Systemdynamisk tilnærming for risikoanalyse av transformasjonen til Nettverksbasert Forsvar

Rune Linchausen Skar

Masteroppgave
Master i informasjonssikkerhet
30 ECTS
Institutt for informatikk og medieteknikk
Høgskolen i Gjøvik, 2006

"*Achieving the full potential of net-centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected.*"

US Department of Defense, 2006[1]

"*We want the troops participating in the drill to know that defeat in information techniques means defeat in actual combat.*"

Commander Fan Changlong of the Jinan Military Area Command (China), leder av øvelse Vanguard-206B , 2006[2]

Institutt for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Sammendrag

Overgangen til et nettverksbasert konsept for krigføring vil medføre en omfattende transformasjon av Forsvaret. Konseptets kjerne ligger i å skape en radikal prosessforbedring gjennom innovativ bruk av informasjons- og kommunikasjonsteknologi. Målet med transformasjonen er å oppnå en radikal forbedring av Forsvarets evne til å skape militær effekt. Den vil medføre omfattende forandring av virksomhetsprosesser, rutiner og hvordan man utfører militære operasjoner. Konseptet muliggjøres gjennom utviklingen av en datamaskinbasert informasjonsinfrastruktur som skal knytte sammen tilnærmet alle enhetene i fremtidens Forsvar. Forsvarets evne til å skape militær effekt vil derfor være svært avhengig av en sikker funksjon for denne informasjonsinfrastrukturen.

Vi har i denne undersøkelsen utviklet en kvalitativ systemdynamisk modell som viser hvordan utilsiktet effekt relatert til risikobildet for informasjonsinfrastrukturen oppstår som et resultat av nettverksorganiseringen. Innsikten i de dynamiske kreftene som virker i systemet og hvordan utilsiktet effekt kan minimaliseres er kommunisert gjennom en problemarketype og en løsningsarketype. Innsikten viser at risikobildet for informasjonsinfrastrukturen endres dynamisk med grad av nettverksorganisering i Forsvaret. Dersom dette forholdet ikke håndteres på en adekvat måte, har det potensiale til å redusere eller i verste fall annullere forventet effekt av nettverksorganiseringen.

Siden Forsvaret i all hovedsak bare kan påvirke risikobildet gjennom en reduksjon av sårbarheter og virkningen av logiske angrep mot informasjonsinfrastrukturen, foreslås følgende policy for Forsvarets transformasjon til Nettverksbasert forsvar;

> **For å sikre realisering av effektpotensialet i Nettverksbasert forsvar, skal økt bruk av ressurser for nettverksorganisering av Forsvaret medføre parallelt økt bruk av ressurser for håndtering av risiko for logiske angrep mot informasjonsinfrastrukturen. Bruken av ressurser skal baseres på en intelligent og kosteffektiv kombinasjon av forebyggende, detekterende og reagerende tiltak.**

Abstract

The transition towards a network centric concept for warfare will cause a comprehensive transformation for the Norwegian Defence. In the core of the concept we find the need to create a radical improvement of the processes through innovative use of information and communication technologies. The purpose of this transformation is to achieve a radical improvement in the Norwegian Defences ability to create military effect. It will bring about an extensive change in operational processes, routines and how we conduct military operations. The concept is enabled through the developement and implementation of a computer-based information infrastruture that will connect virtually all units in the Norwegian Defence of the future. The Norwegian Defences ability to create military effect will therefore be very much dependent of a functional and secure information infrastructure.

In this master thesis we have developed a qualitative model based on system dynamics, that point out how unintended effects that affect the risk level in the information infrastructure manifest itself as a result of the network centric organisation. Knowledge of the dynamic forces that work in this system, and how unintended effect can be minimized is communicated through a problem archetype and a solution archetype. This insight demonstrates that the risk picture for the information infrastructure changes according to the degree of network centric organisation in the Norwegian Defence. If this condition is not handled adequately, it has the potential to reduce or, in the worst case, nullify the anticipated effect of network centric organisation.

The Norwegian Defence can influence the risk picture mainly by reducing the number of vulnerabilities and the impact of logical attacks on the information infrastructure. We therefore propose the following policy for the Norwegian Defences transformation towards a network centric organisation:

> **To ensure the realization of the effect-potential in a network centric defence, increased use of resources in network centric organisation shall be followed by a parallell increased use of resources in handling the risk of logical attacks on the information infrastructure. The use of resources shall be based on an intelligent and cost-effective combination of prevention, detection and reaction measures.**

Forord

Denne masteroppgaven vil fullføre min mastergrad innen informasjonssikkerhet ved Høgskolen i Gjøvik. Mastergraden er gjennomført på deltid fra høsten 2003 til høsten 2006. I samme tidsperiode har jeg arbeidet innen fagfeltet informasjonssystemsikkerhet ved Forsvarets sikkerhetsavdeling.

For alle som jobber med informasjonssystemsikkerhet i Forsvaret, er vi nå inne i en spennende tid. Vi står på terskelen til en transformasjon som skal sikre at Forsvaret blir en potent aktør også i det 21. århundret. Overgangen til et Nettverksbasert forsvar vil medføre en stor økning i Forsvarets avhengighet av datamaskinbaserte informasjonssystemer. Risikohåndtering for disse systemene vil i fremtiden få en direkte innvirkning på Forsvarets evne til å gjennomføre militære operasjoner. Dette krever at vi oppfatter informasjonssystemsikkerhet som noe mer enn en oppfyllelse av kravene i Sikkerhetsloven. Fremtiden krever et aktivt forsvar av våre informasjonssystemer for å sikre vår evne til å skape militær effekt! Jeg håper denne masteroppgaven kan bidra til utbredelsen av et slikt syn i Forsvaret.

Takk til...

Min veileder José J. Gonzalez som har bidratt med sin uvurderlige støtte gjennom hele arbeidet med denne oppgaven. Han har etter min oppfatning bidratt med langt mer enn hva man kan forvente av en travelt opptatt professor. Hans faglige innsikt, evne til å motivere og forkjærlighet til vitenskap og systemdynamisk metode har gjort arbeidet med denne oppgaven til en svært lærerik prosess.

Takk til min sjef, Roger Johnsen, for at han er en uredd og proaktiv person som våger å gjennomføre ting han tror på. Hans innsats for kompetanseheving innen fagfeltet informasjonssystemsikkerhet er den viktigste årsaken til min gjennomføring av dette mastergradstudiet. Han har også bidratt med mange svært viktige faglige innspill.

Takk til alle mine medarbeidere i Forsvarets sikkerhetsavdeling som har hjulpet meg gjennom gode faglige diskusjoner. En spesiell takk til Bjarte Malmedal for hans evne til å motivere til videre arbeid i tunge perioder.

Takk til Kjell-Olav Nystuen ved FFI og Bjørn T. Bakken ved FSS for deres faglige innspill og konstruktive kommentarer til midlertidige versjoner av rapporten.

Den største takken går likevel til min kone Evy og min datter Elén (som ikke var født da jeg startet på denne masteroppgaven) for deres bunnløse tålmodighet og uvurderlige støtte gjennom hele mitt mastergradsstudie. Livet er en lek med slike som dere på laget!

Innhold

Sammendrag . . . . . **i**
Abstract . . . . . **iii**
Forord . . . . . **v**
Innhold . . . . . **vii**
Figurer . . . . . **ix**
Tabeller . . . . . **xi**
1 Innledning **1**
1.1 Bakgrunn og problemstilling 1
1.2 Avgrensning av oppgaven 3
1.3 Forskningsspørsmål 7
1.4 Oppgavens bidrag 8
1.5 Rapportens struktur 9
1.6 Viktigste konklusjoner 9
2 Relatert litteratur **11**
3 Metode **13**
3.1 Valg av metode 13
3.2 Utvikling av CLD-modell for tilsiktet og utilsiktet effekt 19
3.3 Analyse av CLD-modell og forslag til intervensjon for å håndtere uønsket atferdsmønster 21
3.4 Verktøy 22
3.5 Reliabilitet og validitet 22
4 Tilsiktet effekt for NBF konseptet **25**
4.1 Bakgrunn: behov for militær effekt under endrede rammebetingelser . . . 26
4.2 CLD-modell av drivere for anvendelse av NBF konseptet 30
4.3 Oppsummering av drivere for NBF-konseptet 33
4.4 Hvilke endringer nettverksbasert konsept medfører 33
4.4.1 Tradisjonell organisering av forsvaret: plattformbasert forsvar . . . 33
4.4.2 Fremtidens organisering av forsvaret: nettverksbasert forsvar . . . 36
4.5 Utvidelse 1 av CLD-modell: Tilsiktede effekter ved NBF 39
4.5.1 Kilder for kunnskap om teoretisk grunnlag for NBF 39
4.5.2 Militær effekt som resultat av tilstand i tre domener 39
4.5.3 Historiske utfordringer og mulige løsninger i informasjonsalderen . 42
4.5.4 Forholdet mellom økt kapasitet i informasjonsdomenet og militær effekt 45
4.5.5 Sentrale variabler og kausale sammenhenger 49
4.6 Delkonklusjon - tilsiktet effekt av NBF 55
5 Utilsiktet effekt ved implementering av NBF konseptet **59**
5.1 Informasjonssystemet i NBF 59
5.1.1 Informasjonsinfrastrukturen (INI) 59
5.1.2 Tjenesteinfrastrukturen 61

