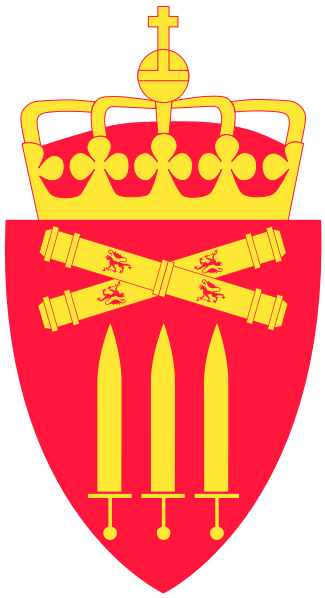


Forsvarets stabsskole

Våren 2008

Masteroppgave

Informasjonsoperasjoner:
Sårbarhetsbetraktninger i en tenkt fremtid

Sjefingeniør Nina Margrethe Grude

Forord

En fantastisk reise over en periode på nesten to år er ved sin avslutning. På den ene siden ser jeg frem til det, men på den andre siden vil jeg savne alle de hyggelige ”kollegene” ved Forsvarets Stabsskole og det å være en del av den unike fagkompetansen skolen besitter. Hvem vet, kanskje våre veier møtes igjen?

Jeg har igjennom begge studieårene fått innblikk og kompetanse på fagområder som i utgangspunktet var ”et sort hull”. Aldri hadde jeg trodd jeg skulle si at militærhistorie og politikk faktisk er så interessant som det viste seg å være! Dette siste året har jeg valgt å utfordre meg selv, og kanskje andre, på å fordype med i faget ”fellesoperasjoner”. Forhåpentligvis vil jeg ha muligheten for å følge dette fagfeltet videre på en eller annen måte. Jeg er stolt av hva jeg har vært en del av, men samtidig ydmyk i forhold til at jeg har mye igjen å lære.

Valget av masteroppgaven er en kombinasjon av tilfeldigheter og egne ideer. Jeg har en svakhet for å lære noe nytt – gjerne innenfor områder som ikke er ”ferdigforsket” fra før. Når muligheten var til stede for å krype inn under huden på det spennende fagfeltet informasjonsoperasjoner var jeg overbevist. Jeg håper at jeg med denne oppgaven vil inspirere andre til å fortsette å forske innenfor dette spennende temaet.

Jeg vil spesielt takke alle dere som har stilt opp for meg med fagekspertise innenfor deres respektive fagfelt. Forsvaret besitter en fantastisk fagkompetanse som jeg i forbindelse med denne oppgaven har dratt nytte av. Jeg vil videre takke min hovedveileder, Hilde Hafnor, og fagmiljøet på FFI med Ronny og Aasmund i spissen. Takk for alt dere har bidratt med og for at jeg også har kunnet opprettholde humøret. Takk også til min bi-veileder Bent Erik Bakken for hans konstruktive tilbakemeldinger.

Avslutningsvis vil jeg først takke C2, primærgruppen min første året. Nils Frode, Roy, Sveinung, Kenneth, Kjell Arne, Dag og John Otto. Takk for at jeg fikk være en av ”gutta”, men samtidig også meg selv! Til slutt vil jeg takke familien – barna mine Håkon og Hannah som nå er lei av at ”mamma gjøre lekser”, og mannen min Sverre for alt han har stilt opp med, herunder ”nattevåk” det siste døgnet, og for at han gav meg denne muligheten.

Oslo, mai 2008, Nina Margrethe Grude

Information operations:

Reflections of vulnerabilities in an imagined future

Abstract

The first electronic war is recognised with what Estonia experienced for three weeks in May 2007. Estonia claimed to be under attack, not in the traditional way, but the victim of a new form of combat – cyberwarfare that ought to be treated as an attack against the state. This incident became a warning for individuals and governments around the world in connection with cyber vulnerabilities and electronic warfare.

Like other nations, Norway also possesses military activities/programs with respect to network based defence. As prerequisite for the concept of network based defence is a functional information infrastructure. Increased control and security of own military information and relative information superiority in relation to adversaries are important aspects. Military units as a large consumer of information opens for increased hostile activities in the information domain.

Information operation is a military function to provide advice and co-ordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries. Info Ops focus is an integrating function concentrating on the information environment rather than a capability of its own. Info Ops objectives can be reached by the planned co-ordination and synchronisation of military capabilities, tools and techniques affecting information or information systems.

The aim of this thesis contains diversity. First an analysis of central vulnerabilities in the transformation of the Norwegian military information infrastructure based on the factor *future military information infrastructure*. Secondly, an analysis of central vulnerabilities in decision-makers dependence on and employment of the information infrastructure that hostile information operation ought to exploit. This part is based on two factors representing aspects influencing decision-makers efficiency – *situation awareness* and *capability and will*.

Innhold

1 Innledning

Den første elektroniske krig er den kalt, cyber angrepene på Estland i april-mai 2007. Hendelsen er uttalt å fungere som"… **a wake-up call for everyone -- for individuals as well as governments -- about cyber vulnerability and electronic warfare**." (*Estonia under cyberattack: The first electronic war*, uthevet i originalteksten). I en periode på tre uker hevdet Estland å være angrepet – ikke i tradisjonell forstand med bomber, missiler, men angrep over Internett (Hollis 2007). Det Estland opplevde var en serie med cyber angrep mot estiske organisasjoners nettsteder, herunder det estiske parlamentet, banker, departementer. De fleste angrepene var typiske "denial of service" (DOS) angrep med en variasjonsbredde fra enkeltstående individuelle metoder til omfattende løsninger som botnett.[1]

Estland karakteriserte angrepene som "act of war". Med utgangspunkt i deres NATO medlemskap ble NATO forespurt om assistanse. Selv om NATO ikke betraktet episoden som utgangspunkt for å trigge alliansens kollektive forsvars forpliktelser (artikkel 5) så sendte NATO eksperter til Estland for å observere hendelsen (Hollis 2007).

Angrepene på Estland er bakgrunnen for at (militære) organisasjoner rundt om i verden har blitt mer oppmerksomme på muligheten for at "cyberspace" vil være en potensiell fremtidig arena for bruk av militære styrker inn under rammene av krigens lover og regler (Hollis 2007).

1.1 Bakgrunn og tema

Det norske forsvaret sitt utviklingsarbeid for å oppnå økt nettverksorganisering omtales som nettverksbasert forsvar (NbF). Sagt på en annen måte er NbF et konsept for samhandling i nettverk. NbF er å betrakte som en utviklingsprosess hvor Forsvaret gradvis blir mer avhengig av en velfungerende informasjonsinfrastruktur (INI). For å sikre at utviklingen går i ønsket retning er det definert en serie tilstandsbeskrivelser for NbF[2]: *Innledende*, *integrerende* og *gjennomgripende* (Enemo 2006). Gradene er ikke eksakte ambisjoner med tiltak og tidsfrister, men gir et bilde av den transformasjonen Forsvaret må gjennom og hvordan man tror at NbF vil påvirke Forsvaret.

Økt kontroll på egen informasjon og relativ informasjonsoverlegenhet i forhold til motparten blir nødvendige forutsetninger for et velfungerende NbF. Dette inkluderer blant annet informasjon

[1] Begrepet botnett benyttes gjerne for nettverk av kompromitterte (data)maskiner som er logisk sammenkoplet og styrt som en sammensatt enhet (Thuv et al. 2007 s. 36).
[2] NbF tilstandsbeskrivelse omtales også som såkalte (modnings)grader (Hafnor et al. 2006 s. 9).

om egne styrker, fiendtlige styrker, om allerede utførte og mulige fremtidige hendelser, i operasjonsteateret og utenfor. Informasjonen formidles gjennom en rekke informasjonskanaler, behandles av en rekke informasjonssystemer og når frem til både involverte og utenforstående med innvirkning på alle nivåer fra politisk/militærstrategisk til enkeltmann.

Militære informasjonsoperasjoner (MIL INFOOPS) er integrerte aktiviteter med den hensikt å påvirke motpartens vilje, forståelse og evne gjennom påvirkning av motpartens informasjon, informasjonssystemer og informasjonsprosesser (AJP-3.10 (A)). Informasjon er på denne måten både et mål og et våpen. Ved å levere sann eller falsk informasjon på rett sted, til rett tid, og i rett form kan informasjon påvirke beslutningstakere og andre. Tilsvarende vil fiendtlig manipulasjon med og i våre egne systemer og prosesser kunne påvirke vår virksomhet negativt.

1.2 Formålet med oppgaven

Formålet med denne oppgaven er todelt. På den ene siden vil oppgaven analysere sårbarheter i transformasjonen frem mot fremtidig militær INI (MIL INI[3]) med utgangspunkt i faktoren *fremtidig MIL INI*. På den andre siden vil oppgaven analysere sårbarheter i beslutningstakeres[4] avhengighet og anvendelse av fremtidig MIL INI. Flere momenter påvirker en beslutningstakers effektivitet hvorav situasjonsbevissthet, evne og vilje er sentrale momenter. Analysen gjennomføres med utgangspunkt i to faktorer som representerer disse momentene – *situasjonsbevissthet* samt *evne og vilje til beslutning*. Denne todelingen samsvarer med de to ledelsesdimensjonene, fremskaffe og anvende, den strategisk ledelsen av Forsvaret baserer seg på (FD 2007). Denne beviste vinklingen på oppgaven kan blant annet sees i sammenheng med at sårbarhet knyttet til MIL INI spenner fra utviklingen av systemene/tjenestene, via den realiserte MIL INI og videre til bruken av denne – alt i lys av teknologi og strukturer, organisasjon, prosesser og individer.

1.3 Problemformulering

Grunnlaget til et fremtidig NbF vil være en MIL INI som tilbyr tilgjengelighet til høykvalitets informasjonstjenester til alle elementer innenfor den militære virksomheten (Alberts, Garstka & Stein 2000 s. 187). Militære styrker har alltid vært sårbare ovenfor fiendtlige påvirkning. Viktigheten av, og striden om, informasjonsdomenet er langt viktigere enn før ikke minst grunnet samfunnet generelt og militære styrkers storforbruk av informasjon. Betydningen av

[3] Begrepet MIL INI vil redegjøres for i kapittel 5.3 MIL INI.

INFOOPS i all militær aktivitet har av den grunn økt og er i dag påkrevet som en del av alle (militære) operasjoner. Potensialet til fiendtlig INFOOPS mot Norge og norske interesser, herunder Forsvarets (operative) virksomhet, antas å være økende med gradene av NbF. Det brukes bevisst ikke begrepet fiendtlig MIL INFOOPS. Grunnen til dette er at det i prinsippet ikke er enkelt å skille på om anslag (i informasjonsdomenet) er MIL INFOOPS, annen INFOOPS, organisert kriminalitet, eller andre typer anslag som f.eks hackervirksomhet.

Sårbarhetsvurderinger er ikke uavhengig av hvilke potensielle trusler som eksisterer. På den internasjonale arena opererer det mange forskjellige aktører som i gitte situasjoner og under gitte betingelser kan representere en utfordring for norsk utenriks-, sikkerhets- og forsvarspolitikk. Frykten for målrettede militære angrep i stor skala med formål om å langsiktig besette norsk territorium var et trusselbilde som under hele den kalde krigen utgjorde de dimensjonerende rammefaktorene (Johansen 2006 s. 14). Etter slutten på den kalde krigen har det utviklet seg en endring i trusselbildet. Sosiale nettverk[5], som samhandlende noder har blitt kjernen i det nye trusselbildet (Johansen 2006 s. 14).

Forsvarets Fellesoperative doktrine (FFOD) skriver (2007 pkt 0574) at grunnlaget for all (operativ) virksomhet er kommando og kontroll (K2) som er det militære begrepet for ledelse av operasjoner. I lys av NbF utviklingen er beslutningstakere mer og mer avhengig av informasjon og informasjonsbaserte systemer for å fatte beslutninger.

Med bakgrunn i oppgavens bakgrunn, tema og formål er følgende to overordnede problemstillinger utformet:

- *Hvilke sentrale sårbarheter eksisterer i transformasjonen frem en mot en fremtidig MIL INI?*
- *Hvilke sentrale sårbarheter i beslutningstakeres avhengighet og anvendelse av MIL INI vil (koordinert) fiendtlig INFOOPS kunne utnytte?*

Begrepet sårbarhet i denne oppgaven brukes i en overordnet/vid forståelse. Sårbarhet er en svakhet, en egenskap, som åpner for uønskede endringer og/eller hendelser i et system. Med system menes sosiale systemer, tekniske systemer samt informasjonsbaserte systemer. En egenskap ved et system kan være en sårbarhet eller en styrke avhengig av forholdene systemet skal operere under. I lys av dette vil det for de valgte problemstillingene objektivt sett være et

[4] Begrepet beslutningstaker i denne sammenheng vil være enhver (militær) ressurs som tar en eller annen form for beslutning som del av, eller relatert til, en militær operasjon.

dilemma å balansere dette. Dette inkluderer å identifisere hva som egentlig er en sårbarhet i forhold til hva som er forhold som kan føre til en sårbarhet. Ved å erkjenne dette dilemmaet vil det kunne diskuteres om alle de sentrale sårbarhetene analysen identifiserer er sårbarheter eller om noen av de ligger nærmere utfordringer. Dette er en diskusjon som oppgaven ikke legger opp til, men som kan betraktes som en analysemessig svakhet og tema for en annen oppgave.

Det er flere årsaker til at oppgavens problemstillinger er relevante. Forsvarssjef Sverre Diesen (FSJ Diesen) har satt økt fokus på NbF ved blant annet opprettelsen av en egen sjef for (fag)området INI (SJ INI). Ved å være klar over og bevisst potensielle sårbarheter i transformasjonen til fremtidig MIL INI, og bruken av denne, vil Forsvaret kunne iverksette tiltak for å imøtekomme fremtiden på en best mulig måte. For eksempel vil SJ INI sin implementeringsplan for NbF kunne avstemmes mot denne oppgavens funn og konklusjoner.

Som en del av NbF transformasjonen er det påstartet og i planfasen flere investeringsprosjekter som vil kunne dra nytte av oppgavens funn hva angår sårbarheter. Dette slik at åpenbare, identifiserte sårbarheter er kjent ved planlegging og gjennomføring av disse investeringene, men også med en ambisjon om at flere av disse sårbarhetene vil kunne unngås og/eller begrenses ved å være de bevisst.

NbF konseptets kritiske avhengighet av informasjon og informasjonsflyt, herunder (fremtidige) trusler mot denne, er alvorlige situasjoner som må håndteres. Å kjenne til sårbarheter i avhengigheten og anvendelsen av fremtidig MIL INI anses av den grunn som interessant.

1.4 Avgrensinger og forutsetninger

Følgende avgrensninger og forutsetninger gjelder for oppgaven:

- Som utgangspunktet for oppgavens analyse vil denne oppgaven etablere en tenkt fremtid. Oppgavens funn og konklusjoner vil være avgrenset til dette, selv om enkelte sårbarheter er sårbarheter som også er potensielle i dag.
- Et overordnet scenario, en konstruert konflikt, vil utarbeides som et kommunikasjonsverktøy for deler av oppgavens datainnsamling. Oppgavens funn og konklusjoner kan i den forbindelse i noen grad avgrenses til utelukkende å gjelde en type trussel.

[5] ”Et nettverk skiller seg fra fastere organiserte enheter ved at de mangler en formell struktur med hierarkisk organiserte ledd…[uten] en klart definert ledelse (selv om enkelte noder i nettverket kan ha en mer sentral rolle en andre)…og bestemte kanaler og formater for informasjonsflyt (Johansen 2006 s. 14).

- Oppgaven er besluttet holdt på et ugradert nivå. Dette medfører at tilgjengelig faktisk empiri vil være mindre enn hvis oppgaven hadde vært høyere gradert.
- Oppgavens utgangspunkt er fiendtlig påvirkning. Det er mindre interessant hvilke kapasiteter påvirkningen gjøres med. Men, konkrete eksempler omtales der det er hensiktsmessig.

1.5 Oppgavens disposisjon

Oppgavens bakgrunn presenteres i de to første kapitlene. Kapittel 1 *Innledning* introduserer oppgavens tematikk, problemstilling og faglige forankring. Presentasjon av oppgavens forskningsmetode gjøres i kapittel 2 *Metode*.

Oppgavens teoretiske grunnlag er basis for oppgavens analysedel. Sentrale konsepter, begreper og teorier som har relevans og innvirkning for oppgaven redegjøres for i kapitlene 3 til 6. Kapittel 3 *Forsvarets operative virksomhet* redegjør i korthet for sentrale elementer, herunder en presentasjon av domenemodellen. Kapittel 4 *Nettverkstenkning og NbF* gir en kort redegjørelse for nettverkstenkning generelt. Deretter presenteres nettverkstenkningen i NATO før Forsvarets konsept, Nettverksbasert forsvar (NbF) introduseres. En sentral del av dette kapitlet er presentasjonen av NbF sine tre tilstandsbeskrivelser. Kapitlet avsluttes med en kort introduksjon av to sentrale NbF begreper situasjonsbevissthet og informasjonsoverlegenhet. Kapittel 5 *Informasjonsinfrastrukturer og MIL INI* starter med å gjøre rede for begrepet ”community of interest”. Deretter beskrives informasjonsinfrastrukturer (INI) generelt før kapitlet presenterer NATO og Forsvarsdepartementets MIL INI. Avslutningsvis gjøres en redegjørelse av begrepet informasjonsstyring. Informasjonsoperasjoner (INFOOPS) presenteres som konsept i kapittel 6 *Informasjonsoperasjoner*. INFOOPS forhold til domenemodellen presenteres også. Kapitlet avsluttes med en redegjørelse av en mulig nasjonal INFOOPS strategi og begrepet militær (MIL) INFOOPS.

Oppgavens analyse og diskusjon skjer over to kapitler. Kapitlene 7 *Sentrale sårbarheter i transformasjonen mot en fremtidig MIL INI* og kapittel 8 *Sentrale sårbarheter i beslutningstakeres avhengighet og anvendelse av MIL INI* analyserer og diskuterer de to overordnede problemstillingene respektivt. Hver analysefaktor avsluttes med en delkonklusjon som hver og en representerer oppgavens kjerne.

Kapittel 9 K*onklusjon* utgjør oppgavens siste del og er en konklusjon på et overordnet nivå som også inneholder forslag til videre forskning innen (fag)området.

2 Metode

Dette kapittelet presenterer oppgavens forskningsdesign, herunder på hvilken måte datainnsamlingen er gjennomført. Hensikten er å åpne for etterprøvbarhet av det arbeid som er gjort. Det (data)underlaget oppgaven bygger på presenteres, samt en vurdering av oppgavens gyldighet og pålitelighet.

Problemstillingen skal vurderes i lys av en tenkt fremtid. NbF grad 2, integrerende NbF, som en metodisk tilnærming i tid. Denne NbF graden sine egenskaper/forventninger utgjør rammebetingelsene for sårbarhetsbetraktningene.

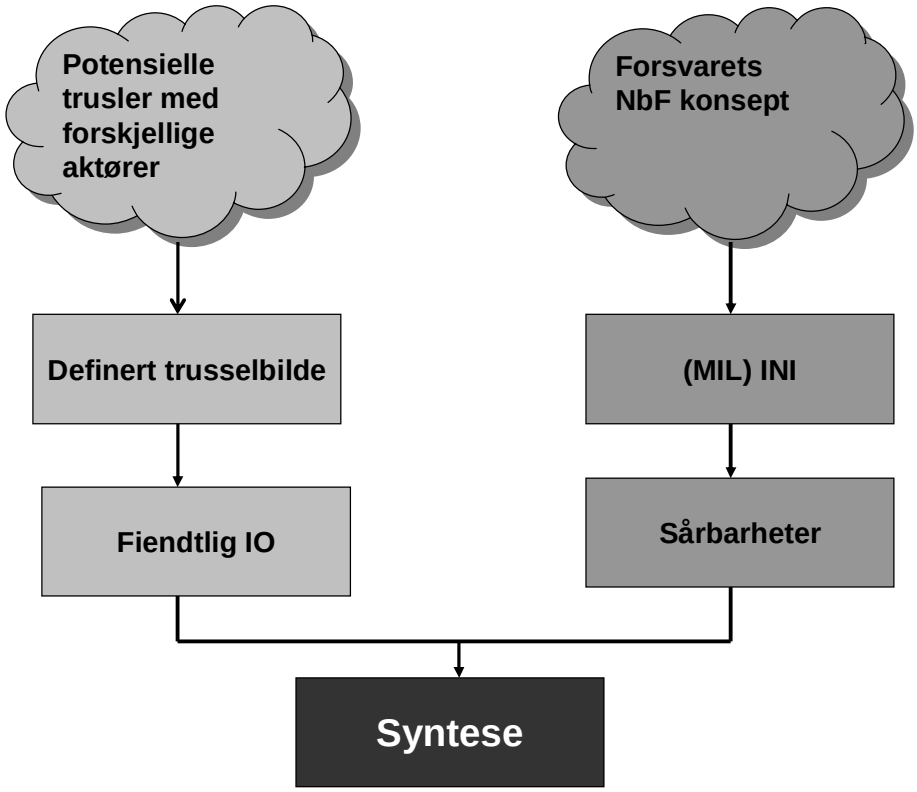
2.1 Forskningsdesign

Med utgangspunkt i oppgavens overordnede problemstillinger er et intensivt undersøkelsesdesign lagt til grunn. Hensikten er å gå i dybden med det formål å skaffe en mest helhetlig kontekstuell forståelse av problemstillingene. Oppgaven har likheter med små-N studier ved at oppgavens problemstillinger (fenomen) belyses fra ulike ståsteder (Jacobsen 2005).

Å analysere utviklingsløp og fremtidige situasjoner innebærer spesifikke utfordringer og krever spesiell håndtering. Bakgrunnen for dette er den reelle mangelen på empirisk underlag for gjennomføring av forskning (Johansen 2006 s. 8). En måte å tilnærme dette på er ved bruk av scenarier og på den måte konstruerer en ”syntetisk” empiri (Johansen 2006 s. 8). Som i all vitenskapelig forskning stilles det en rekke krav som må tilfredsstille. To sentrale krav er kravene om relevans og konsistens og den overordnede målsetningen er ”…at scenariet skal være *realisertbart*…” (Johansen 2006 s. 9).

Hensikten med oppgavens bruk av scenario er som et verktøy for kommunikasjon og diskusjon med ekspertpanel/fagmiljøer som ledd i oppgavens datainnsamlingsprosess (Bakken u.å.). Oppgavens andre problemstilling gjennomføres dels som en scenarioanalyse i lys av en konstruert konflikt (Bakken u.å.). Utgangspunkt for scenarioanalysen har likheter med metoden for langtidsplanlegging som støtte til Forsvarsstudie 2007 (FS07), se figur 1.

Metoden går langs to hovedlinjer. Den venstre delen av modellen tar utgangspunkt i potensielle aktører og utleder en konstruert konflikt for (deler av) oppgavens analyse. Den høyre delen av modellen representerer sårbarheten i det systemet som skal analyseres.



Figur 1 - Metodemodell (fritt etter Hennum & Glærum 2007)

2.2 Datainnsamling

Datainnsamlingen og analysen av data vil gjennomføres med utgangspunkt i kvalitativ metode. Oppgaven vil basere seg på både primær- og sekundærdata (kildetriangulering). Innsamling av data vil gjennomføres i form av dokument-/tekstanalyser, (gruppe)intervju/møter, bruk av ekspertpanel samt bruk av egne erfaringer.

Det er skrevet mange forskningsrapporter/tilsvarende som berører (deler av) oppgavens kontekst. En utfordring er at den tilgjengelige forskningsbaserte litteraturen i liten grad betrakter alle de faktorene denne oppgaven legger til grunn og/eller at de i utgangspunktet er teoretisk fremstilt. Noe konkret fremtidsrettet forskning finnes, men ikke ”skreddersydd” i forhold til denne oppgavens problemformuleringer. En annen utfordring er at mye av aktuell litteratur er gradert.

Primærdata

Hovedinnsamlingen av empiri som underlag for oppgavens analyse er innhentet med utgangspunkt i (gruppe)intervjuer, herunder et nedsatt ekspertpanel. Formålet med (gruppe)intervjuene var å trekke på gruppens samlede (fag)kunnskap, samt håpe på at

dynamikken i gruppeprosessen ville gi ny viten/ønsket synergi, slik som beskrevet av Jacobsen (2005 s. 154).

(Gruppe)intervjuene er gjennomført med personer som alle har en eller annen (faglig) tilknytning til oppgavens tematikk. Informantene representerer forskjellige (fag)områder/enheter som samlet utgjør et tverrfaglig utgangspunkt for datainnsamlingen. I tillegg representerer ressurspersonene forskjellige (operasjonelle) nivåer i Forsvaret.

I forbindelse med forskningens datainnsamling ble det også nedsatte et ekspertpanel. Ekspertpanelet hadde representanter fra følgende forsvarsenheter: Forsvarets Stabsskole (FSTS), Fellesstaben (FST), Forsvarets Sikkerhetsavdeling (FSA), Nasjonal Sikkerhetsmyndighet (NSM) og Forsvarets forskningsinstitutt (FFI)[6]. Formålet med denne tverrfaglige sammensetningen var å gi en ønsket bredde på og kvalitetssikting av datainnsamlingen. Ekspertpanelet møttes samlet på et dagsseminar i FSTS sine lokaler (Akershus festning) 10. april 2008 og bestod av åtte ressurspersoner, inklusive undertegnede. Oppfølging i etterkant er gjort i de tilfeller det har vært behov for dette.

Utgangspunktet for datainnsamlingen til oppgavens første problemstilling har vært en kort presentasjon av oppgavens tematikk generelt og en kort presentasjon av de tanker som ligger til grunn for fremtidig MIL INI. I forbindelse med oppgavens andre problemstiling er utgangspunkt for (gruppe)intervjuene/ekspertpanelet en konstruert konflikt (scenario) i en tenkt fremtid (NbF grad 2). De beskrevne (tilstands)forventninger til NbF grad 2 utgjorde diskusjonene sine rammebetingelser.

Oppgavens primærdata utgjør vesentlige og viktige bidrag i analyse av oppgavens problemstillinger. Alle oppgavens muntlige kilder er listet under eget punkt som en del av kildelisten.

Sekundærdata

Som underlag for oppgavens (teoretiske) grunnlag er det i all hovedsak benyttet litteratur, både norsk og utenlandsk. I tillegg benyttes litteratur fra offentlige kilder, gjennomførte forskningsprosjekter og andre publikasjoner. Skriftlig litteratur er også benyttet som konkret empiri for oppgavens analysedel i den grad dette finnes. Spesielt gjelder dette forskningsinformasjon som har hatt spesiell fokus på fremtidsrettede konsepter, som NbF. Også

[6] Forsvarsdepartementet (FD) var også inviterte, men var forhindret til å delta på selve ekspertpanelseminaret. Samtaler med representant i FD er gjennomført i etterkant.

empiri og/eller erfaringer fra de deler av Forsvaret som omtales som forvaltningsdomenet er tatt med der de har relevans.

Oppgavens sekundærdata utgjør viktige bidrag i analyse av oppgavens problemstillinger.

Gjennomføring

Oppgaven har hatt en stegvis datainnsamlingsprosess. Innledningsvis er det brukt mye tid på å studere skriftlige kilder. Bakgrunnen for dette er å opparbeide en god innsikt i oppgavens kontekst. Dette var også viktig all den tid deler av oppgavens tematikk er utenfor forfatterens fagområde. Denne prosessen har også bidratt til utviklingen av problemstillingene. Den kompetanse som er opparbeidet som del av den innledende ”leseprosessen” er også benyttet som grunnlag for den senere gjennomføringen av (gruppe)intervjuene, herunder ekspertpanelsseminaret. De konkrete gjennomførte (gruppe)intervjuene fungerte også som verktøy for å avdekke nye momenter – både i forhold til spissing og presisering av problemstillingene samt som ledd i oppgavens konkrete datainnsamling. I tillegg var disse en arena for bekjentgjøring av nye fag- og ressurspersoner.

All muntlig datainnsamling er gjennomført som ”åpne samtaler”. Datainnsamling over telefon er søkt til et minimum. Ingen av (grupper)intervjuene er tatt opp på digital lydfil, men empirien er nedfelt i skriftlige og i noen grad elektroniske notater. En del tid under gjennomføring av intervjuer ble benyttet til å ”holde fokus”, men uten for sterk regi. Avviket her er ekspertpanelseminaret som ble gjennomført med mye friere ”tøyler” enn opprinnelig tiltenkt. Bakgrunnen for dette er at den planlagte styringen ikke passet med deltakernes forventninger. Tross dette anses utfordringen med påføring av ”intervjueffekter” som minimal. Et annet moment er at selve gjennomføringen av ekspertpanelet også fungerte som en siste kursendring på problemstillingene.

De valgte analysefaktorene vil igjennom analysen operasjonaliseres til et sett med utledede faktorer. Disse faktorene er utgangspunkt for identifiseringen av de sentrale sårbarhetene. En oversikt over de viktigste funnene presenteres samlet i vedlegg som en del av oppgavens konklusjon.

2.3 Evaluering av metoden

Oppgavens opprinnelige ambisjon var å betrakte sårbarheter i lys av alle NbF sine tre tilstandsnivåer samt innenfor forskjellige typer av scenarier. Disse ambisjonene ble begrenset i løpet av forskningsprosessen blant annet grunnet mangel på tilgjengelige scenarier, oppgavens omfang osv.

Metodiske svakheter

All den tid oppgavens problemstilling opererer med flere komplekse begreper, ble grunnlags- og teoridelen ganske omfattende. Dette var et bevisst valg for å sikre et godt begreps- og teorimessig utgangspunkt for oppgavens analysedel. Oppgavens utstrakte bruk av figurer og tabeller som en del av oppgavens redegjørelser øker også omfanget. Ved at oppgaven spenner såpass vidt har dette gått utover analysens dybde. Dette er en kort oppgave utarbeidet over et halvt år. En oppgave av lengre varighet ville kunne godt inn med dypere analyse på utvalgte områder. Dette til tross, så er det undertegnedes formening at oppgaven gir konstruktiv innsikt innenfor problemområdene og at fremtidig forskning kan fordype seg ytterligere i (utvalgte) områder.

Å skaffe til veile empiri for en (tenkt) fremtid var som beskrevet over også en utfordring. I tillegg viste det seg vanskeligere enn antatt å få intervjuobjektene til å ”forstå settingen”. Tross dette anses den datainnsamling som er gjort å være tilstrekkelig som utgangspunkt for analyse av oppgavens to problemstillinger.

Gyldighet

Metodisk skilles det mellom intern og ekstern gyldighet (Jacobsen 2005 s. 212). Sikring av ekstern gyldighet har aldri vært formålet med denne oppgaven. Oppgavens interne gyldighet utfordres i forhold til den begrensede tilgangen på empiri. Utfordringen favner både tilgjengelig skriftlig materiale, men også mangel på reell (fremtidig) empiri. Kildeutvelgelsen har søkt å ivareta dette. Oppgavens problemstillinger anses ikke å fremme eventuelle ulike agendaer hos de utvalgte informantene og respondentene. Oppgavens gyldigheten å være tilfredsstillende.

Pålitelighet

Hvorvidt forskningens resultater er pålitelige handler om hvor pålitelige forskningens empiri er samt i hvor stor grad datamaterialet er troverdig. (Jacobsen 2005 s. 225). Oppgavens skriftlige kilder anses i all hovedsak å være representative og pålitelige kilder. En utfordring er at mye av den tilgjengelige litteraturen er amerikansk og av den grunn preget av amerikansk tekning. På den andre siden er denne tenkningen i stort det som ligger til grunn for NATO og norsk

tilnærming. En annen utfordring er at ikke all litteratur fra politisk og/eller militærstrategisk side er like forankret som intensjonene var på det tidspunkt den ble skrevet.

Dialog med oppgavens informanter og respondenter ble innledet med en kort presentasjon av oppgavens kontekst og problemstillinger som et ledd i å forberede intervjuobjektene. Forut for gjennomføringen av seminaret med ekspertpanelet ble det i tillegg distribuert noe underlag – konkretisering av oppgavens tenkte fremtid samt den konstruerte konflikten. Den innsamlede empirien er gjennomgått og behandlet med årvåkenhet og bevissthet/nøyaktighet. Tross dette kan empiri være misforstått og/eller feiltolket. Oppgavens pålitelighet anses likevel å være tilfredsstillende.

3 Forsvarets operative virksomhet

Forsvarets overordnede styrings- og plandokumenter beskriver Forsvarets roller og oppgaver (FD 2004; FD 2007). Selv om støtte til det sivile samfunnet i form av suverenitetshevdelse, håndtering av episoder, myndighetsutøvelse og overvåking utgjør en stor del av det daglige arbeidet så er det forberedelser og gjennomføring av (militære) operasjoner som er Forsvarets sin kjernevirksomhet. Forsvarets operative virksomhet omfatter planlegging og ledelse av militære operasjoner i hele konfliktspekteret.

Forsvarets operasjoner utgjør to hovedgrupper – *nasjonale operasjoner*[7] og *operasjoner utenlands*[8]. De delene av Forsvaret som er engasjert i løpende forvaltningsaktiviteter og styrkeproduksjon omtales som daglig virksomhet og favner således ikke inn under kategorien daglige (freds)operasjoner (FFOD 2007 pkt. 0207-0233).

3.1 Stridens domener og domenemodellen

I følge Forsvarets Fellesoperative doktrine så er strid "…er en kamp mellom mennesker hvor hensikten er å påtvinge en eller flere parter sin egen vilje." (FFOD 2007 pkt. 0402). Stridens domener igjennom domenemodellen beskriver det *kognitive domenet, informasjonsdomenet, det sosiale domenet* og *det fysiske domenet* og beskriver i hvilke domener strid føres og hvordan disse henger sammen, se figur 2 (FFOD 2007 pkt. 0408-0413).

