden. Et sikkerhetsinformasjonssystem må opprettes hvor en får inn, analyserer og formidler informasjon om uønskede hendelser. Hvis holdningen i organisasjonen fører til mangelfull rapportering vil grunnlaget for tiltak være dårlig. Hurtigintervjuene viste at 58% har erfart at de selv eller andre har valgt å ignorere sikkerhetstiltak, og 61% har erfart at de selv eller andre har latt være å rapportere brudd. Den interne forskjellen mellom avdelingene i diagram 5, hvor avdeling 2 og 3 har større erfaring med at brudd ikke blir rapportert, sett opp mot avdeling 1 kan indikere at avdeling 1 er flinkere til å rapportere. På den andre siden kan det også være en indikasjon på at de ikke vil innrømme mangelfull rapportering.

At resultatene fra diagram 4 (58% ignorert sikkerhetstiltak) og 5 (61% ikke rapportert brudd) har så høy og lik prosentfordeling på «ja», kan indikere en dårlig holdning og adferd i forhold til security-kultur. Årsaken kan være mangelfull forståelse og kunnskap da flere informanter uttrykker at det ofte skyldes uhell eller manglende forståelse. Derimot uttales det også at både dårlige holdninger og ulike føringer ligger til grunn. Når det i tillegg fremkommer at mange vurdere selv på lavere nivå om sikkerhetsbruddet er alvorlig nok til å rapporteres, skapes det en ekstra sårbarhet for Marinen. Det vil også kunne gjøre det vanskelig for høyere nivå, 1, 2, og organisasjonene som jobber med å kartlegge og håndtere trusselen, å få et reelt bilde av behovet/sikkerhetstilstanden i den taktiske og operative enden av Sjøforsvaret.

NSM viser til at det trengs mer enn bevisstgjøring og kunnskap for å skape en kultur, og tror grunnleggende at mennesker er stolte av arbeidsplassen og ikke ønsker å utvise dårlig holdninger. NSM uttaler videre at det er lettere å få personellet til å forstå bruk av eksempel hjelm, «*fremfor å få en byråkrat å passe på en informasjon som på sikt kan føre til samme konsekvenser dersom noen agere på det*».

For håndtering av komplekse og uforutsigbare situasjoner hvor man står ovenfor en trussel er det behov for å utvise dømmekraft, sensemaking og resilience (Klein, 2011). Skal Marinen som en enhet håndtere tilsiktede handlinger kreves en security-kultur hvor overnevnte begrep er innlemmet.

Andre årsaker til brudd av sikkerhetstiltak og manglende rapportering på hendelser som blir belyst i hurtigintervjuene er bekvemmelighetshensyn, tidspress og operativ kapasitet. Det fremkommer også fra intervjuene at de ønsker at det skal være tillit til at folk rapporterer, men det avhenger at forståelse, kunnskap og holdninger er på plass. Det må være en atmosfære der de ansatte blir oppmuntret til å dele viktig sikkerhetsrelatert informasjon (Reason 1997). I tillegg ønsker informantene se positive resultater fra rapporteringen, som vil kunne motivere til ytterligere rapportering. En annen side her er rapporteringsverktøyet. Det må være kjent og enkelt. Dette utdypes under det organisatoriske aspektet og underpunktet læring, hvor CYFOR foreslår en enklere løsning enn dagens, som systemmessig vil kunne bidra til flere registrerte hendelser.

I følge Reason (1997) er det et lederansvar å legge til grunn for en rapporterende kultur, derav også holdningene til rapportering. For å innlemme security i kulturen må lederne ta sitt ansvar og sette det på dagsordenen for hele organisasjonen og forstå sitt ansvar ovenfor de

ansatte. For å skape de rette holdningene må systemet være enkelt og funksjonelt, ledelsen må ha satt av tid og ressurser. *«Det krever litt av en leder å få endret kulturen, ettersom du i noen tilfeller skal følge gitte prosedyrer, men av og til må det gjøres en vurdering om at du ikke skal følge prosedyren»* (NSM). Dette støttes av Klein (2011) som sier at prosedyrer kan villede oss og føre til at personellet blir passive, følger stegene i prosedyrene uten å tenke over hva de faktisk gjør. Dette utdypes under det organisatoriske perspektivet og underpunkt læring. Roer (2015) mener på den andre siden at arbeidet med å forbedre security-kulturen ikke nødvendigvis må starte fra ledelsen. Dette utdypes O: Ansvarsforhold & sanksjoner.

På spørsmålet om arbeidsmiljøets påvirkning på ansattes sikkerhetshåndtering svarer 61% nei, og 89% svarer nei til at dårlig personellforvaltning har bidratt til sikkerhetsbrudd eller ikke rapportering. Det betyr ikke nødvendigvis at security-miljøet er bra, og informantene som har svart ja beskriver at man blir påvirket hvis en person bryter føringene, og det er lett å følge andre i troen på at det er slik det skal gjøres. Noen av informantene som svarte nei trekker allikevel frem at holdningene kan av og til være dårlige, og det er vanskelig å være den som strammer inn. Faktorer for å skape et klima med tillit og motivasjon for rapportering er blant annet følgende; som at personell er sikret mot disiplinære reaksjoner og at rapportering er konfidensiell (Reason, 1997). Det påpekes også at arbeidsmiljøet og påvirkningen avhenger av hvor mye opplæring som har vært, og at manglende daglig fokus påvirker. Det er liten kritikk til ledelsen, men manglende kunnskap og forståelse for hva som burde gjøres kan være en årsak.

Roer (2015) viser til at vi har et bredt spekter av adferd, og når man er sammen med andre bruker man fra spekteret og tilpasser seg. Vi blir påvirket av miljøet og holdningene til menneskene vi omgås. Misfornøyde ansatte utgjør en stor trussel ifølge FSA, NSM, CYFOR, Nytrøen og Roer, men det fremkommer få uttalelser som underbygger dette. Det kan komme av feil spørsmålsformuleringer, eller at ingen ønsker å innrømme det. I følge NSM er sannsynligvis den beste forsikringen mot innsidetrussel å ha glade og fornøyde ansatte, som føler en stolthet og lojalitet mot arbeidsplassen sin og som føler de blir verdsatt, ivaretatt og tenkt på. NSM underbygger lederansvaret for å endre kultur: *«Forsvaret har vært flinkere til å snakke om lederutdanningen sin enn å utøve den, og jeg tror at man endrer kultur avhengig av hvordan lederen opptrer og hvor bevisst lederen er på det»* (NSM).

Organisatoriske faktorer:

Vi vil i denne delene av oppgaven drøfte resultater fra empiri FS2, «*organisatoriske faktorer*», opp mot teoretisk grunnlag. Drøftingen er delt inn under *prosedyrer & retningslinjer, ansvarsforhold & sanksjoner og læring*.

Prosedyrer og retningslinjer:

Reason (1997) sitt perspektiv på en god sikkerhetskultur innbefatter fire del komponenter og omtaler disse som en informert kultur. Deler av dette innbefatter at ledelsen gjør revisjoner og justeringer av blant annet prosedyrer og arbeidspraksis for å ivareta sikkerheten på en best mulig måte for organisasjonen. Marinen har prosedyrer og retningslinjer på hvordan en skal forholde seg til security og dette er beskrevet i grunnlagsdokument sikkerhet (GDS). De fleste lederne og sikkerhetslederne i avdelingene er kjent med sikkerhetsloven og GDS-dokumentet (spørsmål 5). Klein (2011) påpeker viktigheten av prosedyrer i sin første påstand, hvor prosedyrer bidrar til å evaluere utførelse. Prosedyrene er blant annet en støtte til hukommelsen og skal forhindre forstyrrelser, men utfordringen er at de ikke er sensitive til kontekst (Klein 2011). I intervjuer fremkommer det at *«retningslinjene innenfor fagområdet security er ganske klare i forhold til andre fagområder*» (leder 18), men retningslinjene utføres ulikt i praksis mellom avdelingene. Det er også ulik praksis mellom enheten/fartøyene innad i avdelingene. En sterk organisasjonskultur som setter pålitelighet høyt, vil øke sikkerheten ved at alle på lavt nivå oppmuntres til å reagere likt og riktig (Aven et al., 2013).

På den ene siden kan faktorer som ressurser, herunder personellantall, spille inn som en årsak til ulik praksis, mens det på den andre siden kan være kompetansen og kunnskapsnivået hos personellet. En leder (19) sier at «*ulike kunnskap gir ofte ulik policy*», med ulik policy mener han praksis. En annen leder (37) uttrykker at det «*avhenger av avdelingens ASL sin kunnskap og initiativ*». På den ene siden har Marinen retningslinjer som skal følges, mens det på den andre siden fremkommer i intervjuer at flere sjefer nedover i organisasjonen tillegger strengere krav. Dette er en av kjennetegnene ved en HRO, hvor fokuset hele tiden må være på sikkerhet og pålitelighet gjennom desentralisert styring (Aven et al., 2013). Det kan være en mulig årsak til at avdeling 1 praktiserer retningslinjene strengere enn de andre 2 avdelingene. FSA mener også at det må lages et fornuftig regelsett for praksisen, og dette må følges opp. Det er gjennomgående mange informanter som mener kunnskapen og forståelsen innenfor security og innsidetrussel er for lav blant de ansatte. Prosedyrer blir ofte laget for å endre adferd, men i henhold til Klein (2011) kan det være

enklere og mer effektive måter å gjøre det på. Prosedyren (GDS) sammen med økt kunnskap og forståelse på fagområdet og trusselen, kan bidra til mer lik praksis innad i en avdeling og skape mindre forvirring hos de ansatte når de ser forskjellene som praktiseres. Hovedbudskapet til Klein (2011) er ikke å forkaste prosedyrer, men hva som må gjøres i tillegg for å gjøre et bedre arbeid.