5.1.3 Kommunikasjonsinfrastruktur 62
5.2 Faktorer som inngår i risikoanalyse av INI 65
5.3 INI's verdi 68
5.3.1 INI's verdi for Forsvaret 68
5.3.2 Dynamisk utvikling av INI's verdi 71
5.4 Trussel mot INI 72
5.4.1 Motivasjon for logiske angrep mot INI 74
5.4.2 Evne til logiske angrep mot INI 77
5.4.3 Mulighet for logiske angrep mot INI 81
5.4.4 Dynamisk utvikling av trussel mot INI 81
5.5 Sårbarhet i INI 81
5.5.1 Sårbarhetsskapende faktorer for informasjonssystemer 82
5.5.2 Sentrale egenskaper for INI 85
5.5.3 Dynamisk utvikling av sårbarhet i INI 90
5.6 Utvidelse 2 av CLD-modell: Utilsiktet effekt av NBF implementering 91
5.7 Delkonklusjon - utilsiktet effekt av NBF 94
6 Tiltak for minimalisering av utilsiktet effekt 97
6.1 Problemarketype 97
6.2 Løsningsarketype 103
6.3 Utvidelse 3 av CLD-modell: Risikohåndtering for militær effekt 109
6.4 Delkonklusjon - tiltak for minimalisering av utilsiktet effekt 110
7 Konklusjon og diskusjon 113
7.1 Konklusjon 113
7.2 Begrensninger ved undersøkelsen 114
7.3 Videre arbeid 115
Bibliografi 117

Figurer

1 Nivåer av systemdynamiske modeller [3] 6
2 Kausale linker mellom variabler 14
3 Kausal løkke (selvforsterkende) 15
4 Balanserende kausal løkke (med tidsforsinkelse mellom justering av termostat og faktisk temperatur 16
5 Behaviour Over Time (BOT) graf for variabelen temperatur-gap fra modellen i figur 4 17
6 Fire generiske problemarketyper med tilhørende løsningsarketyper; R = forsterkende feedback løkke; B = balanserende feedback løkke; o = negativ kausalitet; system boundary = organisasjonsgrense [4] 18
7 Utvikling av CLD-modell i to faser 19
8 Drivere for anvendelse av NBF konseptet 30
9 Plattformbasert organisering med statisk inndeling i rom (ansvarsteiger) og grenvis ansvarstildeling [5] 34
10 Eksempel på tradisjonell kommandostruktur [6] 36
11 Nettverksbasert organisering med helhetlig fokus på hele innsatsområdet [5] 38
12 Eksempel på mulig kommandostruktur i NBF[6] 38
13 De tre domener for militære operasjoner [6] 40
14 Situasjonen er definert av tilstanden for en rekke komponenter i innsatsrommet [7] 41
15 Forholdet mellom grad av “fog ”, friksjon og evne til synkronisering i utførelse av militære operasjoner [7] 42
16 Forholdet mellom richness, reach og potensiell evne til å skape verdi[7] . 43
17 Verdikjede for militære operasjoner[7] 44
18 Forbedringer i informasjonsdomenet og det kognitive domenet gir økt effekt i det fysiske domenet[7] 45
19 Verdikjeder fra “Network Centric Warfare Developing and Leveraging Information Superiority” og “Introduksjon til Nettversbasert Forsvar” 46
20 Utvidet verdikjede fra “Understanding Information Age Warfare”[7] 47
21 De fire dogmene i NCW[8] 47
22 Dogmer omsatt til modell[9] 48
23 NCW verdikjede fra NCO CF[10] 49
24 Økt virkning ved økt kvalitet for allokering av mål[11] 50
25 Modell for tilsiktet effekt av NBF konseptet 53
26 Tidshorisont for fullstendig nettverksorganisering av Forsvaret [12] 54
27 Sammenligning av variabler for styrker med og uten Link16 57
28 De ulike nettverkene i NBF [13] 61
29 Referansemodell for NBF [14] 62
30 Komponenter i kommunikasjonsinfrastrukturen for NBF [15] 62

31 Topologi for kommunikasjonsinfrastrukturen i NBF [16] 65
32 Risiko eksisterer der kritisk informasjon (verdi), trussel og sårbarhet overlapper [17] 67
33 "Den indre doktrinesløyfen"[18] 69
34 Elementer som definerer trussel mot et informasjonssystem 73
35 Virkemidler for logiske angrep korrelert med hvilke sikkerhetsegenskaper de angriper 77
36 Økt grad av sofistikerthet for logiske midler for angrep vs behov for teknisk ferdighet for å implementere dem [19] 78
37 Økt grad av sofistikerthet for logiske midler for angrep vs behov for teknisk ferdighet for å implementere dem [20] 85
38 Overgang til et felles nettverk basert på IP-teknologi som bærer for ulike tjenester [21] 87
39 Utilsiktet effekt ved implementering av NBF 92
40 Den generiske problemarketypen Relative control med de tilhørende semigeneriske arketypene Escalation og Drifting goals [4] 98
41 Problemarketype 99
42 Behaviour Over Time (BOT) grafer for sentrale variabler 101
43 Løsningsarketype 104
44 Ulike kombinasjoner av forebyggende, detekterende og reagerende tiltak kan gi samme kvalitative nivå av sikkerhet (alle punkter på kurven representerer samme kvalitative nivå av sikkerhet) i et informasjonssystem [17] 107
45 Risikohåndtering for militær effekt 111

Tabeller

1 Kriterier for utvalg av dokumenter 20
2 Oversikt over organisasjonsmessig tilhørighet og kompetanseprofil for eksperter. 21
3 Forskjeller i begrepsbruk for kvantitativ og kvalitativ metode 22
4 Oversikt over litteratur for bakgrunn og forventet effekt av NBF 26
5 Undersøkelser for validering av NCW hypotese 56
6 Oversikt over sentral litteratur for analyse av utilsiktet effekt. 60
7 Beskrivelse av funksjonsvise beslutningsstøttetjenester i INI 63
8 Beskrivelse av felles kjernetjenester i INI 64
9 Militære basisfunksjoner og deres korresponderende tjenester i INI 70
10 Oversikt over sentral litteratur for minimalisering av utilsiktet effekt. . . . 98

1 Innledning

1.1 Bakgrunn og problemstilling

Anvendelsen av teknologiske nyvinninger for militære formål har gjennom historien ledet til nye metoder for krigføring som avgjørende har endret hvordan en militærmakt har kunnet bekjempe sine motstandere. Slike klare skiller i metodeskifte benevnes ofte "Revolutions in Military Affairs (RMA) ". I følge Andrew F. Krepinevich kan RMA defineres som [22];

> It is what occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase - often an order of magnitude or greater -in the combat potential and military effectiveness of armed forces.

Fra denne definisjonen utledes at en RMA består av fire elementer; teknologisk endring, utvikling av militære systemer basert på den nye teknologien, operasjonell innovasjon og organisatorisk tilpasning. Hvert enkelt element er i seg selv en nødvendig, men ikke tilstrekkelig forutsetning for realisering av den store økningen i militær effektivitet som karakteriserer en RMA. Ny teknologi vil med andre ord ikke være nok i seg selv. En må også utvikle doktriner og organisatoriske konfigurasjoner for å hente ut potensialet for effektivitetsøkning som ligger i den teknologiske nyvinningen.

Et av de mest anvendte eksemplene på en RMA er blitzkrig-konseptet som den tyske hæren introduserte i 1940 for å bekjempe den franske og britiske hæren i nord-frankrike. Konseptet besto i å la pansrede styrker virke tett sammen med støtte fra luftvåpenet. Angrepene ble løpende koordinert ved hjelp av radiosamband. Det var fokus på raske manøvre og mobilitet, samt en desentralisert kommandostruktur. Teknologien som la grunnlaget for konseptet (fly, stridsvogner og radiosamband) var tilgjengelig for begge parter i krigen. Det var imidlertid bare tyskerne som kombinerte den med nye doktriner og nye organisasjonsformer. Resultatet ble en dramatisk økning i effektivitet på slagmarken som gjorde dem overlegen i forhold til sine motstandere.

Flere militærteoretikere mener at vi nå står ovenfor en RMA basert på nyvinninger innen informasjonsteknologien. Forsvarssjef, general Sverre Diesen, bifaller dette synspunktet i et foredrag han holdt for Oslo Militære Samfund i april 2003[5];

> I vår tid er det altså mikroprosessoren og dermed datamaskinen som ved å revolusjonere informasjonsbehandlingen endrer militære organisasjoner like grunnleggende som noen av de foregående RMA'er

Utviklingen innen informasjonsteknologi har lagt grunnlaget for en ny tilnærming til hvordan militære operasjoner ledes og gjennomføres. Konseptet ble opprinnelig utviklet av amerikanske militærteoretikere og fikk navnet Network Centric Warfare (NCW). Det norske Forsvaret har adoptert konseptet og her benevnes det Nettverksbasert forsvar (NBF). NBF beskrives i St.prp 42 Den videre moderniseringen av Forsvaret i perioden 2005-08 [23], som et konsept for hvordan militære operasjoner kan gjennomføres på en

mer effektiv måte, gjennom å knytte sammen enheter, på tvers av forsvarsgrenene og på ulike nivåer i organisasjonen i et nettverk ved bruk av informasjonsteknologi;

> NBF går i korthet ut på å utnytte informasjonsteknologi til å organisere Forsvarets operative struktur og enheter i et samvirkende nettverk. Gjennom deling og utveksling av informasjon på tvers i nettverket, får våre styrker et mer fullstendig og oppdatert beslutningsgrunnlag. Forsvarets enheter får dermed økt mulighet til å handle raskere, mer effektivt og presist, i forhold til det situasjonen krever. For å kunne utnytte denne muligheten, må hastigheten i beslutningsprosessen økes, samtidig som våpensystemer og sensorer må ha en mobilitet, presisjon og rekkevidde som står i forhold til dette. Økt hastighet og kvalitet i beslutningsprosessen kan blant annet oppnås ved å redusere antall kommandonivå, bruke moderne beslutningsstøttesystemer og legge til rette for økt grad av selvorganisering av styrkene. Dette vil medvirke til dramatisk forbedring i effekt i forhold til ressursbruken, og styrke mulighetene for politisk kontroll i en krisesituasjon.