Det kognitive domenet omfatter stridens mentale dimensjon, informasjonen som ligger til grunn i vår situasjonsbevissthet omfattes av informasjonsdomenet, det sosiale domenet favner interaksjonen mellom individer/enheter mens det fysiske domenet representerer de tradisjonelle arenaer for militære operasjoner (FFOD 2007:0410-0413).

[7] Inn under kategorien nasjonale operasjoner er daglige fredsoperasjoner, operasjoner ved nasjonale kriser og operasjoner i væpnet konflikt.
[8] Forsvarets operasjoner utenlands kategoriseres som militære bidrag i fredstid, stabiliseringsoperasjoner, strid mot irregulære styrker og strid mot regulære styrker.

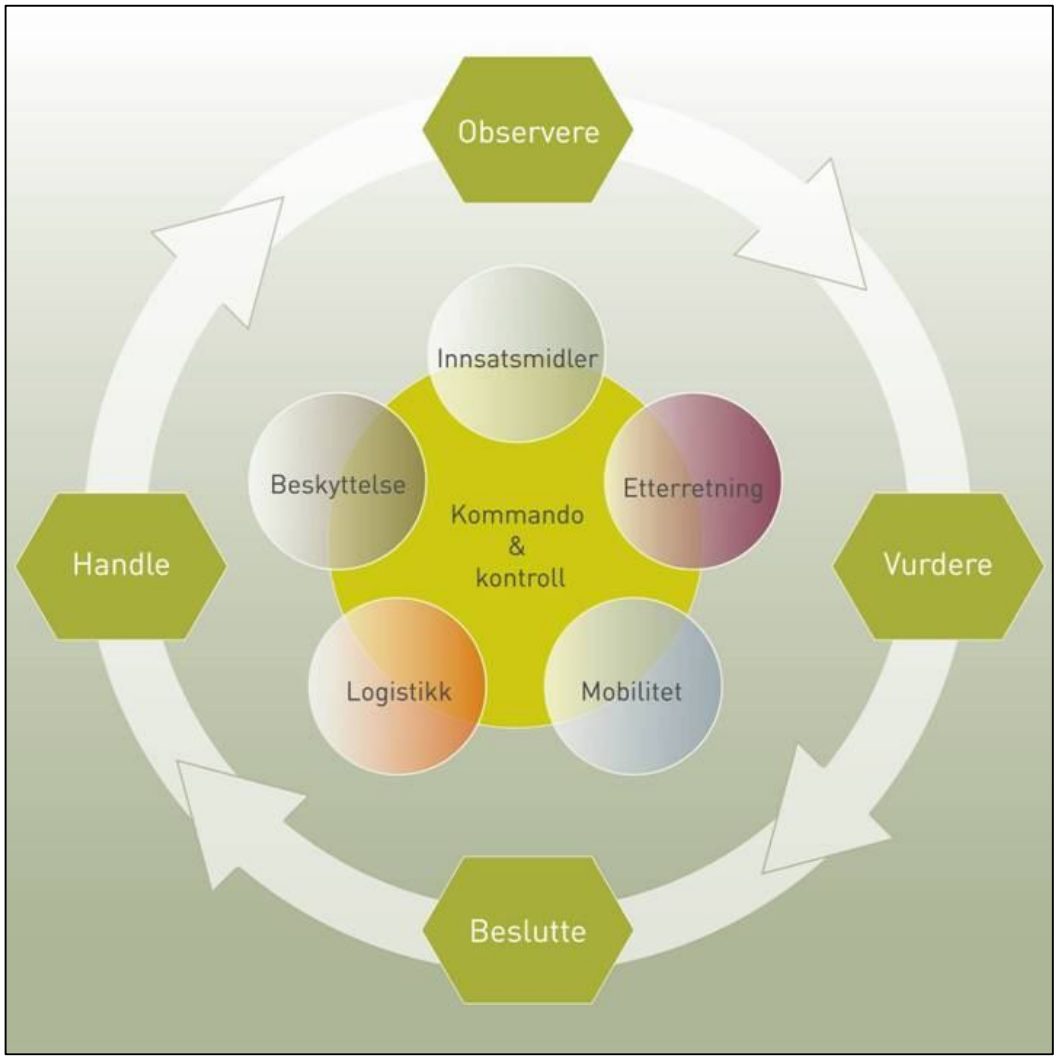
Figur 2 - Domenemodellen (FFOD 2007 s. 70)

3.2 Handlingssløyfen

Handlingssløyfen er slik FFOD ser det "…er en modell for å beskrive hvordan tempo kan oppnås fra det tidspunkt da en hendelse inntreffer til handling iverksettes." (FFOD 2007 pkt. 0428).

Handlingssløyfen består av fire elementer som til sammen utgjør en kontinuerlig prosess hvis formål er å beskrive hvordan tempo kan oppnås som forutsetning for rask beslutningstaking, se figur 3[9].

[9] Handlingssløyfebegrepet ble utviklet av oberst John Boyd (1927-1997) i det amerikanske luftforsvaret på bakgrunn av hans erfaringer som jagerflypilot. Han kalte sin handlingssløyfe for OODA-loop (*Observe*, *Orient*, *Decide* og *Act*). Forsvarets handlingssløyde er slik FFOD ser det (2007 s. 80) en forenkling av OODA-loopen.



Figur 3 – Handlingssløyfen (OODA-loop) og basisfunksjonene (FFOD 2007 s. 78)

3.3 Beslutningstaking

Forsvarets avdelinger og enheter er alle avhengig av et sett med grunnleggende basisfunksjoner: *Kommando og kontroll (K2)*, *innsatsmidler*, *mobilitet*, *beskyttelse*, *etterretninger og logistikk*. K2 funksjonen utgjør kjernefunksjonen og knytter de resterende basisfunksjonene sammen. K2 begrepet innehar mange definisjoner. Denne oppgaven vil bruke FFOD sin beskrivelse av begrepet som det militære begrepet for ledelse av operasjoner. I følge FFOD (2007 pkt. 0574) består begrepet av den organisasjonen, de prosessene og prosedyrene, systemene og det lederskapet som gjør militære sjefer i stand til å lede og kontrollere sine styrker.

Det faktum at informasjonsalderen medfører endringer på alle plan vil også kreve en tettere integrasjon av stridsledelse, planlegging og utførelse av (militære) operasjoner i en sammenhengende og mer parallell prosess. Dette vil kreve et effektivt samvirke mellom alle typer av komponenter i NbF konseptet. I tillegg vil det kreve ”…at deler av

informasjonsbehandlingen helt eller delvis automatiseres dersom, den potensielle tempogevinst skal kunne tas ut." (MFU 2003 s. 26-27). Innføring av beslutningsstøttekomponenter[10] skal bidra til dette. Informasjon benyttes blant annet til problemløsning og for å fatte beslutninger. Beslutninger tas hver dag på grunnlag av tilgjengelig informasjon, kunnskap[11] og erfaringer. Beslutninger kan også fattes på et irrasjonelt grunnlag ut i fra vane eller lyst (Kalseth & Knoop 1996 s. 167).

[10] MFU 2003 omtaler slike komponenter som agenter (MFU 2003 s. 27).
[11] Kunnskapsdimensjonen inntreffer når informasjonen mottas, fortolkes og forstås. (Kalseth & Knoop 1996 s. 167).

4 Nettverkstenkning og NbF

I overgangen fra et industrisamfunn til et informasjons- og kunnskapssamfunn har utviklingen innenfor informasjons- og kommunikasjonsteknologien (IKT) åpnet for nye muligheter på flere samfunnsområder. Nettverkstankegangen oppstod i økonomi- og finanssektoren som en del av globaliseringen av verdensøkonomien. Det er denne måten å tenke nettverk på som er importert til militærsektoren og som blant annet har åpnet for nye muligheter for hvordan militære styrker utformes og opererer (Diesen 2003).

4.1 Nettverkstenkning generelt

I "Darwinian world of business" er det de organisasjoner som ser informasjonens potensial som overlever. Den tilgjengelige informasjonen benyttes for å fatte de rette beslutningene samt utvikle de rette produktene raskt og effektivt (Alberts, Garstka & Stein 2000 s. 21). Produkter i denne sammenhengen vil for eksempel kunne være utvikling av (de rette) militære kapasiteter. Ønsket om konkurransefortrinn er enhver virksomhets målsetning. Stabell og Fjeldstad (1998 s. 414-415) presenterer tre alternative måter å tilnærme seg dette på: V*erdikjede, verksted* og *nettverk*[12]. Det er i følge Stabell og Fjeldstad (1998 s. 415) disse tre generiske tilnærminger som gir grunnlaget for en teori og et rammeverk for analyse av forretningsmessig konkurransefortrinn. Med utgangspunkt i oppgavens tematikk er det bare nettverksalternativet som vil belyses noe mer i detalj.

Verdinettverk er avhengig av en grunnleggende teknologi som knytter sammen kunder (noder) som allerede er, eller ønsker å være, avhengig av hverandre. Det er nettverksdelen av begrepet som understreker at det nettopp er selve nettverket som utgjør verdipotensialet (Stabell & Fjeldstad 1998 s. 427)[13]. FFOD (2007 pkt. 0309) beskriver nettverkstenkning som å kontinuerlig utvikle mennesker, organisasjon og teknologi igjennom mest mulig effektiv ressursorganisering for å oppnå økt integrasjon, situasjonsbevissthet samt forståelse av sjefens intensjon.

Innenfor kommersiell sektor er det eksempler på at økt lønnsomhet, konkurransefortrinn og (informasjons)overlegenhet oppnådd ved å transformere til nettsentriske konsepter [14].

Målsetningen om konkurransefortrinn i form av militær (informasjons)overlegenhet er noe av

---

[12] Stabell og Fjeldstad omtaler de tre verdikonfigurasjonene som "chain", "shop" og "network" (Stabell & Fjeldstad 1998).

[13] Metcalfe's lov beskriver verdipotensialet til nettverk ved å uttrykke at når antall noder i et nettverk øker lineært, så øker den potensielle effektivitetsverdien i nettverket eksponentielt som "square number" av antall noder i nettverket (Alberts, Garstka & Stein 2000 s. 32).

[14] Det presiseres at nettsentriske konsepter ikke automatisk gir effektive organisasjoner, men ved nettsentriske konsepter som grunnleggende tenkning vil det kunne legge til rette for økt effektivitet (Alberts, Garstka & Stein 2000 s. 10).

bakgrunnen for at nettverkstenkningen ble satt på dagsorden også innenfor militære kretser (MFU 2003 s. 6; Alberts, Garstka & Stein 2000 s. 1-2).
Selv grunnideen til nettsentrisk krigføring må sies å være forankret i den teknologiske utviklingen og som "… focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise." (Alberts, Garstka & Stein 2000 s. 98). Men som et resultat av kunnskap om menneskelig atferd i organisasjoner generelt er det viktig å erkjenne at "…[in t]aking the steps toward NCW[15], there is a need to understand what the proposed reorganizations and new technology will mean for the human being working within the organization." (Bjørnstad 2004 s. 8-9).

4.2 NNEC – utviklingen i NATO

Det amerikanske Network Centric Warfare (NCW) konseptet har de siste årene blitt et moteord innen forsvarsdebatten. Tross dette så varierer de ulike tilnærmingene noe, herunder hva de enkelte nasjoner omtaler konseptet som[16]. Storbritannia omtaler konseptet som Network Enabled Capabilities (NEC). I 2003 ble det bestemt at begrepet NATO Network Enabled Capabilities (NNEC) skulle være NATOs betegnelse på konseptet og har siden den gang styrt utvikling innenfor NNEC i alliansen (*NNEC: Utviklingen i NATO*). Norge og Sverige på sin side omtaler konseptet som NbF. (Bjørnstad 2004 s. 7).
NATO Consultation, Comand and Control Agency (NC3A) har utarbeidet en mulighetsstudie i forbindelse med NNEC. Hensikten med studien har vært å utvikle et omfang og visjon for NNEC samt å etablere den nødvendige konteksten for utvikling av Consultation, Command and Control (C3) aspektene i NNEC (NNEC FS 2005 s. 5). NNEC sin transformasjonsstrategi er basert på NATO sitt konsept for operasjonell transformasjon bestående av fire operasjonelle transformasjonsfaser, se figur 4. Idéen er at utviklingen vil være en evolusjonær stegvis prosess for måloppnåelse av de langsiktige ambisjonene i NNEC.

[15] NCW står for Network Centric Warfare og er det amerikanske begrepet for nettsentrisk krigføring.
[16] Det faktum at forskjellige nasjoner legger forskjellige momenter som del av sine respektive nettsentriske konsepter henger blant annet sammen med kulturelle forskjeller nasjonene i mellom (Bjørnstad 2004).

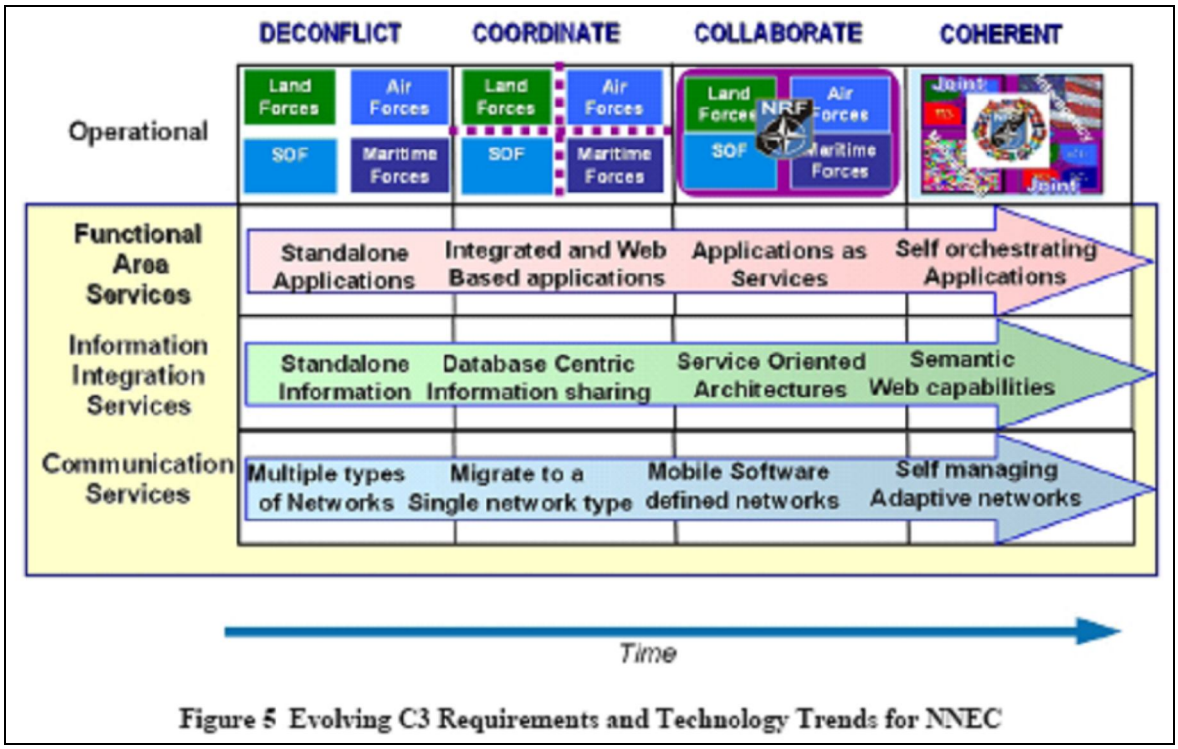


Figure 5 Evolving C3 Requirements and Technology Trends for NNEC

Figur 4 – NATO NEC transformasjonsstrategi (NNEC FS 2005 s. 11).

Hver fase i transformasjonen representerer forskjellige operasjonelle krav, herunder behovet for å utvikle nye system kapabiliteter. De-konflikt fasen (deconfliction phase) representerer funksjonell ”stovepipes” og beskriver situasjonen forut for transformasjonen. Med funksjonelle ”stovepipes” menes bruken av frittstående applikasjoner/systemer, databaser og forskjellige nettverkskommunikasjonstyper. Koordineringsfasen (coordination phase) vil være sentral når det gjelder informasjon og kommunikasjon av visjonen. Samarbeidsfasen (collaboration phase) representerer selve transformasjonsfasen hvor samarbeid på tvers av forsvarsgrener og nivåer er sentralt. Det er også i denne fasen transformasjonen over til et rendyrket tjenestefokusert konsept skjer. Transformasjonen avsluttes med fasen (coherent effects phase) som representerer den modne/fullstendige visjonen. Målsetningen er et sømløst og transparent samarbeid mellom alle involverte parter med den hensikt å oppnå økt operasjonell effektivitet (NNEC FS 2005 s. 11).

4.3 Nettverksbasert forsvar (NbF)

De overordnede rammevilkårene av Forsvarets transformasjon til et nettverksbasert Forsvaret ble presentert i Stortingsproposisjon nummer 42 (2003-2004): *Den videre moderniseringen av Forsvaret i perioden 2005-2008*. NbF er det norske konseptet for nettsentrisk krigføring og er en nasjonal tilpasning av det amerikanske NCW. Konseptet beskriver hvordan militære operasjoner kan gjennomføres ved sammenkopling av militære kapasiteter i nettverk ved bruk av

informasjonsteknologi (MFU 2003 s. 6). Målsetningen er økt stridsevne som i større grad enn før knytter sammen komponenter i innsatsrommet. Dette innebærer et fokusskifte fra hva hver enkelt plattform kan yte, til hva et nettverk av plattformer kan yte. Fremtidsvisjonen er et fleksibel/dynamisk Forsvar som "… kan utnytte skiftende muligheter i innsatsrommet ved en stadig rekonfigurering av den totale styrken i nye styrkekombinasjoner, tilpasset de oppdrag som til enhver tid får prioritet." (MFU 2003 s. 24). Nøkkelen til dette er bruk av moderne teknologi og en fleksibel bruk av menneskelig og organisatoriske ressurser. Organisasjoners og individers evne til å utnytte tilgjengelig informasjon er sentral. Spesielt det å ha et stort fokus på de menneskelige aspekter i konseptet er av Bjørnstad (2004 s. 7) fremhevet som sentralt da enhver organisasjonsutvikling nettopp har utfordring med at menneskelig opptreden vanskelig (umulig?) lar seg prediktere[17]. FFOD beskriver NbF som et samhandlingskonsept for økt fleksibilitet og effektivitet ved å se teknologi, kompetanse, organisering og løpende prosesser i sammenheng (FFOD 2007 pkt. 0453).

4.3.1 NbF tilstandsbeskrivelser

Utviklingen mot NbF vil være en kontinuerlig prosess. I den forbindelse er det definert en serie tilstandsbeskrivelser for NbF: *Innledende*, *integrerende* og *gjennomgripende* (Enemo 2006). Tilstandsbeskrivelsene er en beskrivelse av hvordan det forventes/hvordan man tro at NbF kan komme til å påvirke Forsvaret. Sagt på en annen måte er disse gradsbeskrivelsene et forsøk på å forklare, på et abstrakt nivå, hvordan fremtiden kan komme til å se ut. Gradene er således ikke en oppskrift, men et forsøk på å oppsummere hva en mulig fremtid i lys av NbF utviklingen kan medføre.

Det er skrevet mye om forventninger til NbF og overordnede tiltak er identifisert. FFI betrakter NbF gjennom flere hypoteser som beskriver tiltak som forventes å gi økt effekt (Reitan & Pålhaugen 2004). Disse hypotesene er samlet under seks tema: *Nettverksorganisering av ressurser*, *desentralisering*, *selvsynkronisering*, *intensjonsbasert ledelse*; *sentralisering*; *skape og utnytte felles situasjonsforståelse*; *skape felles intensjon*, *enhetlig utførelse og geografisk uavhengighet*, *mobilitet*. I etterkant har forventningene til NbF blitt bearbeidet videre i NbF tenketank (Enemo 2006). NbF konseptet er operasjonalisert til ni forskjellige faktorer: *Nettverksbesvissthet*, *Doktrine*, *Organisasjon og prosess*, *Eksperimentering /øving/trening /utdanning/ kompetanse*, *Informasjonsinfrastruktur og teknologi*, *Individ og kultur*, *Interoperabilitet (PTO[18])*, *Ledelse, beslutningsprosesser* og *Økonomi* (Enemo 2006), se tabell 1.

[17] Bjørnstad bruker begrepet NCW i tittelen på sin rapport som både i teori og praksis belyser de menneskelige aspektene ved NbF-konseptet (Bjørnstad 2004).
[18] Prosess, teknologi og organisasjon (PTO).

Tabell 1 – NbF tilstandsbeskrivelser[19] (Enemo 2006)

Faktor	**Innledende NbF (grad 1)** Tilsvarer UK NEC: Initial og NNEC: Coordination 3	**Integrerende NbF (grad 2)** Tilsvarer UK NEC: Transitional og NNEC: Integration 4	**Gjennomgripende NbF (grad 3)** Tilsvarer UK NEC: Mature og NNEC: Coherence 5
Nettverksbevissthet	Forsvaret som organisasjon har overordnet kunnskap om NBF	Organisasjonen har en utbredt forståelse for NBF	Organisasjonen har en gjennomgripende evne til å benytte NBF-tankegang i all sin virksomhet
Doktrine	Ingen doktrinære sprang fra dagens situasjon	Konsepter og doktriner er basert på NBF	Utvikling/videreutvikling av konsepter og doktriner er kontinuerlig og løpende
Organisasjon og prosess	Organisasjonen er noe mer fleksibel enn i dag, dog fremdeles med stor grad av sekvensielle prosesser. Organisasjonen er preget av større grad av horisontal koordinering enn i dag, men det er fremdeles stor grad av vertikal styring og faste prosedyrer.	Organisasjonen er mer fleksibel og dynamisk og med flatere struktur enn i Grad 1. Nye prosesser og prosedyrer utvikles, spesielt med tanke på å redusere bruken av sekvensielle prosesser. Organisasjonen preges av å være ved et veiskille, der vertikal styring og faste prosedyrer gradvis må vike for desentralisert styring og horisontal koordinering.	Organisasjonen er dynamisk situasjonstilpasset med parallelle prosesser. Organisasjonen er preget av stor grad av horisontal koordinering (selvorganisering), desentralisert styring og lite distanse mellom overordnet-underordnet-sideordnet.
Eksperimentering /øving/trening /utdanning/ kompetanse	”NBF-filosofien” er integrert i all utdanning. Eksperimentering vektlegges i større grad enn i dag, men det er fremdeles et relativt klart skille mellom dag-til-dag administrativ virksomhet og eksperimentering/trening/øving	Eksperimentering/trening/øving foregår ved hyppige, små-skala, mer fokuserte øvelser.	Intet skille mellom den daglige virksomheten og eksperimentering/-trening/øving
Informasjonsinfra-struktur og teknologi	En teknisk infrastruktur som i hovedsak består av forbedringer av dagens eksisterende utstyr, med proprietære systemer og individuelle løsninger. Eksisterende informasjon er tilgjengelig for flere enn i dag. Et felles nettverk for utvalgte plattformer og komponenter er opprettet, der man har tilgang på et felles situasjonsgrunnlag.	Alt eksisterende materiell og nyanskaffelser er ”Netready”, med vekt på ”PlugNPlay” i et felles gjennomgående kommunikasjonsnettverk. En integrerende informasjonsstyring sørger for at all informasjon som finnes i nettverket kan være tilgjengelig for enhver med behov, uten at det kan garanteres at informasjonen	En helhetlig informasjonsinfrastruktur der ”alt og alle” er på nett. En gjennomgripende informasjonsstyring sørger for at all informasjon i nettverket er tilgjengelig, forståelig og utnyttbar for enhver med behov. En høy grad av teknologisk modenhet muliggjør en effektiv utnyttelse av nettverket. IKT blir sett på

[19] Forsvarets stabsskole (FSTS) har i 2008 fått oppdrag av SJ INI om å konkretisere NbF tilstandsbeskrivelsene ytterligere. Dette arbeidet vil kunne medføre at tabellen som er benyttet i oppgaven i fremtiden ikke nødvendigvis vil samsvare med det som er Forsvarets fremtidige målbilde innenfor NbF.

	Organisasjonens IKT bruk er motivert mer ut fra et rasjonaliseringssynspunkt enn fra et "muliggjørende" synspunkt. Konnektivitet er et nøkkelbegrep.	nødvendigvis kan forstås og nyttiggjøres av alle brukere. Innovativ bruk av IKT blir stadig viktigere i motsetning til IKT som rasjonaliseringsverktøy.	som "muliggjørende" for å bidra til å forbedre eksisterende prosesser eller etablere nye (innovasjon, i motsetning til automatisering).
Individ og kultur	Det enkelte individ identifiserer seg i større grad med grupper innen organisasjonen (avdeling) enn med organisasjonen som helhet. Menneskene i organisasjonen er i hovedsak generalister og heller mot en individorientert arbeidsform. Evnen til å håndtere endringer i organisasjonen er bedre enn hva som er tilfelle i dag (pragmatisk). Mer felles utdanning blir iverksatt for å bygge felles identitet og kunnskap, og man begynner å utdanne mer spesialister.	Spesialister har begynt å erstatte generalister i større og større grad. Evne til samarbeid vektlegges fremfor individorientert arbeidsform. Fellesskapet og Forsvaret som helhet vil bli tillagt større vekt enn i Grad 1. Spesialister har begynt å erstatte generalister i større og større grad. Organisasjon, trening, utdanning og utvelgelse bygger opp under og utvikler flere og mer helhetlige sosiale tilhørigheter, for dermed å gi individene (og organisasjonen som konsekvens) bedre evne til samarbeid, fleksibilitet og evne til å håndtere organisasjons-endringer. Organisasjon, trening, utdanning og utvelgelse bygger også opp under individenes evne til selvstendig tenkning og beslutningstagning; kritisk og innovativ tenkning og beslutningstagning blir vektlagt.	Spesialister/rollespesialisering har erstattet tradisjonell funksjonsinndeling. Evne til samarbeid vektlegges fremfor individorientert arbeid, og fremdyrkes gjennom organisasjonelle incentiver og flere og helhetlige sosiale tilhørigheter. Menneskene identifiserer seg primært med organisasjonen som helhet (i motsetning til subkulturer eller undergrupper). Organisasjonen er ikke-statisk og fleksibel og menneskene er opplært til å fungere i et slikt miljø. Organisasjonen bygger opp under individenes evne til selvstendig tenkning og beslutningstagning. Hvem som skal utføre en spesifikk oppgave er avhengig av hvem som anses mest kompetent.
Interoperabilitet (PTO)	Interoperabilitet er fokusert på samarbeidende avdelinger (på tvers av forsvarsgrener) i militære operasjoner.	Interoperabilitet er gjennomgående internt i Forsvaret og også til dels mot eksterne aktører. Fremdeles fokus på militær interoperabilitet.	Interoperabilitet er gjennomgripende internt i Forsvaret og mot prioriterte eksterne aktører, og sees på som svært viktig også utover det militære domenet.
Ledelse, beslutningsprosesser	Ledelse og beslutningsprosesser er i stor grad basert på prosedyrer og rutiner. Ledelse ved posisjon.	Ledelse og beslutningsprosesser vil være preget av større grad av intuisjon og bruk av nettverket. Hovedsakelig desentralisert makt og beslutningstagning; sentralisert beslutningstagning i strategisk kritiske situasjoner.	Ledelse og beslutningsprosesser vil være kjennetegnet av en god balanse mellom transaksjons- og transformasjonsledelse, med helhetlige tilnærminger til problemløsning. Situasjonstilpasning og effektoppnåelse er et nøkkelbegrep. Ledelse ved kompetanse. Fullt ut desentralisering av makt og beslutningstagning;

			sentralisert beslutningstagning er forbeholdt strategisk kritiske situasjoner.
Økonomi	God kost-effektivitet, i og med at man vil få stor effekt ut av de midler som brukes. Organisasjonen har fokus på såkalte "low-hanging fruits" eller "quick wins".	Dårligere økonomisk kosteffektivitet enn Grad 1. Fokuset vil i større grad være flyttet fra teknologi til organisasjon, noe som kan gi mindre forutsigbarhet i transformasjons-prosessen. Samtidig vil større teknologi-investeringer erstatte dagens arv. På enkelte områder vil derfor tilbakeslag kunne inntreffe.	Bedre kost-effektivitet enn Grad 2

4.3.2 Situasjonsbevissthet

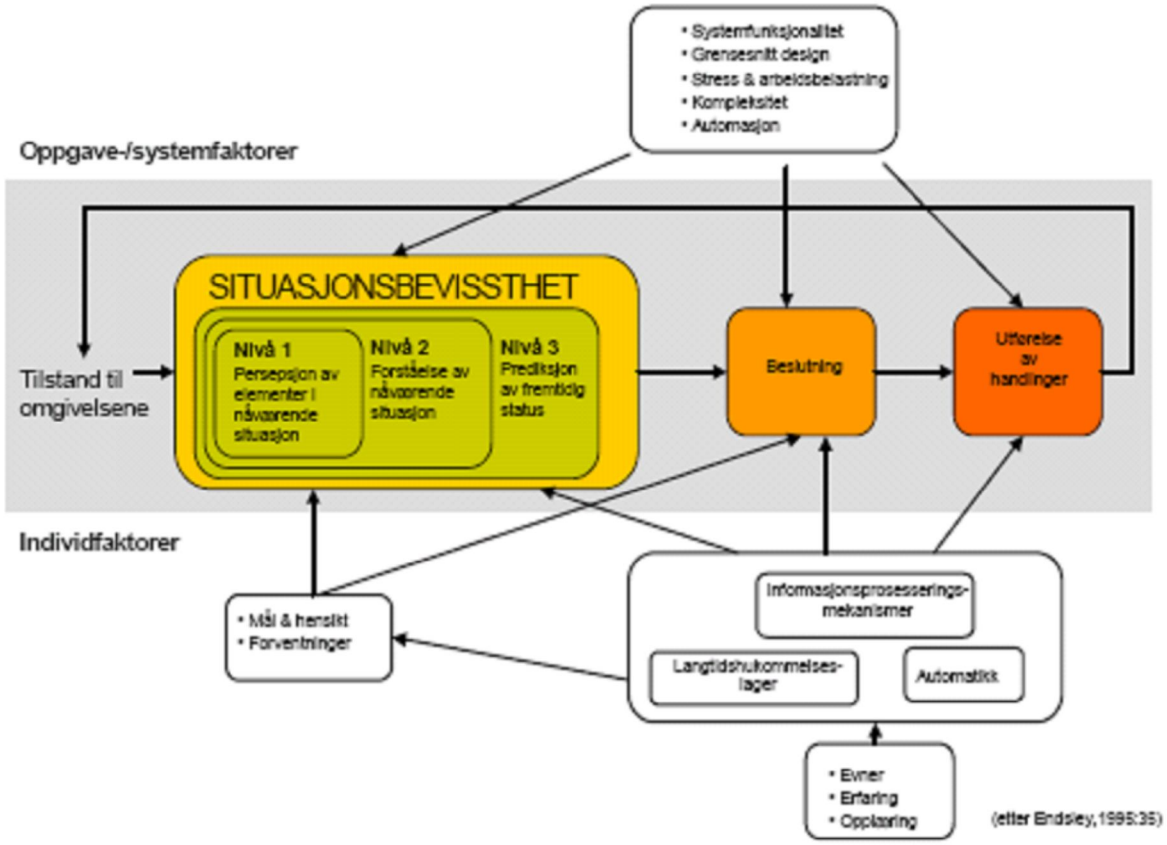
En målsetning med NbF er "… å oppnå størst mulig grad av felles situasjonsbesvissthet…på kortest mulig tid, raskere enn motstanderen, som grunnlag for selvorganisering og selvsynkronisering av effekt rettet mot motstanderens kapasiteter." (MFU 2003 s. 15).

Deler av den informasjonen mennesker skaffer seg lagres i hukommelsen som språklig eller ikke-språklig kunnskap. Denne handlingen forutsetter bevissthet og oppmerksomhet, hvor bevisstheten sammenkopler menneskers indre verden og omgivelsene. Summen av menneskers kunnskap, det de vet og kan utgjør bevisstheten produkt (Olafsen & Bråthen 2004 s. 24).

Den mest anerkjente og siterte situasjonsbevissthetsmodell er utarbeidet av Endsleys (1995 i. Olafsen & Bråthen 2004 s. 24-25[20]). Modellen er en teoretisk modell for situasjonsbevissthet ved beslutningstaking i dynamiske og komplekse situasjoner, se figur 5.

Begrepet situasjonsbevissthet omfatter tre elementer, situasjonsoppfattelse, situasjonsforståelse og situasjonsprediksjon. Begrepene har innbyrdes kvalitetsforskjell (Endsleys 1995 i. Olafsen & Bråthen 2004 s. 25; FFOD 2007 s. 95). Denne oppgaven bruker begrepet situasjonsbevissthet gjennomgående og skiller således ikke på gradsforskjellene i bevisstheten. FFOD poengterer at situasjonsbevissthet "…er en forutsetning for evnen til å synkronisere handlinger uten at de nødvendigvis foreligger en detaljert plan." (FFOD 2007 s. 95).

[20] Endsleys originale figur er oversatt til norsk av Olafsen og Bråthen og er bakgrunnen for at denne oppgaven ikke bruker Endsleys orginale figur.



Figur 3.1 Endsleys modell av situasjonsbevissthet i dynamisk beslutningstakning

Figur 5 – Endsleys situasjonsbevissthetsmodell (Endsleys 1995 i. Olafsen & Bråthen 2004 s. 25).