Ved Klein (2011) påstand en, skapes et dilemma om å gjøre jobben korrekt eller å holde seg til prosedyrene. Hvor å ikke holde seg til prosedyrene kan føre til straff, og å holde seg til prosedyrene men ikke få gjort jobben også kan bli straffet. Det er flere informanter som uttrykker at tidspress kontra det å forholde seg til prosedyrene og retningslinjene kan være utfordrende. På den ene siden er det viktig å gjennomføre jobben innen gitt tidsfrist slik at det ikke lager forsinkelser i planlagt aktivitet, mens personellet på den andre siden er pålagt å følge prosedyrer og retningslinjer innenfor security. Noe som i enkelte situasjoner kan forsinke arbeidet. Det er viktig at personell på lavere nivå signaliserer dette oppover i organisasjonen, slik at ledelsen i Marinen får innsikt og forståelse for situasjonene hvor dette blir et dilemma. Det kan argumenteres for at ledelsen i Marinen bør tilstrebe at ulike føringer som blir gitt ikke kommer i konflikt med hverandre slik at det vanskeliggjør jobben til ansatte på lavere nivå. Reason (1997) påpeker at sikkerhetskulturen handler om den kollektive forståelsen av hva som er farlig og hvordan en klarer å redusere farene, og at dette ofte blir et spørsmål om prioritering på både tid og økonomi.

Det er også ulikheter mellom avdelingene når de skal svare på hvilke føringer som er lagt for å rapportere security-hendelser (Diagram 6). 33% sier at de ville rapportert til sikkerhetsleder og 27 % sier tjenestevei. Avdeling 1 har flertallet på sikkerhetsleder, avdeling 2 vil rapportere tjenestevei mens i avdeling 3 er de mer usikre. Det er hele 25% som ikke vet hvordan de skal rapportere hendelser. På den ene siden kan det være at føringene/prosedyrene er noe uklar, mens det på den andre siden kan være at retningslinjene blir innført ulikt og at dette påvirker opplæringen av de ansatte i de ulike avdelingene. Roer (2015) uttaler at reglementer, innføringen av dem og opplæring hos de ansatte påvirker security-kulturen.

De ansatte, som har deltatt i studien, sier hele 84% at de ville godtatt strengere føringer på bruk av mobil, Pad, PC, for å bidra til å redusere Sjøforsvarets sårbarheter for fiendtlige handlinger (Diagram 7). De ansatte er villig til å strekke seg lang selv om dette kan gå utover deres kontakt med omverden i perioder. Dette overrasker ikke leder (19) som uttaler «*de har begynt å skjønne det*», men påpeker at skal det iverksettes strengere føringer, må alternative

muligheter brukes. FSA mener derimot at løsningen ikke nødvendigvis er strengere krav, ettersom det kan fremkomme at eksisterende krav ikke blir praktisert likt. De mener at det er utfordrende nok å forklare de som er. På den ene siden bør en organisasjon regulere aktivitet gjennom regler og prosedyrer, men samtidig bør de opprettholde evnen til kunnskapsbasert problemløsning hos de ansatte (Tinmannsvik, 2008). Roer (2015) sier at vi må forstå innsidetrusselen og at det ikke hjelper å stramme inn hvis man ikke vet hvorfor og ikke har forståelse. «*Forstå teknologien først før man regulerer bruk og utarbeider policy»*. Også her kommer det til kompetanse/ opplæring innenfor fagområdet og forståelse for trusselbildet hos de ansatte. *«Bedre forståelse vil gjøre at tiltakene blir bedre. De som lager tiltakene må ha kunnskap og forståelse for å få gode tiltak» (171).*

CYFOR på den andre siden mener at vi definitivt bør stille høyere krav i forhold til bruk av mobil, PC, internett og lignende. Ulik praksis på avdelingene og uttalelsene fra FSA og CYFOR kan tyde på at det ikke er helt enighet i hvor streng retningslinjene skal være. Som leder (18) sier: «*Vi er uenig, forskjellig tilnærming*».

Flere ledere tror ikke at det er gjort noen sårbarhets- eller risikoanalyser ved utarbeidelse av GDSene. Lederne er i alle fall ikke informert eller kjent med at det gjøres slike vurderinger. Verken på organisasjons- eller fartøys nivå. Nasjonal sikkerhetsmyndighet (NSM 2015a s.10) sier for å vurdere risiko må det gjennomføres verdi-, trussel- og sårhetsvurderinger. Hvis dette mangler i Marinen, hvordan klarer da ledelsen å vurdere risikoen for så å lage gode prosedyrer og iverksette riktige tiltak?

Det er derimot tilsynelatende mer enighet blant flere informanter at dokumentasjonen og prosedyrer er for tilgjengelig for alle med tilgang til det graderte nettverket (Fisbasis) i Sjøforsvaret. På den ene siden er det viktig å dele dokumentasjon og informasjon, mens det på den andre siden er viktig at dokumentasjonen ikke er for tilgjengelig for alle, da dette kan bli en faktor som kan øke sårbarheten for lekkasjer. CYFOR har også registrert at Forsvaret ikke er flinke på internkontroll i forhold til tilganger på systemene og understreker at dette må tas inn som en del av rutinene og internkontrollen. I det daglige deles det mye informasjon og dokumentasjon på det graderte interne nettverket, uten at de ansatte nødvendigvis merker det med gradering opp til og med begrenset. Dette sammen med at det er alt for mange som har tilgang til informasjonen gjør at en ikke har kontroll på den.

Ansvarsforhold og sanksjoner:

Ved en god sikkerhetskultur søker organisasjonen informasjon om organisatoriske faktorer som kan ha betydning på sikkerheten. Dette handler om å opprette et

sikkerhetsinformasjonssystem og at det gjennomføres proaktiv kontroll av tilstanden i organisasjonen (Reason, 1997). Dette er også et kjennetegn ved en HRO, når det kommer til proaktivt og se etter «*problemer i miljøet*» og melde disse oppover i organisasjonen (Boin et al., 2015). Det er ulike meninger på hvilket nivå innsidetrussel bør håndteres. 47% mener at det bør håndtere på alle nivåer, 36% sier på laveste mulig nivå og oppover i organisasjonen, 9% mener det må håndteres på ledelsesnivå og 8% sier at dette må håndteres fra topp i organisasjonen og nedover (Diagram 8).

Det er ledelsens ansvar å legge til rette for en security-kultur (Reason 1997), men på den andre siden presenterer Roer (2015) det han kaller *«grasrotbevegelsen»* og mener at ansatte på laveste nivå kan starte det nødvendige arbeidet for å utvikle security-kulturen, og ved å vise resultatene til ledelsen vil det kunne føre til deres støtte og nødvendig tildeling av ressurser. En leder (18) uttrykker at slik det nå er det «bottom-up» og at det er personellet på laveste nivå som kjenner regelverket og som skriker etter ressurser for å gjør det som står i regelverket. Lederen mener vi trenger å bygge opp en «topp-down» oppbygging på en sikkerhetsorganisasjon. «*Hvis dette hadde vært topp styrt hadde det kanskje vært mulig*» (Leder 18).

Klein (2011) påpeker i sin påstand fem at ledere kan skape en felles plattform ved å tildele roller og etablere grunnleggende regler i forkant. Men en felles plattform er aldri perfekt og vil kontinuerlig brytes ned, en må derfor kontinuerlig monitorere og reparere den underveis. Svarene fra informantene under hurtig intervju tyder på at det ikke er en lik oppfatning på hvilket nivå innsidetrusselen bør håndteres. Er det da en felles plattform for avdelingene? Det påpekes også i forbindelse med håndtering at «*det er forskjellig måter å håndtere det på, på de forskjellige båtene i forskjellige våpen* (avdelinger)» (161). Flere ledere trekker frem viktigheten i forankring i ledelsen på alle nivåer. Det fremkommer i intervju at det har vært veldig fokus fra øverste ledelse på å bygge opp en safety kultur. «*Ledere blir målt på safety, det har vært prioritert*» (91). En leder (18) uttrykker at skal vi få fokus på security må en gjøre det på samme måte som ved safety, få fokus på det nedover i organisasjonen. Skal security håndteres «*må det tas grep over hele linjen*» (leder 18). Viktigheten av å ha gode rollemodeller ovenfra og ned trekkes frem på lavere nivå, «*hvis sjefen ikke bryr seg så bryr ikke jeg meg*» (423). På den ene siden er det viktig å ha forankring og fokus fra ledelsen, men på den andre siden er det ikke en enmanns jobb når det kommer til security-kultur, det er flere som må involveres (Roer, 2015).

Alle informantene ved hurtig intervju uttrykker at de selv har en eller annen form for ansvar for å sikre arbeidsplassen mot innsidetrussel. Flere snakket om viktigheten av årvåkenhet/ oppmerksomhet, ikke lekke informasjon muntlig eller i sosiale media, overholde regelverket og passe på graderingsnivå og graderte papirer. På den ene siden virker det som at informantene er innforstått med at de har et ansvar for å sikre arbeidsplassen mot innsidetrussel, mens det på den andre siden kan virke som de har fått ulik opplæring på hvilket ansvar hver enkelt har. Kun 19,4% (7 av 36) av informantene trekker frem at de har et ansvar for å rapportere innenfor security, selv om det er føring på at sikkerhetsbrudd skal rapporteres. Dette resultatet kan tyde på deres ansvar for å rapportere ikke er blitt tydelig nok formidlet fra ledelsen. Det er en leders ansvar å legge til rette for en rapporterende kultur (Reason, 1997), men det fordrer også at personellet rapporterer. Rapporterende kultur vil bli drøftet grundigere under organisatoriske faktorer seinere i oppgaven.

Ved en HRO må organisasjonens fokus hele tiden være på sikkerhet og pålitelighet gjennom blant annet organisasjonens redundans og (Aven et al., 2013). Dette er også noe Boin et al. (2015) uttrykker og trekker frem robusthet (resilience) som en faktor i HRO. Leder (19) trekker frem at security organisasjonen har vært et nettverk med dyktige sikkerhetsoffiserer, men at det ikke er noen robust organisasjon. *«Var noen borte satt du egentlig med et betydelig hull selv om en hadde en assisterende stedfortreder. Så man svekkes ganske fort hvis noen er borte*». Det har frem til 1/8-16 kun vært en 100% stilling i Marinen til security, mens alle sikkerhetsledere i avdelingene har hatt rollen som en prosentandel i sin stilling. På den ene siden uttrykker lederne at det er utfordrende med prosentandel innenfor security og at prosentdelen er «*veldig liten*» (Leder 19). Langt fra alle sikkerhetsledere har gjennomført kurs innenfor fagfeltet og «*kravet til kunnskap har økt noe voldsomt den siste tiden»* (leder 19). På den andre siden uttrykkes det at det er viktig å få støtte fra spesialistene i landorganisasjonen og at dette er godt nok. Men hvis den ene 100% stillingen er fraværende på grunn av en eller annen årsak, og dette er støtten for avdelingene på lavere nivå, svekkes robustheten i organisasjonen. Samtidig kommer det frem at ledere kan ikke være spesialisten innenfor security, men at leders rolle er å sørge for at spesialisten får arbeidsrom og at alle hører på vedkommende og søker råd. Dette omhandler også fleksibel kultur hvor en går fra kollegial autoritet, samt at formell rang har mindre betydning. Den med best kompetanse for oppgaven avgjør handlingen når det er nødvendig (Reason, 1997).

