# Målrettet bevissthetsarbeidet for økt sikkerhet i informasjonssystemer

## En tilfellestudie i Forsvaret

## Targeted awareness efforts for increased security in information systems

## A case study in the Armed Forces

av

Morten Bye

&

Jørgen Skryten Ringstad


Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2010

# Sammendrag

Problemeier i Forsvaret beskriver dagens metoder for beskyttelse av informasjonssystemer som uttilstrekkelige. Beskyttelsen er myntet på erfaring av identifiserte og kjente angrepsmetoder, og kan betegnes som reaktiv. Dette sammen med kompleksiteten i informasjonssystemene, gir den målrettede trusselaktør store konkurransefortrinn. Organisasjoner som ikke ønsker å bli den tapende part i kampen om sin informasjon, må derfor identifisere og implementere nye beskyttelsesstrategier.

Vår overordnede hypotese er at en forsvarsstrategi basert på økt kunnskap om fienden kan bidra til et mer proaktivt informasjonssikkerhetsarbeid, og en mer effektiv utnyttelse av tilgjengelige ressurser. Kunnskapen om fienden kan økes ved å sette organisasjonens ansatte i bedre stand til tidlig deteksjon og rapportering av sikkerhetstrusler og hendelser.

Vi har undersøkt om bevissthetsarbeid, i form av et skreddersydd bevissthetsprogram mot organisasjonens behov, er redskapet som kan skape en slik organisasjon. Et litteraturstudium er utført for å undersøke om denne problemstillingen beskrives i litteraturen og identifisere mulige innfallsvinkler til problemet. Forskningsspørsmålene er utledet fra problemstillingen og manglende empiriske funn i litteraturen. Forskningsarbeidet er utført som en tilfellestudie i Forsvaret, i et miljø med ekspertise innen beskyttelse av kritiske informasjonssystemer. Vi skisserer mulige løsningsforslag, som bygger på litteratur og empiriske funn. Vi omtaler sentrale utfordringer som må løses for at en eventuell implementering skal bli vellykket.

Resultatene bekrefter i stor grad problemstilingens gyldighet. Undersøkelsene indikerer også at vår innfallsvinkel er hensiktsmessig. Det eksisterer et stort informasjonspotensial om fienden blant organisasjonens ansatte. Skal en strategi basert på øktfiendeforståelse gjennom økt IS-bevissthet kunne nyttegjøre seg av dette potensialet, nevnes spesielt kommunikasjonsflyten i organisasjonen som et av de viktigste suksesskriteriene.

Realisering av strategien krever at det gjennomføres prosjekter som fortsetter vårt arbeid. Man må gå dypere inn i å identifisere den spesifikke informasjonen om fienden, som behøves for å kunne forsvare informasjonssystemene. Resultater fra denne type arbeid, sammen med en kategorisering av ansattes kunnskapsbehov, vil være viktige innspill til hvordan man skreddersyr bevissthetsarbeidet.

# Abstract

The problem owner in the Norwegian armed forces describes the current methods used to protect our information systems as insufficient. The protection is based on the experience of known and identified attack methods, and can be described as reactive. This, together with the complexity of information systems, provides the targeted threat agent great competitive advantage. Organizations that don`t want to become the losing party in the battle of their information must identify and implement new protection strategies.

Our overall hypothesis is that a defense strategy based on improved knowledge of the enemy can contribute to a more proactive information security work, and a more efficient utilization of available resources. Knowledge of the enemy can be increased by setting the organization's employees in a better position to early detection and reporting of security threats and incidents.

We have investigated if information security (IS) awareness work, in the form of an IS awareness program tailored to your organization's needs, is the tool that can create such an organization. A literature study has been carried out to substantiate the validity of the problem and identify possible approaches to the problem. Research questions are derived with respect to the problem description and lack of the empirical findings in the literature. Research work is conducted as a case study in the military, in an environment with expertise in the protection of critical information systems. We outline possible solution proposals, which highlight key success criteria of an implementation of our approach.

The results confirm the validity of the problem description, and that the project approach to the problem may be appropriate. There exists a huge information potential, about the enemy, among the organization's employees. Particularly is the communication flow within the organization identified as one of the most important success criteria, to make the strategy take advantage of this information potential.

Realization of the strategy requires that project that continues our work is conducted. We need projects aimed at identifying the organization detailed need for information on the enemy. Results from this type of work, together with a classification of employees' knowledge needs, will be important inputs on how to tailor the IS awareness work.

# Om forfatterne

Løytnant Morten Bye og Løytnant Jørgen Skryten Ringstad er begge utdannet ved Hærens Ingeniørhøgskole, avdeling Jørstadmoen og uteksaminert i 2003. Senere har de jobbet med utvikling, etablering og drift av ulike kommunikasjons- og informasjonssystemer i Forsvaret, ved ulike avdelinger i Norge, og i internasjonale operasjoner. Fra 2008 til 2010 har de begge vært studenter ved master i informasjonssikkerhet ved Høgskolen i Gjøvik. Etter endt utdanning i 2010, skal studentene tilbake i arbeid ved Forsvarets kompetansesenter for kommando og kontroll informasjonssystemer (FK KKIS) på Jørstadmoen.

**Takk til:**

Prosjektgruppen ønsker å rette en spesiell takk til våre veiledere professor dr. dr. Jose J. Gonzalez og dr. Finn Olav Sveen for all hjelp i forbindelse med prosjektet. De har bidratt med uvurderlig faglig og metodemessig hjelp og støtte gjennom hele prosjektperioden. I tillegg ønsker vi å takke vår veileder fra Forsvaret Oblt. Roger Johnsen for faglig hjelp og som portåpner innad i Forsvarets organisasjon, og ikke minst som inspirator for prosjektets innfallsvinkel. Den intervjubaserte metoden som er benyttet i forskningen er totalt avhengig av samarbeidsvillige informanter. Vi ønsker med dette å rette en stor takk til våre informanter som med stor velvilje har bidratt med sine synspunkter under intervjuene, og ofret denne tiden i en ellers hektisk hverdag.

Videre ønsker vi å takke Forsvaret og spesielt de ansatte innen FK KKIS, FLO/IKT som gjorde det mulig for oss å gjennomføre denne utdanningen, og for å ha stilt midler og ressurser til rådighet for at dette har latt seg gjøre.

Til slutt vil vi takke våre nærmeste for den hjelp og ikke minst forståelse dere har vist i løpet av de siste to årene. Dette har medført en ekstrabelastning også for dere. Deres velvilje har gjort arbeidet mulig.

# Innhold

1 Introduksjon ..... 1
1.1 Forskningshypoteser ..... 3
1.2 Metode og oppgavens struktur ..... 3
1.3 Oppgavens bidrag ..... 4
1.4 Oppgavens begrensninger ..... 4
1.5 Nøkkelord ..... 4
2 Problembeskrivelse og bakgrunn for prosjektet ..... 5
3 Tidligere arbeider ..... 9
3.1 Konsekvenser av dagens beskyttelsesmetoder ..... 10
3.2 Fiendeforståelse ..... 11
3.3 Informasjonssikkerhetsbevissthet ..... 13
3.4 Bevissthetsprogrammet ..... 17
4 Hypoteser og forskningsspørsmål. ..... 21
5 Intervjumetode ..... 25
5.1 Studie av relevant litteratur/valg av metode ..... 26
5.2 Beskrivelse av metode ved intervju ..... 27
5.2.1 Profilbeskrivelse: Strategisk valgt ekspert ..... 28
5.3 Rammeverk for kvalitative forskningsintervju og sikring av intervjuets kvalitet ..... 28
5.3.1 Brifing ..... 29
5.3.2 Intervjuspørsmål/samtaletema ..... 29
5.3.3 Debrifing/Avslutning ..... 29
5.3.4 Intervjuguide ..... 30
5.3.5 Analyse av transkribert intervju ..... 30
5.4 Beskrivelse av første intervjuguide ..... 31
6 Forskningsresultater og analyse ..... 35
6.1 Innledende intervjurunde ..... 35
6.1.1 Delkonklusjon etter første intervjurunde ..... 49
6.1.2 Erfaringer fra første intervjurunde ..... 52
6.2 Andre intervjurunde ..... 53
6.2.1 Beskrivelse og argumentasjon for andre intervjuguide ..... 53
6.2.2 Resultater og analyse etter andre intervjurunde ..... 56

6.2.3 Delkonklusjoner etter andre intervjurunde ..... 61
6.3 Sammenfatning av resultater ..... 64
7 Mulig løsningsforslag ..... 67
7.1 Bakgrunn for løsningsforslagene ..... 67
7.1.1 Kategorisering av ulike jobbfunksjoners og avdelingers IS-bevissthetsbehov ..... 69
7.1.2 Kommunikasjonsflyt ..... 70
7.1.3 En dynamisk beslutningsmodell ..... 72
7.2 Kort analyse av status i Forsvaret ..... 74
7.2.1 Forsvarets informasjonssystem ..... 74
7.2.2 Sikkerhetsinformasjon ..... 74
7.2.3 Sikkerhetsrapportering ..... 75
7.2.4 Forsvarets organisasjon ..... 75
7.2.5 Forsvarets opplæringsportal ..... 76
7.3 Delkonklusjon ..... 76
8 Sammendrag og avsluttende kommentarer ..... 79
8.1 Videre arbeid ..... 82
9 Forkortelser ..... 85
10 Referanser ..... 87

# Figurer

Figur 1. Prosjektarbeidets overordnede arbeidshypotese versjon 1 ..... 2
Figur 2. Prosjektarbeidets overordnede arbeidshypotese versjon 2.....10
Figur 3. Prosjektarbeidets overordnede arbeidshypotese versjon 3.....41
Figur 4. Prosjektarbeidets overordnede arbeidshypotese versjon 4..... 45
Figur 5. Bevissthetsstigen..... 69
Figur 6. Informasjonsflyt mellom sensor og beslutningstaker .....71
Figur 7. OPSEC modelen.....73
Figur 8. Kommunikasjonsmodellen tilpasset Forsvarets egenskaper. .....77
Figur 9. Prosjektarbeidets overordnede arbeidshypotese versjon 5..... 82

# Tabeller

Tabell 1. Begrepsapparat innen kvantitativ versus kvalitativ metode (Lilledahl & Hegnes 2000) ..... 26

# 1 Introduksjon

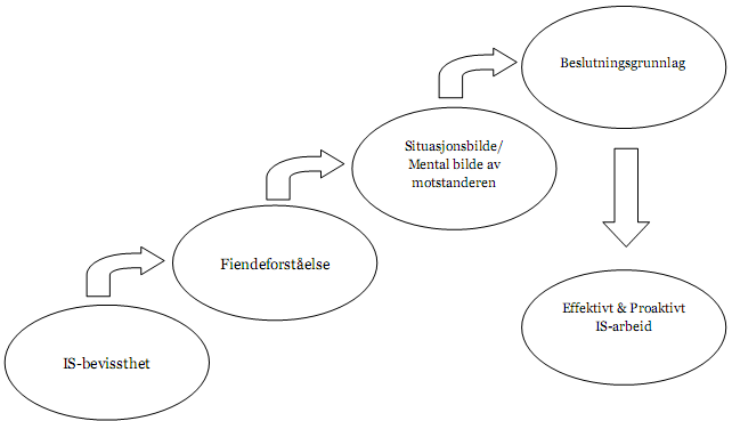
Masterprosjektet skal belyse det som, etter problemeiers mening, er en noe feilslått strategi for informasjonssikkerhetsarbeid (IS-arbeid). Problemeier er i dette tilfellet det norske Forsvaret. Dagens beskyttelsesmetoder kan være utilstrekkelig for å møte en målrettet trusselaktør i cyberspace. I dag er beskyttelse metoden basert på identifisering av angrep ved at man søker etter sårbarheter i egne systemer ved hjelp av i hovedsak kjente angrepsmetoder. Dagens metoder for beskyttelse mot cybertrusselen er i stor grad basert på erfaring av identifiserte og kjente angrepsmetoder. En angrepsvektor må derfor være identifisert og/eller benyttet tidligere før det implementeres mekanismer for å håndtere den. Problemeier i forsvaret argumenterer for at dagens strategi på mange måter er dømt til og mislykkes. Det reaktive handlingsmønsteret legger en øvre begrensning på kvaliteten og yteevnen til beskyttelsestiltakene. Ukjente angrepsmetoder vil med denne metodikken vanskelig kunne oppdages og stoppes. Konsekvensene av strategiens reaktive og erfaringsbaserte egenskaper favoriserer en målrettet trusselaktør. Problemstillingen forsterkes av kompleksiteten i våre informasjonssystemer, som også virker å favorisere angriperen. I tillegg til dette, og i motsetning til andre domener, som for eksempel helse, miljø og sikkerhet (HMS), står informasjonssikkerhetsdomenet ovenfor et dynamisk trusselbilde og trusselaktør. Ambisjonsnivået i prosjektarbeidet er i denne sammenheng ikke å finne en helt ny strategi der den gamle forkastes. Heller er det og sette søkelyset på mulige tilleggstrategier som bør implementeres i organisasjoner som klart har målrettede trusselaktører. Strategienes formål er å danne grunnlaget for et mer proaktivt informasjonssikkerhetsarbeid og en mer effektiv utnyttelse av tilgjengelige ressurser.

Prosjektets første fase omhandlet å undersøke gyldigheten i det beskrevne bakgrunnsproblemet. Resultatene viser at man står ovenfor en høyst avansert motstander som er tilpasningsdyktig. Den målrettede motstanderen, vil med andre ord, kunne tilpasse sine angrepsmetoder ut i fra våre allerede implementerte sikkerhetstiltak.

Det videre prosjektarbeidet baserte seg på en mulig tilnærming og forslag til løsning på problemet. Vi har undersøkt hvilke synergieffekter man kan oppnå ved å øke vektleggingen av de menneskelige faktorene ved informasjonssikkerhet (IS). I figur 1 er løsningsforslagets overordende tankerekke illustrert. Skissen er ment å illustrere sammenhengen mellom de ulike grunnelementene som har utgjort prosjektets generelle arbeidshypotese. Skissen må sees i perspektivet til beslutningstaker for prioriteringen av ressurser for IS-arbeidet. Av skissen ser vi at informasjonssikkerhetsbevissthet[1] (heretter IS-bevissthet), kan anses som grunnelementet. Begrepet IS-bevissthet benyttes i rapporten som en brukers evne til å oppfatte, forstå og forutse IS-truende hendelser i sitt miljø, og handle på bakgrunn av denne evnen. Forklaringen til skissen er som følger. Arbeid for å øke IS-bevisstheten i organisasjonen skal utføres med den hensikt å øke organisasjonens fiendeforståelse. Fiendeforståelsen skal økes med formål om å skape et bedre situasjonsbilde, og et bedre mentalt bilde av motstanderen. Disse skal forbedre og utvide

[1] Vår oversettelse av information security awareness

beslutningsgrunnlaget for prioriteringen av IS-ressurser. I sin tur vil så elementene bidra til et mer proaktivt IS-arbeid og en effektiv utnyttelse av tilgjengelige ressurser.




Figur 1. Prosjektarbeidets overordnede arbeidshypotese versjon 1

Forskningsarbeidet er utført som en tilfellestudie[2] i Forsvaret. Det er blitt samlet empiriske data rundt problemstillingens relevans. Potensialet i å skreddersy et helhetig IS-bevissthetsprogram[3] mot Forsvarets behov for økt fiendeforståelse i cyberverden er undersøkt. Bevissthetsprogrammet benyttes for å øke de ansattes IS-bevissthet (se figur 1), og tilrettelegge for at de ansatte kan bli en aktiv trussel- og hendelsesdetektor. Funnene i litteratur og fra forskningsarbeidet er benyttet til å belyse viktige suksessfaktorer for en vellykket implementering av prosjektets tilnærming til problemet. Rapporten beskriver mulige løsninger på sentrale elementer som må ligge til grunn for å kunne realisere og skreddersy IS-bevissthetsprogrammet, og i sin tur en strategiendring basert på økt IS-bevissthet og fiendeforståelse.

I rapporten foreligger empirisk data som gir sterke indikasjoner på at dagens metoder for beskyttelse er dårlig egnet for forsvar av informasjonssystemene mot den målrettede trusselaktør. Informantene anser kunnskap om motstanderen som fundamental for å lykkes å beskytte informasjonssystemene og verdifull informasjon. I dette perspektivet er det en generell oppfattning av at organisasjonens ansatte kan bidra med viktig informasjon om fienden. Det er grunnlag for å si at det eksisterer et stort potensial i å utnytte denne informasjonen.

De viktigste suksessfaktorer som belyses ved en fremtidig implementering av prosjektets innfallsvinkel er informasjonsflyten i organisasjonen, og behovet for ulike grader eller nivå av IS-bevissthet blant ulike kategorier ansatt. I tillegg krever dynamikken i trusselbildet at beslutningsgrunnlaget er basert på kontinuerlig oppdatert informasjon om motstanderen (se figur 1).

Prosjektarbeidet har grunnet de rammene det var underlagt, ikke kunne definerte konkrete retningslinjer og anbefalinger for en implementering av de omtalte

[2] Tilfellestudie- Oversettelse av det engelske begrepet Case study
[3] IS-bevissthetsprogram: I begrepet ligger et organisert system som benytter ulike metoder for å øke IS-bevisstheten til de ansatte i organisasjonen.

prinsippene i organisasjonen. Derimot gir det anbefalinger for videre arbeid som vil kunne bli bidragsytende i arbeidet med en fremtidig implementering. Viktige forskningsområder her vil være å fortsette vårt arbeide og samle data rundt muligheter og utfordringer innen andre avdelinger i Forsvaret. Videre vil det være nødvendig å identifisere en hensiktsmessig kategorisering av behovet for IS-bevissthet i organisasjonen. Til sist belyses behovet for forskning som kan identifisere og gi en detaljert beskrivelse av hvilke informasjon som kan danne et tilfredsstillende bilde av den målrettede trusselaktør.

## 1.1 Forskningshypoteser

Hypotesene som er benyttet i forskningsarbeidet presenteres her. Dette gjøres for å sette konteksten til arbeidet tidlig i rapporten. Hypotesene er utledet etter arbeid med problembeskrivelsen og litteraturstudien, og denne prosessen og argumentasjon for resultatet er detaljert beskrevet i kapittel 4. I samme kapittel er også forskningsspørsmålene som er benyttet i arbeidet utledet. Svar på forskningsspørsmålene er benyttet for å vurdere hypotesenes gyldighet.

*Hypotese 1:* *Det er sannsynlig at dagens strategi for beskyttelse mot cybertrusselen, gir den avanserte/intelligente motstanderen store konkurransefortrinn.*

*Hypotese 2:* *Det er sannsynlig at en strategi basert på økt fiendeforståelse kan endre dagens beskyttelsestankegang til en forsvarstankegang og gjøre sikkerhetsarbeidet proaktivt i større grad.*

*Hypotese 3:* *Det finnes indikasjoner på at strategien for beskyttelse/forsvar i større grad bør baseres på bevissthetsøkende arbeid, som kan gi grunnlag for et bedre mentalt bilde av motstanderen.*

*Hypotese 4:* *Det er grunn til å tro at veien til bedre informasjonssikkerhet gjennom økt fiendeforståelse, krever et organisert bevissthetsprogram i Forsvaret. Skreddersydd og spisset mot Forsvarets behov.*

## 1.2 Metode og oppgavens struktur

I prosjektarbeidet er ulike metoder benyttet. Det er valgt en metode som skal danne en overordnet struktur i rapporten, og det er valgt ulike metoder direkte relatert til forskningsarbeidet. Den overordnede metoden kalles P`HAPI, metoden, og er beskrevet i (Moxnes 2009). Bokstavene er forkortelse for Problem, Hypotese, Analyse, Policy og Implementering. P i P`HAPI er selve problemet som studeres. I rapporten utgjør dette kapittel 2, sammen med kapittel 3 der en litteraturstudie er benyttet for å undersøke i hvilken grad litteraturen beskriver eller anerkjenner problemstillingen. Litteraturstudien danner også grunnlaget for det videre arbeidet, sammen med problemstillingen. Disse resulterer i formuleringen av hypoteser og forskningsspørsmål i kapittel 4. Kapittel 4 utgjør H i P`HAPI. Analysedelen begynner med valg av passende forskningsmetode i kapittel 5. Analysen avsluttes i kapittel 6 der resultater og analyse av forskningsarbeidet presenteres. Policy i P`HAPI omhandler hva resultatet av arbeidet betyr og hva som bør gjøres for å ta hensyn til resultatet. I

rapporten utgjør dette kapittel 7 der mulige løsninger på de sentrale funnene er beskrevet. I samme kapittel er resultatene fra arbeidet sett opp mot en overordnet status i Forsvaret. Dette for å belyse hvor tilrettelagt Forsvaret er for en fremtidig implementering av en eventuell strategiendring. Implementering (I i P`HAPI), vil innebære en faktisk implementering av løsningene i organisasjonen. Noe som ikke er innenfor rammene i dette prosjektarbeidet. Dog er det beskrevet sentrale problemområder, utfordringer og videre arbeid som må gjennomføres for å kunne implementere og realisere strategiendringen.

For å undersøke problemstillingen slik den er gitt fra problemeier har vi benyttet litteraturstudium, i tillegg til kvalitative forskningsintervjuer av relevante informanter med påfølgende analyse. Detaljert beskrivelse av metoden for intervjuene gis i kapittel 5.

Underveis i rapporten er de ulike kapitlene innledet med et kort sammendrag for å beskrive kapiteles innhold, det enkelte kapitel avsluttes også med en oppsummering av de viktigste resultater i kapitelet. Dette er gjort på stikkordsform i tekstbokser for at innholdet i rapporten skal kunne følges på en rask og oversiktlig måte.

## 1.3 Oppgavens bidrag

I introduksjonen viser vi til prosjektgruppens ønske om å belyse det som, etter problemeiers mening, er en noe feilslått strategi for informasjonssikkerhetsarbeid. Oppgaven skal derfor bidra til;

- Å belyse svakheter med dagens strategi for IS-arbeidet, og derigjennom rette søkelyset mot behovet for andre innfallsvinkler og tilleggsstrategier.
- Å inspirere til andre tankeprosesser rundt måten vi beskytter våre informasjonssystemer i dagens teknologiske samfunn.
- Å bidra til et mer proaktivt IS-arbeid, gjennom å vise potensialet i å øke effektiviteten og utnyttelsen av tilgjengelige IS-ressurser.
- Økt forståelse av trusselbildet, og den målrettede trusselagenten.

## 1.4 Oppgavens begrensninger

Prosjektets problemstilling anses som meget omfattende, og det vil kreve ytterligere fremtidig arbeid før en omfattende strategiendring basert på prosjektets innfallsvinkel skal kunne realiseres. Tilgjengelige ressurser har derfor blitt konsentrert rundt å undersøke problemstillingens gyldighet gjennom litteraturstudier og intervju med informanter. I tillegg analyseres mulige løsninger på de identifiserte problemområdene. Utvalget av informanter er en begrensende faktor, da disse hovedsakelig ser problemet fra samme operasjonsmiljø, men resultatet gir allikevel gyldige funn ut i fra dette perspektivet.

## 1.5 Nøkkelord

Informasjonssikkerhet, Sikkerhetsutdanning, Sikkerhetsopplæring Sikkerhetskultur Informasjonssikkerhetsbevissthet, Situasjonsbevissthet, Fiendeforståelse.

# 2 Problembeskrivelse og bakgrunn for prosjektet

**Kapittelets innhold:**

- Presentasjon av prosjektets belyste problem, basert på problemeiers uttalelser og litteratur.
- Problem (P`HAPI)

Problemeier i Forsvaret ved Oblt. Roger Johnsen[4], hevder at det kan være systemiske mangler ved hvordan kampen for å sikre informasjonssystemer foregår i dag. Da beskyttelsesmetoden medfører at beskytterne ligger et steg bak angriperne.

Problemeier etterlyser en strategi som gjør det mulig å endre den skisserte situasjonen. Samtidig må strategien kunne danne grunnlag for en mer effektiv utnyttelse av tilgjengelige IS-ressurser. Vi presenterer her problemeiers beskrivelse av problemet, supplert med nødvendig bakgrunnsinformasjon til leseren.

Informasjonssikkerhet (IS) i dagens teknologiske verden har adoptert en rekke konsepter og metoder fra mer tradisjonelle domener, spesielt fra helse, miljø og sikkerhet (HMS[5]). Mange av utfordringene som eksisterer eksempelvis innen HMS har klare paralleller til informasjonssikkerhet. Når en trussel eller sårbarhet er identifisert i systemet, implementeres mekanismer for å forhindre eller håndtere dem. Å identifisere sårbarheter og beskytte seg mot disse er en viktig del av informasjonssikkerheten. Identifiserte sårbarheter gjøres gjerne kjent for alle, og bidrar til en stor del av det samlede trusselbildet. I IS-miljøet er det kjent at trusselaktøren ofte kan lykkes med å benytte kjente sårbarheter i sine angrep. Det mest effektive vil være om trusselaktøren selv lykkes å identifisere en sårbarhet som ikke vi i vår kvalitetssikring har avdekt. Angrep basert på slike sårbarheter vil mest sannsynlig være vellykket.

Problemeier viser i denne sammenheng spesielt til konsekvensene av hvordan ulike typer kvalitetsforbedringsprosesser er valgt implementert innen informasjonssikkerhetsdomenet. Generelt vil kvalitetsforbedring være helt nødvendig å implementere om man skal kunne forbedre og øke kvaliteten på prosesser i en organisasjon. Informasjonssikkerhetslitteraturen anbefaler også at informasjonssikkerhetsarbeidet implementeres i de helhetlige kvalitetsforbedringsprosessene i organisasjonen (Calder & Watkins 2008 s.38- 41). Vektlegging av kvalitetsforbedring er derfor like gjeldende innen IS-domenet så vel som andre domener. Problemet er hvilke prosesser man vektlegger å kvalitetsforbedre i det helhetlige systemet.

[4] Oblt. Roger Johnsen er referert til som problemeier i rapporten.
[5] HMS – Helse, miljø og sikkerhet

Måten vi omtaler dette aspektet i rapporten gjør det nødvendig å definere hva som menes med kvalitetsforbedring, og hvordan det kan implementeres. I en studie angående hvordan man kan skape mer pålitelige organisasjoner sier Winston et al. (2005) at organisasjoner opererer innen tre operasjonsdomener. Det første nivået er det reaktive domene, der man reparerer etter at systemet har feilet. Planleggingsdomenet er neste nivå, der en forsøker å identifisere, reparere og utbedre feil og mangler før systemet feiler. Det tredje og siste domenet er presisjonsdomenet. Her forsøker man, i tillegg til å reparere og utbedre feil og mangler, hele tiden å forbedre systemet slik at det ikke skal feile. Vi vil henvise til disse som reaktiv, proaktiv og kontinuerlig kvalitetsforbedring. Det er her også interessant å se at de fleste organisasjoner befinner seg i det reaktive operasjonsdomenet (Winston et al. 2005). Videre konkluderes det med at for å lykkes med sine mål er det nødvendig med kontinuerlig kvalitetsforbedring.

Problemeier bemerker at denne problemstillingen er høyst relevant for Forsvarets organisasjon. Det beskrives at informasjonssikkerhetsarbeidet benytter seg av metoder som utelukkende er tuftet på prosedyrer for reaktiv kvalitetssikring av informasjonssystemene. Man baserer seg på at en angrepssignatur er kjent. Forskjellige tekniske systemer, slik som IDS/IPS og brannmur, og standarder oppdateres med signaturene for å være i stand til å gjenkjenne og stoppe angrep Disse "listene" over kjente sikkerhetsproblemer er kjent for alle, inkludert fienden[6]. Det benyttes derfor en overvekt av ressurser på å kvalitetsforbedre reaktive beskyttelsestiltak. I mange tilfeller vil dette gi verdifull informasjon til fienden.

Ser man på dagens innfallsvinkel på informasjonssikkerhetsarbeid (IS-arbeid) er det derfor sannsynlig at man følger en reaktiv kvalitetsforbedringsstrategi. Trusselbildet en står ovenfor ved informasjonssikkerhet, i motsetning til eksempelvis HMS, kan gjøre denne fremgangsmåten utilstrekkelig. Spesielt da den avanserte og potensielt målrettede trusselaktøren introduseres.

De potensielle truslene og sårbarhetene som eksister i cyberverdenen har lenge vært omtalt i litteraturen og i nyhetsbildet. Den siste tiden kan det virke som situasjonen i mye større grad virker å bli et militærstrategisk og muligens politisk tema (Markoff et al. 2010). Bekymringene dreier seg i så måte om informasjonskrigføring (cyberkrigføring), og hvilke konsekvenser et angrep i cyberverden kan få for en organisasjon eller en nasjon. De utfordringene nasjoner og sivile organisasjoner står ovenfor med tanke på informasjonskrigføring, belyses i sikkerhetsselskapet McAfee`s sikkerhetsrapport for 2009 (McAfee 2009). USAs president Barack Obama har uttalt at USA har opprettet en egen cyberkommando som skal forbedre beskyttelsen av militære datanettverk, og som skal koordinere defensive og offensive cyberoppdrag (Baldor 2009). Den amerikanske presidenten ser på cybertrusselen som en av de største utfordringene USA står ovenfor. Grunnet truslene den innebærer mot nasjonens sikkerhet så vel som dens økonomiske ressurser. Dette indikerer at det potensielt eksisterer en målrettet motstander eller fiende i cyberverden.

[6] En fiende er her å betrakte som en som ønsker å oppnå uautorisert tilgang til vår informasjon og/eller hindre autorisert tilgang.

Det er her vist til at sikkerhetskonseptet kan være basert på at den parten som er i forsvar alltid ligger ett steg bak og beskytter seg mot en type angrep etter at det er utført. Dagens konsept er derfor basert på disse predefinerte "listene" over hva som er ansett som et angrep og hvordan det ser ut. Implementerte sikkerhetsmekanismer er basert på disse listene. Dersom en hendelse oppstår som ikke på forhånd er definert som sikkerhetstruende, vil den ikke bli oppdaget. Dagens metoder kan således medføre at en aktør med skumle hensikter stiller med et stort konkurransefortrinn. Fienden kan gjennom analyser av de predefinerte listene identifisere hvilke angrep våre systemer mest sannsynlig er beskyttet mot. Dette kan gjøre fienden i stand til å tilpasse målrettede angrep, og enklere oppnå vellykkede angrep med bakgrunn i denne informasjonen.

Problemeier viser videre til problemets kompleksitet. Strategien som benyttes i dag for å løse problemet, finne og tette alle sikkerhetshull, kan ha egenskaper som gjør at en med stor sannsynlighet vil mislykkes i å nå sine mål. I hvilken grad en lykkes, bestemmes av mengden tilgjengelige informasjonssikkerhetsressurser. Denne situasjonen kan begrunnes i at et sikkerhetshull kan eksistere i hver linje kode, i forholdet mellom hver linje kode og i en hver transaksjon mellom linjer med kode. Dette medfører sannsynligvis en NP- komplett[7] problemstilling, en problemstiling som ikke lar seg løse inne polynomial tid[8] med dagens metoder. Dette kan beskrives ved hjelp av "The halting problem of Turing machines" som sier at enkelte matematiske problemer er så komplekse at de ikke kan løses på en datamaskin (Hopcroft & Ullman 1969 s. 108-109). Det å lage et dataprogram som skal kunne detektere og fjerne alle sikkerhetshull i et softwareprogram eller kunne detektere alle typer av dagens og fremtidens datavirus er et slikt problem (Audestad 2005). Dersom dette er tilfelle underbygger situasjonen hvor komplekst det er å forsvare et informasjonssystem. Forsvareren står ovenfor et umulig problem, å finne alle mulige angrepsvektorer, mens angriperen kun trenger én tilgjengelig angrepsvektor for å lykkes. Dette er en kjent problemstilling innen informasjonssikkerhetsfaget. På tross av dette virker det som at man forsøker å løse problemet med overnevnte strategi. Hvilket belyser behovet for andre innfallsvinkler. I ethvert praktisk tilfelle vil en ikke bare stå ovenfor et teoretisk umulig problem, men man vil også være underlagt en begrenset mengde av ressurser for å løse problemet. Målet vil være å benytte denne endelige mengden ressurser slik at en oppnår en størst mulig grad av informasjonssikkerhet innen de rammene en er underlagt. Ikke minst at disse sikkerhetsressursene prioriteres slik at de har størst mulig effekt for organisasjonens overordnede målsetning.

Konsekvensen av de overnevnte faktorer gjør at problemeier etterlyser andre strategier for hvordan vi sikrer våre informasjonssystemer. Problemeier ønsker i større grad og aktivt forsvare egne informasjonssystemer, kontra dagens passive beskyttelse. Flere grunnlegende problemer må løses før dette skal muliggjøres. Problemeier nevner her

[7] NP står for Nondeterministic Polynomial, begrepet benyttes på problemer som ikke er løsbare, på en datamaskin, innen polynomsk tid. Problemer som kan løses i polynomsk tid er håndterbare, dvs. mulig å løse på en datamaskin.

[8] Polynomial tid, i begrepet ligger det at et det er mulig for et program Q og løse problemet P, når tiden (antall regneskritt) begrenses av et polynom (et endelig heltall) på størrelse med problemet. Den presise definisjonen benytter seg av tuningmaskiner se (Hopcroft & Ullman 1969)

blant annet at man må ha en informasjonsinfrastruktur (II) som er mulig å forsvare. I dette ligger det at man må bygge en II som har de mekanismer som gjøre det mulig og detektere, overvåke, begrense og kontrollere angrep. I overført betydning må derfor mekanismene gjøre det mulig å skille et angrep fra lovlige handlinger. Et annet problemområde er fiendeforståelse, tatt i betraktning den målrettende trusselaktør. Det er behov for en overordnet strategi som legger til rette for at man kan danne seg et bedre mentalt bilde av fienden. Man må kunne danne seg et beslutningsgrunnlag som gjør det mulig å avgjøre hvordan avdekke og identifisere en fiende og reagere på et angrep. Beslutningsgrunnlaget bør baseres på en forståelse av fiendens strategier, operasjonelle metoder og teknisk-taktiske prosedyrer (TTP). Dagens metoder og løsninger er beste egnet til å detektere fiendes TTP innen cyberverden. Imidlertid kan en fiende benytte seg av metoder som går utenfor cyberverdenen for å trenge seg inn i et system. Et slikt eksempel er å ta kontakt med ansatte per telefon med det formål å lure de til å gi fra seg passord, brukernavn og annen nyttig informasjon. Problemeier medgir at dette bildet gir et snevert grunnlag til å danne seg et bilde av den målrettede trusselaktør. Da sammensetningen av cyberverden gjør det utfordrende å skille mellom angrep som kan betegnes som støy, og hva som er målrettede angrepsforsøk.

Problembeskrivelsen som er gitt i dette kapittelet har vært utgangspunkt for prosjektarbeidet. Målet var at arbeidet skulle resultere i et helhetlig løsningsforslag som kan benyttes i videre forskning og en eventuelt fremtidig implementering.

**Kapittelets resultater:**

- Dagens metoder beskrives som reaktive. Reaktiviteten gjør seg gjeldende i beskyttelsen og kvalitetsforbedringen av informasjonssystemer. De er basert på erfaring av tidligere hendelser
- Den reaktive metoden å beskytte seg på, er spesielt dårlig egnet for å forsvare seg mot en stadig mer reell målrettet motstander
- Problemeier har et behov for en ny strategi, for aktivt å kunne forsvare systemene, basert på økt kunnskap om fienden, og fordele IS-ressursene mer effektivt.

# 3 Tidligere arbeider

Kapittelet er ment som en beskrivelse av i hvilken grad bakgrunnsproblemet for oppgaven er berørt og underbygget av tilgjengelig litteratur. Videre ble litteratur som kunne indikere en foretrukket innfallsvinkel til problemet identifisert. En naturlig forlengelse av problemstillingen var å undersøke i hvilken grad litteraturen beskriver konsekvenser ved dagens strategi for beskyttelse. I tillegg ble det undersøkt om litteraturen omtaler en målrettet motstander. Spesielt med tanke på hvilke karakteristikker, litteraturen gir, om motstanderens angrepsmetoder i forhold til implementerte beskyttelsestiltak. Reaktivitet i IS-arbeidet ble ansett som et nøkkelord i denne sammenheng.

**Kapittelets innhold:**

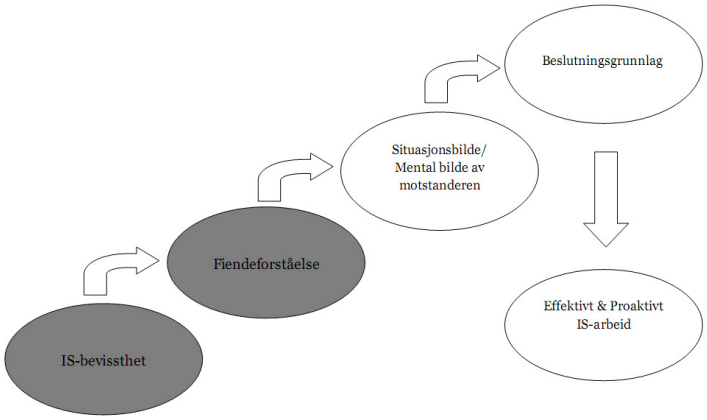
- Identifikasjon av relevant litteratur
- Drøfting av relevant litteratur
- Relevant litteratur sattes i sammenheng med prosjektets innfallsvinkel og kontekst
- Anses som del av Problem i P`HAPI

Informasjonssikkerhet forbindes ofte med tekniske løsninger (Anderson 2001). Dette kan bety at den tekniske delen av informasjonssikring får en uforholdsmessig stor del av oppmerksomheten. I kontrast til dette sier andre deler av litteraturen at de menneskelige faktorer er de viktigste for å oppnå god informasjonssikkerhet. De ansatte spiller en meget viktig rolle i organisasjonens informasjonssikkerhet, ut i fra deres kompetanse, adferd og årvåkenhet (Albrechtsen 2007). Albrechtsen(2007) beskriver dette som den menneskelige barrieren. Det vises til at dette er den siste barrieren man kan sette sin lit til dersom alle andre implementerte midler svikter, og som kan detektere og unngå at uønskede hendelser skal skje. Kompetansen og kunnskapen til brukeren vil ha en stor betydning for hvor robust denne barrieren vil være (Albrechtsen 2007).