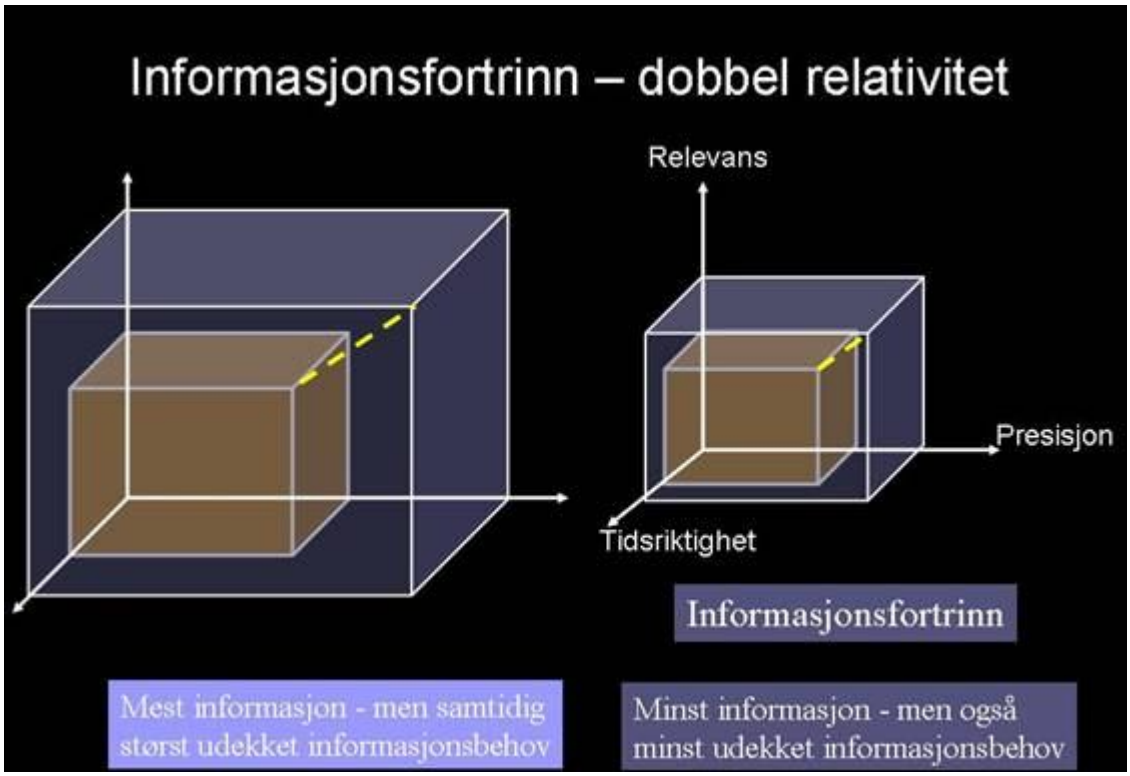
4.3.3 Informasjonsoverlegenhet

Tilgang på (riktig og) tilstrekkelig informasjon er sentralt for at beslutningstakere og andre skal kunne inneha tilstrekkelig situasjonsbevissthet for derigjennom på en rask måte kunne omsette informasjonen til handling[21]. Denne tilstanden omtales gjerne som informasjonsoverlegenhet. Målsetningen er å inneha relativ informasjonsoverlegenhet i forhold til motstanderen. Denne oppgaven vil ikke beskrive i detalj hva informasjonsoverlegenhet er utover at det er en tilstand som bare oppnås når en styrke har muligheten for å utnytte en overlegen informasjonsposisjon relativ til motstanderen (Berglund 2004 s. 13).

Idéen med informasjonsoverlegenhet er et grunnleggende godt prinsipp, men prinsippet er forbundet med en dobbel relativitet, se figur 6. Som informasjonskuben til venstre viser så vil en situasjon med mest informasjon samtidig være den situasjonen med størst udekket informasjonsbehov. Sammenlignet med kuben til høyre så gir tilgang på mindre informasjon

[21] FFOD (2007 s. 92) omtaler det å kunne omsette informasjon til handling som beslutningsoverlegenhet.

samtidig minst udekket informasjonsbehov. Dette er tilstander det er viktig å være bevisst – både ved ”innsamling” av informasjon for å skaffe situasjonsbevissthet, men også som grunnlag for beslutningstaking.



Figur 6 - Informasjonsfortrinn og prinsippet om dobbel relativitet (Ødegaard 2002)

5 Informasjonsinfrastrukturer og MIL INI

En viktig forutsetning for NbF konseptet er en velfungerende og fremtidsrettet MIL INI hvor samarbeid og deling av informasjon er sentrale prinsipper. Ved å realisere MIL INI som en tjenesteorientert arkitektur legges det til rette for at informasjonstjenester tilgjengeliggjøres igjennom NbF konseptet (Hafnor 2006 s. 9).

5.1 "Community of Interest"

Community of Interest (COI) omhandler såkalte interessefellesskap som er en gruppering av mennesker, en konstruksjon, med felles mål, interesser, oppgaver og/eller oppdrag som grunnlag for felles behov for å utveksle og dele informasjon. Det felles behovet må ha et omforent språk (vokabular) for at informasjonsutveksling skal kunne skje. Sagt på en annen måte er COIs virtuelle samhandlingsarenaer (Hafnor 2006 s. 14).

COIs kan dannes til enhver tid. Det ikke er noen begrensninger eller regler forbundet med dannelsen av COIs. Medlemmer kan være medlemmer i flere COIs samtidig og medlemskap kan være både frivillig og obligatorisk. Deling av informasjon skjer både internt mellom medlemmene i en COI og eksternt, dvs mellom forskjellige COIs. De finnes forskjellige typer av COIs: *Situasjonsbestemt, Funksjonsorientert, Kryssfunksjonell* og *Ad hoc* (Hafnor 2006 s. 14-15). Situasjonsbestemte COIs utnytter de ressurser som eksisterer i nettverket. Institusjonelle COIs utvikler ressurser i form av vokabularer, datamodeller og metadatastrukturer. Funksjonsorienterte COIs på sin side involverer aktører innenfor spesifikke fag- og kompetansemiljøer. Mens kryssfunksjonelle COIs utgjør tverrfaglige interessefellesskap på tvers av flere fag- og kompetansemiljøer (Hafnor 2006 s. 17).

Forsvaret har i dag naturlige slike interessefellesskap i form av funksjonelle og faglige (kompetanse)miljøer hvor logistikk og K2 er to eksempler. Prinsippet i COI går dog utover slike fagsøyler ved at interessegruppene gjerne er tverrfaglige samt geografisk og organisatorisk uavhengige.

5.2 Informasjonsinfrastrukturer

I takt med den økte oppmerksomheten rundt Internett har opprettelsen av INI vært heftig debattert blant politiske aktører. En infrastruktur i henhold til Hanseth og Monteiro (1998 kap. 1) er en ureduserbar enhet som er delt av et stort fellesskap og hvor den samme "tingen" benyttes av alle brukerne. I forhold til informasjonssystemer, som gjerne er utviklet for å ivareta dedikerte

organisatoriske oppgaver, så har INI ingen fast hensikt for å rettferdiggjøre sin eksistens. Sagt på en annen måte så kan INI sees på som ”neste generasjons” informasjonssystemer.

Tenkningen rundt INI har også vokst frem innenfor mer avgrensede miljøer (”communities”). Individuelle organisasjoner har adoptert begrepet for å beskrive den samling av informasjonssystemer, brukere, informasjonsartefakter, (arbeids)prosesser, og integrasjonen av alle disse faktorene, som er en naturlig del av virksomheten (Hanseth & Monteiro 1998 kap. 1).

Et viktig punkt når vi belyser INI er at fremtidens infrastruktur vil være en utvidelse, kombinasjon, substitusjon og ”pådytting” (eng: superimposition) av de deler som allerede er en del av (informasjons)strukturen. Med andre ord (fremtidens) INI utvikles aldri fra bunnen av. Videre vil arbeidet med å etablere en velfungerende INI være forbundet med en omfattende sosioteknisk bestrebelse/anstrengelse (Hanseth & Monteiro 1998 kap. 1).

Den økte tilgangen på informasjon i Forsvaret skjer følge Berglund (2004 s. 16; JP-3.13 1998 s. I-13-I-14) i tre informasjonsinfrastrukturer samtidig:

- Den globale informasjonsinfrastruktur (GII); den verdensomspennende sammenkoblingen av kommunikasjonsnettverk, datamaskiner, databaser etc.
- Den nasjonale (NII); NII er lik GII men for nasjonale anliggende. Det gjøres oppmerksom på at NII i denne sammenheng ikke samsvarer med NATO sin MIL INI betegnelse som også forkortes NII. Det er også mulig å tenke tilsvarende tredeling nettopp med NATO NII som mellomliggende nivå.
- Forsvars INI (MIL INI); MIL INI er tett integrert med NII og brukes om de midler, mennesker og organisasjoner som sammenbinder og støtter militære styrkers operasjoner på alle nivå.

5.3 MIL INI

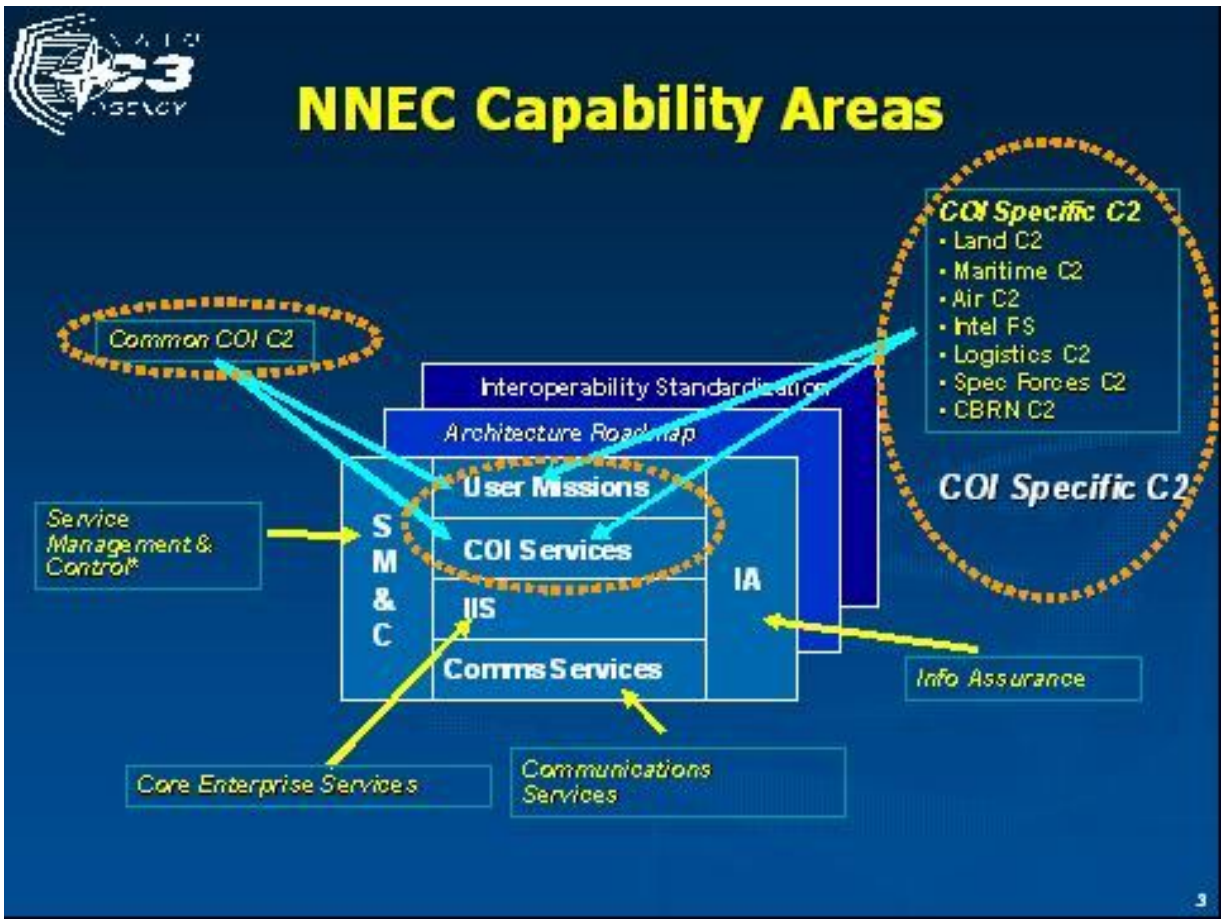
Det eksisterer mange nasjonale beskrivelser og definisjoner av INI i militær kontekst, heretter omtalt som MIL INI. MFU 2003 definerer informasjonsinfrastrukturen til å være ”…[k]ombinasjonen av informasjonssystemene, informasjonsbehandling og kommunikasjonsløsninger.” (MFU 2003 s. 26). Hedenstad definerer MIL INI som ”… *en sammenkopling (netting) av ressurser*…som muliggjør deling av informasjon og samarbeid mellom aktørene som har tilgang til nettet.” (Hedenstad 2002 s. 10, kursiv i originalteksten).

FFOD (2007 pkt. 0458-0459) omtaler MIL INI som alle informasjonssystemer som sørger for kommunikasjon mellom komponentene i systemet; hovedkomponentene *sensorkomponenter*, *beslutningskomponenter* og *innsatskomponenter* i tillegg til *beslutningsstøttekomponenter* og *samhandlingskomponenter*. Doktrinen beskriver videre at MIL INI består av teknisk utstyr for *bearbeiding*, *lagring*, *distribuering* og *presentasjon* og at infrastrukturen også omfatter *menneskene* som opererer og støtter systemene samt *standarder* og *prosedyrer* (FFOD 2007 pkt. 0460).

5.3.1 NATO referansemodell for INI (NATO NII)

NATO har som del av sitt NNEC arbeid utarbeidet en Networking and Information Infrastructure (NATO NII) som samsvarer med vår MIL INI referansemodell, se figur 7.

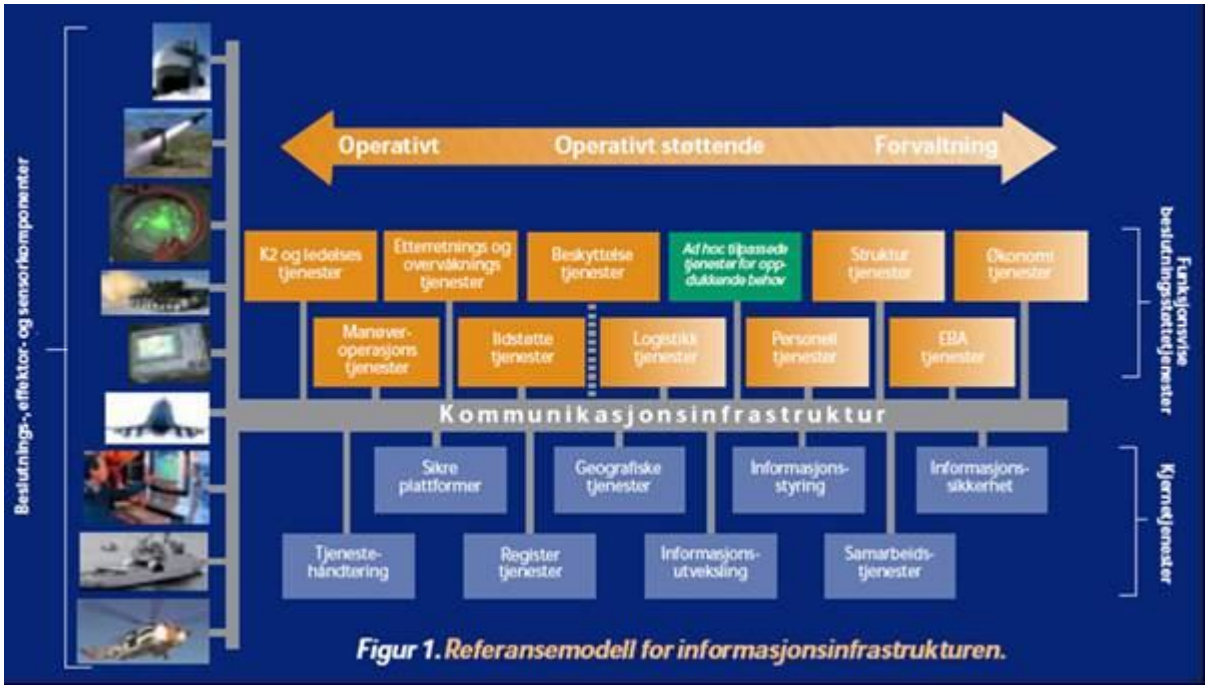
I NATO arbeides det med en tjenesterammeverk som operasjonaliserer den overordnede referansemodellen. Hensikten med et slikt tjenesterammeverk er å forankre NATO NII arbeidet internt i alliansen, samt opp mot nasjonale MIL INI initiativ.



Figur 7 - NATO Networking and Information Infrastructure (NATO 2008).

5.3.2 FDs referansemodell for INI

Som en del av Forsvarets strategiske policy for bruk av IKT er det utarbeidet en omforent MIL INI referansearkitektur, se figur 8. Denne referansemodellen består av fire overordnede tjenesteområder: *Funksjonsvise beslutningsstøttetjenester*; *felles kjernetjenester*; *kommunikasjonsinfrastruktur* og *sammensatte løsninger*. Hvert og et av disse overordnede tjenesteområdene består av et sett av underliggende tjenester. Referansearkitekturen vil være en sentral premissgiver for det videre arbeidet med NbF og MIL INI i Forsvaret, herunder fremtidige materiellinvesteringer.



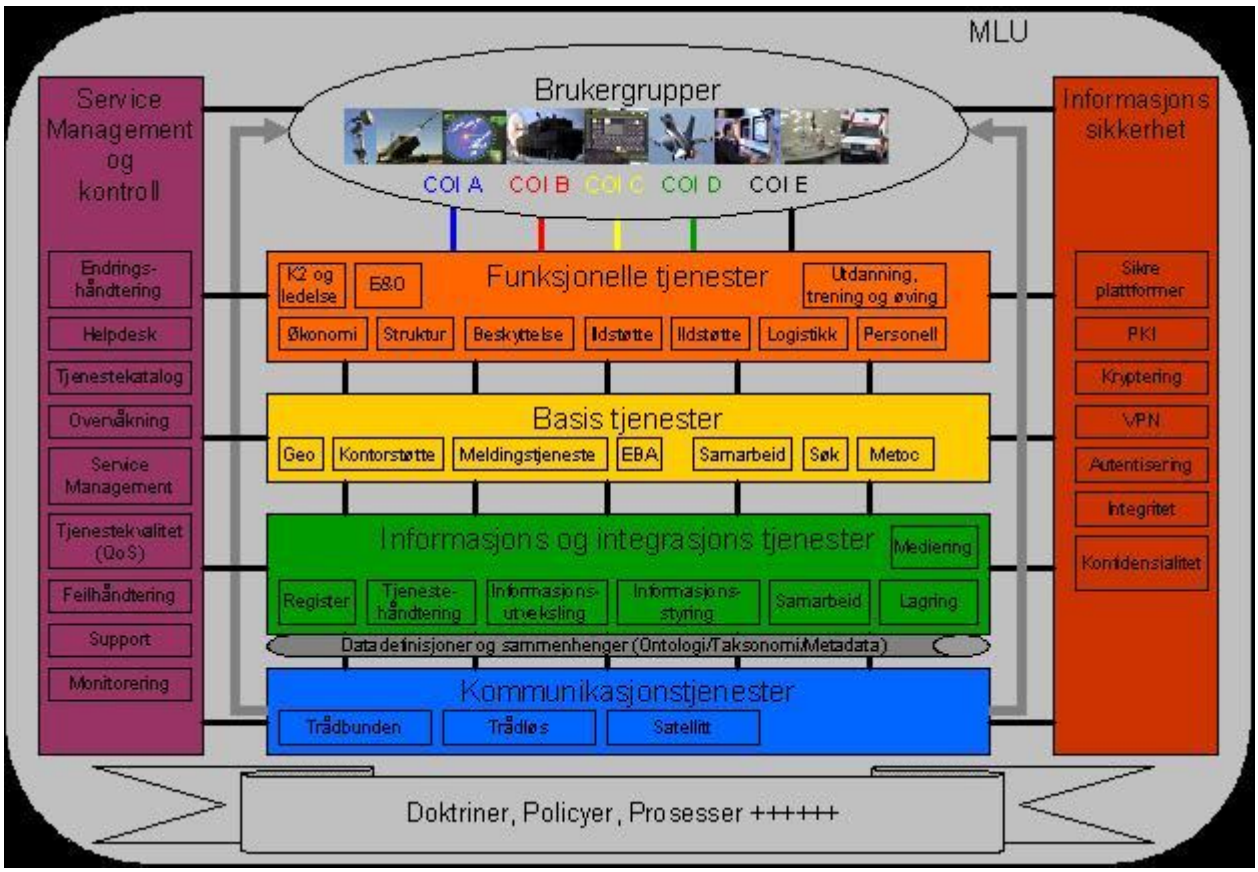
Figur 8 - Forsvarsdepartementet (FD) sin referansemodell for MIL INI (IKT 2005)

I regi av FD pågår det i skrivende stund en revisjon av FDs referansemodell for MIL INI. Innspill til dette arbeidet er fremsendt FD, men det er ikke gjennomført noe konkret revisjonsarbeid enda. Den foreslåtte reviderte referansemodellen samsvarer i stor grad med det transformasjonsområdet og NATO NII arbeidet som gjøres i NATO, se figur 9.

5.4 Informasjonsstyring

Ønsket og behovet for styringen av informasjon har alltid vært til stede, men har endret seg i takt med den globale utviklingen av informasjonsteknologien. Tidlig var informasjonsstyring tradisjonelt begrenset til filvedlikehold og styring av filer, mens det etter hvert også kom til å inkludere ”data- og informasjonsvedlikehold”. Denne endringen medførte behov for

grunnleggende teoriforståelse og god kompetanse innenfor fagområdet informasjonsstyring. En visjon i profesjonelle informasjonsmiljøer er å kunne imøtekomme "rett informasjon til rett person i rett tid". Problemet har vært at profesjonene har manglet gode nok metoder og verktøy for å kunne imøtekomme denne visjonen (Kalseth & Knoop 1996 s. 9).



Figur 9 - Utkast til ny referansemodell for MIL INI (EXP 2008)

MFU definerer informasjonsstyring[22] "…som planlegging, budsjettering, håndtering og kontrollering av informasjon gjennom hele dens livssyklus…for på en sikker måte å skaffe riktig informasjon, til rett tid og sted, fra sikre kilder, i en form brukere kan forstå og bruke for å utføre oppdraget effektivt." (MFU 2003 s. 28). FFOD omtaler informasjonsstyring som "…prosessen som skal sikre at den kvalitativt beste informasjonen når frem til og danner et best mulig beslutningsgrunnlag for riktig bruker… [og omfatter] rutiner, prosesser og systemer for produksjon, lagring og styring av informasjon…" (FFOD 2007 pkt. 0467). Sagt på en annen måte ligger kravet om beslutningstaking som grunnlag for den (operative) beslutningsprosessen.

[22] Begrepet informasjonsstyring inneholder slik det er presentert i MFU (2003 s. 30) fem hovedelementer: *Ressursstyring, virksomhetsprosesser, utvikling av informasjonsstruktur, tilveiebringelse av informasjonsteknologi* og *sikkerhet*.

I hvor stor grad en gjennomføring av en (militær) operasjon er å anse som vellykket er i henhold til MFU 03 (2003 s. 27) i stort avhengig av i hvilken grad dens informasjonsbehov er tilfredsstilt. Informasjonsstyring medfører å ha et bevisst forhold til hvordan informasjonen innhentes, behandles, distribueres og brukes for å sikre informasjonsbehovet til egen militær operasjon og egne militære styrker. Sagt på en annen måte er informasjonsstyring et virkemiddel for å (MFU 2003 s. 29):

- sikre relevant informasjon til egne beslutningsprosesser (gjennomføring av handlings-/beslutningssløyfer, f eks OODA-loop)
- spre informasjon om beslutninger og intensjoner (ordregiving mm)
- sikre at underlagte ledd har tilgang til informasjon som gir grunnlag for rasjonell og effektiv virksomhet (planlegging og gjennomføring av (militære) operasjoner)

For å oppnå tilsiktet effekt av NbF er effektiv informasjonsstyring sentralt. Følgende overordnede krav for effektiv informasjonsstyring er utarbeidet (FFOD 2007 pkt 0469): Menneskelig og maskinell bearbeiding, skyv- og trekkprinsipper, beskyttelse og seleksjon, tilkopling til sivile systemer og interoperabilitet med NATO. Hedenstad (2002 s. 18) skriver i sin rapport at informasjonsstyringen påvirker MIL INI ved at den "…setter rammene for hvilken informasjon som skal inn i infostrukturen og hvordan informasjonen behandles og fordeles.".

5.4.1 Informasjonssikkerhet

Sikkerhet handler overordnet om å beskytte mot uønskede hendelser, hvor hendelser løst kan grupperes i to hovedretninger – villede handlinger eller hendelser og ikke-villede handlinger eller hendelser[23] (Thuv et al 2007 s. 19). Informasjonssikkerhet bygger på tre sentrale prinsipper – *konfidensialitet*, *integritet* og *tilgjengelighet*[24]. Det redegjøres kort hva oppgaven legger i disse tre begrepene.

Konfidensialitet

Med konfidensialitet menes hemmeligholdelse av informasjon eller (informasjons)ressurser. Dette behovet er spesielt stort innenfor statsmakten og industrien. Forsvaret er et eksempel på en statlig virksomhet hvor prinsippet om konfidensialitet er sentralt. Konfidensialitet har rotfeste i militære styrkers prinsipp om "need to know" (Bishop 2003 s. 4), hvor hensikten blant annet er å sikre tilgang på informasjon utelukkende til de som har behov for denne. Beskyttelse av ressurser

[23] Fokus er enten på hendelser som skyldes bevisst utførte og planlagte handlinger, eller på utilsiktede konsekvenser av ulykker, tilfeldigheter, force majeure osv som ikke er utført med (menneskelig) overlegg.

er et annet viktig aspekt ved konfidensialitet ved at for eksempel systemkonfigurasjoner ikke ønskes kjent, hvilket utstyr som benyttes ønskes skjult osv.

Integritet

Integritet refereres til påliteligheten/troverdigheten til informasjonen og (informasjons)ressursene. Normalt er begrepet uttrykt som det å forhindre urettmessig eller uautorisert forandring. Begrepet er sammensatt og inkluderer både data integritet (innholdet i informasjonen) og opprinnelses integritet (selve datakilden, også kalt autentisitet/påliteligkontroll) (Bishop 2003 s. 5). Prinsippet om integritet faller inn i to kategorier – forebygging/avverging og oppdagelse/oppklaring[25] (Bishop 2003 s. 5).

Tilgjengelighet

Med begrepet tilgjengelighet menes det faktum å kunne bruke informasjon og (informasjons)ressurser som ønsket og er et viktig aspekt ved funksjonsstabilitet/pålitelighet. Et ikke tilgjengelig system er minst like kritisk som ikke fravær av system (Bishop 2003 s. 6). Sikkerhetsaspektet i tilgjengelighet favner blant annet bevisste forsøk på å hindre tilgang på (nødvendig) informasjon eller (informasjons) tjenester ved å gjøre disse utilgjengelige. Tilgjengelighetsblokkering som DOS er et eksempel i så måte (Bishop 2003 s. 6).

Oppsummert kan det sies at informasjon (eller data) som ikke skal kunne leses av andre enn autoriserte brukere er konfidensialitet. Med begrepet "autorisert bruker" menes en bruker som er autorisert for en handling når han har implisitt eller eksplisitt tillatelse til å utføre handlingen (Thuv et al. 2007 s. 20)[26]. Informasjon som bare skal kunne endres eller slettes av autoriserte brukere faller inn under integritet og informasjon som skal være tilgjengelig for autoriserte brukere er forenelig med tilgjengelighetsprinsippet (Thuv et al. 2007 s. 20).

5.4.2 Metadata

Metadata betraktes gjerne som data om data. Bibliotekskartotekskort er eksempler på hva slags katalogisering/"data om data" som er ment. En definisjon av metadata som gjerne benyttes i forbindelse med MIL INI er: "Metadata is data which assists in the identification, descrition,

[24] De engelske begrepene på de tre datasikkerhetsprisnippene er confidentiality, integrity og availability (Bishop 2003 s. 3).

[25] Den første kategorien, forebygging/avverging, søker å vedlikeholde påliteligheten av dataene/informasjonen ved å blokkere ethvert uautorisert forsøk på endre data/informasjon eller forsøk på å endre data/informasjon på uautoriserte måter, for eksempel ved manipulasjon igjennom fiendtlig INFOOPS. Den oppdagende/oppklarende kategorien på sin side gjør ingen forsøk på å hindre brudd på integritet da den utelukkende rapporterer at dataenes/informasjonens pålitelighet ikke lengre er tilforlatelig/pålitelig (Bishop 2003 s. 5).

evaluation and selection of an information object." (Hafnor 2006 s. 21). Formuleringen "object" forstås i denne sammenheng som data-/informasjonsressurs.

Metadatakonseptet ikke er noe nytt og revolusjonerende, men anvendelsen er å betrakte som aktualisert på ny – også innenfor nye bruksområder. Som Hafnor (2006 s. 22, kursiv i originalteksten) skriver i sin rapport: "I en nettsentrisk militær kontekst vil alle brukere både *produsere* og *forbruke* (konsumere) metadata for *nettbasert informasjon*." I militær kontekst vil metadata brukes av både produsent og forbruker til for eksempel søking, lokalisering og utvelgelse. I tillegg benyttes metadata til å beskrive strukturelle og rasjonelle egenskaper ved data-/informasjonsressursene, ressursenes formater, sikkerhetsnivå, semantikk osv (Hafnor 2006 s. 22). "Enterprise Metadata" er den er mekanismen som brukes for at brukere skal kunne oppdage og (gjen)finne ressursene på tvers gjennom hele virksomheten – i hele nettverket (Hafnor 2006 s. 10).

[26] Dette håndteres normalt ved å først å autentisere (verifisere) brukeren for dernest knytte en identitet til brukeren. Tilgangskontroller benyttes videre for å kontrollere at brukeren oppfører seg innenfor tillatte rammer (Thuv et al 2007 s. 20).

6 Informasjonsoperasjoner

"More than a fishbowl, in fact, the global information environment has become a battlespace in which the technology of the information age – which is the aspect that we all too frequently focus on – is used to deliver critical and influential content in order to shape perceptions, manage opinions, and control behavior…[og t]his new battlespace is focused on the "wetware", the "grey matter" of the brain in which opinions are formed and decisions made." (Kuehl u.å. s. 4). Informasjon er av Kuehl uttalt å være det mest (kanskje eneste) effektive våpen på denne nye slagmarken (Kuehl u.å. s. 4).

Det eksisterer flere begreper som i større eller mindre grad relaterer seg til begrepet informasjonsoperasjoner (INFOOPS). Denne oppgaven vil kort beskrive ett av disse – begrepet informasjonskrigføring[27]. Noen militærteoretikere argumenterer med at informasjonskrigføring er det som gjøres når INFOOPS ikke lykkes (Kuehl u.å. s. 12). Andre har et videre syn på hva INFOOPS er, ved at intensjonen er å gjennomføre INFOOPS som en strategisk kampanje igjennom hele livsløpet til en konflikt, fra fred til krig tilbake til fred. Av den grunn er INFOOPS mye mer omfattende enn informasjonskrigføring, og det er innenfor INFOOPS at den fulle tverrdepartementale integrasjonen og sivilmilitære integrasjonen må skje (Kuehl u.å. s. 12-13).

Grunnet samfunnets og militære styrkers store forbruk av informasjon er striden om informasjonsdomenet i dag helt sentralt (FFOD 2007 pkt. 0592). Begrepet INFOOPS som begrep er relativt nytt, men metodikken i seg selv er gammel. Individers iboende trang for å påvirke andre for å oppnå egne ønsker og mål har alltid vært tilstede. For eksempel skal Sun Tzu ha hatt som filosofi at " All warfare is based on deception" (Tzu u.d.)

Ideen ved INFOOPS er å påvirke informasjon for på den måten å gripe "…direkte inn i menneskets kognitive prosesser som danner grunnlaget for all beslutningstaking." (MFU 2003a s. 2). "The most important concept to remember about IO[28] is that it is not a weapon per se; it is a process. IO is a way of thinking about relationships. IO is an enabler, a "source multiplier," a tool that increases one's ability to shape the operational environment…It is also a strategy, a campaign, and a process that is supported by traditional military forces (Kuehl u.å.s. 6).

INFOOPS avviker i forhold til tradisjonelle (militære) operasjoner ved at de i utgangspunktet ikke er rettet mot det fysiske domenet, selv om INFOOPS i sammenheng med konkrete innsatser i det fysiske domenet kan virke gjensidig forsterkende. Ambisjonen er i stedet å mer direkte

[27] Den engelske betegnelsen er Information Warfare.
[28] Information Operations, en annen betegnelse som brukes om INFOOPS.

påvirke det kognitive domenet, "…herunder de tankeprosesser som ligger til grunn for motstanderens situasjonsoppfatning og beslutningstaking, gjennom påvirkning av informasjon." (FFOD 2007 pkt. 0594).