Det fremkommer i empiri at både sikkerhetsledere og ledere ikke har en lik forståelse for hvem Marinen samarbeider med om cybertrussel og hva organisasjonene (FSA, CYFOR, NSM) har ansvar for. Samtlige sikkerhetsledere og ledere trekker frem LKM. «*LKM er*

sentral i Sjøforsvaret for å koordinere all den virksomheten her» (Leder 18). Det kan tyde på at det ikke er godt nok kommunisert i Marinen hva de ulike organisasjonene (FSA, CYFOR, NSM) kan tilby av støtte til Marinen på de ulike nivåene. En leder (37) sier «*jeg tror at mye av det security baserte rapporteres til FSA direkte fra fartøyet, men ute av Sjøforsvarets håndtering. Jeg vet ikke så mye hva FSA gjør med det etterpå*». Klein (2011) sier vi trenger tilbakemelding på prosessen, men ikke minst må tilbakemelding gi mening. Det er derfor viktig å få tilbakemelding på det som rapporteres. Derimot argumenteres det imot at tilbakemelding i seg selv ikke er tilstrekkelig (Klein, 2011). I komplekse situasjoner må vi lære å tolke tilbakemeldingene, knytte handlingene til konsekvenser, sortere ut relevante og tilfeldige årsakssammenhenger.

En rettferdig kultur mener Reason (1997) er nesten et uoppnåelig ideal. Sanksjoner og rettferdig kultur henger tett sammen med rapporterende kultur, hvor frykt for represalier kan hindre rapportering. På de ene siden bør personellet være sikret mot disiplinære reaksjoner, så langt det lar seg gjøre (Reason, 1997). Mens det på den andre siden bør være uakseptabelt å gi full «immunitet» fra straff på alle handlinger som kunne ha/har bidratt til uønskede hendelser. Fire informanter trekker frem at det vil motivere hvis de er fokus på læring og ikke straff. Flere informanter prater om frykt for personlige negative konsekvenser (121, 343) og negative sanksjoner, som eksempel å «*bli forflyttet til annet tjenestested*» (433), «*frykt for å ikke få opprykk*» (171), «*redd for å bli hengt ut og miste tilliten fra ledelsen*» (212) eller «*at det kommer på papiret*» (363). To informanter i henholdsvis avdeling 2 og 3, henviser til «trusler» om straff ved eksempel militærpolitiet (MP), noe som kan bidra til at de kanskje ikke vil rapportere hendelser i fremtiden. Det er derimot viktig at lederne støtter seg på det apparatet som eksistere og bruker blant annet MP, som rådgivere, og ikke nødvendigvis for å straffe (CYFOR). En forutsetning for å skape en rettferdig kultur er at det er enighet i organisasjonen hvor linjen mellom akseptabel og uakseptable handlinger er satt (Reason, 1997). Hele 22 % av informantene svarte ja på spørsmålet om risikoen for å miste sikkerhetsklareringen er en faktor som hindrer i å rapportere sikkerhetsbrudd. 42% svarte nei (Diagram 9). Alle (minus en informant), som svarte JA på dette spørsmålet tilhørte avdeling 3, dette tilsvarer 58% av avdeling 3 sine informanter. På den ene siden tyder resultatene at det er forskjeller i hvordan avdelingene kommuniserer hva som er akseptable og ikke akseptable handlinger, og hva konsekvensene eventuelt kan bli for den enkelte. Mens det på den andre siden kan være at dette er kommunisert fra organisasjonen men at informantene allikevel har en frykt og mulig mistillit til håndteringen av et rapportert sikkerhetsbrudd.

Læring:

Ved en HRO må organisasjonens fokus hele tiden være på sikkerhet og høy pålitelighet gjennom blant annet kontinuerlig læring (Aven el al., 2013) Av alle «subkulturer» er en lærende kultur mest sannsynlig den letteste å skape, men den vanskeligste å få til å virke (Reason, 1997). Den omhandler informasjonsinnhenting gjennom observasjoner, refleksjon, planlegging og handling. Det er handling som mest sannsynlig kan skape en utfordring i organisasjonen (Reason, 1997). For å få til læring er det derfor viktig å ha en rapporterende kultur som motiverer personellet til å rapportere feil og hendelser (Reason, 1997). Hele 61 % av informantene uttaler at de har erfart at de selv eller andre har latt være å rapportere brudd på sikkerhetstiltak og føringer (Diagram 4). Det kan være en utfordrende oppgave å få personell i en organisasjon til å rapportere hendelser, spesielt når det kommer til å rapportere egne feil (Reason, 1997). Det bør derfor være en takhøyde i en lærende organisasjon hvor det er åpenhet som gir operativt personell en trygghet til å rapportere (Tinmannsvik, 2008). Westrum (1992) referer til «lisens til å tenke», hvor organisasjoner tar imot nye ideer og at det aktivt søkes etter informasjon og at feil fører til undersøkelser. Det fremkommer mange grunner som hinder for at informantene ikke rapporterer. Noen informanter trekker frem at nærhet til kollega og venner kan ha hindret dem i å rapportere sikkerhetsbrudd. Flere informanter prater om bekvemmelighetshensyn, tidspress, merarbeid og operativ kapasitet som årsak. Andre informanter og CYFOR uttaler at det de må bli vant til at det kommer noe positivt ut av rapportering og at det må komme tilbakemeldinger på det som er rapportert. En faktor som er viktig ved en rapporterende kultur er at tilbakemeldingene er rask, tilgjengelig og forståelig for de som rapporterer (Reason, 1997). En sikkerhetsleder sier: *«så får en sikkert et litt ullent svar tilbake»*, dette kan tyde på at enkelte tilbakemeldinger ikke er helt forståelig for mottaker.

På spørsmålet om de opplever at rapportering blir fulgt opp (Diagram 10) svarte 56% JA, 0% svarte NEI, 5% svarte av og til, mens 39% svarte vet ikke. På den ene siden er det positivt at ingen svarte nei på dette spørsmålet, men det er derimot hele 39 % som ikke vet om rapporteringen blir fulgt opp. Dette kan tyde på at tilbakemeldingene på rapporter kan være noe manglende og kan bidra til å redusere læring og motivasjonen for fremtidig rapportering. Det kan derimot være at det er kommet tilbakemeldinger, men at tilbakemeldingene ikke rekker frem til alle. En annen faktor som er viktig for å få en rapporterende kultur, er at det er lett å rapportere (Reason, 1997). På den ene siden uttrykker flere informanter at rapporterings- verktøyet oppleves som tung grodd, mens det på den andre siden uttrykkes at det er ønskelig med mer kunnskap om verktøyet. CYFOR har påpekt til FSA at

rapporteringssystemet må forenkles, ettersom de tror det vil senke terskelen for å rapportere. En leder (18) uttrykker at det er enklere å rapportere innenfor safety, mens innenfor security skal det være mer formelt.

Det fremkommer også at noen er usikre på hvor grensen går på hva som skal rapporteres og det påpekes at det ikke skilles mellom små og store brudd. Det kan derfor argumenteres for at organisasjonen tydelig bør formidle hva som skal rapporteres. Mange informanter uttrykker at de gjør en egenvurdering på om bruddene er alvorlig nok til å rapportere. Dette må ses i kombinasjon med kompetansen og forståelsen hos personellet. Den med best kompetanse avgjør handlingen (Reason, 1997), men hva hvis avgjørelsen om å ikke rapportere gjøres på et lavt kompetansenivå. Dette kan bidra til å hindre læring i organisasjonen og organisasjonens mulighet til å stoppe eventuelle lekkasjer. Turner og Pidgeon (1997) viser til forskning hvor mange av ledetrådene vi trenger for detektere en krise i emningen er tilgjengelig i organisasjonen, men beslutningstakere i organisasjonsledelsen klarer ikke samle ledetrådene før det er for seint. Det bør derfor sterkt oppfordres til at mistanker om insidere og sikkerhetsbrudd rapporteres oppover i organisasjonen slik at ledere på høyere nivå kan vurdere trender og tiltak. Tiltak som eksempel; prosedyreendringer, kompetanseheving på personell eller holdningsskapende tiltak.

En informert kultur har kunnskap om alle faktorer som har betydning for sikkerheten og bruker denne proaktivt ved å finne tiltak for å hindre uønskede hendelser i fremtiden (Reason, 1997). Organisasjonens kompetanse og vilje til å trekke de riktige konklusjoner på hendelser som er rapportert i sikkerhetsinformasjonssystemet bidrar til en lærende organisasjon (Reason, 1997). Evnen til å kunne implementere tiltak krever fleksibilitet i organisasjonen, men også hos den enkelte medarbeider. På spørsmålet om tiltak blir iverksatt og endringer utført for å gjøre det mulig å gjennomføre i praksis (diagram 10 høyre side), svarte: 36% svarte JA, 9% svarte NEI, 8% svarte av og til, mens 25% svarte vet ikke. Resultatene kan tyde på at det er uenighet blant informantene om tiltak blir iverksett og endringer utført for å gjøre det mulig å gjennomføre i praksis. Resultatet hvor 25% svarer vet ikke, kan blant annet tyde på de ikke har vært involvert i noen situasjoner hvor tiltak har blitt iverksett, eller at de ikke har kompetansen eller forståelsen til å ta slike vurderinger. Det fremkommer under intervju at det er viktig at de som iverksetter tiltak bør forstå utfordringene og ha praktisk kjennskap til avdelingene. På den ene siden er det viktig at samarbeids organisasjoner som NSM, FSA og CYFOR tilegner seg kunnskap om de avdelingene de skal rådføre. Mens det på den andre siden er personellet som jobber i

avdelingen som kjenner utfordringene og har den beste praktiske kjennskapen. Det er derfor viktig at det er en god kommunikasjon mellom avdelingene og organisasjonene som kan støtte i utarbeidelse av tiltak. En felles forståelse er essensielt, og team som har opparbeidet et felles utgangspunkt vil i større grad lykkes (Klein, 2011). Samtlige sikkerhetsledere sier ja på spørsmålet om vurderinger av tiltak og nødvendige endringer av nye tiltak blir gjort. Det blir gjort endringer og justering på tiltak, hvor det eksempel blir gjort tilpasninger som skal opprettholde security, men samtidig ivareta safety. Det er viktig å ha lett tilgang til eksempel graderte rom for å stanse en eventuell brann. Men samtidig skal en overholde føringer hvor det graderte rommet skal være låst i henhold til regelverk. Prioriteringen her kan være utfordrende og det bør derfor være en del av en sårbarhetsvurdering på nivå 5.