Med bakgrunn i dette valgte vi å konsentrere arbeidet rundt de menneskelige faktorene ved informasjonssikkerhet, og hvordan en kan fokusere på disse ved en eventuell strategiendring. Vi valgte å undersøke om man i større grad kan basere IS-arbeidet på de menneskelige faktorene når man ønsker å forstå og lære mer om motstanderen. Mulige synergieffekter mellom økt IS-bevissthet og økt fiendeforståelse måtte studeres. Illustrasjonen av vår overordende tankerekke i introduksjonen (figur.1) vises her i figur 2. Av figur 2 (merkede felt) ser vi at vi i dette avsnittet diskuterer mulige effekter på fiendeforståelsen ved et målrettet arbeid med å øke IS-bevisstheten i organisasjonen.

Dette dreier seg i hovedsak om å undersøke om et identifisert behov for informasjon kan dekkes ved hjelp av å sette brukerne av systemet i stand til å identifisere, oppfatte og forstå sikkerhetsrelaterte hendelser i sin hverdag. Generelt sett er det en begrenset

mengde med bakgrunnslitteratur som omhandler emnene i den kontekst og perspektiv som betraktes i prosjektet. Allikevel er det identifisert litteratur som kaster lys på delemner og faktorer som er høyst relevant for prosjektets vurderinger. Derfor er ikke alle momenter og kilder som er trukket fram ment å kunne gi et direkte og entydige svar på den ene og rette løsning. Kildene er benyttet for å kaste lys over emnene, og til å indikere et mulig løsningsforslag.




Figur 2. Prosjektarbeidets overordnede arbeidshypotese versjon 2

## 3.1 Konsekvenser av dagens beskyttelsesmetoder

Etter at avgjørelesen om å konsenterer arbeidet mot de menneskelige sidene ved IS var fattet, søkte vi i litteratur som helhetlig beskriver dagens metoder og strategier for beskyttelse. McGraw (2002) og Jemal H. Abawajy et al. (2008) beskriver hvordan de fleste organisasjoner håndterer sikkerhetsrisikoer på en reaktiv måte. Dette gjøres gjennom å investere i teknologi designet for å beskytte mot kjente sårbarheter og overvåke angrep/inntrengning etter hvert som de oppstår. Nye beskyttelsestiltak og metoder utvikles som et resultat av et identifisert og vellykket angrep, eller sikkerhetstruende hendelse. Et eksempel her er oppdatering av antivirusprogrammer ved hjelp av publisering av signaturer. Etter hvert som ny skadelig kode oppdages, formidles det en signatur på denne slik at brukerne skal være beskyttet.

Beskyttelsesmetoden er dermed basert på en kontinuerlig søken etter løsninger på de problemene som dukker opp, i stedet for å fokusere på å gjøre programvaren mer sikker i utgangspunktet. Det gjør at beskyttelsen er fundamentert på problemets symptomer og ikke selve årsaken til problemet. McGraws (2002) sin artikkel omhandler design og vedlikehold av programvare. Selv om vårt syn på sikkerhet i prosjektet er bredere, er problembeskrivelsen sammenlignbart med vårt prosjekt.

Igure & Williams (2008) fremstiller også utfordringene med å identifisere ukjente sårbarheter, og hvordan beskyttelse av informasjonssystemer foregår. Det er her foreslått at man gjennom å analysere karakteristikken til de kjente sårbarhetene vil en kunne få innsikt i nye/ukjente sårbarheter. Denne fremgangsmetoden er begrunnet i en vurdering av hvordan anbefalt praksis for informasjonssikkerhet i dag. Spesielt innen sikring av informasjonssystemer, slik det er vist til i (McGraw 2002). Dette sammenfaller således med problembeskrivelsen i dette prosjektet. Ved å implementere

løsninger som for eksempel antivirus, brannmurer, IDS etc., vil en i prinsippet være underlagt et regime der en total beskyttelse er avhengig av at alle sårbarheter er kjent.

De ovenstående kildene betrakter generelle aspekter angående sikkerhet og pålitelighet i informasjonssystemer. De berører aspekter som er relevante for problemstilingen. Metoden som beskrives vil til dels være effektiv mot de generelle truslene som bruker kjente angrepsmetoder. Konsekvensen av denne formen for læringsbasert metodikk, er at en motstander som gjennomfører et angrep basert på en ukjent angrepsvektor vil kunne gjennomføre sine handlinger uoppdaget. Den identifiserte litteraturen rundt dette perspektivet er noe begrenset, men sannsynliggjør at dagens beskyttelsesmetoder er basert på erfaring og læring og kan beskrives som reaktive.

Problemstillingen forutsetter at motstanderen tilpasser sine angrepsmetoder basert på kunnskap om våre i beskyttelsesmekanismer. Det kan enkelt argumenteres for dette er tilfelle, siden det kontinuerlig dukker opp nye typer angrep selv om vi tetter "gamle" sårbarheter. Det kan sies at det ligger i sakens natur. At nettopp angriperens tilpassninger og dynamikk er bakgrunnen for at nye angrepsmetoder stadig dukker opp. Dette er delvis beskrevet i (Nunez 2008). Der vises det til at trusselbildet er i konstant forandring, og at tregheten i oppdatering og oppgradering av beskyttelsessystemer gjør at den forsvarende part stadig går tapende ut av kampen. Fienden ligger konstant ett steg foran på grunn av skjevheten i kunnskapsfordelingen (McGraw 2002). Grunnet det stadig skiftende trusselbildet, med såkalte zero day exploits[9] og adaptive angrepsmetoder, kan det være sannsynlig at motstanderen tilpasser sine prosedyrer til de beskyttelsestiltak som er implementert (Nunez 2008).

Symantecs årlige sikkerhetsrapport viser at de utviklet 2,8 millioner nye signaturer mot identifiserte trusler i 2009 (Fossi et al. 2010). Dette utgjør 51 % av alle signaturer Symantec har utviklet siden 2002. Vi anser ikke denne målingen som et uttrykk for den reelle økningen i antall nye angrepsmetoder. Da en rekke andre faktorer påvirker Symantecs motiver for utvikling av nye signaturer. Like fullt kan målingen gi en indikasjon på hvor rask utviklingen av nye metoder skjer. Ikke minst størrelsen og kompleksiteten på problemet og dynamikken i trusselbildet.

Identifisert litteratur beskriver at informasjonssikkerhet og evne til deteksjon av sikkerhetstruende hendelser ofte i stor grad er myntet på erfaring (McGraw 2002; Nunez 2008). Med tanke på at en slik metode krever kontinuerlig utvikling og oppdatering, kan det være sannsynlig at trusselaktører stadig utvikler nye angrepsmetoder. Dette med bakgrunn i å omgå de beskyttelsesmekanismer/metoder som er implementert.

## 3.2 Fiendeforståelse

Kompleksiteten til problemet utgjør en stor del av grunnlaget for problemstillingen. Den benyttes som en del av argumentasjonen for behovet for at andre IS-strategier må identifiseres. Vi erkjenner, ut i fra funnene i litteraturen, at dagens metoder forsøker å

[9] Zero Day Exploit – En sårbarhet ukjent for andre, og det foreligger derfor ingen sikkerhetsoppdatering som sikrer brukerne mot sårbarheten.

løse beskyttelsesproblematikken ved å erfare problemets symptomer. Vår erkjennelsen gjorde at vi søkte i litteratur som setter søkelyset på problemet, nemlig fienden og forståelsen av den målrettede motstander. Problemeier viser også til dette som et problemområde som må løses for i større grad å kunne forsvare egne informasjonssystemer. Dette resulterte i et søk etter relevant litteratur innen fiendemodellering. Dette er også i tråd med beslutningen om å konsentrere arbeidet mot de menneskelige sidene ved IS.

Blant annet beskriver Kott & McEneaney (2006), at å ta hensyn til motstanderens karakteristikker og oppførsel er essensielt for å lykkes i enhver konkurransepreget situasjon. Spesielt blir det å identifisere motstanderens hensikt trukket frem. Motstanderens hensikt blir beskrevet som; motstanderens ønskede sluttresultat, begrunnelse for å etterstrebe denne sluttilstanden, og hvilket nivå av motivasjon/forpliktelse den har til å lykkes (Kott & McEneaney 2006). I tillegg er det viktig å identifisere motstanderens kapasiteter, og hvilke metoder motstanderen benytter for å oppnå sine hensikter (Kott & McEneaney 2006). Jo mer kunnskap en har om fienden jo bedre kan en forutsi sin motstanders handlinger. Dermed kan forsvaret tilpasses og ressursene fordeles mer effektivt. Videre er viktigheten av å kjenne til alle relevante aspekter av det systemet en ønsker å kontrollere beskrevet i (Malerud 2008). En effektiv utnyttelse og tilpassing av ressursen er som kjent en stor del av problemeiers ønske til sluttresultatet av en eventuell strategiendring.

Å kunne forstå sin fiendes hensikt og forutse dens videre trekk er et komplekst problem. Kott & McEneaney (2006) beskriver kritiske elementer for å kunne skaffe seg et bedre bilde av fienden. Det er essensielt å studere fiendens tidligere trekk og reaksjoner i ulike situasjoner. Informasjon om hvilke politiske agendaer de har, evner den sitter inne med, infrastrukturen den har tilgjengelig og menneskelige faktorer anses også som kritisk. Denne teorien er beskrevet med tanke på militær planlegging og operasjoner. Det kan allikevel argumenteres for at prinsippene kan benyttes også med tanke på angrep og forsvar av informasjonssystemer, siden man i begge tilfeller kan stå ovenfor en motstander med de sammen egenskaper. Spesielt i militær sammenheng kan det være enklere å argumentere for at har en og samme motstander i cyberverden og i den fysiske verden.  Således kan dette vise til viktige indikatorer som kan gi oss økt kunnskap om fienden.

Den identifiserte litteraturen over som beskriver emnet, konsentrerer seg i stor grad om å beskrive viktigheten av fiendeforståelsen under utviklingsfasen av et system. At en i størst mulig grad kjenner til motstanderens mål og motivasjon for angrep under en tidlig fase av systemutviklingen. Dette er et paradoks i seg selv da den kontinuerlige kvalitetsforbedringen (utviklingen) av beskyttelsestiltakene er begrunnet i at motstanderen tilpasser seg de implementerte tiltakene.

Litteraturen sier allikevel at kunnskap om fienden har en direkte innvirkning på å lykkes i en konkurransepreget situasjon, der man må fatte avgjørelser og prioritere sine ressurser. Litteraturen viser også til mulige indikatorer som til eksempel fiendes hensikt, kapasiteter, og metoder samt tidligere trekk og reaksjoner. Disse bør evalueres og tolkes i prosessen med å kunne forutse motstanderens fremtidige handlinger.

## 3.3 Informasjonssikkerhetsbevissthet

IS- bevissthet ble som kjent valgt som innfallsvinkel til arbeidet, vi undersøkte derfor hva som finnes av vitenskapelig litteratur angående emnet. Det viser seg også her at det er relativt lite omtalt i den generelle litteraturen, sammenliknet med mer teknisk rettet litteratur (Botha & Gaadingwe 2006). Det finnes også her få kilder angående IS-bevissthet, som egner seg for den spesifikke vinklingen i prosjektet. Som bakgrunn for å sette IS-bevissthet i perspektiv har vi derfor benyttet oss i stor grad av Petri Puhakainens doktorgradsavhandling fra 2006 (Puhakainen 2006). Forfatteren har identifisert 59 kilder som omhandler emnet over en tidsperiode på 20 år (1985-2005), noe som bevitner at mengden av forskning er begrenset (Puhakainen 2006). Avhandlingens formål er å undersøke begrepet IS-bevissthet (awareness), og hvordan brukerne av et informasjonssystem kan påvirkes for å etterfølge gitte retningslinjer angående informasjonssikkerhet. Hvilke ulike metoder som finnes og hvordan disse metodene kan benyttes. Denne avhandlingen er således godt basert og begrunnet i den litteraturen som er/var tilgjengelig innen emnet, og det er definert områder der den eksisterende litteraturen er mangelfull. Spesielt kan det nevnes at et fåtall av de overnevnte artiklene er basert på empiriske data, og at de fleste er basert på konseptuelle analyser.

Puhakainen (2006) har foreslått teorier for hvordan menneskers bevissthet kan økes gjennom å utvikle IS-bevissthetsprogram. Teoriene er kategorisert i tre deler. 1)Utdanning/trening, 2)Informasjonskampanjer, og 3) Belønning og straff. Avhandlingen er i stor grad beskrivende og konseptuel, men er underbygget av empiriske data på deler av de teoriene som er foreslått. Dette er i hovedsak med tanke på bruken av utdanning og/eller trening (Puhakainen 2006). En tilnærming til designteoriene er også beskrevet i Jemal H. Abawajy et al.(2008) og R.S. Shaw et al.(2009).

Selve begrepet bevissthet er benyttet inne en rekke fagemner, potensielt medfører dette at en hver leser legger tolker begrepet ulikt og tillegger det ulike egenskaper. Det er derfor identifisert IS-litterur som beskriver egenskaper og omtaler begerpet, og som er relevant for prosjektet. R.S. Shaw et al.(2009) sier at forsking har identifisert tre ulike nivåer på bevissthet. Disse nivåene er Oppfatte (Perception nivå 1), Forstå (Comprehension nivå 2), å forutse (Projection nivå 3). En beskrivelse av begrepene gjengis her:

- Nivå 1 Oppfatte, innbefatter brukerens bevissthet om at det eksisterer ulike trusler i sitt forretningsmiljø. Brukeren evner å detektere ulike typer trusler.
- Nivå 2 Forstå, omhandler evnen de ansatte har til å benytte informasjon fra ulike kilder (sensorer), tolke disse, og kunne benytte denne kunnskapen til å redusere risiko i sitt miljø. Brukeren må derfor kunne analysere og vurdere farene fra ulike sikkerhetsrisikoer.
- Nivå 3 Forutse, Omhandler brukernes evne til å forutse hvordan fremtidige angrep vil se ut. Brukeren skal med bakgrunn i sin IS-bevissthet være i stand til proaktiv endring av sin adferd, og eventuelt sitt miljø, for å redusere eller fjerne mulige IS-trusler fra sine omgivelser. Det endelige målet med et

effektivt program for IS-bevissthet, er å utstyre brukeren med denne evnen (R.S. Shaw 2009).

Robustheten til en den menneskelige barrieren vil naturlig nok variere over tid og med tanke på den enkelte ansattes IS-kompetanse og kunnskap. Valentine (2006) sier at tradisjonelle bevissthetsprogram benyttet en "one-size-fits-all" innfallsvinkel. Disse reflekterer ikke over ansattes jobbfunksjon eller kompetanse (Valentine 2006). Valentine viser til at jobbfunksjonen kan indikere spesifikke behov for IS-bevissthet og kompetanse. Teknisk personell trenger muligens dyptgående og spesifikk IS-bevissthet rettet for mot bestemte prosesser eller systemer. Ansatte i helpdesk funksjoner med tilgang til sensitivinformasjon, vil sannsynligvis ha behov en spesifikk IS-bevissthet rundt ulike social engineering- teknikker (Valentine 2006). Valentine argumenterer for en metode som skreddersyr utdanningsprogrammet til organisasjonens behov, og tar hensyn til den ansattes jobbfunksjon. Metoden består av tre faser; Verdisetting, identifisering og utdanning (Valentine 2006).

Litteraturen i de to avsnittene over viser at det er behov får kunne identifisere hvilket bevissthetsnivå de ansatte befinner seg på. Dette kan indikere behovet for IS-bevissthets økende arbeid mot den bestemte ansatt eller kategori ansatt. Det benyttes store økonomiske ressurser på bevissthetsprogrammer, og det er et behov for å kunne måle hvilken effekt disse har på IS(R.S. Shaw 2009). Kruger og Kearney (2006) sier at slik data også kan benyttes til å velge de typer bevissthetsprogrammer som er mest kostnadseffektive og treffer organisasjonens behov. Forfattere av litteraturene har derfor en rekke argumenter som viser til viktigheten av å kunne identifiserer og måle organisasjonens og dens ansattes bevissthestsnivå.

En studie utført i 2007 av PricewaterhouseCoopers på oppdag fra ENISA[10], studerer viktigheten av IS-bevissthet, metoder for å øke IS-bevissthet og ikke minst hvilke indikatorer som benyttes for å måle effekten av dette arbeidet. Data er her samlet inn fra en rekke statlige departementer og bedrifter. Formålet med studien var å identifisere hvordan disse i dag måler hvor effektivt IS-bevissthetsarbeidet er i deres organisasjon (ENISA 2007). Studien identifiserer og beskriver en rekke metoder som benyttes til dette i dag, og viser til hvilke som er mest benyttet. Resultatet viser at få av metodene er kapable til å måle det man ønsker, nemlig faktisk adferdsendring. Allikevel argumenteres det for at klasseromsundervising er en metode som gir størst effekt sammenliknet med andre metoder. I rapporten argumenteres det også for at man kontinuerlig må måle effekten av arbeidet, og gjøre dette til en kontinuerlig og iterativ prosess som kan brukes til å optimalisere IS- bevissthetsarbeidet.

Janne M Hagens doktorgradsavhandling fra 2009 omhandler effektiviteten til ulike IS-tiltak, og har konsentrert seg om i hvilken grad de ansatte følger organisasjonens sikkerhetspolicy. De ansattes bevissthetsnivå kan være en begrensende faktor for å oppnå ønsket sikkerhet (Hagen 2009). Resultatet fra arbeidet indikerer at god overvåkning praksis kan påvirke det formelle systemet og ledelsens holdinger til sikkerhet. Samtidig viser arbeidet at et godt formelt system bidrar til de ansattes mulighet og evne til å detektere sikkerhetsbrudd. Sistnevnt sammen med rapportering

[10] ENISA The European Network and Information Security Agency

kan ytterligere forbedres ved å trene/utdanne de ansatte i IS med bruk av e-læringsprogrammer (Hagen 2009). Arbeidet argumenterer derfor for å drive kontinuerlig sikkerhetsutdanning og bevisstgjørende arbeid (Hagen 2009).

Albrechtsen (2007) har gjort en empirisk undersøkelse der arbeidet har vært konsentrert om å identifisere brukerens rolle i informasjonssikkerhet og hvilke oppfattninger brukerne selv har av emnet, gjennom å intervjue ansatte i ulike organisasjoner. Dette er undersøkelser av kvalitativ art. Dette arbeidet er brukt for å begrunne hvordan ulike metoder for bevissthetsbygging kan oppfattes, og i hvilken grad de oppfyller den tenkte hensikten. Resultatene viser at brukere er motiverte til å drive IS-arbeid. Alikevel utøver de få individuelle handlinger som bedrer sikkerheten, de har også begrenset kunnskap om hva de eventuelt kan gjøre (Albrechtsen 2007). Det vises til at IS-arbeidet kan medføre en interessekonflikt mellom funksjonalitet og ønsket informasjonssikkerhet. I tillegg viser arbeidet at ulike motiver og prioriteringer kan medføre en adferd mot uakseptable risiko. Albrechtsen (2007) viser her til en modell av Jens Rasmussen (Rasmussen 1997), for å indikere at dette medfører utfordringer for personer som innehar ansvaret for IS. En av Albrechtsens informanter henviser godt til disse utfordingene gjennom følgende uttalelse:

”Informasjonssikkerhet er ikke min jobb, jeg må konsentrere meg om mine egne arbeidesoppgaver og stole på at et IS-system er på plass. IS er ikke noe jeg burde tenke på.”

I lys av denne uttalelsen vil de sannsynligvis være nødvendig for IS-personellet å utføre IS-bevissthetsøkende arbeid. Et arbeid som kan bli en motvekt til en adferd som kan medføre en uakseptabel risiko i organisasjonen.

Albrechtsen har gjennomført ytteligere forskningsarbeide basert på empiriske undersøkelser. I en publikasjon er effekten av en IS-bevissthetsprogram undersøkt (Albrechtsen & Hovden 2010). Det interessante med dette programmet er at det legges vekt på en aktiv deltagelse av de ansatte i mindre grupper. Den indiviuduelle adferdsendringen og bevissthetsøkningen kommer som en effekt av opparbeidet kunnskap på et organisatorisk nivå, av gruppeprosesser og felles refleksjoner rundt emene (Albrechtsen & Hovden 2010). Hvilket er en motsetning til de mer tradisjonelle metoden som beskrives. Der legges det ofte vekt på å nå flest mulige ansatte med metoder som i større grad er basert på enveis kommunikasjon, fra ekspert til mottaker. Her benyttes ofte formelle presentasjoner, e-mail, plakater og brosjyrer. Resulatet fra arbeidet viser en positiv endring av de ansattes IS-bevissthet og adferd. Endringen viser seg også å vedvare over tid (Albrechtsen & Hovden 2010). Enkelte prinsipper viser seg å være sentrale for å oppnå suksess. Spesielt trekker vi her frem at de ansattes termer og språk benyttes, at lokalt uutalt kunnskap[11] deles og at gruppeprosessen styres med en avslappet holdning, som mulggjør gjensidig tillit i gruppen (Albrechtsen & Hovden 2010).

De nevnte publikasjonene er benyttet i Albrechtsen doktorgradsavhandling (Albrechtsen 2008), hvor formålet var å undersøke IS forvaltingen/styringen av de ansatte. Avhandligen belyser derfor en rekke viktige aspekter som må tas hensyn til i

[11] Uutalt kunnskap: vår oversettelse av det engelske begrepet tacit knowlege

en helhetlig strategiendring i vårt prosjektsperspektiv, men de blir for omfattende å omtale innenfor prosjektes begresninger.

Videre er det identifisert ulike studier som argumenterer for å forandre måten en ser på bevissthetstrening, blant annet (Bishop 2007) og (Jemal H. Abawajy et al. 2008).

Foregående litteratur argumenterer for nødvendigheten og effekten av å drive IS-bevissthetsøkende arbeid. Litteraturen viser til viktige faktorer å ta hensyn til ved en implementering av denne type arbeid. Det argumenteres for at ulike metoder kan benyttes i et IS-bevissthetsprogram, ut i fra hvilke type publikum man ønsker å nå. Det virker også å være ulike syn på hvilke metoder som er mest effektive. Dette må også vurderes ut i fra organisasjonens behov og tilgjengelige ressurser. Av dette ser vi igjen behovet for et system som kan vise til målbare resultater. Gjennom dette tilsier litteraturen også at det kan argumenteres for at en generell økning av forståelse og kunnskap vil sette organisasjonen bedre i stand til å observere motstanderens handlingsmønster. Bevissthetsbygging vil med dette handle om å benytte menneskene i organisasjonen som sensorer, og sette dem i stand til å oppfatte, forstå og kommunisere informasjon slik at et best mulig felles situasjonsbilde og forståelse av fiendens hensikt og kapasiteter, kan oppnås. Litteraturen som er identifisert omhandler således bevissthetsbygging generelt sett. Vi har ikke funnet noe bakgrunnsmateriale, ut over det nevnte, som knytter resultatet av en slik bevissthetsbygging direkte til det å danne seg et oppdatert bilde av motstanderen.

Dersom det kan vises til at en økt IS-bevissthet øker antallet indikatorer, som videre øker kunnskapen om fiendens virkemåte og motiver. Vil det i henhold til Kott & McEneaney (2006) være grunnlag for at økt bevissthet kan effektivisere forsvaret av informasjon.

Kildene beskriver ulike aspekter av bevissthet. Den ene siden av dette er det som ofte omtales som brukerbevissthet (user-awareness). Dette er definert som den generelle bevisstheten som finnes hos menneskene som er involvert. Dette kan være de ansatte, ledelsen etc. For å oppnå dette må uformelle kontroller implementeres for at ansatte i organisasjonen skal forstå sin rolle i informasjonssikkerhetsarbeidet, viktigheten av sikkerhetsrutiner m.m. (Albrechtsen 2007).

Et annet aspekt av begrepet bevissthet er den forståelsen av, kunnskapen om og bevisstheten på den fienden en står ovenfor, som ligger hos de som direkte arbeider med forsvar av informasjon. Dette vil typisk være de som arbeider direkte med informasjonssikkerhet. CND[12] avdelinger, CERT[13] avdelinger etc., og deres bevissthet og kunnskap om trusselaktører samt deres teknikker, taktikker og strategier, og denne bevisstheten betydning for virksomhetens evne til å avsløre og håndtere sikkerhetstruende hendelser. Dette aspektet av bevissthet er derfor nært knyttet til det som omtales som fiendeforståelse/fiendebilde i denne oppgaven.

I vårt tilfelle vil det være nødvendig å undersøke om økt effektivitet kan oppnås ved å benytte en større andel av ressursene på IS-bevissthetsarbeid. Relasjonen mellom økt

[12] CND- Computer Network Defense
[13] CERT – Computer Emergency Response Team

bevissthet i organisasjonen, og redusert risiko er beskrevet i Sveen et al. (2009). Artikkelen sannsynliggjør at ved å øke den generelle bevisstheten i organisasjonen vil en få en økt og mer presis innrapportering av sikkerhetsrelaterte hendelser. En suksessfaktor for å oppnå dette er at det opprettes en toveis kommunikasjon mellom brukerne og CERT-avdelingen. Tilbakemeldinger på status og de positive konsekvensene av innrapporterte hendelser, viser seg å være suksessfaktor for og motiverer brukere til aktivt å rapportere sikkerhetshendelser (Sveen et al. 2009). Gjennom å etablere prosedyrer som sikrer dette samspillet mellom vanlige brukere og de som arbeider med informasjonssikkerhet kan en oppnå lavere risiko og økt forståelse av fienden. Det refereres her til figur 2, der sammenhengen mellom økt IS-bevissthet og økt fiendeforståelse er skissert i sammenheng med prosjektets overordende målsetting. Nemlig en mer effektiv utnyttelse av IS-ressurser og et mer proaktivitet i IS-arbeidet.

Det er her identifisert kilder som omtaler økt bevissthet innen en organisasjon, litteraturen viser at det kan føre til en rapportering og kommunikasjon innad i organisasjonen som ikke nødvendigvis bare øker i mengde, men som også er av høyere kvalitet. I tillegg er det vist til at bevissthetsnivået generelt sett kan være en begrensende faktor for informasjonssikkerheten. Dette indirekte at relevant informasjon, for å lære om og forstå motstanderen, kan oppfattes i organisasjonen og benyttes av beslutningstagere, dersom forholdene ligger til rette.

## 3.4 Bevissthetsprogrammet

Det er ikke i tilstrekkelig grad identifisert litteratur som omtaler utvikling og innføring av bevissthetsprogrammer, spesielt med tanke på vinklingen i dette prosjektet. Dette gjelder i stor grad de undersøkelsene av sammenhengen mellom en generell IS-bevissthet i organisasjonen og CND personellet evne til å danne seg et oppdatert fiendebilde. Imidlertid er det valgt å benytte seg av en tilfellestudie som beskriver en innføring og drift av et IS-bevissthetsprogram. Vi har analysert hvilke anbefalinger som gis, og undersøke i hvilken grad annen litteratur bidrar til å sannsynliggjøre gyldigheten av denne tilfellestudien. Tilfellestudien er valgt på bakgrunn av at den i stor grad er basert på reelle undersøkelser, praktiske gjennomføringer og faktiske tilfeller. Vi har derfor valgt å analysere denne reelle beskrivelsen av hvordan et bevissthetsprogram kan gjennomføres (Wright & Kakalik 2006, s187-205). Her er det beskrevet et tilfelle som implementerer mange av de retningslinjene som er beskrevet i annen bakgrunnslitteratur. I tillegg har programmet rutiner for kontinuerlig oppfølging, forbedring og måling av programmets effektivitet. Analysen av tilfellestudiet vil gjøres med det formål å identifisere suksesskriterier som kan benyttes i det videre arbeidet opp i mot Forsvarets organisasjon. Det er derfor utført litteraturstudie for å undersøke gyldigheten av den omtale tilfellestudien, og i hvilken grad de identifiserte suksesskriterier anerkjennes av annen litteratur. Funnene anses derfor som generaliserbare også utenfor Forsvaret.

Boken *Information Security – Contemporary Cases* (Wright & Kakalik 2006) beskriver ulike reelle scenarioer innen informasjonssikkerhet. En av disse casene omhandler som nevnt utvikling og gjennomføring av et IS-bevissthetsprogram i et av de største forsikringsselskapene innen helse og personforsikringer i USA, Aetna Inc. Programmet, slik det er beskrevet i casen, ble innført i 1999 og har siden mottatt

profesjonell anerkjennelse. Blant annet ble programmet i år 2000 beskrevet av SANS institute[14] som "modellen andre organisasjoner burde følge". Det er beskrevet at dette programmets suksess var på bakgrunn av at Aetna lykkes i å etablere et kostnadseffektivt program som forbedret brukernes bevissthet og sikkerhetsadferd på en målbar måte. Bevissthetsprogrammet var basert på realistiske mål, samtidig som det knyttet informasjonssikkerhet sammen med det generelle forretningsmiljøet i organisasjonen. Det er også tilpasset det eksisterende miljøet og organisasjonskulturen. Programmet benyttet seg av flere ulike metoder for å spre sikkerhetsbudskapet for å sikre at alle ble inkludert i sikkerhetsutdanningen. Ikke minst ga programmet muligheten for å måle effekten i form av økt kunnskap og endret adferd, samt at det var sikret støtte fra ledelsen. Ikke bare i forkant, men også vedvarende kontinuerlig støtte. Disse suksessfaktorene implementerer anbefalte metoder fra annen litteratur og er i tillegg understøttet av reelle resultater. Analysen av denne casen vil senere i prosjektet benyttes til å undersøke om disse prinsippene kan være egnet for Forsvaret. Vi vil se på hvordan dette eventuelt kan gjennomføres, hvilke tilpasninger må ligge tilgrunn, og om dette kan være realiserbart. Videre vil det betraktes om de positive effektene som kan oppnås kan tilføre ny kunnskap og forståelse av det trusselbildet en står ovenfor.

For å beskrive og analysere dette programmet skal vi gå nærmere inn på de identifiserte suksessfaktorer fra Case 7 (Wright & Kakalik 2006). Annen litteratur blir benyttet for å bekrefte eller avkrefte gyldigheten til disse faktorene:

- Kostnadseffektivitet
  - Organisasjonstilhørighet og tildeling av ansvarsområder har vært en avgjørende faktor for å sikre effektivitet og gjennomslagskraft i programmet. Sentralisering og konkretisering av sikkerhetsvirksomheten sikret et helhetlig og kosteffektivt program. Programmet benyttet målrettede virkemidler med en lav relativ kostnad, viktigheten av dette underbygges i artikkelen (Power & Forte 2006). I artikkelen belyses til eksempel at å benytte seg av elektronisk distribuerte nyhetsbrev kan gi god effekt, spesielt når man ser effekten opp i mot de lave kostnadene. Dog tilsier annen litteratur et denne metoden har begrenset effekt sammenliknet med metoder som baseres på toveis kommunikasjonen (Albrechtsen & Hovden 2009; Sveen et al. 2009). Viktigheten av og evaluerer kostnadseffektiviteten er derimot like gjeldende og underbygges ytterligere i NIST 800-50 (NIST 2003). Her beskrives det at en i planleggingsfasen må vurdere de enkelte tiltaks kostnader og ha en klar oppfatning av hvilke økonomiske rammer en er underlagt. Det vises til at det minimum av krav en har til programmets resultater må kunne dekkes innenfor disse rammene. Det vises til at dette i planleggingsfasen identifiserer kravet til økonomiske midler og sikrer økonomisk støtte for implementering og kontinuerlig drift (NIST 2003).

[14] SANS Institute. Forsknings- og utdanningsorganisasjon etablert i 1989. SANS står for SysAdmin, Audit, Network, Security. *http://www.sans.org*

- Målbare resultater
    - Organisasjonen benytter seg av ulike virkemidler for å kontrollere og måle effekten programmet. Både for å sikre at programmet har effekt over tid, og kontinuerlig forbedring. Viktigheten av å utarbeide metrikker for å kunne måle bevissthetsprogrammets effektivitet er beskrevet ytterligere i artikkelen av McCoy & Fowler (2004). Eksempler på slike metrikker er beskrevet i (NIST 2003 Appendix B). Det vises til at slike faktorer er utfordrende å identifisere, og det beskrives å benytte seg av statistikk og analyse av trender for å identifisere programmets effektivitet. Å kunne produsere målbare resultater vil være essensielt i prosessen med kontinuerlig forbedring og utvikling (NIST 2003; Power & Forte 2006).

- Realistiske mål
    - Etablering av realistiske mål for ulike personellkategorier, basert på en grundig vurdering av de emnene som er viktige innen hver kategori (Siponen 2001). I tillegg anbefales det å utarbeide realistiske mål innefor hvert aspekt av bevissthetsprogrammet (bevissthetsnivå, utdanningsnivå, sertifisering etc.) (NIST 2003)

- Tilpasning til ulike mennesker og funksjoner samt organisasjonskultur og dermed bør man benytte ulike metoder for spredning av budskapet.
    - Et viktig element i denne sammenhengen er å identifisere ulike kategorier av personell som skal omfattes av programmet (McCoy & Fowler 2004). Dette kan bidra til å utvikle et tilpasningsdyktig og differensiert program som benytter flere ulike metoder for spredning av budskapet på en måte som er tilpasset målgruppen (NIST 2003). Valentine (2006) argumenterer også for en tilpassing opp i mot jobbfunksjoner. Valentine sier at det vil virke demotiverende for de ansatte å måtte delta på et omfattende opplærings eller utdannigsopplegg så lenge det ikke treffer det faktiske behovet innen den enekltes jobbfunksjon. På tross av disse anbefalingene virker de tradisjonelle bevissthetsprogrammene å benytte en fellesløsning i stedet for individuelt tilpassede løsninger til hver jobbfunksjon (Valentine 2006).

- Sammenknytning informasjonssikkerhet og forretningskultur
    - Programmet er tilpasset den kulturelle egenart som eksisterer i organisasjonen. Denne faktoren er ytterligere beskrevet i (NIST 2003). Her fokuseres det på at bevissthetsprogrammet må utvikles i tråd med organisasjonens overordende mål. Dette er ikke minst viktig med tanke på å sikre at en får og beholder tilstrekkelig støtte fra ledelsen.

- Sikre kontinuerlig støtte fra ledelsen.
    - Hierarkisk plassering av ansvarsområdet har vist seg å ha avgjørende betydning for å gi tilstrekkelig myndighet til å gjennomføre programmet, samt opprettholde ledelsens støtte. Det anbefales at hierarkisk plassering av tilgjengelige økonomiske midler og ansvaret for planlegging og gjennomføring av programmet gis til en sentral myndighet (NIST 2003).

Casen er benyttet og studert på bakgrunn av den praktiske tilnærmingen som er beskrevet. De omtalte faktorene er implementert og benyttet i praksis, noe som kan indikere deres gyldighet. Gyldigheten forsterkes av at man har implementert systemer for å kontrollere og måle effekten av tiltakene. Nettopp dette danner grunnlaget for en kontinuerlig kvalitetsforbedringsprosess, med en evaluering av om de benyttede tiltakene er de best egnede eller ikke. Videre er det identifisert ytterligere kilder som sannsynliggjør faktorenes gyldighet. Det beskrives i litteraturen at en tilpasning til hver enkelt organisasjon og tilfelle er av avgjørende betydning. Det vil derfor ikke være en fremgangsmåte/metode som er passende i enhver situasjon (McCoy & Fowler 2004) og (NIST 2003). Derfor er egen organisasjonsbevissthet en viktig faktor for å lykkes. Derfor er det i det videre arbeidet funnet nødvendig å vurdere suksessfaktorene i den kontekst som er aktuell i dette prosjektet og ved studier av Forsvarets organisasjon forsøke å identifisere i hvilken grad dette er relevant og passende. I tillegg vil vi forsøke å undersøke om det finnes spesifikke egenskaper ved organisasjonen som gjør at det kan finnes ytterligere suksessfaktorer som må tas hensyn til.

Litteraturstudiet er gjennomført som beskrevet innledningsvis, ved hjelp av nøkkelordsøk på anerkjente vitenskapelige databaser. Referanser i interessante artikler har blitt benyttet for å identifisere annen relevant litteratur. Det er også benyttet annen faglitteratur og bøker. Litteraturstudiet må vurderes med tanke på de ressurs og tidsmessige begrensninger prosjektet er underlagt. Dette kan gjøre at relevant litteratur ikke er identifisert og tatt hensyn til.

**Kapittelets resultater:**

- Grunnleggende mangler ved tradisjonelle, reaktive metoder for beskyttelse av informasjonssystemer
- Det er svært sannsynlig at den målrettede trusselaktør eksisterer og utgjør en reell trussel mot organisasjonen
- Trusselbildet er dynamisk og tilpasningsdyktig
- Informasjonsoverlegenhet er avgjørende
- Forskning, understøttet av empiri, gir anbefalinger angående bevissthetsøkende arbeid.
- Det er identifisert relevant litteratur angående delemner, men koblingen mellom bevissthetsøkning og fiendebilde er lite omtalt.

# 4 Hypoteser og forskningsspørsmål.

I dette delkapittelet presenteres prosjektets forskningshypoteser med tilhørende forskningsspørsmål. Svar på forskningsspørsmålene vil ikke benyttes til å forkaste eller beholde hypotesene, men som en argumentasjon og indikasjon på en økt eller minsket tiltro til hypotesenes gyldighet. Videre forskning vil så baseres på resultatet av forskning på de respektive forskningsspørsmål, og tiltroen til hypotesene.

**Kapittelets innhold:**

- Presentasjon av prosjektets hypoteser med tilhørende forskningsspørsmål
- Hypoteser i (P`HAPI)

Problemstillingen henviser til at dagens strategi for beskyttelse av informasjonssystemer medfører at dagens beskyttelsestiltak gjør at den som forsvarer systemene ligger et steg bak angriperen. Strategien beskrives som reaktiv og gir den avanserte motstanderen store konkurransefortrinn, da kjente sårbarheter gjøres kjent for alle inkludert fienden. Fienden kan benytte informasjonen til å tilpasse og målrette sine angrepsmetoder. Litteratur sannsynliggjør at dette er tilfelle, men det er ikke identifisert litteratur som kan vise til empiriske data i sin argumentasjon. Vi formulerer derfor en forskningshypotese rundt dette.