Det er bestemt på politisk nivå i Norge at Forsvaret skal transformeres for å kunne operere nettverkssentrisk (mao etter konseptet NBF). Dette fremgår av St.prp.nr.1 (2003-2004) for budsjetterminen 2004, som fastslår i kapittel 4.6 [24] at Forsvaret, som en del av en helhetlig omstillingsprosess, skal anvende NBF som konseptuelt rammeverk for deres fremtidige militære operasjoner:

> Overgangen til et nettverksbasert forsvar, med en utvikling mot et integrert databasert informasjonssystem for sensorer, beslutningstakere og våpensystemer inngår i omstillingsprosessen

Det integrerte datamaskinbaserte informasjonssystemet er en avgjørende komponent for realisering av NBF-konseptet. Innføringen av NBF vil følgelig bety økt avhengighet av informasjons- og kommunikasjonsteknologi (IKT) for gjennomføring av vellykkede militære operasjoner. Denne utviklingen mot økt IKT-avhengighet gjenspeiler den senere tids samfunnsutvikling i de fleste industriland. IKT forenkler og forbedrer de fleste virksomheter og er et viktig virkemiddel for effektiv produksjon av offentlige og private tjenester. Det er en viktig del av nær sagt alle samfunnsfunksjoner, for eksempel bank- og finansvesen, trafikkstyringssystemer, kraft- og vannforsyning, ledelsessystemer og massemediene.

Samtidig som Forsvaret og samfunnet generelt blir stadig mer avhengig av IKT, ser vi en massiv økning i antall angrep mot slike systemer. Angrepene blir også stadig mer sofistikerte. Det eksisterer en mengde teknikker og teknologiske løsninger som aktører med ulike mål og motiver kan anvende for å angripe systemene. Gjennom angrepene kan de tilegne seg uautorisert innsyn, endre innhold i og hindre autorisert tilgang til informasjon. Denne dualiteten i den teknologiske utviklingen er politisk anerkjent i Norge og den er blant annet beskrevet i St.prp.nr.42 (2003-2004) Den videre moderniseringen av Forsvaret i perioden 2005-2008 [23]:

> Spredningen av avansert teknologi og moderne samfunnskritiske avhengighet av teknologi for å kunne fungere, har skapt grobunn for nye sikkerhetsutfordringer. Faren for spredning av masseødeleggelsesvåpen og moderne våpenteknologi står sentralt i dette bildet, jf. kapittel 3.4.2. Teknologiutviklingen har også skapt nye muligheter for å ramme både det sivile samfunn og militære motstandere ved hjelp av nye virkemidler og asymmetriske strategier. Konsekvensene av å sakke akterut i den teknologiske utviklingen vil i enkelte tilfelle kunne være av avgjørende betydning i negativ retning,

både for evnen til å ramme en motstander på en effektiv og differensiert måte, og for evnen til effektiv beskyttelse av egne militære styrker og befolkning.

Hypotesene om hvordan NBF skaper økt militær effekt beskrives vanligvis i deterministiske termer: de postulerer at dersom du nettverksorganiserer en forsvarsmakt, vil den skape mer militær effekt. En slik beskrivelse vitner om et hendelsesorientert "verdenssyn" basert på enkle og lineære forhold mellom årsak og virkning. Fra et systemdynamisk synspunkt vet vi at dette ofte leder til manglende måloppnåelse eller i verste fall at vi forverrer problemet vi prøver å løse. Slik uventet dynamikk benevnes i systemdynamikken "Policy Resistance": tendensen til at intervensjoner blir forsinket, utvannet eller forpurret av systemets respons på den opprinnelige intervensjonen [25]. I denne konteksten kalles den effekten som vi ønsket å realisere gjennom intervensjonen **tilsiktet effekt**. Effekten vi ikke forutså; effekten som "virker tilbake" og forpurrer vårt forsøk på å løse et problem, ansees som en sideeffekt og kalles **utilsiktet effekt**. Policy Resistance oppstår ofte fordi beslutningstakere ikke er klar over eller ikke forstår omfanget av responser på intervensjonene som virker i systemet. Det eksisterer et potensielt motsetningsforhold mellom det deterministiske synet som legges til grunn for NBF og det faktum at NBF realiseres gjennom datamaskinbaserte informasjonssystemer, som historien har vist, i stadig økende grad utsettes for vellykkede logiske angrep ("Hacking"). Dette forholdet leder oss til å fremsette følgende problemstilling:

> **Kan tilsiktet effekt av NBF påvirkes av utilsiktet effekt relatert til informasjonssystemsikkerhet og hvordan kan man eventuelt minimalisere den utilsiktede effekten?**

1.2 Avgrensning av oppgaven

Det er vanlig å dele inn informasjonsinfrastruktruer i tre hovedklasser etter geografisk beliggenhet og funksjon [26]:

GII Global Information Infrastructure

NII National Information Infrastructure

DII Defense Information Infrastructure

Det eksisterer en rekke ulike definisjoner av disse begrepene, men dersom vi ser på de individuelle ordene i begrepene, får vi en relativt god forståelse for hva det er snakk om. Global, National og Defense refererer til geografisk avgrensing og funksjon. Med informasjon menes som oftest data med meta-informasjon slik at den gir mening og infrastruktur kan beskrives som underliggende fundament eller grunnlag for et system eller en organisasjon. Begrepene omhandler altså systemer som benyttes for utveksling av informasjon globalt, nasjonalt eller innenfor en forsvarsmakt. Vi kan øke presisjonen i dette utsagnet ved å se på noen definisjoner av begrepene [27]:

International Standards Organization definerer GII som; *en infrastruktur som er i stand til å understøtte utviklingen, implementeringen og interoperabiliteten for informasjonstjenester og applikasjoner som allerede eksisterer eller kommer til å eksistere i fremtiden gjennom informasjonsteknologi, telekommunikasjon og forbrukerelektronikk.*

Department of Defense (USA) definerer NII som; *settet av informasjonssystemer og nettverk som en nasjon er avhengig av for å fungere.*

Department of Defense (USA) definerer DII som; *et sømløst nett av kommunikasjonsnettverk, datamaskiner, databaser, data og andre kapabiliteter som imøtekommer behovet til brukerne i DoD for informasjonsprosessering og informasjonstransport i fred, alle typer kriser, konflikter, humanitær støtte og krig.*

DII er et subsett av NII som igjen er et subsett av GII. Det ligger i problembeskrivelsens natur at informasjonssystemene vi vil fokusere på i denne rapporten er avgrenset til de som Forsvaret er avhenging av for å utføre militære operasjoner i fred, krise og krig. NBF handler om transformasjon av Forsvaret, ikke det norske samfunnet eller verden som sådan. I denne oppgaven vil vi følgelig fokusere på DII for Norge og legger DoD's definisjoner til grunn for å avgrense DII fra NII og GII.

Implementasjon av NBF kan medføre utilsiktet effekt innen flere ulike deler av systemet som Forsvaret er en del av og samvirker med. Siden informasjonssystemer er så grunnleggende viktig for NBF, er informasjonssystemsikkerhet et viktig felt som bør vurderes. Det eksisterer imidlertid flere mulige tilnærminger for å vurdere om implementeringen av NBF kan medføre utilsiktet effekt relatert til informasjonssikkerhet. Et eksempel i denne sammenhengen er et systemdynamisk studie som er utført i forbindelse med innføring av det som kalles eDrift i norsk olje- og gassindustri. I dette studiet valgte man å fokusere på hvordan mengde og rekkefølge for bruk av ressurser for endring av prosesser og tilegnelse av ny kunnskap påvirket sårbarhet [28]. I vår oppgave vil vi undersøke om tiltakene som skaper tilsiktet effekt i NBF kan medføre utilsiktet effekt relatert til informasjonssystemsikkerhet. Risiko og sikkerhet blir ofte definert som komplementære størrelser slik at den ene størrelsen kan beregnes ut fra den andre. Høy risiko tilsvarer lav sikkerhet, og omvendt [29]. Dette medfører at vi vil fokusere på eventuell utilsiktet effekt relatert til de tre grunnlegende komponentene for risiko i informasjonssystemer; verdi, sårbarhet og trussel.