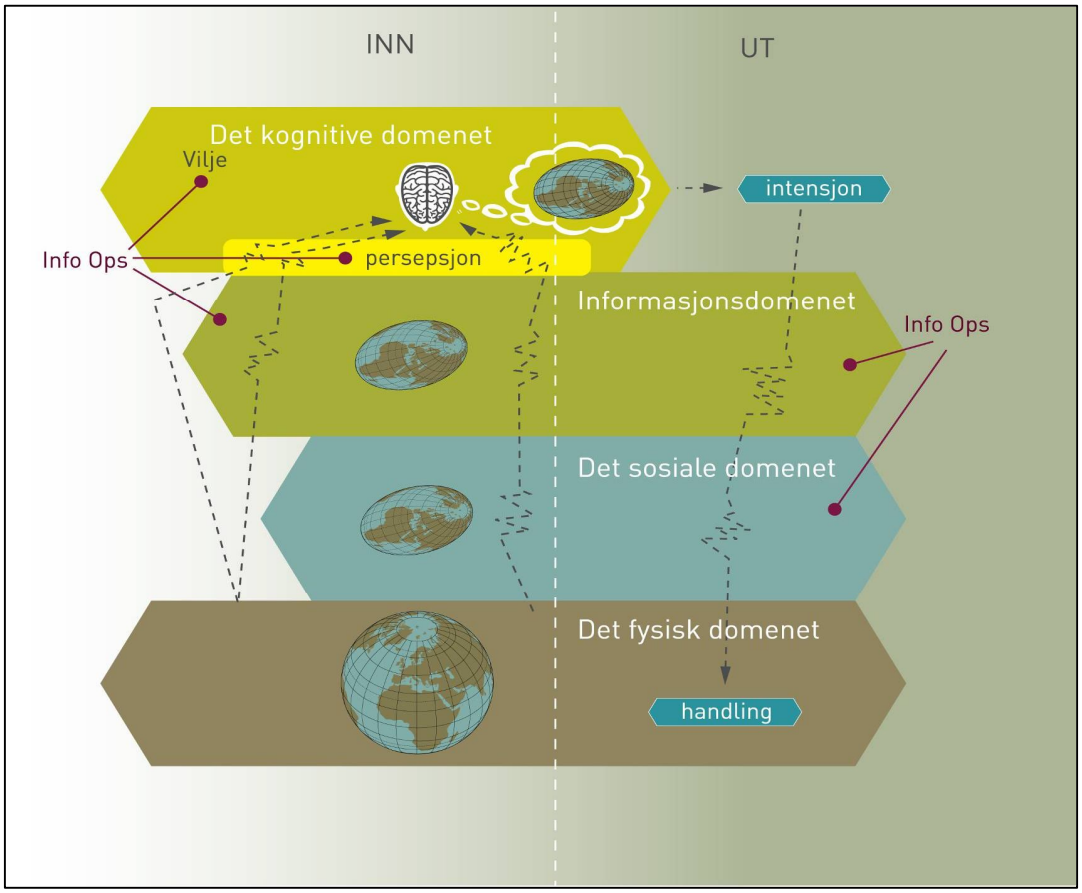
Som mange andre begreper og konsepter har også INFOOPS sitt rotfeste i USA. USA's INFOOPS tilnærming er et forsøk på å utvikle et sett med doktrinelle tilnærminger for hennes militære og diplomatiske styrker til å bruke operasjonalisere informasjonens makt (Kuehl u.å. s. 11). USA har hatt sin Joint Doctrine for Information Operations siden 1998 som "… represents a significant milestone in defining how joint forces use information operations (IO) to support our national military strategy." (JP-3.13 1998)[29]. Begrepet har siden tidlig i tusenårsskiftet fått større vektlegging av koordineringsaspektet herunder behovet for økt politisk kontroll.

INFOOPS konsepter som er utarbeidet i forskjellige nasjoner, samt INFOOPS arbeidet i NATO og EU, har stor grad av harmoniseiring. Tross dette er det fortsatt diskusjoner, både på militær og sivil side, om hva INFOOPS er, bør være og graden av politisk kontroll. Det er dog enighet om"…at informasjonsoperasjoner vil ha en økende og i visse tilfeller avgjørende betydning for vellykket håndtering av fremtidige kriser og konflikter av så vel asymetrisk som symetrisk karakter." (MFU 2003a s. 2).

6.1 Forholdet INFOOPS og domenemodellen

FFOD har en figur som på en god måte viser INFOOPS sine nedslagsfelt i de forskjellige domene og hvordan INFOOPS påvirker de forskjellige domene respektivt, se figur 10[30]. INFOOPS rettes mot det kognitive domenet for å påvirke oppfattelser, persepsjoner, evner og vilje. Det sosiale domenet påvirkes i forhold til samholdet individer og organisasjoner i mellom. Informasjonsdomenet påvirkes av INFOOPS for å påvirke informasjon og informasjonsoverføring (FFOD 2007 pkt. 135).

[29] Den amerikanske doktrinen beskrivelse av grunnleggende INFOOPS prinsipper samsvarer i stort med hva som ligger i utkast til NATO doktrinen (JP-3.13 1998 s. vii-viii).
[30] Selv om modellen som viser INFOOPS treffpunkter i domenemodellen er utarbeidet som del av en norsk militær doktrine anses modellen av forfatteren å være av en generell art som kan sees på prinsipielt – ikke bare som del av en militær kontekst.



Figur 10 – Forholdet mellom INFOOPS og domenemodellen (FFOD 2007 pkt. 134).

6.2 INFOOPS i NATO

INFOOPS som konkret "programområde" i NATO er relativt nytt[31]. Siste revisjon av NATO sitt militære policy dokumentet innenfor INFOOPS ble gjort våren 2007 (MC 422/3 2007). Denne policyen beskriver at INFOOPS utgjør tre beslektede aktivitetsområder:

- Informasjonsaktiviteter[32] med fokus på endringer, påvirkning og/eller forsterke tolkninger og holdninger
- Informasjonsaktiviteter med fokus på sikre/bevare og beskytte Alliansens "freedom of manoeuvre" i informasjonsdomenet

[31] Policy dokumenter og formaliserte/godkjente doktriner for kapabiliteter som gjerne koordineres og integreres i INFOOPS aktiviteter har lengre levetid. Et eksempel er NATO sin doktrine for psykologiske operasjoner (PSYOPS) som ble godkjent i 2003 (AJP-3.10.1 (A) 2007).
[32] NATO omtaler informasjonsaktiviteter som handlinger som er designet for å påvirke informasjon og/eller informasjonssystemer (AJP-3.10 2008).

- Informasjonsaktiviteter med fokus på kontrakommando, funksjoner og kapabiliteter ved å påvirke data og informasjon som brukes i motstanders og andre aktørers militære prosesser.

NATO doktrine for INFOOPS eksisterer i en "Pre-Ratification Draft" av doktrinen AJP-3.10 Allied Joint Doctrine for Information Operations (AJP-3.10 2008). NATO definerer (MIL) INFOOPS[33] som "…a military function to provide advice and co-ordination of military information activities in order to create desired effects on the will, understanding and capability of adversaries, potential adversaries and other NAC approved parties in support of Alliance mission objectives." (MC 422/3 s. 3; AJP-3.10 s. 13a).

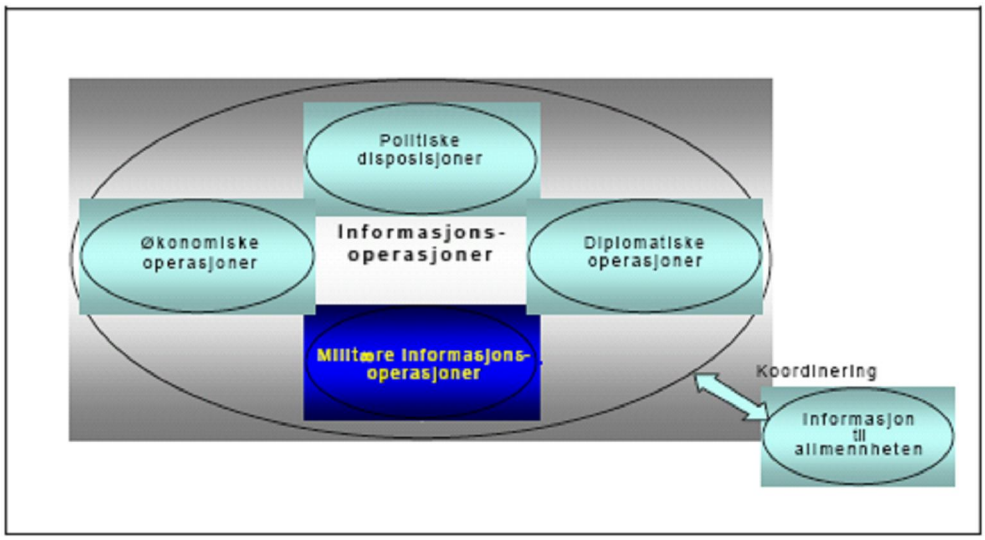
NATO har igjennom Research and Technology Organisastion (RTO) Task Group SAS-057 identifisert kartlagt INFOOPS initiativ i forskjellige nasjoner og identifisert likheter og ulikheter mellom nasjoner og NATO sine respektive tilnærminger til INFOOPS. Arbeidsgruppens konklusjon var at i stort så synes det som om det er en felles forståelse av INFOOPS i NATO og de nasjonene som var del av arbeidet om at INFOOPS tjener som en koordinerende og/eller integrerende funksjon. På den andre siden er det forskjeller som "…to some extent have to be attributed to culturally different approaches to military operations as a whole." (SAS-057 2006 s. ES-1). For å ha et omforent utgangspunkt for arbeidet etablerte arbeidsgruppen sin egen beskrivelse av INFOOPS – som "…co-ordinated military activities within the information domain to affect information and information systems…" (SAS-057 2006 s. ES-1).

6.3 Norsk INFOOPS strategi?

Som en del av FSJ Militærfaglige utredning i 2003 ble visjonene med Norges (militære) INFOOPS konsept beskrevet. Overordnet ble INFOOPS presentert som en koordinerende og integrerende strategi som utnytter synergier mellom (statlige) virkemidler, som del av den politiske konsultasjons- og beslutningsprosess, for å støtte egne nasjonalstrategiske eller alliansestrategiske mål. Hensikten er på den ene siden å påvirke (andre parters) beslutningstakere som har innflytelse, samt å beskytte egne (og vennlige) beslutningstakere på den andre siden[34]. På den måten har INFOOPS både en offensiv og en defensiv side hvor påvirkningen kan skje både synlig, mer diskret eller skjult avhengig av type påvirkning og mot hvem og/eller hva (MFU 2003a s. 2-3).

[33] NATO bruker det generelle begrepet INFOOPS. Denne oppgaven vil bruke begrepet MIL INFOOPS når det er strategien innenfor militær kontekst som menes.

INFOOPS som mulig nasjonalt konsept består av "… politiske disposisjoner[35], diplomatiske operasjoner[36], økonomiske operasjoner[37] og militære informasjonsoperasjoner, tett koordinert med informasjon til allmennheten (P&I)." (MFU 2003a s. 3), se figur 11.



Figur 11 - INFOOPS som overordnet nasjonal strategi (MFU 2003a s. 3)

6.3.1 MIL INFOOPS

Som beskrevet over så er forslaget fra FMU 03 å se på INFOOPS som en "tverrfaglig" strategi som favner (alle) statens virkemidler. Militær INFOOPS (MIL INFOOPS) vil med dette som utgangspunkt være den delen av strategien som utøves av en stats militære organisasjon og som integrerer og koordinerer relevante militære virkemidler med politisk-strategisk nivå.

Den norske definisjonen av MIL INFOOPS slik den er nedfelt i FSJs militærfaglige utredning 2003 inneholder en offensiv og en defensiv dimensjon (MFU 2003a s. 4):

> *Militære informasjonsoperasjoner (MIL INFO OPS) er koordinerte tiltak iverksatt for å påvirke andre parters beslutningstakere til støtte for egne overordnede mål, ved å påvirke deres informasjon, informasjonsbaserte prosesser og –systemer, samtidig som vi utnytter og beskytter egen informasjon, informasjonsbaserte prosesser og -systemer.*

Den definisjonen av INFOOPS som er i FFOD samsvarer mer med NATO sin definisjon: "Informasjonsoperasjoner er koordinerte tiltak som iverksettes for å skape ønskede effekter på

---

[34] Det presiseres at den norske INFOOPS strategien er utarbeidet før NATO sin endring rundt fokus på påvirkning av besklutningstakere.
[35] Med politiske disposisjoner menes "…"erklæringer" i en eller annen form fra landets politiske ledelse." (MFU 2003a s. 3).
[36] Diplomatiske operasjoner "…omfatter all kontakt på yrkesdiplomatisk nivå." (MFU 2003a s. 3).
[37] Innenfor økonomiske operasjoner favnes tiltak som sanksjoner overfor andre land, frysing av utenlandske konti, sperring av pengeoverføringskanalser osv (MFU 2003a s. 3).

forståelse, vilje og evne hos motstandere, potensielle motstandere samt andre målgrupper…" (FFOD 2007 pkt. 0593).

6.3.2 MIL INFOOPS kjerneaktiviteter og kapasiteter

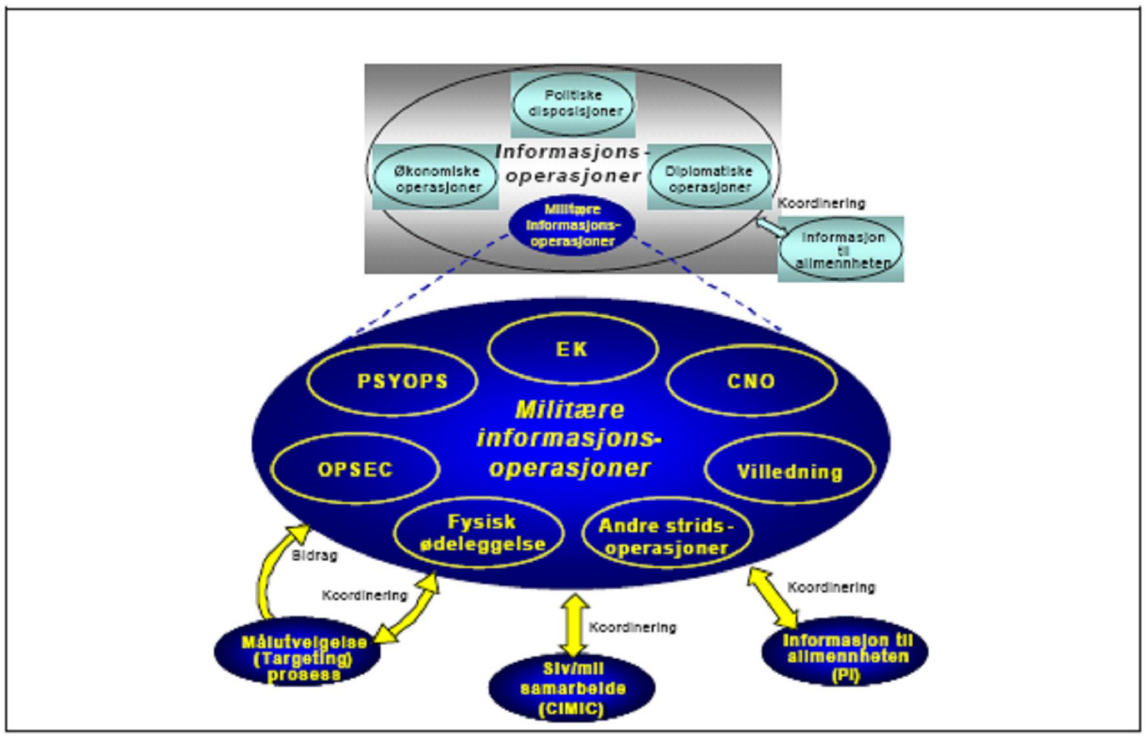
Overordnet kan INFOOPS sies å ha tre sentrale (kjerne) aktivitetsområder – påvirkningsaktiviteter, counter-command aktiviteter og informasjonsbeskyttelses aktiviteter. Alle disse er spesielt rettet mot å påvirke (beslutningstakeres) vilje, forståelse og evne (MC 422/3 2007 s. 4; AJP-3.10 u.å. s. 1-7; FFOD 2007 s.136).

I utgangspunktet omfatter MIL INFOOPS alle relevante militære kapasiteter hvor koordinering og integrering er nødvendig og/eller hensiktsmessig for å støtte opp under en overordnet strategi (MFU 2003a s. 4). MIL INFOOPS kan sees på som en styrkemultiplikator hvor hensikten er "…å øke den totale effekten av de militære virkemidler som settes inn i en operasjon." (Jørstad 2007). Sagt på en annen måte er MIL INFOOPS ikke tradisjonelle operasjoner som iverksettes. Det er den effekt som ønskes igjennom iverksatte militære handlinger som åpner for om handlingen er forenelig med INFOOPS eller ikke.

MIL INFOOPS består av et sett med kapabiliteter i tillegg til koordinerings og bidragsmessige forankringer til henholdsvis Targetingprosessen samt funksjonene P&I og CIMIC. Figur 12 viser de mest fremtreende enkeltkapasitetene relatert til MIL INFOOPS.

Enkeltkapasiteter må være av en slik art at de lar seg koordinere for at de skal være relevante i MIL INFOOPS sammenheng. I tillegg må de være "…mobile og modulære i sin oppbygging og organisasjon..." (MFU 2003a s. 4) og brukes der det er behov.

Selv om visjonen/ambisjonen i MFU 03 var en tverrdepartementalt INFOOPS strategi, er det ikke implementert en slik nasjonal tilnærming i dag. Bakgrunnen for dette er ukjent, men en mulig årsaksforklaring kan være at den påkrevde forankringsprosessen i forhold til strategien ikke har vært gjennomført (godt nok) og/eller ikke har vært vellykket. I tillegg er det kanskje heller ikke nasjonal modenhet ennå for et slikt tverrdepartementalt INFOOPS samarbeid. I lys av den form for trusler vi ser i dag, både nasjonalt og internasjonalt, de typer konflikter vi bidrar i, nye operasjonskunstkonsepter og nye operasjonstyper tilsier at et slikt tverrdepartementalt samarbeid vil fremtvinge seg innenfor for flere områder, hvor INFOOPS er ett slikt område.



Figur 12 - De mest fremtredende MIL INFOOPS virkemidlene (MFU 2003a s. 5). I den siste tiden er også virkemidlene Key Leader Engagament (KLE) og Presence, Posture og Profile (PPP[38]) trukket frem som fremtredende MIL INFOOPS kapasiteter.

Som underlag for analysen i denne oppgaven vil jeg betrakte INFOOPS fra et overordnet ståsted, der formålet er å påvirke ”noen” for å oppnå ”noe”. Sagt på en annen måte er det for analysens del ikke sentralt hvorvidt den fiendtlige INFOOPS gjennomføres med spesielle kapabiliteter. På den andre siden vil det igjennom diskusjonen eksemplifiseres med bruk av konkrete (INFOOPS) kapasiteter der det er naturlig.

INFOOPS har alltid hatt betydning på slagfeltet. Sir Basil Liddle Hart skal ha uttrykt at ”Wars are not won or lost on the fields of Battle, but in the Hearts and Minds of Political Leaders and even more important, Public Opinion.” i sin bok ”*Thoughts of War*” (1944) (Jørstad 2007).

I dagens konflikter er slagfeltet mer transparent enn noen gang. Ordre som gis er synlig på alle nivå, medias kontinuerlige tilstedeværelse og det faktum at taktiske handlinger kan gi strategiske effekter er eksempler på dette. ”*Den strategiske korporal*” er et begrep som beskriver dette forholdet. På den andre siden er det også slik at strategiske beslutninger og handlinger kan gi operasjonelle og taktiske effekter. Dette kan beskrives ved begrepet ”*den stridstekniske minister*”, for å sitere en medstudent av meg. MIL INFOOPS bidrag i denne sammenhengen er å

bidra med militære virkemidler for å ivareta overordnede (nasjonale) sikkerhetsbehov. ”Som en følge av nye sikkerhetspolitiske samhandlingsmønstre øker betydningen av informasjon som ressurs- og som følgelig også behovet for INFOOPS.” (Jørstad 2007).

[38] Med presence menes den fysiske tilstedeværelsen av militære styrker. Hvordan militære aktører opptrer omtales som posture, mens profile favner bruk av militære aktører til å transmittere ”key messages” (Jørstad 2007).

7 Sentrale sårbarheter i transformasjonen mot en fremtidig MIL INI

Transformasjonen mot fremtidig MIL INI styrer mot noen overordnede mål (visjon) med følgende egenskaper (Hafnor 2006 s. 10):

- Sømløs tilgjengeliggjøring og deling av tjenester og ressurser.
- Arbeidsprosesser på tvers av fag-, kompetanse- og organisasjonsenheter.
- Tilgjengeliggjøring av tjenester og arbeidsprosesser på tvers av kommandonivåer og brukerkontekster .

Denne transformasjonen medfører store endringer både på infrastrukturens oppbygging (struktur) og på de grunnleggende prinsippene for bruk av strukturens forskjellige tjenester (innhold). Hensikten med dette kapitlet er å analysere sentrale sårbarheter i denne transformasjonen med utgangspunkt i faktoren *fremtidig MIL INI*. Kapitlet avsluttes med en delkonklusjon.

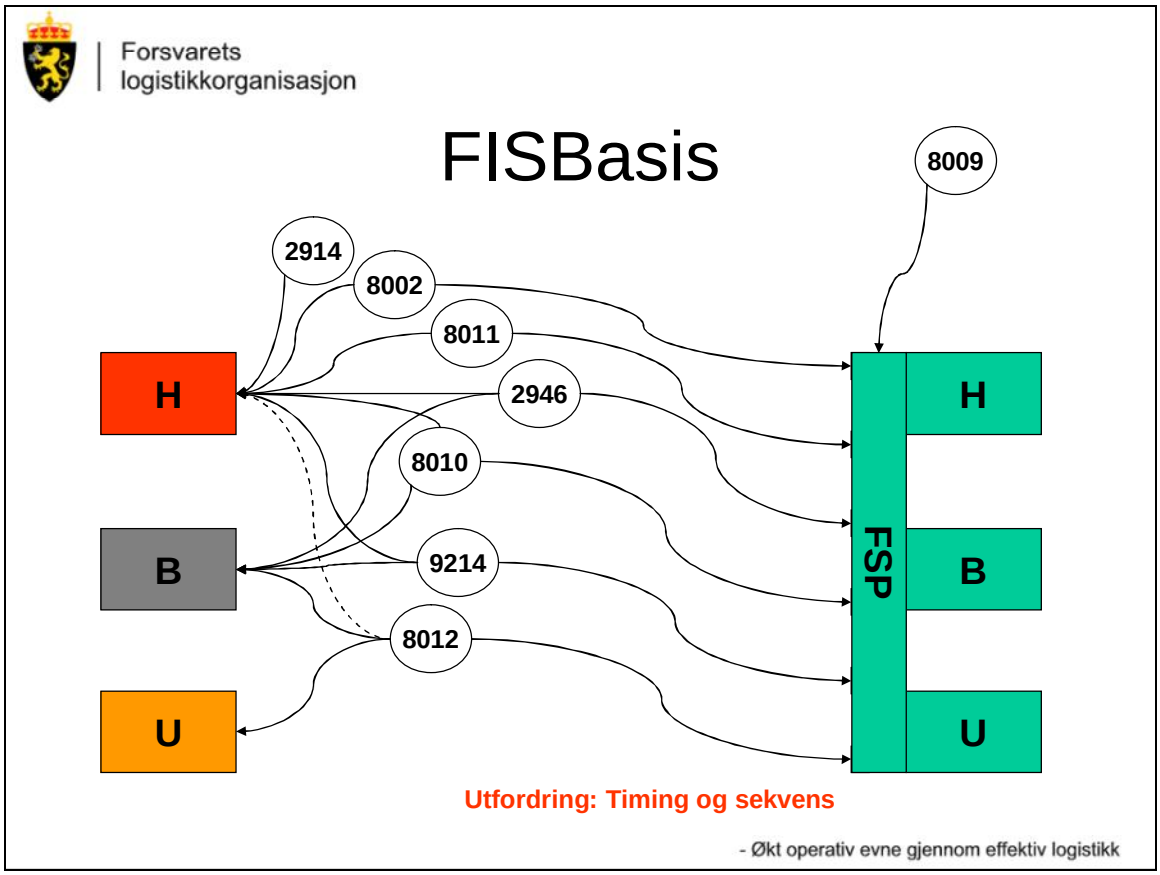
7.1 MIL INI prosjektportefølje

For å lykkes med en videre utvikling av en velfungerende MIL INI vil (alle) Forsvarets (materiell)investeringer måtte vurderes innenfor konseptet av NbF. Den påkrevde transformasjonen krever en rekke investeringer[39]. Forsvarets Logistikkorganisasjon, Investering (FLO/I) er allerede involvert i realiseringen av flere INI-prosjekter og ytterligere flere prosjekter kommer. Relasjonene mellom disse prosjektene er store. Mange av prosjektene er direkte avhengig av hverandres leveranser. Andre har/får avhengigheter grunnet utsettelser, forsinkelser. Noen prosjekter har dels store overlapp i forhold til hva de skal levere. Alt dette representerer sentrale sårbarheter. Et eksempel er den fordelen det er for prosjekt P8009 Felles kjernetjenester dersom prosjekter/aktiviteter i tilknytning til Forsvarets sikre plattformer ”times”. Jo færre (sikre) plattformer MIL INI kjernetjenester kan forutsette som aktuelle kjøremiljø jo bedre (FLO/IKT 2008). Figur 13 er ment å illustrere denne konkrete utfordringen.

FLO/I har iverksatt tiltak for å skaffe seg nødvendig oversikt over situasjonen. Det synes åpenbart at (materiell)investeringene også på et politisk/(militær)strategisk nivå er nødt for å ”sorteres riktig” for på en bedre måte legge grunnlaget for de rette investeringene, i rett rekkefølge (FLO/IKT 2008). Denne formen for sentral styring er nedfelt i Forsvarets IKT policy (IKT 2005). På den andre siden ligger det også ansvar på det enkelte prosjekt i å være

[39] Også andre former for tiltak vil være påkrevd uten at dette er sentralt her.

oppmerksom på disse utfordringene og bidra til at Forsvarets fremtidige investeringer gjennomføres på en best mulig måte.



Figur 13 – Prosjekter som har relasjoner til Forsvarets sikre plattformer (FSP) (FLO/IKT 2008)

I tillegg til at mange av prosjektene er direkte avhengig av hverandres leveranser, vil ønske om "bottom up" styrte krav og investeringer gi en del potensielle sårbarheter/utfordringer. (EXP 2008). På mange måter er det en utfordring at enkelt miljøer/prioriterte enheter aksepteres å anskaffe utenfor de rammer som er satt for blant annet å sikre interoperabilitet. Anskaffelser til spesialstyrkene representerer et slikt miljø. Det kan være mange årsaker til det. Ikke gode nok (tekniske) løsninger, for lang tid for anskaffelse og sikkerhetsmessig godkjenning, operasjonsmønstre endres fra gang til gang. Hovedårsaken er å sikre optimale arbeidsforhold, herunder god nok sikkerhet, for denne typen militære kapasiteter (FOHK 2008). Videre er det kanskje både nødvendig og ønskelig at prioriterte enheter skal få velge ”fra øverste hylle”. Men, da må også Forsvaret erkjenne dette ansvaret, derigjennom denne totalkostnaden.

En annen sentral utfordring er kravet om samarbeid. Når disse miljøer begynner å samarbeide med tilsvarende miljøer i andre departement, for eksempel Justisdepartementet, kan dette resultere i potensielle sårbarheter. Forskjellige grunnleggende profesjonskulturer, forskjellige (tekniske) systemer/tjenester og/eller gradsnivåer er eksempler[40]. I verste fall vil det være en sårbarhet at tverrdepartemental interoperabilitet ikke samsvarer med den grunnleggende (tekniske) arkitekturen i MIL INI. En annen utfordring/mulig sårbarhet ved (allmenn) aksept for slike spesialinvesteringer er at det kan spre seg til andre mindre kritiske og/eller prioriterte (fag)miljøer; "…til slutt vil avdelingssjefene selv beslutte hva han vil ha som operative/taktiske verktøy.". (EXP 2008). Også i slike tilfeller vil det kunne være argumenter som taler for spesielle løsninger. Poenget er at det forplikter alle nivåer i størst mulig grad å imøtekomme overordnede føringer og fagmyndighetsprinsipper.

7.2 Investering i fellesløsninger

Transformasjonen fra "stovepipesystemer" til en modell med gjennomgående vertikale og horisontale tjenester medfører en del grunnleggende bevisstgjøringer. Dette er noe som må erkjennes og ikke minst aksepteres av brukere (og tjenester) på alle nivå. Endringer av holdninger og erkjennelse av at alle må "gi og ta" for fellesskapets beste vil være viktige momenter. Kulturelle endringer i hele Forsvaret (og hele NATO) vil være et sentralt punkt. Igjen en rekke sentrale sårbarheter/utfordringer som er en naturlig følge av MIL INIs endrede struktur. På den andre siden er det slik at gjennomgripende tjenester vil kunne gi brukere (og tjenester) økte/nye muligheter.

Forvaltningsdelen av Forsvaret er godt i gang med å investere i fellesløsinger. Dette er viktige erfaringer å ta med seg all den tid det i fremtiden ikke vil skilles i samme grad mellom operativt og forvaltningsmessig domene. Disse miljøene flyter sammen over tid hvor MIL INI vil være en felles grunnstruktur. Føringer rundt fellesløsninger på tvers av forsvarsgrener er også nedfelt i IKT policyen (IKT 2005). Forsvarets personellsystem (FIS/P P3) er et eksempel på en tidligere investering som lyktes med en fellesløsning i et PTO-perspektiv. En grunn for at dette prosjektet lyktes var en sentral styring og vilje mot etablering av omforente løsninger på tvers av forsvarsgrener og prosessområder. Mangel på (sentral) styring og vilje vil kunne være direkte sårbarheter/utfordringer i slike investeringer. FIS/P P3 brukes også i en "totalforsvarskontekst".

[40] Selv om antall forskjellige (tekniske) løsninger/tjenester i MIL INI øker ved en grad av "frislipp" så er det mulig å stille krav for å sikre (teknisk) intereoperabilitet.

Siviltjenesteadministrasjonen[41] bruker systemet for å forvalte personene som avtjener sivil verneplikt. FIS/P P3 representerer således et informasjonssystem med tverrdepartemental bruksdomener (COIs).

Også Program LOS er sentral med sine PTO-leveranse. Deler av den produksjonssatte løsningen er gjort innenfor rammene av hva andre nasjoner gjør. Leveransen for strukturforvaltning er et eksempel på dette hvor både det tyske og det danske forsvaret benytter samme utviklede forsvarsspesifikke løsning. Slike tiltak vil være et godt utgangspunkt for fremtidige multinasjonale (nettbaserte)løsninger. På den andre siden fremtvinges det fra funksjonelle miljøer (og kanskje også politiske miljøer?) å "skreddersy"/tilpasse standard løsningene til særnorske behov. En grunn for dette kan være at Forsvaret ikke evner å tenke nytt og/eller evner (og viljer) til å endre Forsvarets virksomhet. Dette er spesielt i de situasjoner hvor det er mangler/avvik sammenlignet med dagens løsninger. Det skal dog sies at standard IKT-systemer gjerne ikke er utformet med (norske) særegne militærspesifikke, for eksempel Heimevernsordningen, og kanskje heller ikke offentlige, forvaltningsregler. Videre uttrykker Forsvaret et ønske om å tilpasse seg bedriftsøkonomiske og andre sivile prinsipper. I den forbindelse bør det forplikte og vurdere endring av Forsvarets virksomhet som et alternativ til å tilpasse standardløsninger[42]. IKT policyen er også klar på at Forsvarets virksomhet "…skal om nødvendig tilpasses slik at standardprosesser og standard programvare kan benyttes der dette er mulig." (IKT 2005 s. 7). Dette er momenter som må vurderes i forkant av beslutninger om investeringer slik at Forsvaret har en klar oppfatning av hvor stor evne og ikke minst vilje det er for tilpassing av virksomheten i stedet for å tilpasse systemene. I verste fall vil virksomhetsstrategien bli et resultat av teknologiske valg – ikke teknologi som understøtter virksomhetens strategi.

Løpende forvaltning av (spesial)tilpasninger vil kunne medføre utfordringer som vil måtte aksepteres. Ikke samsvar mellom hva som tilsynelatende er strategiske føringer og hva som de facto gjøres vil være utfordringer som må håndteres. Også behovet for og graden av redundans må tas høyde for "fra dag en" (EXP 2008). Hvis ikke vil dette kunne være en sårbarhet hvis (sentrale deler av) tjenestene er utilgjengelige.

[41] Siviltjenesteadministrasjonen sorterer under Justisdepartementet.
[42] Teknisk skreddersøm av standardløsninger er lite hensiktsmessig, og vil ofte både blir mer omfattende og mer ressurskrevende enn utvikling av egne spesialtilpassede løsninger.

7.3 Valg av samarbeidspartnere

Forsvarets (materiell)anskaffelser vil ha strategiske konsekvenser nasjonalt. Internasjonalt har dette konsekvenser i forhold til samhandling med allierte og andre samarbeidsnasjoner. Det er stort (politisk) fokus på multinasjonalt samarbeid som blant annet fremkommer i anbefalte retningslinjer for utviklingen av Forsvaret i årene 2009-2012 (NOU 2007 s. 7)[43].

I dag er det et konkret norsk-svensk samarbeid i forbindelse med nytt artillerisystem (FLO/IKT 2008)[44]. I tillegg er det konkret samarbeid mellom Norge og Sverige rundt norsk styrkebidrag inn EU Nordic Battle Group. Det ble også nylig avhold et møte i Polyteknisk Forening med forsvarssamarbeid i Norden som tema hvor ønsket om et tettere forsvarssamarbeid ble presentert (Watne & Knutsen 2008).

Valg av samarbeidspartnere vil ofte kunne gi føringer for egenskaper i anskaffelser. En sentral utfordring er om anskaffelser og samarbeid skal skje innenfor rammen av hva våre allierte gjør, eller om det skal samhandles med nasjoner som har likhetstrekk med våre egne nasjonale behov. Ikke minst i lys av alle de konsekvensene som følger slike strategiske valg som utdanning, kompetanseheving, relasjonsbygging osv.

Et annet område hvor det diskuteres økt samarbeid er mellom Forsvaret og industrien. Slik samarbeid har vært en naturlig del av Forsvarets (operative) virksomhet i en lengre periode. FLO har fått et oppdrag fra Forsvarsdepartementet (FD) om å gi en tverrfaglig vurdering av hensiktsmessigheten av allerede etablerte avtaler[45] samt muligheten for å inngå nye tilsvarende samarbeidsavtaler (FLO/IKT 2008). Strategiske industriavtaler samtidig som det både er ønskelig med økt samarbeid innenfor NATO og økt nordisk samarbeid vil på den ene siden åpne for industrielle muligheter – også utenfor Norges grenser. På den andre siden vil slike avtaler kunne være en potensiell sårbarhet for å få til multinasjonalt samarbeid samt en helhetlig styring av Forsvaret. En annet sårbarhet er at Forsvaret må evne og utnytte slike avtaler slik at strategiske industriavtaler ikke blir ”spill for galleriet”[46] med svekket troverdighet som resultat.