*Hypotese 1:* *Det er sannsynlig at dagens strategi for beskyttelse mot cybertrusselen, gir den avanserte/intelligente motstanderen store konkurransefortrinn.*

Et nøkkelord i problembeskrivelsen er reaktivitet, og konsekvensen av den reaktive beskyttelsen er at forsvaret av informasjonssystemer blir liggende et steg bak angriperen. For å kunne indikere sannsynligheten av hypotese 1, og underbygge problemstillingen samt samle empiriske data rundt dette må arbeidet kunne indikere svar på forskningsspørsmål 1.1.

1.1 Finnes det informasjon som indikerer eller motbeviser, at dagens beskyttelsesmetoder i hovedsak er fundamentert på erfaring og læring fra kjente vellykkede angrep og kan beskrives som reaktive?

Selv om arbeidet med forskningsspørsmål 1.1 skulle bekrefte den reaktive beskyttelsen, er det alene ikke nok til å sannsynliggjøre hypotese 1. Skal hypotesen kunne sannsynliggjøres må forskningen også kunne sannsynliggjøre at den målrettede og avanserte trusselaktør eksisterer. Litteraturen anerkjenner at denne motstanderen eksisterer, men viser til lite empiri i sin argumentasjon. Det er også identifisert lite litteratur som beskriver en dynamisktilpassningsdyktig motstander, som kan tilpasse sine angrep med bakgrunn i våre beskyttelsestiltak. Sistnevnte ble ansett som sentralt å undersøke og utrede, før vi kunne argumenterer for en økt eller minket tiltro til hypotese 1, og for å underbygge behovet for andre IS-strategier. Svar på

forskningsspørsmål 1.2, sammen med 1.1, vil derfor gi økt eller minket tiltro til hypotese 1.

1.2 Finnes det informasjon som indikerer eller motbeviser, at motstanderen tilpasser sine taktiske og tekniske prosedyrer til våre tiltak, og metoder for innhenting av trusselinformasjon?

Det argumenteres for andre innfallsvinkler og strategier for IS-arbeidet gitt av problemeier, og fra funn i litteraturen. Beslutningen om å studere potensialet ved i større grad å konsentrere arbeidet rundt selv problemet, fienden, førte til at emnet fiendemodellering ble studert. Vi anser innfallsvinkelen som noe utradisjonell med tanke på dagens massive konsentrasjon rund tekniske implementeringer innen IS-domenet. Dette underbygges også i en studie av 20 ulike sikkerhetskonferanser (Botha & Gaadingwe 2006). Studien viser at rapporter til disse konferansene har blitt mer og mer teknisk rettet. Statistikken viser at også innen fagmiljøet er det mest aktivitet innen tekniske løsninger (Botha & Gaadingwe 2006). Funn i litteraturen innen fiendemodellering, relevant for prosjektet, var også noe begrenset. Men litteraturen viser at fiendeforståelsen er essensiell innen en konkurransepreget situasjon, og beskriver dette som viktig å ta hensyn til i utviklingsfasen av et system. Dette er et paradoks i seg selv. Problemet er jo nettopp det, at fienden vi står ovenfor sannsynligvis er dynamisk og tilpasningsdyktig i stor grad. Det kan derfor antas at det er et kontinuerlig behov for å kjenne sin motstanders mål og motivasjon for angrep, og ikke fortrinnsvis kun i utviklingsfasen. Vi formulerer derfor en hypotese rundt dette til det videre forskningsarbeidet.

*Hypotese 2:* *Det er sannsynlig at en strategi basert på økt fiendeforståelse kan endre dagens beskyttelsestankegang til en forsvarstankegang og gjøre sikkerhetsarbeidet proaktivt i større grad.*

Litteraturen er lite beskrivende i detalj angående hvilke indikatorer som vil være utslagsgivende for fiendeforståelsen i prosjektets perspektiv. Dette er grunnlende informasjon for å indikere gyldigheten av hypotese 2. Forskningsspørsmål 2.1 er formulert med dette formålet.

2.1 Hvilke indikatorer har betydning for fiendeforståelsen?

Videre formulerer vi forskningsspørsmål 2.2. For å besvare dette må det fremskaffes empirisk data rundt hvordan fiendeforståelsen faktisk påvirker eller avgjør ressurstildelingen innen beskyttelse av dagens informasjonssystemer.

2.2 Finnes det indikasjoner om at økt kunnskap om fienden kan gjøre oss bedre i stand til en dynamisk tilpasning av forsvarsressursene iht. endringer i trusselbildet?

Forskningen som skal gi oss økt eller minket tiltro til hypotese 2 vil i prosjektet begrenses til arbeidet med forskningsspørsmålene 2.1 og 2.2. Litteraturen beskriver videre ulike metoder for å øke IS bevisstheten til ansatte innen en organisasjon. Litteraturen er i hovedsak begrenset til konseptuelle analyser. Derfor har vi vektlagt litteratur som viser til noe empiri. Skal det være grunnlag for si noe om

bevissthetsøkende arbeid i organisasjonen, om det er vellykket implementert og skaper grunnlag for en bedre fiendeforståelse, kreves det at det gjøres forskning på dette. Med andre ord må det undersøkes om det finnes synergieffekter mellom økt IS-bevissthet og økt fiendeforståelse. Ut av litteraturen er det mulig å argumentere og sannsynliggjøre denne sammenhengen, men vi har ikke identifisert noe litteratur som beskriver denne måten å benytte eller skreddersy bevissthetsarbeidet. Vi formulerte derfor hypotese 3, som sier følgende:

*Hypotese 3:* *Det finnes indikasjoner på at strategien for beskyttelse/forsvar i større grad bør baseres på bevissthetsøkende arbeid, som kan gi grunnlag for et bedre mentalt bilde av motstanderen*

For å kunne besvare hypotese 3 i tråd med situasjonen problemeier foreskriver formulerte vi forskningsspørsmål 3.1, der Forsvaret direkte involveres i arbeidet.

3.1 I hvilken grad har bevissthetsnivået en betydning for Forsvarets fiendeforståelse?

Et av hovedformålene med prosjektarbeidet er å forsøke å identifisere om andre IS-strategier muliggjøre en mer effektiv utnyttelse av tilgjengelige ressurser enn dagens strategi. I hvilken grad valgte innfallsvinkel faktisk gjør dette vil også være med å kunne sannsynliggjøre hypotese 3. Formuleringen av forskningsspørsmål 3.2 vil derfor kunne benyttes i argumentasjon innen de overnevnte problemstillinger.

3.2 Er det sannsynlig at en strategiendring basert på økt bevissthet kan gi grunnlag for en mer effektiv ressursutnyttelse og bedret sikkerhet?

Problemeier skisserer problemet ut fra Forsvarets perspektiv, og etterlyser som nevnt en annen strategi som bedrer dagens situasjon. Det faller derfor naturlig å undersøke i hvilken grad våre hypoteser er gjeldende innen Forsvaret. Grunnet ønske om å undersøke dette har vi formulert hypotese 4.

*Hypotese 4:* *Det er grunn til å tro at veien til bedre informasjonssikkerhet gjennom økt fiendeforståelse, krever et organisert bevissthetsprogram i Forsvaret. Skreddersydd og spisset mot Forsvarets behov.*

Innledningsvis ansees det som nødvendig å identifisere i hvilken grad et bevissthetsprogram er implementert i dag. Dette vil reflektere hvilke muligheter det er for å skreddersy dette mot å gi en økt fiendeforståelse i Forsvaret, så fremt resultatet av det tidligere arbeidet tilsier at innfallsvinkelen potensielt vil kunne gi ønsket effekt. Litteraturstudiet er ikke benyttet til å identifisere om dette er implementert i Forsvaret tidligere. Vi formulerte forskningsspørsmål 4.1 med tanke på dette, og tilfellestudien rettet mot Forsvaret benyttes i all hovedsak for å sannsynliggjøre hypotesen og besvare forskningsspørsmålene. I samtaler med problemeier har det kommet frem at Forsvaret potensielt vil kunne dra nytte av dette, men det kreves videre forskning. Det kan her legges til at sensitivitetsproblemetikken vil bli tatt hensyn til, og kan medføre at arbeidet blir beskrevet overfladisk og generelt i rapporten.

4.1 I hvilken grad er IS-bevissthetsprogram implementert i Forsvaret i dag.

Resultatet av litteraturstudien gir bakgrunnsmateriale som belyser ulike suksesskriterier ved for hvordan man implementerer et bevissthetsprogram i en organisasjon. Litteraturen anbefaler også ulike prinsipper og metoder for å drive et vellykket og effektivt IS- bevissthetsarbeid. Denne kunnskapen vil bli benyttet i det videre arbeidet for undersøke om overnevnte også er egnet for Forsvaret, og er formulert i prosjektets siste forskningsspørsmål.

4.2 *Finnes det egnede kilder fra litteraturen som gir anbefalinger med tanke på utvikling og gjennomføring av bevissthetsprogrammer som kan være egnet for Forsvaret.*

**Kapittelets resultater:**

- Prosjektets hypoteser med tilhørende forskningsspørsmål er presentert med forklaringer
- Utarbeidet på bakgrunn av problembeskrivelse og litteraturstudiet
- Danner grunnlaget for den videre forskningen i prosjektet

# 5 Intervjumetode

**Kapittelets innhold:**

- Identifikasjon av egnet forskningsmetode
- Begrunnelse for valget av metode(r) og vurdering av egnethet
- Beskrivelse av metoden, med fremgangsmåte, styrker og svakheter
- Analyse (P`HAPI)

Masterprosjektets problemstilling er inspirert av problemeier i Forsvaret. Imidlertid er problemstillingens formulering tydelig relevant også utenfor Forsvarets organisasjon. I forskningen for å besvare forskningsspørsmålene er det blitt benyttet, i størst mulig grad, ugraderte kilder til informasjon. Dette er blitt underbygget av informasjon samlet fra problemeiers organisasjon. Prosjektet er utført som en tilfellestudie[15] i Forsvaret, og kvalitative metoder er benyttet. Å benytte seg av tilfellestudie som metode innebar at prosjektgruppen måtte underlegge seg en rigorøs tilnærming til de retningslinjene som er anbefalt for denne typen forskning. Prosjektet har således fulgt og benyttet seg av metodiske anbefalinger slik det er gjengitt i (Yin 2008). Begrunnelsen for valget av tilfellestudie som metode er basert på de anbefalingene som gis, og ved at problemstillingen og studiet som sådan ansees å være godt egnet for denne metoden. Yin (2008) viser til tre faktorer som er avgjørende for at tilfellestudie skal være egnet;

- forskningsspørsmålene inneholder ”hvordan” eller ”hvorfor” spørsmål
- forskeren har liten innvirkning på de hendelser som skal undersøkes
- forholdene som skal undersøkes er reelle tilfeller, og foregår i sanntid

Med tanke på de faktorene som er gjengitt over er våre forskningsspørsmål ansett som et egnet scenario for en tilfellestudie. I tillegg samt at våre undersøkelser angående hvordan aktuelle temaer oppfattes ivaretatt og implementert fra informantene ståsted, underbygger valget av tilfellestudie som metode. Forskningsspørsmålene som er underlagt hypotese 3 og 4, inneholder ikke direkte spørreordene slik de står over, men ”i hvilken grad” sammenlignes med ”hvordan”. Videre er systemet vi har undersøkt slik at prosjektgruppen ikke har hatt noen innvirkning på hendelsene, og var således en passiv observatør til hendelser som foregikk i sanntid.

Det innledende arbeidet var naturlig nok en litteraturstudie av relevant litteratur opp mot problemstillingen, og er presentert i kapittel 3. Dette arbeidet har fulgt de anbefalinger som er gitt rundt å benytte seg av denne typen forskning. Litteratursøk har hovedsakelig vært utført på anerkjente databaser som ACM, IEEE, Springerlink og så videre. Begrensninger i dette arbeidet kan ha medført at relevant litteratur ikke har blitt tatt hensyn til, eller blitt vektlagt. På tross av disse begrensningene, har

[15] Tilfellestudie - oversettelse av det engelske begrepet Case Study

litteraturstudiet ført til formuleringen av prosjektets hypoteser og forskningsspørsmål i kapittel 4. Dette ble som kjent utgangspunktet for prosjektets videre forskningsarbeid. Til forskningsarbeidet ble metodevalget for innhenting av data, basert på intervju og diskusjoner med informanter med ekspertise innen de respektive emnene.

## 5.1 Studie av relevant litteratur/valg av metode

Fagemnet informasjonssikkerhet blir ofte forbundet med hemmeligholdelse og konfidensialitet. At det i tillegg ble valgt å utføre en tilfellestudie i Forsvaret, kan ha medført at denne problemstillingen forsterkes. Samtidig anså vi antallet relevante informanter med tilstrekklig kompetanse på emnene som en begrensende faktor. Aspektene som belyses her gjorde at vi anså det som en krevende prosess å få tilgang til nødvendig informasjon. Videre anså vi at temaene underbygget valget av kvalitative metoder, da arbeidet kunne baseres på en dyptgående datainnsamling fra få informanter.

Validitet, pålitelighet og generalisering nevnes som viktige prinsipper innen forskning, og benyttes ved vurdering av datakvalitet, kvaliteten på forskningsarbeidet og gyldigheten til forskningsresultatet. Innen kvalitativt forskning benyttes ofte en noe annerledes begrepsbruk (se tabell 1) (Lilledahl & Hegnes 2000). Det kvalitative begrepsapparatet vil bli benyttet, siden kvalitative metoder benyttes i prosjektarbeidet.

| Kvantitativ metode | Kvalitativ metode | Begreps forklaring ved kvalitativ metode |
|---|---|---|
| Pålitelighet | Troverdighet | Vurdering av fremgangsmåte og forskningsprosess. Skal kunne analyseres av andre, og være utført på en tillitsvekkende måte. |
| Validitet | Bekreftbarhet | Omhandler kvalitet på tolkningen, og at forståelsen forskeren kommer frem til skal kunne bekreftes av annen forskning |
| Generalisering | Overførbarhet | Kan tolkninger og forståelsen også være gjeldende i andre sammenhenger? |

Tabell 1. Begrepsapparat innen kvantitativ versus kvalitativ metode (Lilledahl & Hegnes 2000)

Utfordringen som er skissert innledningsvis i dette delkapittelet måtte håndteres, samtidig som de omtalte forskningsprinsippene måtte etterleves. En beskrivelse av hvordan tilgangen til informasjon og på hvilket nivå denne informasjonene er gitt, er viktige parametere da troverdigheten og bekreftbarheten til oppgaven skal evalueres

(Sveen et al. 2008). Dette kan implisitt være en vurdering av oppgavens kvalitet. Vi valgte derfor å beskrive denne prosessen i metodekapittelet.

## 5.2 Beskrivelse av metode ved intervju

For å skape troverdighet til forskingsarbeidet er utvalgsstrategien som ble benyttet for å identifisere informanter beskrevet og argumentert for nedenfor. Informasjonsbehovet i denne tilfellestudien krevde at de utvalgte informantene oppfylte enkelte kriterier. Det ble ikke ansett som nødvendig at hver enkelt informant oppfylte alle kriteriene, men aktuelle informanter måtte kunne bidra med informasjon om en eller flere av fagemnene sammen med det første kriteriet. Kriteriene er valgt ut fra en vurdering av hvilke kunnskap og informasjon som ble ansett som viktige for prosjektet. En generell kunnskap om Forsvarets organisasjon er vektlagt. Videre ble informantene valgt ut med tanke på deres erfaring og/eller nåværende funksjon med relevans for prosjektets emner. Generelle kunnskaper om informasjonssikkerhet var en forutsetning. Personell knyttet til avdelinger som har informasjonssikkerhet som en av hovedoppgavene ble derfor benyttet. Det ble videre definert kriterier som beskriver spesialiserte kompetanseområder, som er relevante for prosjektet.

1. Informanten må ha kjennskap til Forsvaret og dagens situasjon i forbindelse med sin ekspertise.
2. ekspertise innen generell informasjonssikkerhet
3. ekspertise innen bevissthetsbygging
4. ekspertise innen fiendemodellering

Da informantene må oppfylle ulike kriterier for å være kvalifisert til å bli valgt ut som informanter vil denne strategien kunne betegnes som en kriterieutvalgsstrategi (Patton 2002 s. 243). Denne utvalgsstrategien[16] kan klassifiseres som en hensiktsmessig utvalgsstrategi, hvor man strategisk og hensiktsmessig identifiserer informanter ut ifra forskningsarbeidets formål og ressurser (Patton 2002 s. 243). Dette betyr at sannsynligheten for å bli valgt ut som informant ikke er lik for hvert individ innen et gitt utvalg av mulige informanter.

Tilgangen til og identifiseringen av informanter kunne vært oppnådd ved en formell henvendelse til Forsvaret. En slik henvendelse ville måtte inneholdt en beskrivelse av problemstilling, formålet med masterprosjektet og utvalgskriterier til informanter. I tillegg til at denne innfallsvinkelen ville benyttet en formell inngangsport til Forsvaret ville den, om den var vellykket, kunne medført at enkelte autoriseringer og etiske problemstillinger kunne bli løst på et overordnet nivå. Fremgangsmåten ville også vært mulig å benytte for personer uten kunnskap om Forsvarets organisasjon, og derfor vil derfor enklere kunne repeteres. Innfallsvinkelen ville etter all sannsynlighet vært meget tidkrevende, da henvendelsen ville måtte prosesseres gjennom en rekke ”flaskehalser” før den nådde frem til aktuelle informanter. Strategien ble ikke valg med bakgrunn i at den ble ansett som for tidkrevende for de begrensningene prosjektet er underlagt.

[16] Utvalgsstrategi oversettelse av det engelske begrepet sampling strategy

Deltagerne i prosjektgruppen er ansatte i Forsvaret, i tillegg til at problemstillingen er inspirert av problemeier innen Forsvaret. Det var derfor naturlig å benytte denne kunnskapen til å redusere en ellers tidkrevende prosess. Problemeier ved Oblt. Roger Johnsen kunne også fylle rollen som en strategisk valgt ekspert. En kort profilbeskrivelse følger. Profilbeskrivelsen er ment som argumentasjon den strategiske ekspert besitter nødvendig kompetanse til å identifisere troverdige portåpnere (Sveen et al. 2008). Slik kunne prosjektgruppen korrekt og effektivt identifisere informanter som oppfyller en eller flere av utvalgskriteriene. Portåpnerne som også oppfylte kriteriene, ble i enkelte tilfeller benyttet som informanter. I tillegg henviste de strategisk valgte informantene videre til andre aktuelle informanter innen sitt fagdomene, som igjen viste til nye informanter. Dette er en iterativ prosess som ble avsluttet når prosjektgruppen identifiserte en informasjonsmetning[17]. Utvalgsstrategien som skisseres her benevnes ofte som en snøball- eller kjedestrategi (Patton 2002 s. 243).

### 5.2.1 Profilbeskrivelse: Strategisk valgt ekspert

Eksperten (Oblt. Roger Johnsen) har sivil mastergradsutdanning i tillegg til høyere militær utdanning fra krigs- og stabsskole. Det kan derfor argumenteres for en formell utdanning og kompetanse innen fagdomenet og Forsvaret. Kompetansen har i tillegg til formell utdanning vært opparbeidet gjennom en yrkeskarriere innen Forsvaret. Eksperten har her bekledd en rekke ulike stillinger fra ordinær arbeidstaker til mellomleder og høyere lederstillinger. Han har mer enn 20 års erfaring i Forsvaret i ulike stillinger fra avdelingsnivå til strategisk nivå, hvorav de 10 siste årene i lederfunksjoner innen sikkerhetstjeneste. Ut i fra dette argumenteres det for at eksperten har kompetanse som strekker seg fra det operative til det strategiske, innen det militærfaglige så vel som det teknologiske faget. Vi mener profilbeskrivelse viser at eksperten tilfredsstiller våre krav til en ekspert, og tatt i betraktning prosjektarbeidets tilgjenglige ressurser, særlig tidsressurser, vil uttalelser fra eksperten benyttes til og identifisere de første portåpnerne innen de respektive fagdomener.

## 5.3 Rammeverk for kvalitative forskningsintervju og sikring av intervjuets kvalitet

Da relevante eksperter/informanter var identifisert, kontaktet og samtykket til å inngå i prosjektet med sine uttalelser og betraktinger rundt emnene, ble tid og sted for intervjuer avtalt. For å sikre at disse kvalitative intervjuene skulle frembringe de resultatene vi ønsket, ble et rammeverk som skulle sikre kvaliteten på det som måtte fremkomme benyttet. Rammeverket er i stor grad basert på anbefalinger fra Kvale (1997), og er presentert under. Intervjuformen vi benytt oss av i arbeidet var av halvstrukturert karakter og foregikk uten strenge rammer. Det ble lagt til rette for at intervjueren kunne følge opp det som fremkom fra intervjupersonen, med oppfølgingsspørsmål eller kontrollspørsmål. Allikevel var det nyttig å inneha en viss predefinert struktur slik at samtalen ble holdt innen gjeldende kontekst. Dette ble gjennomført ved hjelp av intervjuer som fulgte enkelte temaer. Rammeverket ble således generalisert med tanke på hvilke temaer intervjuet skulle følge, da ulike

[17] Med informasjonsmetning menes har at man får bekreftet og repetert tidligere gitt og kjent informasjon.

informanter ble valgt ut fra deres ekspertise innen ulike temaer. Dette betyr at en tilpasning av rammeverket ble utført til hvert intervju. En grundig forberedelse anses som viktig for at intervjuet og resultatet av det skal bli godt (Kvale 1997).

### 5.3.1 Brifing

Intervjueren beskrev konteksten for intervjuet, og formidlet en kort presentasjon av prosjektgruppens medlemmer. De første minuttene av et intervju ble ansett som svært avgjørende, og det var viktig å etablere en god kontakt og relasjon med intervjuobjektet (Kvale 1997). Innledningen var bygget på de opplysninger som ble gitt i et informasjonsskriv, som på forhånd ble distribuert til informantene (vedlegg 1), samt en videre utdypning av hvorfor den aktuelle eksperten ble utvalgt.

### 5.3.2 Intervjuspørsmål/samtaletema

Temaene som ble diskuteres i hvert intervju ble, som nevnt tidligere, tilpasset i henhold til ekspertens/informantens fagfelt. Dette betyr at det ble tatt en vurdering i hvert tilfelle. Samtalene i intervjuene varierte derfor fra å stille konkrete spørsmål til mer eller mindre veiledende samtaler om temaet. Dette ble gjort ved å koble den enkelte informants forventede kompetanse og fagområde opp mot de hypoteser og forskningsspørsmål som er satt i prosjektet. Betraktningene dannet grunnlaget for en intervjuguide som ble utarbeidet og tilpasset til den enkelte intervjurundene samt intervjuobjektets profil. Intervjuguiden inneholder de emner som skal tas opp, samt rekkefølge. Dette er et hjelpemiddel som skulle sikre kvaliteten på intervjuet og holde samtalen innen de rammene prosjektet definerer. Intervjuguidene som ble benyttet er vedlagt i vedlegg 2 og 4, og disse spørsmålene definerer rammene for de semi-strukturerte intervjuene.

Et godt forskningsspørsmål og et godt intervjuspørsmål er ikke alltid to sider av samme sak, og det kan være viktig å tilpasse forskningsspørsmålene slik at de bli enklere å forstå og eventuelt dele dem opp i flere deler. Litteraturen anbefaler å legge vekt på at spørsmålene ivaretar den dynamiske delen av intervjuet, at de skaper en positiv interaksjon og er motiverende. Samtidig er det viktig at det tematiske/faglige elementet ivaretas. En god kombinasjon av dette bør tilstrebes (Kvale 1997).

Intervjuspørsmålene i denne sammenhengen ble altså tilpasset situasjonen, både i forkant ved å vurdere profilen til den enkelte informant, men også kontinuerlig i løpet av intervjuet avhengig av fremdriften. Forskningsspørsmålene som er definert i prosjektet er tematisk inndelt slik at de som tilhører hypotesene 1 og 2 i hovedsak dreier seg om å bekrefte bakgrunnsproblematikken for prosjektet. Hypotesene 3 og 4 er mer dreiet mot Forsvarets organisasjon, hvordan prinsippene er ivaretatt i dag, samt hvordan eventuelle anbefalte prinsipper kan implementeres.

### 5.3.3 Debrifing/Avslutning

I etterkant av intervjuet ble det foretatt en debrifing ovenfor intervjuobjektet ved hjelp av en rask gjennomgang av det som framkom. Vi fikk på denne måten verifisert bekreftbarheten av våre notater av det som kom frem i løpet av samtalen. Avslutningsvis fikk intervjuobjektet anledning til å tilføye det han/hun eventuelle selv ønsket.

### 5.3.4 Intervjuguide

Intervjuguiden skal som nevnt inneholde en oversikt over de emnene/spørsmålene som skal tas opp i intervjuet og hvilken rekkefølge de skal ha. Dette utarbeides på bakgrunn av intervjuobjektets fagfelt og ekspertise og nedenfor er temaer/spørsmål definert i henhold til hvilke utvalgskriterier som er benyttet ved valg av den aktuelle informanten. Det er utarbeidet utdypende intervjuspørsmål på bakgrunn av forskningsspørsmålene, og disse vil bli valgt og benyttet ved hvert enkelt intervju. I kapittel 5.4 og 6.4 gis det en beskrivelse av utarbeidelsen av prosjektets to intervjuguider. Gjennomgående i kapittel 6 blir spørsmålene i intervjuguidene gjengitt med tilhørende fortettet, kategoriserte og analyserte resultater.

### 5.3.5 Analyse av transkribert intervju

Informantens svar og meninger ble notert fortløpende mens intervjuet pågikk. Det transkriberte materialet ble som nevnt verifisert med intervjuobjektet og benyttet for videre analyse. Analysen startet allerede i planleggingen av intervjuet slik at prosessen kunne foregå allerede mens intervjuet pågikk. Ved analyse av intervjudata ligger nøkkelen i å spørre seg hva det er en vil finne ut i intervjuet og hvorfor for å kunne vurdere hvordan (metode) en skal gjøre det (Kvale 1997).

Valg av analysemetode er noe man gjør i forkant av intervjuet, ikke etterpå, slik at store deler av analysen foregår mens intervjuet pågår. Dette har flere fordeler.

Først og fremst vil det frembringe et nivå av saklighet i intervjuet, som er spisset mot det opprinnelige målet en har med intervjuet. Som nevnt er valg av metode basert på at en spør seg, hva en ønsker å finne ut av og hvorfor. En grundig vurdering av valg av metode i forkant sikrer sakligheten samt, minimerer ”overhead” som må sorteres ut i etterkant. Dersom en utfører mange intervjuer kan mengden data bli enormt stor og dermed mer eller mindre verdiløs for analyse innenfor de tidsrammene en er underlagt.

Det finnes ingen standardmetode som er best i et hvert tilfelle, for å komme frem til dypere meninger og implikasjoner ved et intervju. Imidlertid finnes det referanser til standardteknikker for analyse av kvantitativ data i litteraturen (Kvale 1997).

Med bakgrunn i Kvales (1997) anbefalinger til slik analyse er tre metoder i all hovedsak valgt. Første steg i analysen var en meningsfortetting, der en søker å finne essensen i personens meninger til kortere formuleringer som gjengis med få ord. Videre ble referatene fra de ulike intervjuene sammenfattet og kategorisert der det lot seg gjøre. Denne meningskategoriseringen ble utført i etterkant av intervjurundene der det ble identifisert hvilke kategorier svarene falt inn under. Dette gjør at det på en visuell og strukturert måte kan vurderes hvordan ulike aspekter vektlegges blant intervjuobjektene. Dette gjør at store datamengder kunne sammenfattes og gjorde det mulig å teste resultatene mot hypotesene definert i prosjektet. Videre ble det utført en ad hoc basert analyse, slik at det kunne foretas en dypere tolkning av enkelte av uttalelsene, og se sammenhenger og strukturer (Kvale 1997).

## 5.4 Beskrivelse av første intervjuguide

Intervjuguiden vises i sin helhet i vedlegg 2. I dette kapittelet blir prosessen med utarbeidelse av intervjuguiden presentert, samt en beskrivelse av knytningen mellom intervjuspørsmål og faktiske forskingsspørsmål. Beskrivelsen vil, slik vi ser det, forenkle evalueringsprosessen av kvaliteten på arbeidet da det vil belyse graden av troverdighet og bekreftbarheten til arbeidsprosessen. I tillegg økes sannsynligheten for at vi i større grad kan identifisere svakheter i prosessen og uønskede variabler som kan ha påvirket resultatet. Vi kunne da ta hensyn til dette i analyser og konklusjoner, og enklere kontrollere ulike variabler.

Intervjuene var som kjent semi-strukturerte og hadde en åpen form. Det var viktig at intervjuet, i så stor grad det lot seg gjøre, ikke inneholdt ledende spørsmål. Vi valgte derfor å begynne med så åpne spørsmål som mulig. Det antas at troverdigheten til hypotesene øker jo mer åpne spørsmål man kan stille, og allikevel få informasjon som kan indikerer deres gyldighet.

I lys av argumentasjonen over, valgte vi og innlede intervjuet med et åpent spørsmål rundt hvilke utfordringer informanten ser ved å oppnå en effektiv beskyttelse av informasjonssystemer, ut i fra dagens situasjon. Skulle kunnskapsfordelingen og reaktivitet komme frem ville det i det minste indikere at miljøet har anerkjent problemstillingen. Samtidig åpnet spørsmålet for informasjon om andre relevante og mulige sammenfallende temaer. Det ble valgt å dele dette i to innledende spørsmål for ikke å begrense informantens svaralternativ innledningsvis. Oppfølgningsspørsmål ble ut i fra informantenes svar formulert fortløpende. Vi valgte derfor ikke å formulere generiske oppfølgingsspørsmål forut for intervjuene. De to innledende spørsmålene ble formulert slik:

1. Hva anser du som de/den største utfordring(ene) ved effektiv beskyttelse av forsvarets informasjonssystemer?

2. Om man skulle endre noe ved dagens innfallsvinkel arbeidsmetode/strategi, hva mener man burde prioritere?

Spørsmål 1 ble ansett som åpent og ikke begrensende ut i fra hvilke utfordringer informanten ønsker å dele og legge vekt på. Formuleringen ble valgt for ikke å være ledende ovenfor informanten. Spørsmål 2 anses som mer begrensende, siden det retter seg mer mot helhetlig strategi og arbeidsmetoder. I tillegg ligger den en indirekte oppfordring i å dele informasjon om hva informanten anser som utfordringer med dagens strategi, ved å belyse hva som først burde endres.

3. I hvilken grad syntes du at dagens beskyttelsestiltak er tilpasset et gjeldende trusselbilde?

Spørsmål 3 skal belyse om informanten, i sitt arbeide, er bevisst et trusselbilde. Samtidig indikerer det om informanten ser sammenhenger med sine arbeidesoppgaver opp i mot en trussel og/eller trusselaktør. Et svar vil samtidig kunne indikere i hvilken grad informantene mener beskyttelsestiltakene evalueres opp mot et trusselbilde eller ikke. Det ble lagt opp til at informanten kunne ty til en bred

definisjon av trusselbilde. Informanten fikk beskjed om dette ved behov. Dette fordi begrepet fort kan oppfattes som begrensende.

4. Hvilke informasjonskilder benyttes for å danne trusselbilde og prioritere tilgjengelige ressurser?

Vi formulerte spørsmål 4 for å samle data rundt hvordan man danner seg et trusselbilde. Opplysninger rundt dette anses som meget interessant opp i mot vårt løsningsforslag. Det vil i første omgang kunne gi direkte informasjon om hvordan man danner seg et trusselbilde, og i hvilken grad dette faktisk gjøres. Med bakgrunn i ønsket om at informanten kunne benytte en bred definisjon på trusselbildet, ble det ved behov også opplyst om dette her. Et eksempel kan være at informanten kunne betrakte et virus som en trussel. Vi antar at om en slik type tilleggsinformasjon er nødvendig vil dette i seg selv indikerer at man i liten grad konsentrerer seg om den målrettede motstanderen. Følgelig kan det argumenteres, også her, for reaktive arbeidsmetoder. Likefullt vil et svar kunne gi opplysninger om man faktisk benytter informasjonskilder innad i organisasjonen. Eksempelvis da trender eller opplysninger avledet av innrapporterte sikkerhetshendelser fra organisasjonen. Samtidig vil svaret også indikere om man faktisk endrer prioriteringen av tilgjengelige ressurser på bakgrunn av en hendelse eller endring i omgivelsene man ønsker å kontrollere.

5. Hvilke fordeler mener du man har når man skal ”forsvare” kontra ”angripe” et informasjonssystem?
    a. Hva med angrep kontra forsvar?

Det ble utarbeidet en rekke ulike formuleringer av spørsmål 5. Formålet med dette spørsmålet var fortrinnsvis å identifisere i hvilken grad informanten mener at den ene parten stiller med et konkurransefortrinn. Opplysninger her vil i så måte direkte kunne indikere gyldigheten av hypotese 1. Formuleringen av spørsmål 5 ble valgt siden det direkte kunne gi informasjon om hva som anses som fordelene i ved å være i de ulike posisjonene. Samtidig vil formuleringen kunne fungere som et kontrollspørsmål mot tidligere delt informasjon. Dette er på bakgrunn av at spørsmålets formulering kan oppfattes som at vi ønsker å bekrefte at det er klare fordeler ved å være i forsvar. Grunnet litt uenighet om formuleringen ville føre frem, ble det utarbeidet et oppfølgningsspørsmål som går direkte på dette.

6. Hvem av partene har, etter din mening, størst sannsynlighet for å lykkes? En angriper eller en forsvarer av et informasjonssystem?

Spørsmålene har i frem til dette punktet i mer eller mindre grad konsentrert seg om parten som er i forsvar (om oss selv i lys av kategorien vi intervjuer). De forsøker å samle relevant data om hvordan en CND avdeling opererer. Problemstillingen i prosjektet retter seg inn mot den måltrettede og avanserte motstander, informasjon om hvordan en eventuell motstander av denne typen oppfattes er derfor meget interessant. Spørsmålene har heller ikke, slik de er formulert, ledet informanten i retning av den type motstander, da dette ikke er nevnt i spørsmålsformuleringene. Opplysninger som har kommet frem til dette punktet i intervjuene, kan indikere at informanten i stor grad anser denne type motstander som en stor utfordring og trussel, og kan sannsynliggjøre vår problemstilling.

7. I hvilken grad tror du motstanderen samler informasjon om oss, og kartlegger våre beskyttelsestiltak?

Spørsmål 7 er i mye større grad enn tidligere spørsmål direkte rettet mot å samle informasjon som kan indikere gyldigheten av hypotese 1. og forskningsspørsmål 1.2. Det er sannsynlig at informasjon som kan indikere dette allerede er kommet frem i svar på tidligere spørsmål. Spørsmål 7 gir også mulighet for innsamling av data som kan indikere at en målrettet og avansert motstander faktisk eksisterer. Samtidig er det et strategisk spørsmål som vil lede samtalen inn mot emnet.

8. Hvilke metoder og kilder tror du motstanderen benytter for å samle informasjon om oss?

I problemstillingen argumenteres det for at angriperen i stor grad kan benytte legitime og åpne kilder for og identifisere våre beskyttelsestiltak, samt tilpasser sine angrep ut i fra dette. Spørsmål 8 skal samle data rundt informantenes syn på hvordan angriperen opererer. Grunnet prosjektets perspektiv er det essensielt å samle data rundt angriperens strategi og metoder. Hvis informanten selv ikke kommer inn på temaet, vil spørsmål 9 bli benyttet. Spørsmålet er formulert nettopp for å samle data rundt fiendens strategier og arbeidsmetoder.

9. Hvilke angrepsstrategier blir benyttet av fienden?
    a. Er det mulig at fienden tilpasser sine angrepsmetoder ut i fra hvilke beskyttelsestiltak vi har gjennomført?

Spørsmålene som til nå er beskrevet er kapable til å holde samtalen innenfor formålstjenelige rammer. Spørsmålene er formulert med tanke på at de ikke skal være ledende i for stor grad, men samtidig være på en slik måte at vi forventet svar som var nyttige for prosjektets vinkling. Sammen med annen litteratur mener vi at spørsmålene skulle kunne samle data som kan benyttes til å indikere eller motbevise gyldigheten til hypotese 1 med forskningsspørsmål. I tillegg anser vi det som sannsynlig at analysen av data fra disse spørsmålene også kan benyttes i arbeidet med resterende forskningsspørsmål. Dette er på bakgrunn av spørsmålenes relative åpne form. Dette vil tilsi at det er sannsynlig at informantene uttaler informasjon som er nyttige utover det enkelte spørsmål. Resterende del av intervjuet ønsket vi å benytte til å samle data rundt hvilke type informasjon informantene anser som bidragsytende i forhold til å øke sitt eget og avdelingenes bevissthetsnivå. Spørsmål 10 og 11 går direkte inn på dette.

10. Hvilke kunnskap/ informasjon mener du er viktig å kunne tilegne seg for å utøve et effektivt forsvar av et informasjonssystem?

11. Hvilke informasjon/kunnskap tror du øker din egen årvåkenhet og situasjonsbevissthet? (primært i for å kunne detektere, forsvare/avverge et angrep)
    a. Hva med avdelingens årvåkenhet?

Prosjektarbeidets strategiske innfallsvinkel er i stor grad basert på at man gjennom økt fiendeforståelse kan muliggjøre et kostnadseffektivt forsvar av egne informasjonssystemer. Spørsmål 12 i intervjuguiden ble benyttet om informanten ikke har utpekt kunnskapen om fienden som relevant for egen og avdelingens bevissthet.

12. Anser du din kunnskap om fienden(angriperen) som viktig?
    a. Hvorfor/hvorfor ikke

Intervjuguidens siste spørsmål har en helhetlig formulering rundt hvilke type informasjon som må foreligge og som muliggjøre realiseringen en dynamisk og tilpasningsdyktig CND avdeling. Spørsmålet har fire oppfølgningsspørsmål som vil benyttes ved behov. De vil sammen forsøke å samle relevant data som kan benyttes som utgangspunkt for videre arbeid, da spesielt med forskningsspørsmål 2.2, 3.1, 3.2 og 4.2.