Sikker funksjon i et informasjonssystem er avhengig av følgende tre basisegenskaper:

1. Konfidensialitet; at systemets funksjon og datainnhold er sikret mot innsyn.
2. Integritet; at systemet er sikret mot manipulering av systemets funksjon og datainnhold.
3. Tilgjengelighet; at systemet er sikret mot avbrudd i sin forventede funksjon og at systemet har tilgang til nødvendig datainnhold.

Hendelser som medfører brudd på en eller flere av disse basisegenskapene kan ha utspring i ulike årsaker. Det er vanlig å skille mellom villede og tilfeldige ikke-villede hendelser [30]. Eksempler på årsak til tilfeldige hendelser kan være tekniske feil eller ødeleggelser som følge av en naturlig hendelse, for eksempel fra lynnedslag. Villede hendelser er derimot hendelser som har sin årsak i menneskers vilje til å forårsake ødeleggelse eller forstyrrelse. Dette er altså bevisste angrep mot informasjonssystemer hvor målet er å ramme en eller flere av basisegenskapene for sikker funksjon. Virkemidler mot informasjonssystemer vil i hovedsak inngå i følgende kategorier [30];

Fysiske Fysiske trusler er rettet mot å skade infrastruktur med mål å redusere tilgjengeligheten til informasjonssystemene. Disse kan være rettet mot så vel den tekniske informasjonsinfrastrukturen som selve informasjonen som er nødvendig for systemenes funksjon. Målene for slike angrep vil være sentrale datamaskiner, lagringsmedia for informasjon, forbindelsesveier og knutepunkt i kommunikasjonsnett og driftssentraler som står for styring og kontroll av informasjonssystemene. Fysiske

trusler vil også kunne rettes mot infrastrukturer som informasjonssystemene igjen er avhengig av. Kraftforsyning er et eksempel på en slik infrastruktur.

Elektroniske Den elektroniske trusselen er en form for fysisk trussel, men skiller seg fra denne ved at det kun er de elektroniske komponentene i systemet som utnyttes, forstyrres eller ødelegges som følge av virkemiddelbruken. En skiller i første rekke mellom elektromagnetisk jamming, elektromagnetiske strålingsvåpen og elektromagnetisk avlytting.

Sosiale Mennesker inngår som en viktig ressurs både i planlegging, operativ drift av og bruk av informasjonssystemer. Menneskene utgjør derfor også en mulig angrepsvektor mot et informasjonssystem. Systemadministratorer og/eller brukere av et system kan med eller uten eget viten påvirkes til å gjøre gale ting, gjennom metoder som villedning, propaganda eller utpressing.

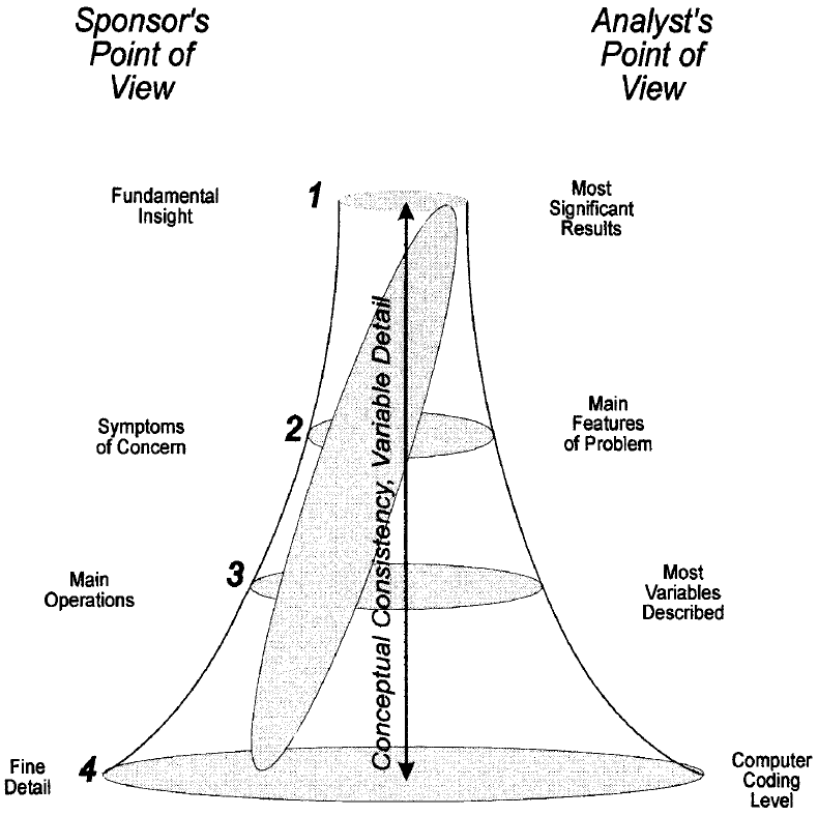
Logiske Logiske trusler dreier seg om et sett med virkemidler direkte rettet mot informasjonssystemenes logiske funksjon. Virkemidler for logiske angrep kan grovt deles inn i direkte systemangrep og programvareangrep. Begge formene for logiske angrep vil kunne være rettet mot alle egenskapene til et informasjonssystem; integritet, tilgjengelighet og konfidensialitet.

Vi vil i denne oppgaven avgrense oss til å vurdere risiko realtert til villede logiske trusler. Vår trussel og sårbarhetsvurdering vil derfor være avgrenset til denne kategorien. Avgrensningen begrunnes for det første med at tidsrammen for masteroppgaven ikke gjør det mulig å vurdere alle kategoriene. Av de fire kategoriene er det logiske angrep som er nyest og eksplisitt spesifikke for datamaskinbaserte informasjonssystemer. Det er også innenfor denne kategorien en har sett størst utvikling de senere år, samt at en del sentrale aktører i Forsvaret vurderer denne som den mest sannsynlige angrepsvektoren mot deres informasjonssystemer i fremtiden. Dette fremgår blant annet av følgende sitat fra en rapport utgitt av Forsvarets forskningsinstitutt i 2004 [16];

> Physical robustness is likely to become less important as the threats to military networks are likely to move from physical attacks to cyber attacks, initiated both inside and outside the Norwegian borders.

En komplett systemdynamisk analyse av komplekse systemer krever ofte en kvantitativ simulering for å gi valide og pålitelige svar. Noen av autoritetene innen systemdynamikken hevder sågar at dette er den eneste riktige tilnærmingen til analyse av komplekse systemer. Sterman [25] begrunner et slikt syn med at kompleksiteten i menneskers mentale modeller er for stor til at vi kan resonnere oss frem til en forståelse av dem. Han mener imidlertid også at kartlegging av mentale modeller relatert til problemstillingen er en viktig og ofte nødvendig del av en systemdynamisk prosess. Andre sentrale personer i det systemdynamiske miljøet mener at kvalitative systemdynamiske modeller kan benyttes som frittstående verktøy for forståelse av underliggende årsaksforhold i komplekse systemer. Et slikt syn støttes blant annet av Wolstenholme [31] og Coyle [32]. Coyle's tilnærming til den systemdynamiske prosessen er å utvikle modeller på flere nivåer hvor han både starter og avslutter med Causal Loop Diagram modeller (CLD-modeller; også kjent som influensdiagrammer, se kapittel 3 for beskrivelse). De

ulike nivåene fremgår av figur 1, hvor hver ellipse representerer en CLD-modell av økende størrelse og detaljeringsgrad ettersom man beveger seg nedover i kjeglen. Coyle postulerer at det er både gjennomførbart og nødvendig å lage flere diagrammer av det samme problemet/utfordingen siden de har ulike bruksområder. Diagrammene kan være svært ulike med tanke på hvilken grad av detaljer de inneholder, men alle omfatter de samme konsepter. De ulike nivåene omhandler altså det samme, men de uttrykker det på ulike måter for å passe ulike publikum.



Figur 1: Nivåer av systemdynamiske modeller [3]

En systemdynamisk undersøkelse starter vanligvis på nivå 2 hvor modellereren ("analyst i modellen") prøver å fange klientens forståelse for systemet og trekke ut hans mentale modeller om hvordan systemet virker. Ettersom man samler inn mer informasjon videreutvikles modellen til nivå 3. Ofte stopper arbeidet her og resultatet er en ren kvalitativ modell. Dersom en kvantitativ modell er berettiget, utvikles denne på nivå 4 hvor man kan benytte strenge konvensjoner for å identifisere nivåer, flytrater og det matematiske forholdet mellom disse. Nivå 1 av kjeglen benyttes bare mot slutten av prosessen for å identifisere de viktigste funn og innsikt i systemet.

I denne oppgaven vil vi avgrense oss til kvalitativ modellering i form av CLD-modeller. Det innebærer at vi vil holde oss til de tre øverste nivåene i figur 1. Avgrensingen begrunnes ut fra tre forhold:

Problemstilling Kvalitativ CLD-modell er et passende verktøy i forhold til oppgavens problemstilling. Ved å modellere hvordan den tilsiktede effekten ved NBF opp-

står og hvilken utilsiktet effekt dette kan medføre, legges et godt grunnlag for kunnskap, forståelse og innsikt for de kausale løkkene som virker i systemet. Dette kan bidra til å utvide de mentale modellene til beslutningstakere for utvikling av NBF i Forsvaret og følgelig lede til hypoteser om hvordan utilsiktet effekt kan reduseres i størst mulig grad. Kvalitative modeller er ofte enklere å forstå enn kvantitative modeller for personer som ikke har kjennskap til systemdynamikk. En initial kvalitativ undersøkelse kan således vinne aksept hos beslutningstakere for en dypere undersøkelse ved hjelp av kvantitative modeller.