6.3 FS3: På hvilken måte kan security-kulturen i Marinen forbedres?

Vi vil under dette punktet drøfte på hvilken måte security-kulturen i Marinen kan forbedres sett i lys av oppgavens teoretiske rammeverk. Ut ifra drøftingen rundt FS1 og 2 ser vi under dette punktet på muligheter Marinen har for å utvikle security-kulturen. Grunnet at oppgaven er ugradert går vi ikke i detaljer på det som kan beskrive sårbarheter eller teknologiske tiltak.

Drøftingen av FS1 og 2 viser at innsidetrusselen er høy, og den hurtige teknologiske utviklingen krever at Marinen som organisasjon klarer å følge utviklingen med oppdatering av prosedyrer, opplæring og teknisk utstyr. Drøftingen av forskningsresultatene opp imot det teoretiske rammeverket, som definerer en god security-kultur, HRO og sensemaking, skulle belyse trusselbildet og i tillegg hva som kjennetegner dagens security-kultur i Marinen. Resultatet av drøftingen viser at Marinen i et security-aspekt ikke innehar MTO-faktorene som kreves for å tilfredsstille en god kultur, og det er store grunnleggende mangler både på kunnskap og forståelse. Dette betyr ikke at Marinen ikke lever opp til beskrivelsen av en HRO i andre aspekt som safety og det operasjonelle arbeidet, og har et sterkt utgangspunkt for å utvikle security-kulturen. Vi vil derfor videre ta for oss hvilke mulige tiltak som vil kunne være med å forbedre Marinens security-kultur.

Det fremkom klart fra forskningsresultatene at security som fag ikke er gjennomgående implementert i Forsvarets utdanningssystem. Opplæringen de ansatte har fått på security er i henhold til resultater fra intervjuene meget ulik og oppfattes som litt tilfeldig. Informantene fra fagintervjuene understrekte viktigheten av at security blir en del av den gjennomgående utdanningen og at den røde tråden må være der både i utdannelse og praksis. I følge Reason (1997) har en god kultur kunnskap om alle faktorer som har betydning for sikkerheten. Dette innebærer at security må bli en del av fagplanen for Forsvarets utdanningssystem, og at det

implementeres i den praktiske opptreningen, øvelser og daglig virke. Det holder ikke bare med innføring av nye reglementer og prosedyrer, det må også gjennomføres en opplæring for å forstå å ta det i bruk (Roer, 2015).

Hvis personellet ikke forstår egne sårbarheter, verdier og trusler de kan stå ovenfor vil det i henhold til Boin et al. (2015) kunne skape splittelse i håndteringen av situasjoner, og det de står ovenfor kan oppdages for seint til å beskytte seg. NSM og CYFOR viser til eksemplets makt, og hvordan de tar det i bruk under formidling av security-kunnskap. Det er lettere å få en forståelse for krav og føringer hvis de ansatte ser hvorfor det stilles krav til håndtering av security, og eksempler på allerede inntrufne hendelser bidrar til økt forståelse på en fengende måte. Det fremkommer av intervjuene at personellet ønsker å verne om egen organisasjon, men må da få kunnskapen om hva som står på spill og hvordan de kan bistå i security-arbeidet. Dette leder videre til rapportering hvor de ansatte må få opplæring i hva som er sikkerhetstruende hendelser for å være i stand til å gjenkjenne indikasjoner på brudd for å kunne rapportere dem. Organisasjonens kompetanse og vilje til å trekke riktige konklusjoner på rapporterte hendelser i et sikkerhetsinformasjonssystem er med å bidrar til en lærende kultur (Reason, 1997). Det bør ikke være noe tvil for de ansatte hva som skal rapporteres og hvordan, som innebærer en opplæring og et effektivt rapporteringssystem.

I følge Reason (1997) vil ledelsens gjennomføring av revisjoner og justeringer av prosedyrer og arbeidspraksis bidra til at ledere og ansatte har den siste gyldige kunnskapen om MTO-faktorene som i sin helhet kan virke inn på sikkerheten i et system. Det betyr å innføre prosedyrer og regelverk som er tilpasset til organisasjonens virke, som fungerer i fred, krise og krig ved at de er overordnet nok til å kunne tilpasses enhver situasjonen. Ved å lære personellet prosedyrer i en scenario-setting vil de i tillegg se nytten av prosedyrene, forstå begrensningene og det vil hjelpe dem å tilegne seg noe av den tause kunnskapen nødvendig for å effektivt ta i bruk prosedyrer (Klein, 2011).

Det er ifølge Reason (1997) et lederansvar å legge til rette for en rapporterende kultur. Når vi innledningsvis i kapittelet påpeker behovet for kompetanse gjelder det også ledere. NSM (2015a) uttrykker at det må gjennomføres verdi-, trussel- og sårbarhetsvurderinger for å vurdere risiko. Det er ganske graverende at resultater fra intervjuer tyder på at sårbarhetsvurderinger enten ikke gjennomføres nedover i organisasjonen eller at dette ikke er kjent blant lederne. Kompetanse nivået hos ledere innenfor fagfeltet security må heves for at lederne kan være i stand til utøve ansvaret for å innarbeide security i organisasjonen. Her må også ønsket security-struktur være på plass. Det vil være en utfordring å få implementert

security i organisasjonen og skape en security-kultur hvis det ikke ligger til grunn et mandat som beskriver hvilket arbeid som må gjøres og setter nødvendige ressurser tilgjengelig.

Reason (1997) påpeker at det kreves investering i kvalitet, motivasjon og erfaring hos førstelinje ledere for at organisasjonen skal ha fleksibiliteten til å lære av situasjoner og implementere nye tiltak. I følge Reason (1997) og Tinmannsvik (2008) vil stor takhøyde hvor det er lov å gjøre feil, trygghet og tillitt til å rapportere egne feil bidra til en lærende organisasjon. Videre vil økt kunnskap og forståelse være nødvendig for å forstå hvilken trussel man står ovenfor, men også for å ha mindfulness, må ansatte vite hva de skal være oppmerksomme på og evne å forstå situasjonen (Weick & Sutcliffe, 2007). Erfaring krever også kunnskap og forståelse i bunn, hvor det kreves et arbeid over tid hvor man bevisst forsøker å forbedre security-kulturen for samtidig å bygge erfaringen, som igjen gir muligheten for mindfulness og sensemaking. Forskningen har vist at når vi snakker om security har Marinen et innledende behov for økt kunnskap og forståelse for å utvikle security-kulturen. Marinen står ovenfor komplekse og tvetydige situasjoner hvor de er nødt til å utvise mindfulness og sensemaking når tilsiktede uønskede hendelser inntreffer. Som en HRO må Marinen lære av nesten hendelser og forberede seg på å forvente å møte ubehagelige overraskelser fremfor å forsøke å forutse og kontrollere uforutsigbare risiko (Klein, 2011).

7. Konklusjon

Funnene i studien viser at innsidetrusselen utgjør en betydelig trussel som Forsvaret, herunder Marinen, ikke kan ignorere. For å håndtere en trussel og redusere risiko har vi analysert innsamlede data under MTO-faktorene som påvirker organisasjonens evne til å håndtere tilsiktede uønskede hendelser. Funnene viste at Marinen ikke har tilstrekkelig kunnskap og forståelse til at det kan eksistere en god security-kultur. Dette baseres på manglende opplæring av ansatte innenfor security, i tillegg til at security ikke er et gjennomgående fag i Forsvarets utdannelsessystem.

Det fremkommer av studien at manglende forståelse av trusselbildet hos de ansatte skaper motvilje for både rapportering og til å gjennomføre pålagte krav. Holdningene hos de ansatte fremkommer ikke grunnleggende dårlige, men påvirkes av at andre ansatte og ledere ikke følger pålagte krav eller utviser en security-adferd, som igjen kommer av manglende kompetanse og enkeltvis dårlige holdninger. Ulik forståelse og kompetanse hos lederne kan også være en årsak til at retningslinjene praktiseres ulikt i avdelingene i Marinen.

Det er utfordrende å følge den teknologiske utviklingen, og ikke alle ansatte vil kunne være kjent med alle aspektene ved teknologien som nyttes i organisasjonen. I følge intervjuresultatene ønsker personellet forståelse for hvilke sårbarheter teknologien rundt dem gir, og beskriver hvordan deres manglende forståelse kan utnyttes. Resultatene viser et sterkt behov på alle nivå for å gjennomføre sårbarhets- og risikoanalyser/risikostyring, og kunne bygge et mest mulig riktig bilde av situasjonen Marinen står ovenfor. Dette er nødvendig for å kunne gi øverste ledelse og politiske nivå en forståelse av hva som kreves for å følge den teknologiske utviklingen og at de dermed kan være villig til å disponere nødvendige ressurser og godkjenninger til mulige løsninger for å håndtere trusselen.

Resultatene belyser også utfordringene ved rapporteringssystemet. Her er det ikke bare et behov for et forenklet rapporteringsregime, men et behov for å tilrettelegge for rapportering ved å bygge tillit gjennom å oppfordre til rapportering, vise at det betyr noe ved å gi tilbakemeldinger og presentere endringer og tiltak. Det fremkommer ikke at de ansatte skylder på ledelsen for manglende security-kompetanse, unntatt når det er snakk om ressurser og tid for å ivareta aspektet, men resultatene indikerer at security ikke står på den daglige agendaen til lederne. Årsakene tolkes til å være manglede kompetanse, men også manglende ressurser og tid.