13. Hva slags informasjon må til for å skape en organisasjon som kan tilpasse sitt cyberforsvar (CND) mot en dynamisk trussel/trusselbilde?
    a. (Hvilke informasjon kan gi oss et oppdatert og korrekt trusselbilde?)
    b. Tas det hensyn til innrapporterte hendelser ved fordeling av ressurser?
    c. I hvilken grad mener du slik informasjon kan bidra til økt kunnskap om fienden.
    d. Hva tror du ville være de viktigste egenskaper ved denne informasjon (Tid, kvalitet, hvem, hva hvor, resultat, m.m.)?

**Kapittelets resultater:**

- Prosjektet baseres på kvalitative forskningsintervjuer og litteraturstudier
- Anbefalinger angående metodikk er beskrevet og vurdert i gjeldende kontekst
- Intervjuguide er utarbeidet og begrunnet
- Danner grunnlaget for den videre forskningen i prosjektet

# 6 Forskningsresultater og analyse

**Kapittelets innhold:**

- Dokumentasjon av forskningsintervjuenes forløp og resultater
- Fortløpende analyse av intervjuresultater
- Beskrivelse av resultatenes relevans og sannsynliggjøring av forskningshypoteser
- Erfaringer fra intervjuer som danner grunnlaget for videreutvikling av metodebruk
- Analyse (P`HAPI)

## 6.1 Innledende intervjurunde

En meningsfortetting og meningskategorisering av intervjuresultatene er foretatt og gjengitt nedenfor. Kategorisering av svarene er foretatt i de tilfellene prosjektgruppen har ansett at det lar seg gjøre. Det betyr at noen av spørsmålene er av slik art at svarene ikke egner seg for kategorisering og svarene er derfor kun gjengitt i forkortet form. Basert på den kvalitative fremgangsmetoden som er valgt er det ikke lagt vekt på kvantitative størrelser for å beskrive resultatene. Det er derimot heller valgt å gjengi svar som i hovedsak sier det samme flere ganger innunder hver kategori. Det er i vedelegg 3 gjengitt svarene slik de ble fremsatt av informantene, med en muntlig fremstilling på svarene for å fange svaret i størst mulig grad slik det fremkom. I dette kapittelet er svarene sammenfattet og analysert. Informantene bestod av eksperter med ulikt fagfelt slik at det fantes en viss divergens i hvilken grad vi fikk svar på alle spørsmål, eller kun deler av dem. Derfor er det ulikhet i mengden svar som er innhentet under hvert spørsmål. Intervjuguiden for den innledende runden bestod av spørsmålene under med påfølgende svar.

Det er som videre analyse foretatt en ytterligere tolkning av resultatene, spesielt med tanke på å trekke fram og belyse aspekter som er relevante for hensikten med det enkelte intervjuspørsmål og prosjektet som helhet. Dette vil innebære som det er henvist til tidligere en form for *ad hoc* tolkning av resultatene, der det kan foretas en dypere tolkning av enkelte av uttalelsene, og se sammenhenger og strukturer (Kvale 1997).

1. ***Hva anser du som de/den største utfordring(ene) ved effektiv beskyttelse av forsvarets informasjonssystemer?***

    a. **Organisasjonsmessige og menneskelige faktorer**

    Det er en gjennomgående oppfatning blant informantene at det generelle kunnskapsnivå i organisasjonen er en stor utfordring. Det fremstilles at dette medfører mange brukerfeil med dertil

sikkerhetsbrudd. Dette begrunnes med at manglende opplæring gir et fravær av påkrevet forståelse for informasjonssikkerhetens betydning og viktighet for organisasjonen. Videre legges det vekt på et fravær av tilstrekkelig støtte og forankring for å utføre et effektivt informasjonssikkerhetsarbeid i organisasjonen. Dette sammenfaller med det generelle kunnskapsnivået, men medfører det informantene beskriver som utilstrekkelig ressurstildeling og myndighet til å oppnå god informasjonssikkerhet. På denne måten gjør kunnskapsnivået at informasjonssikkerhetstiltak ikke gis tilstrekkelig prioritet.

**b. Trusselen i seg selv**

Trusselbildets egenskaper trekkes fram som en avgjørende utfordring. Et komplekst og uoversiktlig trusselbilde gjør det vanskelig å skille ut målrettede trusselaktører.

**c. Lovgivning**

Det påpekes at den lovgivning og de formelle prosedyrer en er underlagt i sikkerhetsarbeidet, legger begrensninger på effektiviteten. Det beskrives at dette gjør seg spesielt gjeldende ved en kontinuerlig tilpasning av egne tiltak. Formelle prosedyrer forsinker prosessen med tilpasning, da endringer krever en langvarig godkjenning. Dette beskrives som en selvpålagt sårbarhet. Videre påpekes det at lovgivningen, spesielt et sterkt personvern, gjør identifikasjon og straffeforfølging av fiender vanskelig.

**d. Reaktive beskyttelsestiltak**

Informantene beskriver at informasjonssikkerhetsarbeidet er basert på et handlingsmønster som er reaktivt. Enkelte informanter utrykker at tiltakene som benyttes utlukkende er reaktive. Tiltak iverksettes etter en hendelse har inntruffet. Denne reaktiviteten forsterkes av treghet i sikkerhetsgodkjenningsregimet, da tilpasninger av beskyttelsen tar lang tid.

**e. Teknisk/Systemkonfigurasjon**

Det ble til dels lagt vekt på manglende tekniske virkemidler og investeringer som en avgjørende utfordring. Dette utspeiler seg ved at det i visse tilfeller ikke finnes mulighet for deteksjon og sporbarhet i systemene.

**Analyse:** Som det fremgår av resultatene er det stor variasjon i hva de ulike ser på som de største utfordringene. Uten å lede intervjuobjektene inn på de faktorene som er relevante for vår problemstilling ble en rekke interessante synspunkter registrert. Med bakgrunn i vår hensikt med spørsmålet er det interessant å registrere at utfordringer med et reaktivt handlingsmønster utheves ved flere intervjuer. I tillegg ble det trukket fram faktorer som ble beskrevet å forsterke dette handlingsmønsteret, eksempelvis ved at formelle prosedyrer forsinker prosessen med å være tilpasset et gjeldende trusselbilde. En annen interessant problemstilling som fremkom var utfordringene med å identifisere den målrettede trusselen og klare å skille denne

trusselen fra den generelle mengden av støy på nettverket. Disse uttalelsene bidrar dermed til å sannsynliggjøre hypotese 1, som lyder:

*Hypotese 1:* *Det er sannsynlig at dagens strategi for beskyttelse mot cybertrusselen, gir den avanserte/intelligente motstanderen store konkurransefortrinn.*

Videre er det tilnærmet gjennomgående at intervjuobjektene belyser menneskelige aspekter som en stor utfordring. Opplæring, kunnskap og forståelse blir omtalt og bidrar til å bekrefte grunnlaget for prosjektets hypotese om at IS-bevissthetsbygging er et relevant forbedringspotensial i organisasjonen.

2. ***Om man skulle endre noe ved dagens innfallsvinkel arbeidsmetode/strategi, hva mener man burde prioritere?***

    a. **Menneskelige faktorer**
    Et gjennomgående tema blant informantene er økning av det generelle kunnskapsnivået i organisasjonen. Det beskrives et behov for opplæring for å øke denne kunnskapen, forståelsen og holdningene blant de ansatte. I tillegg blir det trukket fram at sikkerhetskonseptet må forankres hos ledelse og samarbeidende parter. Videre påpekes viktigheten av å øke forståelsen for det operative behovet blant sikkerhetspersonell, slik at sikkerhetsarbeidet understøtter organisasjonenes overordnede mål.

    b. **Tekniske midler**
    Enkelte anbefaler å innføre ytterligere tekniske virkemidler som umyndiggjør brukeren slik at mulighetene for brukerfeil reduseres, samt tekniske muligheter for deteksjon og sporbarhet. På den annen side poengteres det i større grad at tekniske virkemidler tilbyr en falsk trygghet.

    c. **Lovgivning/regelverk**
    Et gjennomgående tema blant informantene omhandler tilgjengeliggjøring og tilpasning av lovverk og formelle prosedyrer. Det påpekes at dette må gjøres smidigere og tilpasses mot et mål om økt sikkerhet. Det beskrives at dette er med bakgrunn i at sikkerhetsarbeidet bør ha et mål om økt sikkerhet, ikke kun å etterleve regelverket. På denne måten blir regler og prosedyrer en sikkerhetstrussel i seg selv. Spesielt påpekes et rigid regime basert på sikkerhetsgodkjenning og gradering av informasjonssystemer.

    d. **Reaktivitet**
    Det omtales at en mer helhetlig tilnærming til deteksjon og reaksjon kan gjøre organisasjonen proaktiv i større grad.

**Analyse:** Intervjuspørsmålet anses som en oppfølging til spørsmål 1. Som det fremkommer av svarene er det i hovedsak de samme momentene som belyses.

Et interessant moment er at det reaktive handlingsmønsteret som fremkom som en utfordring i spørsmål 1, virker å være betydelig mindre omtalt når innfallsvinkelen er å foreslå en endring. Med tanke på det reaktive handlingsmønsteret finner vi kun forslag til indirekte forbedringer av faktorer som bidrar til et reaktivt handlingsmønster. Økt smidighet i formelle prosedyrer, tilpasning av regelverk, ytterligere implementering av tekniske løsninger etc. Selv om den reaktive problemstillingen anerkjennes i spørsmål 1 (ut i fra svarene), ønsker man i stor grad å forbedre dagens situasjon med de samme tradisjonelle reaktive metodene. Problemstillingen krever en utradisjonell løsning, da det nettopp er de tradisjonelle metodene som medfører problemstillingen. Dette underbygger behovet for andre innfallsvinkler og at man i større grad tenker utenfor boksen. Prosjektetgruppen ønsker som kjent å bidra til dette.

Som det fremkommer av analysen i spørsmål 1, finner vi også her en trend i at intervjuobjektene trekker fram menneskelig aspekter som viktig. Opplæring, kunnskap, holdingsendringer og bevissthetsbygging omtales, og er således svært interessant med tanke på prosjektets innfallsvinkel. Det er også viktig å legge merke at det er et ønske om å øke sikkerhetsfolkets forståelse av det operative behovet. Dette er momenter som vektlegges i det videre arbeidet, spesielt i utarbeidelsen av et løsningsforslag.

3. ***I hvilken grad er syntes du at dagens beskyttelsestiltak er tilpasset et gjeldende trusselbilde?***

    a. ***Tilpasset:***
    Organisasjonen tilpasser sine tiltak, og det beskrives at dagens handlingsmønster oppdager og stanser langt på vei det meste av de hendelser en står ovenfor.

    b. ***Ikke tilpasset:***
    Uttalelsene som beskriver hvordan organisasjonen ikke er tilpasset føyer seg hovedsakelig inn i to kategorier. Det første er hvordan organisasjonen prioriterer informasjonssikkerhetsarbeidet. Det beskrives at de ikke er tilpasset gjennom utilstrekkelig støtte, naive holdninger, manglende investeringer etc. Det andre som vektlegges er handlingsmønsteret til de tiltakene som er iverksatt. De omtales som reaktive, og det er lite prioritet på tiltak som kan detektere og hindre en målrettet trussel. Trusselbildet er dynamisk, mens sikkerhetstiltakene kommer som et resultat av erfaring og blir lagt til i etterkant.

**Analyse:** Blant de svarene som omhandler utfordringer/mangler ved hvordan beskyttelsen er tilpasset, fremkommer det momenter som bidrar til å bekrefte våre hypoteser. Spesielt trekkes reaktivitet og erfaringsbasert beskyttelse frem her, hvilket styrker tiltroen til hypotese 1. Det bekreftes at det finnes en målrettet trussel en er dårlig forberedt på å møte, der utfordringen ligger i å skille denne trusselen ut fra den totale mengden. Det beskrives et reaktivt

handlingsmønster som ikke er i stand til å håndtere et dynamisk trusselbilde. Svarene sannsynliggjør også at man i dag kun konsentrerer seg om å oppfylle et minimum av sikkerhet, styrt av erfaring og lovgivning.

4. ***Hvilke informasjonskilder benyttes for å danne trusselbilde og prioritere tilgjengelige ressurser?***

    a. **Åpne kilder**

    Det er en gjennomgående oppfatning at en svært viktig kilde for å tilegne seg slik informasjon finnes i åpne kilder. Det beskrives at informasjonen kommer fra ulike sikkerhetsselskaper som publiserer signaturer, til sine kunder eller åpent på internett. I tillegg trekkes andre ikke-komersielle kilder fram som for eksempel sikkerhets-communities etc. Det nevnes også at de åpne kildene ofte er på etterskudd og bruker for lang tid på å være oppdaterte.

    b. **Samarbeidspartnere**

    Det beskrives at informasjon innhentes fra ulike samarbeidspartnere. Informantene nevner ulike statelige og private organisasjoner både nasjonalt og internasjonalt. Imidlertid nevnes det at informasjonsdelingen innad i Forsvaret pågår i begrenset grad.

    c. **Egne observasjoner**

    Observasjoner og overvåkning av egne systemer nevnes som kilder til viktig informasjon for å danne seg et trusselbilde. Egne sensorer reagerer på hendelser.

**Analyse:** Intervjuobjektene gir en generell oversikt over hvilke kilder informasjonen kan komme fra. Uten ledende spørsmål finnes det relativt begrenset informasjon blant svarene som kan bidra til å sannsynliggjøre våre hypoteser, annet enn at det foreligger en innsamling av informasjon for å danne seg et bilde av fienden. Et svært interessant aspekt er at det generelt nevnes lite angående informasjonsflyt mellom avdelinger innad i egen organisasjon, og at det sågar beskrives at slik informasjonsflyt foregår i liten grad. En tolkning kan derfor være at det eksistere et forbedringspotensial her.

5. ***Hvilke fordeler mener du man har når man skal "forsvare" kontra "angripe" et informasjonssystem?***

    a. **Fordeler med forsvar**

        i. **Kunnskap om eget system**

        Fordelen ved å kjenne seg selv og sitt eget system trekkes frem. En vil i utgangspunktet ha store muligheter for å være bevisst sine egne styrker og svakheter og kan prioritere sitt informasjonssikkerhetsarbeid deretter. Det beskrives at en målrettet aktør ofte vil gjennomføre rekognosering og kartlegging i forkant av et angrep. Denne aktiviteten kan være en indikator og således en fordel for forsvareren.

**ii. Læring om fienden**

Informantene beskriver at fiendens aktivitet kan benyttes til fordel for forsvareren. Fiendtlig aktivitet kan detekteres og overvåkes. Deretter kan det vurderes om den potensielle skaden angrepet kan medføre gjør at det skal stoppes, eller om en skal fortsette å overvåke og lære om fienden. Således vurderer flere av informantene det slik at om det finnes fordeler eller ikke med å være i forsvar avhenger av forsvarerens evne til deteksjon og læring.

**b. Utfordringer med forsvar/fordeler med angrep**

**i. Kunnskapsunderlegenhet**

En generell kunnskapsunderlegenhet beskrives av informantene. Angriperen sitter med initiativet og kan selv velge fritt hvordan han går fram. Hvilke metoder som skal benyttes, hva som er målet, motivasjonen, når angrepet gjennomføres osv.

**ii. Angrepsvektorer/kompleksitet**

Det generelle problemet med den høye kompleksiteten i systemene omtales som et problem for forsvareren. I angrep trenger du bare finne en feil, mens forsvareren må finne alle. I tillegg kan et avansert og målrettet angrep gjemme seg i en enorm mengde av trafikk som gjør det vanskelig å skille ut et reelt angrep.

**iii. Tilpasning til situasjon og beskyttelsestiltak**

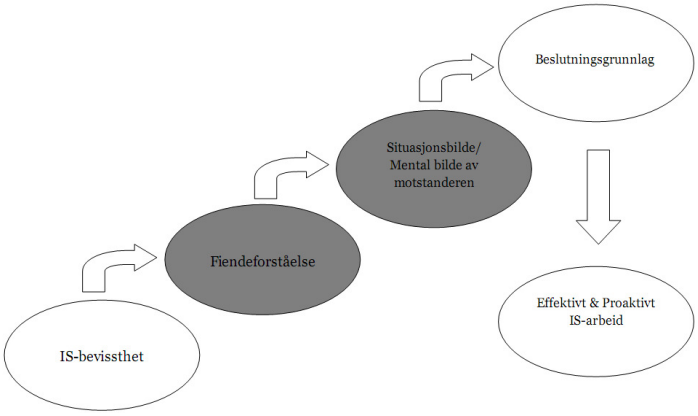
Angriperen har initiativet og kan kontinuerlig tilpasse seg den til enhver tid gjeldende situasjon. Det er kjent hvilke beskyttelsestiltak som er gjeldende og angrep kan tilpasses deretter. Den kartleggingen som foregår er i seg selv en indikasjon som sannsynliggjør at angriperen tilpasser seg våre beskyttelsestiltak. Erfaringsbasert forsvar er i seg selv et stort problem. Den reaktive måten å beskytte seg på er i seg selv på bakgrunn av at angriperne tilpasser seg. Et interessant aspekt som trekkes fram er angriperens motivasjon. Mens den som beskytter et system er underlagt mange andre motiver for sin drift, støtte organisasjonens generelle mål, om økonomisk vinning, støtte liv og helse, følge lover og regler etc. Mens en angriper kanskje kun har et mål, eks økonomisk vinning. Dette gjør at den forsvarende part har ytterligere mål og begrensninger for sine operasjoner som angriperen ikke behøver å ta hensyn til.

**Analyse:** Blant svarene finnes informasjon som kan bidra til å sannsynliggjøre påstander i prosjektet. Det belyses at den forsvarende part må finne og beskytte alle angrepsvektorer, mens angriperen kun trenger å finne en for å utføre sitt angrep. Det finnes svar som underbygger at kompleksiteten i systemene gjør at en metode basert på å tette identifiserte sikkerhetshull, er svært vanskelig. Dette øker tiltroen til hypotese 1. Angriperen kan, ved hjelp av rekognosering og kartlegging, lære om våre

beskyttelsestiltak og tilpasse sitt angrep deretter. Et interessant aspekt som fremkommer er at det virker å være en utbredt forståelse av at i egenskap av å være en målrettet aktør vil trusselen operere med en omfattende rekognosering og kartlegging i forkant av et angrep. Dette momentet må sees i sammenheng med spørsmål 6. Informantene viser til to fordeler man har som forsvarer av et informasjonssystem, lære om fienden og kjenne seg selv. Opplysningene indikerer gyldighet i prosjektets hypoteser, spesielt hypotese 2, da informantene faktisk her indirekte erkjenner at kunnskap om fienden er viktig for å kunne beskytte egne systemer. Hypotese 2 sier:

*Hypotese 2:* *Det er sannsynlig at en strategi basert på økt fiendeforståelse kan endre dagens beskyttelsestankegang til en forsvarstankegang og gjøre sikkerhetsarbeidet proaktivt i større grad.*

Sett i forhold til illustrasjonen av prosjektets overordende arbeidshypotese indikerer disse funnene sammenhengen mellom fiendeforståelse og situasjonsbilde/mentalt bilde av motstanderen. Se figur 3.




Figur 3. Prosjektarbeidets overordnede arbeidshypotese versjon 3

Dette sammen med at kunnskap om seg selv, anses også som en viktig faktor underbygger vår tiltro til at en innfallsvinkel der man ved å øke IS-bevisstheten kan være en mulig løsning. Et skreddersydd bevissthetsprogram vil nettopp kunne bidra til å øke kunnskapen om seg selv. Samtidig som det kan tilrettelegge for at de ansatte blir en trussel og hendelsesdetektor/sensor, som sannsynligvis vil kunne gi nyttig informasjon om fienden.

### 6. *I hvilken grad tror du motstanderen samler informasjon om oss, og kartlegger våre beskyttelsestiltak?*

Det er en gjennomgående holdning og forståelse blant informantene at egne systemer er utsatt for kartlegging og rekognosering med tanke på beskyttelsestiltak.

**a. Rekognosering**
Det beskrives at trusselaktører samler informasjon om systemet gjennom innsamling av all den informasjon som ligger åpent, for senere å starte rekognosering/kartlegging over nettverket og/eller via andre kilder som for eksempel social engineering. Det er en holdning blant informantene at slik aktivitet i hovedsak kommer fra målrettede aktører.

b. **Reaktiv beskyttelse**
Det kommer frem at den reaktive beskyttelsen gir en klar fordel for angriperen. Nettopp fordi det aldri finnes en kur før viruset har vært iverksatt. Erfaringsbasert forsvar er i seg selv et stort problem. Den reaktive måten å beskytte seg på er i seg selv en konsekvens av at motstanderen tilpasser seg allerede implementerte sikkerhetstiltak.

**Analyse:** Resultatet bekrefter langt på vei at personellet oppfatter at det foreligger indikasjoner på at motstanderen utfører rekognosering og kartlegging for å innhente informasjon om oss og våre systemer. Det belyses at dette er spesielt gjeldende med tanke på en målrettet aktør. På denne måten kan resultatet her kunne sannsynliggjøre påstandene i hypotese 1 generelt, og bidra til å besvare forskningsspørsmål 1.2 spesielt.

Forskingsspørsmål 1.2:

*Finnes det informasjon som indikerer eller motbeviser, at motstanderen tilpasser sine taktiske og tekniske prosedyrer til våre tiltak, og metoder for innhenting av trusselinformasjon?*

Det belyses i tillegg eksplisitt at det reaktive handlingsmønstret en benytter seg av, i prinsippet er på bakgrunn av at en står ovenfor en fiende som innhenter informasjon og tilpasser seg våre systemer og beskyttelsestiltak. Dette bidrar dermed til å besvare forskningsspørsmål 1.2.

***7. Hvilke metoder og kilder tror du motstanderen benytter for å samle informasjon om oss?***

**a. Åpne kilder**
Åpne kilder trekkes fram som en viktig kilde, både offisiell informasjon som gjøres tilgjengelig for alle, men også informasjon som utilsiktet deles av ansatte på for eksempel sosiale medier.

**b. Social engineering**
Det fremkommer fra informantene at det foregår målrettet informasjonsinnhenting direkte mot personell med kunnskap i organisasjonen. Dette kan være at man fysisk blir kontaktet av personer, eller at kontakten skjer på internett. Social engineering etc.

**c. Tekniske virkemidler**

Tekniske midler kan benyttes for å samle informasjon. Det utføres aktiviteter over nettverket som kun har til hensikt å samle informasjon om våre systemers konfigurasjon. Dette kan ofte være kamuflert som annen type trafikk.

**d. Kjøp og salg av informasjon**

Det beskrives at det finnes markeder for kjøp og salg av slik informasjon, og at dette dermed kan være en kilde en trusselaktør kan benytte seg av.

**Analyse:** Intervjuobjektene gir en generell oversikt over hvilke kilder motstanderen kan benytte seg av for å samle informasjon om oss. De belyser i hovedtrekk fire kategorier, hvor av en er tekniske virkemidler. Prosjektgruppen tolker dette til at informantene anerkjenner dette av en rekke andre kilder og mulige angrepsvektorer. Vi legger til grunn at det kun er innen den tekniske delen en CND- avdeling har som oppgave å detektere og hindre angrepsforsøk. Det er også her informantene tidligere har belyst at de kan lære om fienden og dens målsettinger m.m. Tidligere er det kommet frem at det er viktig å ha så mye kunnskap om fienden som mulig, når man skal forsvare et informasjonssystem. Samlet sett mener vi at dette er opplysninger man må vektlegge og reflektere over i arbeidet med et eventuelt løsningsforslag. Løsningsforslaget bør derfor muliggjøre en informasjonsinnsamling om fiendes aktiviteter i andre angrepsvektorer enn hva CND- avdelingen kontrollerer. Svarene viser igjen også at informanten mener angriperen samler informasjon om oss og våre beskyttelsestiltak, i den hensikt å tilpasse egne angrep basert på denne informasjonen.

***8. Hvilke angrepsstrategier blir benyttet av fienden?***

Generelt vises det til en strategi som baseres på en langvarig kartlegging/rekognosering i forkant av et raskt angrep.

***a. Er det mulig at fienden tilpasser sine angrepsmetoder ut i fra hvilke beskyttelsestiltak vi har gjennomført?***

Informantene beskriver en generell forståelse av at dette er tilfelle. Fienden benytter seg av de angrepsvektorene som er tilgjengelige til enhver tid, og benytter seg av kartlegging i forkant for å identifisere disse. Videre vises det til at denne fremgangsmåten er avhengig av at det finnes en viss målrettethet i angrepet. Derfor belyses det at med tanke på dette spørsmålet er det i stor grad avhengig av hvor sofistikert og målrettet den aktuelle fienden er. Videre vises det til ulike tekniske eksempler på slik tilpasning og det belyses at fiendens tilpasning i seg selv gir grunnlaget for den kontinuerlige og reaktive tilpasningen av beskyttelsestiltak.

**Analyse:** Spørsmålet ble i utgangspunkete tiltenkt stilt ved behov. Allikevel ble spørsmålet stilt til alle informantene. En gjennomgående trend blant svarene er at det forutsettes en målrettet aktør for at elementet av tilpassning gjør seg gjeldende. Det

beskrives en metodikk som innebærer langvarig kartlegging før et angrep iverksettes, som ofte er tilpasset teknologisk og strukturell oppbygning av systemer og beskyttelsestiltak. På denne måten kan resultatet her kunne sannsynliggjøre påstandene i hypotese 1 generelt, og bidra til å besvare forskningsspørsmål 1.2 spesielt. De sier følgende:

*Hypotese 1:* *Det er sannsynlig at dagens strategi for beskyttelse mot cybertrusselen, gir den avanserte/intelligente motstanderen store konkurransefortrinn.*

Forskningsspørsmål 1.2:

*Finnes det informasjon som indikerer eller motbeviser, at motstanderen tilpasser sine taktiske og tekniske prosedyrer til våre tiltak, og metoder for innhenting av trusselinformasjon?*

***9. Hvilke kunnskap/ informasjon mener du er viktig å kunne tilegne seg for å utøve et effektivt forsvar av et informasjonssystem?***

**a. Kunnskap om fienden/trusselbildet**

Kunnskap om trusselaktøren belyses som vital informasjon, hvem de er, hvilke kapasiteter de besitter, hva de er ute etter osv.

**b. Kompetanse/Utdanning**

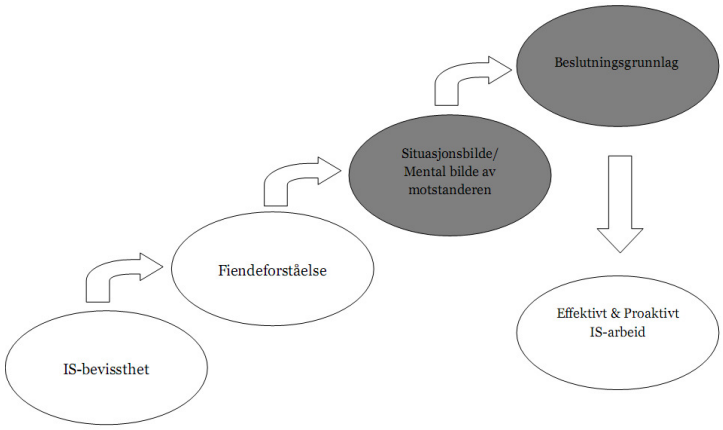
Det er en gjennomgående oppfatning blant informantene at den generelle tekniske kompetansen er viktig, i tillegg til sikkerhetskompetanse. Det vises til at dette er viktig for å kunne utnytte sine ressurser på en optimal måte. Videre belyses det at denne kompetansen er ferskvare, og at det derfor er viktig med en kontinuerlig oppdatering og heving av denne. Et interessant aspekt som ble belyst var å følge med på og tilegne seg kunnskap om sårbarhetsbildet, og at dette ofte var viktigere enn trusselbildet. Dette ble begrunnet med at det ofte ikke var så viktig hvor angrepet kom fra, men mer essensielt var det å være klar over sårbarheten og kunne detektere, eventuelt stanse, angrepet som utnyttet den.

**c. Kunnskap om seg selv/egne systemer**

Kunnskap og bevissthet om seg selv og egne systemer omtales som viktig. Opprettholde en bevissthet på egen teknologi og infrastruktur, egenskapene til den programvare man benytter osv.

**Analyse:** Det belyses flere aspekter som er ansett som viktige. Av relevans for prosjektet finnes det at kunnskap om trusselaktøren er viktig. Hvem er de ulike trusselaktører, hvilke kapasiteter besitter de og hva er deres motivasjon. Informantene beskriver dette og fiendebildet (situasjonsbildet) som vital informasjon når man skal utøve et effektivt forsvar av et informasjonssystem. Vi referer igjen til vår tankerekke,

og argumenterer for at funnene indikerer sammenhengen og viktigheten av at et korrekt og oppdatert situasjonsbilde/mentalt bilde av fienden og beslutningsgrunnlaget for prioriteringen av ressurser (se figur 4).




Figur 4. Prosjektarbeidets overordnede arbeidshypotese versjon 4

Videre blir det lagt vekt på egen generell sikkerhetskompetanse, og en kontinuerlig oppdatering av slik kunnskap/kompetanse, med bakgrunn i at dette feltet er i rask endring og utvikling. Således fremkommer det opplysninger som bidrar til å sannsynliggjøre hypotese 2 generelt, og forskningsspørsmål 2.2 spesielt som er formulert slik;

Forskningsspørsmål 2.2:

*Finnes det indikasjoner om at økt kunnskap om fienden kan gjøre oss bedre i stand til en dynamisk tilpasning av forsvarsressursene iht. endringer i trusselbildet?*

Et interessant synspunkt viser til at kunnskap om trusselaktøren er underordnet kunnskap om sårbarheter. Det hevdes å være uviktig hvem som står bak angrepet, mens det viktige er kun å reparere en sårbarhet som er kjent. Dette er således noe motstridende mot våre påstander, men kan tolkes å være et viktig element dersom en faktisk følger et reaktivt handlingsmønster, og kan dermed bekrefte en slik reaktivitet.

***10. Hvilke informasjon/kunnskap tror du øker din egen årvåkenhet og situasjonsbevissthet? (primært for å kunne detektere, forsvare/avverge et angrep)***

**a. Situasjonsbevissthet, kunnskap om fienden og informasjonsutveksling**

Evnen til å opprettholde en generell situasjonsforståelse omtales som viktig. Det å kunne holde seg oppdatert på hva som skjer av operative hendelser og i samfunnet for øvrig gjør en i stand til å forstå sammenhengen mellom fysiske og virtuelle hendelser, samt å forstå informasjonssikkerhetsarbeidets hensikt for organisasjonen.

Det vises til at det ligger store utfordringer i å få samlet all relevant informasjon på ett sted for å kunne oppnå denne bevisstheten. Med dette vises det til informasjonsflyt og rapportering fra organisasjonen som helhet, og dette omtales som svært viktig, i tillegg til at de som tar i mot denne informasjonen må være i stand til å behandle den og sette den i sammenheng. Videre vises det til at informasjon som omhandler trusselaktøren generelt øker egen situasjonsbevissthet. Det omhandler hvem trusselaktøren er, hvor han kommer fra, operasjonsmønster etc.

***b. Hva med avdelingens årvåkenhet?***

i. Informantene beskriver elementer innen samme kategorier som over, men i tillegg noe vekt på å etablere egne rutiner og prosedyrer som legger til rette for å øke en felles oppdatert situasjonsbevissthet og kunnskap om trusselbildet. Det beskrives med å etablere rutiner i egen avdeling som understøtter å oppnå en felles situasjonsbevissthet, briefinger om nye sårbarheter, ondsinnet kode, etc.

**Analyse:** Det trekkes fram at situasjonsbevissthet har en sterk sammenheng med operative hendelser og hva som ellers skjer i samfunnet. Informasjon som dette må settes i sammenheng for å danne seg en helhetlig bevissthet. Videre er det interessant at det trekkes fram viktigheten av at CND avdelingen kan tilegne seg informasjon fra den øvrige delen av organisasjonen, og at dette er en viktig kilde for danne seg et korrekt situasjonsbilde. Videre blir det trukket fram at interne kommunikasjonskanaler er viktige, som kan legge grunnlaget for en felles situasjonsbevissthet. I lys av dette kan det tolkes at svarene kan bidra til å sannsynliggjøre påstander fremsatt i prosjektet. Det indikeres at den øvrige organisasjonen besitter vital informasjon og at rutiner for å kommunisere denne informasjonen er viktige. Således bidrar svarene til å underbygge hypotese 3, som sier at man i større grad bør basere seg på en bevissthetsmodell som skal gi et bedre mentalt bilde av motstanderen.

***11. Anser du din kunnskap om fienden(angriperen) som viktig?***

**a. *Hvorfor/hvorfor ikke***

Det er en gjennomgående oppfatning at kunnskap om trusselaktøren er viktig for å lykkes, og det er interessant at det sies eksplisitt at dette er spesielt viktig i en situasjon der en ønsker å gjøre analyser, lære om fienden, kunne forutsi og hindre fremtidige angrep. Det vises til at morgendagens trusler er i stadig endring, og at en derfor må lage seg en kunnskapsbase over reelle aktører.

**Analyse:** I utgangspunktet var spørsmålet tenkt benyttet i de tilfeller informanten selv ikke belyste tema fiendeforståelse. Resultatet viser at de nesten alle informantene kom inn på tema som trussel og trusselaktør ved tidligere spørsmål. Vi valgte allikevel

å stille spørsmålet til alle informantene. Det kan legges til at en av informantene (hadde ikke vært inne på tema tidligere) begynte sitt svar med sitat "Ja, ledene spørsmål for øvrig" sitat slutt. En klar indikasjon vi må ta hensyn til i analysen. Samtidig må vi legge vekt på spørsmålets formål og ikke minst at de fleste informantene selv hadde belyst temaet. Trenden i svarene tilsier at kunnskap om fiende er et meget viktig element for å kunne øke egen og avdelingens bevissthet. Funnene indikerer at økt fiendeforståelse bidrar til å øke CND-avdelingens IS-bevissthet. Det kan derfor argumenteres for at en økt fiendeforståelse også bidrar til å øke IS-bevisstheten til de som skal forsvare informasjonssystemene. Det fremheves som spesielt viktig for å kunne forutsi og hinder fremtidige angrep. Hvilket er i overensstemmelse med vår innfallsvinkel. En informant viser også til at egne avdelinger kan bidra med denne type informasjon, sammen med andre sensorer. Igjen kommer det frem viktige momenter til arbeidet med prosjektets løsningsforslag.

12. ***Hva slags informasjon må til for å skape en organisasjon som kan tilpasse sitt cyber-forsvar (CND) mot en dynamisk trussel/trusselbilde?***

    a. ***Hvilke informasjon kan gi oss et oppdatert og korrekt trusselbilde?***

       Svarene som fremkom var av stor variasjon. Det omtales viktigheten av å være oppdatert på kjente trusler og sårbarheter slik at en beskyttet mot det som er allment kjent. Videre vises det til viktigheten av å tilegne seg kunnskap om trusselaktøren, innebefattet hvilke kunnskap fienden besitter. Med tanke på at trusselaktøren benytter åpne kilder for å tilegne seg informasjon er det viktig å være aktiv og tilegne seg denne kunnskapen selv. Det omtales at den informasjonen som må til for å holde personellet oppdatert på fagfeltet er viktig, samt evne til å sette denne kunnskapen i sammenheng med det øvrige som skjer i samfunnet og operasjonsmiljøet. Denne informasjonstilegnelsen er en kontinuerlig vedvarende prosess. Videre virker det å være en generell forståelse av at evnen til å skape forståelse og støtte for informasjonssikkerhetsarbeidet er viktig. Selv om dette mulig ikke direkte gir svar på spørsmålet om hva informasjonsbehovet, var dette et gjennomgående tema.

**Analyse:** Spørsmålets helhetlige formulering gir igjen en stor divergens i svarene. En mulig trend er at kunnskap og forståelse er nøkkelord som nevnes i flere sammenhenger. Utover dette medfører divergensen at det vanskelig kan trekkes andre konklusjoner ut fra svarene. Intensjonen med spørsmålet var å samle data rundt informasjonsbehovet, hvilket i liten grad blir belyst i svaret på første kontrollspørsmål.

***b. Tas det hensyn til innrapporterte hendelser ved fordeling av ressurser?***

Svarene på dette spørsmålet varierte i stor grad. Enkelte hadde en forståelse av at innrapporterte hendelser ble tatt hensyn til i stor grad, mens andre mente dette ble benyttet i liten grad og at det forligger et stort potensial i å benytte denne informasjonen. Det ble omtalt at rapporteringsrutinene ikke var gode nok, at den generelle bevisstheten og kunnskapen i organisasjonen ikke legger til rette for rapportering, rapportene ikke tilflyter det rette personellet osv.

**Analyse:** Enkelte av forskningsspørsmålene krever at vi til en viss grad samler informasjon om dagens status. I det minste er det behov for å identifisere et eventuelt potensial ved prosjektets innfallsvinkel. Oppfølgningsspørsmål 12.b har rot i dette behovet. Svarene indikerer at informantene mener det ligger nyttig informasjon i slike rapporter, og at det til en viss grad utnyttes i dag. Flere av svarene viser imidlertid at informantene mener det ligger et potensial i å utnytte denne informasjonen bedre. Svarene indikerer også at informantene mener denne informasjonen vil kunne bidra til en helhetlig situasjonsforståelse. Informasjonen må benyttes i sammen med eksisterende informasjon, til å danne et mer helhetlig og bedre beslutningsgrunnlag. Et annet viktig element som belyses er at informasjonen må tilfalle korrekte personer.

***c. I hvilken grad mener du slik informasjon kan bidra til økt kunnskap om fienden.***

Svarene viser en gjennomgående oppfatning av at rapporter om sikkerhetshendelser kan bidra til økt fiendeforståelse. Det omtales blant annet som den beste måten å kunne oppnå denne kunnskapen, og korrelere hendelser og vise trender, for å oppnå en mer proaktiv tilnærming.