---

[43] ”Det bør utvikles et tettere og dypere samarbeid med andre land om militære styrker og militær virksomhet…” (NOU 2007 s. 7).

[44] Det er etablert et ”Memorandum of Understanding (MoU)” mellom forsvarsmaktene i Norge og Sverige angående samarbeid innen utvikling og produksjon av styrker til landbasert indirekte ildstøtte (FLO/IKT 2008).

[45] I 1997 inngikk Forsvaret (den gang Hærens forsyningskommando) en avtale med CCIS House A/S hvis hovedformål var å regulere et samarbeid for utvikling og produksjon av Hærens K2IS i et 20 års perspektiv.

[46] Erfaringene med dagens inngåtte rammeavtaler er et eksempel på det. Leverandører som i dag har avtaler har i varierende grad gitt utrykk for at avtalene ikke benyttes og at Forsvaret heller benytter åpninger, som er merkantilt tilstede, i andre spesialinngåtte avtaler.

7.4 Helhetlig og sømløs informasjons- og tjenestetilbyder

En sentral komponent i femtidens MIL INI er et sett med etablerte kjernetjenester. Dette er grunnleggende tjenester som enten kan brukes av (slutt)brukere direkte eller av andre funksjons-/brukerspesifikke tjenester[47]. Det er å foretrekke at alle (sluttbruker)tjenester bruker samme grunnleggende kjernetjenester for på den måten å sikre tjenesteinteroperabilitet. I tillegg vil (slutt)brukere kunne ha tilgang til et rikere tjenestespekter i fremtiden som åpner for mer innovativ bruk av IKT[48]. Potensielle sårbarheter/utfordringer inntreffer i situasjoner hvor innovativ bruk av IKT er i konflikt med (vel)etablerte fellestjenester. En annen sårbarhet/utfordring er at feil og mangler i kjernetjenestene vil kunne ramme "alt og alle". Manipulasjon av informasjonselementer og/eller introduksjon av nye ikke-autoriserte (kjerne)tjeneste som et resultat av fiendtlige INFOOPS handlinger vil være konkrete sårbarheter. Et eksempel vil for eksempel kunne være at fiendtlige INFOOPS manipulerer søketjenesten slik at tjenesten enten gir feil resultat, den søker mot feil kilde, den "leser" hva som søkes etter osv.

En annen potensiell sårbarhet er det som kan synes som avvik i hvilken retning det styres mot mellom forskjellige multinasjonale initiativ. På den ene side er Norges og NATO enige om veien mot en rendyrking av modulbaserte tjenester. På den andre side er det deler av industrien som oppleves å foretrekke mer tradisjonelle løsninger som databasereplikasjon. Et eksempel er initiativene til henholdsvis Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition (MAJIIC)[49] på den ene siden og Multilateral Interoperability Programme (MIP)[50] på den andre (TRADOK 2008)[51]. Det kan synes naturlig at industrien betrakter transformasjonen mot sømløse tjenester som en form for "trussel". Mange av Forsvarets og NATOs samarbeidspartnere har på mange måter hatt en monopolsituasjon – både teknisk og merkantilt. Industrien derimot erkjenner at det ikke er noen vei utenom enn å tjenestebasere sine systemer/produkter for å sikre fremtidig "overlevelse". Et eksempel er SAP som i dag utgjør hjertet i Forsvarets forvaltningssystem (FIF).

En annen sårbarhet ved gjennomgående tjenester (og prosesser)[52] er at (informasjons)endringer som gjøres ett sted vil påvirke bruken av det samme informasjonsobjektet andre steder – gjerne på tvers av prosess- og COI grenser. Forsvarets investeringer i et fremtidig forvaltningssystem

[47] Eksempler på slike kjernetjenester er: Registertjenester, geografiske tjenester og tjenester for informasjonsutveksling.
[48] Innovativ bruk av IKT er av forventingene som ligger i NbF konseptet.
[49] MAJIIC er en del av NORCCIS som på mange måter kan sees på som en nettsentrisk system suite (Nesse 2006; *NORCCIS brosjyre*).
[50] MIP er et initiativ for utveksling/innsamling av informasjon fra forskjellige kilder (Strømsod 2003).
[51] Når det er sagt er det uttalt at industrien er "på gli" i forhold til fremtidens visjon om sømløse, modulbaserte tjenester også i MIP (FORV 2008).

(FIF) er et eksempel på dette. Utgangspunkt er en felles IKT-løsning som er basis for alle programmets investeringer. Beslutninger som gjøres i enkeltprosjekter på sentrale informasjonsobjekter vil kunne skape en ”bordet fanger” situasjon for fremtidige leveranser ved at informasjonsmodellen som utgjør kjernen i (felles)løsningen ligger fast. I tillegg vil store felles systemer/informasjonselementer gjøre Forsvaret mer sårbart i forhold til at menneskelige (og systemmessige feil). Introduksjon av feil på informasjonselementer i en del av virksomheten vil kunne få alvorlige, uønskede konsekvenser andre steder. Men hva er alternativet? Hvis svaret er systemmangfold så kommer mange av dagens sårbarheter til overflaten. Noen eksempler er manglende datakonsistens, manglende transparens i systemene, manglende sanntidsegenskaper og økte kostnader ved å opprettholde (system)mangfold (FORV 2008).

Fremtidig MIL INI, med sømløs tilgjengeliggjøring og deling av informasjonstjenester/-ressurser, medføre at dagens prosessfokus må vike for en mer rendyrket data-/informasjonsorientering (Hafnor 2006 s. 12-14). En slik kursendring vil kreve en form for avlæring av den prosesstenkningen vi har i dag og er således en potensiell sårbarhet. Når det er sagt er det fullt mulig å se for seg en MIL INI struktur som vil inneha både helhetlige og prosessuelle fellesløsninger på den ene siden og frittstående dataressurser/informasjonstjenester på den andre siden. En annen konkret sårbarhet/utfordring som ble fremmet under ekspertpanelseminaret er faren for at konseptet kopler sammen for enhver pris (EXP 2008).

En potensiell sårbarhet med MIL INI er at deler av den kan komme i en ”lock-in” situasjon. Med ”lock-in” forstås en situasjon hvor den grunnleggende teknologien som er fastlagt gjør det kostbart (umulig?) å benytte konkurrerende teknologier (Hafnor 2004 s. 24-25). I en allerede økonomisk presset situasjon er dette potensielle sårbarheter som ikke skal undervurderes. I verste tall vil valgte teknologiske prinsipper/løsninger gi føringer på Forsvarets fremtidige investeringer.

7.5 Administrasjon og tjenestehåndtering

Akkurat som Internett kan fremtidig internasjonal MIL INI sees på som en rekke nettverk som igjennom ”gjensidige avtaler” er sammenkoplet med den hensikt å tilgjengeliggjøre nettverksressurser (MIL INI tjenester). Et slikt fellesskap ”eies” på den måten av mange aktører. I forhold til Internett som må sies å ha liten grad av overordnet styring, har fremtidens MIL INI styring i form av gjennomgående service og management tjenester.

[52] Gjennomgående tjenester og prosesser vil i denne sammenheng også kunne være felles tekniske IKT-løsninger.

Fremtidens (MIL) INI vil bestå av langt flere grunnleggende (informasjons)tjenester, et økt antall aktører/brukere og typer av aktører/brukere – også på tvers av sikkerhetsnivåer. Utgangspunktet er at slik tjenestehåndtering skjer sentralt som i seg selv er en sårbarhet (EXP 2008). Dette vil kreve en økt bevissthet rundt administrasjon og tjenestehåndtering. Dette er nytt, selv om det innenfor forvaltningsdomenet i dag er iverksatt tiltak for å etablere felles forvaltningsregime på tvers av hele FIF[53]. En fremtid med forskjellige adgangs- og sikkerhetskontrollsystemer vil kunne resultere i konkrete sårbarheter ved (tekniske) konflikter i den grunnleggende strukturen. I tillegg medfører bruk av flere forskjellige ”tilgangssystemer” sosiale sårbarheter. Multinasjonale operasjoners (MIL) INI, sammensatt av mange nasjonale MIL INI, herunder de respektive landene sine eksterne grensesnitt, vil kunne være vanskelig å kontrollere.

7.6 Gjennomgående integrasjon

Å gå fra frittstående (toveis) grensesnitt mellom sluttbrukersystemer til et gjennomgående ”integrasjonslag” er en sentral endring i fremtidens MIL INI. Informasjonen og tjenestene er tilgjengelige gjennom standardiserte grensesnitt (IKT 2005 s. 8). Dette vil være en stor endring både teknologisk og i forhold til menneskelige og organisatoriske faktorer og utgjør potensielle sårbarheter. På den ene siden medfører integrasjonshåndtering ved bruk av et standardisert integrasjonslag en forenkling for forvaltningen og administrasjon. Dette ved at integrasjonslaget stiller krav til tjenestene, som ønsker å uveksle data, må tilfredsstille. På den andre siden vil prinsippet kunne øke sårbarheten ved ett integrasjonslag som ansvarlig for all datautveksling internt (og eksternt) i MIL INI – ”single-point-of-failure”.

Integrasjonsfagmiljøet i Forsvaret har allerede opparbeidet seg erfaring med etablering av et felles integrasjonskonsept. Dette er viktige erfaringer å ta med seg videre. Det må ikke oppfattes at det ikke vil være mulig med spesialhåndtering av grensesnitt mellom tjenester. Men avvik fra etablerte standarder må håndteres slik at det naturlig oppfattes som en del av den samme helhet. Jo flere avvik fra standardene som eksisterer, jo større utfordringer har man i forhold til vedlikehold og samspill mellom ulike standarder (behov for proxyer[54]). Dette vil øke systemets kompleksitet, noe som igjen øker sannsynligheten for sårbarheter ovenfor fiendtlig INFOOPS.

[53] FIF forvaltningsregimer er forankret i Information Technology Infrastructure Library (ITIL) som e et konsept for beste praksis (”best practice”) i hvordan IT/forvaltningsprosesser best utføres.
[54] Med proxy menes et grensesnitt (interface) for en tjeneste som i utgangspunktet er remote, ressursintensiv eller vanskelig å benytte/bruke direkte (*Proxy*).

Prinsippet om en gjennomgående integrasjonsløsning vil også kunne medføre at (deler av) arven vil måtte påkostes dels betydelige endringer som øker den økonomiske sårbarheten. En annen sårbarhet er at det kanskje ikke er (teknisk) mulig å endre systemarven i det hele tatt.

En siste potensiell sårbarhet/utfordring i forhold til ”fritt tilgjengelig informasjon” er faktiske formelle kriterier utenfor Forsvaret som pålegger (godkjennelse og) kontroll av informasjonsspredning, for eksempel konsesjon fra Datatilsynet. På den andre siden er det ikke slik at alle skal kunne få aksess til alt selv om konseptet åpner for det. Fremtidens MIL INI vil (logisk og/eller fysisk) måtte håndtere sensitiv/prioritert informasjon til utvalgte miljøer. For eksempel er det et stort fokus i Forsvaret på å beskytte identiteten til personell som tjenestegjør i utenlandsoperasjoner (FFI 2008). Hva som er påkrevd og hvordan dette skal løses må tas som en del av utarbeidelsen av et velutviklet informasjonsstyrings konsept.

7.7 Sikkerhetsaspekter

Operasjonssikkerheten (OPSEC) skal hindre en motstander fra å skaffe seg informasjon om våre operasjoner, objekter, kapasiteter og intensjoner (FFOD 07 pkt. 0597). Sikkerhetsloven ([Sikkerhetsloven 1998]), herunder forskrift om informasjonssikkerhet (INFOSEC) ([Informasjonssikkerhet 2001]), er utformet med dette som utgangspunkt. Dette er muligens her den største utfordringen er med et fullt ut gjennomført NbF. Det må endringer til i både nasjonale (Sikkerhetsloven) og i NATO policyer for å få til NbF visjonen (EXP 2008).

Godkjente tekniske løsninger for flyt av informasjon fra lavere til høyere graderingsnivå finnes. I tillegg ligger det til rette for tekniske løsninger for informasjonsspredning fra høyere graderingsnivå. Mye vil dreie seg om grensetrekking og nye sikkerhetsprinsipper. En sårbarhet er om det vil være vilje innenfor (sikkerhets)miljøene til å imøtekomme behovet for nye og/eller endrede sikkerhetsprinsipper; hvor høy risiko Forsvaret og de politiske miljøene er villig til å operere under (EXP 2008). Dette vil dreie seg mye om holdninger, risikohåndtering og vilje til endring. På den andre siden så står det i Forsvarspolitisk utvalg sin offentlig utredning (NOU 2007:15 s. 22) et behov for økt fokus på operasjonssikkerhet. Bakgrunn er i at utnyttelsen av ny teknologi kan åpne for nye sårbarheter og trusler, for eksempel ved at kritiske funksjoner sentraliseres og at det blir færre enheter.

Det skal dog sies at det er iverksatt aktiviteter hvor det sees på endringer fra dagens regelbaserte sikkerhetskonsept (forebyggende sikkerhet) til mer fremtidsrettede sikkerhetskonsepter for eksempel et mer risikobasert sikkerhetsregime. Forebyggende sikkerhet angir egentlig bare et

minimumsnivå av sikkerhet, mens et risikobasert regime er det mulig å ”gå opp og ned” alt avhengig av trusselen og intensiteten (EXP 2008). Dette vil fordre systemer som kan avdekke unormale hendelser og et bakenforliggende apparat som håndterer dette (EXP 2008). En annen stor utfordring er hvordan sikkerheten til de enkelte informasjonsobjekter skal ivaretas. For eksempel hvordan merke informasjonsobjekter med rett gradering? Enkle og enhetlige sikkerhetsløsninger som etableres vil være et bedre utgangspunkt for sikker informasjonsflyt som igjen antagelig reduserer sårbarheten. I tillegg vil mer enhetlig sikkerhetsløsninger være et bedre utgangspunkt for alle de andre MIL INI investeringene/tiltakene som skal ha Forsvarets sikre plattformer som kjøremiljø som tidligere diskutert.

Et tiltak rundt bedre informasjonsflyt kan være å avhende dagens ugraderte to-nivå løsning på FISBasis Begrenset løsningen[55]. Dette vil kunne være et tiltak som vil kunne lette en fremtidig toveis kommunikasjon mellom graderingsnivåene Begrenset og Hemmelig. På den andre siden vil en slik beslutning kunne medføre et økt behov for tilgjengeliggjøring/tilgang på Forsvarets ugradert løsning – spesielt for de miljøer i Forsvaret som i stor grad er avhengig av ugradert kommunikasjon i sine daglige gjøremål. I tillegg er denne ugraderte to-nivåløsningen en direkte sikkerhetsrisiko.

Nasjonal Sikkerhetsmyndighet (NSM) har nylig utgitt et temahefte rundt *Nettsamfunn og sikkerhet* (NSM 2008). Dette som et resultat av at det eksisterer eksempler på alvorlige sikkerhetsbrudd ved at gradert informasjon er tilgjengeliggjort i nettsamfunn (*Utfordringer i nettsamfunn*). Det siteres fra temaheftet: ”Sikkerhetsgradert og annen sensitiv informasjon ble offentliggjort. Mange ansatte med tilgang til sikkerhetsgradert informasjon gjorde seg synlige for det vi kaller potensielle trusselaktører.” (NSM 2008 s. 4). Sårbarheten i den forbindelse henger blant annet sammen med enkeltindividers generelle mangel på kunnskap og bevissthet omkring behovet for INFOSEC. I tillegg er de lite bevisst hvilken rolle de selv spiller som ”aktør på nett” (NSM 2008 s. 5).

En annen konkret sårbarhet, som også gjelder dagens MIL INI, er at det på nettsamfunn beskrives hvordan Forsvarets system kan omgås for å aksessere nettsamfunnet gjennom Forsvarets Intranettløsning (Løvland 2008). Spredningen av slik informasjon kan åpne for direkte fiendtlig utnyttelse som igjen kan være skadelidende for Forsvaret. Slike sårbarheter bekreftes også ved gjennomført forskning på andre områder. FFI (Thuv et al 2007) har gjennomført en sårbarhetsanalyse av Internett. Fremtidens INI kan sies å ha mange likhetstrekk

[55] Dette konkrete forslaget ble presentert for representant for Forsvarets sikre plattformer på FLO/IKT avdelingen for Beslutningsstøttetjenester (FLO/IKT BST) sitt fagseminar april 2008 (FLO/IKT 2008).

med Internett slik vi kjenner det i dag. Med dette som utgangspunkt er det formålstjenelig å skue til de sårbarhetsvurderinger som er gjort av Internett for å kunne dra erfaring og lærdom over i en MIL INI kontekst. Et viktig moment fra FFIs forskning er at alle systemer som er tilknyttet Internett på et eller annet tidspunkt vil kunne være sårbare overfor angrep –"…alt fra et sikkerhetshull i en tjeneste til et sikkerhetshull i en avansert teksteditor…" (Thuv et al 2007 s. 17). Et eksempel her vil for eksempel kunne være FDs ugraderte nett som på mange måter er departementets daglige hovedverktøy sammenlignet med Forsvarets graderte løsninger. Når det er sagt har FDs selvsagt også graderte løsninger som brukes daglig.

Dagens sikkerhets- og akkrediteringsprosess er tung og tidkrevende. For å kunne legge forholdene til rette for visjonen om sømløse tjenester, løpende tilknytning av nye MIL INI-komponenter vil fremtiden kreve langt mer fleksible prosesser. Hvorvidt løsninger er å "forhåndsakkreditere" potensielle samarbeidspartnere/brukere, endrede sikkerhets- og akkrediteringsprosesser må sees på som en del av transformasjonen for å på den måten avstemme hvilke muligheter som finnes og hva som anses mest formålstjenelig for på den måten å minimere disse potensielle sårbarhetene[56].

En siste sårbarhet er hvordan et økt tverrdepartementalt samarbeid vil måtte forholde seg til forskjellige (tekniske) løsninger, forskjellige semantisk forståelse, forskjellige kulturer for håndtering av gradert informasjon osv. Et eksempel er at (kjente) forskjeller mellom Forsvaret og Politiet. Etablering av en felles kultur og ikke minst felles erkjennelse og (tekniske) løsninger, i det minste løsninger med felles sikkerhetsprinsipper i bunn, er en viktig som en del av et økt samarbeid. I tillegg må det jobbes med ytterligere holdningsskapende arbeid – ikke minst rundt sårbarhetene med lekkasjer/tilsvarende til media.

7.8 Sivil tjenestetilkopling

Ett område som er kandidat for utstrakt sivil-militært samarbeid er innenfor logistikk. Dagens logistikkonsept kan sies å være basert på forbruksprognoser med den hensikt å sikre strøm av forsyninger til rett sted i rett tid. I tillegg er logistikken i all hovedsak et nasjonalt ansvar. I fremtiden vil konseptet være basert på reell logistikk, gjerne omtalt som *behovsrettet logistikk* (form for "*just in time*"). Konsekvensen er at den totale logistikkflyten vil kunne reduseres fordi strømmen av forsyninger og tjenester vil være et produkt av de behov som blir etterspurt i

[56] Det er å anta at de erfaringene Forsvaret har fra Joint Warfare Centre (JWC) kan bidra i prosessen. Der må det i dag håndteres problemer med fysisk og logisk separasjon av løsninger/systemer avhengig av hvilke nasjonalitet som trenes (DVU 2008).

operasjonsområdet. Dette vil kreve kontinuerlig tilgang på relevante og fleksible transportmidler samt behovet for å redusere logistisk hale ved variantbegrensninger som igjen stiller krav til materiellinvesteringene – en økt sårbarhet (Christensen 2003).

Logistikk –og Støttekonseptet for Forsvaret beskriver kort hvordan Forsvarets fremtidige målbilde bør være. Dette beskriver et nettverksbasert forsvar der logistikkorganisasjonen inngår som en integrert del, og hvordan dette vil lede til ytterligere krav til hurtighet og fleksibilitet (FST 2004:13)[57]. Det faktum at Forsvaret ikke lengre har ressurser til å sitte på store lagre og ikke besitte egen (vedlikeholds)kompetanse innenfor alle fagområder, men må/vil bruke sivile organisasjoner for etterforsyninger og/eller (vedlikeholds)arbeid, er også konkrete sårbarheter. Dette vil medføre nødvendigheten av sivil integrasjon mot MIL INI i tillegg til at Forsvaret må ha tillit til sine (sivile) samarbeidspartnere. Problemstillingen med utro (eksterne) tjenere og/eller insidere vil være sårbarheter som Forsvaret må erkjenne at eksisterer og håndtere deretter. ”De smarte har aldri noe på seg!” (EXP 2008). Et eksempel her er sikkerhetsklareringsprosessen. Den prosessen sjekker alle relevante registre, men det er fullt mulig å ha ”svin på skogen” uten at dette er registrert. For eksempel har Forsvaret nulltoleranse i forbindelse med bruk av narkotika, mens granskningsrapporter viser store mørketall (EXP 2008).

I tillegg er det mange argumenter for et utstrakt tverrdepartementalt samarbeid, spesielt mellom Forsvars- og Justisdepartementet, men kanskje også Utenriksdepartementet i lys av Norges internasjonale engasjement. Utbedret interoperabilitet med andre nasjonale enheter som politi, toll og fiskerimyndigheter er også fokusert på av Hafnor (2006 s. 12-14) og av henne omtalt som ”Joint National Interoperability”. Et annet konkret eksempel hvor sivil tilkopling anses aktuelt er mot Meteorologisk institutt i forhold til værdata. Dette vil gi en konkret sårbarhet i forhold til tilgjengeligheten og kvaliteten på værdatainformasjon. For eksempel benytter kyst radarkjeden sivile værdata for å sikre sanntids tilgjengelighet (EXP 2008).

Kravet om interoperabilitet med sivile samarbeidspartnere gir store utfordringer/potensielle sårbarheter. Innenfor fagområdene logistikk, beskrevet over, og andre deler av den offentlig forvaltningen stilles ofte de samme (tekniske) krav til IKT-løsninger/tjenestene. Bruk av veletablerte offentlige og/eller kommersielle standarder for utveksling av informasjon ligger gjerne til grunn. På den andre siden er det ikke gitt at det er de samme standardene og/eller prinsippene for informasjonsutveksling Forsvaret legge til grunn i MIL INI. En annen potensiell

[57] ”Et fremtidig logistikk konsept må fokusere på å understøtte nettverksorienterte effektbaserte operasjoner...Logistikksystemet må kunne håndtere hurtige skift i operasjonsmønstre og prioriteringer, og kunne respondere raskt på stadig skiftende behov for logistisk understøttelse.” (FST 2004 s. 13).

utfordring kan være at andre (offentlige) samarbeidspartnere ikke er på samme modenhetsgrad av tjenestetenkning som Forsvaret. Fremtidig samhandling med sivile aktører[58] i et aktuelt innsatsområde som del av internasjonale operasjoner vil også øke sårbarheten – både i forhold til faktisk evne til samhandling, men også i forhold til (offentlig og/eller uutalt) vilje til samhandling. I tillegg øker sårbarheten i forhold til "militær kontroll".

7.9 Delkonklusjon

I dette kapitlet er det diskutert en rekke utfordringer og (potensielle) sårbarheter som følge av transformasjonen mot fremtidens MIL INI. Mange av sårbarhetene er det mulig å begrense omfanget av ved å være de bekjent og ved å iverksette tiltak. Denne oppsummeringen vil presentere utvalgte sårbarheter utledet fra den gjennomførte analysen.

Forsvares MIL INI prosjektporteføljе er stor med mange komplekse relasjoner og avhengigheter – både tekniske, men også sosiale og informasjonsmessige avhengigheter. Uten en sentral styring og kontroll på iverksatte (materiell)investeringer vil det kunne medføre utvikling og innfasing av overlappende og/eller motstridende løsninger som i fremtidig MIL INI skal kunne samhandle. I tillegg vil spesielle anskaffelser inn mot prioriterte miljøer som eksempelvis spesialstyrkene åpne for at nettopp disse anskaffelser vil være inngangsporten for fiendtlig INFOOPS – kanskje med utgangspunkt i at behovet for slike løsninger er så viktige at sikkerhetsaspekter lempes på. Jo mer kompleks, og kanskje til og med inkonsistens, MIL INI jo mer krevende med total sikkerhetsmessig forvaltning. En angriper på sin side trenger bare å finne og utnytte én sårbarhet – og ikke nødvendigvis tekniske sårbarheter.

Ved investeringer i fellesløsninger er det en iboende spenning ved at ikke alle løsninger passer for alle. Denne utfordringen fører også til flere systemer/løsninger, både antall systemer, men også spesialtilpassede systemer, som skal samhandle – både teknisk og et omforent begrepsapparat. Mangel på sentral styring og vilje til å vurdere etablerte prosesser fremfor tilpassing av standardløsninger er potensielle sårbarheter. Også tidsaspektet kan fungere som en sårbarhet ved at strategiske anskaffelser har så dårlig tid at beslutninger gjøres og/eller endres til fordel for raskere leveranser enn "riktig" leveranse.

Jo flere som velges som sentrale samarbeidspartnere jo mer krevende er det å få til fremtidig samarbeid. Selv om samarbeid i NATO legger til rette for dette med utstrakt bruk av etablerte standarder, vil det å måtte forholde seg til alle disse, som også kanskje internt er inkonsistente,

[58] Sivile aktører i denne sammenheng vil typisk være Governmental organisations (GOs) og Non-governmental

øke sårbarheten. Særnasjonale krav som ikke fravikes gjør at NATO også må operere med flere standarder enn det strengt tatt er behov for. Ved å samarbeide med andre nasjoner som ikke er pålagt/selv ønsker å følge for eksempel NATO sine etablerte standarder kompliserer bildet ytterligere. Sårbarheter i (internasjonale/etablerte) standarder kan utnyttes av en motpart. Utstrakt samarbeid vil også medføre sårbarhet i form av mer behov for kompetanse, utdanning og relasjonsbygging. I tillegg blir en helhetlig styring av Forsvaret de-fragmentert.

MIL INI konseptet med sine felles kjernetjenester er sårbare ved at feil/manipulasjon vil kunne ramme ”alt og alle” ved at disse tjenestene fungerer som ”single point of failure”. For å sikre en fremtidig helhetlig og sømløs tjenestetilbyder er det også viktig at det ikke investeres i forskjellige retninger. I den forbindelse er det avgjørende at Forsvaret besitter fagkompetanse og evner å styre slike investeringer i tillegg til at det stilles krav. All den tid fremtidens MIL INI ikke etableres fra ”bunnen av” vil det også være en sårbarhet at de første (grunnleggende) investeringene/løsningene vil legge føringer på kommende tjenester. I den forbindelse er det viktig å ha en helhetlig arkitekturmessig tilnærming i alle investeringer/aktiviteter. De tekniske løsningene er også viktig å være klar over ved at sentrale servere (på en gitt kommandoplass) som for eksempel inneholder kritiske informasjonstjenester vil kunne medføre at fiendtlig INFOOPS rettet mot informasjonsdomenet slår ut sentrale kommandoplasser.

Ved at fremtidig MIL INI, i likhet med Internett, har svært mange aktører, tjenester og typer av disse vil det kunne påkreve et antall regimer for administrasjon og tjenestehåndtering – regimer som igjen vil måtte samhandle. For eksempel vil en underleverandør i en nasjon ha behov for å samhandle med aktører i en annen nasjon. Eller som kanskje verre er at underleverandører i to forskjellige nasjoner har behov for å samhandle og i verste fall gjør dette helt utenfor militær kontroll. Jo mer utstrakt MIL INI blir jo flere tilkoplingspunkter er det å utnytte for fiendtlig INFOOPS.

En fremtidig MIL INI vil måtte forholde seg til den arven som er. I noen tilfeller vil det være situasjoner hvor det ikke er (teknisk) mulig, ei heller kanskje ønskelig, å bytte slike løsninger ut. I tillegg kan arven i seg selv ha iboende sårbarheter med utgangspunkt i den programvaren de er utviklet i og de arkitekturvalg som på det tidspunktet systemene ble utviklet var ”state of the art”. Slike iboende sårbarheter kan være umulig å fjerne og kan på den måte representere (kjente) sårbarheter som kan utnyttes av en motpart.

---

organisations (NGOs).

Sikkerhet er gjerne trukket frem som store utfordringer i NbF konseptet. Informasjonsflyt mellom graderingsnivåer, gjerne kombinert med iboende sårbarheter i (grunnleggende) systemer/løsninger er konkrete sårbarheter som må håndteres. For (teknisk) å imøtekomme disse sårbarhetene må det være evne og vilje til å endre grunnleggende sikkerhetsprinsipper. Konkret er sikring på informasjonsobjektsnivå en sårbarhet som må håndteres. For eksempel vil et informasjonsobjekt måtte beskrives med metadata for å være i stand til å bli funnet i et søk. Hvis informasjonsobjektet er høyere gradert så kompliserer dette situasjonen ved at metadata må beskrive informasjonsobjekter uten å "avsløre" innholdet.

Ved å gå i en retning av mer risikobasert sikkerhetsregime vil dette kunne åpne for nye sårbarheter hvor en beslutningstakers egen risikovillighet vil være avgjørende og varierer mellom forskjellige individer. En annen sårbarhet i forhold til å endre grunnleggende sikkerhetsprinsipper er å sikre nødvendig grad av kompetanse(heving) og bevisste individer med de rette holdningene.

Logistikkfunksjonen er et område hvor fremtidig MIL INI er sårbar i lys av konseptet sin utstrakte samhandling med sivile aktører. Behovsrettet logistikk gjør Forsvaret sårbart i forhold til etterforsyninger/tilsvarende. Dette er en (ny) arena som fiendtlig INFOOPS kan utnytte – ikke minst ved å angripe mål utenfor militært ansvarsområde, som for eksempel å slå ut sentrale transportårer og bruk av insidere i underleverandører. Andre sårbarheter er i den grad sivil tilkopling er påkrevd og hvor den/de sivile enheter ikke er interoperabel med de militære miljøene. Temporære løsninger vil kunne fremtvinge seg, med den konsekvens at det svakeste leddet vil være en arena for fiendtlig påvirkning og derigjennom en kanal inn i militære systemer. Et eksempel vil kunne være (nasjonale krise) hvor forskjellige departementer blir påkrevd å samhandle.

8 Sentrale sårbarheter i beslutningstakeres avhengighet og anvendelse av MIL INI

"A decision-maker's effectiveness is a function of *will*, *understanding* and *capability*..[og] a decision-maker must have the will to act, an understanding of the situation to act and possess the capability to act." (AJP-3.10 2008 s. 14, kursiv i originalteksten). Forsvarets IKT policy (2005 s. 9) uttrykker at nettverksbaserte operasjoner gir en økt avhengighet av MIL INI, herunder økt mottakelighet/følsomhet for manipulasjon, degradering og tap (av denne).

I følge Zanini og Edwards (2001 s. 41) vil teknologien i informasjonsalderen kunne bistå terrorister og andre aktører i å utføre tre hovedtyper av offensive INFOOPS – persepsjonsledelse og propaganda, angrep på virtuelle/logiske mål med den hensikt å bryte disse ned og som bruk for fysisk ødeleggelse. Militære enheter som storforbruker av informasjon muliggjør økt fiendtlig fokus på tiltak for å påvirke beslutningstakere og andre – påvirkning som er forenelig med fiendtlig INFOOPS[59]

Hensikten med dette kapitlet er å analysere sentrale sårbarheter i beslutningstakere sin avhengighet og anvendelse av fremtidens MIL INI med utgangspunkt i faktorene *situasjonsbevissthet* samt *evne og vilje til beslutning*. Før selve analysen beskrives oppgavens tenkte fremtid og den konstruerte konflikt (scenario) presenteres. Dette som utdypende bakgrunnsinformasjon. Hver av analysefaktorene avsluttes med en delkonklusjon.

8.1 Tenkt fremtid

Oppgavens tenkte fremtid samsvarer med NbF grad 2, *integrerende NbF*. Det er egenskapene ved den tenkte fremtiden (NbF grad 2) som er av interesse. Tidspunktet for når denne fremtiden inntreffer er ikke sentralt for analysen [60]. Kapittel 4.3.1 NbF tilstandsbeskrivelser presenterer de forskjellige modenhetsgradene til NbF med sine forskjellige egenskaper.

Med utgangspunkt i Enemo (2006) sine ni opprinnelige NbF faktorer har undertegnede avledet noen overordnede faktorer for å forenkle prosabeskrivelsen av den tenkte fremtids egenskaper. Dette tiltaket er utelukkende gjort som en metodisk forenkling, se vedlegg B. Det presiseres også at ikke alle faktorene er tatt med som del av den deskriptive beskrivelsen.

[59] Kjernen i INFOOPS er overordnet å påvirke vilje, evne og forståelse.
[60] I den grad identifiserte sårbarheter påvirkes av den generell samfunns- og teknologiske utviklingen vil det i oppgaven tas inn som en naturlig del av analysen og diskusjonen.

NbF grad 2 – integrerende NbF

Nettverksorganisering: Det forventes et mer fleksibelt og dynamisk Forsvar, med flatere struktur og en utbredt forståelse for NbF. Hvorvidt flatere struktur betyr færre operasjonsnivåer eller andre tiltak som "flater ut" Forsvaret er ikke uttalt presist. Mange mener at operasjonsnivåer forsvinner og/eller at nivåene kan komme til å se forskjellige ut[61]. En nettverksorganisering vil kunne medføre (indirekte) effekter som økt tempo i (beslutnings)prosesser, bedre muligheter til å koordinere i alle dimensjoner, bedre forutsetninger for kontroll og økt evne til å overvåke. Prosess- og prosedyreutvikling vil inntreffe, spesielt i forhold til å redusere sekvensielle prosesser. Vertikal styring og faste prosedyrer vikes gradvis til fordel for desentralisert styring og horisontal koordinering.