Ressurser Tidsrammen for masteroppgaven gir ikke rom for utvikling av både en kvalitativ og en kvantitativ simulerbar modell av problemstillingen. Vi har derfor fokusert på å utvikle en kvalitativ modell som kan bevisstgjøre Forsvaret på problematiske forhold.

Kompetanse Forfatteren har liten grad av erfaring med systemdynamiske metoder. Utvikling av kvantitative simulerbare modeller kan være svært krevende og ligger utenfor hans kompetanseramme på dette tidspunkt.

Hele eller deler av modellen som utvikles i denne oppgaven vil kunne benyttes som grunnlag for en fremtidig kvalitativ simulerbar modell (nivå fire i figur 1. Ut fra dette mener vi at avgrensningen for oppgaven er i tråd med god praksis innen vitenskapelige arbeider: den bygger på eksisterende kunnskap og legger grunnlaget for videre forskning i fremtiden.

1.3 Forskningsspørsmål

Problemstillingen i oppgaven er et resultat av det potensielle motsetningsforholdet mellom det deterministiske synet som legges til grunn for konseptet NBF og dets avhengighet av informasjonssystemer som skal operere i et så fiendtlig miljø som det krise og krig representerer. Slike miljø er også komplekse i sin natur; krig er på mange måte en kontinuerlig prosess som svinger mellom tiltak iverksatt for å bekjempe fienden og fiendens mottiltak for å møte disse. I denne konteksten er det naturlig å anta at store endringer i Forsvarets operasjonskonsept over tid vil resultere i en reaksjon fra omgivelsene. En systemdynamisk tilnærming er derfor trolig en god metodikk for å utvikle en bedre innsikt og forståelse for denne situasjonen. Målet er å undersøke om tiltakene vi iverksetter for å oppnå tilsiktet effekt kan resultere i uforutsette reaksjoner fra systemet. Det første steget i denne prosessen vil være å identifisere kjeder av kausale sammenhenger som sammen danner et bilde av forventet resultat av iverksatte tiltak:

Forskningsspørsmål 1 Hva er den forventede effekten av NBF og hvordan skal denne realiseres?

Det neste steget i prosessen vil være å identifisere mulige uforutsette reaksjoner som kan oppstå som et resultat av tiltakene for realisering av NBF. Her kan det også oppstå kjeder av kausale sammenhenger som danner et bilde av hva som skjer og hvordan dette eventuelt kan påvirke tilsiktet effekt. Siden vi har avgrenset denne oppgaven til å fokusere på informasjonssystemsikkerhet, gir det følgende spørsmål:

Forskingsspørsmål 2 Kan implementeringen av NBF medføre utilsiktet effekt relatert til informasjonssytemsikkerhet og hvordan påvirker eventuelt denne realiseringen av den tilsiktede effekten?

Et viktig moment i systemdynamikken er at årsaken til et problem ofte ligger i strukturen til systemet vi undersøker. Målet er da å identifisere hvilke deler av systemet som kan påvirkes på en slik måte at utilsiktet effekt kan reduseres eller fjernes. I vår oppgave vil dette innebære å vurdere hvordan en kan oppheve eller redusere eventuelt negativ virkning av endringen innen risikobildet. Denne utfordringen gir oss det tredje og siste forskningsspørsmålet:

Forskningsspørsmål 3 Hvordan kan eventuell utilsiktet effekt minimaliseres?

1.4 Oppgavens bidrag

Implementasjon av NBF innebærer en signifikant endring av flere sentrale forhold i Forsvaret. Vi vil se store endringer relatert til for eksempel kommando og kontroll, informasjon og informasjonssystemer, organisasjonsstruktur, kompetanse, økonomi og prosesser for militære operasjoner. Det er sannsynlig at flere av disse endringene vil medføre utilsiktet effekt. Denne oppgaven vil bidra til økt presisjon og bedre forståelse for sammenhengen mellom risiko relatert til informasjonsinfrastrukturen og evne til å realisere den potensielle effektforbedringen i NBF gjennom:

- Økt innsikt i kausale sammenhenger (uttrykt ved en feedbackstruktur som forbinder bakgrunn, tiltak og effekt) gir bedre forståelse for hvordan tilsiktet effekt skal realiseres.
- Økt innsikt i kausale sammenhenger (uttrykt ved en feedbackstruktur som forbinder årsak og effekt) mellom implementasjon av NBF og informasjonssikkerhet gir bedre forståelse for hvordan utilsiktet effekt oppstår.
- Økt innsikt i vekselvirkningen mellom implementasjon av NBF og informasjonssikkerhet (representert ved kausale sammenhenger med eventuelle ikke-lineariteter, forsinkelser og feedback) gir bedre forståelse for hvordan utilsiktet effekt kan forringe eller forpurre tilsiktet effekt av NBF.
- Analyse av systemet for identifikasjon av generiske problemstrukturer med forslag til hvordan disse kan håndteres for å minimalisere utilsiktet effekt.

Forståelse for disse forholdene vil sette beslutningstakere med ansvar for å implementere NBF i Forsvaret et bedre grunnlag for å treffe valg som reduserer faren for Policy Resistance. Ved å vurdere hvordan intervensjonene over tid vil gi respons fra andre deler av systemet, vil de kunne utarbeide løsninger som gir større grad av måloppnåelse på både kort og lang sikt [33];

> Identifying and drawing out the behavior over time of key variables is an important first step toward articulating the current understanding of the system. Drawing out future behavior means taking a risk, the risk of being wrong. The fact is, any projection of the future will be wrong, but by making it explicit, we can test our assumptions and uncover inconsistencies that may otherwise never get surfaced.

De kvalitative modellene som utvikles i denne oppgaven kan benyttes som utgangspunkt for andre systemdynamiske studier av NBF på minst to mulige måter:

- Hele eller deler av modellen kan videreutvikles til kvantitative simulerbare modeller. Dette vil kunne bidra til økt presisjon og dybde i kunnskap relatert til problemstillingen.
- Den delen av modellen som beskriver tilsiktet effekt av NBF kan benyttes som utgangspunkt for å identifisere utilsiktede effekter relatert til andre områder enn informasjonssikkerhet. Den vil således kunne bidra til at en større del av "spekteret av utilsiktede effekter " kan avdekkes.

1.5 Rapportens struktur

Etter innledningen består rapporten av seks kapitler. Disse har følgende innhold:

Kap 2: Relatert litteratur Plasserer oppgaven i forhold til andre arbeider innen problemområdet og arbeider som har benyttet systemdynamikk for lignende problemstillinger. Identifiserer mangler ved tidligere arbeider som vi vil adressere i denne oppgaven.

Kap 3: Metode Begrunnelse for valg av metode, gjennomføring av datainnsamling og analyse, samt en beskrivelse av de systemdynamiske virkemidlene som anvendes i oppgaven.

Kap 4: Tilsiktet effekt I dette kapittelet utvikler vi versjon 1 og 2 av en dynamisk modell som viser henholdsvis bakgrunnen for NBF og hypotesen om hvordan NBF skal skape mil effekt. Modellen identifiserer sentrale variabler for tilsiktet effekt og deres kausale relasjon.

Kap 5: Utilsiktet effekt Med utgangspunkt i en definisjon av risiko for informasjonssystemer og variablene som endres for å oppnå tilsiktet effekt, utledes utilsiktet effekt. Vi utvider modellen fra kapittel 4 og viser hvordan utilsiktet effekt påvirker tilsiktet effekt.

Kap 6: Tiltak for minimalisering av utilsiktet effekt Analyse av hvilke tiltak en bør velge for å minimalisere utilsiktet effekt og motvirke Policy Resistance. Analysen omfatter identifisering av en problemarketype og en løsningsarketype, samt en konkretisering av hvilke tiltak som er mest hensiktsmessige. Kapittelet inneholder et forslag til policy som vil motvirke Policy Resistance ved implementering av NBF. Det utarbeides også en siste utvidelse av den dynamiske modellen som viser hvordan policyen motvirker utilsiktet effekt.

Kap 7: Konklusjon og forslag til videre arbeid Besvarer problemstillingen som ble fremsatt i rapportens første kapittel og angir noen problemstillinger som bør besvares i fremtidige arbeider.

1.6 Viktigste konklusjoner

Implementeringen av NBF avhenger av realiseringen av en informasjonsifrastruktur som skal knytte sammen tilnærmet alle enheter i Forsvaret. Den tilsiktede effekten er en økt evne til å skape militær effekt som en følge av at bedre informasjonskvalitet og informasjonsdeling gir bedre virkning per enhet og lavere tid per engasjement.

Den utilsiktede effekten av overgangen til et nettverksorganisert Forsvar er en økning av verdi, trussel og sårbarhet for den underliggende informasjonsinfrastrukturen. Med

andre ord er det slik at risikobildet for informasjonsinfrastrukturen øker dynamisk med graden av nettverksorganisering Forsvaret oppnår. Realiseringen av denne risikoen innebærer at trusselagenter vil gjennomføre et økt antall vellykkede logiske angrep mot informasjonsifrastrukturen. Denne utviklingen vil motvirke tilsiktet effekt ved at den reduserer informasjonskvalitet og informasjonsdeling i informasjonsinfrastrukturen.