**Analyse:** Informantene mener helt klart at denne type informasjon er viktig for det totale bildet. Det kan utnyttes i større grad, og at denne type informasjon og kan medføre en mer proaktiv tilnærming.

***d. Hva tror du ville være de viktigste egenskaper ved denne informasjon (Tid, kvalitet, hvem, hva, hvor, resultat, mm)?***

***i.* Rutiner og egen reaksjon**

Svarene som faller under denne kategorien beskriver ikke kun egenskaper ved selve informasjonen, men også egenskaper ved egen organisasjon som beskrives som viktige. Dette omhandler i hovedsak egne rutiner angående hvordan informasjonen behandles, samt forståelse og støtte fra ledelsen. I tillegg omtales viktigheten av å gi tilbakemeldinger på de innrapporterte hendelsene. Videre er det beskrevet at tilleggsinformasjon om hendelsen er viktig, eksempelvis hvilke tiltak er gjort og hvilke erfaringer som kan trekkes av hendelsen.

***ii.*** **Trusselinformasjon**

Det ble beskrevet at informasjon om hvem som står bak angrepet er viktig dersom denne informasjonen foreligger. I tillegg sies det at det er viktig at trusselinformasjonen er så korrekt og tidsriktig som mulig.

***iii.*** **Korrekt informasjon om hendelsen**

Informasjon som er knyttet til selve hendelsen er sammenfattet i denne kategorien. Det ytres at det i visse tilfeller kan være viktig med rask rapportering og behandling av informasjonen. Videre beskrives det at detaljnivået angående hendelsen kan være viktig, spesielt med tanke på å kunne se sammenhenger og korrelere informasjon.

**Analyse:** Svarene er kategorisert i tre kategorier. Egne rutiner og reaksjoner, her vises det blant annet til faste rutiner, erfaring og lære av egne feil. Prosjektgruppen tolker dette som reaktive handlingsmønster. De faller inn under den mer tradisjonelle måten å tenke kontinuerlige kvalitetsforbedringsprosesser på, som prosjektgruppen tidligere har belyst mulige svakhetene ved. Ellers indikerer de ulike svarene at informasjonsflyt og kommunikasjon i organisasjonen anses som meget viktig. Kategorien trusselinformasjon anses ikke å tilføre ny informasjon. Korrekt informasjon om hendelsen blir vektlagt hos en del av informantene, tid anses her som viktig av flere. Svarene gir i mye mindre grad enn hva prosjektgruppen hadde håpet en mulighet til å avlede et informasjonsbehov, og eventuelle viktige indikatorer eller detektorer som må prioriteres. Således konkluderes det med at faktorer som var avgjørende for spørsmålsstillingen må videreføres til neste intervjurunde.

### 6.1.1 Delkonklusjon etter første intervjurunde

Ved å analysere og tolke resultatene fra den første intervjurunden, kan den samlede vurderingen gi indikasjoner, og sannsynliggjøre deler av våre hypoteser og forskningsspørsmål. En samlet vurdering er at det denne intervjurunden har, om ikke bevist, sannsynliggjort deler av prosjektets hypoteser og bidratt til å besvare deler av forskningsspørsmålene. Dette innebærer, slik analysen av de enkelte spørsmålene viser, i all hovedsak hypotesene 1,2 og til dels 3 med tilhørende forskningsspørsmål. Disse temaene er berørt helt eller delvis, og prosjektgruppen anser at det er etablert en forståelse for bakgrunnsproblemet blant ekspertuttalelsene. Det vil her vurderes fortløpende i hvilken grad prosjektgruppen mener de enkelte hypoteser og forskningsspørsmål er tilstrekkelig begrunnet. Dette vil i tillegg danne et grunnlag for en vurdering av innholdet i neste intervjurunde.

*Hypotese 1:* *Det er sannsynlig at dagens strategi for beskyttelse mot cybertrusselen, gir den avanserte/intelligente motstanderen store konkurransefortrinn.*

Vår misjon med denne hypotesen er å bekrefte om bakgrunnsproblemet for oppgaven er reell og gir grunnlag for videre studier. Prosjektgruppen anser at resultatet fra den første intervjurunden gav resultater som sannsynliggjør hypotese 1. Det trekkes frem momenter ved flere av intervjuspørsmålene som kan underbygge dette. Det reaktive handlingsmønsteret som er beskrevet i dette prosjektet ble gjengitt av en overvekt av personene ved flere av spørsmålene. Det gir grunnlag for å bekrefte det som i prosjektet er omtalt som en reaktiv kvalitetsforbedringsmodell. Det sies at det med dagens regime aldri finnes en kur før, eks viruset, er iverksatt. En innfører statiske beskyttelsestiltak mot en dynamisk trussel. Videre belyses det strukturelle og prosedyremessige faktorer som forsterker dette problemet. Det virker å være en gjennomgående forståelse av at en som forsvarer stiller svakt i konkurransen mot en målrettet motstander.

1.1 Finnes det informasjon som indikerer eller motbeviser, at dagens beskyttelsesmetoder i hovedsak er fundamentert på erfaring og læring fra kjente vellykkede angrep og kan beskrives som reaktive

Som beskrevet over danner intervjuresultatene en sannsynliggjøring av at det, i organisasjonen, foreligger et reaktivt handlingsmønster ved beskyttelse mot cybertrusselen. Det beskrives at reaktive og statiske metoder ikke er i stand til å håndtere et dynamisk trusselbilde.

1.2 Finnes det informasjon som indikerer eller motbeviser, at motstanderen tilpasser sine taktiske og tekniske prosedyrer til våre tiltak, og metoder for innhenting av trusselinformasjon?

Påstanden om at motstanderen tilpasser sine metoder og handlingsmønster til våre beskyttelsestiltak bekreftes av en gjennomgående forståelse av at det gjennomføres kontinuerlige kartlegginger av egne systemers strukturelle og teknologiske oppbygning. Dette fremkommer, slik resultatet viser, gjentatte ganger ved ulike intervjuspørsmål. Det nevnes også at dette er kjernen i problemet med den reaktive beskyttelsen. Det konkluderes dermed at hypotese 1 med tilhørende forskningsspørsmål er tilstrekkelig sannsynliggjort og besvart av involverte eksperter.

*Hypotese 2:* *Det er sannsynlig at en strategi basert på økt fiendeforståelse kan endre dagens beskyttelsestankegang til en forsvarstankegang og gjøre sikkerhetsarbeidet proaktivt i større grad.*

Hypotese 2 sier at det er en sammenheng mellom økt fiendeforståelse og økt proaktivitet i sikkerhetsarbeidet. Flere av spørsmålene i intervjurunden var myntet på informasjonsinnsamling rundt hypotese 2. En korrelasjon av svarene gir data som sannsynliggjør denne hypotesen. Indirekte opplysninger om at fordelen med å forsvare seg er å lære om fienden, indikerer at fiendeforståelsen anses som viktig for å beskytte egne systemer. For de som står ovenfor en målrettet aktør, er fiendeforståelsen desto viktigere. Kunnskap om fiendens målsettinger, kapasiteter, motivasjon og metoder anses som verdifull informasjon. Det indikeres at om man besitter denne kunnskapen, kan man i større grad kontrollere og overvåke/monitorere et angrep. Man kan i så måte sørge for at angriperen ”holdes i en sikker del” av systemet, og selv avgjøre når man ønsker å avbryte angrepet.

2.1 Hvilke indikatorer har betydning for fiendeforståelsen?

Overordende indikatorer viser seg å være fiendes målsetting, motivasjon, kapasiteter og metoder. Det er også viktig med kunnskap om hendelser i samfunnet generelt og om operative hendelser spesielt. Opplysninger viser videre at en rekke kilder benyttes til å samle informasjon om trusselbildet og trusselaktører. Det vises spesielt til åpne kilder og til samarbeidspartnere, som i stor grad også er tilgjengelig for fienden. Det kommer også frem at det i praksis kun benyttes indikatorer som CND avdelingen har kontroll over i dag.

2.2 *Finnes det indikasjoner om at økt kunnskap om fienden kan gjøre oss bedre i stand til en dynamisk tilpasning av forsvarsressursene iht. endringer i trusselbildet?*

Forskningsspørsmålet er besvart ut i fra at kunnskap om fienden anses om essensiell ved beskyttelse av egne systemer. Kunnskap om fiendens mål, motivasjon, metode og kapasiteter muliggjør en forsvarstankegang. Blant annet nevnes det at man kan ta avgjørelser på om man skal la angrepet fortsette for å lære mer om fienden eller om man velger avsluttet angrepet (stenge fienden ute).

*Hypotese 3:* *Det finnes indikasjoner på at strategien for beskyttelse/forsvar i større grad bør baseres på bevissthetsøkende arbeid, som kan gi grunnlag for et bedre mentalt bilde av motstanderen.*

En samlet analyse av svarene informantene gir, øker vår tiltro til gyldigheten av hypotese 3. Kunnskapen om fienden virker å være en nøkkelfaktor for å lykkes i å forsvare eget system mot en målrettet trusselaktør. En bevissthetsmodell som gjør organisasjonen i stand til å danne et bedre bilde av motstanderens målsettinger, motivasjoner, kapasiteter og metoder kan danne grunnlaget for en forsvarsstrategi. Det vises til at det er viktig med en helhetlig situasjonsbevissthet. Der man i tillegg til kunnskap om cyberverden og tekniske perspektiver, ser sammenhenger til operative og samfunnsmessige hendelser. Opplysninger indikerer at det ligger et potensial i å utnytte organisasjonen som helhet i IS-arbeidet, da den øvrige organisasjonen besitter vital informasjon.

3.1 I hvilken grad har bevissthetsnivået en betydning for Forsvarets fiendeforståelse?

Opplysninger viser, som det er argumentert for over, at bevissthetsnivået har en betydning for fiendeforståelsen. Det vises til en helhetlig situasjonsbevissthet og kunnskap om samfunnet og operative hendelser. Svarene indikerer også at det er en synergi her, en bedre fiendeforståelse gir også en bedre situasjonsbevissthet. Dette gir indikasjoner hva angår CND avdelingen spesielt. Informantene mener også at det ligger et stort potensial i å utnytte informasjon som den øvrige organisasjonen besitter. Det trekkes det frem at informasjonsflyten og informasjonsdeling i organisasjonen er nøkkelfaktorer for at dette skal bli vellykket.

3.2 Er det sannsynlig at en strategiendring basert på økt bevissthet kan gi grunnlag for en mer effektiv ressursutnyttelse og bedret sikkerhet?

Forskningsspørsmålet kan delvis besvares gjennom en korrelasjon av opplysninger som har kommet frem i arbeidet med hypotese 2 og 3. Data indikerer at det er en sammenheng mellom bevissthet og fiendeforståelse, og at økt fiendeforståelsen gir grunnlag for en endring fra beskyttelse til forsvar av egne systemer. Av svarene fremgår det allikevel at flere opplysninger og synspunkter må samles rundt dette forskningsspørsmålet for i større grad øke vår tiltro til hypotesen.

Resultatet av den første intervjurunden gir prosjektet et behov for videre intervjuer. Som det fremkommer av resultatene vil dette gjelde spesielt med tanke på hypotese 4, men også hypotese 3. Den første intervjurundens siste spørsmål er som spørsmålenes begrunnelse forteller, ment å kunne sannsynliggjøre påstanden fremsatt i hypotese 4, men prosjektet anser denne påstanden som relativt lite berørt og understøttet av ekspertuttalelser. Dette gjelder med tanke på ordlyden ”innføring av et organisert bevissthetsprogram”. Imidlertid har det fremkommet at det foreligger en felles forståelse blant intervjuobjektene at det finnes et behov for en generell økning av kunnskap og forståelse for informasjonssikkerhet i alle ledd i organisasjonen. Dette kan indikere at videre intervjuer kan gjennomføres for å bidra til å besvare forskningsspørsmålene fremsatt under hypotese 4. Således konkluderes det med at neste intervjurunde i hovedsak vil omhandle dette, sammen med arbeidet med hypotese 3, spesielt forskningsspørsmål 3.2 En vurdering av utarbeidelsen av intervjuguide for denne intervjurunden er gjengitt i kapittel 6.4.

### 6.1.2 Erfaringer fra første intervjurunde

Det er gjort en del erfaringer fra intervjurunden som vil danne grunnlaget for forberedelsene til neste runde. De positive erfaringer kan derfor videreføres samt at de negative faktorer kan unngås og/eller forbedres. Dette gjelder rent generelle prosedyrer rundt forberedelse og gjennomføring. Det er viktig at intervjuguiden er gjennomtenkt og begrunnet for det første å sikre at intervjuene resulterer i interessante svar som kan bekrefte/avkrefte våre påstander. For det andre ligger en stor utfordring i at gjennomføringen og spørsmålsstillingen foregår på en måte som sikrer et vitenskapelig gyldig resultat. Dette vil i hovedsak være å sørge for at selve gjennomføringen av intervjuet i størst mulig grad er lik i hvert tilfelle. Samt at spørsmålsstillingen er av en slik art at den ikke er ledende i for stor grad. Resultatet fra denne runden tilsier at intervjuguiden er sterkt styrende for hvordan disse faktorene blir ivaretatt. Erfaringen tilsier derfor at utarbeidelse av intervjuguiden er svært viktig for resultatet.

En erfaring vi gjorde etter den første intervjurunden er at en analyse og tolkning av intervjuet, i mye større grad en antatt, krever en totalvurdering av intervjusamtalen. Dette fordi informanten ofte som svar på et aktuelt spørsmål kommer med uttalelser som ikke gir data det aktuelle spørsmålet hadde som formål å samle inn. Imidlertid kan uttalelsene være svært relevant for emner/spørsmål som er stilt tidligere eller senere i intervjuet. Derfor er det dokumentert svar under de enkelte spørsmål som ikke er direkte relevante for spørsmålet spesielt, men relevante for prosjektet som helhet. Denne metoden for innhenting av data innebærer en vurdering av balansen mellom å unngå ledende spørsmål, samtidig som en søker å lede samtalen inn på de temaer og emner som er interessante. Dette innebærer en stor utfordring med tanke

på forberedelser, med kanskje mest av alt med tanke på å styre intervjuet mens det pågår.

Det overordnede synet på informasjonssikkerhet og den konseptuelle/helhetlige vinklingen på prosjektet kan være fjernt fra enkeltes hverdag. Eksempelvis kan enkelte kategorier av sikkerhetspersonell ha et svært teknisk perspektiv på emnene. Samtalen vil dermed i stor grad dreie seg rundt dette. Således har prosjektgruppen forsøkt å kategorisere personellet og tilpasse intervjuet deretter. De ulike intervjuobjektene har stor divergens i bakgrunn, arbeidsområde, interesse osv, slik at det varierer i stor grad hvor mye intervjuet må styres for å holde det innenfor prosjektets interesseområde. Totalt sett vurderer prosjektgruppen at dette har foregått innen de rammer som er akseptable.

Videre er det erfart at vinklingen prosjektet har kan gjøre at enkelte intervjuobjekter inntar en forsvarsposisjon i løpet av intervjuet. Prosjektets emner peker på faktorer som tilsier at den jobben som gjøres i dag ikke er tilstrekkelig og dermed er feilslått. Vi har erfart at enkelte kan innta en forsvarsposisjon fordi de anser at den jobben de gjør kritiseres. Dette er en faktor som ikke er tillagt en svært avgjørende rolle for resultatet, men prosjektgruppen har valgt å vurdere dette fortløpende og la det være ett av innspillene til analyse av resultatet. Dette er muligens en faktor som bidrar til behovet for en helhetlig analyse av alle spørsmålene. Da ofte en og sammen informant kan komme med motstridene opplysninger med bakgrunn i at informanten har inntatt en forsvarsposisjon på et av spørsmålene. Hvilket også indikerer viktigheten av en gjennomtenkt ordlyd i spørsmålsformuleringene.

Å basere innhentingen av data på flere intervjurunder har i seg selv vist seg å være svært positivt. Å kunne etablere en intervjuguide som favner om alle aspekter ved prosjektet har vist seg å være meget vanskelig. Derfor er det nyttig å kunne differensiere temaer og benytte tidligere resultater for å utarbeide videre intervjuguider.

Denne metoden for innhenting av kvalitative data innebærer en relativt stor arbeidsmengde. Dette gjelder både i forberedelsene av intervjuet, gjennomføring av intervjuene og ikke minst analysen av resultatene. Erfaringen er med dette at prosjektet i det videre arbeidet tillegger denne prosessen tilstrekkelig tid og ressurser for å sikre et godt resultat.

## 6.2 Andre intervjurunde

Vi presenterer her arbeid og resultater relatert til andre intervjurunde. Først beskrives og argumenteres det for utarbeidelsen av intervjuguiden som ble benyttet og videre presenteres resultater og analyse.

### 6.2.1 Beskrivelse og argumentasjon for andre intervjuguide

Intervjuguiden til andre intervjurunde er utarbeidet med bakgrunn i funn etter første intervjurunde, samtidig som vi ønsket å ta høyde for opparbeidet erfaring. Selv om en presentasjon og argumentasjon anses som en del av metoden i prosjektarbeidet, valgte vi å presentere den her. Dette skulle medføre en naturlig flyt og kontinuitet i

informasjonen for leseren av rapporten. Argumentasjonen for utarbeidelsen av andre intervjuguide må sees i sammenheng med allerede presentert arbeid og resultater.

Resultatet av gjennomført forskning og delkonklusjoner, etter første intervjurunde, viser at det er opparbeidet tilstrekkelig data som sannsynliggjør bakgrunnsproblemet. Spesielt med tanke på reaktive tiltak og at det faktisk eksisterer en målrettet trussel. I tillegg til at de reaktive tiltakene ikke er egnet for å beskytte seg mot en målrettet trusselaktør. Videre er det fremvist en forståelse for at menneskene i organisasjonen innehar (eller i potensielt innehar) informasjon som er nyttig for å øke CNDs (FOST[18]) fiendeforståelse. I tillegg er det erkjent at kunnskap om fienden er essensielt for proaktivt å kunne tilpasse sine ressurser. Det er etablert en sammenheng mellom økt IS-bevissthet og fiendeforståelse. Det er konkludert med at det videre arbeidet konsentreres om hypotese 4 og tildels hypotese 3 med de respektive forskningsspørsmål. Formålet med andre intervjurunde blir derfor å samle informasjon som kan benyttes til å indikere gyldigheten til hypotese 3 og 4, og besvare tilhørende forskningsspørsmål.

Det ble i første intervjurunde etablert en kontakt med en rekke informanter. Samtlige sa seg villig til fortsatt å bidra til prosjektet. Dette sammen med tidsaspektet gjorde at vi i stor grad ville benytte disse informantene også i andre intervjurunde, men at et fåtall nye informanter ble involvert. Begrunnelsen for dette er at prosessen med å komme i kontakt med nye informanter med spesialkompetanse innen for eksempel bevissthetsbyggende arbeid ble ansett som for tidkrevende. En mulig konsekvens av at tidsaspektet må tas hensyn til, at brorparten av de samme informantene vil bli benyttet, er at emnene og spørsmålene som er formulert er tilpasset kompetansen til de overnevnte informantene. Sistnevnte må tas hensyn til, spesielt med tanke på at dette kan medføre en begrensning av oppgaven. Vi formulerte spørsmål som var rettet inn mot å skaffe dataene det henvises til ovenfor, innenfor disse begrensingene. Spørsmålene og begrunnelsen for spørsmålsformuleringene presenteres under.

Utgangspunktet for andre intervjurunde bygger på analysen av resultatene fra første intervjurunde. Hensynet til argumentasjon i forrige avsnitt medført at vi valgte en innfallsvinkel der vi innledningsvis konserterte spørsmålene rundt informasjon og informasjonsflyt. Spesielt i hvilken grad det er viktig at CND avdelingen innehar en kontinuerlig forståelse av hva det faktiske operative behovet for CNDs tjenester er. Dette har kommet fram delvis i runde 1, men kun som tilleggsopplysninger. Intervjuguiden er tredelt der den enkelte del har et spesifikt formål. Dette er beskrevet fortløpende.

Valget av innfallsvinkel gjorde at vi formulerte følgende spørsmål innledningsvis.

1. *Hvilken betydning har din forståelse og kunnskap rundt det operative behovet og målsettinger for din prioritering av arbeidsoppgaver og ressurser?*

2. *Hvilke type informasjon mener du er viktig i denne sammenheng?*

[18] FOST - Forsvarets Sikkerhetstjeneste

3. *I hvilken grad mener du at FOST (CND) får informasjon om det operative behovet og tilpasser seg deretter?*

Begrunnelsen for spørsmålsformuleringen og rekkefølgen er at vi først ønsker å samle data som kan etablere viktigheten av denne kunnskapen. Her også data som kan sannsynliggjøre hvilken effekt denne kunnskapen har på måten CND avdelingen kan prioritere sine arbeidesoppgaver og ressurser. Spørsmål 2 er formulert for å indikere hvilke type informasjon informanten anser som essensiell i denne sammenhengen. Spørsmål 3 vil i sin tur kunne samle opplysninger som indikerer om denne type informasjon foreligger i dag. Rekkefølgen og formuleringen vil derfor muliggjøre en analyse av gapet mellom hvilke informasjon informantene anser som viktig og hva som faktisk foreligger i dag. Opplysningene vil kunne indikere forbedringspotensialer, og ikke minst kunne benyttes som viktige innspill til hvordan man skal skreddersy et IS- bevissthetsprogram mot forsvarets behov. Her da spesielt med hensyn til CND avdelingens særbehov.

En nøkkelfaktor for prosjektets innfallsvinkel er at menneskene i organisasjonen (som sensorer) kan settes i stand til å tilegne seg og formidle relevant data om trusselaktører til CND avdelingen. Andre del av intervjuguiden skal samle informasjon som indikerer hvilken kunnskap de ansatte trenger for å kunne bli en slik ressurs. Flere av informantene har ekspertise fra CND. Det er derfor også naturlig å utnytte denne ekspertisen til å samle data som indikerer om CND avdelingen kan bidra til å øke bevisstheten til de øvrige ansatte. Opplysningene vil benyttes som innspill til et bevissthetsprogram rettet mot den øvrige organisasjonen.

4. *Hvilken kunnskap trenger de operative å få for å kunne bidra til bedre sikkerhet, og gi verdifull informasjon til fiendebilde?*

5. *Hvilken opplæring gis de ansatte i denne sammenheng i dag?*

6. *Kan CND avdelingen bidra til å dekke informasjonsbehovet de ansatte har for å øke sin informasjonssikkerhetsbevissthet og evne til å opptre som en sensor. (Med sensor menes her en kapasitet som kan detektere og formidle sikkerhetsinformasjon. Det er underliggende her at en sensor må tilføres informasjon ("tunes") for å gjennomføre denne funksjonen).*

7. *I så fall hvordan mener du CND avdelingen kan bidra til dette?*

Etter at det foregående spørsmål er stilt vil informantene bli opplyst om formålet med spørsmålene. Svarene skal analyseres med tanke på å identifisere viktige faktorer ved et bevissthetsprogram. De vil kunne benyttes som innspill til et bevissthetsprogram i Forsvaret, som er skreddersydd mot økt fiendeforståelse. Et siste spørsmål formuleres derfor for å gi informantene mulighet til å komme med ytterligere kommentarer/innspill til et slikt program. Dette skal kunne fange opp andre innfallsvinkler informantene anser som viktig i lys av at de får direkte informasjon om formålet med overstående spørsmål.

8. *I hvilken grad mener du at det eksisterer IS-bevissthetsøkende arbeid i Forsvaret i dag?*

Vi valgte å avslutte det siste intervjuet med å vise til at vi undersøkte effekten av å implementere et IS- bevissthetsprogram i Forsvaret. I lys av dette ønsket vi å gi informantene mulighet til å komme med ytterligere kommentarer i forhold til programmets formål. Vi benyttet følgende formulering til dette.

*La oss si at det skal implementeres et IS-bevissthetsprogram i Forsvaret. Det er et ønske om at programmet skal utformes slik at det oppnås positive effekter også for CND avdelingen og deres fiendeforståelse. Hvilke innspill har du til utformingen av et slikt program?*

### 6.2.2 Resultater og analyse etter andre intervjurunde

Andre intervjurunde er gjennomført etter samme metode og prinsipper som den innledende runden. Resultatene ble transkribert fortløpende mens intervjuet pågikk og dannet grunnlaget for videre analyse. Som tidligere ble det foretatt en meningsfortetting, samt en kategorisering av svarene som fremkom. Også her var enkelte av spørsmålene av en slik art at de ikke la grunnlag for at kategorisering kunne finne sted, og kun de fortettede ytringene la grunnlaget for videre analyse. Det er i vedlegg 5 gjengitt svarene slik de ble fremsatt av informantene, med en muntlig fremstilling av svarene for å fange svaret i størst mulig grad slik det fremkom. Med bakgrunn i den kvalitative metoden som benyttes i prosjektet er det under gjengitt svarene på en sammenfattet form, som videre er analysert. Begrunnelsen for valget av emner og utforming av de enkelte spørsmål er gjengitt i kapittel 6.2. Intervjuguiden for den andre intervjurunde bestod av spørsmålene under med påfølgende svar. Analysen som er foretatt er en ytterligere tolkning av resultatene, spesielt med tanke på å trekke fram og belyse aspekter som er relevante for hensikten med det enkelte intervjuspørsmål og prosjektet som helhet. Dette er etter samme metode som første intervjurunde.

1. ***Hvilken betydning har din forståelse og kunnskap rundt det operative behovet og målsettinger for din prioritering av arbeidsoppgaver og ressurser?***

    i. **Dialog/informasjonsflyt**
    Det beskrives at å etablere og opprettholde en kommunikasjonsflyt med ledelsen er viktig, og at å understøtte den operative tjenesten er CND avdelingens overordnede mål. Gjennom dialog synliggjøres organisasjonens overordnede prioriteringer og virksomhet slik at CND ressursene kan tilpasses dette.

    ii. ***Operativ forståelse***
    Gjennom den nevnte kommunikasjonsflyten kan en være bevisst på organisasjonens totale virksomhet, hvilke verdier de besitter, samt hvilke konsekvenser et bortfall av tjenester vil ha. CND må prioritere sine ressurser slik at de har best mulig militær effekt.

**Analyse:** Det foreligger en klar oppfatning blant samtlige informanter at en kontinuerlig forståelse og kunnskap om den operative virksomheten i den øvrige organisasjonen er svært viktig for utøvelsen av sine CND funksjoner. Det belyses at

dette gir grunnlaget for å skape et korrekt bilde av hva behovet er for deres tjenester og at prioritering av egne arbeidsoppgaver og ressurser er en naturlig følge av dette. I hovedsak belyses viktigheten av en etablert dialog med de ulike avdelingene CND skal støtte, samt med organisasjonens øverste ledelse. Dette underbygger resultater fra første intervjurunde der operativ forståelse ble omtalt som viktig for CND avdelingen. Således er spørsmålet rettet mot å sette intervjuet inn i ønsket sammenheng, og belyse i hvilken grad informanten anser det som viktig å sette sitt CND arbeid inn i en operativ sammenheng.

2. ***Hvilke type informasjon mener du er viktig i denne sammenheng?***

   Det belyses at viktig informasjon omhandler en kontinuerlig kunnskap om de aktuelle operasjoner/aktiviteter som pågår. Dette innebefatter hvilke kritiske verdier som finnes, prioriteringer fra operativ ledelse, i hvilken grad ulike systemer benyttes og hvordan, konsekvenser ved bortfall og kapasitet/evne til å håndtere en hendelse finnes hos de ulike avdelinger.

**Analyse:** Svarene som fremkom omhandler i hovedsak å etablere en kontinuerlig kommunikasjon med det operative miljøet om deres virksomhet og prioriteringer. Hvilke kapasiteter de selv besitter, samt konsekvenser av et angrep/bortfall av systemer. Ut over dette er det interessant å registrere at det ble nevnt kunnskap om egne kapasiteter sett i sammenheng med det operative behovet. Dette ble omtalt som viktigheten av at CND avdelingens kjennskap til egne kapasiteter og begrensninger for å kunne sette dette i sammenheng med det operative behovet for CNDs tjenester.

3. ***I hvilken grad mener du at FOST (CND) får informasjon om det operative behovet og tilpasser seg deretter?***

   Det er en generell forståelse av at det foreligger et potensial med tanke på å være tilpasset det operative behovet for CND-tjenester. Dette foregår i en viss grad, men det foreligger ingen automatikk i at avdelingen besitter et oppdatert situasjonsbilde.

**Analyse:** Svarene var samlet sett begrenset med tanke på innhold, og det kan være begrunnet i et ønske om ikke å uttale gradert opplysninger. Imidlertid var det en gjennomgående oppfatning at slik informasjon er svært viktig og at det foreligger et potensial med tanke på dette. Hensikten med spørsmålsformuleringen og rekkefølgen var å utføre en gapsanalyse mellom informasjonsbehovet og hvilke informasjon som er tilgjengelig i dag. Det er lite grunnlag for å kunne analysere i hvilken grad det finnes et gap mellom det informantene anser som kravet til slik informasjon, og det som faktisk foreligger. Imidlertid ble det belyst at det foreligger et forbedringspotensial her, som kan være et innspill til hvordan et IS-bevissthetsprogram kan skreddersys med tanke på CND avdelingens behov. En bedre informasjonsflyt og deling virker igjen å være en nøkkelfaktor for å kunne realisere dette. Funnene etter de tre innledende spørsmålene bidrar til å sannsynliggjøre prosjektets tredje hypotese. Kunnskap om egen organisasjon vil være en viktig faktor med tanke på å basere sin prioritering av ressurser på en bevissthetsmodell.

4. ***Hvilken kunnskap trenger de operative å få for å kunne bidra til bedre sikkerhet, og gi verdifull informasjon til fiendebilde?***

   i. **Generell bevissthet**
   Det vises til at en generell kunnskap om informasjonssikkerhet må ligge til grunn.

   *ii.* **Kunnskap om prosedyrer og FOST/CND**
   Kunnskap om egen virksomhet og bruk av informasjonssystemer belyses som viktig. Videre er det en generell oppfatning at det er viktig at de informasjonssikkerhetsmessige kapasitetene som finnes hos FOST gjøres kjent for alle. I tillegg er informasjon om hvordan disse kapasitetene kan benyttes omtalt som viktig. Det dreier seg i hovedsak om å informere om CNDs kapasiteter, hvordan de kan kontaktes, rapporteringsrutiner etc.

   *iii.* **Informasjon om trusler**
   En kontinuerlig informasjon om aktuelle trusler og trender, slik at den enkelte ansatte og enkelte avdeling kan sette dette i sammenheng med sin hverdag og sitt operative miljø.

   *iv.* **Kommunikasjonsflyt**
   Selv om denne kategorien ikke gir et direkte svar på det aktuelle spørsmålet er det valgt å omtale dette da dette fremkom ved flere av intervjuene. Det vises til at det er essensielt at det opprettes kommunikasjonskanaler der denne informasjonsflyten kan finne sted.

**Analyse:** Svarene omhandler i stor grad å informere om hvilke kapasiteter CND avdelingen innehar, i tillegg til å informere om aktuelle trusler og hendelser for å øke bevisstheten. Selv om det å etablere kommunikasjonsflyt ikke kan anses å være en kunnskap som tilegnes er det interessant å vurdere dette i den grad at det må informeres om disse kommunikasjonskanalene og hvordan de kan benyttes. Svarene sett under ett kan gi indikasjoner på at en generell økning bevissthetsnivå kan ha positive effekter for CND-avdelingens grad av fiendeforståelse. Derfor fremkom det informasjon her som bidrar til relevant informasjon for hypotese 3, gjennom å bidra til å besvare tilhørende forskningsspørsmål.

5. ***I hvilken opplæring gis til de ansatte i denne sammenheng i dag?***

   Det foreligger en generell oppfatning av at denne typen opplæring foreligger i begrenset grad i dag. Det vises til at den sikkerhetsopplæringen som foregår er rettet mot personell med sikkerhetsrelaterte stillinger i de ulike avdelingene, og at det i stor grad er opp til dette personellet selv å oppsøke slik informasjon/opplæring. Videre er det dette personellet som har ansvaret for å videreformidle informasjon og drive opplæring på det øvrige personellet i egen avdeling. Utover dette gjøres relevant og oppdatert sikkerhetsinformasjon tilgjengelig på et intranett.

**Analyse:** Disse funnene indikerer igjen et forbedringspotesial innen Forsvaret. Det er etablert målrettet opplæring mot bestemte jobbfunksjoner i de ulike avdelingene, men det er den enkelte selv som må oppsøke denne type opplæring. Opplæring og videreformidling av sikkerhetsinformasjon innen egen avdeling vil variere ut i fra kompetansen og kunnskapen til sikkerhetspersonellet ved den enkelte avdeling. Det antas også, i mer eller mindre grad, at egeninteressen til den enkelte ansatte avgjør i hvilken grad relevant og oppdatert sikkerhetsinformasjon oppsøkes ved hjelp av Forsvarets intranett. Dette intervjuspørsmålets formål er i all hovedsak å kunne besvare forskningsspørsmål 4.1. Svarene har ikke frembrakt en komplett beskrivelse av hvordan slik opplæring foregår i organisasjonen pr i dag, men det er en klar oppfatning at dette foregår i begrenset grad, og at det foreligger et klart potensial i denne sammenhengen.

6. ***Kan CND avdelingen bidra til å dekke informasjonsbehovet de ansatte har for å øke sin informasjonssikkerhetsbevissthet og evne til å opptre som en sensor. (Med sensor menes her en kapasitet som kan detektere og formidle sikkerhetsinformasjon. Det er underliggende her at en sensor må tilføres informasjon ("tunes") for å gjennomføre denne funksjonen).***

   Det er en gjennomgående forståelse blant informantene, at CND avdelingen kan bidra med denne type informasjon. De besitter informasjonen og evnen til å tilby denne. Det vises til at det er vesentlig i denne sammenhengen at det foreligger en kontinuerlig informasjonsflyt, som er tilpasset det aktuelle trusselbildet og det operative situasjonsbilde. Utover å bekrefte at avdelingen innehar denne kompetansen og kapasiteten, vises det til at det må utvikles kommunikasjonslinjer og prosedyrer som gjør dette mulig.

**Analyse:** Det er interessant for prosjektets innfallsvinkel at det er en gjennomgående forståelse av at CND besitter både kunnskap og kapasiteter til å dekke dette informasjonsbehovet, sågar at dette kan være den eneste kilden til slik informasjon innad i Forsvarets organisasjon. Videre omtales begrensninger i etablerte kommunikasjonskanaler som en utfordring for å gjennomføre dette. Svarene sett under ett bekrefter således de konklusjoner som ble trukket fra første intervjurunde, og er bidragsytende for å sannsynliggjøre hypotese 3.

7. ***I så fall hvordan mener du CND avdelingen kan bidra til dette?***

   Det vises til viktigheten av å dele den kunnskap som CND innehar. Videre belyses det at dersom en sensor skal fungere er det viktig at kommunikasjon flyter begge veier mellom CND-avdelingen og de øvrige avdelinger og personell. Derfor er det viktig at en innrapportert hendelse blir tatt på alvor og at det blir gitt tilbakemelding til den/de som rapporterte. Informantene belyser at dagens prosedyrer for informasjonsdeling fra CND-avdelingen i stor grad er basert på at utpekt sikkerhetspersonell hos den enkelte avdeling har ansvaret for å informere sin egen avdeling. Det fremkom en forståelse av at dette

fungerer i varierende grad. I tillegg finnes det ingen kontroll på hvordan dette fungerer. Derfor ble det ytrer at CND kunne bidra med en mer direkte opplæring og kontinuerlig informasjonsdeling til et bredere publikum, og tilpasse dette til det operative miljøet personellet opererer i.

**Analyse:** Informantene viser en gjennomgående oppfatning av at CND avdelingen besitter mulighet og evne til å tilby denne informasjonen. Videre er det identifisert at det er utfordringer med tanke på dagens prosedyrer for slik informasjonsdeling. Utover dette er det få konkrete slutninger som kan trekkes av svarene med tanke på detaljerte beskrivelser av hvordan CND kan dekke dette informasjonsbehovet. Et interessant aspekt som ble belyst var viktigheten av at informasjonsflyten fra CND avdelingen må være tilpasset det enkelte operative miljø. Det vises også til behovet for å nå ut til et bredere publikum. Et helhetlig bevissthetsprogram vil kunne gi dette om man implementerer krav om deltagelse og målbare resultater.

8. ***I hvilken grad mener du at det eksisterer IS-bevissthetsøkende arbeid i Forsvaret i dag?***

   Det beskrives at slik arbeid utføres i en viss grad i dag. Driftsorganisasjonen gir instrukser for bruk av systemene, som brukerne må signere på. Det benyttes informasjonsspredning via intranett, e-læringskurs og sikkerhetskonferanser. Videre er sikkerhetsorganisasjonen organisert slik at det er det lokale sikkerhetspersonellets ansvar å holde seg oppdatert og følge opp eget personell internt. Informasjon til dette personellet gjøres tilgjengelig via intranett og ukentlige brifer. Imidlertid virker opplæringen og arbeidet å være lite oppdatert, spesielt mot det dynamiske trusselbildet.

   **Analyse:** Konklusjonen er således at det ikke finnes noen offisielle programmer som favner om alle ansatte og det nevnes at en ny kompetansestrategi må utvikles. De samlede resultatene tilsier at de tiltakene som er implementert i begrenset grad innehar egenskaper som gjør det mulig å kontrollere i hvilken grad de er effektive. Dette er begrunnet i at informasjon gjøres tilgjengelig, men det finnes lite eller ingen oppfølging på hvem som tilegner seg denne kunnskapen. Intervjuspørsmålets formål var i hovedsak å kunne bidra til å besvare forskningsspørsmål 4.1. De samlede svarene kan ikke anses å kunne gi et helhetlig beskrivende svar på i hvilken grad bevissthetsøkende arbeid foregår, men indikerer at det finnes forbedringspotensial her.