INI og teknologi: Materiell/tjenester "Netready", med vekt på "PlugNPlay" i et felles gjennomgående kommunikasjonsnettverk. Integrerende informasjonsstyring sikrer informasjonstilgjengelighet, dog uten "bruksgarantier". Tilrettelegging for økt samhandling. Mer innovativ bruk av IKT.

"Den militære profesjon": Spesialister med spisskompetanse erstatter generalister med bredde kompetanse. Individuell og institusjonell evne til samarbeid og mer helhetlig sosial tilhørighet vektlegges. Håndtering av løpende organisasjonsendringer og fleksibilitet vektlegges. Ledelse og beslutningsprosess er mer preget av intuisjon og bruk av nettverket. Evne til selvstendig tenkning og beslutningstagning er vektlagt. Hovedsakelig desentralisert makt og beslutningstagning. Sentralisert beslutningstagning i strategisk kritiske situasjoner.

Interoperabilitet: Gjennomgående interoperabilitet i Forsvaret og dels mot eksterne aktører. Det er ikke presisert hvilke eksterne aktører som vil være naturlige samhandlingsaktører, men det er å anta at både sivile aktører i teateret og på hjemmearena er mulige representanter. Fokus på militær interoperabilitet.

Oppsummert vil Integrerende NbF medføre at antall brukere og tjenester øker. Forsvaret vil være mer avhengig av tjenestene. Samhandling i nettverk med nye typer aktører – sivile som andre militære (og potensielt motstandere?). Organisasjonsstrukturen "flates ut", herunder desentralisert beslutnings- og informasjonshåndtering og økt tempo i prosesser. Andre sentrale egenskaper er fleksibilitet, kravet om need-to-share; tillit og dynamisk akkreditering.

[61] Nbf kjernegruppe sier i sin sluttrapport til Forsvarsstudie 2007 (FS07): "Hierarkiet skal bestå, i henhold til Forsvarets styringsprinsipper. Samtidig er nettverket mer tverrfaglig, matriseorganiserte og "flate". Til sammen betyr dette en økt fleksibilitet i organiseringen." (NBF 2007 s. 4).

8.2 Konstruert konflikt

Dagens konflikter

Dagens konflikter har endret seg i forhold til ”norm” under den kalde krigen. Fra i den kalde krigen å ha en spenning mellom to motpoler, supermaktene USA og Sovjetunionen, ser vi en tendens etter 1989 at denne spenningen er oppløst til fordel for andre spenningsforhold. Mer kompleks interaksjon/samhandling mellom statlige og ikke-statlige aktører hvor globalisering og konkurranse om ressurser kombinert med ideologiske, religiøse og kulturelle forskjeller gir økt usikkerhet. Parallelt med dette har vi hatt en ”informasjons revolusjon”.

”Cyber angrep” foregår jevnt både i konvensjonelle og ikke-konvensjonelle konflikter. USA, UK og mange andre nasjoner i Vesten har egne ”cyber warfare” kapabiliteter. Men også nasjoner som Kina, Liberia osv utvikler egne kapabiliteter. I tillegg utvikles slike kapabiliteter av terror organisasjoner, sympatisører, hacker grupper osv, ofte med (stilltiende) samtykke av ”host nations” - kapabiliteter som har potensial til å skadeliggjøre vestlige informasjonssystemer, kommunikasjon og infrastruktur i kommende konflikter (Berglund 2004 s. 17).

Scenariobeskrivelse

Norge bidrar i konfliktdomenet[62] med et militært styrkebidrag som del av en større allianse. Styrkebidraget har vedvart en lengre periode og det planlegges i utgangspunkt ikke endringer i forhold til dette. Alliansen har styrkebidrag fra NATO, PfP-nasjoner samt andre villige. Det norske styrkebidraget må sees på som relativt lite, men bidraget består av kritiske ressurser (nisjekapasiteter) som for eksempel spesialstyrker.

De norske styrkene må forholde seg til nasjonale caveats og alliansens ROEs i tillegg til nasjonal- og internasjonal lov.

Norge innehar kapasitet for militære datanettverksoperasjoner (CNO-enhet) samt kapasitet for deployerbar kommunikasjon og informasjon (CIS TG).

Trusselbeskrivelse

Utgangspunktet er en langvarig konflikt mot en irregulær styrke forenelig med begrepet ”netwar”. I følge Arquilla og Ronfeldt (2001 s. 6) er begrepet netwar en forkortelse for tradisjonell militær krigføring, hvor forkjemperne (eng: protagonist) benytter nettverksorganisering[63]. Forkjempernes doktriner, strategier og teknologier er i samsvar med

[62] Betegnelsen domene er benyttet for å poengtere at (dagens og) fremtidens konflikter ikke trenger å være knyttet til tradisjonelle og/eller spesifikke operasjons-/konfliktområder.
[63] Disse forkjemperne består gjerne av spredde organisasjoner, små grupper, og individer som kommuniserer, koordinerer og utfører sine handlinger/kampanjer i en ”internettet”/samhandlede nettverk – ofte uten noen konkrete

informasjonsalderen for øvrig og begrepet er oppstått med forankring i en konflikt- og kriminalitetsmodus på samfunnsnivå.

Konflikten har pågått med varierende intensitet. Både den irregulære styrken og alliansen er periodisk involvert i kamphandlinger, noen ganger med tap av liv. Også det norske bidraget har måttet tåle tap av liv. Stater i nær tilknytning til konfliktdomenet opptrer politisk aggressive i tillegg til at deres militære styrker øker sitt aktivitetsnivå, spesielt i "grenseområdene".

Verdensopinionen har varierende syn på det internasjonale militære bidraget og store bidragsnasjoner utfordres med tidvis reduserende støtteerklæringer fra egne borgere og andre nasjoner. Også i Norge, internt i regjeringen, men også blant befolkningen, er det varierende syn på det norske bidraget, ikke minst i forhold til hvordan styrkene bidrar/brukes. Enkelte nasjoner planlegger å trekke ut sine styrker, mens andre nasjoner vurderer økte/nye bidrag.

Den irregulære styrken har en viss teknologisk grunnkompetanse som gjør at denne utgjør en reell trussel for fiendtlig INFOOPS anslag. Den irregulære styrken ønsker at Norge skal trekke ut sine militære styrker og velger derfor å påvirke operasjonen (og det norske samfunnet) med en rekke koordinerte anslag forenelig med en fiendtlig INFOOPS; den irregulære fienden er bevisst på å påvirke nasjonale holdninger for på den måten å presse politisk miljø til å trekke styrkene ut. Vedlegg C gir en beskrivelse av den irregulære styrken sin planlagte anslag og et mulig hendelsesforløp. Det presiseres at de beskrevne anslagene og hendelsesforløpet utelukkende har vært et utgangspunkt for diskusjon og datainnsamling – ikke som en faktisk "historie" som analysen skal ta utgangspunkt i. Dette for ikke å være en begrensende faktor. Av den grunn vil analysen kunne trekke frem sårbarheter som ikke direkte kan henvises til scenariets beskrevne anslag/hendelsesforløp.

8.3 Situasjonsbevissthet

Slik FFOD (2007 pkt. 0594) beskriver det så har fiendtlig påvirkning, forenelig med INFOOPS, ambisjonen om å påvirke de tankeprosesser som ligger til grunn for individers situasjonsoppfatning og beslutningstaking igjennom påvirkning av informasjon. Sett i lys av domenemodellen påvirkes"…det kognitive domenet…for å påvirke persepsjoner og vilje…det sosiale domenet for å påvirke samholdet individene imellom, og mot informasjonsdomenet for å påvirke informasjon og informasjonsoverføring." (FFOD 2007 s. 135).

---

sentral ledele. Begrepet netwar er ment å dekke det faktum at nettverksbasert konflikt og kriminalitet vil være sentrale fenomener i de kommende tiårene (Arquilla & Ronfeldt 2001 s. 6).

En beslutningstakers situasjonsbevissthet påvirkes blant annet av informasjonsmengden, kvaliteten på informasjonen og informasjonsstyringen (FFOD 2007 pkt. 0587).

8.3.1 Informasjonsmengde

I mange virksomheter er det tradisjon for å bevare all informasjon ”for sikkerhets skyld”. Praksisen kan ha rot i uklarheter rundt hvilket behov virksomheten har samt mangel på klare roller og ansvarsforhold. Som et ledd i å minske sårbarheten på dette området er dette en tradisjon/kultur som bør utbedres (Kalseth & Knoop 1996 s. 30). Dette som et ledd i utvikling av et velutviklet informasjonsstyringssystem.

Fremtidens MIL INI vil inneha langt mer tilgjengelig informasjon på tvers av brukergrupper og sikkerhetsnivåer enn det som er tilfellet i dag. På den ene siden åpner dette for at alle har anledning til å ”se og vite” alt. På den andre siden er det en åpenbar fare for informasjonsmetning. Denne sårbarheten er også bekreftet av Berglund (2004 s. 16). Selv om mengden informasjon kan være en sårbarhet så er det ikke mengden informasjon i seg selv som er utfordringen. En konkret sårbarhet er filtrering av informasjon som påser at den viktige informasjonen ikke ”drukner” i mengden (EXP 2008). For eksempel viser mailsystemet på FISBasis allerede i dag tendenser til slik ”overload”. Det er ikke unormalt at sjefer (og andre) uttaler ”…jeg har så mye i innboksen min at jeg ikke har sett meldingen din”. Hvorfor blir det slik? Mye av ansvaret ligger på den som er avsender av informasjonen. Ofte inkluderes en rekke (kopi)adressater for å sikre spredning av informasjon. En mulig årsak er at det ikke er noe felles ”informasjonsbank” eller andre alternativer hvor interessenter kan søke etter tilgjengelig informasjon. Når det er sagt har vi noen systemer som kan sies å ha noen slike egenskaper. For eksempel Forsvarets Intranett, Doculive, Ferdaball (erfaringsdatabase), forskjellige prosjektarkiv og fellesdisker. Utfordringen er at disse systemene/løsningene ikke benyttes etter intensjonen samt at de ikke har den funksjonalitet og detaljeringsgrad som skal til for å operere som ”informasjonstilbyder”. I tillegg vil sosialt nettverksamarbeid, blant annet igjennom medlemskap i forskjellige COIs, fremme mer informasjonsflyt og derigjennom økt sårbarhet.

Fremtidens nettverksorganisering vil kreve en langt større iboende kultur for å tenke helhet for på den måten å ivareta fellesskapets beste. Å bedre situasjonsbevisstheten ved samhandling og informasjonsdeling på tvers i nettverket vil kreve både evne og vilje. Et eksempel i den forbindelse er dagens regelbaserte sikkerhetsregelverk som ikke kan sies å tilfredsstille de krav og behov som fremtvinger seg i morgendagens konsepter. Et sikkerhetskonsept basert på en mer

dynamisk risikovurdering og som ivaretar sikkerheten helt ut i endesystemene vil være viktig for fremtidig dynamisk informasjonsflyt (Hafnor 2006 s. 11; Gagnes et al. 2005 s. 21).

Evne og vilje til deling av informasjon vil også kreve interoperabilitet og tilgjengelighet (Hafnor 2006 s. 11). I lys av oppgavens konstruerte konflikt er dette konkrete sårbarheter – både den faktiske (og fysiske) evnen for informasjonsdeling, hvor interoperabilitet er et sentralt. Men, også viljen til å utveksle informasjon, hvor tillitsbegrepet er sentralt. Dette gjelder både på tvers av nasjoner, men også mellom (fag)miljøer nasjonalt og i selve konfliktdomenet. For eksempel er tilgang på etterretningsinformasjon grunnlag for gjennomføring av militære operasjoner. I fremtidige nettverksbaserte operasjoner vil løpende flyt av etterretningsinformasjon være påkrevd. For at dette skal kunne skje, må det være vilje til informasjonsspredning av etterretningsinformasjon. Spørsmålet er hvorvidt det eksisterer en slik vilje. En sårbarhet er hvis viljen avviker mellom forskjellige (operasjonelle)nivåer. I tillegg er det kanskje også lovverk som er hindringer for slik spredning? Et eksempel er gjennomføring av etterretninger mot egne borgere. Og hva med tillit? I lys av oppgavens konstruerte konflikt hvor den norske styrkene er del av en multinasjonal allianse, kanskje med nye NATO medlemsland enn de som pr i dag er medlemmer, gjør at dette er en sentral sårbarhet. I tillegg er det kanskje ikke faktisk mulig å tilgjengeliggjøre informasjonen grunnet ikke-interoperable MIL INI tjenester – både mellom de militære deltakernasjonene[64], men også mot sivile aktører i konfliktdomenet og tverrdepartementalt.

Ved at vi gjør oss mer avhengig av informasjon vil dette kunne medføre at militære operasjoner vil måtte ta nye typer av terreng for blant annet å kommunisere i felt. For eksempel ved utplassering av radiolinkmaster som i seg selv er sårbare objekter for fiendtlige INFOOPS[65]. På den andre siden kan satellitt vurderes som kommunikasjonsnode som også øker kommunikasjonskapasiteten blant annet igjennom muligheter for langdistansekopling av MIL INI (EXP 2008). Vil en (norsk) satellitt være en fremtidig forutsetning for MIL INI? Norsk tilgang på satellitt kan for eksempel skje ved egen anskaffelse, bilateralt samarbeid eller ved å leie kommersielt. Alle disse alternativene medfører nye sårbarheter, hvor graden av sårbarheten kan variere i lys av type eierskap. Det er flere eksempler på ”kapring” og forstyrrelser av kommunikasjonssatellitter gjennomført både av nasjoner og forskjellige interesseorganisasjoner (Lowe 2006; *Asian Economic News*).

---

[64] Det hevdes i noe litteratur at de nyeste NATO medlemslandene ikke nødvendigvis makter/evner å følge tritt med Alliansen (teknologiske) NbF implementering. Også etablerte medlemsnasjoner strever med å følge den (teknologiske) utviklingen (Berglund 2004 s. 1).

[65] Radiolink master er også utsatt ovenfor andre fiendtlige handlinger uten at dette er sentralt for oppgaven.

Fiendtlige koordinerte INFOOPS ”anslag” forenelig med oppgavens konstruerte trussel vil også medføre et stor grad av samtidig informasjon som skal tilgjengeliggjøres og behandles/fortolkes – gjerne på forskjellige nivåer, i forskjellige (fag)miljøer og i forskjellige nasjoner. Alt dette er med på å øke sårbarheten.

8.3.2 Informasjonskvalitet

Et annet problem med informasjon er informasjonens kvalitet. Kvalitet for hvem og til hvilket formål? Oppgavens fremtid forventer informasjonstilgang uten å garantere forståelse og nyttegjørelse. Dette henger blant annet sammen med grunnleggende forskjeller i bruk og fortolkning av begreper – semantiske sårbarheter[66]. Det er ikke gitt at fremtidig MIL INI vil ha grunnlaget for én kollektiv begrepsforståelse. Det som faktisk skjer er i NATO er en bevist styring mot et lavere ambisjonsnivå (NATO 2008)[67]. Erfaringer fra dagens investeringer i FIF viser at det å inneha en inngående virksomhetsforståelse, herunder ”rett” forståelse av virksomhetens (informasjons)begreper er sentralt[68]. Situasjoner oppleves hvor parter kommuniserer og hvor de involverte mener (og tror) de har samme oppfattelse – samme mentale modeller. Realiteten er at de ikke har det. Dette er utfordringer som øker sårbarheten i forhold til mulig feil bruk og fortolkninger av informasjonsobjekter samt fordyrende løsninger.

I situasjoner hvor det samhandles med sivile (og andre militære) aktører vil denne sårbarheten øke blant annet grunnet forskjellige (stamme/fag)språk. Det er et faktum at individer har tendenser til å kommunisere upresist og tvetydig/flertydig som representerer individuelle sårbarheter som gjør det vanskelig (Danielssen 2005 s. 34). Dette forsterkes når operasjoner bruker samme jobbspråk. Selv om engelsk benyttes i multinasjonale operasjoner er det store kvalitetsforskjeller mellom bruk og fortolkning blant nasjoner som har engelsk som morsmål og i andre nasjoner (Bjørnstad 2005 s. 10). Berglund (2004 s. 13) poengterer dette på en illustrativ måte hvor han uttrykker muligheten av å forstå og prosessere informasjon for å være i stand til å lette Clausew ”fog of War”[69]. Direkte manipulasjon av informasjonsobjekter vil også øke sårbarheten. Bruk av informasjonsobjekter med dårlig kvalitet, eller i verste fall bruk av manipulert informasjon, som grunnlag for beslutninger vil kunne være kritisk (Berglund 2004 s. 16).

---

[66] Med semantikk forstås meningsinnhold (INI 2008).
[67] Etter undertegnedes mening bør det settes krav til en større grad av felles enighet og oppfattelse av forskjellige (operative) virksomhetsbegreper (ontologi, eksakt mening gitt sammenhengen begrepet er brukt (INI 2008) internt i Forsvaret enn hva som vil være mulig i en allianse.
[68] Når det er sagt er det ikke gitt at to individer er omforente om hva som er ”rett” forståelse heller. Igjen spiller ontologien en sentral rolle.

Masterdata management er et sentralt stikkord for å håndtere utfordringer med kollektiv begrepsforståelse. I tillegg er det sentralt ved tettere og tettere system- og tjenesteintegrasjon samt i forbindelse med automatisert dataflyt. Å klart definere hvem som har ansvar for de forskjellige informasjonsobjektene, herunder informasjonsobjektenes syntaks og semantikk er viktig. Igjen representerer FIF forvaltningen noe positivt som nettopp har fokus på masterdata management[70]. Men hva når samhandlingen skjer utenfor de militære kretser. I hvor stor grad vil masterdata management utover det militære domenet sammenfaller med hva som gjøres innenfor andre departementer og/eller opp mot sivile samarbeidspartnere?

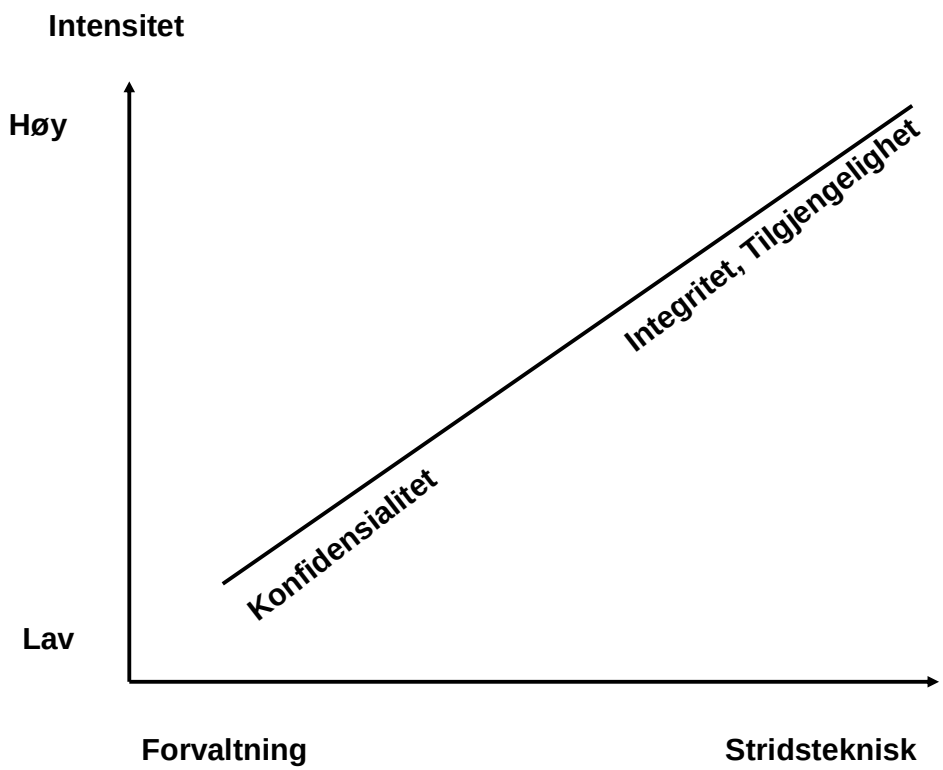
I lys av oppgavens konstruerte trussel vil fiendtlige anslag ved direkte manipulasjon i MIL INI strukturen være en konkret sårbarhet. Direkte påvirkning av sensorer, villedning osv vil gjøre at kvaliteten på informasjonen forringes. På den andre siden er nettopp flere sensorer i nett, med (dels) overlappende "area of responsibilities", en muliggjøring for å etablere en helhetlig situasjonsbevissthet selv om (noen) av sensorene manipuleres. Tross dette er det en sårbarhet i seg selv å fange opp dette. Problemet med insidere er en annen sårbarhet når det gjelder direkte manipulasjon i MIL INI. For eksempel vil den økende bruken av sivil logistikk introdusere en stadig økende gruppe utenfor Forsvaret og/eller den militære operasjonen som får innblikk i styrkenes lokalisering, bevegelser, planer osv (FFI 2008).

Verdivurdering av informasjonen er et annet viktig område. Informasjonen er å betrakte som ferskvare – både i forhold til den direkte verdien/kvalitet, men også i forhold til sårbarheten for at informasjonen kommer på avveie. Sagt på en annen måte vil informasjonens verdi svekkes over tid, herunder graden av sårbarhet. Et paradoks er kanskje at den informasjon som anses å ha kortest levetid er den som gjelder "her og nå" i en operasjon[71]. Mens forvaltningsinformasjon, som sentrale trusselvurderinger, materiellinvesteringer, erfaringsrapporter osv er mer strategisk viktig informasjon? Graderingen av informasjonen vil problematisere dette. Dessuten vil graderingen kunne "gå ut på dato". Vil det å betrakte informasjonssikkerheten i lys av informasjonenes "ferskvareverdi" være en fremtidig løsning – et fremtidig krav? Og hvordan påvirker konfliktens intensitet hvor sårbare vi er ovenfor fiendtlig INFOOPS? Anslag i MIL INI på det tidspunktet konflikten skalerer til høyere nivå (knekkpunktene) kan være mer sårbart enn anslag når en konflikt først har "satt seg" på et intensitetsnivå (NATO 2008; FORV 2008). På

[69] Berglund beskriver Clausewitz "fog of war" som sjefers udekkede informasjonsbehov (Berglund 2004 s. 12).
[70] Masterdata management er en sentralt del av det nye foreslåtte forvaltningsregimet for FIF (INI 2008).
[71] Operasjonelle planer og ivaretakelse av OPSEC er selvsagt sentralt igjennom hele operasjonen i tillegg til etterretningsinformasjon osv. Poenget er av en prinsipiell art.

den andre siden vil kanskje sårbarheten variere i lys av konfliktens/operasjonens intensitet samt hva slags type informasjon det er snakk om, se figur 14.

Figuren søker å vise hvordan sårbarheten varierer (type sårbarhet) som en funksjon av intensitet og informasjonstype (EXP 2008). I situasjoner hvor prinsippet om konfidensialitet må lempes på vil verdivurderinger sees i lys av ”ad hoc” risikovurderinger. Tradisjonelle risikostyringskonsepter som risiko og sårbarhetsanalyser (ROS) har til nå vært benyttet, men dette blir for tungvindt i situasjoner hvor risikovurderinger må gjennomføres raskt (EXP 2008).



Figur 14 – Sårbarhet på informasjonsobjekter som en forenklet funksjon av intensitet og informasjonstype (EXP 2008).

8.3.3 Informasjonsstyring

Fremtidenes MIL INI ser for seg en integrerende informasjonsstyring[72] som sikrer informasjonstilgjengelighet. Det å etablere et slikt informasjonsstyringssystem, som er fleksibelt nok i forhold til å håndtere organisatoriske, teknologiske og prosessuelle/informasjonsmessige endringer, er en stor jobb. Selv om fremtidens konsept legger opp til en sømløs, tilgjengeliggjøring av informasjon, vil det fremtvinge seg løsninger som styrer informasjonsflyten. Løsning en forutsetning for å påse at riktig informasjon tilkommer rette interessenter På den andre siden er informasjonsstyring også et verktøy for å minimere faren for informasjonsmetning.

Hvordan skal Forsvaret og alliansen imøtekomme utfordringene som inntreffer som del av den sømløse informasjonstilgangen? Utforming av en informasjonsstrategi kan være en nøkkel for suksess. En informasjonsstrategi vil synliggjøre sammenhengen mellom virksomhetens overordnede mål, virksomhetens oppgaver & ansvar, kjerneaktivitetene og den rollen som informasjons- og kunnskapsbehandlingen spiller (Kalseth og Knoop 1996:45). Også forskning som er gjort viser nytteverdien av et informasjonsstyrings konsept som håndterer tilflyt av informasjon til beslutningstakere. Erfaringene med en ”information management cell” er funnet positive i forhold til å avlaste kommandogruppen med rett informasjon til rett tid. Dette medførte at kommandogruppen unngikk informasjonsmetning (FOHK 2006 s. 6). Både FD og Forsvarets operative hovedkvarter (FOHK) har i dag enheter for Information Management (IM) under oppbygging (Hyndøy 2008). Sårbarheten er hvorvidt de ressursene som betjener disse funksjonene bare oppfattes å være ressurser med spesiell kunnskap om (utvalgte) informasjonssystemer, herunder generell teknisk kompetanse (Hyndøy 2008). Det som vil være påkrevd vil være tung faglig teoretisk og praktisk kompetanse innenfor fagfeltet informasjonsstyring. Fagmiljøene ved Forsvarets Arkiv avdeling (FAA) og Forsvarets kompetansesenter for kommando kontroll informasjonssystemer (FKKIS) antas å ha mye faglig å bidra med i forbindelse med etablering av et fremtidig informasjonsstyringskonsept[73]. Hvorvidt fremtiden vil påkreve distribuerte IM-celler som vil ha fokus på filtrering av informasjonsflyt vil fremtiden vise.

Et annet moment i forhold til informasjonsstyring er hvorvidt all informasjons skal være tilgjengelig for alle (EXP 2008). Et eksempel er hvordan informasjon (dokumenter) påtegnet

[72] Det engelske begrepet for informasjonsstyring er Information Management (IM). IM som begrep benyttes også i miljøer i Forsvaret. Denne oppgaven vil bruke IM når det er snakk om etablerte (fag)miljøer i Forsvaret.
[73] Til orientering så har P8009 Felles kjernetjenester som del av ressursene under delprosjekt Utvikling en fast representant fra FKKIS (FLO/IKT 2008).

NATO Unclassified åpent distribueres uten i det hele tatt å tenke begrensning av informasjonsflyt. NATO Unclassified er ikke det samme som ”fri flyt” forankret i prinsippet om ”Need to know”. På den andre siden vil fremtiden styre mot prinsippet om ”Need to share”. Men vil det ikke uansett være grader av ”Need to share”, blant annet for å minimere faren for informasjonsmetning? Og vil ikke en ukritisk ”fri flyt” av informasjon, i verst fall på Internett, kunne være en direkte sårbarhet i forhold til insidere, utro tjenere, hackere osv.

MIL INI medfører også nye krav til informasjonsstyring ved at for eksempel (slutt)bruker selv må vurdere (egen) nytteverdi av informasjonen som er tilgjengelig som en del av kvalitetsvurderingen av informasjonen, se kapittel 8.3.2 Informasjonskvalitet. I tillegg må de selv ta ansvar ved registrering/tilgjengeliggjøring av informasjon til andre. Potensielle sårbarheter er knyttet til holdninger og et bevisst forhold til dette. Hvordan ”tagge” graderte informasjonsobjekter for senere å kunne gjenfinne er en annen potensiell sårbarhet/utfordring (FFI 2008)[74].

8.3.4 Delkonklusjon

I lys av prinsippet om tilgjengelighet er det igjennom analysen identifisert en rekke sårbarheter. Økt avhengighet av informasjon som en naturlig del av den daglige (operative) virksomheten gjør at utilgjengelig MIL INI vanskeliggjør situasjonsbevissthet. Denne sårbarheten kan være både av menneskelig og teknisk art. I tillegg er det en sårbarhet med utgangspunkt i en økt deling av informasjon på tvers av (bruker)grupper og nivåer.

En økt informasjonsmengde som en naturlig følge av fremtidig MIL INI øker også sårbarheten i forhold til individuell og organisatorisk informasjonsmetning. I verste fall vil viktig informasjon ”bli borte”. Koordinerte fiendtlige anslag forenlig med fiendtlig INFOOPS vil kunne resultere i en uhåndterlig mengde informasjon som må prosesseres og fortolkes samtidig. Dette vet fienden å utnytte – ikke minst ved bevisst bruk av medienes tilstedeværelse i konfliktdomenet.

Også evne og vilje til informasjonsdeling er en identifisert sårbarhet. Dette forholdet kan forsterkes med rigide og statiske regelverk. I tillegg vil manglende tillit direkte kunne påvirke ønsket (og kravet?) om informasjonsdeling. Også behov for å ta nye typer av terreng vil kunne være direkte konsekvenser av NbF konseptet i fremtiden. Det ligger også et mulig behov for/krav om at NbF konseptet vil påkreve tilgjengelighet på en (nasjonal) kommunikasjonssatellitt. Dette vil kunne gjøre Forsvaret direkte sårbar gjennom fiendtlig ”satellittkapring”. I tillegg vil

[74] Hafnor har skrevet en rapport hvor hun rikt beskriver bruk av metadata og dens potensialer i en fremtidig MIL INI (Hafnor 2006) .

sårbarheten som følger tilgang på en kommunikasjonssatellitt variere avhengig av hva slags ”eierforhold” Forsvaret har til denne.

Prinsippet om integritet kan knyttes til en sentral sårbarhet ved fremtidig MIL INIs manglende evne til å frembringe felles forståelse blant alle aktørene/samarbeidspartnere. Dette forholdet forsterkes jo mer kompleks ”nettverk”/MIL INI blir. Også nasjonalt vil dette kunne inneholde konkrete sårbarheter som må håndteres, for eksempel ved fremtvunget tverrdepartementalt samarbeid uten tilstrekkelig grad av felles forståelse.

Menneskers latente forskjeller ved oppfattelse og fortolkning av informasjon er en sårbarhet som alltid vil være der. Når det i tillegg er slik at en multinasjonal operasjons arbeidsspråk også forringer dette forholdet gir dette økte sårbarheter. Spesielt i situasjoner hvor oppdrag skal forstås og beslutninger skal fattes. Det er store forskjeller mellom innfødte engelsktalende individer/enheter og enheter som har engelsk som andre eventuelt tredje språk.

Informasjonsstyring vil være et fagområde som i fremtiden vil være sentralt. Ved ikke å være i stand til å styre rett informasjon til rett sted på rett tid, vil dette kunne forringe (deler av) militære operasjoner og medføre konkrete sårbarheter – både ved at informasjon ikke er tilgjengelig som påkrevd, men også ved at informasjon kan komme andre i hende og/eller ikke gjenfinnes ved søk. Selv om ”disse andre” er egne ansatte eller ansatte hos tredjepart, er utfordringen med utro tjenere og/eller insidere konkrete sårbarheter.

Problemstillingen med graderte informasjonsobjekter og ”taggingen”/metadatamerkingen av disse kan medføre sårbarheter ved manglende kvalitet og kontroll. I tillegg vil summen av (graderte) informasjonsobjekter være en sårbarhet ved at denne summen samlet vil få høyere graderingsnivå enn de forskjellige (graderte) informasjonsobjektene isolert sett.

En annen sårbarhet er at denne funksjonen ikke forankres skikkelig og at det settes likhetstrekk mellom informasjonsstyring og tradisjonelle ”stabsfunksjoner”. En siste sårbarhet er at den konstante spenningen/fokus på stillingsrammer vil kunne gjøre det vanskelig å argumentere for slike nødvendige fagmiljøer.

8.4 Evne og vilje til beslutning

Tross endringer i væpnede konflikters karakter, samt introduksjon av nye konsepter og våpensystemer, så er de grunnleggende elementene i væpnede konflikters natur alltid til stede. Friksjon, usikkerhet og kaos samt fare og stress er elementer som alltid vil være tilstede og påvirke beslutningstakere (FFOD 2007 s. 75). Hvis i tillegg MIL INI settes ut av spill med den konsekvens at beslutningstakere mister kontroll vil dette kunne berøre evne og viljen til fortsatt kamp, herunder evne og vilje til å ta beslutninger.