I følge resultatene fra datainnsamlingen vil læring i Marinen være vanskelig uten at rapporteringssystemet brukes effektivt og gir et bilde av behov for ressurser og tiltak. De ansatte har ikke tillit til at rapporteringssystemet fungerer og gir resultater, og ser derfor ikke hensikten med å rapportere.

Forslag til videre forskning

Denne studien ble gjennomført på et ugradert nivå, og for en organisasjon som Marinen hvor gradert material og informasjon håndteres daglig ville det vært hensiktsmessig å gjennomføre en tilsvarende forskning på gradert nivå. I tillegg vil det vært interessant å se om omstillingsprosessen som pågikk i 2016, hvor det var gjort store strukturendringer i organisasjonen, førte til endringer i forhold til security-kulturen. Hvilke ressurser som må til for å opprette en tilstrekkelig security-struktur i Marinen ble ikke kartlagt i denne studien. Det ville vært interessant å forske på for å se hva som kreves av personell og tid for at en organisasjon som Sjøforsvaret hadde fått en security-organisasjon som var i stand til å forbedre security-kulturen.

8. Referanser

Antonsen, 2009. *Safety culture, theory, method and improvement,.* England: Ashgate Publishing Company.

Austeng, K. M. J. T. J. I. M. O. M., 2005.. *Uncertainty analysis - Context and foundations, ISBN 978-82-92506-27-1.* [Internett]
Available at:
https://www.ntnu.no/documents/1261860271/1262010703/Concept%2010%20UncertaintyContext%20Summary.pdf
[Funnet 12 August 2016].

Aven, T., 2008.. *Risk Analysis – Assessing Uncertainties beyond Expected Values and Probabilities..* New York, Wiley: s.n.

Aven, T., 2009. *Risikostyring.* 2 red. Oslo: Universitetsforlaget.

Aven, T., 2014a. *Risk, surprises and black swans: fundamental ideas and concepts in risk assessment and risk management..* s.l.:Abingdon: Routledge.

Aven, T., 2014b. *Implications of black swans to the foundations and practice of risk assessment and management. Realiability Engineering and Saystem Safety.* s.l.:s.n.

Aven, T. et al., 2013. *Samfunnssikkerhet.* 5 red. s.l.:Universitetsforlaget.

Aven, T. & Flage, R., 2009. *Expressing and communicating uncertainty in relation to quantitative risk analysis.* [Internett]
Available at: http://gnedenko-forum.org/Journal/2009/022009/RATA_2_2009-01.pdf
[Funnet 11 August 2016].

Aven, T., Røed, W. & Wienche, H. S., 2010. *Risikoanalyse; prinsipper og metoder med anvendelse.* 2 red. s.l.:Universitetsforlaget.

Bartnes, L. M. O. R. L. &. T. I. A., 2006. *Safety vs security?.* New Orleans, USA.: s.n.

Blaikie, N., 2014. *Designing social rearch..* 2 red. Cambridge, UK: Polity Press.

Boin, A., Hart, P., Stern, E. & Sundelius, B., 2005. *The politics of Crisis Management.* 14. printing 2015 red. Cambridge: University of Cambridge.

Bovens, M. & 't Hart, P., 1996. *Understanding Policy Fiascoes..* New Brunswick: Transaction Publishers..

Børresen & Helseth, 2013/02712.. *Cyberdomenet, cybermakt og norske interesser.,* Oslo: Forsvarets forskningsinstitutt (FFI).

Dagbladet (DB), 2013. *Dagbladet.* [Internett]
Available at: http://www.dagbladet.no/2013/03/20/nyheter/sor-korea/utenriks/politikk/26298272/
[Funnet 15 Mai 2016].

Denk, A. & Johan., L., 2015. *masteroppgave: Rapporteringskultur i Sjøforsvaret.* [Internett]
Available at: https://brage.bibsys.no/xmlui//handle/11250/2366984
[Funnet 15 Mai 2016].

digitalguardian, 2016. *Insider threat definition.* [Internett]
Available at: https://digitalguardian.com/blog/what-insider-threat-insider-threat-definition
[Funnet 27 Mai 2016].

FOKUS, 2016. *Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordinger,* s.l.: Fokus.

Forsvaret, 2010. *Direktiv – Krav til sikkerhetsstyring i Forsvaret.* Oslo: Forsvarsstaben.

Forsvaret, 2016a. *Forsvaret.* [Internett]
Available at: https://forsvaret.no/organisasjon
[Funnet 3 September 2016].

Forsvaret, 2016b. *Sjøforsvaret.* [Internett]
Available at: https://forsvaret.no/sjoforsvaret
[Funnet 2 Mai 2016].

Forsvaret, 2016c. *Kysteskadren.* [Internett]
Available at: https://forsvaret.no/fakta/organisasjon/Sjoeforsvaret/Kysteskadren
[Funnet 2 Mai 2016].

Forsvaret, 2016d. *Cyberforsvaret.* [Internett]
Available at: https://forsvaret.no/cyberforsvaret
[Funnet 16 Mai 2016].

Forsvaret, 2016e. *Spørsmål og svar.* [Internett]
Available at: https://forsvaret.no/fakta/organisasjon/Etterretningstjenesten/sporsmaal-og-svar
[Funnet 16 Mai 2016].

Forsvaretsdepartementet, 2013-2016. *Langtidsplan "Et forsvar for vår tid".* [Internett]
Available at: https://www.regjeringen.no/globalassets/upload/fd/temadokumenter/ltp-presentasjon-fmin_komprimert_siste.pdf
[Funnet 23 Mars 2016].

Forsvarsdepartementet, 1998 nr 10. *Sikkerhetsloven: Lov om forebyggende sikkerhetstjeneste.* Oslo: Cappelen akademiske forlag.

Forsvarsdepartementet, 2014. *Forsvarsdepartementets retningslinjer for informasjonssikkerhet i forsvarssektoren. "FD`s cyberretningslinjer".* [Internett]
Available at:
https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf
[Funnet 9 mars 2016].

Forsvarssjefen, 2013. *Etterretningsdoktrinen.* s.l.:Forsvarsdepartementet.

Gass, N. O. o., 2003. *www.norskoljeoggass.no.* [Internett]
Available at: https://www.norskoljeoggass.no/Global/Retningslinjer/HMS/Sikring/091%20-%20Sikring%20og%20forsyninger%20av%20materiell%20i%20olje%20og%20gassindustrien%20.pdf
[Funnet 23 Mars 2016].

Guldenmund, F. W., 2000. *The nature of safety culture: a review of theory and research. Safety Science 34(1-3): 215-257 (251).* s.l.:s.n.

Jacobsen, D. I., 2012. *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode..* 2 utgave, 4.opplag red. s.l.:Høyskoleforlaget AS, Kristiansand..

Johannessen Asbjørn, T. P. A. K. L., 2009. *Introduksjon til samfunnsvitenskapelig metode.* 3 utgave 5 opplag red. s.l.:Abstrakt forlag AS, Oslo.

Langdridge, D., 2011. *Psykologisk forskningsmetode.* 2 red. Trondheim: Tapir Akademisk Forlag.

LaPorte, T. a. C. P., 1991. *Working inpractice but not in theory. Theoretical challenges of "High-Realiability Organisations..* s.l.:Journal of public administrations Research anf theory,1 s. 19-47.

Lipshitz, R. S. O., 1997.. Coping with Uncertainty: A Naturalistic Decision-Making Analysis. . I: *Organizational behavior and human decision prosesses.* s.l.:Vol. 69, No. 2, pp. 149-163,Article no. OB972679.

Malcolmson, J., 2009. *What is Security Culture? Does it differ in content from general Organisational Culture? ..* [Internett]
Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5335511
[Funnet 23 Mars 2016].

Marøy J., W. S., 2015. *Bacheloroppgave: Kultur for forebyggende sikkerhetstjeneste i Sjøforsvaret..* s.l.:Avdeling for økonomi og ledelsesfag. Høgskolen i Hedmark..

Nasjonal sikkerhetsmyndighet, 2015a. *Sikkerhetsfagligeråd,* Oslo: NSM.

Nasjonal sikkerhetsmyndighet, 2016. *OM NSM.* [Internett]
Available at: https://www.nsm.stat.no/Om-NSM/
[Funnet 16 Mai 2016].

Nasjonalsikkerhetsmyndighet, 2015b. *1.halvårsrapport,* OSLO: NSM.

Nasjonalt sikkerhetsmyndighet, 2014. *Verivurdering objektsikkerhet,* Oslo: NSM.

National Cybersecurity and communications Integration Center. U.S department of homeland security. , 2014. *Combating the Insider Threat.* [Internett]
Available at: https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf
[Funnet 27 Mai 2016].

Norsk senter for informasjonssikring, 2016. *NorSIS.* [Internett]
Available at: https://norsis.no/om-norsis/
[Funnet 16 Mai 2016].

NOU, N. o. u., 2000:24. *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeid i samfunnet,* Oslo: Justis- og politidepartementet.

NOU, N. o. u., 2015:13. *Digital sårbarhet- sikkert samfunn.,* Oslo: Departementenes sikkerhets- og serviceorganisasjon. Informasjonsforvaltning.

Office of the national counterintelligence executive,, 2011. *Foreign spies stealing US economic secrets in cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011..* [Internett]
Available at:
https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf
[Funnet 13 August 2016].

Reason, J., 1997. *Managing the Risks of Organizational Accidents.* 2011 red. England: Ashgate Publishing Limited.

Roer, K., 2015. *Build a security culture.* Cambridgeshire: IT Governance Publishing.

Searchseurity.techtarget., 2010. *Searchseurity.techtarget.com.* [Internett]
Available at: Searchseurity.techtarget.com/definition/insider-threat
[Funnet 27 Mai 2016].

Sjøforsvaret, 2016. *Sikkerhetshåndbok.* 7 red. Bergen: Sjøforsvarsstaben, Avdeling for Sikkerhet og Kvalitet (SST ASK).

Stikholmen, B.-O., 2012. *Sikkerhetskultur i Sjøforsvaret- En studie av sikkerhetskulturen og i hvilken grad den samsvarer med sikkerhetsstyring,* Oslo: Masteroppgave Forsvarets høgskole.