9. ***La oss si at det skal implementeres et IS-bevissthetsprogram i Forsvaret. Det er et ønske om at programmet skal utformes slik at det oppnås positive effekter også for CND avdelingen og deres fiendeforståelse. Hvilke innspill har du til utformingen av et slikt program?***

*i.* **Rapportering av hendelser**
Det er en generell oppfatning at rapporteringsrutinene er en avgjørende faktor for hvordan informasjon fra den øvrige organisasjonen kan bidra til CNDs fiendebilde. Det belyses at prosedyrene må forenkles slik at den mentale terskelen for å gjennomføre rapportering senkes slik at den enkelte for det første er klar over at hendelser skal rapporteres, og for andre hvordan det gjøres. I denne sammenhengen vil informasjon om CND avdelingen og deres kapasiteter være viktig. Det vises til viktigheten av at alle rapporter følges opp og ikke minst at CNDs rolle i programmet kan være å gi tilbakemeldinger på alle rapporter.

*ii.* **Differensiering av tiltak**
Det belyses at de enkelte tiltak må tilpasses og differensieres til ulike typer personell. Denne tilpasningen må sees i sammenheng med den operative situasjonen personellet/avdelingen befinner seg i til enhver tid.

iii. **Spredning av informasjon**
En økning i bevissthet og IS-kunnskap må ligge til grunn for en generell endring i sikkerhetskulturen. Videre må det skapes en forståelse hos de enkelte av hvilke kapasiteter og tjenester FOST CND besitter. En generell spredning av informasjon fra CND avdelingen angående aktuelle trusler og trender gis som innspill, gjerne gjennom eksempler.

*iv.* **Myndighet og støtte**
For å lykkes med slik tiltak vises det til viktigheten av at en sørger for å skaffe tilstrekkelig støtte fra ledelsen til gjennomføringen. Dette for å gi tilstrekkelige midler, samt opprettholde en kontinuerlig myndighet.

**Analyse:** Det vises til ulike faktorer som generelt vil være suksessfaktorer for et IS-bevissthetsprogram, blant annet å sikre tilstrekkelig støtte hos ledelsen, differensiere tiltak etc. Utover de generelle fordelene dette vil medføre vises det til at dette også gjelder for å sørge for at programmet kan gi CND avdelingen nyttig informasjon om trusselbildet. Gjennom spredning av sin kunnskap kan CND gjøre organisasjonen i stand til å rapportere sitt bilde av trusselsituasjonen, slik at CND kan benytte seg av denne informasjonen og potensielt tilpasse sitt trusselbilde i henhold til dette. Intervjuspørsmålets formulering forutsetter at hypotese 4 fremsatt i dette prosjektet er gjeldende og hensikten var å identifisere informantenes innspill og meninger om hvordan et bevissthetsprogram burde utformes og gjennomføres.

### 6.2.3 Delkonklusjoner etter andre intervjurunde

Resultatene fra den første intervjurunden gav grunnlag for tidligere omtalte konklusjoner med tanke på i hvilken grad de var i stand til å sannsynliggjøre prosjektets hypoteser og bidrag til å besvare forskningsspørsmål. Den andre

intervjurunden ble utarbeidet med tanke på disse konklusjonene og er således ment å dekke de mangler vi fant der. Som tidligere nevnt er dette i stor grad gjeldende for hypotese 4 i sin helhet og deler av hypotese 3. Emner som er dekket av disse hypotesene er dekket helt eller delvis, og prosjektgruppen anser at det er fremkommet informasjon som er relevante for de nevnte hypoteser.

I motsetning til første intervjurunde søkte vi til dels informasjon som ikke er like godt egnet for å sannsynliggjøre ved hjelp av ekspertuttalelser. Dette har flere årsaker. For det første er selve ordlyden på enkelte forskningsspørsmål slik at enkeltuttalelser fra et fåtall eksperter ikke nødvendigvis gir et godt inntrykk av virkeligheten. Dette gjelder, slik det fremkommer senere, eksempelvis forskningsspørsmål 4.1; *"I hvilken grad er IS-bevissthetsprogram implementert i Forsvaret i dag?"*. Her er ordlyden slik at en grundigere undersøkelse av organisasjonen måtte ligge til grunn for å danne et tilstrekkelig svar. For det andre, dersom dette skulle kunne besvares av eksperter, ville det måtte identifiseres eksperter på nettopp dette feltet. Prosjektets avgrensning (tid, ressurser og tema) gjorde at den andre intervjurunden i stor grad benytter seg av de samme informantene som ved første runde, og dette i hovedsak er personell med fagfelt innen CND. Dette forsvares gjennom at for prosjektets innfallsvinkel vil CND eksperters oppfatning av dette, være vel så relevant som hva det offisielle svaret fra organisasjonen ville være. Derfor må de konklusjoner som vises til betraktes med denne bakgrunnen.

Analyse og konklusjoner fra første intervjurunde belyste at den andre intervjurunden ble konsentrert rundt temaer knyttet til forskningsspørsmål 3.2, samt hypotese 4. Forskningsspørsmålene presentert under hypotese 4 er i varierende grad egnet for den valgte intervjumetoden, spesielt med utgangspunkt i de informanter som vi hadde tilgang til. Som nevnt er forskningsspørsmål 4.1 delvis egnet, mens 4.2 er definert å være uegnet for å besvare ved hjelp av intervjuer og blir derfor i sin helhet omhandlet ved hjelp av litteraturanalyse. Dette er med tanke på at formuleringen på spørsmålet er direkte rettet mot en litteraturanalyse.

"Forskningsspørsmål 4.2: Finnes det egnede kilder fra litteraturen som gir anbefalinger med tanke på utvikling og gjennomføring av bevissthetsprogrammer som kan være egnet for Forsvaret".

Det påfølgende beskriver hvordan prosjektet anser i hvilken grad den andre intervjurunden har oppnådd informasjon som er relevant for å besvare de nevnte hypoteser/forskningsspørsmål.

*Hypotese 3:* *Det finnes indikasjoner på at strategien for beskyttelse/forsvar i større grad bør baseres på bevissthetsøkende arbeid, som kan gi grunnlag for et bedre mentalt bilde av motstanderen.*

3.2 Er det sannsynlig at en strategiendring basert på økt bevissthet kan gi grunnlag for en mer effektiv ressursutnyttelse og bedret sikkerhet?

Generelt sett kan det vises til opplysninger som sannsynliggjør påstanden om at økt bevissthet gir grunnlag for et bedret mentalt bilde av fienden. Den andre intervjurunden omhandler egenskaper ved økt kunnskap og bevissthet blant ulike

grupper i organisasjonen, og ikke minst kommunikasjonen mellom dem. Det er en klar oppfatning at en generell økning i kunnskap, holdninger og forståelse for informasjonssikkerhet i organisasjonen er viktig, dersom det generelle sikkerhetsnivået skal økes. Ikke minst for å oppnå en informasjonsflyt som kan bidra til å danne CND avdelingens fiendebilde. Den andre intervjurunden har således omtalt temaer som informantene anser å danne grunnlaget for at dette skal være mulig. Spesielt blir det lagt vekt på operativ forståelse og tilpasning. Viktigheten av å inneha en kontinuerlig oppdatert forståelse av det operative situasjonsbildet, og å kunne etablere en forståelse av hva dette betyr for enkeltpersonell og avdelinger er et gjennomgående tema i svarene. Den operative forståelsen omtales som essensiell også for CND avdelingen i deres tilpasning og prioritering av ressurser.

Således konkluderes det med at det er en nær sammenheng mellom det å danne seg et fiendebilde (i den hensikt å prioritere ressurser) og operativ forståelse. Det vises til at det reelle fiendebildet omfatter de trusselaktører som utgjør en trussel mot de verdier som til enhver tid er tilpasset det operative situasjonsbildet. På bakgrunn av dette er det fremkommet opplysninger som beskriver hvilke faktorer som er viktige for at dette skal være mulig. I all hovedsak dreier dette seg om å etablere kommunikasjonsflyt, for å oppnå en felles situasjonsbevissthet hos alle parter i organisasjonen. Med tanke på CND-avdelingens fiendebilde isolert sett er det beskrevet at informasjonsflyt fra CND-avdelingen til samarbeidende parter kan være essensiell, og danne grunnlaget, for at verdifull informasjon om trusselaktører føres tilbake til CND.

Disse opplysningene bidrar til å sannsynliggjøre hypotese 3, og forskningsspørsmål 3.2 spesielt.

*Hypotese 4:* *Det er grunn til å tro at veien til bedre informasjonssikkerhet gjennom økt fiendeforståelse, krever et organisert bevissthetsprogram i Forsvaret. Skreddersydd og spisset mot Forsvarets behov.*

Samlet sett gir begge intervjurundene informasjon som viser en forståelse av at en generell økning av informasjonssikkerhetsmessige kunnskaper og holdninger vil være positivt for informasjonssikkerheten i Forsvaret. Det vises til at det foreligger et potensial i slik type opplæring. Videre er det etablert en knytning mellom en økt bevissthet i organisasjonen og et bedret trusselbilde hos CND-avdelingen, forutsatt at det etableres egnede kommunikasjonskanaler. I forhold til hypotesens ordlyd er det også vist til viktigheten av at slik opplæring må tilpasses det til enhver tid gjeldende operative situasjonsbilde. Dette sees i sammenheng med hypotesens påstand om at et slikt program skal være skreddersydd og tilpasset forsvarets behov, og at Forsvarets behov i stor grad er styrt av et operativt situasjonsbilde. På denne måten har prosjektet frembrakt opplysninger som sannsynliggjør gyldigheten til hypotese 4.

### 4.1 I hvilken grad er IS-bevissthetsprogram implementert i Forsvaret i dag.

Som nevnt tidligere er forskningsspørsmålets formulering noe uegnet med tanke på den kvalitative metoden som er valgt for intervjuene, spesielt er det gjeldende med

tanke på at informantene ikke er valgt ut på grunn av sin ekspertise angående dette. Dette er en svakhet i prosjektet med hensyn på å besvare dette forskningsspørsmålet isolert sett. Imidlertid er det ikke sentralt i prosjektet å identifisere en komplett analyse av hva som faktisk finnes av bevissthetsprogram i organisasjonen.

Derimot er det vel så interessant å undersøke hvilken oppfatning CND personellet har av dette spørsmålet, med tanke på prosjektets innfallsvinkel. Hadde prosjektets rammer tillatt en grundigere undersøkelse av de faktiske forhold, kunne dette vært sammenlignet med CND personellets oppfatning. Som vist over ble de utvalgte informantene presentert et spørsmål angående dette, og konklusjonen viser at de ikke oppfatter at det finnes noe offisielt bevissthetsøkende arbeid som omfatter alle, samt at de tiltakene som er implementert ikke gir mulighet for å måle virkning. Derfor er det med tanke på å besvare dette forskningsspørsmålet identifisert informasjon som viser at CND personellet oppfatter at det foreligger et potensial med tanke på bevissthetsøkende arbeid.

4.2 Finnes det egnede kilder fra litteraturen som gir anbefalinger med tanke på utvikling og gjennomføring av bevissthetsprogrammer som kan være egnet for Forsvaret.

Som det vises til i innledningen finnes det ikke grunnlag for å besvare dette spørsmålet direkte med bakgrunn i kvalitative forskningsintervjuer med de utvalgte informanter. Imidlertid ble det valgt å spørre de enkelte informanter hvordan de mente et slikt program burde utformes og gjennomføres. Dette ble gjort for å undersøke hvilke suksessfaktorer de identifiserte, i sin operative sammenheng, for å kunne sammenligne dette med de anbefalinger som gis i litteraturen.

## 6.3 Sammenfatning av resultater

Det er her gitt en sammenfatning av forskningens resultater i forkortet form. Disse resultatenes implikasjoner vurderes i neste kapittel.

- Organisasjonen står ovenfor målrettede trusselaktører, og er utfordrende å identifisere fra den totale mengden lovlig og ulovlig trafikk.

- Trusselaktøren bruker mye tid på kartlegging og rekognosering av implementerte beskyttelsestiltak. Dette gjør at angriperen kontinuerlig kan tilpasse sine angrep med bakgrunn i beskyttelsen. Den målrettede trusselaktør kan derfor beskrives som dynamisk tilpasningsdyktig i forhold til våre beskyttelsestiltak og innhentingsplaner.

- Dagens reaktive metoder for informasjonssikkerhet anses, blant informantene, som dårlig egnet for å forsvare seg mot den målrettede trusselen.

- I arbeidet med å beskytte informasjonssystemene anser informantene kunnskap om trusselen som fundamental for å kunne lykkes.

Tatt i betraktning det tilhørende miljøet og ekspertisen til informantene, betrakter vi funnene, det vises til i de fire første punktene, som sterke bevis for resultatenes gyldighet.

- Litteratur og våre forskningsresultater viser at økt informasjon om fienden vil kunne bidra til et bedre situasjons- og fiendebilde. Kunnskapen vil utvide beslutningsgrunnlaget for en mer effektiv og proaktiv prioritering av tilgjengelige IS-ressurser.

- Det er et generelt behov for å øke IS-bevisstheten i organisasjonen. Det belyses som en av utfordringene ved å oppnå god informasjonssikkerhet og forståelse for IS-arbeidet.

- I perspektivet til informantene anses de ansatte i organisasjonen som en kapasitet som kan bidra med viktig informasjon om fienden. Informasjonen vil kunne supplere dagens informasjonskilder. I dag foreligger det et stort potensial i å utnytte informasjonen de ansatte innehar.

- En økning i den generelle IS-bevisstheten i organisasjonen kan gjøre de menneskelige sensorene bedre rustet til å bidra med viktig informasjon om trusselaktøren(e).

    - Slik opplæring foregår i begrenset grad i dag

    - Dette forutsetter en kategorisering av de ulike ansatte og de ulike avdelinger som må være kontinuerlig tilpasset det gjeldende operative miljøet.

Det virker å være en generell oppfatning blant informantene rundt det som belyses i punktene over. Det foreligger derfor indikasjoner på at prosjektets innfallsvinkel er fornuftig. I denne sammenheng er det viktig å belyse at det virker å være en noe divergens i oppfatningen informantene har rundt hvor realiserbart og matnyttig en implementering vil være for CND-avdelingen og løsningen av deres oppdrag. Spesielt gjelder dette de to sistnevnte punkt. Samtidig virker de informanter som sitter i jobbfunksjoner med et mer overordnet ansvar for ressursene å være meget positive. I dette perspektivet vektlegges viktigheten av neste punkt.

- Å opprette formålstjenlige kommunikasjonslinjer vil være essensielt for å oppnå denne informasjonsflyten, og det krever effektiv kommunikasjon mellom de ulike aktørene. Disse aktørene innebefatter CND-avdelingen, ulike kategorier av brukere/ansatte i organisasjonen, beslutningstagere/sjefer og IKT driftspersonell.

- En felles forståelse av CND-avdelingens kapasiteter, samt det operative behovet for CND-tjenester vil være avgjørende for hvor effektivt CND ressursene kan fordeles.

- Det gjeldene trusselbildet må også kontinuerlig kommuniseres for å sette de ansatte i stand til å detektere og rapportere de hendelser som er av betydning.

Oppsummeringen av de viktigste resultatene må ses i sammenheng med prosjektets tilgang og utnyttelse av informanter fra samme kompetansemiljø. Resultatene kan derfor ikke med godt grunnlag evalueres med tanke på muligheter og begrensinger fra andre avdelinger innen Forsvaret. Spesielt kan det her vises til operative miljøer, og andre avdelinger med et ansvar for informasjonssikkerhet i Forsvaret.

**Kapittelets resultater:**

- Sannsynliggjort hypotese 1
  - Reaktivt, erfaringsbasert handlingsmønster
  - Problemer med å skille ut den målrettede motstander
- Sannsynliggjort hypotese 2
  - Kunnskap om fienden er essensielt for å lykkes og sette dette i sammenheng med en større helhet
  - Det finnes indikasjoner på at fienden kartlegger våre tiltak
- Sannsynliggjort hypotese 3
  - En bevissthetsmodell som gjør organisasjonen i stand til å danne et bedre bilde av motstanderens målsettinger, motivasjoner, kapasitet og metoder kan danne grunnlaget for en forsvarsstrategi
- Indikasjoner på at hypotese 4 er gyldig
  - Organisasjonen har et potensial med tanke på bevissthetsøkende arbeid

# 7 Mulig løsningsforslag

**Kapittelets innhold:**

- Analyserte resultater og litteratur benyttes for å presentere en mulig løsning
- Analyse gjennomførbarhet i Forsvaret
- Policy (P`HAPI)

Et av målene i masterprosjektet var å kunne utarbeide et mulig løsningsforslag. Forskningsdelen av arbeidet har som kjent vært utført innen Forsvaret, der problemeier selv har identifisert og utledet problemstillingen. Vi har som utgangspunkt ment at arbeidet skulle resulterer i et spesifikt løsningsforslag mot en fremtidig implementering i Forsvaret. Vi vil innledningsvis presentere et generelt og overordnet løsningsforslag. Løsningsforlaget er basert på funnene i litteraturstudien sammen med tilfellestudiet. Identifiserte nøkkelfaktorer fra arbeidet, og faktorer som anses som essensielle å ta hensyn til ved en eventuell implementering blir beskrevet.

## 7.1 Bakgrunn for løsningsforslagene

Problemeier viser til ønske om en mer effektiv utnyttelse av tilgjengelige IS-ressurser samt i større grad å kunne forvare egne informasjonssystemer mot den reelle og målrettede trusselaktør. At organisasjonen står ovenfor en målrettet trusselaktør er sannsynliggjort gjennom svar og analyse av spørsmålene 6,7 og 8 fra intervjurunde 1. Her viser informantene en gjennomgående oppfatning av at motstandere bedriver informasjonsinnhenting om oss, bedriver kartlegging av våre beskyttelsestiltak og tilpasser sine angrep deretter.

Fiendeforståelsen blir i litteraturen beskrevet som essensiell for utfallet i en hver konkurranseutsatt situasjon. Egen forskning indikerer at nøkkelen for en effektiv og dynamisk tilpasning av tilgjengelige IS-ressurser ligger i fiendeforståelsen og et oppdatert trusselbilde. For Forsvarets organisasjon sannsynliggjøres dette gjennom informantenes svar på spørsmålene 9,10 og 11 fra intervjurunde 1, der kunnskap om fienden/trusselaktører er svært viktig. Problemet ligger i dynamikken i fiende- og trusselbildet, hvilket indikerer at det er behov for kontinuerlig å tilpasse forsvaret av eget informasjonssystem i takt endringen i trusselsituasjonen mot egen organisasjon. Dette er omtalt av informantene i spørsmål 3 fra intervjurunde 1, der de gir sin vurdering av hvor godt beskyttelsestiltakene er tilpasset et gjeldende trusselbilde. Hovedsakelig omtaler informantene at de ikke er tilpasset i tilstrekkelig grad. Et interessant element fra intervjuene i denne sammenhengen er at det ved flere tilfeller ble ytret at nøkkelen til suksess for den parten som er i forsvar, ligger i å ha tilstrekkelig evne til deteksjon og læring (Spørsmål 5, Intervjurunde 1). En rekke åpne

kilder kan benyttes for å beskrive og frembringe informasjon om kjente trusler og trusselaktører. Den bestemte målrettede trusselaktøren mot egen organisasjon, som vår problemstilling omhandler, vil i liten grad belyses og identifiseres i de åpne kildene. Skal man kunne detektere og lære om hvilke målrettede og aktive trusselaktører egen organisasjon faktisk står ovenfor, vil dette derfor måtte detekteres av sensorer i den enkelte organisasjon. Organisasjonens CND avdeling vil kunne spille en viktig rolle i denne sammenheng ved å benytte egne ressurser og implementerte sikkerhetsmekanismer/sensorer til å overvåke og detektere angrepsforsøk over nettverket. Slike avdelinger vil derfor kunne danne seg et godt bilde av trusselsituasjonen og til enhver tid gjeldende trusselaktører i cyberverden.

Identifiserte problemområder her, er den omtalte reaktiviteten og kompleksiteten i beskyttelsen som gjør at en målrettet aktør ofte vil kunne lykkes med ukjente angrepsvektorer. Det er også utfordrende å skille angrep fra den målrettede aktøren fra de mer tilfeldige angrep. Resultatet fra vår forskning viser at informantene er enige i dette, og at det ligger et stort informasjonspotensial blant ansatte i organisasjonen med tanke på å kunne samle ytterligere verdifull informasjon om den målrettede trusselaktør.

De ansatte spiller en meget viktig rolle i organisasjonens informasjonssikkerhet, ut i fra deres kompetanse, adferd og årvåkenhet (Albrechtsen 2007). Den menneskelige barrieren, er den siste barrieren man kan sette sin lit til, og som kan detektere og unngå at uønskede hendelser skal skje (Albrechtsen 2007). Disse henvisningene ble benyttet i argumentasjonen og som grunnlag for valget av innfallsvinkel til problemet i prosjektet. En suksessfaktor for å kunne oppnå dette er at informasjonssikkerhet gjøres til en del av organisasjonskulturen (R.S. Shaw 2009). Det argumenteres for å drive kontinuerlig IS-utdanning og bevisstgjørende arbeid. Innfallsvinkelen til løsningsforslaget er basert på tidligere arbeid innen emnet IS- bevissthet, og litteratur som gir anbefalinger ved innføring av et IS-bevissthetsprogram.

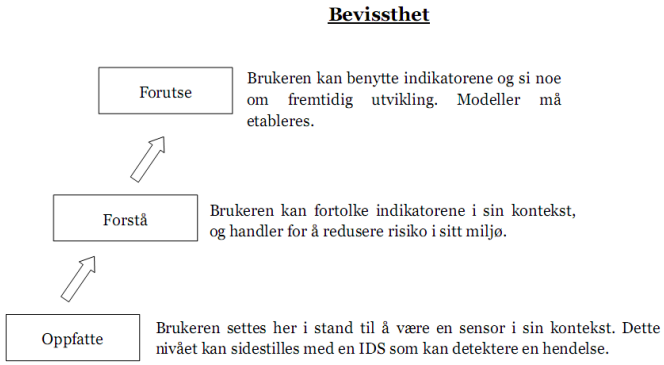
Bevissthetsprogrammet skal muliggjøre og tilrettelegge for at organisasjonens ansatte i større grad kan bli en dynamisk tilpasset trussel- og hendelsesdetektor. Detektoren vil kunne eksistere i alle avdelinger ved ulike nivåer og i de ulike miljøer organisasjonen består av. Denne egenskapen forutsetter at detektoren er tilpasset sine omgivelser og sitt miljø. Det er derfor sannsynlig at detektoren er kapabel til å detektere og identifisere trusler og trusselaktører i en tidlig fase. Sammen med eksisterende tekniske detektorer (IDS, antivirus, brannmurer osv.), vil de ansatte derfor kunne tilføre nyttig informasjon og kunnskap om fienden.

Funn i litteraturen sier at man i et slikt tilfelle kan måle effekten av sikkerhetstiltakene opp i mot organisasjonens sikkerhetspolicy (Hagen 2009). I motsetning til identifisert litteratur, undersøker vårt arbeid derfor potensialet av å skreddersy bevissthetsprogrammet mot å samle informasjonen om fienden. I prinsippet skulle ikke dette være annerledes enn å skreddersy IS-programmet mot å få de ansatte til å følge organisasjonens sikkerhetspolicy. En av utfordringene ved å muliggjøre dette belyses også i egen forskning, nemlig den hurtige endringen og dynamikken i sårbarhet og trusselbildet. Bevissthetsprogrammet må kunne håndtere denne dynamikken. Essensielt for alle typer sensorer er at de må kalibreres og justeres for i

størst mulig grad kunne detektere og rapportere om reelle og interessante hendelser. Det er problematisk om for få hendelser detekteres og rapporteres. Mens det i motsatt tilfelle ikke ønskelig at for mange uviktige hendelser rapporteres da dette også krever ressurser å analysere. Sensorene må derfor tilpasses dette behovet som også vil kunne inneha en viss dynamikk. I rapporten omtaler vi dette med begrepet kalibrering. Nedenfor fremhves det vi anser, men bakgrunn i vår forsking, som sentrale elementer å vektlegge for å oppnå en vellykket implementering av et IS- bevissthetsprogram med de formålene beskrevet i rapporten.

### 7.1.1 Kategorisering av ulike jobbfunksjoners og avdelingers IS-bevissthetsbehov

Litteraturstudien viser til tre ulike nivåer av bevissthet. Disse nivåene er Oppfatte (Perception nivå 1), Forstå (Comprehension nivå 2), å forutse (Projection nivå 3). Vår tilnærming til dette er illustrert i figur 5. Vi referer til denne som bevissthetsstigen.




Figur 5. Bevissthetsstigen

Bevissthetsprogrammet skal hjelpe de ansatte til å ta stegene i bevissthetsstigen. Vårt forskningsarbeid sammen med funn fra litteraturen indikerer at IS- programmet som skal støtte de ansatte på veien, må skreddersys den faktiske situasjonen i organisasjonen, rundt den enkelte avdelingen og om mulig også den enkeltes jobbfunksjon.

Et formålstjenlig bevissthetsprogram må derfor skreddersys mot operasjonsmiljøene organisasjonens avdelinger opererer i. Den enkelte avdeling kan derfor ha sin egen bevissthetsstige tilpasset sitt operasjonsmiljø. Som det fremgår av resultatene fra intervjuene foretatt i prosjektet, her spesielt intervjurunde 2, er det et klart samsvar med dette. Både med tanke på viktigheten av en grunnleggende bevissthetsøkning generelt i organisasjonen, samt at slik opplæring og informasjonsflyt må være tilpasset den enkelte jobbfunksjon, den enkelte avdeling og deres operative miljø. Dette skal muliggjøre en behovsprøvd tilpasning av hvilket bevissthetsnivå ulike kategorier ansatte bør befinne seg i, for å nå et definert mål om bevissthet og kunnskapsnivå. I litteraturen det henvises til i forbindelsen med nivåene i vår bevissthetsstige sier (R.S. Shaw 2009) at det ultimate målet til et bevissthetsprogram er å utstyre brukeren med evnen til å forutse IS-hendelser. Både litteraturen (Valentine 2006) mfl, og egen

forskning (eks andre intervjurunde spørsmål 9.) viser at det er det er behov for differensiering av tiltakene opp i mot ulike personellkategorier og jobbfunksjoner.

Vi argumenterer for at betydningen av dette, sett opp i mot vår bevissthetsstige, er at det sannsynligvis ikke er behov for å utruste alle ansatte med evnen til å forutse, eller neste steg som vil være å forutsi fremtidige IS-hendelser og trusler. Det kan argumenters for at de hendelsene som i så måte er kritiske å identifisere er de IS-hendelser som er initiert av den målrettede trusselaktør eller fiende. I overført betydning vil dette være det samme som å kunne forutse fiendens fremtidige handlinger i Cyberverden. Betydningen av å kunne forutse fiendens fremtidige handlinger reflekteres i sin tur over på evnen til å øke effekten av egne sikkerhetstiltak og ikke minst effektiviteten av egne CND-operasjoner. Evnen til å kunne forutsi fremtidige hendelser vil derfor være ensbetydende med muligheten til den mest effektive utnyttelsen av tilgengelige IS-ressurser. Samtaler med vår strategisk utvalgte ekspert gir informasjon som argumenter for betydningen av dette i militær sammenheng.

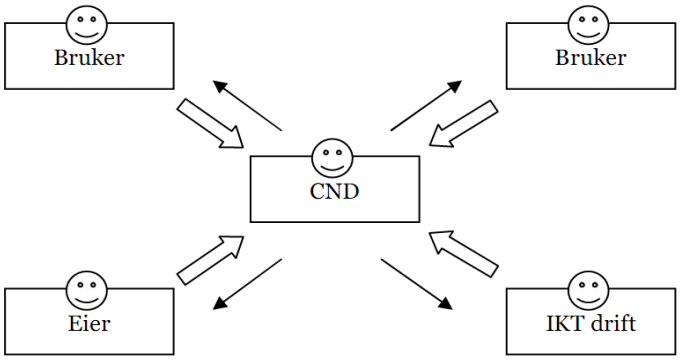
> Sitat ” På samme måte som for øvrige militære kapabiliteter er den operative nytten av CND avhengig av dens evne til å forhindre at fienden lykkes i sine målsettinger og samtidig bidra til å nå egne målsettinger. Av dette ser vi at CND ikke bør avgrenses til en passiv eller parerende kapabilitet, men anvendes aktivt for å nå egne målsettinger.”Sitat slutt

Evnen til å forutse vil derfor kunne begrenses til personer som sitter på de øverste nivåene innen avdelinger som styrer ressursene og prioriterer IS-beskyttelsestiltakene. Beslutningsgrunnlaget eller situasjonsbildet man benytter, vil ved hjelp av bevissthestsprogrammet kunne dannes med informasjon fra de menneskelige sensorer, som supplerer dagens metoder for informasjonsinnhenting. Dette vil sannsynligvis kreve at nye informasjonsinnhentingsplaner utarbeides.

En siste utfordring vi belyser, vil være å besvare hvilke informasjon og indikatorer man vil måtte benytte for å danne det overnevnte situasjonsbildet. Resultatene fra vårt arbeid gir få konkrete innspill til dette i denne sammenheng. Derimot er det avdekket at en gjennomgående egenskap med elementene i problemstillingen (sårbarheter, trusselbildet, fienden m. m) er at det alle er dynamiske. Informasjonsbehovet til det helhetlige situasjonsbildet vil derfor også være dynamisk. Elementene som presenteres i de neste to underkapitlene, fremheves i lys av dette. De skal fange dynamikken og muliggjøre en kontinuerlig kalibrering av de menneskelige sensorer så vel som prioriteringen av implementerte beskyttelses- eller forsvarstiltak.

### 7.1.2 Kommunikasjonsflyt

Vår forskning tilsier at det for CND avdelingen, ligger et stort potensial i å samle verdifull informasjon om fienden i den øvrige organisasjonen. Kommunikasjonsflyten blir identifisert som en nøkkelfaktor ved bevissthetsprogrammet dersom de ansatte i organisasjonen skal kunne bli en trussel- og hendelsessensor. Informasjonsflyten må være slik at informasjonen tilflyter de korrekte beslutningstakere (se figur 6). Beslutningstageren er i dette perspektivet en beslutningstager i CND avdelingen. Pilene indikerer informasjonsflyten. Merk at det i skissen er vist til tre ulike kategorier ansatte. Litteratur og egen forskning tilsier at en rekke organisasjoner vil ha behov for en mer detaljert kategorisering.




Figur 6. Informasjonsflyt mellom sensor og beslutningstaker

Resultatet av vårt arbeid belyser her flere viktige aspekter ved informasjonsflyten. En hver teknisk sensor må konfigureres og tilpasses de hendelser man ønsker den skal detektere. Det samme gjelder for den menneskelige sensoren. Dette vises ved informasjonspiler fra CND til de øvrige kategorier av ansatte. En rekke argumenter tilsier at kommunikasjonsflyt denne veien er den viktigste, spesielt i lys av dynamikken i trusselbildet og sårbarheter. Informasjon om dagens og muligens fremtidige trender i angrepsmetoder kan anses som en "konfigurering og tilpasning" av de ansattes IS-bevissthet, og en metode å skreddersy IS-bevisstheten mot informasjonsbehovet til beslutningstager. Informasjonen må derfor tilflyte de øvrige ansatte. Det vil kunne medføre en økt deteksjon og rapportering av hendelser og angrepsmetoder, og økt rapportering av mulige sårbarheter i systemer og prosesser. Hvilket i sin tur betyr økt informasjon om fienden og en potensielt tidligere deteksjon av aktivitet fra en kjent eller ukjent målrettet trusselaktør.

Kommunikasjonsflytens betydning, skissert her ved vår kommunikasjonsmodell, er derfor den mest grunnleggende og sentrale faktoren for en effektiv og dynamisk kalibrering av de menneskelige sensorer. Det er også essensielt med informasjon som synliggjør hvilken rolle CND avdeling har, og informasjon om hva CND avdelingen kan bidra med, for at den enkelte avdeling skal kunne fullføre sitt oppdrag.

Informantene vektlegger enkelhet i rapporteringsrutiner, og tilbakemeldinger til brukere angående status og positive effekter av deres innmeldte hendeler som viktig for å opprettholde motivasjonen til rapportering fra de ansatte. Sveen et al. (2009) omtaler dette som kvaliteten på behandlingen av innrapporterte hendelser og beskriver at dette har innvirkning på motivasjonen til å rapportere hendelser.

En rekke av informantene som er benyttet i prosjektet tilhører Forsvarets CND-avdeling. Dette har til en viss grad styrt innfallsvinkelen til våre intervjuer, og det viser seg her at informantene omtaler forståelsen og kunnskap om det operative miljøet og behovet som viktig. Det kommer frem at denne kunnskapen er med på å øke deres og avdelingens IS-bevissthet og mulighet til å prioritere egne ressurser og kapasiteter. Informasjon om pågående operasjoner, ulike prioriteringer, hvilke systemer og prosesser som benyttes og hvordan de benyttes, omtales som viktig. Siden en CND

avdeling er til for å støtte de operative avdelinger vil denne type informasjon indikere hvilke verdier som er kritiske eller ikke, og derfor danne grunnlag for å prioritere CNDs ressurser.

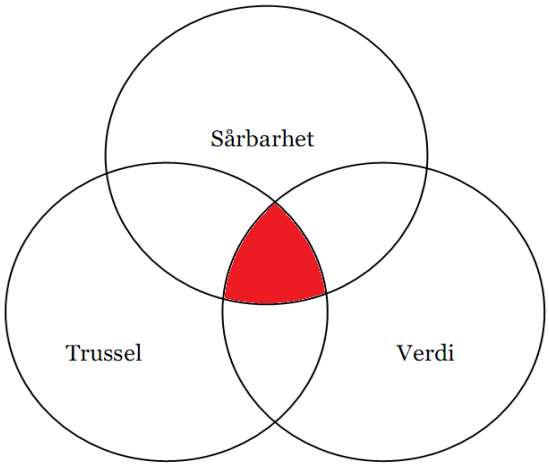
### 7.1.3 En dynamisk beslutningsmodell

Informasjonen som sensorene detekterer sammen med kunnskap om det operative behovet vil øke beslutningsgrunnlaget for tildeling av tilgjengelige IS-ressurser. Her vises det også til tre velkjente begreper innen IS, sårbarheter, trusler og verdi. Vårt arbeid belyser et felles trekk ved disse, nemlig at de er dynamiske og i konstant endring. Dette krever at man kontinuerlig oppdaterer beslutningsgrunnlaget for ressurstildelingen i forhold til den dynamiske endringen i de tre nevnte elementene. Dette vil derfor kreve dynamiske beslutningsmodeller.

En mulig modell som kan benyttes til dette er skissert i figur 7. Modellen er beskrevet som en risiko identifiseringsmodell i (Bass & Robichaux 2001), og refereres til som en adaptiv OPSEC[19] modell i (Chairman of the Joint Chief of Staff 1997). Modellen er enkel og overordnet, men den inneholder grunnlegende elementer innen informasjonssikkerhet, verdi, trussel og sårbarhet. I overnevnte dokumenter er verdi beskrevet som kritisk informasjon. I figur 6 ser vi at det er kommunikasjonskanaler mellom kategorier ansatte og organisasjonens CND avdeling.

Vår forskning viser at de ulike kategorier ansatte sannsynligvis er kapable til å kommunisere ulike typer informasjon. Et eksempel på dette kan være at eier (operativ sjef) kommuniserer hvilke verdier som eksisterer og hva som til en hver tid er kritisk, IKT driftspersonell kan kommuniser sårbarheter, og brukere kan kommunisere informasjon som indikerer ulike trusler eller hendelser. Igjen ser vi at kommunikasjonsmodellen er av avgjørende betydning for muligheten til en effektiv benyttelse av OPSEC modellen. Dette er elementer som er berørt i intervjuene. Generelt er det etablert en forståelse for at den øvrige organisasjonen kan bidra med informasjon som gjør CND bedre i stand til å danne seg sitt fiendebilde, gjennom innrapportering av hendelser etc. Utover dette har intervjuene frembrakt informasjon angående viktigheten av at CND innehar informasjon om organisasjonens operative behov for CND tjenester. Det kan i denne sammenhengen sammenlignes med verdielementet i modellen under (figur 7), da de operative prioriteringene vil være styrende for hva som er ansett som kritisk verdi.

[19] OPSEC – Oprational Security, Operasjonssikkerhet




Figur 7. OPSEC modelen

Av modellen i figur 7 kommer det frem at risiko eksisterer i overlappingen (det merkede området) mellom sårbarhet, trussel og verdi. Størrelsen og fasongen på elementene endres kontinuering. Hvilket betyr at den faktiske risiko organisasjonen står ovenfor er dynamisk, og endres i takt med gjeldende situasjon i de tre andre elementene. Dette viser seg spesielt å gjelde da våre forskningsresultat viser at en rekke organisasjoner potensielt kan stå ovenfor en målrettet og dynamisk tilpasningsdyktig trusselaktør.

Det kan også argumenteres for at OPSEC modellen kan benyttes til ytterligere å lære om fienden. Nettopp ved å gjennomføre korrelasjon av informasjon. Eksemplifisert kan man se for seg en militær operasjon. Den operative sjef har rapportert om kritiske IS-verdier ved ulike deler av en operasjon. Fra planleggingsfasen til gjennomførelse. I samme tidsforløp rapportens ulike IS-hendelser, potensielle sårbarheter og trusler inn via menneskelige og tekniske sensorer. En korrelasjon av denne informasjonen vil derfor potensielt kunne medføre økt kunnskap om fiendes strategier, operasjonelle metode og taktiske/tekniske prosedyrer opp i mot våre strategier og operasjonelle metoder. OPSEC modellen vil derfor kunne ta høyde for tidsaspektet. Den muliggjør en læring om fiendens handlinger opp i mot vår egn evne til å oppnå og utføre våre målsettinger, strategier og operasjonelle metoder.

Et argument i prosjektet er at man besitter en endelig mengde IS-ressurser, og at dette på mange måter taler til fordel for angriperen. På den andre siden sitter angriperen også med en endelig mengde tilgjenglige ressurser, noe som vil utligne fordelen om vi benytter våre tilgjengelige ressurser effektivt.