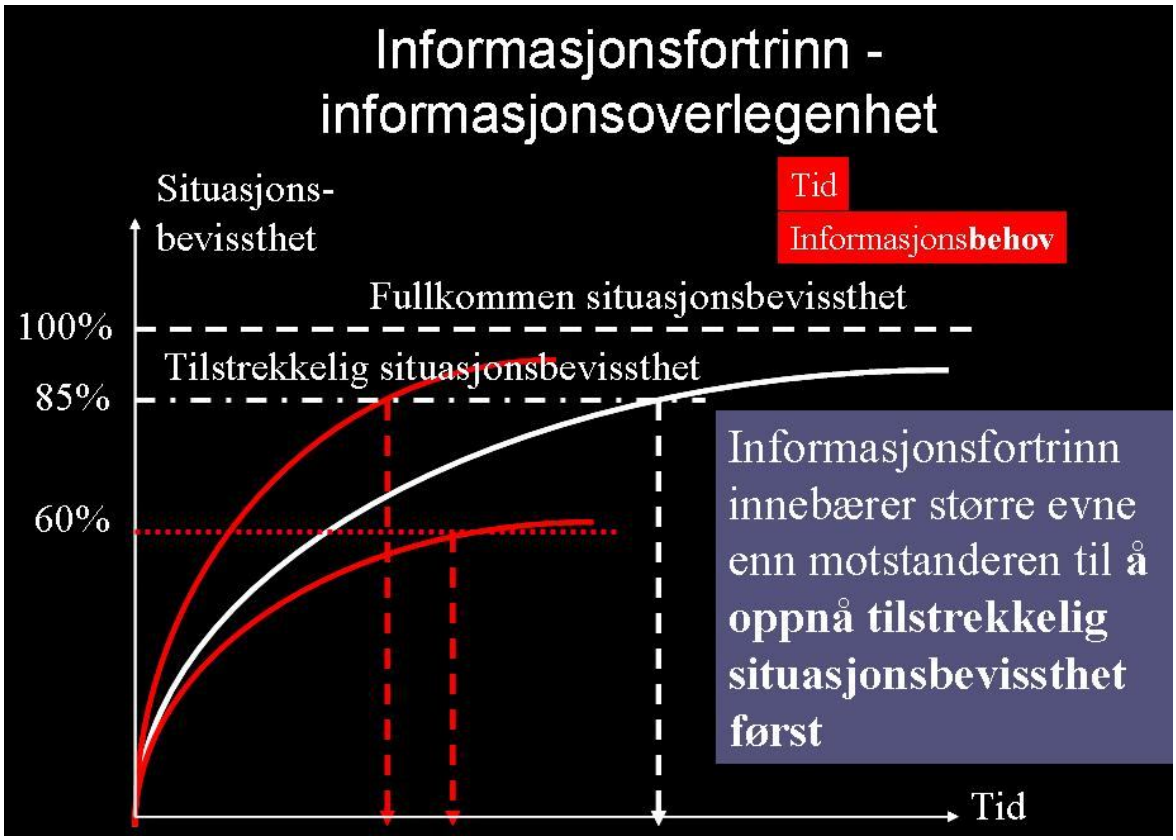
8.4.1 Individuell versus kollektiv situasjonsbevissthet

Den menneskelige hjerne har evne til å oppfatte og bedømme – en evne som langt overskride et hvert system. Samtidig eksisterer det menneskelige begrensninger som må tas hensyn til (FFOD 2007 pkt. 0588). Selv om to individer har tilgang på den samme informasjonen vil nødvendigvis ikke de samme individene oppfatte situasjonen likt. Dette henger sammen med den erfaring, kunnskap, kultur osv som de respektive individene har. I tillegg vil språk og nasjonale kulturelle forskjeller forsterke denne problemstillingen i en multinasjonal operasjon. Dette er alle sårbarheter som Forsvaret må være bevisst og i størst mulig grad håndtere.

Visjonen om den fullkomne situasjonsbevisstheten vil være veldig tidkrevende (og kanskje umulig?) å oppnå. I tillegg vil den kunne variere på individuelt og på kollektivt nivå. Av den grunn må beslutninger fattes på en antatt tilstrekkelig grad av situasjonsbevissthet, se figur 15. En potensiell sårbarhet er å erkjenne når det er opprettet tilstrekkelig grad av situasjonsbevissthet i en gitt situasjon. Forskjellige individer vil ha forskjellige bekvemhetssoner i forhold til dette. Personlighet, personlige egenskaper, erfaring, kunnskap, evne til mønstergjenkjenning er alle faktorer som påvirker dette. I tillegg fremmer komplekse situasjoner i seg selv stress og usikkerhet. Fiendtlig påvirking vil kunne utnytte dette til egen fordel – ikke minst med utgangspunkt i et økt antall potensielle noder[75] å påvirke – både lokalt i konfliktdomenet og ved utstrakt bruk av media for å påvirke verdenssamfunnet.

Ved erkjennelsen av at avvik i opplevd situasjonsbevissthet kan opptre er det av interesse å diskutere tillit. I hvor stor grad vil det være en gjensidig tillit i en konflikt som opprettholder lokal beslutningstaking. Vil denne variere ut i fra konfliktens intensitet? En fare er at den sentrale ledelsen ”overtar” en situasjon. Dette skjer gjerne i situasjoner med stor medie fokus.

[75] Noder i denne sammenheng er sensorer, effektorer, beslutningstakere osv.



Figur 15 - Tilstrekkelig grad av situasjonsbevissthet (Ødegaard 2002)

Det vil også kunne være forskjellige oppfattelser av situasjonsbevisstheten mellom forskjellige (militære) operasjoner som bidrar inn i samme konflikt. Også i forhold til sivile aktører vil nødvendigvis ikke disse ha den samme situasjonsbevisstheten som de militære styrkene. Dette kan for eksempel skyldes forskjellige og/eller ikke koordinerte målsetninger. En viktig avsluttende betraktning er at teknologi aldri vil erstatte mennesker. Et fortsatt viktig fundament for å skape situasjonsbevissthet/-forståelse er personlig møte (FFOD 2007 pkt. 0588).

8.4.2 Desentralisert versus sentralisert situasjonsbevissthet

NbF konseptet åpner for større grad av desentralisert ledelse og horisontal koordinering. Fremtidens MIL INI vil ha informasjonsflyt av sanntidsinformasjon i strukturen, på tvers av operasjonsnivåer og sikkerhetsdomener, gjerne kombinert med grafisk informasjon. Et bilde sier i følge ordtaket mer enn 1000 ord. Men er det nødvendigvis slik. Vil for eksempel det å betrakte en grafisk representasjon av et situasjonsbilde sentralt sikre samme (kollektiv) situasjonsbevissthet lokalt? Krigens iboende natur vil forsterke oppfattelsen av situasjonen lokalt – en forsterkning som ikke nødvendigvis verken er, eller lar seg representere i en MIL INI. På den måten kan det være ubevisste (og/eller) bevisste avvik i oppfattelsen og bevisstheten av

situasjonen lokalt sammenlignet med hva som tilfellet sentralt. I tillegg vil media på sin måte bidra til at (den kollektive) sentrale (situasjons)bevisstheten forsterkes/fortolkes i lys av medias makt. Dette vet fienden å kunne utnytte. Bevisst bruk av media er og blir en sentral del av fiendtlig offensiv INFOOPS.

Samtidig uttrykker NbF konseptet at sentralisert ledelse skal utøves i "strategisk kritiske situasjoner". Hva betyr nå dette? Hvem skal vurdere hvorvidt situasjonen er strategisk kritisk? En sårbarhet ved fremtidens nettverksorganisering er det som gjerne omtales som micromanagement – eller den "stridstekniske minister" for å sitere en medelev. Allerede i dag erfares at den sentrale (politiske) styringen inntreffer "med en gang det brenner" – og langt tidligere enn hva både dagens og morgendagens konsept legger opp til (FOHK 2008)? En årsak til dette kan være at de operasjoner Forsvaret deltar i er så politisk følsomme at den militære tilliten ikke er tilstede av frykt for å skape ubalanse i det politiske liv – både nasjonalt, men også i en internasjonal kontekst. En annen årsak er kanskje at tilliten er der, men at den politiske dimensjonen både ønsker og forventes å være oppdatert når media kommer på banen Dette er sårbarheter som en fiendtlig motpart vet å utnytte til sin fordel – spesielt i den type konflikter som oppgaven adresserer.

På den andre siden er det klart at de konflikter som er forenelig med fremtidens trusler av natur er mer komplekse. Media evige tilstedeværelse og de store vekslingene i konflikters intensitet medfører at taktiske beslutninger i innsatsområdet vil kunne få strategiske konsekvenser. I utgangspunktet er det ikke noe problem med at lavnivå beslutninger kan medføre strategiske konsekvenser hvis den politiske tilliten er tilstede. Sårbarheten inntreffer som følge av at det ikke nødvendigvis er klare skiller/regler for når beslutningen skal fattes desentralisert eller sentralisert og/eller ved at tilliten svekkes ved (menneskelige) feil(beslutninger). Dette igjen vil kreve enda mer fleksible beslutningstakere som i den ene øyeblikket må tilpasse seg/underlegge seg sentralisert ledelse. Ved neste beslutning skjer denne desentralisert.

En militær profesjon med oppdragsbasert ledelse som sin grunnleggende ledelsesfilosofi er et godt utgangspunkt for å gi beslutningstakere mulighet til å handle på den måten de selv anser formålstjenelig innenfor de overordnede rammer/føringer. Sagt på en annen måte er oppdragsbasert ledelse et godt utgangspunkt for de-sentralisert beslutning. På den andre side er det slik at jo flatere, mindre kontrollert struktur, jo større fare for de-fragmenterte subsystemer. Alle subsystemene vil ut i fra subsystemets og individenes erfaringer, kultur, språk og holdninger oppfatte oppdraget på forskjellige måter (FOHK 2008). En annen teoretisk utfordring med mange subsystemer er at disse etter hvert vil kunne suboptimalisere sine beslutninger til eget

beste; den (militære) operasjonen sin helhetlige beste kan vike til fordel for lokalt oppfattet beste. Hvis vi i tillegg til dette også trekker inn krigens iboende natur, hvor fare, stress og kaos er sentrale faktorer, og det faktum at individer har et sterkt overlevelsesinstinkt, vil subsystemer kunne handle langt mer "hardt" enn ønskelig (FOHK 2008). Slike ukontrollerte handlinger blant militære subsystemer kan være direkte sårbarheter i militære operasjoner.

Forskningsprosjektet "Human Factors in NCW" har igjennom sin forskning identifisert funn som er i kontrast til vår tids/dagens litteratur vedrørende organisering av militære operasjoner. På den andre siden er funnene i lys av grunnleggende teori om informasjonsprosessering/-bearbeiding reelle. Oppsummert viser forskningen en viktig overordnet observasjon om at nettverkssentriske organisasjoner nødvendigvis ikke gir noen høyere grad av opplevd situasjonsbevissthet ei heller bedre forståelse av situasjonen. Faktum er at forskningen viste en tendens til det motsatte (Hærem, Myrseth & Bakken 2006:45).

8.4.3 Tillit og avdelingsånd

Samtrening og tillitsbygging er viktig i forhold til å opprettholde operative militære strukturer. Vedvaring av dagens høye rotasjonstakt på militært personell gir utfordringer i forhold til å bygge opp gjensidige tillitsforhold (NOU 2007:15 s. 55-56). En sjef vil være villig til å ta høyere risiko hvis han kjenner sine ressurser og hva de er gode for, enn i situasjoner hvor det ikke er etablert et tillitsforhold og hvor ressursenes kapasitet er ukjent. I de tilfeller hvor de sosiale båndene er sterke, bygget på gjensidig tillit vil et nettverks effektivitet forsterkes. I den type konflikter som oppgaven legger til grunn er dette en styrke som det fiendtlige nettverket har. På den andre siden er dette helt klart et området hvor et sammensatt militært styrkebidrag er sårbare (Arquilla & Ronfeldt 200 s. :xi).

Tillit tar tid og utvikle og er en forutsetning for fremgang i strid (Larsson, Fors & Nilsson. 2006 s. 172). Nødvendig grad av tillit antas i noe forskning å være vanskelig å etablere ved tilfeldig sammensatte konstellasjoner i internasjonale operasjoner (Larsson, Fors & Nilsson. 2006 s. 175). Samtrening er i den forbindelse sentralt og et tiltak for å minimere sårbarhet i lys av tillit. På den andre siden kan nettopp den felles trussel i seg selv gjøre at tillitsutviklingen skjer raskt (Larsson, Fors & Nilsson. 2006 s. 175). To faktorer som påvirker rask utvikling av tillit er ledelsesutvelgelsen og den bakgrunn/det ryktet individet har. Det andre er lederens holdninger og oppførsel ved uforutsette problemer (Larsson, Fors & Nilsson. 2006 s. 173). Begge disse faktorene er potensielle sårbarheter i lys av den tillitsbyggingen som er påkrevd.

Kulturelle forskjeller mellom militære styrker, mellom sivile og militær bidrag samt mellom ulike nasjonaliteter er problematisk og kan være direkte sårbarheter som fienden vet å utnytte.

Mellomledere fra forskjellige nasjoner oppfattes å ha store forskjeller i kompetanse som igjennom etnosentriske oppfattelser kompliserer gjensidig samarbeid (Larsson, Fors & Nilsson. 2006 s. 167).

Forskningen har vist at NbF som konsept påfører beslutningstakere forskjellige og vanskelige krav/forventninger og ett hovedinntrykk er at mange aspekter ved mellommenneskelig interaksjon må håndteres før en nettsentrisk (kommando)struktur gir fordeler i en operasjon (Hærem, Myrseth & Bakken 2006 s. 45). Tvil og usikkerhet skaper mistro/mistillit og representerer et utgangspunkt som ikke er til oppdragets beste og kan være direkte sårbarheter i lys av operasjonens handlinger (Tillberg 2006 s. 78).

8.4.4 Kompetanse

Nettverkskonsepter som NbF vil stille andre krav til ledere og ønsker andre personlighets- og lederegenskaper enn hva som tradisjonelt har vært etterspurt. Viktige egenskaper innenfor NbF konseptet forventes å være evnen til å ta initiativ, tilpasningsdyktighet, risikovillighet og helhetsinnsikt. ”Nettverkskrigeren” bør også ha evne til å fordøye data mentalt og å kunne se sammenhengen i tilgjengelig informasjon. Evnen til å utnytte kunnskapen og erfaringene til å lage eget mentalt bilde av situasjonen er sentralt Og evne til å operere på alle nivå samtidig. For eksempel å kunne identifisere operative og strategiske konsekvenser ut i fra taktiske handlinger er viktig. Likeledes å kunne identifisere de operative og taktiske konsekvensene av det strategiske bildet (Christensen 2003).

De færreste antas å ha alle de påkrevde egenskaper for å håndtere kompleksiteten ved å operere i et nettverk. Enda færre antas å ha lederegenskaper innenfor det NbF konseptet forventer i tillegg. Ønskede kompetanseprofiler er konkrete sårbarheter. Det er ikke gitt at sjefer som er effektive i et hierarkisk kommandosystem er like egnet til å operere i et NbF konsept. Dette vil få strategiske konsekvenser i forhold til utdanning, trening, utvelgelse av fremtidens offiserskorps og ledere. En mulig trøst er at dagens 20-åringer sies å håndtere informasjonsmengder bedre enn nåværende (leder)generasjon. Forsvarets utfordring blir å rekruttere, motivere og beholde slike ressurser noe som også kan betraktes som sårbarheter dersom slike lederprofiler utvikles.

Utgangspunktet for den kultur og handlemåte Forsvaret ønsker å utvikle er nedfelt som en del av det operative grunnlaget i FFOD og er et positivt tiltak for å sikre omforent fellesoperativ basis. For å minimere kulturelle sårbarheter internt i Forsvaret er det viktig at lik filosofien utvikles og benyttes innenfor alle områder av Forsvarets virksomhet. Dette er også viktig mellom forskjellige nasjoners militære styrker for å redusere de kulturelle fagmilitære sårbarhetene i

multinasjonale operasjoner. Bjørnstad (2004 s. 17)omtaler iboende kulturelle forskjeller mellom nasjoner som vil være grunnleggende sårbarheter som må håndteres.

Forskningsprosjektet *"Human Factors in NCW*" har gjort observasjoner som kan synes som om det stilles økte krav til individers informasjonsprosessering ved nettverksorganisering. I tillegg vil det bli økt behov for opplæring og trening i beslutningstaking i nettverksbaserte strukturer slik at beslutningstakingen skal skje mest mulig optimalt (FOHK 2006). Dette bekrefter Løvbuktens uttalelse om at fremtidens Forsvar "…vil være mer krevende og gi lederne **større utfordringer**…" (Løvbukten 2008 s. 96, uthevet i originalteksten). Eksperimentene har dessuten fått bekreftet hvor viktig det er å tidlig iverksette trening av personell i et PTO perspektiv, i rett kontekst, forut for iverksetting av nye konsepter/tilsvarende (FOHK 2006). Uten slike tiltak er dette sårbarheter som vil hemme NbF utviklingen. Et eksempel er at selv om det synes åpenbart at det er en felles enighet om at utenlandsmisjoner innebærer å operere i vanskelige og uforutsigbare omstendigheter så omfatter ikke den militære teoriutdanningen dette. "Erfarenheter och beskrivningar från internationella uppdrag verkar spela en underordnad betydelse i utvecklingen militär yrkespraktik." (Tillberg 2006 s. 83).

8.4.5 Roller og ansvar

En fleksibel rollefordeling på tvers av forsvars- og våpengrener, med fleksibel bruk av sensor-, våpen- og ledelseskomponenter er sentralt i NbF tilnærmingen (MFU 2003 s. 10). En militær struktur med de-sentralisert beslutningstaking vil stille store krav til erkjennelser og bekjennelser av hvilket eksakt ansvar og hvilke roller de enkelte beslutningstakerne har. Investeringer i et vel gjennomtenkt og fleksibelt ansvars- og rolleregime vil også være av stor viktighet blant annet som grunnlag for hensiktsmessig informasjonsstyring. Mangel av dette representerer konkrete sårbarheter (FORV 2008).

Den hierarkiske strukturen Forsvaret har i dag har sin spesielle styrke i form av å være et de-konflikt organ. Intensjonen også i den hierarkiske strukturen er at beslutninger/konflikter skal gjennomføres på så lavt nivå som mulig og at de overliggende nivåene utgjør det nivået som de-konflikter situasjoner når det måtte trenges. I rollen som "forhandlingsledere" vil de kunne de-konflikte slik at styrker på taktisk nivå unngår blue-on-blue situasjoner osv (FOHK 2008). Spesielt hvordan de-konflikt leddet er tenkt i nettverksorganisering er ikke klart. Det synes som om det er lite hensiktsmessig å overlate dette til toppen. Faren er at den sentrale ledelsen i Forsvaret ikke bare de-konflikter i de situasjoner hvor dette er påkrevd, men at de "fristes" til økt aktivt engasjement i operasjonen blant annet grunnet konseptets tilrettelegging for felles situasjonsbevissthet.

En annen observasjon som er gjort av NOBLE er at fast innarbeidet struktur, det vil si gamle handlingsmønstre, preger de operative (nettverksbaserte) prosessene. Sagt på en annen måte så er klare kommandolinjer/handlingsmønstre vesentlig for å drive operasjonen. Dette ble av eksperimentgruppen påpekt at kan ha sammenheng med lite konkret kompetanseheving innenfor NbF som konsept. Eksperimentgruppen har videre konkludert med at "...[m]estring av nettverksorganisering, eller nye arbeidsprosesser krever definering av systemet og roller, og trening/øving i den formen å operere sammen på." (FOHK 2006).

8.4.6 Tempo

Økt tempo i (beslutnings)prosesser er et grunnleggende prinsipp i NbF konseptet. I et desentralisert beslutningssystem vil sjefen hele tiden kunne ta den lokale pulsen ved at hans reelle situasjonsbevissthet øker utover innsikten i et digitalt fellesbilde. Delegering av myndighet til den lokale sjefen reduserer med andre ord tiden det tar å beslutte et engasjement, men da må det også være villighet til å akseptere at det på lavt nivå vil blir gjort feilvurderinger (Gjelsten & Rekkedal 2004). På en annen side vil kanskje økt tempo være det som minst er ønskelig. På den måten vil de muligheter og den informasjonsrikheten som er i fremtidens MIL INI være en direkte sårbarhet i forhold et potensial for "over-raske" beslutninger. I tillegg er det en forventing i verdensopinionen om at militær tilstedeværelse kan vise til konkrete effekter. I den forbindelse er også tidsfaktoren en sårbarhet? På den andre siden er nettopp tidsdimensjonen det som av fienden utnyttes til sin fordel.

En annen sårbarhet som vil kunne påvirke operasjoners tempo er (operasjonelle) begrensninger i Rules of Engagements (ROEs) og/eller nasjonale caveats. I hvor stor grad den naturlig (samfunns)utviklingen medfører at operasjoners basis ROEs justeres mer i tråd med konfliktenes karakter er usikkert. Dagens ROEs har på mange måter svakheter (og kanskje mangler?) for å kunne raskt ivareta situasjoner innenfor "cyber-"/informasjonsdomenet. Et eksempel her er at det ikke i utgangspunktet er lov til å slå ut (sivile) radiostasjoner så fremt de ikke åpenbart brukes til fiendtlige handlinger. Det eksisterer rutiner for hvordan ROEs kan endres og/eller godkjennelse av nye. Dette kan være tidkrevende prosesser. I den grad raske beslutninger er essensielt kan dette være en direkte sårbarhet som kan utnyttes. På den andre siden hvis tempo ikke er viktig er det nødvendigvis ingen hindring. Lovverket har også svakheter (og mangler) i lys av (fiendtlig) INFOOPS aktiviteter (Hollis 2007; FOHK 2008).

8.4.7 Robusthet og teknologi

Gjennomføring av beslutninger med utgangspunkt i beslutnings(støtte)tjenester forutsetter at de etablerte MIL INI tjenestene har en betydelig grad av robusthet, inkludert utholdenhet og redundans. Opprettholdelse av funksjonalitet/tjenester over langt tid, og under betydelige påkjenninger, herunder direkte angrep fra en fiende, er sentralt. Deler av systemet må kunne være operativt selv om andre deler slås ut (FFOD 2007 pkt. 0590). Dette fordrer redundante tjenester og/eller løsninger.

En angriper kan utføre overlagte handlinger for å utnytte en sårbarhet i et system. Resultatet kan være konkrete sikkerhetsbrudd med negative endringer i konfidensialitet, integritet, tilgjengelighet (Thuv et al 2007 s. 21). NSM har nylig sendt ut sikkerhetsvarsel "…om målrettede trojanere i Norge." (Krekling 2008). Som en del av denne varsel er de offentlige institusjoner listet som allerede er utsatt for angrep. Forsvarssektoren er en av disse. Også Statsministerens kontor (SMK) og menneskerettighetsorganisasjoner er forsøkt angrepet (Krekling 2008). Angrepene gjennomføres ved bruk av individers e-postadresser og fremsende e-post fra kilder som tilsynelatende er anerkjente kilder (Krekling 2008). Dagens relativt enkle måte å "hacke" en persons e-postadresse kan slik sett sees på som en klar sårbarhet ovenfor logiske dataangrep[76].

Så lenge tilliten og tilgjengeligheten til MIL INI er tilstede går operasjoner sin gang. Men, fra det tidspunktet at tilliten til MIL INI svekkes for eksempel ved ikke tilgjengelige tjenester, vil lokale beslutningstakere kunne etablere egne (lokale) løsninger dersom den militære virksomheten sentralt ikke selv har alternative løsninger. Slike lokale initiativ/tiltak har en tendens til å "slå rot" og det vil være et stor oppgave å gjenoppbygge den tapte tilliten slik at primærløsningen igjen benyttes etter intensjonen.

Et annet tillitsmoment er gjenoppbygging etter et fiendtlig angrep mot MIL INI. Når friskmelde INI etter angrep? Hvordan vite at ikke andre deler av strukturen er angrepet? FSA har også begynt å se på metoder for å håndtere restrisiko som også er et stort satsningsområde i NATO (EXP 2008). På den andre siden vil det kunne praktisere kildekritikk i innholdet i MIL INI i lys av hvordan vi utøver (bør utøve) kildekritikk på Internett i dag (EXP 2008). Over tid vil forskjellige kilder læres å kjenne, herunder mønstergjenkjenning av (fiendtlige) aktiviteter og hendelser, men også i forhold til egen informasjon. For eksempel opparbeides kunnskap om

[76] Ved tilgang på navn og arbeidssted kommer du ofte langt i forhold til å identifisere e-postadresser.

normale etterforsyningsdata over tid, som gjør at avvik fra kjente mønstre vil kunne oppfattes. Problemet kan være at informasjonen nødvendigvis ikke kommer fra ”den kjente kilden” (EXP 2008).

Ved at (deler av) MIL INI ikke er tilgjengelig når beslutninger skal fattes åpner NbF konseptet for selvstendig og innovativ tenkning. Selvstendig og innovativ tenkning varierer med hvilke individer som fungerer i hvilke roller. Igjen er det egenskaper, kompetanse og erfaring som påvirker. Hvor vidt innovativ tenkning betyr at beslutningstakeren benytter alternative tjenester han ”har for hånden” er vanskelig å predikere, men konseptet kan legge til rette for det. På den andre siden er det ikke sikkert at alternative og tilgjengelige komponenter verken er sikkerhetsmessig godkjent og/eller interoperable. Dette er potensielle sårbarheter i anvendelsen av MIL INI. Hvorvidt slike komponenter likevel benyttes avhenger av sentral ledelse og/eller individers risikovillighet, som kanskje avviker. Konfliktens intensitetsnivå på beslutningstidspunktet og type beslutning påvirker også. ”Har du ikke tilstrekkelig K2, bruker du det du har for hånden for eksempel sivile tjenester.” (EXP 2008). Kanskje blir man nødt for å akseptere at dette skjer på taktisk nivå? Og kanskje er det ok? Uansett hva slags redundante løsninger/tjenester som vil være tilgjengelig så er svakheter i MIL INI sin robusthet en fremtidig sårbarhet[77].

Forsvarets IKT policy gir som omtalt i forrige analysekapitel føringer rundt bruk av standardiserte og kommersielle systemer og løsninger. Grunnleggende svakheter i slike systemer er i utgangspunktet direkte sikkerhetsrisikoer (EXP 2008). På den andre siden vil denne risikoen begrense seg all den tid de militære løsningene er på lukkede nettverk. Utfordringen i fremtidens MIL INI er hvorvidt det er mulig å sikre og skjerme MIL INI på samme måte som i dag. Den utstrakte samhandlingen med sivile og andre allierte øker sårbarheten. I tillegg har en nasjon ingen (overordnet) kontroll over utstrekningen til en annen alliert (og/eller sivil samarbeidspartner) sin MIL INI. På FISBasis i dag opereres det ofte i gråsoner for eksempel ved bruk av minnepinner for datautveksling mellom nett og/eller sikkerhetsdomener. Slik bruk av ”frittstående informasjonsutvekslingsmedier” er potensielle sårbarheter.

Generell beskyttelse mot alle former for uautorisert bruk og/eller misbruk er viktig. ”Human beings are the weakest link in the security mechanisms of any system.” (Bishop 2003 s. 3).

Deployerbar MIL INI vil være avhengig av et konfliktdomenes geografi og fysiske omgivelser. Dette kan være mer sårbart enn for eksempel båndbredde. På den andre siden er det opplagt at

båndbredde, strømforsyning og overføringshastigheter er områder som i dag er sårbare i lys av de informasjonsintensive løsningene/tjenestene som eksisterer. Noen miljøer hevder at fremtidig NbF og fortsatt norsk deltagelse i internasjonale operasjoner vil kreve nasjonal kontroll på (norsk) kommunikasjonssatellitt og at denne vil være "ryggsøylen" i MIL INI (EXP 2008; NBF 2007 s. 13). På den andre siden er kanskje dette "…behovet scenarioavhengig – nasjonalt mindre viktig, men mye større i for eksempel Afrika." (EXP 2008).

8.4.8 Delkonklusjon

Selv om den menneskelige hjerne har unike evner til å oppfatte og gjøre bedømmelser så er dette ingen garanti for at to eller flere individer oppfatter og bedømmer samme situasjon likt. Kulturelle forskjeller og språk er faktorer som forsterker dette. Avvik mellom individuell og kollektiv situasjonsbevissthet vil kunne være konkrete sårbarheter i forhold til faktisk å evne og etablere felles situasjonsbevissthet. Forskjellige oppfatninger vil ytterligere kunne medføre forskjellige tiltak – som kanskje også divergerer og/eller medfører konkrete "konfliktsituasjoner".

Det er en erkjennelse av at den fullkomne situasjonsbevisstheten ikke lar seg imøtekomme. Individuelle forskjeller om hva som er tilstrekkelig grad av situasjonsbevissthet vil kunne medføre usikkerhet og Forsvaret kan oppleve varierende prosedyrer og rutiner i sine operasjoner. Konflikters iboende natur vil forsterke denne sårbarheten. Fiendtlig bevisst bruk av media vil også vanskeliggjøre det å etablere kollektiv situasjonsbevissthet på alle de operasjonelle nivåene, inkludert den oppfattelsen nasjonale borgere opparbeider seg.

Tillit er et sentralt moment ved erkjennelsen av at avvik mellom individuell og kollektiv situasjonsbevissthet kan inntreffe. I hvor stor grad det vil være en gjensidig tillit også i situasjoner hvor det er kompliserte beslutninger som skal fattes kan diskuteres. Avvik mellom desentraliserte og sentrale nivåer vil være en enda mer kompliserende faktor. En potensiell sårbarhet er at ledelsen "tar over" i langt større grad enn konseptet legger opp til. Igjen forsterkes denne sårbarheten av medienes evige tilstedeværelse i konfliktdomenet. På den andre siden er det lokalt at "den rette" pulsen på situasjonen oppleves.

En annen sårbarhet ved desentralisert situasjonsbevissthet er at etablerte subsystemer over tid kan begynne å opptre irrasjonelt sett med andre/sentralt nivå sitt syn. Subsystemer kan etter hvert velge suboptimale løsninger helhetlig sett. Kombinert med konflikters iboende natur vil

[77] Det er også viktig å presisere at redundans også er sentralt i forhold til generell slitasje og andre påkjenninger. Nok ressurser (materiell og pax) er et stikkord. I tillegg til økonomi.

desentraliserte fattede beslutninger kunne være ”langt hardere” enn ønskelig – i det minste fra et politisk/militærstrategisk synspunkt.

I hvor stor grad en sjef/beslutningstager er villig til å ta høy risiko avhenger av den gjensidige tilliten det er mellom ham og hans medarbeidere. Høy rotasjonstakt på militært personell gjør det vanskelig med langvarig tillitsbygging. Dette bøtes på ved mange anledninger med samtrening i forkant av operasjoner, men det er ikke mulig å opparbeide dype tillitsrelasjoner i løpet av samtreningstiden, selv om det selvsagt er bedre enn ingenting.

Nye konsepter som NbF, med tilhørende MIL INI, vil også kreve annen kompetanse for lederne enn det som kreves i dag. Det er konkrete sårbarheter hvis Forsvaret ikke lykkes med å utvikle kompetansesystemene til å ivareta fremtidens behov forut for at denne fremtiden inntreffer. Andre sårbarheter i lys av kompetanse er manglende evne til å fordøye informasjonsmengden mentalt og (egen) evne til å se sammenhenger i informasjonsbildet. Også manglende evne til å se konsekvenser på tvers av (operasjonelle) nivåer vil kunne være direkte sårbarheter – og sårbarheter som fienden vet å utnytte. Det er å anta at fienden er kjent ved den sterke norske politiske bindingen mot Forsvaret.

Hvis ikke aktørene i en fremtidig MIL INI har tilgjengelig et veletablert rolle og ansvarskonsept vil dette være sårbarheter for eksempel ved behov for dekonflikting. Forskning viser også at det er lett å ”jobbe som før” ved at etablerte handlingsmønstre benyttes fremfor å ta i bruk nye prinsipper.

I den type konflikter som oppgaven legger til grunn er det en konkret sårbarhet med for raske beslutninger. Tid er en faktor som irregulære styrker vet å utnytte ved at deres horisonter gjerne går over generasjoner (”våre barnebarns barn”). Tidsdimensjonen er også en sårbarhet for (militære) operasjoner ved at verdenssamfunnet forventer å se løpende resultater – nesten før tiltak er iverksatt. Dette som en form for legitimering av (militær) tilstedeværelse.

Operasjonelle ROEs og/eller nasjonale caveats vil også være konkrete sårbarheter i forhold til (operasjonelt) tempo. Det er å håpe at det fremover skjer en utvikling i forhold til praksis ved at for eksempel en operasjons ROEs i større grad enn i dag legger til rette for økt militær aktivitet i informasjonsdomenet.

Å opprettholde MIL INI tjenester over tid vil kunne kreve redundans i tjenster/løsninger. På den andre siden vil det uansett grad av redundans være sårbarheter. For eksempel er det relativt enkelt i dag å ”gjette seg til” en persons emailadresse så lenge navn og arbeidsgiver er kjent. Det

er også konkrete økninger i målrettende aktiviteter i informasjonsdomenet mot norske sentrale miljøer/organisasjoner.

Så lenge tilliten til MIL INI er tilstede blant annet som følge av dens tilgjengelighet er alt såre vel. Når denne tilliten utfordres vil lokale initiativ påtvinge seg. Når slike initiativ først har ”satt seg” skal det mye til å gjenoppbygge tiliten til MIL INI. I tillegg er det en konkret sårbarhet at lokale (påkrevde) initiativ nødvendigvis ikke tilfredsstiller all påkrevd ”formalia” for eksempel godkjente sikkerhetsløsninger.

Sentrale føringer rundt bruk av standardiserte og kommersielle systemer gjør også Forsvaret sårbart ved grunnleggende svakheter/sårbarheter i disse systemene. Noen fagmiljøer trekker også frem en fremtidig sårbarhet ved mangel på tilgang til (nasjonal) kommunikasjonssatellitt og/eller ved at tilgangen er der, men sårbarheten er i forhold til potensiell kapring av satellitt og/eller sårbarhet ovenfor insidere og utro tjenere. Det er et godt prinsipp å avslutte med at den menneskelige faktor alltid vil være det svakeste leddet i ethvert sikkerhetssystem.

9 Konklusjon

Denne masteroppgaven har hatt som formål å identifisere og analysere sentrale sårbarheter i transformasjonen mot en fremtidig MIL INI, forenelig med egenskapene til NbF grad 2, integrerende NbF. Videre har oppgaven bestått i å analysere sentrale sårbarheter i beslutningstakeres avhengighet og anvendelse av MIL INI gitt en fremtidig konstruert konflikt. Denne todelingen av oppgaven samsvarer med oppgavens to overordnede problemstillinger. Disse problemstilingene er forankret i de to ledelsesdimensjonene som de strategiske ledelsen av Forsvaret har som grunnprinsipp – fremskaffe og anvende.

I forbindelse med den første problemstillingen har jeg valgt å fokusere på analyse av selve den fremtidige oppbyggingen av MIL INI. Denne faktoren er igjennom analysen operasjonalisert til en rekke utledede analysefaktorer. Innenfor hver og en av disse er sentrale sårbarheter analysert og diskutert.