En systemdynamisk løsning på denne situasjonen i Forsvarets favør innebærerer økt bruk av ressurser for å motvirke logiske angrep mot informasjonsinfrastrukturen parallelt med økningen av ressursbruk for nettverksorganisering. Dersom økningen i antall og virkningen av vellykkede logiske angrep kan motvirkes i tide og i nødvendig utstrekning samtidig som man implementerer NBF, vil det være mulig å oppnå den potensielle effektforbedringen som forventes av en nettverksorganisering av Forsvaret.

2 Relatert litteratur

Som en del av forbedredelsene til denne oppgaven har vi lest gjennom en relativt stor mengde litteratur om NBF. Vi har også kontaktet ulike kompetansemiljøer i Forsvaret for å forsikre oss om at den litteraturen vi har lest ansees som kjernelitteratur for emnet. Det har likevell ikke vært mulig å identifisere noen eksplisitte risikoanalyser for implementeringen av NBF i Forsvaret.

Det eksisterer en rekke dokumenter som beskriver hva NBF er og hvordan konseptet vil lede til økt evne for å skape militær effekt. Dette er i hovedsak dokumenter som er utgitt av Forsvarsdepartementet[34, 35, 36, 15, 37, 14], enheter i Forsvarets militære organisasjon (FMO) [38, 39, 40, 41, 6, 42, 43, 12, 5, 21, 44], Forsvarets Forskningsinstitutt [45, 13, 16] og en del organisasjoner som enten er en del av eller direkte knyttet til det amerikanske forsvaret [46, 7, 8, 10, 47, 9]. Flere av disse uttaler at informasjonssikkerhet er viktig for NBF, men ingen gir noen dypere vurderinger av hvorfor det er viktig eller hvilken relasjon det har til konseptets evne til å skape militær effekt. Det er heller ingen av dokumentene som gir noen vurdering av om behovet for sikkerhet vil endres ved implementeringen av NBF. De fleste dokumentene som uttaler seg om sikkerhet har også med et syn om at det er kryptologi som skal løse sikkerhetsproblemet. Vi mener at dette er et for snevert syn på en svært kompleks problemstilling. At sikkerhet er viktig i informasjonssystemer som benyttes til viktige oppgaver er det lett å si seg enig i. Kryptologi er en av flere mulige virkemidler en kan benytte for å sikre informasjon, men langt fra den eneste. Det er altså et behov for en analyse av hvordan overgang til et nettverksbasert konsept kan påvirke risiko relatert til informasjonssystemsikkerhet. Vår oppgave vil derfor være den første vi kjenner til som gjennomfører en risikoanalyse av implementeringen av NBF.

Som det fremgår av bibliografien har vi benyttet en anseelig mengde litteratur i arbeidet med denne rapporten. Siden vår metode er basert på litteraturstudier (i tillegg til intervjuer), mener vi det er mer naturlig at vi refererer til litteraturen der den er anvendt. Det gir etter vår mening en bedre flyt og helhet i oppgaven. For å bedre oversikten over anvendt litteratur i de ulike delene av rapporten, gis det en oversikt i innledningen til kapittel 4, 5 og 6. Oversiktene viser den mest sentrale litteraturen som er anvendt i forhold til emnet kapittelet omhandler.

Det eksisterer en mengde studier innen informasjonssikkerhet som benytter systemdynamikk som metode. Et arbeid som har vært en svært viktig motivator for vårt valg av denne metodikken er en risikoanalyse av overgangen til eDrift i den norske oljenæringen [48, 28, 49]. Situasjonen man står ovenfor der har mange likhetstrekk med Forsvarets overgang til et nettverksbasert konsept.

eDrift går i korthet ut på økt anvendelse av IKT i produksjon av petroleumsprodukter for å redusere kostnader, øke produksjon og øke levetiden for oljebrønner. IKT benyttes her for å bedre utnyttelsen av bore- og produksjonsdata, samt økt grad av samarbeide mellom personell på oljeplattformene og kontrollsentre på land. Konseptet muliggjøres ved at oljeplattformene knyttes sammen med et eller flere kontrollsentre ved hjelp av datamaskinbaserte nettverk. Endringen medfører at mange av oljeselskapenes

virksomhetskritiske prosesser blir avhengige av sikker drift av informasjonssystemene. I denne sammenhengen ble systemdynamikk anvendt for å analysere hvordan overgangen til eDrift kunne påvirke risikobildet for oljeselskapene, samt utlede tiltak for å minimalisere de identifiserte driverne for økt risiko. Studiet har resultert i en rekke interessante funn. Et av de mest sentrale er hvordan risikobildet for systemet er avhengig av hvordan en anvender ressurser for utvikling av arbeidsprosesser og utvikling av ny kunnskap for menneskene som skal fungere i de nye prosessene. Vårt fokus vil være noe mer teknisk rettet, men den overordende tilnærmingen vil være den samme; hvordan kan endringene NBF medfører over tid påvirke konseptets evne til å oppfylle tilsiktet effekt.

3 Metode

3.1 Valg av metode

Problemstillingen i denne oppgaven er etter vår mening klar og beskrivende [50]. Vi vurderer problemstillingen som klar siden det, hver for seg, eksisterer relativt mye kunnskap om NBF og risiko for informasjonssystemer. Det vi søker svar på i denne oppgaven er om det vil eksistere en vekselvirkning mellom implementasjon av NBF og grad av informasjonssystemsikkerhet i NBF. Vi ønsker videre å avdekke om dynamikken mellom disse to elementene over tid kan medføre en forringet eller forhindret måloppnåelse for NBF.

Problemstillingen er beskrivende siden vi fokuserer på å fremskaffe økt forståelse for dynamikken i et gitt tilfelle; ved implementasjon av NBF i Forsvaret. Generalisering er følgelig ikke et mål for denne undersøkelsen. Andre nasjoner som kan sammenlignes med Norge vil imidlertid trolig også kunne benytte seg av resultatet.

Vår vurdering av problemstillingen leder til et intensivt undersøkelsesopplegg [51] hvor vi konsentrerer oss om å gå i dybden for å forsøke og få en så helhetlig forståelse som mulig for problemstillingen i den aktuelle konteksten. Innsamling og analyse av data vil derfor utføres ved hjelp av kvalitative metoder [52]:

Datainnsamling Dokumentanalyse og en form for semistrukturerte intervjuer av en gruppe strategisk utvalgte eksperter.

Strukturering og analyse Kvalitative systemdynamiske teknikker; CLD-modeller og systemarketyper.

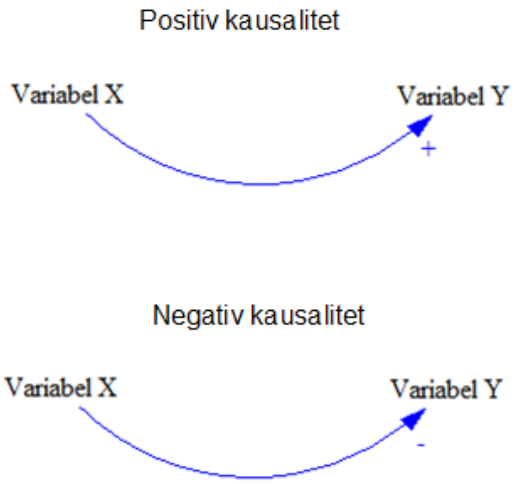
Valg av systemdynamikk som metode for strukturering og analyse bygger på en antakelse om at et slikt helhetlig syn på effekt av endring gir innsikt som leder til beslutninger med høyere grad av måloppnåelse. NBF representerer en stor endring for Forsvaret; det er en innovasjon som forventes å skape positiv effekt. En av de viktigste forutsetninger for at en innovasjon skal gi høyest mulig effekt er at en forstår hvordan den passer i organisasjonens situasjon og kontekst. Systemdynamikken er en metodikk som tilbyr et sett av verktøy for å forstå "det store bildet" i en slik situasjon. Systemdynamiske prosjekter starter som oftest med et problem som må løses eller en uønsket adferd som skal korrigeres eller unngås [53]. I vårt tilfelle er det den siste tilnærmingen som gjelder: vi ønsker å innføre NBF på en måte som gjør at uønsket adferd (utilsiktet effekt) ikke oppstår og forringer eller forpurrer den tilsiktede effekten av innovasjonen.

Som analysemetode er systemdynamikk fundamentalt forskjellig fra tradisjonelle former for analyse [54]. I bokmålsordboka defineres analyse som: "metode som går ut på å dele opp en helhet i mindre deler"[55]. I systemdynamikken fokuserer man ikke på individuelle delene av det som undersøkes, men på feedback relasjonene mellom det en undersøker og andre deler av systemet. Målet er å fange opp eventuelle vekselvirkninger mellom delene i et system som over tid kan motvirke måloppnåelse. CLD modeller er et verktøy som kan benyttes for å identifisere slike feedbacksløyfer i et system [56]. Vi vil derfor utvikle en CLD-modell for å fange opp feedbackstrukturene som virker mellom

intervensjonene ved implementasjonen av NBF og sikkerheten i de relaterte informasjonssystemene.