Sundseth, R. –. u. i. C. F. i. O. m. S., 2013. *Cyberoperasjoner – utfordringer i Cyber..* [Internett]
Available at: http://www.oslomilsamfund.no/files/speech_files/433-2013-02-18-Sundseth.docx
[Funnet 15 Juni 2016].

Tablet, N., 2010. *The black swan: the impact of the highly improbable..* 2 red. New York: Random house Trade Paperbacks.

Tinmannsvik, R., 2008. *"Stille avvik" – trussel eller mulighet? I Tinmannsvik, R. (red.): Robust arbeidspraksis. Hvorfor skjer det ikke flere ulykker på sokkelen..* Trondheim: : Tapir akademisk forlag.

Tv2, 2016. *Tv2.no.* [Internett]
Available at: http://www.tv2.no/a/8027496
[Funnet 15 Juni 2016].

Verdensgang (VG), 2016. [Internett]
Available at: http://www.vg.no/nyheter/innenriks/hoeyre/hoeyretopper-fikk-hemmelige-forsvars-

papirer-fra-ukjent-e-post-avsender/a/23768331/
[Funnet 23 August 2016].

Verdensgang (VG), 2016. *VG.no.* [Internett]
Available at: http://www.vg.no/nyheter/innenriks/hoeyre/hoeyretopper-fikk-hemmelige-forsvars-papirer-fra-ukjent-e-post-avsender/a/23768331/
[Funnet 19 August 2016].

Weick, K. a. S. K., 2007. *Managing the Unexpected.* 2 red. s.l.:San Fran Wood. Jossey- Bass.

Weick, K. E., 1995 . *Sense Making in Organizations..* Thousand Oaks: Sage Publications..

Weick, K., Sutcliffe, K. & Obstfeld, D., 1999. Organizing for High Reliability: Processes of collective Mindfulness. I: R. Sutton & B. Staw, red. *Research in Organizational Behavior.* s.l.:Standford Jai Press, pp. 81-123.

Westrum, R., 1992. Cultures with requisite imagination.. I: J. Wise, D. Hopkins & P. Stager, red. *Verification of complex systems: Human factors issues.* Berlin: Springer- Verlag, pp. 401-416.

Oversikt over vedlegg

- Vedlegg A – Hurtig intervju: informasjonsskriv, samtykkeskjema, intervjuguide
- Vedlegg B – Lederintervju: informasjonsskriv, samtykkeskjema, intervjuguide
- Vedlegg C – Fagintervju: informasjonsskriv, samtykkeskjema, intervjuguide
- Vedlegg D – Godkjenning fra Norsk senter for forskningsdata (NSD)

VEDLEGG A

Informasjonsskriv til informanter hurtig intervju.

Hei.

Vi er 2 kapteinløytnanter som jobber fulltid i forsvaret innenfor fagfeltet security og safety. Vi har vært i forsvaret i ca 16 år og har bakgrunn som navigatører i Minevåpenet, MTB våpenet samt Kystjeger kommandoen som skipssjefer på stridsbåt 90N.

Vi er nå i slutt fasen på en mastergrad i **Risikostyring og Sikkerhetsledelse ved Universitetet i Stavanger**, og vil i den sammenheng gjennomføre intervjuer til masteroppgaven som skal leveres 12 Oktober 2016. Tid og sted for intervju avtales nærmere.

Masteroppgaven blir skrevet som UGRADERT.

Foreløpig problemstillingen er som følger:

Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?

Avgrensinger:

Oppgaven avgrenses til å omhandle innsidetrussel.

Foreløpig forskningsspørsmål:

1. **Hva er trusselbildet i Sjøforsvaret i forbindelse med cyberdomenet?**
2. **Hva er kjennetegn med Kysteskadrens cyber sikkerhetskultur?**
3. **På hvilken måte kan cyber sikkerhetskulturen i Kysteskadren forbedres?**

Konfidensialitet/ anonymitet:

Dere som blir intervjuet vil ha full anonymitet i oppgaven. Det vil ikke bli nevnt navn, kjønn, grad, stilling eller avdeling. Hver informant vil få et informant- og avdelings nummer som kun oppgavens medlemmer vil vite. Denne oversikten lagres på et begrenset område og vil bli slettet når oppgaven leveres. Eksempel: Hvis du er respondent nr 12 og tilhører avdeling 3, vil du få respondentnummer 123.

Gjennomføring av intervju:

Vi vil gjennomføre semistrukturert hurtig intervju som tar **ca 15-20 minutter.** Dere vil i starten av intervjuet bli spurt om vi kan ta opptak av intervjuet til vårt etterarbeidet. Vi vil forsikre dere om at det kun vil være oppgavens medlemmer som vil høre på opptakene og disse slettes når masteroppgaven er levert.

Ved spørsmål ta kontakt på telefon [redacted] eller [redacted].

Med vennlig hilsen KL Charlotte Hille & KL Charlotte Myr

Samtykke til å delta i forskningsprosjektet

Jeg er villig til å delta i forskningsprosjektet Ja Nei

Jeg samtykker at dette intervjuet kan tas opp på bånd Ja Nei

Jeg samtykker at dataene kan lagres på PC med informant nummer Ja Nei

Jeg samtykker at dataene kan lagres på PC med organisasjonenes nummer Ja Nei

Dette arket inkludert eventuelle opptak vil bli slettet/makulert når masteroppgavens sensur foreligger.

Jeg har mottatt skriftlig informasjon om prosjektet og er villig til å delta i studien:

Signatur:

Sted: _____ Dato: __ / __ 2016

Intervjuguide: Semistrukturert hurtig intervju nivå 4-5 Marinen

Fase 1: Rammesetting

1. Løs uformell prat (1-3 min). Hvem er vi og hvem er «de»?

Bakgrunnsinformasjon

Intervjuet vil inngå i en masteroppgave knyttet til mastergrad i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Det er i forkant sendt ut detaljert informasjon om hva intervjuet omhandler og skal brukes til.
Intervjuere:
Charlotte Myr & Charlotte Hille: Presentasjon.

2. Informasjon (1-3 min)

Foreløpig problemstilling:

Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?

Taushetsplikt og anonymitet:

Dere som blir intervjuet vil ha full anonymitet i oppgaven. Det vil ikke bli nevnt navn, kjønn, grad, stilling eller avdeling. Hver informant vil få et informant- og avdelings nummer som kun oppgavens medlemmer vil vite. Det er kun en av oppgavens medlemmer som har tilgang til oversikten og denne vil bli slettet når oppgaven leveres. Eksempel: Hvis du er informant nr 12 og tilhører avdeling 3, vil du få nummer 123. Dere kan når som helst trekke dere fra studien ved å kontakte oppgavens medlemmer.

Ønsker å minne deg på at oppgaven er ugradert, ønsker du derimot å komme med eksempler som er gradert informasjon må mobiler tas ut av rommet. Denne informasjonen vil ikke bli benyttet i oppgaven.

Er det noe som er uklart eller er det andre spørsmål til intervjuet?

Vi ønsker å ta opptak for å unngå at vi mister informasjon eller sammenheng. **Signering av skjema for samtykke til deltagelse og opptak.** Disse vil bli slettet når masteroppgavens sensur foreligger i oktober- desember 2016.

Fase 2: Intervju:

Med alle: menes personell intervjuet på nivå 4-5 fra UM-OK

Med SL: menes ASL/DSL/KSL

1. Hva mener du er innsidetrussel og tror du det er en reell trussel du kan møte? Utdyp gjerne (Alle, SL)
2. På hvilket nivå må innsidetrusselen håndteres? (Alle, SL)
3. Er Sjøforsvaret sårbar for innsidetrussel? Ev hvorfor? (Alle, SL)
4. Hva betyr innsidetrussel for deg som ansatt i Forsvaret? (Alle, SL)
5. Finnes det pålagt sikkerhetsdokumentasjon for håndtering av cybertrussel? Ev hvilke? (SL)
6. Hvem har ansvaret for å ivareta håndteringen av innsidetrussel? Og hvem samarbeider dere med om cybertrusselen? (SL)
7. Hva er Forsvarets/ Sjøforsvarets sikkerhetspolicy (Alle, SL)
8. Har dere fått opplæring i innsidetrussel? Eventuelt håndtering av det? Hva slags opplæring/hvor ofte? (Alle, SL)
9. Hvilket ansvar har du for å sikre arbeidsplassen mot innsidetrusselen? (Alle, SL)
10. Ville du godtatt strengere føringer på bruk av mobil/ Pad/ pc/ internett/ minnepinne/ privat bruk av media for å bidra til å redusere Sjøforsvarets sårbarheter for fiendtlige handlinger? (Alle, SL)
11. Har du erfart at du eller andre har valgt å ignorere sikkerhetstiltak/føringer? Eksempel: «ikke bruk personlig minnepinne i gradert pc/bruk av mobil i rom for gradert tale». (Alle, SL)
12. Har du erfart at du selv eller andre har latt være å rapportere brudd på sikkerhetstiltak/føringer? (Alle, SL)
13. Har arbeidsmiljøet påvirket din håndtering av sikkerheten? Eksempel: i den betydning at andre har brutt sikkerhetskrav (dårlig holdning), og dette har ført til at også du har brutt dem vel viten om at det var et brudd? (Alle, SL)
14. Har dårlig personellforvaltning fra lokal og høyere ledelse påvirket deg til å begå sikkerhetsbrudd, eventuelt påvirket deg til å la være å rapportere? Eksempel: rapportering når aldri frem/blir ikke håndtert derfor ingen hensikt å rapportere, eller dårlig personellbehandling som leder til at man ikke bryr seg om føringer som skaper merarbeid. (Alle, SL)
15. Hva motiverer eller hindrer deg i å rapportere sikkerhetsbrudd? (Alle)

- Hva kan motivere eller hindre personellet i å rapportere sikkerhetsbrudd? (SL)
- Oppfølgingsspørsmål: Er risikoen for å miste sikkerhetsklareringen en faktor som hindrer deg i å rapportere sikkerhetsbrudd? Alle)

16. Hvilke føringer er lagt for rapportering av cyber/security hendelser? (Alle, SL)
17. Brukes det noe form for belønning for god sikkerhetspraksis?
    Oppfølgingsspørsmål: Ville det vært hensiktsmessig slik du opplever sikkerhetsholdningene blant kollegaer? (Alle)
18. Opplever du at rapportering blir fulgt opp? Kan du utdype? (Alle, SL)
19. Blir tiltak iverksatt og endringer utført for å gjøre det mulig å gjennomføre i praksis? Kan du utdype? (Alle, SL)
20. Blir det gjort vurderinger av tiltak og nødvendige endringer, ev nye tiltak (SL)? Kan du utdype?
21. Hvordan håndteres rapportering av sikkerhetshendelser knyttet til innsidetrussel? Opplæring? (SL)

Fase 3: Avslutning:

- Har du avsluttende spørsmål eller kommentarer?