Nøkkelen til suksess, mener vi, ligger i å være best mulig i stand til å identifisere endringen i organisasjonens risiko. I modellen er det nettopp i kryssingen mellom de overnevnte elementer at beslutningsgrunnlaget for en kostnadseffektiv ressurstildeling eksisterer (merket felt i figur 7). Dersom en beslutningstager skal kunne foreta en kontinuerlig prioritering av sine CND ressurser vil det i dette perspektivet være essensielt å ha en kontinuerlig tilflyt av informasjon som kan beskrive hvor risikoen befinner seg til enhver tid. Prosjektet har gjennom litteratur og intervjuer vist til at den øvrige organisasjonen kan fylle dette informasjonsbehovet.

Modellens egenskaper medfører at den har klare fordeler og ulemper. Modellens enkelhet kan være en begrensning for en praktisk tilnærming, men benyttes her for å danne det konseptuelle grunnlaget i prosjektet. Vektlegging av fordelen med enkelhet og ikke minst overførbarhet til en rekke situasjoner og beslutningsmiljøer (generisk), gjør at vi har tro på dens relevans inne prosjektarbeidets perspektiv.

## 7.2 Kort analyse av status i Forsvaret

Resultatene av vårt arbeid har til nå blitt benyttet til å argumentere for sentrale faktorer som må legges til grunn for å kunne realisere en IS-strategi der den menneskelige barrieren tillegges større oppmerksomhet. Et utvidet bevissthetsprogram skreddersydd mot organisasjonen skal muliggjøre dette. Innledningsvis i kapittel 7 ble det vist at vi ønsket å benytte resultatene av vår forskning til å anbefale et mer spesifikt løsningsforslag spisset mot Forsvaret, og Forsvarets behov. Hypotese 4 med forskningsspørsmål reflekterer i stor grad dette. Grunnet en rekke faktorer og begrensinger, beskrevet i kapittel 6.5, gjør det vanskelig og utarbeide et mulig implementerbart løsningsforlag spisset mot Forsvaret. Videre forskning og fremtidig arbeidet kreves før dette er mulig. Like fullt kan vårt arbeid benyttes til å belyse hvilke muligheter og eventuelt begrensinger som eksisterer innen Forsvaret i dag. I arbeidet med dette delkapittelet har vi derfor utført en overordnet analyse av eksisterende mekanismer i Forsvaret. Dette blir benyttet til å antyde om de identifiserte nøkkelfaktorer fra litteraturen og i egen forskning enkelt kan oppnås innen Forsvaret. Forbedringspotensialer blir også belyst.

Denne analysen konsentrer seg om overordnet status og forsøker å danne et statusbilde opp mot de identifiserte nøkkelfaktorer fra litteraturen.

### 7.2.1 Forsvarets informasjonssystem

Forsvaret har et felles informasjonssystem, FisBasis B, som alle ansatte har tilgang til. I tillegg til å være Forsvarets primære informasjonssystem, et arbeidsverktøy de nødvendige kontorstøttefunksjoner, er FisBasis B Forsvarets primære informasjonskanal. Ansatte får her tilgang til forsvarets intranettsider, hvor nyheter og informasjon om Forsvarets respektive avdelinger publiseres. Brukerstøttefunksjoner og innmelding av feilmeldinger kan gjøres elektronisk via disse intranettsidene. Prosjektgruppen har gjort en innledende analyse av tilgjengelig informasjon relevant for masterprosjektets problemstilling, og identifiserte nøkkelfaktorer fra Aetna studien (Wright & Kakalik 2006).

### 7.2.2 Sikkerhetsinformasjon

På FisBasis B kan brukeren enkelt få tilgang til sikkerhetsinformasjon via en snarvei på arbeidsstasjonens oppgavelinje. Informasjonssidene inneholder brukerinstrukser til ulike informasjonssystemer som benyttes i Forsvaret. Linker til lover og regler med tilhørende forskrifter og linker til lokale sikkerhetsorganisasjoner. I tillegg til dette publiseres relevante nyheter og sikkerhetsinformasjon på intranettsiden til Forsvarets sikkerhetstjeneste. En rekke av artiklene som publiseres fremstår som informative og kunnskapshevende med hensyn til lesernes IS-bevissthet. Den enkelte ansatte virker derfor enkelt å kunne få tilgang til denne type sikkerhetsinformasjon via en sentral informasjonskanal. Imidlertid er informasjonen hovedsakelig publisert på to ulike

steder. Skillet virker å være på generell sikkerhetsinformasjon og arbeide på Forsvarets Sikkerhetstjeneste (FOST) sine sider, og informasjon som går spesifikt på bruken og drift av de respektive informasjonssystemer på "sikkerhetsinformasjon" sidene. Denne informasjonen har også kommet frem under våre intervjuer, og det vises til at dette er CND avdelingens metode for og informere de ansatte om alt fra direktiver til trender i angrepsmetoder.

### 7.2.3 Sikkerhetsrapportering

På intranettsidene til FOST finnes informasjon om, og direktiv for sikkerhetsrapportering. Direktivet for sikkerhetsrapportering gir retningslinjer for hvordan sikkerhetsrapporteringen skal utføres i praksis. Det vises til ulike forhold som skal rapporteres. Her stadfestes det at observasjoner, hendelser eller mistanke om hendelser som kan indikere alt fra etterretningsvirksomhet og undergravingsvirksomhet til sårbarheter i elektroniske informasjonssystemer og rutiner skal rapporteres. Det vises også til hvilke rapportertingslinjer som skal benyttes. Rapporteringslinjene varierer til en viss grad ut i fra type hendelse og hvilke avdeling hendelsen rapporteres fra. Sikkerhetsrapportenes første kontaktpunkt, etter den rapporterende, er avdelingens lokale sikkerhetsleder/offiser. Den lokale sikkerhetslederen har videre ansvar for å prosessere sikkerhetsrapporten gjennom kommandolinjen(e). I prosjektets perspektiv er det viktig å understreke at alle sikkerhetsrapporter av denne typen meldes inn til FOST.

Et generisk rapporteringsskjema/mal som skal benyttes til alle typer hendelser det henvises til over. Rapporteringsskjema er delt i to, del en fylles ut av rapporterer, mens del to fylles ut av overordende myndighet i rapporterende avdeling eller på vegne av autoriserende sjef. På informasjonssidene vises det til at malen gjør at rapporten skal bli skjematisk oppbygd, samt at det stiller krav til utfyller med tanke på detaljer og vurderinger.

I sammenheng med dette ble det gjort en analyse av hvilke retningslinjer eller informasjon som er publisert rundt dette på sikkerhetsinformasjonssidene. På lik linje med tidligere gis brukeren her mer spesifikk informasjon mot håndteringen av sikkerhetsbrudd og hendelser i informasjonssystemene (eksempelvis FisBasis B). Retningslinjene viser i sin tur til de samme rapporteringsrutiner og skjema det er henvist til tidligere. FOST får dermed i en tidlig fase også informasjon om hendelser relatert til informasjonssystemene.

### 7.2.4 Forsvarets organisasjon

FOST som organisasjon er kommandomessig underlagt sjefen for Forsvarsstaben med direkte linjer til Forsvarssjefen. Sikkerhetslitteratur viser nettopp til at en suksessfaktor for å gjøre sikkerhetsarbeidet vellykket er at lederen bør være lokalisert i organisasjonens øvre ledelse, dette for å sikre kontinuerlig støtte fra ledelsen. Organiseringen viser i så måte at dette er anerkjent i Forsvaret. Vi ønsker ikke å debattere for organisatorisk tilhørighet for personell som skal utvikle og drive et bevissthetsprogram. Men ut i fra en av de identifiserte nøkkelfaktorer også i Aetna (Wright & Kakalik 2006), ville en enkelt kunne oppnå den anbefalte organisatoriske tilhørigheten dersom de ble en del av eksempelvis FOST.

### 7.2.5 Forsvarets opplæringsportal

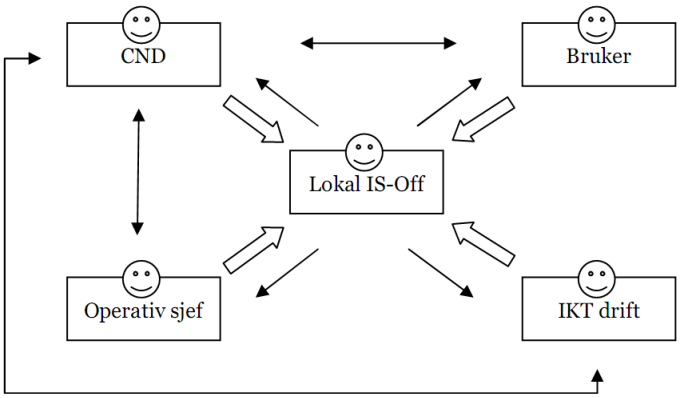
Elektroniske opplæringsprogrammer og tester er allerede implementert på FisBasis gjennom forsvarets opplæringsportal. Det er tilrettelagt for at brukere selv kan melde seg på ønskede ekurs. I tillegg er det en del obligatoriske kurs og tester som må gjennomføres og bestås før brukeren får tilgang til ulike typer applikasjoner. Et eksempel kan være skreddersydde elektroniske opplæringsprogrammer mot kontorverktøy som Word og Excel eller årlige tester i kunnskap innen sanitet, minebevissthet m.m.

## 7.3 Delkonklusjon

Analysen er utført på publisert informasjon på FisBasis B, og det er kun benyttet tekstkilder. Analysen viser i at en rekke tekniske mekanismer som må ligge til grunn for et helhetlig IS-bevissthetsprogram allerede er implementert, og eksisterer. Den viser at enkelte organisatoriske faktorer også ligger til rette. Sistnevnte vil ikke utbroderes og arbeides videre med i denne rapporten, spesielt med hensyn til sensitivitetsproblematikken. Likevel kan det her konkluderes med at man kan oppnå tilstrekkelig myndighet og kontinuerlige støtten av ledelsen om man implementerer de ansvarlige for IS-bevissthetsprogrammet korrekt i organisasjonen. Litteraturen anbefaler å benytte en rekke metoder for å oppnå et vellykket IS-bevissthetsprogram, hvilket er mulig med dagens løsninger og struktur innen Forsvaret. Informasjon kan spres via felles epostsystemer, via en sentral intranettside, eller ved hjelp av IS-kampanjer. Informantene meddeler at CND avdelingen i dag har mulighet til å tilby konkret IS-informasjon og kurs til ulike typer avdelinger. Dette kan spisses mot den enkeltes avdelings oppdrag og systemer.

Videre eksisterer tekniske løsninger som muliggjør elektroniske IS-kurs, og tester/ prøver. Gjennom dette kan man sikre kontinuitet i kompetansen, og oppnå målbare resultater gjennom obligatoriske tester for alle ansatte og ulike kategorier ansatte. Data kan benyttes til å identifisere hvilke bevisstgjørende tiltak som har mest effekt og er mest kostnadseffektive.

Det viser seg at den enkelte avdeling har jobbfunksjoner direkte rettet mot sikkerhet. Det er allerede utarbeidet ulike sikkerhetskurs og målrettet utdanning for denne kategori ansatt. Opplysninger tilsier også at forholdene ligger meget godt til rette for at denne kategorien ansatte kan skreddersy et IS-bevissthetsprogram mot den enkelte avdelings operasjonsmiljø. Vår kommunikasjonsmodell kan derfor tilpasses disse egenskapene ved forsvarets organisasjon. Figur 4 viser en skisse av vårt forslag.




Figur 8. Kommunikasjonsmodellen tilpasset Forsvarets egenskaper.

I figur 8 har den lokale IS offiseren blitt sentralt plassert. I det henseende å være ansvarlig for å skreddersy bevissthetsarbeidet mot avdelingens situasjons- og operasjonsmiljø. Samtidig kan offiseren opptre som et bindeledd i kommunikasjonsflyten. CND har i tillegg direkte kommunikasjon med de ulike aktører, med mulighet for å spre viktig eller generell informasjon og ikke minst få direkte tilbakemeldinger eller rapporter om viktige hendelser.

Viktigheten av dette blir belyst i vårt arbeid gjennom både litteraturstudiet og egne forskningsresultater. Dagens situasjon er slik at den enkelte ansatt i denne type stillingskategori selv må ta initiativet og oppsøke denne type kurs og utdanning. For å sikre et generelt og helhetlig kompetansenivå i Forsvaret, er det derfor nødvendig å spesifisere kurs og kompetanse krav i stillingsbeskrivelser, samt ansvarsområder i ulike stillingsinstrukser.

Utover dette er det ikke utført konkret arbeid mot å identifisere ulike kategorier ansatte og hvilke kompetanse eller kunnskapsnivå den enkelte kategori bør befinne seg på. Det refereres her til bevissthetsstigen (figur 5), som kan benyttes som referanse i arbeidet med å differensiere og identifisere de ulike kategoriene ansatte og de ulike krav til den enkelte kategori.

Forskningsresultatet viser at det mest sentrale elementet ved en implementering og strategiendring basert på beskrivelsen i prosjektet er kommunikasjonslinjer og informasjonsflyt. Her ligger et stort forbedringspotensial innen Forsvaret, og det virker nødvendig å etablere egne fora for dette arbeidet. Et stikkord i denne sammenheng er informasjonsdeling. Data fra intervjuene indikerer at det allerede er iverksatt en rekke prosesser mot dette, og ikke minst se på en nyere tilnærming til metoder for kunnskap og informasjonsledelse.

Informasjon i dette delkapittelet indikerer at det med relativt enkelt grep kan implementeres et bevissthetsprogram i Forsvaret, hvor en rekke av de identifiserte suksessfaktorer oppfylles. Fremtidig arbeid er påkrevet for å identifisere ulike personellkategorier og hvilke kompetanse eller bevissthetsnivå de ulike kategoriene bør inneha, samt forbedre kommunikasjonsflyt. Det er også identifisert data i dette kapittelet som kan benyttes til å indikere svar på forskningsspørsmål 4.1 og 4.2 samt

gyldigheten av Hypotese 4. Det er åpenbare positive effekter av å implementere et helhetlig IS-bevissthetsprogram i Forsvaret. Det vil øke robustheten til den menneskelige barrieren og medføre økt informasjonssikkerhet.

**Kapittelets resultater:**

- Kategorisert og tilpasset bevissthetsøkning, gjennom et målrettet og dynamisk bevissthetsprogram
- Opprettelse av effektiv og formålstjenlig kommunikasjonsflyt
- Opprette en felles situasjonsbevissthet som kontinuerlig integrerer IS-arbeidet i en operativ sammenheng
- Det foreligger tekniske og organisatoriske forhold i Forsvaret som legger grunnlaget for at løsningen er gjennomførbar.

# 8 Sammendrag og avsluttende kommentarer

**Kapittelets innhold:**

- Sammendrag av prosjektets resultater og kommentarer
- Vurdering av forskning og metodevalg, i forhold til troverdighet, bekreftbarhet og overførbarhet
- Videre arbeid

Prosjektet har gjennom forskningen forsøkt å sannsynliggjøre de hypoteser som er fremsatt. I hovedsak er det etablert en forståelse for at problembeskrivelsen er gyldig, generelt sett og innad i organisasjonen. Således knytter det seg liten usikkerhet til påstanden om at organisasjonen står ovenfor reelle målrettede trusselaktører, samt at dagens metoder for beskyttelse ikke er optimal for å håndtere denne trusselen. Videre er det diskutert og undersøkt andre strategier for å være bedre rustet for dette. De påstander som er fremsatt med tanke på dette, å benytte seg av bevissthetsøkning generelt i organisasjonen som videre kan gi CND avdelingen økt fiendeforståelse, er derimot ikke bevist som det eneste rette. Det er derimot sannsynliggjort at dette kan være fornuftig å undersøke videre. En overvekt av informantene belyser at den generelle kunnskapen og bevisstheten, med tanke på informasjonssikkerhet, er en av de største utfordringene informasjonssikkerheten i organisasjonen står ovenfor.

Dette prosjektets innfallsvinkel er i utgangspunktet basert på en økt forståelse og kunnskap av en målrettet motstander i cyberspace. Prosjektarbeidet har hatt dette som hovedmål, men undersøkelser har vist at måten en CND avdeling danner seg dette fiendebildet er komplekst og sammensatt. Prosjektet har vært konsentrert om undersøkelser angående i hvilken grad denne kunnskapen kan finnes i den øvrige organisasjonen og om CND kan nyttiggjøre seg av dette for å danne sitt fiendebilde. Denne sammenhengen er sannsynliggjort i løpet av prosjektarbeidet, og denne innfallsvinkelen har gjort at det er identifisert faktorer og utfordringer som må ligge til grunn dersom dette skal være gjennomførbart. Spesielt ble viktigheten av å etablere egnede kommunikasjonskanaler og rutiner, spesielt vektlagt blant informantene.

Det kan derfor være store fordeler med en generell bevissthetsøkning, selv om en ikke fokuserer spesifikt på CND avdelingens fiendebilde, slik det er gjort i dette prosjektet. I dette perspektivet er det heller ikke prosjektgruppens hensikt at organisasjonen skal konsentrere seg fullt og helt om den målrettede trusselen, da denne samlet sett kan stå for en liten del av den samlede trusselen. Den risikoen en kontinuerlig står ovenfor som ikke kan betegnes som målrettet (ofte omtalt som ”støy” i rapporten) vil selvsagt være svært viktig å beskytte seg mot. Det er derimot etablert en forståelse for at målrettede trusselaktører eksisterer og at de potensielt kan gjøre stor skade, gjennom de egenskapene som er belyst.

Prosjektet har benyttet de metoder som er beskrevet for å undersøke relevante temaer og gyldigheten av de fremsatte hypoteser. Som forskning vil prosjektets resultater måtte vurderes med tanke på de begrensinger det har vært underlagt. Dette gjelder både med tanke på metodevalg og implementasjon av disse, men også ressurs- og tidsmessige begrensinger. Den forskningen som er basert på litteraturstudier er gjennomført innen de rammer prosjektet var underlagt og det er vurdert at dette har frembrakt et dekkende bilde av hva som fantes av tidligere relevant arbeid. Imidlertid vil det kunne knyttes noe usikkerhet til at det kan være tidligere gjennomført studier og forskning som ikke er identifisert og dermed ikke tatt hensyn til. Den delen av forskningen som er basert på kvalitative forskningsintervjuer ble gjennomført iht. anbefalinger slik det er dokumentert. Imidlertid vil det være knyttet noe usikkerhet til slik type forskning med tanke på tilfeldigheter og subjektive vurderinger fra informantene. I tillegg vil denne metoden kreve innpass hos den organisasjonen en undersøker slik at en får tilgang til de informantene en ønsker. Dette kan være tidkrevende og kan gå på bekostning av de utvalgskriteriene en har satt for informantene. På den annen side er det en effektiv metode for å frembringe relevant informasjon når informanter med ekspertkompetanse er identifisert og intervjuet.

Det er beskrevet i prosjektets metodedel at forskning og resultater gjennomføres etter de prinsipper som er presentert i tabell 1 (s. 26). De kvalitative begrepene fra tabellen, og som prosjektet er underlagt er gjengitt under. Det er med dette vurdert i hvilken grad prosjektet forskning og resultater er i henhold disse anbefalingene, som en vurdering av forskningens kvalitet (Lilledahl & Hegnes 2000).

*Troverdighet:* Fremgangsmåten benyttet i prosjektet ble hovedsaklig valgt på bakgrunn av to faktorer. Kvalitative undersøkelser basert på ekspertuttalelser er en effektiv form å innhente data, der tid og ressurser utgjør en begrensning i prosjektet. Prosjektet har med denne metoden identifisert nøkkelpersonell ved hjelp av portåpnere i organisasjonen, og hentet informasjon fra disse på en tidsmessig rask og effektiv måte. Videre er metodevalget begrunnet i at undersøkelsene var av slik art at det var påkrevet med informanter som i utgangspunktet var kompetente til å uttale seg om emnene i prosjektet. Forfatternes posisjon i den aktuelle organisasjonen har også bidratt til effektiv datainnhenting. Fremgangsmåten er således gjennomført og dokumentert etter de anbefalinger som er gitt, slik at det skal være mulig for leseren å følge hvert trinn i prosessen. Det er forsøkt sikre konsistens i rapporten på en reflektert måte gjennom en kontinuerlig vurdering av styrker og svakheter med metoden, samt å belyse de motsetninger som er identifisert i forskningen. Prosjektets forslag til løsning er forsøkt begrunnet på bakgrunn av de resultater forskningen har frembrakt. Videre er dette satt i sammenheng med den aktuelle organisasjonen for å begrunne gjennomførbarhet og troverdighet.

*Bekreftbarhet:* Vurderingen av denne faktoren baseres på om de resultater, konklusjoner og tolkninger som er funnet i prosjektet, kan bekreftes av annen forskning. Datainnhentingen som er basert på ekspertuttalelser vil i en viss grad være preget av informantenes subjektive vurderinger. I lys av informantenes anonymitet kan det være at å etterprøve forskningen og oppnå de eksakt samme resultatene ikke lar seg gjennomføre fullt ut. I tillegg kan rammene rundt forskningen betraktes som unike med tanke på tidsrom, miljø etc., samt at resultatene kan være preget av

forskernes egne tolkninger. Allikevel er det i stor grad vist til sammenfallende svar og funn, både fra de ulike informantene og den litteraturen som er identifisert og beskrevet. Derfor vurderes det slik at bekreftbarheten på forskningen er oppnådd i den grad som er akseptabelt. Dette er sikret gjennom rapporten ved å beskrive fremgangsmåte og resultater på en kritisk måte ved å vurdere feilkilder og/eller faktorer som kan ha påvirket forskningen. Den høye graden av konsistens i ekspertuttalelser og øvrige forskningsresultater styrker bekreftbarheten i forskningen. Prosjektets forslag til løsning er utformet etter en begrunnet tolkning og analyse av de resultater forskningen har frembrakt. Allikevel er løsningsforslaget i stor grad basert på subjektive tolkninger av prosjektgruppens medlemmer og valgt eksperter. Således vil bekreftbarheten med tanke på løsningsforslaget være preget av dette og må sees på som et forslag, og ikke som den ene rette løsningen. Annen forskning vil kunne vektlegge andre faktorer og løsningen må sees i lys av dette.

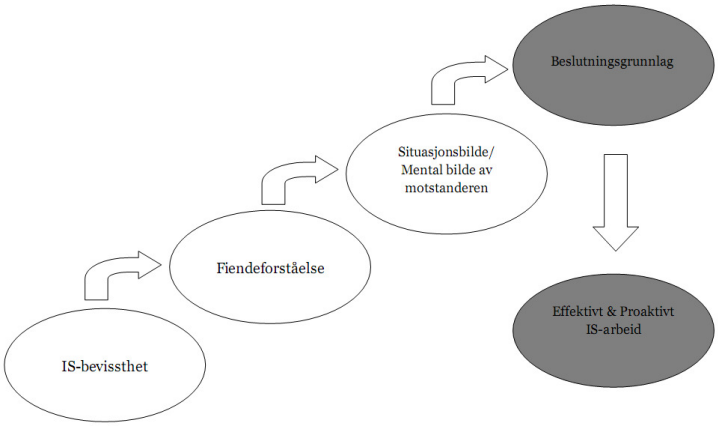
*Overførbarhet:* Problembeskrivelse og inspirasjon til prosjektet stammer fra forsvarets organisasjon. I tillegg er en stor del av forskningen/datainnhentingen gjennomført som en tilfellestudie i Forsvaret. Det er allikevel naturlig å tro at de problemstillinger som er presentert i dette prosjektet har stor overføringsverdi for andre organisasjoner, både andre statlige instanser og private organisasjoner. Således er det videre forsøkt i stor grad å omtale emnene på en generell måte, og ikke kun i Forsvarets kontekst. Slik det er beskrevet omhandler prosjektet den delen av risikoen som stammer fra målrettede aktører. Dersom det kan vurderes slik at det finnes en risiko for at målrettede trusselaktører vil utføre et angrep mot organisasjonen, og at dette kan ha så store konsekvenser at risikoen bør reduseres, vil innfallsvinkelen i prosjektet i utgangspunktet være gjeldende. Som eksempel er det nærliggende å trekke frem industrispionasje etc. Således er prosjektets temaer og resultater ikke ment å være spesialiserte for Forsvaret, men overførbare ovenfor andre organisasjoner og kontekster. Dette perspektivet er forsøkt ivaretatt gjennom arbeidet ved å ha en åpen og generell utvalgsstrategi ved valg av informanter, samt at intervjuene er gjennomført uten å legge de spesifikke egenskapene ved organisasjonen til grunn. Imidlertid er det i rapportens sammenfalling av resultater trukket frem faktorer som kan betegnes som spesifikke for organisasjonen. Dette forsvares gjennom at det er forsøkt å bidra til en mer spesifikk og interessant konklusjon for Forsvarets som problemeier, samt å belyse spesifikke faktorer som krever videre forskning for organisasjonen. Uavhengig av den kontekst temaet vurderes i, vil ytterligere forskning og undersøkelser måtte finne sted. Dette er utdypet noe i kapittel 8.1, Videre arbeid. Dette er i hovedsak begrunnet i at hovedelementer i prosjektet baseres på at faktorer må undersøkes i hvert enkelt tilfelle, og tilpasses den enkelte organisasjon og det miljøet den til enhver tid opererer i. Generelt sett kan prosjektets forslag til løsning være relevant også i andre sammenhenger. Allikevel kan det være egenskaper ved Forsvaret som gjør at deler av det som er presentert ikke kan overføres direkte til andre sammenhenger, eller som bør vektlegges mer eller mindre.

Det var i utgangspunktet en ambisjon for prosjektarbeidet om å gjennomføre en mer detaljert undersøkelse med tanke på implementasjon av de omtalte prinsippene, i Forsvaret. Dette viste seg å være for tidkrevende, men vi håper at konklusjoner fra dette arbeidet kan danne et grunnlag for videre studier og en eventuell innføring av

nye prinsipper for informasjonssikkerhet generelt og hvordan CND danner sitt fiendebilde spesielt.

## 8.1 Videre arbeid

Arbeidet som er gjort i dette prosjektet kan oppfattes spesifikt med tanke på innfallsvinkel og hensikt. Det er funnet indikasjoner som viser at prosjektets overordende arbeidshypotese det kan være hensiktsmessig innfallsvinkel til løsning på problemet. Da nøkkelen til et proaktivt IS-arbeid og en vellykket utnyttelse av ressursene ligger i et oppdatert og korrekt beslutningsgrunnlag (figur 9). Vi presenterer derfor avslutningsvis vår illustrasjon (figur 9), og benytter denne til å henvise til hvor vi anbefaler videre arbeid og forskning.




Figur 9. Prosjektarbeidets overordnede arbeidshypotese versjon 5

Prosjektarbeidet har i sin helhet inkludert personell som til daglig arbeider med ulike emner innen informasjonssikkerhet, og har sitt hovedfokus på dette. Som prosjektet har kommet frem til er IS-arbeidets effektivitet for organisasjonen, svært avhengige av at det etableres kommunikasjon og samarbeid med de øvrige deler av organisasjonen.

Spesielt viktig vil være å fortsette vårt arbeide og samle data rundt muligheter og utfordringer innen andre avdelinger i Forsvaret. Personell med fagfelt utenfor det rent informasjonssikkerhetsmessige feltet må derfor involveres. Det er sannsynlig at det her eksisterer en rekke utfordringer som må løses før en fremtidig implementering og realisering av prosjektets innfallsvinkel skal være mulig. Fremtidig arbeid og prosjekter må derfor utføres for å kunne identifisere utfordringer og muligheter i andre miljøer og avdelinger i Forsvaret. Spesielt bør det vektlegges å identifisere muligheter og begrensinger ved deling av kritisk informasjon blant operative avdelinger. Det kreves også fremtidig arbeid for å identifisere potensialet ved et tettere samarbeid mellom ulike avdelinger med ansvarsområder innen sikring av informasjon og informasjonssystemer. Dagens lovgivning kan være et nøkkelord og en begrensning i denne sammenheng.

Videre vil arbeidet med dette temaet kreve grundigere undersøkelser og tilpasninger til de ulike elementene ved organisasjonen. De suksessfaktorene som er identifisert i prosjektet vil måtte tilpasses og implementeres for å nå ønskede mål. Spesielt vil en

tilpasning og kategorisering av de ulike avdelinger og personellkategorier undersøkes grundig for å kunne skreddersy en formålstjenlig IS-bevissthetsprogram. Dette danner som kjent grunnelementet i vår tankerekke (se figur 9)

Til sist belyses behovet for forskning som kan identifisere og gi en detaljert beskrivelse av hvilke informasjon som kan danne et tilfredsstillende bilde av den målrettede trusselaktør. Dette utgjør situasjonsbildet og det mentale bildet av fienden i figur 9. Det er også behov for arbeid som kan identifisere andre kritiske elementer som må tas hensyn til i beslutningsgrunnlaget (figur 9), og som kan påvirke proaktiviteten i IS-arbeidet.

**Kapittelets resultater:**

- Problembeskrivelsen er reell og gyldig
- Forslag til løsning er relevant og interessant, men ikke beskrevet som det eneste rette
- Kvalitative forskningsmessige prinsipper som troverdighet, bekreftbarhet og overførbarhet er vurdert ivaretatt
- Temaet krever videre undersøkelser og forskning

# 9 Forkortelser

CND - Computer Network Defense

CERT – Computer Emergency Response Team

ENISA - The European Network and Information Security Agency

FLO/IKT - Forsvaret Logistikk Organisasjon avdeling for Informasjonsjons- og kommunikasjonstjenester

FK KKIS - Forsvarets kompetansesenter for kommando og kontroll informasjonssystemer

FOST- Forsvarets Sikkerhetstjeneste

FSA- Forsvarets sikkerhetsavdeling

HMS- Helse miljø og sikkerhet

IS- Informasjonssikkerhet

II- informasjonsinfrastruktur

NP- Nondeterministic Polynomial

TTP- Taktiske - tekniske prosedyrer

# 10 Referanser


Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, 26 (4): 276-289.

Albrechtsen, E. (2008). *Friend or foe? Information security management of employees*. Trondheim: Norwegian University of Science and Technology, Thesis No. 2008:101.

Albrechtsen, E. & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers & Security*, 28 (6): 476-490.

Albrechtsen, E. & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security*, 29 (4): 432-445.

Anderson, R. (2001). *Why Information Security is Hard-An Economic Perspective*. Proceedings of the 17th Annual Computer Security Applications Conference, s. 358. 872155: IEEE Computer Society.

Audestad, J. (2005). *Telektronikk 1. Four reasons why 100% security cannot be achieved'. s. 38-47.* Tilgjengelig fra: http://www.telenor.com/en/resources/images/Page_038-047_tcm28-45150.pdf (sist lest: 30.06.2010 )

Baldor, L. C. ( 2009). *Obama announces U.S. cyber security plan President lays out goals for dealing with threats, will name 'cyber czar'*: MSNBC, nyhetsartikkel. Tilgjengelig fra: http://www.msnbc.msn.com/id/30998004/ (sist lest: 30.06.2010 ).

Bass, T. & Robichaux, R. (2001). *Defense-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations*. Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE. 64-70 vol.1 s.

Bishop, M. (2007). Teaching for conceptual change in security awareness. *The IEEE Computer Society*.

Botha, R. A. & Gaadingwe, T. G. (2006). Reflecting on 20 SEC conferences. *Computers & Security*, Volum 25 (4): 247-256.

Calder, A. & Watkins, S. (2008). *IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002*. 4 utg.: Kogan Page Ltd.

Chairman of the Joint Chief of Staff. (1997). *Joint Doctrine for Operations Security*, Joint Pub 3-54. http://www.iwar.org.uk/iwar/resources/us/jp3_54.pdf, (sist lest: 30.06.2010 )

ENISA. (2007). Information security awareness initiatives: Current practice and the measurement of success.: PricewaterhouseCoopers LLP / The European Network and Information Security Agency (ENISA).

Fossi, M., Turner, D., Johnson, E.et al. (2010). Symantec Global Internet Security Threat Report Trends for 2009. Volum XV. Tilgjengelig fra: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf (sist lest: 30.06.2010 ).

Hagen, J. M. (2009). *The Human Factor behind the Security Perimeter: Evaluating the Effectiveness of Organizational Information Security Measures and Employees' Contribution to Security,*. Oslo: University of Oslo.

Hopcroft, J. E. & Ullman, J. D. (1969). *Formal languages and their relation to automata*: Addison-Wesley Longman Publishing Co., Inc. 262 s.

Igure, V. & Williams, R. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *Communications Surveys & Tutorials, IEEE*, 10 (1): 6-19.

Jemal H. Abawajy, K. Thatcher & Kim, T.-h. (2008). Investigation of Stakeholders Commitment to Information Security

Awareness Programs. *2008 International Conference on Information Security and Assurance*.

Kott, A. & McEneaney, W. M. (2006). *Adversarial Reasoning: Computational Approaches to Reading the Opponent's Mind*: Chapman \& Hall/CRC.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25 (4): 289-296.

Kvale, S. (1997). *Det kvalitative forskningsintervju*. 1 utg. Oslo: Ad notam Gyldendal. 236 s. s.

Lilledahl, G. & Hegnes, A. W. (2000). *Kvalitativ metode, Forelesningsnotat*. Tilgjengelig fra: http://www.giaever.com/sosiologi/KM.htm#_Toc496898517 (sist lest: 30.06.2010 ).

Malerud, S. (2008). Modelling human social behaviour in conflict environments using complex adaptive systems: Norwegian Defence Research Establishment.

Markoff, J., Sanger, D. E. & Shanker, T. (2010). *In Digital Combat, U.S. Finds No Easy Deterrent*: The New York Times. Tilgjengelig fra: http://www.nytimes.com/2010/01/26/world/26cyber.html?pagewanted=1 (sist lest: 30.06.2010 ).

McAfee. (2009). *Virtual Criminology Report 2009 Virtually Here: The Age of Cyber Warfare* [Rapport]. Tilgjengelig fra: http://resources.mcafee.com/content/NACriminologyReport2009 (sist lest: 30.06.2010 ).

McCoy, C. & Fowler, R. T. (2004). *"You are the key to security": establishing a successful security awareness program*. Proceedings of the 32nd annual ACM SIGUCCS conference on User services, Baltimore, MD, USA, s. 346-349. 1027882: ACM.

McGraw, G. (2002). Managing software security risks. *Computer*, 35 (4): 99-101.

Moxnes, E. (2009). *Presidential address: Diffusion of System Dynamics", System Dynamics Society*. Proceedings of the 27th International Conference of the System Dynamics Society, Albuquerque: Tilgjengelig på: http://www.systemdynamics.org/publications.htm#PresAddresses (sist lest: 30.06.2010 )

NIST. (2003). *NIST Special Publication 800-50, Building an Information Technology Security Awareness and Training Program*. Computer Security Division Information Technology Laboratory: U.S Department of Commerce.

Nunez, Y. F. (2008). *Maximizing an Organization's Information Security Posture by Distributedly Assessing and Remedying System Vulnerabilities*. Networking, Sensing and Control, 2008. ICNSC 2008. IEEE International Conference on. 1148-1152 s.

Patton, M. Q. (2002). *Qualitative research and evaluation methods*. 3 utg. Thousand Oaks, Calif.: Sage Publications. 688 s.

Power, R. & Forte, D. (2006). Case Study: a bold new approach to awareness and education, and how it met an ignoble fate. *Computer Fraud & Security*, 2006 (5): 7-10.

Puhakainen, P. (2006). A design theory for information security awareness. *Faculty of science, department of information processing science, University of Oulu*.

R.S. Shaw, C. C. C., Albert L. Harris, Hui-Jou Huang. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, 52 (1): 8.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, 27 (2-3): 183-213.

Siponen, M. (2001). Five dimensions of information security awareness. *SIGCAS Comput. Soc.*, 31 (2): 24-29.

Sveen, F. O., Sarriegi, J. M. & Gonzalez, J. J. (2008, July 20 – 24). *The Access Problem*. Proceedings of the 26th International Conference of the System Dynamics Society, Athens, Greece.

Sveen, F. O., Gonzalez, J. J. & Sarriegi, J. M. (2009). Incident response and users awareness. *Presented at NISK 2009 Conference*.

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud & Security*, 2006 (6): 17-19.

Winston, L., Monus, P., Cardella, T.et al. (2005, July 17-21). *Modeling Sustainable Organizational Change – Why Did Change at BP Lima Sustain While the Change at DuPont Faded Away?* Conference Proceedings The 23rd International Conference of the System Dynamics Society, Boston. 13 s.

Wright, M. A. & Kakalik, J. S. (2006). *Information Security: Contemporary Cases*: Jones and Bartlett Publishers, Inc.

Yin, R. K. (2008). *Case Study Research: Design and Methods (Applied Social Research Methods)*: Sage Publications, Inc.

**Vedlegg 1.**

# Skriv til informanter.

## Henvendelse til potensielle informanter

**Introduksjon**: Lt. Morten Bye og Lt. Jørgen Skryten Ringstad er studenter på masterstudiet i Informasjonssikkerhet ved Høgskolen i Gjøvik, og skal utføre sin masteroppgave våren 2010. Oppgaven er valgt av prosjektgruppen, og utformet i samarbeid med veiledere fra Høgskolen i Gjøvik og Forsvaret. Den foreløpige tittelen på oppgaven er:

***"En ny informasjonssikkerhetsstrategi***

***– En kasusstudie i Forsvaret"***

Prosjektet skal fokusere på de administrative og konseptuelle forhold som avgjør hvordan tilgjengelige informasjonssikkerhetsressurser blir fordelt. Prosjektet skal i hovedsak fokuserer rundt den reelle, avanserte og ressurssterke cybertrusselen som Forsvaret står ovenfor på sine nettverk. Masterprosjektet skal studere om man, ved å øke sin kunnskap, motivasjon, holdninger angående informasjonssikkerhetsmessige forhold (ofte kalt awareness), kan bedre sin kunnskap og forståelse av fienden, og med dette bidra til et mer proaktivt informasjonssikkerhetsarbeid i Forsvarets organisasjon. Det skal undersøkes om økt bevissthet vil kunne bidra til et mer korrekt bilde av den dynamiske trusselen, slik at man også kan oppnå en mer effektiv utnyttelse av tilgjengelige ressurser. Arbeidet ønsker derfor å danne grunnlaget for en endring av informasjonssikkerhetsstrategien fra en reaktiv beskyttelsesstrategi til en proaktiv forsvarsstrategi, der kvalitetsforbedring fokuseres på selvet problemet, den dynamiske fienden, fremfor resultatet av problemet, tetting av sikkerhetshull.