En CLD-modell består av to typer grunnleggende elementer; variabler og linker. En variabel er en tilstand, situasjon, handling eller beslutning som påvirker, og kan påvirke andre variabler. En variabel kan være kvantitativ (målbar, eks; produktivitet, profitt) eller kvalitativ ("myk", eks: motivasjon, tillit). En link indikerer en kausal sammenheng mellom to variabler, eller en endring i tilstanden for variablene. Det eksisterer to ulike typer kausale sammenhenger;

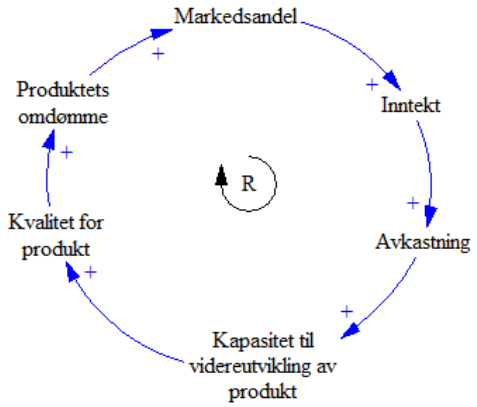
1. De to variablene kan variere i **samme retning**. En slik relasjon mellom to variabler benevnes **positiv kausalitet** (se øverste tegning i figur 2).Dette indikeres med et + tegn på linken (pilen) som knytter variablene sammen. Dersom variabel X øker, vil variabel Y også øke, og dersom variabel X reduseres, reduseres også variabel Y.
2. De to variablene kan variere i **motsatt retning** En slik relasjon mellom to variabler benevnes **negativ kausalitet** (se nederste tegning i figur 2).Dette indikeres med et - tegn på linken (pilen) som knytter variablene sammen. Dersom variabel X øker, vil variabel Y reduseres, og dersom variabel X reduseres, vil variabel Y øke.



Figur 2: Kausale linker mellom variabler

Når en gruppe variabler knyttes sammen i en sammenhengende løkke, kalles det en kausal løkke (engelsk: Causal Loops). En kausal løkke er et konseptuelt verktøy som avslører dynamiske prosesser hvor kjedeeffekten(e) av en årsak (cause) kan spores gjennom et sett av relaterte variabler, tilbake til den opprinnelige årsaken (effekt). Hver kausale løkke forteller en historie. Historien viser hvordan effekten av en årsak/endring etterhvert virker tilbake på den originale årsaken/endringen [57]. Et eksempel på en slik kausal løkke fremgår av figur 3. Figuren viser kjedeeffekten av en bedrifts kvalitetsforbedring på et produkt. Forbedring av kvalitet øker omdømme for produktet, som igjen øker markedsandelen for produktet (selger mer enn sine konkurrenter siden deres pro-

dukt har et bedre rykte), som igjen øker bedriftens inntekter, som igjen øker avkastningen, som igjen øker bedriftens mulighet for å forbedre produktet enda mer (får ressurser til videreutvikling). Til slutt lukkes den kausale løkken ved at forbedringen av produktet gir enda bedre kvalitet. Så gjentar løkken seg etter samme mønster.



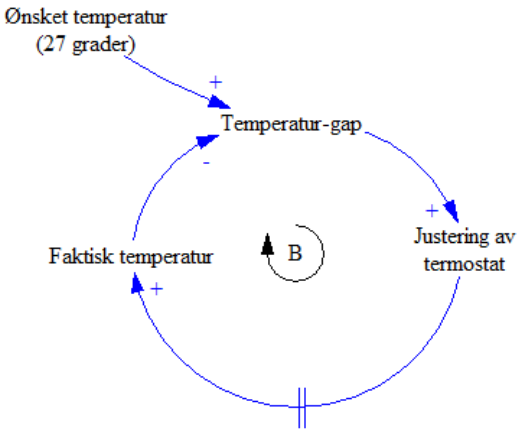
Figur 3: Kausal løkke (selvforsterkende)

Det eksisterer to ulike typer kausale løkker. Den første kalles en selvforsterkende løkke (engelsk: Reinforcing Loop) eller positiv feedback og markeres med en R. Slike løkker representerer voksende eller synkende effekt. Modellen i figur 3 er et eksempel på en selvforsterkende løkke med positiv effekt. Den viser at jo mer en bedrift satser på kvalitetsforbedring, jo mer vil de tjene og kunne forbedre sine produkter enda mer. Det er viktig å være klar over at hvordan en løkke utvikler seg er avhengig av konteksten. Som et eksempel kan en også tenke seg at dersom en bedrift satser mye penger på å forbedre et produkt, vil de måtte sette opp prisen på produktet. Dersom ikke kundene føler at kvalitetsforbedringen er verdt den økte prisen, vil bedriften selge færre av produktet. De vil da tjene mindre og har mindre penger til fortsatt produktutvikling, som til slutt resulterer i at de leverer et dårligere produkt enn sine konkurrenter, med den påfølgende reaksjonen at de selger enda mindre. Dette er et eksempel på en selvforsterkende løkke med synkende effekt.

Den andre typen kausale løkker kalles balanserende løkke (engelsk: Balancing Loop) eller negativ feedback og markeres med en B. Denne typen løkker søker stabilitet eller å bringe et system tilbake til et ønsket nivå. Et eksempel på en slik løkke kan være en termostat (se figur 4).

I et slikt system utgjør forskjellen mellom ønsket temperatur (27 grader) og den faktiske temperaturen i et rom et gap som utløser en justerende handling (dersom ønkset temperatur er høyere enn faktisk temperatur, økes mengden varme som tilføres rommet) av termostaten. Etter en forsinkelse resulterer handlingen i en justering av temperaturen i rommet. Altså reduseres gapet. Denne syklusen gjentar seg til gapet er lukket; når temperaturen i rommet har nådd ønsket temperatur.

I den siste løkken har vi et eksempel på en viktig egenskap i systemdynamiske modeller; forsinkelse. I et systemdynamisk perspektiv er en forsinkelse tiden mellom en årsak og en virkning (Markert i modellen i figur 4 som || på linken mellom justering av ter-



Figur 4: Balanserende kausal løkke (med tidsforsinkelse mellom justering av termostat og faktisk temperatur

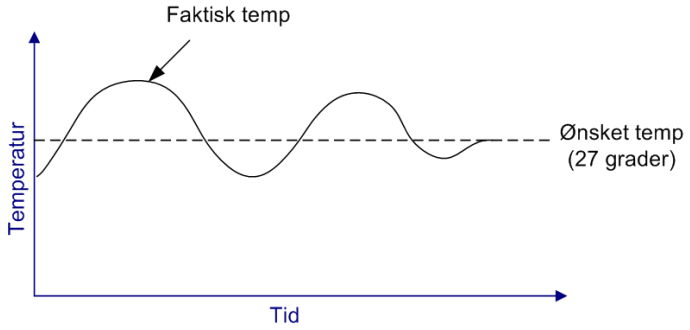
mostat og faktisk temperatur). Problemet med forsinkelser er at de kan forårsake at relasjoner mellom årsak og virkning tilsløres over tid og rom. Mangel på kjennskap til slike forsinkelser kan medføre feilaktig forståelse for hvordan et system fungerer med det resultat at en fatter feilaktige beslutninger. De kan medføre spesielt store utslag i balanserende løkker. Dersom vi vi benytter termostaten fra forrige eksempel, kan dette forklares som; jo større forsinkelsen er, jo større vil oscilleringen mellom ønsket og faktisk temperatur være og jo lengre tid vil det ta før systemet når sitt mål (at faktisk temperatur blir lik ønkset temperatur) og oppnår stabilitet.

I følge Coyle [58] er CLD-modeller viktige systemdynamiske verktøy som har flere ulike bruksområder;

1. De gir en kompakt beskrivelse av komplekse problemer som ellers kan kreve flere siders beskrivelse som ofte blir uoversiktlige.
2. De kan fungere som agenda og holde fokus for diskusjoner om det aktuelle problemområdet de beskriver. De har en fordel i forhold til tradisjonelle, serielle agendaer gjennom at de viser relasjonene mellom faktorene som duskuteres.
3. Identifisering av kausale løkker i diagrammer kan hjelpe til å forklare observert atferd i et problemdomene.
4. De kan danne grunnlaget for utvikling av kvantitative simulerbare modeller.

Et annet systemdynamisk verktøy som ofte benyttes sammen med CLD-modeller er "Behaviour Over Time" (BOT) grafer. BOT grafer viser utviklingsmønster for en variabel over tid [57]. Utviklingsmønsteret kan indikere variasjoner og trender for den aktuelle variabelen, for eksempel vekst, reduksjon, oscillering eller en kombinasjon av disse. I slike grafer viser x-aksen alltid tiden, mens y-aksen representerer en måleverdi for variabelen det er snakk om. BOT grafer benyttes for å indikere den overordnede retningen og variasjonen i variabelens utvikling, ikke den eksakte numeriske verdien for variabe-

len. De er således gode hjelpemidler for å kommunisere forventet utvikling for en gitt variabel. Figur 5 viser et eksempel på hvordan en BOT graf for utviklingen av variabelen temperatur-gap i termostat-systemet fra figur 4 kan se ut. Forsinkelsen medfører at faktisk temperatur oscillere rundt ønsket temperatur før den oppnår sitt mål og stabiliserer seg slik at faktisk temperatur er lik ønsket temperatur (gapet mellom ønsket temperatur og faktisk temperatur lukkes).