- Er det noen spørsmål du mener vi burde stilt deg i denne sammenhengen?

VEDLEGG B

Informasjonsskriv til informanter ledere.

Hei.

Vi er 2 kapteinløytnanter som jobber fulltid i forsvaret innenfor fagfeltet security og safety. Vi har vært i forsvaret i ca 16 år og har bakgrunn som navigatører i Minevåpenet, MTB våpenet samt Kystjeger kommandoen som stridsbåt 90N sjefer.
Vi er nå i slutt fasen på en mastergrad i **Risikostyring og Sikkerhetsledelse ved Universitetet i Stavanger**, og vil i den sammenheng gjennomføre intervjuer til masteroppgaven som skal leveres 12 Oktober 2016. Tid og sted for intervju avtales nærmere.

Masteroppgaven blir skrevet som UGRADERT.

Foreløpig problemstillingen er som følger:
Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?
Avgrensinger:
Oppgaven avgrenses til å omhandle innsidetrussel.
Foreløpig forskningsspørsmål:

4. **Hva er trusselbildet i Sjøforsvaret i forbindelse med cyberdomenet?**
5. **Hva er kjennetegn med Kysteskadrens cyber sikkerhetskultur?**
6. **På hvilken måte kan cyber sikkerhetskulturen i Kysteskadren forbedres?**

Konfidensialitet/ anonymitet:
Dere som blir intervjuet vil ha full anonymitet i oppgaven. Det vil ikke bli nevnt navn, kjønn, grad, stilling eller avdeling. Hver respondent vil få et respondentnummer som kun oppgavens medlemmer vil vite. Oversikten over respondenter lagres på begrenset nett og vil bli slettet når oppgaven leveres.
Gjennomføring av intervju:
Vi vil gjennomføre ustrukturert/ åpent intervju som tar **ca 50-60 minutter.** Dere vil i starten av intervjuet bli spurt om vi kan ta opptak av intervjuet til vårt etterarbeidet. Vi vil forsikre dere om at det kun vil være oppgavens medlemmer som vil høre på opptakene og disse slettes når masteroppgaven er levert. Dere kan trekke dere fra studien helt frem til oppgaven leveres.
Ved spørsmål ta kontakt på telefon [redacted] eller [redacted]

Med vennlig hilsen KL Charlotte Hille & KL Charlotte Myr

Samtykke til å delta i forskningsprosjektet

Jeg er villig til å delta i forskningsprosjektet Ja Nei

Jeg samtykker at dette intervjuet kan tas opp på bånd Ja Nei

Jeg samtykker at dataene kan lagres på PC med informant nummer Ja Nei

Jeg samtykker at dataene kan lagres på PC med organisasjonenes nummer Ja Nei

Dette arket inkludert eventuelle opptak vil bli slettet/makulert når masteroppgavens sensur foreligger.

Jeg har mottatt skriftlig informasjon om prosjektet og er villig til å delta i studien:

Signatur:

Sted: _____ Dato: __ / __ 2016

Intervjuguide: ustrukturert /Åpent intervju ledere nivå 3,4,5 Marinen.

Fase 1: Rammesetting

1. Løs uformell prat (1-3 min). Hvem er vi og hvem er «de»?

Bakgrunnsinformasjon

Intervjuet vil inngå i en masteroppgave knyttet til mastergrad i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Det er i forkant sendt ut detaljert informasjon om hva intervjuet omhandler og skal brukes til.

Intervjuere:
Charlotte Myr & Charlotte Hille

2. Informasjon (5 min)

Foreløpig problemstilling:

Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?

For å kunne si noe om mulige og nødvendige tiltak for å skape en god cyber sikkerhetskultur er det viktig å danne et bilde av dagens ståsted, hvordan organisasjonen håndterer trusselen, og hvilken støtte ekstern fagorganisasjon kan bidra med. Deres erfaringer og kompetanse vil bidra til å kartlegge situasjonen, trusselen og håndteringsmuligheter for forbedring.

Taushetsplikt og anonymitet:

Dere som blir intervjuet vil ha full anonymitet i oppgaven. Det vil ikke bli nevnt navn, kjønn, grad, stilling eller avdeling. Hver informant vil få et nummer som kun oppgavens medlemmer vil kjenne til. Dere kan når som helst trekke dere fra studien ved å kontakte oss.

Ønsker å minne deg på at oppgaven er ugradert, ønsker du derimot å komme med eksempler som er gradert informasjon må mobiler tas ut av rommet. Denne informasjonen vil ikke bli benyttet i oppgaven

Er det noe som er uklart eller er det andre spørsmål til intervjuet?
Vi ønsker å ta opptak for å unngå at vi mister informasjon eller sammenheng. **Signering av skjema for samtykke til deltagelse og opptak.** Dette vil bli slettet når masteroppgavens sensur foreligger i oktober- desember 2016.

Fase 2: Erfaringer:

3. Overgangsspørsmål: (5-10 min)

Hva slags erfaringer har du med cybersikkerhet og egen organisasjons håndtering av trusselen, mer konkret opp imot innsidetrussel?

Fase 3: Fokusering:

4. 8 nøkkelspørsmål vi kan treffe frem: (40min)

22. Hvordan ivaretar Sjøforsvaret fagfeltet security vs. safety? Organisasjonsmessig og prosedyrer, hendelser, rapportering?
23. Hvordan håndtere Sjøforsvaret innsidetrusselen?
    a. **Støtte til intervjuer i samtalen:** Gjennomføring av kartlegging av sårbarheter, risikoanalyse, hvordan håndteres resultatet, tidsaspektet for utbedringer – er tidsaspektet tatt med i analysen? Hvem deltar/forankring i organisasjonen?
24. Hvordan følger Sjøforsvaret opp teknologisk utvikling/rapporterte hendelser/anbefalinger/forbedringstiltak? (Som blant annet kommer fra CERT, NSM, FSA, CYFOR)
25. Hvem samarbeider Sjøforsvaret med for å ivareta Cybertrusselen? – hvem har ansvaret for hva?
26. Hvilke utfordringer har Sjøforsvaret ift trusselen mtp øvelser, utenlandsoppdrag, daglig virke?
27. Hvordan ser Sjøforsvaret for seg å forbedre evnen til å håndtere cyber trusselen når vi blir mer og mer avhengig av teknologi og cyberdomenet samtidig som utviklingen på området er hurtigere enn hva man klarer å følge med prosedyrer og dokumentasjon?
28. Hvilke, eventuelt er nok, ressurser er gitt for håndtering av cybertrusselen? Samsvarer personell og ressurser med sårbarhetsvurderingene og tiltak nødvendige for å redusere risikoen tilstrekkelig?

5. Oppfølgingsspørsmål/sjekkliste ved behov

- Hvor står Sjøforsvaret i arbeidet med å bygge opp en evne til å håndtere innsidetrusselen?
- Hva er den reelle trusselen/risikoen vs. ressurser/midler/effekt av valgte tiltak?
- På hvilket nivå må det initialt tas grep?
- Samsvarer papiret med praksis? Må det utarbeides ytterlige føringer/dokumentasjon?
- Er det skriftlige føringer på samarbeidet med andre etater?

Fase 4: Tilbakeblikk

6. Oppsummering (ca. 10-15 min)

- Vår oppsummering/tilbake lesning
- Har vi forstått deg riktig?
- Er det noe du vil legge til?

Vi setter stor pris på din deltagelse og støtte i forbindelse med vår masteroppgave.

Informasjonsskriv til fageksperter.

Hei.

Vi er 2 kapteinløytnanter som jobber fulltid i forsvaret innenfor fagfeltet security og safety. Vi har vært i forsvaret i ca 16 år og har bakgrunn som navigatører i Minevåpenet, MTB våpenet samt Kystjeger kommandoen som skipssjefer på stridsbåt 90N. Mer om vår bakgrunn kan utdypes i starten av intervjuet.

Vi er nå i slutt fasen på en mastergrad i **Risikostyring og Sikkerhetsledelse ved Universitetet i Stavanger**, og vil i den sammenheng gjennomføre intervjuer til masteroppgaven som skal leveres 12 Oktober 2016. Tid og sted for intervju iht avtale.

Masteroppgaven blir skrevet som UGRADERT.

Foreløpig problemstillingen er som følger:

Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?

Avgrensinger:

Oppgaven avgrenses til å omhandle innsidetrussel knyttet til sikkerhetskultur.

Foreløpig forskningsspørsmål:

1. **Hva er trusselbildet i Sjøforsvaret i forbindelse med cyberdomenet?**
2. **Hva er kjennetegn med Kysteskadrens cyber sikkerhetskultur?**
3. **På hvilken måte kan cyber sikkerhetskulturen i Kysteskadren forbedres?**

Konfidensialitet/ anonymitet:

I forkant av fag intervjuene vil vi avklare muligheten for å referere til intervjuet ved bruk av både person- og organisasjonsnavn. Vi vil sende dere ferdigarbeidet tekst, hvor vi henviser til deres uttalelser, for godkjenning i god tid før masteroppgaven leveres.

Gjennomføring av intervju:

Vi vil gjennomføre et åpent intervju som tar ca 1 time. Dere vil i starten av intervjuet bli spurt om vi kan ta opptak av intervjuet til vårt etterarbeid. Vi vil forsikre dere om at det kun vil være oppgavens medlemmer som vil høre på opptakene og disse slettes når masteroppgaven er levert. Ved spørsmål ta kontakt på telefon [redacted] eller [redacted]

Med vennlig hilsen Charlotte Hille & Charlotte Myr

Samtykke til å delta i forskningsprosjektet

Jeg er villig til å delta i forskningsprosjektet Ja Nei

Jeg samtykker at dette intervjuet kan tas opp på bånd Ja Nei

Jeg samtykker at dataene kan lagres på PC med navn Ja Nei

Jeg samtykker at dataene kan lagres på PC med organisasjonens navn Ja Nei

Hvis nei på de to siste:

Jeg samtykker at dataene kan lagres på PC med organisasjons nummer Ja Nei

Dette arket inkludert eventuelle opptak vil bli slettet/makulert når masteroppgavens sensur foreligger.