Oppgavens andre problemstilling har tatt utgangspunkt i to faktorer, situasjonsbevissthet samt evne og vilje til beslutning. Samlet påvirker disse tre elementene en beslutningstakers effektivitet som igjen vil kunne påvirke selve operasjonen.

Igjennom oppgavens gjennomførte analyser er det identifisert en rekke sentrale sårbarheter. Disse er oppsummert i sine respektive kapitler gjennom separate delkonklusjoner. Vedlegg C og D presenterer analysens samlede hovedfunn på en lettfattet form.

Jeg har sett at fremtides sårbarheter vil være påvirket av hvilke beslutninger og tiltak vi gjør i dag. Av den grunn anses det viktig å avstemme oppgavens hovedfunn med planlagte og/eller iverksatte NbF og MIL INI initiativ. Dette for på en best mulig måte å imøtekomme den løpende utvikling herunder mulighet for å redusere virkningen av flere av de identifiserte sårbarhetene. På grunnlag av dette er det naturlig å anta at oppgavens hovedfunn vil kunne ha reell nytteverdi.

Det er imidlertid viktig å huske at hovedfunnene er gjennomført med begrenset datainnsamling, både i forhold til analysen fremtidsvurdering og benyttet reell tid.

Et annet viktig moment er det som innledningsvis er omtalt som en analysemessig svakhet ved at oppgaven benytter en romslig definisjon av begrepet sårbarhet. Dette er med på å komplisere skillet mellom konkrete sårbarheter og forhold som kan føre til konkrete sårbarheter.

I gjennom denne oppgaven er følgende områder identifisert som mulige for videre forskning:

- Det vil være interessant å gjennomføre mer detaljerte sårbarhetsbetraktninger basert på mer omfattende datainnsamling, gjerne i relasjon til formalisert ”fremtidsforskning”.
- Det vil også være av interesse å gjennomføre mer formaliserte sårbarhets- og risikoanalyser for (deler av) oppgavens tematikk.
- Ytterligere vil det være interessant å analyser sentrale sårbarheter i lys av forskjellige typer scenarioer, herunder militære operasjoner i en større sikkerhetspolitisk sammenheng.

Vedlegg A – Kildeliste

AJP-3.10. (2008). Pre-Ratification Draft: *Allied Joint Doctrine for Information Operations*. Brüssel, NATO Stadardisation Agency.

AJP-3.10. (u.å.). 4th Study Draft: *Allied Joint Doctrine for Information Operations*. Brüssel, NATO Stadardisation Agency.

AJP-3.10.1(A). (2007). *Allied Joint Doctrine for Psychological Operations*. Brüssel, NATO Stadardisation Agency.

Alberts, D.S., Garstka, J.J., Hayes, R.E. & Signori, D.A. (2001). *Understanding information age warefare (2nd Ed)*. USA, The Command and Control Research Program (CCRP Publiction Series). (Lokalisert på World Wide Web: http://www.dodccrp.org/html4/contact.html).

Alberts, D.S., Garstka, J.J. & Stein, F. (2000). *Network Centric Warefare – Developing and Leveraging Information Superiority (2nd Ed)*. USA, The Command and Control Research Program (CCRP Publiction Series). (lokalisert på World Wide Web: http://www.dodccrp.org/html4/contact.html).

Arquilla, J. & Ronfeldt, D. (2001). *Networks and Netwars*. USA, RAND

Asian Economic News. (Publisert 21. mars 2005) Asia, Hong Kong. Lokalisert 23.. mai 2008 på World Wide Web: http://findarticles.com/p/articles/mi_m0WDP/is_2005_March_21/ai_n13458208.

Bakken, B.E. (u.å.). *Undervisningsmatr BI: Sesjon 6, Scenarioanalyse*. Oslo, Handelseshøyskolen BI. (Lokalisert 4. april 2008 på World Wide Web: http://www.bi.no/users/fgl95002/sivoksesjon6.ppt).

Berglund, J. (2004). Thesis Master of Science in Defense analysis: NETWORK CENTRIC WARFARE: A REALISTIC DEFENSE ALTERNATIVE FOR SMALLER NATIONS?. Monterey, California, Naval Postgraduate School.

Bishop, M. (2003). *Computer Security – Art and Science*. USA, Addison-Wesley, Pearson Education Inc.

Bjørnstad, A.L. (2005). *Part I: Allied Warrios 2004 – Pilot study and analysis of cross-cultural organizational issues*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2005/01709).

Bjørnstad, A.L. (2004). *NCW IN THEORY AND PRACTICE: A human factors perspectives on why it might work and why we might not get there*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2004/02106).

BST (2008). *Diverse presentasjoner gjennomført ved FLO/IKT BST sitt fagseminar 23. april 2008*. Kolsås, Forsvarets Logistikkorganisajson/IKT.

Christensen, J.I. (2003). Utfordringer/implikasjoner med Nettverksbasert Forsvaret. Norsk Militært Tidsskrift, 173(4), s. 25-29.

Danielssen, T. (2005). *Hovedoppgave: Data- og Informasjonsfusjon*. Trondheim, Luftkrigsskolen (KS II/II Kull 54).

Denning, D.E. (2001). Activism, Hacktivism, and Cyberterrorism: The Internet as a tool for influencing foreign policy. I: Arquilla, J. & Ronfeldt, D. *Networks and Netwar*. USA, RAND.

Diesen, S. (2003). Forsvarets konsept for nettverkssentrisk krigføring. *Norsk Militært Tidsskrift, 173*(5), s. 4-13.

Enemo, G. (2006). *NBF tenketank: Resultater pr april 2006*. Kjeller, Forsvarets forskningsinstitutt (FFI/NOTAT-2006/01225).

Estonia under cyberattack: The first electronic war. (29. mai 2007). Lokalisert 7. april 2008 på World Wide Wed: http://www.lunchoverip.com/2007/05/estonia_under_c.html.

FD (2007). *Den strategiske ledelsen av Forsvaret: Organisering, roller og ansvar FD - FST*. Oslo, Forsvarsdepartementet.

FD (2004). *Styrke og Relevans: Strategisk konsept for Forsvaret*. Oslo, Forsvarsdepartementet.

FST (2004). *Logistikk- og støttekonseptet for Forsvaret*. Oslo, Forsvarsstaben.

FFOD (2007). *Forsvarets Fellesoperative doktrine*. Oslo, Forsvarsstaben.

FOHK (2006)[78]. *Eksperimentrapport Mennesket i NbF: Et samarbeid mellom NOBLE og Forsvarets institutt for ledelse*. Stavanger, Fellesoperativt hovedkvarter – Konseptutvikling og eksperimentering.

[78] Eksperimentrapporten er ikke datert, men det fortolkes at denne eksperimentrapporten (norsk kortutgave) er skrevet i forbindelse med hovedrapporten til Hærem, Myrseth, & Bakken *Research Project: Human Aspects of Decision Making in Network Centric Systems.*

[Informasjonssikkerhet (2001)]. *Forskrift av 1. juli 2001 (FOR 2001-07-01 nr. 744) om Informasjonssikkerhet*. Oslo, Forsvarsdepartementet. (Lokalisert 19. mai 2008 på World Wide Web: http://www.lovdata.no/all/nl-19980320-010.html).

Fridheim, H., Hagen, J. & Henriksen, S. (2001). *EN SÅRBAR KRAFTFORSYNING – Sluttrapport etter BAS3*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2001/02381).

Gagnes, T., Eggen, A., Hedenstad, O.E., Rasmussen, R. & Sletten, G. (2005). *Operative beslutningsstøttetjenester – fremtid NBF*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2005/03584).

Gjelsten, R. & Rekkedal, N.M. (2004). Et nettverksbasert forsvar – noen refleksjoner. Norsk Militært Tidsskrift, 174(10), s. 14-21.

God sikkerhet og skjerming av sensitiv informasjon forebygger etterretning og sabotasje. (Publisert 22. februar 2008). Kolsås, Nasjonal Sikkerhetsmyndighet. Lokalisert 29. februar 2008 på World Wide Web: http://www.nsm.stat.no/Aktuelt/Nytt-fra-NSM/Forebyggende-arbeid/.

Hafnor, H. (2006). *INI som nettsentrisk virksomhetsomgivelse – bruk av "enterprise metadata" og "communities o finterest" (COIs)*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2006/00862).

Hafnor, H. (2004). *Aktør-Nettverk teori som teoretisk rammeverk og praktisk verktøy for å analysere informasjonsinfrastrukturer i et NbF*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2004/00223).

Hafnor, H., Enemo, G., Bjørnstad, A.L. & Reitan B. (2006). *Sluttrapport for prosjekt 879 NBF i operasjoner*. Kjeller: Forsvarets forskningsinstitutt (FFI/RAPPORT-2006/03966).

Hanseth, O. & Lyytinen, K. (u.å.). Theorizing about the design of Information Infrastructures: design kernel theories and principles. (Lokalisert 19. mai 2008 på World Wide Web: http://heim.ifi.uio.no/~oleha/Publications/ISRinfrastructurefinal05-12-05.pdf).

Hanseth, O. & Monteiro, E. (1998). Understanding Information Infrastructures. Lokalisert 11. mars 2008 på World Wide Web: http://heim.ifi.uio.no/~oleha/Publications/bok.html.

Hedenstad, O.E. (2002). *Informasjonsstrukturer i NbF*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2002/03973).

Hennum, A.C. & Glærum, S. (2007). *Metode for langtidsplanlegging – støtte til FS 07*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2007/02174).

Hollis, D.B. (2007). Why states need an international law for information operations. *Lewis & Clark Law Review*, 11(4), s. 1023-1061. (Lokalisert 18. april 2008 på Worl Wide Web: http://www.lclark.edu/org/lclr/objects/LCB_11_4_Art7_Hollis.pdf).

Hyndøy, J.I. (2008). *Felles Situasjonsbevissthet i norske hovedkvarter*. Oslo, Forsvarets Stabsskole

Hærem, T., Myrseth, H.P. & Bakken, B. (2006). *Research Project: Human Aspects of Decision Making in Network Centric Systems*. Norway, Norwegian Defence Leadership Institute, Norwegian School of Management & Norwegian Battle Lab & Experimentation.

IKT (2005). *Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i Forsvaret*. Oslo, Forsvarsdepartementet. (Lokalisert 29. februar 2008 på World Wide Web: http://www.regjeringen.no/upload/FD/Reglement/Policy_militaer_tilpasning_IKT_2oppl.pdf).

INI (2007). *Beskrivelse av programområde informasjonsinfrastruktur: Plan for perioden 2006-2009+*. Oslo, Forsvarsdepertementet. (Lokalisert 29. februar 2008 på World Wide Web: http://www.regjeringen.no/upload/FD/Reglement/Programomraade_informasjonsinfrastruktur.pdf).

Jacobsen, D.I. (2005). *Hvordan gjennomføre undersøkelser?: Innføring i samfunnsvitenskaplig metode*. Kristiansand, Høyskoleforlaget.

Johansen, I. (2006). *Scenarioklasser i Forsvarsstudie 2007: En morfologisk analyse av sikkerhetspolitiske utfordringer mot Norge*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2006/02664).

JP-3.13. (1998). *Joint Doctrine for Information Operations*. USA, Joint Chiefs of Staff.

Jørstad, N.P. (2007). *INFORMASJONSOPERASJONER: Orientering Psyopskurs 19 nov 07*. Oslo, Forsvarets Stabsskole.

Kalseth, K. & Knoop, A.T. (1996). *Dokumentbehandling*. Bærum, NKI Forlaget.

Kuehl, Dan. (u.å.). *Information Operations: The Hard Reality of Soft Power*. Storbritannia, Information Resources Management College, National defense University.

Krekling, D.V. (15. mai 2008). *Virusalarm hos Jens og Kristin*. Oslo, Nettavisen. Lokalisert 15. mai 2008 på World Wide Web: http://www.nettavisen.no/it/article1835884.ece.

Larsson, G., Fors M. & Nilsson, S. (2006). Ledarskap och tillit. Analys och värdering av befintlig forskning ur ett Nordic Battle Group perspektiv. I: Berggren, A.W. (red), *Människan i NBF: Med ökad internationell förmåga i fokus*. Stockholm, Försvarshögskolan

Lowe, C. (30. august 2006). *Israel wants to jam sats*. Military.com. DefenseTech.org. Lokalisert 23. mai 2008 på World Wide Web: http://www.defensetech.org/archives/002717.html.

Løvbukten, A. (2008). Fremtiden krever mer av Forsvarets leder. *Forsvarets Forum*, *2008*(1-2), s. 96-97.

Løvland, T. (2008). Fant gradert informasjon på Facebook. *Forsvarets forum, 2008*(5), s. 10-11.

MC 422/3. (2007). *Military Decision on MC 422/3: NATO military policy on Information Operations*. North Atlantic Treaty Organisation.

MFU. (2003). *Forsvarssjefens militærfaglige utredning 2003: Konsept for nettverksbasert anvendelse av militærmakt – Grunnlag*. Oslo, Forsvarsstaben. (Lokalisert 11. mars 2008 på World Wide Web: http://www.mil.no/multimedia/archive/00016/Konsept_for_nettverk_16358a.pdf).

MFU. (2003a). *Forsvarssjefens militærfaglige utredning 2003: Militære informasjonsoperasjoner (MIL INFO OPS)*. Oslo, Forsvarsstaben. (Lokalisert 28. mars 2008 på World Wide Web: http://www.mil.no/multimedia/archive/00027/Milit_re_informasjon_27745a.pdf).

NBF (2007). *Grunnlagsdokument for Forsvarssjefens anbefaling om utviklingen av nettverksbasert forsvar. Sluttrapport NbF kjernegruppe, Forsvarsstudie 07*. Oslo, FS07.

Nesse, L. (2006). *MAJIIC: Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition*. NATO, NC3A. Lokalisert 20. mai 2008 på World Wide Web: http://www.nato.int/docu/update/2007/pdt/majic.pdt.

NNEC FS. (2005). *NATO Network Enabled Capability Feasibility Study: Executive Summary version 2.0*. North Atlantic Treaty Organisation, NATO Consultation, Command and Control Agency.

NNEC: Utviklingen i NATO. (u.d.) Oslo, Fellesstaben. Lokalisert 27. februar 2008 på Forsvarets intranettsider (FISBasis Begrenset): http://intranett.mil.no/fst/fellesstaben/start/article.jhtml?articleID=731647.

NORCCIS brosjyre. (u.d.) Lysaker, Teleplan. Lokalisert 14. mai 2008 på World Wide Web: http://www.teleplan.no/download/norccis/NORCCIS_Brochures.pdf.

NOU 2007:15, dvs.: *Et styrket forsvar*. Oslo: Departementenes servicesenter.

NSM (2008). *Nettsamfunn og sikkerhet*: *Temahefte 1/2008*. Kolsås, Nasjonal Sikkerhetsmyndighet. (Lokalisert 14. mai 2008 på World Wide Web: http://www.nsm.stat.no/Publikasjoner/).

Olafsen, R. & Bråthen, K. (2004). *Beslutningstaking i nettverksbasert forsvar – Kognitive perspektiver*. Kjeller, Forsvarets forskningsinstitutt (FFI/NOTAT-2004/00814).

Proxy. (u.d.) Wikipedia, Wiktionary. Lokalisert 25. mai 2008 på World Wide Web: http://en.wiktionary.org/wiki/proxy.

Reitan, B.& Pålhaugen, L. (2004). *Forventningene til nettverksbasert forsvare – 6 tema*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2004/04004).

SAS-057. (2006). Information Operations: Analysis Support and Capability Requirements. North Atlantic Treaty Organisation, Research and Technology organisation (RTO Technical Report). (Lokalisert 7. November 2007 på World Wide Web: http://www.rta.nato.int/).

[Sikkerhetsloven. (1998)]. Lov av 1. juli 2001 (LOV-1998-03-20-10) *om forebyggende sikkerhetstjeneste*. Oslo: Forsvarsdepartementet. (Lokalisert 19. mai 2008 på World Wide Web: http://www.lovdata.no/all/nl-19980320-010.html).

Stabell, C.B. & Fjeldstad, Ø.D. (1998). Configuring value for competitive advantages: on chains, shops, and networks. *Strategic Management Journal, 1998*(19), s 413-437. (Lokalisert 6. mars 2008 på World Wide Wed: http://www.agbuscenter.ifas.ufl.edu/5188/miscellaneous/configuring_value.pdf).

St.prp. nr. 42. (2003-2004), dvs.: Forsvarsdepartementet. (2004). *Den videre moderniseringen av Forsvaret i perioden 2005-2008*. Oslo: Departementet.

Strømsod, L.C. (1. oktober 2003). Strengthened capabilities in new systems. Oslo, Programme Jupiter. Lokalisert 14. mai 2008 på World Wide Web: http://www.mil.no/languages/english/start/article.jhtml?articleID=57642.

Sundfør, H.O. (2006). *Samhandlingskonsept for operasjoner: Et mulig konsept og eksperimentskisser*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2006/03308).

Thuv, A., Windvik, R., Nystuen, K.O. & Sivertsen, T. (2007). *Sårbarheter i Internett*. Kjeller, Forsvarets forskningsinstitutt (FFI/RAPPORT-2007/00903).

Tillberg, P. (2006). Om militärt yrkeskunnande i intertaionella uppdrag – en kunnskapsöversikt. I: Berggren, A.W. (red), *Människan i NBF: Med ökad internationell förmåga i fokus*. Stockholm, Försvarshögskolan.

Tzu, Sun (u.d.). *Utvalgte Sun Tzu sitater*. Brainyquote.com. Lokalisert 23. mai 2008 på World Wide Web: http://www.brainyquote.com/quotes/authors/s/sun_tzu.html.

Utfordringer i nettsamfunn. (7. mai 2008) Kolsås, Nasjonal Sikkerhetsmyndighet. Lokalisert 14. mai 2008 på Forsvarets intranettsider (FISBasis Begrenset): http://intranett.mil.no/start/article.jhtml?articleID=750906.

Watne, M. & Knutsen, M. (23 april 2008). Alle gode ting er tre. Oslo, Forsvarets mediesenter. Lokalisert 28. april 2008 på World Wide Web: http://www.mil.no/start/article.jhtml?articleID=160679.

Zanini, M. & Edwards, S.J.A. (2001). The networking of terror in the information age. I: Arquilla, J. & Ronfeldt, D. *Networks and Netwar*. USA, RAND.

Ødegård, J.C. (2002). *Presentasjon av NbF konseptet* (filnavn: NBF-konspekt[79] 130902). Rygge, Luftforsvarets Utviklings- og Kompetansesenter. Lokalisert 15. mai 2008 på Forsvarets intranettsider (FISBasis Begrenset): http://www.luft.mil.no/luks/start/aktuelt/nbf/briefer.

Muntlige kilder

Bakken, Bent Erik (Professor / Bi-veileder) – Forsvarets Skolesenter (FSS)

Bakken, Bjørn (Forsker) – Forsvarets Skolesenter (FSS)

Bolæren-Hansen, Egil (Komkapt) – Forsvarsdepartementet (FD)

EXP 2008. *Seminar med nedsatt ekspertgruppe 10. april 2008.*

- Botnan, Jørgen (Oing) – Nasjonal Sikkerhetsmyndighet (NSM)
- Eriksson, L. Magnus (Maj) – Forsvarets Stabsskole (FSTS)

[79] Det er denne skrivefeilen i linken på nettlokasjonen.

- Nygård, Jørund (NK / Oblt) – Forsvarets sikkerhetsavdeling (FSA)
- Nystuen, Kjell-Olav (Forsker) – Forsvarets forskningsinstitutt (FFI)
- Reitan, Bård (Forsker) – Forsvarets forskningsinstitutt (FFI)
- Thuv, Aasmund (Forsker) – Forsvarets forskningsinstitutt (FFI)
- Windvik, Ronny (Forsker) – Forsvarets forskningsinstitutt (FFI)

FLO/IKT 2008. *Fagseminar FLO/IKT avdeling for beslutningsstøtte 23. april 2008*.

FOHK 2008. *Intervju med utvalgte fagpersoner 29. april 2008.*

- Aarrestad, Frank Terje (Oblt) – Forsvarets operative hovedkvarter (FOHK)
- Berglund, Jan (Kom) –Forsvarets operative hovedkvarter (FOHK)
- Jørstad, Nils Petter (Maj) – Forsvarets operative hovedkvarter (FOHK)
- Myrseth, Hans Petter (Orlkapt) – Forsvarets operative hovedkvarter (FOHK)

FORV 2008. *Intervju/møter med utvalgte fagpersoner innen forvaltningsdomenet våren 2008*.

- Borstad, Bredo (Ekstern konsulent) – LOS-Programmet/ Drift og videreutvikling (LOS/DVU)
- Jordan, Leif-Erik (Maj) – Forsvarets logistikkavdeling/ IKT Avdeling for beslutningsstøttesystemer (FLO/IKT BST)
- Solhaug, Jan Morten (NK / Oblt) – LOS-Programmet/ Drift og videreutvikling (LOS/DVU)
- Øderud, Kai (Oblt) – Forsvarsstaben/ Personell, Økonomi og Styring (FST/PØS)

Hafnor, Hilde (Forsker / Hovedveileder) – Forsvarets forskningsinstitutt (FFI)

INI 2008. *Intervju/møter med fagpersoner ved INI Stab våren 2008*.

- Holmedal, Tord-Arve (Oblt) – Forsvarsstaben/ Fellesstaben INI (FST/FS INI)
- Stikbakke, Carl Christian (Oblt) – Forsvarsstaben/ Fellesstaben INI (FST/FS INI)

Myhre, Bent Ivan (Maj) – Forsvarets Stabsskole (FSTS)

NATO 2008. *Intervju/møter med fagpersoner i NATO våren 2008.*

- Halaas, Lasse (Nasjonal teknisk ekspert) – NATO Consultation, Command and Control Agency (NC3A)

- Hallingstad, Geir (Scientist) – NATO Consultation, Command and Control Agency (NC3A)

Sandbakken, Herleif (Oblt) – Forsvarsdepartementet (FD)

TRADOK 2008. *Intervju med utvalgte fagpersoner 22. april 2008*.

- Brustad, Arle (Seksjonssjef / Oblt) - Hærens transformasjons- og doktrinekommando (TRADOK)
- Howlid, Tor Magne (Kap) - Hærens transformasjons- og doktrinekommando (TRADOK)

Vedlegg B – Avledede NbF faktorer

Dette vedlegget viser hvordan Enemo (2006) sine ni opprinnelige NbF faktorer, som en metodisk forenkling, er avledet som en del av beskrivelsen av NbF grad 2.

Enemoe (2006) sine faktorer	Grude sine avledede faktorer
Nettverksbevissthet	**Nettverksorganisering**
Doktrine	
Organisasjon og prosess	
Informasjonsinfrastruktur og teknologi	**MIL INI og teknologi**
Individ og kultur	**”Den militære profesjon”**
Ledelse, beslutningsprosesser	
Eksperimentering /øving/trening, /utdanning/ kompetanse	
Interoperabilitet (PTO)	**Interoperabilitet**
Økonomi	**Økonomi**

Vedlegg C – Planlagte fiendtlige anslag og mulig hendelsesforløp

Dette vedlegget beskriver den irregulære styrkens planlagte anslag og mulige hendelsesforløp.

Fire hovedanslag planlegges:

- *Anslag A:* En liten gruppe på tre-fire personer gjør begrensede fysiske anslag i Norge med fokus på infrastruktur som er sentral for det norske samfunnet. Anslaget er ikke ment for å skade, men for å vise evne.
- *Anslag B:* En liten gruppe gjør logiske anslag over Internett mot infrastruktur som er sentral for det norske samfunnet, sammen med å "slippe meldinger" (PSYOPS/villedning) for å påvirke norsk opinion og myndighetene.
- *Anslag C:* En liten gruppe i operasjonsområdet angriper IKT-systemet til de norske styrkene gjennom bruk av innsidere, og derigjennom fysisk adgang, i Norges leir.
- *Anslag D:* Fiendtlig overvåkings- og etterretningsaktiviteter gjennomføres med utgangspunkt i den irregulære styrken sine kontakter inn i formelle etterretningsorganisasjoner. Fremmede staters etterretningsaktivitet mot Norge og norske interesser er på et vedvarende høyt nivå. Mye informasjon er åpent tilgjengelig i det norske samfunnet som gir gode vilkår for aktivitetene til fremmede etterretningstjenester. Militært er både NATO-medlemskapet, Norges deltagelse i internasjonale operasjoner, samt Forsvarets nasjonale kapasiteter og doktriner av etterretningsmessig interesse. I disse sammenhengene fremstår også norske private og offentlige aktører i utlandet som aktuelle og utsatte etterretningsmål. Videre er flere staters etterretningsvirksomhet innrettet mot eksilmiljøer som oppholder seg i Norge.

Et tenkt hendelsesforløp vil kunne være som følger:

- *Forberedelser:*
  Gruppe A drar til Norge og forbereder angrep. Samtidig tiltar etterretnings- og overvåkingsaktiviteter mot Forsvaret og det norske samfunnet.
- *Ønsker meddeles og anslag (mot Norge) varsles:*
  Det varsles om fremtidig anslag (om en uke?) ved at gruppe B defacer utvalgte hjemmesider som når mange. I tillegg oppretter de nye nettsamfunn på Internett. De

fremstiller seg som frigjørere som vil ha Norge ut av operasjonsområdet og som foretrekker at dette gjøres uten vold. Gruppe D bruker aktiv allerede (nasjonale) nettsamfunn med den hensikt å skaffe til veie sentral og/eller gradert informasjon.

- *Første anslag mot (kritisk) norsk infrastruktur:*
  Gruppe A utplasserer jammekoffert for å dra ned kommunikasjon og støtter gruppe B som stanser togtrafikken i en begrenset periode.
- *Andre anslag mot (kritisk) norsk infrastruktur:*
  Et tilsvarende angrep gjentas etter en uke. Gruppe B slipper villedningspost fra statsministerens kontor, som omtaler situasjonen som dramatisk og utenfor kontroll, men at dette må holdes hemmelig for opinionen og andre partier på Stortinget.
- *Fiendtlige overvåkings- og etterretningsaktiviteter:*
  Gruppe D gjennomfører overvåkings- og etterretningsaktiviteter for å fore fiendtlig INFOOPS i deres planlegging og gjennomføring av koordinerte anslag. I tillegg utnytter gruppe D tilgjengelig informasjon om Forsvaret, Forsvarets kapasiteter osv som ligger åpent på forskjellige ”samhandlingsarenaer” på Internet.
- *Sette scenen i operasjonsområdet:*
  ”Dummyangrep” på informasjonssystemene i operasjonsområdet. Falsk video med voldshandlinger fra norske styrker på sivile i operasjonsområdet slippes. Det hevdes at denne har blitt hentet fra informasjonssystemene til Forsvaret (eller Norge) og at Forsvaret (militæret) dekker opp om overgrep. Falsk epost slippes fra FOHK som tilsynelatende kjenner til problemene, men som ikke bryr seg. Gruppe B varsler om anslag mot styrkene i operasjonsområdet og sier de ikke har noen valg all den tid Norge med sine militære styrker går løs mot sivilbefolkningen.
- *Utnyttelse av norske styrkers avhengigheter av IKT:*
  Gruppe C gjennomfører et tyngre IKT-angrep mot Forsvarets/innsatsstyrkens informasjonssystemer ved direkte angrep i Logistikksystemet.

Vedlegg D – Sentrale sårbarheter i transformasjonen mot en fremtidig MIL INI

Hensikten med dette vedlegget er å liste oppgavens hovedfunn i forbindelse med oppgavens første problemstilling.

Analysefaktor	Utledet analysefaktor	Sentral sårbarhet
(MIL) INI komponentstruktur	**INI prosjektportefølje**	Komplekse relasjoner mellom anskaffelser
		Ingen har total oversikt over (materiell)investeringene
		Overlappende og motstridende løsninger
		Strategiske investeringer går i flere retninger
	Investeringer i fellesløsninger	Ingen fellesløsninger passer alle
		Endring av Forsvaret vs spesialtilpasninger
		Lempning av sikkerhetskrav
		Tidsfaktoren styrer løsningen
		Endelige løsninger avviker fra den besluttede løsning
		Mangel på helhetlig tenkning og lite fokus på redundans
	Valg av samarbeidspartnere	Krav til bruk av mange standarder
		Mange samarbeidspartnere er mer ressurskrevende (utdanning, kompetansebygging, relasjonsbygging,…)
		Vanskeliggjør helhetlig styring av Forsvaret; minste felles multiplum fremfor helhetlig arkitektur
	Helhetlig og sømløs informasjons- og tjenestetilbyder	Feil i kjernetjenester er kritisk; fare for single point of failure”
		Ukritisk sammenkopling
		(Tekniske) ”lock-ins”
		Strategiske investeringer har forskjellige

		arkitekturmessige prinsipper
		Innledende investeringer vil kunne gi føringer på senere investeringer
		”Tviholder” på etablerte prosesser
	Administrasjon og tjenestehåndtering	Fremtidens MIL INI et lite Internett
		Håndtering av mange regimer for adgangskontroll
		Antallet aktører og tjenester gjør at man mister kontroll
	Gjennomgående integrasjon	Ett integrasjonslag – ”single point of failure”
		Arven må tas med sine (kjente) iboende sårbarheter
		Kompleks tilgangskontroll/”merking” av informasjonsobjekter
		Gjeldende lovverk kan begrense informasjonsflyten
	Sikkerhetsaspekter	Informasjonsflyt mellom graderingsnivåer
		Bruk av internettjenester
		Mange sårbarheter i (grunnleggende) systemer
		Risikohåndtering vs Sikkerhetsloven
		Individers/organisasjoners holdninger og bevissthet
		Vilje til endring
	Sivil tjenestetilkopling	Sentrale (logistikk)konsepter gir føringer ift utstrakt sivil tilkopling.
		Sivile aktører samme standarder og/eller ikke samme grad av modenhet i tjenestetekning
		Mangel på nasjonal INI kan fremtvinge (ikke sikkerhetsgodkjente) temporære løsninger

		Bruk av sivile samarbeidspartnere/-tjenester gjør at militær ende-til-ende kontroll ikke lengre er mulig

Vedlegg E – Sentrale sårbarheter i beslutningstakeres avhengighet og anvendelse av MIL INI

Hensikten med dette vedlegget er å liste oppgavens hovedfunn i forbindelse med problemstilling nummer to.

Analysefaktor	Utledede analysefaktorer	Sentrale sårbarheter
Situasjonsbevissthet	**Informasjonsmengde**	Avhengighet av økt deling av informasjon på tvers av grupper og nivåer
		Utilstrekkelig evne til informasjonshåndtering – både teknisk og menneskelig
		Fare for informasjonsmetning
		Rigide og statiske regelverk
		Manglende evne og vilje til informasjonsdeling
		Manglende tillit som grunnlag for informasjonsdeling
		Utilstrekkelig informasjon om fienden pga manglende kunnskap og kilder
		Nye typer terreng må tas for å sikre egen tilgang på informasjon
		Sikring av egen tilgang på informasjon vil kunne legge føringer for (ny)anskaffelser
		Koordinerte fiendtlige anslag øker informasjonsmengden
	Informasjonskvalitet	Tilgjengeliggjøring av informasjon ved gitt behov uten tilstrekkelig kvalitetskontroll
		Manglende felles forståelse fører til

		feil bruk og tolkning av informasjonsobjekter; integritet er mer enn dataintegritet, hvor det er integriteten i forståelsen som til syvende og siste er viktig
		Systemets manglende evne til å fremskaffe felles forståelse
		Manglende evne til omstilling (individer) i dynamiske beslutningsprosesser
	Informasjonsstyring	Manglende evne til å styre informasjonen rett; rett informasjon på rett sted til rett tid
		Manglende evne til dynamisk å fange opp brukernes behov
		Manglende kvalitet og innhold på merking/"taggig" av informasjonsobjekter som grunnlag for senere gjenfinning
Evne og vilje til beslutning	**Individuell vs kollektiv situasjonsbevissthet**	Manglende evne til å oppnå tilstrekkelig felles situasjonsbevissthet
		Manglende evne til å håndtere media
		Teknologien vil aldri fullt ut kunne erstatte personlig møte i søken etter felles situasjonsbevissthet
	Desentralisert vs sentralisert situasjonsbevissthet	Uklarheter om beslutninger skal fattes desentralisert eller sentralt
		Faren for micromanagement; sentralt nivå overtar med en gang "det brenner"
		Ukontrollerte og irrasjonelle handlinger i militære subsystemer
	Tillit og avdelingsånd	Høy rotasjonstakt

		Mistillit
		Kulturelle forskjeller
	Kompetanse	Krav til annen kompetanse enn det som er tilgjengelig
		Manglende evne til å fordøye data mentalt og se sammenhenger i informasjonen
		Manglende evne til å operere på flere nivåer samtidig
		Manglende evne til å identifisere konsekvenser på alle nivåer fra handlinger på alle nivåer
	Roller og ansvar	Uavklarte roller og ansvar
		Mangel på dekonfliktsledd
		Mangel på kompetanse
		Gamle handlingsmønstre videreføres
	Tempo	For raske beslutninger kan være sårbart
		Delegert myndighet og ønske om høyt (operasjonelt) tempo kan medføre feilvurderinger
		Tilsynelatende dårlig utnyttelse av tiden sett med verdenssamfunnet sine øyne
		Lovverk og rigide godkjennelsesprosesser kan forringe ønsket tempo for eksempel ved godkjenning av (nye) ROEs.
	Robusthet og teknologi	Uansett redundans i løsningen så er det en viss sårbarhet der
		Føringer i bruk av standard og kommersiell programvare har (kjente) iboende sikkerhetshull/svakheter

		Utilgjengelig MIL INI medfører lokale løsninger som kanskje ikke innehar ønsket/påkrevd grad av sikkerhet
		Mistillit til MIL INI er vanskelig å gjenoppbygge