En viktig del av prosjektarbeidet vil være å innhente korrekt informasjon angående hvordan de nevnte forhold er implementert og fungerer i dag innen Forsvaret, samt hvilke potensialer som eventuelt måtte finnes. Prosjektgruppens valg av metode er i denne sammenhengen blant annet å basere seg på uttalelser fra identifiserte eksperter innen området (Kvalitative forskningsintervju). Informantene blir identifisert ut i fra ekspertuttalelser om hvilke personer, med tilknytning til Forsvaret, som kan inneha nødvendig kompetanse innen de ulike fagdomener relevant for vår problemstilling

**Gjennomføring.** Det er planlagt at intervjuene skal foregå som semistrukturerte samtaler, basert på en felles innfallsvinkel distribuert på forhånd (dette dokumentet). Det vil bli gjort notater under intervjuene som danner grunnlaget for et møtereferat den aktuelle informanten får tilsendt i etterkant. Dette gjør at informanten kan kontrollere at prosjektgruppen har oppfattet riktig budskap og eventuelt komme med tilleggskommentarer/opplysninger. I utgangspunktet gjennomføres intervjuene på informantens tjenestested.

**Gradering/Konfidensialitet**. Oppgavens sluttresultat vil så langt det lar seg gjøre holdes ugradert. Derfor vil graderte opplysninger som eventuelt vil fremkomme av samtaler måtte identifiseres av den aktuelle ekspert.

**Med vennlig hilsen**

Morten Bye

Jørgen Skryten Ringstad

**Vedelegg 2**

## Intervjuguide første intervju runde.

Intervjuguide.

Innledende intervju.

1. Hva anser du som de/den største utfordring(ene) ved effektiv beskyttelse av forsvarets informasjonssystemer?

2. Om man skulle endre noe ved dagens innfallsvinkel arbeidsmetode/strategi, hva mener man burde prioritere?

3. I hvilken grad er syntes du at dagens beskyttelsestiltak er tilpasset et gjeldende trusselbilde?

4. Hvilke informasjonskilder benyttes for å danne trusselbilde og prioritere tilgjengelige ressurser?

5. Hvilke fordeler mener du man har når man skal "forsvare" kontra "angripe" et informasjonssystem?
    b. Hva med angrep kontra forsvar?

   Hvem av partene har, etter din mening, størst sannsynlighet for å lykkes? En angriper eller en forsvarer av et informasjonssystem?

6. I hvilken grad tror du motstanderen samler informasjon om oss, og kartlegger våre beskyttelsestiltak?

7. Hvilke metoder og kilder tror du motstanderen benytter for å samle informasjon om oss?

8. Hvilke angrepsstrategier blir benyttet av fienden?
    a. Er det mulig at fienden tilpasser sine angrepsmetoder ut i fra hvilke beskyttelsestiltak vi har gjennomført?

9. Hvilke kunnskap/ informasjon mener du er viktig å kunne tilegne seg for å utøve et effektivt forsvar av et informasjonssystem?

10. Hvilke informasjon/kunnskap tror du øker din egen årvåkenhet og situasjonsbevissthet? (primært i for å kunne detektere, forsvare/avverge et angrep)
    a. Hva med avdelingens årvåkenhet?

11. Anser du din kunnskap om fienden(angriperen) som viktig?
    a. Hvorfor/hvorfor ikke

12. Hva slags informasjon må til for å skape en organisasjon som kan tilpasse sitt cyber-forsvar (CND) mot en dynamisk trussel/trusselbilde?

    a. (Hvilke informasjon kan gi oss et oppdatert og korrekt trusselbilde?)
    b. Tas det hensyn til innrapporterte hendelser ved fordeling av ressurser?
    c. I hvilken grad mener du slik informasjon kan bidra til økt kunnskap om fienden.
    *d.* Hva tror du ville være de viktigste egenskaper ved denne informasjon (Tid, kvalitet, hvem, hva hvor, resultat, m.m)?

**Vedlegg 3.**

## Kategoriserte svar fra første intervjurunde.

1. *Hva anser du som de/den største utfordring(ene) ved effektiv beskyttelse av forsvarets informasjonssystemer?*
    a. **Menneskelige faktorer**
        i. Lite opplæring, manglende kunnskap gir mange brukerfeil/sikkerhetsbrudd
        ii. Manglende felles forståelse av informasjonssikkerhetens betydning i organisasjonen.
        iii. Manglende forståelse og støtte
        iv. Manglende opplæring og forståelse av informasjonssikkerhet
        v. En generell forståelse og forankring for å drive et effektivt informasjonssikkerhetsarbeid i forsvaret
        vi. En generell manglende forståelse i organisasjonen. Sikkerhetspersonell med ansvar er ofte en "lettvekter" i organisasjonen som mangler myndighet og gjennomslagskraft.
    b. **Trusselen i seg selv**
        i. Et komplekst og uoversiktlig trusselbilde gjør det vanskelig å skille ut den målrettede trusselen fra generelt "støy".
        ii. Et komplekst trusselbilde, fienden er overalt, vanskelig å skille mellom fiende og venn.
    c. **Lovgivning**, straffeforfølging er vanskelig, spes på tvers av landegrenser
        i. Store skiller på nasjoners lovgivning angående temaet. Det som er ansett som en forbrytelse her kan være legitimt for andre.
        ii. Sterkt personvern i Norge gjør sikkerhetsarbeidet vanskelig
        iii. Formelle prosedyrer forsinker prosessen fra deteksjon til reaksjon, i for stor grad.
        iv. Sikkerhetsgodkjenning av graderte systemer fører til sårbarheter i seg selv, pga treghet med å godkjenne endringer av konfigurasjon.
    d. **Reaktive beskyttelse**
        i. Manglende forsvarbarhet i infrastrukturen
        ii. Handler kun etter en hendelse har inntruffet, brannslukking.
        iii. Sikkerhetsgodkjenningsregime forsterker det reaktive handlingsmønsteret, pga treghet.
    e. **Teknisk/Systemkonfigurasjon**
        i. Manglende sporbarhet i informasjonssystemer gir ikke mulighet for å følge opp hendelser.
        ii. Manglende utstyr/investeringer.

2. *Om man skulle endre noe ved dagens innfallsvinkel arbeidsmetode/strategi, hva mener man burde prioritere?*
    a. **Menneskelige faktorer**

i. Opplæring / forståelse / bevissthetsbygging
ii. Øke forståelsen for det operative behovet blant sikkerhetsfolk
iii. Menneskelige faktorer, holdningsendringer
iv. Få forankret sikkerhetstenkingen hos ledelsen og samarbeidende parter.

b. **Tekniske midler**
   i. Tekniske begrensinger som "umyndiggjør" brukeren
   ii. Tekniske midler gir falsk trygghet.
   iii. Prioritere sporbarhet i systemene.
   iv. Manglende overvåkning på en del ugraderte nettverk

c. **Lovgivning/regelverk**
   i. Tilgjengeliggjøre regelverket og legge til rette for at det kan følges
   ii. Sikkerhetsgodkjenninger er slik at systemet godkjennes og glemmes. Dette betyr at lovgivning og prosedyrer må tilpasses bedre.
   iii. Øke smidigheten i formelle prosedyrer, for å sikre raskere reaksjon, og bedre posisjonen i informasjonskonkurransen,
   iv. Kutte ut sikkerhetsgradering av informasjonssystemer. Informasjon skal graderes, ikke systemet. Gir interoperabilitet med samarbeidspartnere, i tillegg mindre kompleksitet som gjør det lettere for brukeren å unngå sikkerhetsbrudd

d. **Reaktivitet**
   i. En mer helhetlig tilnærming til deteksjon og reaksjon.

3. *I hvilken grad er syntes du at dagens beskyttelsestiltak er tilpasset et gjeldende trusselbilde?*

***a. Tilpasset:***

i. Til en viss grad, kommer an på hva som er målet. Trenger ikke alltid være slik at en ønsker å stenge en angriper ute hver gang. Slippe den inn for å kontrollere den og lære hva som er hensikten osv.
ii. Dagens tiltak tar oppdager det meste. Tekniske tiltak stopper det meste, mens manuell analyse av personell detekterer en del av restrisikoen.

***b. Ikke tilpasset:***

i. Fagpersonellet vil, men får ikke god nok støtte
ii. Manglende forståelse, naive holdninger, virus og trojanere har fokus, for liten fokus på at det finnes en målrettet trussel som ikke fanges opp.
iii. Tror Norge er dårlig forberedt på en koordinert trussel. Ingen god strategi for å møte en slikt angrep.
iv. En del er klar over trusselbildet, men tiltakene er ikke på plass.
v. Trusselbildet er dynamisk, mens sikkerhetstiltakene kommer som et resultat av erfaring.

vi. Utfordringen i dag er at beskyttelsen stort sett basert på signaturer, henger alltid etter. Dette betyr at noen har oppdaget problemet tidligere. Etterretningsforsøk vil derfor kanskje aldri bli oppdaget fordi det kan skje ved hjelp av metoder vi ikke kjenner til og ikke reagerer på. Et reaktivt handlingsmønster.
vii. Umulig å kunne blokkere alt, pga den reaktiviteten som finnes i de mekanismer som brukes i dag.

4. *Hvilke informasjonskilder benyttes for å danne trusselbilde og prioritere tilgjengelige ressurser?*
    - **a. Åpne kilder**
        i. Virusselskaper, signaturer
        ii. Sikkerhets-communities, prognoser og analyser av hendelser
        iii. Benytter åpne kilder, men de er oftest langt på etterskudd
    - **b. Samarbeidspartnere**
        i. NORCert
        ii. Samarbeidsparter, både i Norge og utlandet, e-tjenesten, NSM pluss andre CERT lignende organisasjoner i Nato.
        iii. Begrenset deling av informasjon innad i Forsvaret.
    - **c. Egne observasjoner**
        i. Drive egen forskning / undersøkelser for å lære.
        ii. Egne sensorer.
    - **d. Generelt**
        i. Er veldig reaktive i den generelle sikkerhetstankegangen

5. *Hvilke fordeler mener du man har når man skal "forsvare" kontra "angripe" et informasjonssystem?*
    - **a. Fordeler med forsvar**
        - **i. Kunnskap om eget system**
            1. Kjenner ditt eget system godt
            2. Kjenner ditt eget system godt, infrastruktur etc, og kan lede angrepet dit det ikke gjør så stor skade.
            3. Kjennskap til systemet, kjenner arkitektur, sårbarheter, egne angrepsvektorer, vha ville jeg gjort? Lære seg forsvar ved å tenke som en angriper
            4. Du kjenner ditt eget system, du vil som angriper måtte kartlegge, noe forsvareren kan oppdage og kan iverksette sine tiltak.
        - **ii. Læring om fienden**
            1. Først detektere fienden og kanskje også finne ut hva han vil. Ut fra svaret finne ut hvor han går videre. Kaste han ut eller vente og se hva han er ute etter. Kan lære av å monitorere hans bevegelser
            2. Kan hende du som forsvarer vil at angriperen skal lykkes med hensikt, for å lære. Informasjonsfortrinnet kan være overlegen ift informasjon, men det kommer an på hvor gode vi er,

vi må sitte med samme kompetanse som angriperen for å finne ut hva han vil

3. Hvis angrepet oppdages, kan forsvareren velge hvilke metoder vi skal bruke, stoppe, kanalisere, eller slippe de inn og lære av hva som skjer
4. Med en forsvarbar infrastruktur vil det være en fordel for den forsvarende part. Du kan se hva angriperen gjør, følge med, selv om han er inne på nettet kan vi observer finne ut om metoder, motivasjon etc, og hvis vi har kontroll på han, vet vi hva som eventuelt er kompromittert.

iii. Som forsvarer er fordelen at dersom man er god nok til å tenke som en angriper, kan utvikle seg til stadighet. Må bli bedre hele tiden.

**b. Utfordringer med forsvar/fordeler med angrep**

**i. Kunnskapsunderlegenhet**

1. Som forsvarer vet du ikke noe om angrepet, hva det innebærer, når det kommer, hva de er ute etter osv.
2. En fordel for angriperen er at han kan bygge opp sitt angrep over tid, planlegge, rekognosere, legge inn bakdører etc.

**ii. Angrepsvektorer/kompleksitet**

1. I angrep trenger du bare finne en feil, mens forsvareren må finne alle.
2. Kan gjemme seg i støy, forsvinner i mengden, de fleste angrep går gjennom nettrafikk, lett å gjemme eg i en enorm mengde av webtrafikk.
3. Kommer an på situasjonen, systemet er stort, mange angrepsvektorer, finnes store muligheter for å komme seg under ”radaren”.
4. Kommer veldig an på situasjonen, og hvordan systemet er. I utgangspunktet er det slik at angriperen har en mulighet til å angripe hvor han vil, mens vi må beskytte alt.

**iii. Tilpasning til situasjon og beskyttelsestiltak**

1. I dag legges exploitet på et sted der brukeren går og henter det selv, vanskelig å detektere at det foregår noe muffens. Dvs lurer brukeren til å initiere angrepet selv, slik at beskyttelsesmekanismer unngås.
2. Angriperen utvikler seg enormt mye raskere, har et stort nettverk. Større økonomisk vinning, og det er kanskje eneste motivasjon, mens eks CND i Forsvaret skal støtte en operasjon, liv og helse.
3. Velge tidspunkt, mål, hvordan, (metode), skjule ditt angrep, legge inn bakdører, samle informasjon. Trenger ikke fysisk tilgang, en operativ setting der du ikke risikerer liv og helse.

4. Norsk personell er naive, og dette kan utnyttes. Benytte seg av dette og dreie angrepene mot personlige mailer etc, som utnytter denne naiviteten/tillitten

6. *I hvilken grad tror du motstanderen samler informasjon om oss, og kartlegger våre beskyttelsestiltak?*
   i. Ja helt sikkert.
   ii. Ja, det er naturlig
   iii. Ja, kontinuerlig

**b. Rekognosering**

i. Ja, vil vite mye om systemet, mye info ligger åpent om systemet, den tekniske delen av det, starte rekognosering senere.
ii. Flere steg, kartlegging (er det ok å bruke resurser på dette?) Hente ut informasjon, kan kreve et større nettverk, trenger hjelp av andre, salg av informasjon
iii. De kartlegger mye, mange legger ut mye informasjon på sosiale nettverk slik at det kan finnes mye her. Samarbeidspartnere legger ut informasjon som kan være sensitiv. Kontrakter etc. Eks studenter i Norge med andre agendaer enn bare studier. Social engineering
iv. Aktøren kan være av varierende type, organisert kriminalitet kartlegger nok ikke så mye, de infiserer flest mulig for å plukke opp informasjon (id, kredittkort info etc), mens en mer målrettet angriper vil tilpasse sine metoder etter de tiltak en har implementert. Men tror ikke dette foregår i omfattende grad.

**c. Reaktiv beskyttelse**

i. Fordelen for angriperen er at det finnes aldri en kur før viruset har vært iverksatt. Erfaringsbasert forsvar er i seg selv et stort problem. Den reaktive måten å beskytte seg på er i seg selv på bakgrunn av at angriperne tilpasser seg.

7. *Hvilke metoder og kilder tror du motstanderen benytter for å samle informasjon om oss?*

**a. Åpne kilder**

i. Drive samling på åpne kilder
ii. Følger med på åpne kilder selvfølgelig.
iii. Kan være åpne kilder.
iv. Internett blir brukt mer og mer, alt skjer etter hvert der, henter ut informasjon fra internett.
v. Åpen informasjon som vi selv legger ut.
vi. Sosiale medier

**b. Social engineering**

i. Social engineering
ii. Social engineering
iii. Social engineering
iv. Kontakte personell direkte (på nett etc.).
v. Ønsker å finne en bruker som har ønskelig informasjon
vi. Humint
vii. insider treath

**c. Tekniske virkemidler**

i. Teknisk; portscan etc..
ii. Teknisk angrep
iii. Teknologi
iv. Prodding mot våre nettverk
v. Eks Portscanning, nettverkskartlegging, det som kan se ut som et tradisjonelt virusangrep i ulike varianter, kan være en kilde for de som rekognoserer. Leser reaksjonsmønstre, leser ut info om systemet, OS versjon, oppdateringsstatus etc.

d. **Kjøp og salg av informasjon**,

i. Finnes informasjonen kan den kjøpes.
ii. Flere land har cyberstrategi, store ressurser, metode er alt etter intensjonen for å finne en inngangsvektor.
iii. Gjøre egne etterretninger.

*8. Hvilke angrepsstrategier blir benyttet av fienden?*

i. Langvarig kartlegging/rekognosering. Når det er utført kommer et raskt angrep.
ii. Vil følge en generell strategi med rekognosering i forkant av et angrep, etc.

*b. Er det mulig at fienden tilpasser sine angrepsmetoder ut i fra hvilke beskyttelsestiltak vi har gjennomført?*

i. Ja helt sikkert, bruker de mulighetene som finnes, er feks ICMP åpent vil en skjule sin kode i ICMP trafikk.
ii. Kartlegger nettverket, maskiner etc., så hvilke porter som er tilgjengelig.
iii. Finnes mange tekniske muligheter som i seg selv sier oss at de tilpasser seg.
iv. Tilpasser seg i den grad at han er målrettet, den rekognosering som er nevnt tidligere er svaret på dette
v. Stor forskjell på avansert fiende og script kiddies
vi. Eks domenet ligger på flere servere, samt bytter IP adresser kontinuerlig for å skape seg redundans. Eksempel på at aktørene tilpasser seg.
vii. Exploit på server osv, brukeren initierer selv at han blir angrepet. Trojanere som er tilpasset og kan brukes til hva en vil. Spredning på USB pinner blir faktisk mer og mer vanlig

viii. Man bruker det som funker, venter med de virkelige sakene til man trenger dem, venter med de nyeste våpnene.
ix. Variere mye fra land til land, hackere, terrorister etc. mål og mening er svært forskjellig. Noen vil ikke være skjult. Vi ser at feks et botnet maribosa, 70 varianter av dette som tilpasses til hva det skal brukes til. Et eksempel på at en trussel tilpasser seg.
x. Ja, endrer metoder også under kartlegging, prodder og ser på resultatet, hvordan vi reagerer.
xi. Det er ikke utenkelig, men kan ikke si det konkret, generelt sett vil det være naturlig, så lenge det er en viss målrettethet i det.
xii. Ja, eks brannmurer, har gjort at klientside angrep har blitt mer vanlig. Samme med zero-day exploits vil omgå dagens mekanismer. Så det tror jeg i stor grad, det er en kontinuerlig utvikling. Eks utviklingen av confickr viruset, skifte av IP adresser og domenegenerering. Det viser at det hele tiden er et våpenkappløp.

9. *Hvilke kunnskap/ informasjon mener du er viktig å kunne tilegne seg for å utøve et effektivt forsvar av et informasjonssystem?*
   a. **Kunnskap om fienden/trusselbildet**
      i. Mye om trusselaktøren og hvilke kapasiteter de besitter
      ii. kjenne fienden
      iii. Hvem fienden er, kunne kartlegge hva den er ute etter, det er essensielt
      iv. Være klar over det trusselbildet som er gjeldende.

   b. **Kompetanse/Utdanning**
      i. Ha kunnskap om angrep av datanettverk,
      ii. Kunnskap om optimal utnyttelse av tekniske midler
      iii. Grunnleggende kunnskap om datanettverk, ip mac, nat , protokoller, etc..
      iv. Følge sårbarhetsbilde, kanskje viktigere en trusselbildet, ikke så viktig hvor det kommer fra
      v. Første grunnkompetanse, blir fort foreldet, men viktig for å bygge videre på. Ikke råd til kurs etc, må ha egne øvelser, lab, inspirasjon fra nett, utdanne oss selv. Må hele tiden tenke nytt
      vi. Informasjonssikkerhetskompetanse er ferskvare, utviklingstrekk, nye systemer som kommer inn, nye sårbarheter, hvordan jobber de andre.
      vii. Generell grunnleggende kompetanse om faget
      viii. Kontinuerlig kompetanseheving, det er ferskvare, viktig og ha mulighet til å oppdatere seg innen fagfeltet
      ix. Grunnleggende utdanning

   c. **Kunnskap om seg selv/egne systemer**
      i. Hva er unormaliteter

ii. Hvilke IP ranger er normalt skumle
iii. Viss oversikt over sårbarheter i de ulike sw en benytter
iv. Kjenne teknologien, hvordan skal det virke, og hvordan har vi og andre funnet ut at det egentlig virker
v. Holde systemer og applikasjoner oppdatert til en hver tid

d. Det viktigste er å knytte kontakter med andre nasjoner, skape forpliktelser. CWID har gitt en del innfallsporter, knyttet relasjoner. Teknisk er vi veldig på høyden. Vi må være flinke med integriteten, skape tillitt og relasjoner.
e. Forsiktighet med hvilke nettsteder en er på.

10. *Hvilke informasjon/kunnskap tror du øker din egen årvåkenhet og situasjonsbevissthet? (primært i for å kunne detektere, forsvare/avverge et angrep)*

**a. Situasjonsbevissthet, kunnskap om fienden og informasjonsutveksling**

i. Kunnskap om operative hendelser, sammenhenger mellom fysiske og virtuelle hendelser.
ii. Holde seg oppdatert på hva som skjer i samfunnet, holde seg oppdatert på trusselbildet, hvem er på frammarsj. Bruker mye åpne kilder, hva skjer, hvem står bak, få en bedre forståelse av hva som skjer. Henger ofte sammen med andre ting i samfunnet som skjer. Eks dagbladet blir angrepet etter karikatur. Estland-saken er et godt eksempel.
iii. All info om noe som er unormalt er viktig, utfordringen er å få samlet all informasjon på et sted. Alle varsler om at noe er unormalt. Som forsvarer/ CND, viktig med informasjon/tilbakemeldinger fra organisasjonen
iv. Operatørene klarer å sette informasjonen i sammenheng. Da et angrep skjer, må vi kunne si hvilke konsekvenser dette har. Dette betyr at det kanskje aldri er to streker under svaret. Når noe skjer må det være en kraftsamling, fordele søket av informasjon, åpne kilder etc.
v. Hvor kommer fienden fra, hvilke tjenester prøver han å utnytte, i tillegg til info fra åpne kilder og samarbeidspartnere

Spille hverandre gode, jobbe i team, tenke høyt og jobbe med de samme oppgavene.

***b. Hva med avdelingens årvåkenhet?***

Samme kategorier som over, men i tillegg noe vekt på å etablere egne rutiner og prosedyrer som legger til rette for å øke en felles oppdatert situasjonsbevissthet og kunnskap om trusselbildet

i. Andre ting enn nettverk, vil det være viktig med det operative hendelsesforløpet,

ii. Andre etterretninger, finnes det fysiske hendelser som har en sammenheng med sikkerheten.
iii. Viktig å forstå trusselen, essensen i hva vi driver med.
iv. Returen av den informasjonen en har, må dele informasjon innad, snakker vi om hele forsvaret, må vi ha en informasjonskanal som vi kan stole på
v. Blir mye av de samme som forrige spm. Felles grunnlag og forståelse, snakker samme type språk, tenke likt.
vi. Kommer an på hensiktet, stoppe et angrep, eller kontrollere. Ikke alltid hovedhensikten å stoppe noen, da prøver det bare et sted vi ikke vet om. Kan godt få slippe inn slik at vi kan kontrollere og monitorere hva de gjør. En ting som er ekstremt viktig er å kjenne lendet. Det første er kjennskap til eget system, slippe dem inn og finne informasjon om fienden, hvilke kapasiteter han har, hvilke motivasjon, etc.
vii. Trusselaktør, motivasjon, metode, virkning på egen avdeling
viii. Lager grafisk situasjonsbilde ut av det, kunne gi en rask situasjonsbilde
ix. Briefinger om nye sårbarheter, ondsinnet kode, etc

11. *Anser du din kunnskap om fienden(angriperen) som viktig?*
    ***e.*** *Hvorfor/hvorfor ikke*

i. Ja, nye nasjoner som plutselig har fått en oppblomstring, kan indikere at noe kan skje
ii. Ja, vertfall i setting om å gjøre analyse, forhindre fremtidige angrep. De avanserte truslene er kanskje i stor grad sammenkoblet, og derfor svært vanskelig å lære om den. Men all kunnskap om fienden er viktig
iii. Ja for å tenke på morgendagens trusler som er i stadig endring, må lage seg en kunnskapsbase over aktuelle aktører.
iv. Normalt tenkes det tre operasjonslinjer, det ene er stanse/ sinke, skadevurdering, mulighet for å slå tilbake. Hva dette medfører for informasjonssystemet er viktig,
v. Ja, for i større grad kunne forutsi hva en avansert aktør vil kunne gjøre, på hvilken måte og med hvilken hensikt.
vi. Ønsker å kjenne fienden så godt som mulig, kan fås gjennom ulike sikkerhetsfirmaer, eller andre avdelinger i forsvaret, samarbeidspartnere, i tillegg finner vi ut en del vha egne sensorer.

12. *Hva slags informasjon må til for å skape en organisasjon som kan tilpasse sitt cyber-forsvar (CND) mot en dynamisk trussel/trusselbilde?*

***f.*** *(Hvilke informasjon kan gi oss et oppdatert og korrekt trusselbilde?)*
i. Problemet er at en trussel ikke oppdages før den har slått til, reaktivitet. Hvilken kompetanse den andre sitter på, holde seg

oppdatert hele tiden på hvilke muligheter som er gjort tilgjengelig på internett, det ligger oppskrifter på utnyttelse av sårbarheter. Det kommer nye hver dag.

ii. I tillegg svært viktig å patche med en gang
iii. Holde seg oppdatert
iv. Teknisk personell med god kunnskap om konfigurasjon og bruk, samt personell med god forståelse av samfunnet generelt, hvilke sårbarheter vi har etc.
v. Deteksjon av hva som skjer i systemet, kjenn deg selv og hva er viktig å beskytte
vi. Det viktigste er at ting blir tatt muntlig, folk leser ikke ting
vii. Mye informasjon, fordele informasjon innad i teamet, spesialister på de ulike områder, fra bits `n bytes, til operasjonsmåter for å danne en operasjon. Det kritiske er tidsaspektet
viii. Snakke forsvarets språk for å få gjennomslag og forståelse.
ix. Noen kan prodde på de kildene vi har for å skaffe seg informasjon
x. Få forståelsen utenifra for informasjonssikkerhet, og få aksept. NBF tenkning vil medføre en restrisiko, setter inn forsterkede mekanismer for å detektere dette. Viktig med informasjon om det operative spillet, basert på informasjon fra tidligere aktivitet.
xi. Informasjon om nye sårbarheter, og om dette har blitt utnyttet her, og få implementert en fix så fort som mulig.

***g.*** *Tas det hensyn til innrapporterte hendelser ved fordeling av ressurser?*

i. Ja det tror jeg, ser vi at det skjer mye et sted, er det en indikasjon på noe er i gang. Alle samles i en sikkerhetsrapport hver uke
ii. Benyttes i en viss grad, lære av feil.
iii. I noen grad, det tilflyter ofte ikke de rette folka. Eks fisb går til FLO og blir der.
iv. Viktig, (men erfaringen er at en ikke får noe melding tilbake.) kan være en god kilde til informasjon, sette hele sikkerhetssituasjonsbildet i sammenheng.
v. Kan si mye om mulige angrepsvektorer, kanskje ikke så mye om angriperens identitet.
vi. Ligger et stort potensial der.. merker det i alle sammenhenger, svært liten bevissthet blant brukerne, innen teknologi og sikkerhet. Brukerne må opplæres til å være mer bevisst. Og denne informasjonen kan helt klart benyttes til å skape et bilde av trusselen. Gjøres svært lite av i dag, stort potensial.

***h.*** *I hvilken grad mener du slik informasjon kan bidra til økt kunnskap om fienden.*

i. Kunne sikkert blitt brukt i større grad.
ii. Absolutt, den beste måte å bidra til slik kunnskap. Kunne vært gjort noe teknisk, samle inne loggdata etc.
iii. Helt klart, overvåking av alarmer dette kan indikere at noe skjer, viser trender, korrelere informasjon. Et senter som tar imot hendelser som korreleres. Avhengig av et oppdatert situasjonsbilde. Kan skape en mer proaktiv tilnærming.
iv. Uten denne kunnskapen, kan det være vanskelig å se trender. Skal vi skape en sikkerhetskultur trenger vi informasjon. Viktig å skape en forståelse for at sikkerhet er viktig. Så få tiltak som mulig men de skal være effektive.
v. Helt klart en del av det totale bildet, finnes informasjon der som kan være viktig

***i.*** *Hva tror du ville være de viktigste egenskaper ved denne informasjon (Tid, kvalitet, hvem, hva hvor, resultat, mm)?*

***i.*** **Rutiner og egen reaksjon**

1. Ende opp på riktig sted, er faste rutiner, men går nok ikke alltid i orden. Kan ligge hos forståelsen i ledelsen, blir ikke tatt seriøst nok.
2. Hvilke tiltak er gjort
3. Hvilke erfaringer kan vi dra
4. Dra nytte av de feila som er gjort, bunnlinja er opplæring
5. Viktig med tilbakemeldinger ved innrapportering.
6. Denne muligheten er lite benyttet i dag.
7. Skal vi mot NBF må vi ha en bedre informasjonsflyt, dele informasjon.
8. Må kommuniseres på en måte folk forstår. Opplæring så folk forstår og kan gjennomføre innrapportering på en nyttig måte. Økt sikkerhetsbevissthet ute i organisasjonen gjør oss mindre sårbare for virus-støy. Brukerne kan sitte på mye informasjon som er interessant.

***ii.*** **Trusselinformasjon**

1. Selvfølgelig, hvem som står bak
2. Korrekt og tidsriktig,

***iii.*** **Korrekt informasjon om hendelsen**

1. Kan være tidskritisk, men kanskje ikke alltid.
2. Konkret og korrekt, tidspunkt og hva som skjedde er godt beskrevet. Detaljnivå, konkret informasjon. Rapporter om hendelser utenfor systemene, eks bil i porten, kan være viktig, korrelere informasjon. FOST sitt ansvar er å gi et korrekt bilde. Kan sikkert bli bedre til å korrelere informasjon. Det handler mye om

kunnskap og holdninger for å kunne nyttiggjøre seg av informasjonen.

3. Prioritering, sannsynlighet for en falsk positiv, må kontrolleres at det er reelt før det når CND, tidsaspektet er viktig.
4. Eks sammenhenger med overvåking av fysiske alarmer, må se flerdimensjonalt. Korrelasjon av informasjon fra ulike kilder.

Vedlegg 4.

## Intervjuguide andre intervjurunde.

1. *Hvilken betydning har din forståelse og kunnskap rundt det operative behovet og målsettinger for din prioritering av arbeidsoppgaver og ressurser?*

2. *Hvilke type informasjon mener du er viktig i denne sammenheng?*

3. *I hvilken grad mener du at FOST (CND) får informasjon om det operative behovet og tilpasser seg deretter?*

4. *Hvilken kunnskap trenger de operative å få for å kunne bidra til bedre sikkerhet, og gi verdifull informasjon til fiendebilde?*

5. *I hvilken opplæring gis til de ansatte i denne sammenheng i dag?*

6. *Kan CND avdelingen bidra til å dekke informasjonsbehovet de ansatte har for å øke sin informasjonssikkerhetsbevissthet og evne til å opptre som en sensor. (Med sensor menes her en kapasitet som kan detektere og formidle sikkerhetsinformasjon. Det er underliggende her at en sensor må tilføres informasjon ("tunes") for å gjennomføre denne funksjonen).*

7. *I så fall hvordan mener du CND avdelingen kan bidra til dette?*

8. *I hvilken grad mener du at det eksisterer IS-bevissthetsøkende arbeid i Forsvaret i dag?*

9. *La oss si at det skal implementeres et IS-bevissthetsprogram i Forsvaret. Det er et ønske om at programmet skal utformes slik at det oppnås positive effekter også for CND avdelingen og deres fiendeforståelse. Hvilke innspill har du til utformingen av et slikt program?*

**Vedlegg 5.**

## Kategoriserte svar fra andre intervjurunde.

1. *Hvilken betydning har din forståelse og kunnskap rundt det operative behovet og målsettinger for din prioritering av arbeidsoppgaver og ressurser?*

    *1.1* Dialog/informasjonsflyt
        i. *Dialog med ledelsen i egen avd*
        ii. *Dialog med ledelsen i organisasjonen*

    *1.2 Operativ forståelse*
        i. *Forståelse av Forsvarets totale virksomhet, hvilke verdier de besitter og konsekvensen av bortfall*
        **ii.** *Forstå hvilke tjenester som er kritiske for operasjoner, liv og helse.*

2. *Hvilke type informasjon mener du er viktig i denne sammenheng?*

    *2.1* Operativ forståelse
        i. Hvilke operasjoner som pågår
        ii. Hvilke kapasiteter innehar den enkelte operative avdeling selv, med tanke på å håndtere hendelser
        iii. Hvilke kapasiteter har vi selv
        iv. Kritiske verdier
        v. Hvilke prioriteringer har den enkelte lokale sjef
        vi. Hvilke prioriteringer har Forsvarets øverste ledelse
        vii. Hvordan brukes systemene, innhente slik info både fra det operative miljøet samt driftsmiljøet.

    *2.2* Konsekvensanalyse
        i. Hvilke konsekvenser vil et angrep ha for operasjonene

3. *I hvilken grad mener du at FOST (CND) får informasjon om det operative behovet og tilpasser seg deretter?*

        i. I begrenset grad
        ii. Er et potesiale her
        iii. Informasjonsutvekslingen er ikke optimal slik at det er vanskelig å være tilpasset en gjeldende operativ situasjon.

4. *Hvilken kunnskap trenger de operative å få for å kunne bidra til bedre sikkerhet, og gi verdifull informasjon til fiendebilde?*
    *4.1* Kunnskap om prosedyrer og FOST/CND
        i. Være klar over hvilke kapasiteter FOST/CND avdelingen i Forsvaret besitter

ii. Hvilke tiltak kan settes inn. (hvilke kapasiteter finnes i egen avdeling, FOST og organisasjonen for øvrig)
iii. Hva skjer i egne systemer, og vite hvordan en kan reagere, hvem kan kontaktes og hvordan. Det operative miljøet må besitte slik kompetanse selv eller vite hvor de kan få støtte med denne kompetansen.

*4.2* Informasjon om trusler

i. Bevisstgjøring av aktuelle trusler, og sette dette i sammenheng med andre samfunnsmessige hendelser.

*4.3* Kommunikasjonsflyt

i. For å oppnå dette må kommunikasjonskanaler etableres

5. *I hvilken opplæring gis til de ansatte i denne sammenheng i dag?*

i. Svært lite
ii. Ingen offisiell og helhetlig opplæring
iii. Opplæring er i stor grad rettet mot personell med sikkerhetsrelaterte stillinger.
iv. Opplæring forutsetter oftest at den enkelte initierer dette selv.
v. Det finnes muligheter, men er i stor grad rettet mot sikkerhetspersonell, og krever at en er interessert og søker denne kunnskapen selv.

6. *Kan CND avdelingen bidra til å dekke informasjonsbehovet de ansatte har for å øke sin informasjonssikkerhetsbevissthet og evne til å opptre som en sensor. (Med sensor menes her en kapasitet som kan detektere og formidle sikkerhetsinformasjon. Det er underliggende her at en sensor må tilføres informasjon ("tunes") for å gjennomføre denne funksjonen).*

i. FOST kan bidra i stor grad med slik informasjon'
ii. Er et potensial her
iii. FOST kan drive bevisstgjøring, trekke fram eksempler og informere
iv. CND besitter både kompetanse og evne til dette, men mangler direkte kommunikasjonskanaler.

7. *I så fall hvordan mener du CND avdelingen kan bidra til dette?*

i. Dele den kunnskap som CND sitter på.
ii. For at en sensor skal fungere er det viktig at kommunikasjon flyter begge veier. Derfor er det viktig at en innrapportert hendelse blir tatt på alvor og at det blir gitt tilbakemelding til den som rapporterte

8. *I hvilken grad mener du at det eksisterer IS-bevissthetsøkende arbeid i Forsvaret i dag?*

    *i.* Det finnes i en viss grad.
    *ii.* Driftsorganisasjonen gir instrukser for bruk av systemene som brukerne må signere på.
    *iii.* E-læringskurs og sikkerhetskonferanser.
    *iv.* Videre er sikkerhetsorganisasjonen organisert slik at det er det lokale sikkerhetspersonellets ansvar å holde seg oppdatert og følge opp eget personell. Informasjon til disse gjøres tilgjengelig. Imidlertid virker opplæring å være lite oppdatert.
    *v.* Det finnes ingen noen offisielle programmer som favner om alle og det nevnes at en ny kompetansestrategi må utvikles.
    *vi.* Må lages en ny kompetansestrategi

9. *La oss si at det skal implementeres et IS-bevissthetsprogram i Forsvaret. Det er et ønske om at programmet skal utformes slik at det oppnås positive effekter også for CND avdelingen og deres fiendeforståelse. Hvilke innspill har du til utformingen av et slikt program?*

    *9.1* Rapportering av hendelser
        i. Lavere terskel for rapportering
        *ii.* Alle rapporter må tas hensyn til og gi en tilbakemelding til den som rapporterer.
        *iii.* Informere og promotere FOST slik at brukerne vet hvem/hva de er, og føler seg komfortable med å rapportere.
        *iv.* Gjøre rapporteringsrutiner så enkelt at rapportering foretas
    *9.2* Differensiering av tiltak
        *i.* Kategorisere programmet og tilpasse programmet til ulikt personell.
    *9.3* Spredning av informasjon
        *i.* Skape en forståelse hos den enkelte av hvilke kapasiteter/ tjenester FOST besitter
        *ii.* Informere om trusler, gjerne gjennom eksempler
        *iii.* Opprettholde informasjonsflyten. Den som rapporterer må få tilbakemelding.