Jeg har mottatt skriftlig informasjon om prosjektet og er villig til å delta i studien:

Signatur:

Sted: _____ Dato: __ / __ 2016

Intervju guide: Åpne fagintervjuer /samarbeids organisasjoner

Fase 1: Rammesetting

1. Løs uformell prat (1-3 min). Hvem er vi og hvem er «de»?

Bakgrunnsinformasjon

Intervjuet vil inngå i en masteroppgave knyttet til mastergrad i risikostyring og sikkerhetsledelse ved Universitetet i Stavanger. Det er i forkant sendt ut detaljert informasjon om hva intervjuet omhandler og skal brukes til.

Intervjuere:

Charlotte Myr & Charlotte Hille

2. Informasjon (5 min)

Foreløpig problemstilling:

Hva kan Sjøforsvarets ledere gjøre for å skape en god cyber sikkerhetskultur?

For å kunne si noe om mulige og nødvendige tiltak for å skape en god cyber sikkerhetskultur er det viktig å danne et bilde av dagens ståsted, hvordan organisasjonen håndterer trusselen, og hvilken støtte ekstern fagorganisasjon kan bidra med. Deres erfaringer og fagkompetanse vil bidra til å kartlegge situasjonen, trusselen og håndteringsmuligheter for forbedring.

Tema: Security, innsidetrussel, læring

Taushetsplikt og anonymitet:

Vi har i forkant av intervjuet avklart med deg om vi kan benytte person- og organisasjonsnavn. Er dette noe du fortsatt ønsker? Alt som blir benyttet i masteroppgaven fra dette intervjuet blir oversendt til deg for godkjenning i god tid før masteroppgaven leveres. Dere kan når som helst frem til oppgaven leveres trekke deg som «fageksperter»

Ønsker å minne deg på at oppgaven er ugradert, ønsker du derimot å komme med eksempler som er gradert informasjon må mobiler tas ut av rommet. Denne informasjonen vil ikke bli benyttet i oppgaven.

Er det noe som er uklart eller er det andre spørsmål til intervjuet?

Vi ønsker å ta opptak for å unngå at vi mister informasjon eller sammenheng. **Signering av skjema for samtykke til deltagelse og opptak.** Dette vil bli slettet når masteroppgavens sensur foreligger i oktober- desember 2016. Det er kun oppgavens medlemmer som skal lytte til opptakene og deles ikke med andre.

Fase 2: Erfaringer:

3. Overgangsspørsmål: (5-10 min)

Hva slags erfaringer har du med cybersikkerhet og gitte organisasjon, mer konkret innsidetrussel, sikkerhetskultur?

Fase 3: Fokusering:

Det vil være en åpen dialog gjennom hele samtalen. Spørsmålene er til hjelp for oss som intervjuere. Det kan hende de svarer på mange spørsmål uten at vi trenger å spørre de. Navn i parentes går til organisasjonen vi er hos.

29. Hvordan håndteres innsidetrusselen i deres arbeid, og hvordan er kommunikasjon med Sjøforsvaret mtp forståelse og arbeid med å håndtere trusselen? (FSA)
30. Hvordan støtter dere Sjøforsvaret med å skape forståelse for innsidetrusselen og arbeidet med å håndtere den, og hvordan kan Sjøforsvaret bidra til bedre samarbeid? (NSM, CYFOR)
31. Hvordan fordeles ansvaret for opplæring, rapportering, håndtering, oppfølging mellom NSM, FSA, CYFOR og Sjøforsvaret når det kommer til cybertrussel, da spesielt ift hvordan man håndterer behovet for forbedring, iverksettelse av tiltak, vurdering av effekt osv? (Sårbarhetsvurdering, risikoanalyser) (NSM, FSA, CYFOR)
32. Rapportere Sjøforsvaret cyber/security hendelser til FSA på generell basis? Hva er hensiktsmessig og hvordan kan Sjøforsvaret bli bedre? (FSA)
33. Hvilken konsekvens kan bruk av private mobil/pc/Pad/minnepinner/internett på base/bygninger/fartøy hvor gradert materiale og systemer befinner seg utgjøre? (FSA, NSM, CYFOR, CLTRe)
34. Bør man stille høyere/strengere krav til mobil/internett bruk på jobb, og bruk av sosiale medier til Sjøforsvarets personell? (FSA, NSM, CYFOR, CLTRe)
35. Hva er deres anbefalinger til tiltak Sjøforsvaret kan gjøre for å håndtere cybertrusselen, spesifikt innsidetrusselen, og hvilken betydning sikkerhetskulturen har for måloppnåelse? (FSA, NSM, CYFOR, CLTRe)

36. Er det ressurser, midler, stillinger til å reelt kunne håndtere cybertrusselen i Sjøforsvaret og det arbeidet dere støtter Sjøforsvaret med? Evt hva gjøres for å møte dette? (NSM, FSA, CYFOR)
37. Hvordan skiller dere safety og security ift innsidetrussel og sikkerhetskultur? (NSM, CYFOR, CLTRe)
38. Rapportere Sjøforsvaret cyber/security hendelser til dere på generell basis? (NSM)
39. Dere nevner på sikkerhetskonferansen 2016 at innsidetrussel og hvordan individer kan bli utsatt for press som fører til at de oppgir informasjon. Er det realistisk å bli utsatt for trusler i slik grad ukrainske familiemedlemmer ble av russiske tjenester i Ukraina konflikten? (NSM)
40. Er det mulig og hensiktsmessig for generell opplæring av cybertrusselen på rekruttskole/befalsskole/krigsskole/fartøyskurs nivå for å skape tilstrekkelig forståelse? (CYFOR)
41. På hvilket nivå er det hensiktsmessig med opplæring av ansatte på innsidetrussel for å innarbeide en god sikkerhetskultur? (CLTRe)
42. Hvordan kan den økte nettverksbaseringen påvirke innsidetrusselen i Forsvaret, og hvordan håndtere dere innsidetrusselen? (CYFOR, CLTRe)
43. Hvilke utfordringer ser dere ved bruk av eksternt personell/2./3. parts leverandører når det kommer til innsidetrussel? (CYFOR)
44. Hva legger dere i begrepet sikkerhetskultur? (CLTRe)

4. Oppsummering (ca. 10-15 min)

- Vår oppsummering/tilbake lesning
- Har vi forstått deg riktig?
- Er det noe du vil legge til?

Vi setter stor pris på din deltagelse og støtte i forbindelse med vår masteroppgave.

Riana Steen
Institutt for medie-, kultur- og samfunnsfag Universitetet i Stavanger Postboks
8002 Postterminalen
4068 STAVANGER

Vår dato: 15.06.2016 Vår ref: 48731 / 3 / ASF Deres dato: Deres ref:

TILBAKEMELDING PÅ MELDING OM BEHANDLING AV PERSONOPPLYSNINGER

Vi viser til melding om behandling av personopplysninger, mottatt 20.05.2016. Meldingen gjelder prosjektet:

48731	*Cyber sikkerhetskultur*
Behandlingsansvarlig	*Universitetet i Stavanger, ved institusjonens øverste leder*
Daglig ansvarlig	*Riana Steen*
Student	*Charlotte Nordbø Myr*

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, 12.10.2016, rette en henvendelse angående status for behandlingen av personopplysninger.

Vennlig hilsen

Kjersti Haugstvedt

Amalie Statland Fantoft

Kontaktperson: Amalie Statland Fantoft tlf: 55 58 36 41 Vedlegg: Prosjektvurdering

Personvernombudet for forskning

Prosjektvurdering - Kommentar

INFORMASJON OG SAMTYKKE Prosjektnr: 48731

I følge meldeskjemaet skal deltakerne i studien informeres skriftlig og muntlig om prosjektet og samtykke til deltakelse. Informasjonsskrivet er godt utformet.

FRIVILLIGHET TIL DELTAGELSE

Studentene som skal gjennomføre prosjektet er ansatt i Sjøforsvaret, hvor det rekrutteres informanter fra. Ved rekruttering fra eget nettverk er det viktig å ta hensyn til konfidensialitet og at forespørselen rettes på en slik måte at frivilligheten ved deltagelse ivaretas. Studenten bekrefter på e-post mottatt 09.06.2016, at det ikke eksisterer noe avhengighetsforhold mellom respondentene og studentene. Videre viser studentene til at frivillighet til deltakelse påpekes også muntlig ved rekruttering.

TEMA FOR INTERVJU

Temaet for intervju er sikkerhetskultur i Sjøforsvaret, og enkelte av spørsmålene går ut på om informantene har unnlatt å rapportere sikkerhetsbrudd. Det er derfor viktig at studentene gjennomgående sikrer anonymiteten til respondentene, noe de også viser til at de gjør i e-post mottatt 09.06.16. Det er kun studentene som vet hvem respondentene er.

PUBLISERING

På e-post mottatt 09.06.2016, viser studentene til at det kun er informanter fra fagintervju som det skal publiseres personopplysninger om. Vi minner om at dere må innhente eksplisitt samtykke til å publisere personopplysninger om disse respondentene.

INFORMASJONSSIKKERHET

Personvernombudet legger til grunn at dere behandler alle data og personopplysninger i tråd med Universitetet i Stavanger sine retningslinjer for innsamling og videre behandling av forskningsdata og personopplysninger.

PROSJEKTSLUTT OG ANONYMISERING

I informasjonsskrivet har dere informert om at forventet prosjektslutt er 12.10.2016. Ifølge prosjektmeldingen skal dere da anonymisere innsamlede opplysninger. Anonymisering

innebærer at dere bearbeider datamaterialet slik at ingen enkeltpersoner kan gjenkjennes. Det gjør dere ved å slette direkte personopplysninger, slette eller omskrive indirekte personopplysninger og slette digitale lydopptak.

ANDRE TILLATELSER

Personvernombudet forutsetter at dere innhenter eventuelle nødvendige tillatelser og godkjenninger fra ledelsen i forsvaret til å intervjue deres ansatte.