Figur 5: Behaviour Over Time (BOT) graf for variabelen temperatur-gap fra modellen i figur 4

Systemarketyper er CLD-modeller som viser generiske feedbackstrukturer relatert til kjente atferdsmøster (for eksempel “limits to growth ” og “fixes-that-fail”). De kan benyttes som verktøy for både diagnostisering av eksisterende problemer og fremtidsanalyse [59]:

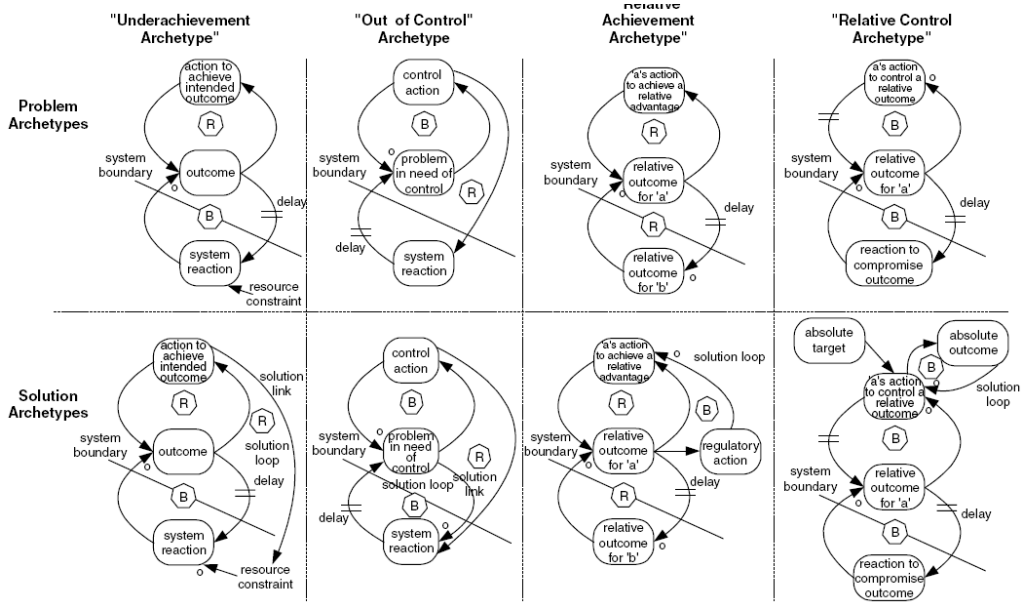
Diagnose Underliggende årsaksforhold kan identifiseres gjennom å påpeke systemarketyper i problemets systemstruktur.

Prognose Fremtidige utilsiktede konsekvenser kan identifiseres gjennom å påpeke systemarketyper i systemstrukturen for en foreslått løsning.

Disse egenskapene gjør at systemarketyper er egnet som verktøy for å vurdere om vekselvirkningen mellom implementasjon av NBF og sikkerhet i de relaterte informasjonssystemene kan medføre utilsiktede konsekvenser. Vi er spesielt interessert i om det kan oppstå forhold som vil lede til forringet eller forpurret måloppnåelse for NBF. Analyse av CLD-modellen vil derfor baseres på identifisering av systemarketyper da dette gir begrunnet prediksjon om mulige utilsiktede konsekvenser.

Systemarketyper ble initialt utviklet som frittstående systemdynamiske verktøy for å klassifisere generiske strukturer i systemer som medfører kjente atferdsmønstre over tid. De er et resultat av mange års erfaring med kvalitativ og kvantitativ systemdynamisk modellering og kan anvendes for å utvikle forståelse i nye anvendelsesområder [60]. Wolstenholme har vist at tidligere identifiserte systemarketyper bare er delvis generiske og at de kan slås sammen til et redusert sett bestående av fire generiske problemarketyper med tilhørende løsningsarketyper (se figur 6).

En problemarketype har som kjennetegn at dens atferd over tid ikke er sammenfallende med forventet effekt for den entiteten som initierte den. En løsningsarketype er



Figur 6: Fire generiske problemarketyper med tilhørende løsningsarketyper; R = forsterkende feedback løkke; B = balanserende feedback løkke; o = negativ kausalitet; system boundary = organisasjonsgrense [4]

et generisk forslag til hvordan utilsiktet effekt fra en problemarketype kan minimaliseres. Den grunnleggende strukturen i disse systemarketypene er en generisk arketype bestående av to feedback løkker. Den øverste løkken tilsvarer forventet effekt som er et resultat av handlinger iverksatt i en del av en organisasjon med en tilsiktet effekt som mål. Den nederste løkken tilsvarer utilsiktet effekt som er et resultat av en reaksjon fra en annen del av eller fra utsiden av organisasjonen. Streken som er merket med “system boundary” representerer en organisasjonsmessig grense som “gjemmer ”den utilsiktede effekten fra de som iverksatte handlingen med mål om en tilsiktet effekt. Dette fremhever at organisasjonsmessige grenser ofte er en avgjørende faktor for hvordan ulike systemer utvikler seg over tid. Det å eksplisitt identifisere slike grenser kan ofte forklare hvorfor en helhetlig, systemisk ledelse og utvikling er vanskelig.

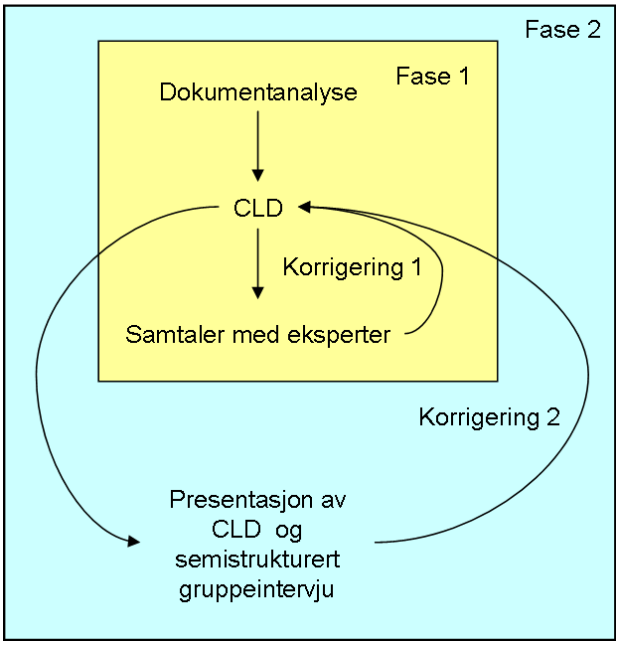
Det eksisterer flere ulike kilder for datainnsamling ved utvikling av CLD-modeller; artikler fra massemedia, historiske og statistiske dokumenter, policydokumenter, forskningsrapporter og intervju med interessenter (eng: stakeholders)[57]. En vanlig metode for den sist nevnte tilnærmingen er gruppeintervjuer med sentrale interessenter for problemstillingen [61]. I slike sesjoner søker man å eksternalisere en felles mental modell for relasjonen mellom variabler som er sentrale for problemstillingen[62, 63]. Modellen uttrykkes ved en CLD som dermed representerer feedbackstrukturen til systemet avgrenset av problemstillingen. Vi har i vår oppgave valgt en kombinert tilnærming til datainnsamling. Vi har benyttet dokumentanalyser og fortløpende samtaler med eksperter som grunnlag for utvikling av modeller. Disse ble deretter presentert for en annen gruppe eksperter med et påfølgende semistrukturert gruppeintervju for å avdekke om modellene var sammenfallende med deres oppfatning av problemstillingen. Årsaken til vår tilnærming er relatert til to forhold:

- Modellutvikling basert på gruppeintervjuer krever et team av modellutviklere [62]
- Det var vanskelig å samle alle ekspertene til en felles gruppeintervju. Problemet er relatert til at ekspertene vi hadde tilgang til var geografisk spredt og hadde svært stramme arbeidstidsskjemaer.
- Det er faglig krevende å gjennomføre gode gruppeintervju hvor en interaktivt utvikler CLD-modeller fortløpende. Siden forfatteren av denne rapporten har liten erfaring med systemdynamikk og slike gruppeintervjuer, var ikke dette gjennomførbart.

De påfølgende to kapitlene beskriver hvordan den valgte metoden ble anvendt i forhold til hvert forskningsspørsmål.

3.2 Utvikling av CLD-modell for tilsiktet og utilsiktet effekt

Utviklingen av CLD-modellen for de tilsiktede og utilsiktede effektene, samt relasjonen mellom dem ble utført i to faser (se figur 7). Fase 1 ble gjennomført i løpet av ca en måned, mens fase 2 ble gjennomført på en dag.



Figur 7: Utvikling av CLD-modell i to faser

Den første fasen startet med at forfatteren utviklet en initial CLD-modell på bakgrunn av informasjon i et utvalg av dokumenter. Dokumentene som ble benyttet ble valgt ut på grunnlag av kriterier som fremgår av tabell 1.

Kriteriene for utvalg av dokumenter for tilsiktet effekt er basert på en antakelse om at Forsvaret og politiske myndigheter (i stor grad representert ved Forsvarsdepartementet) er en pålitelig kilde til informasjon om den mentale modellen som ligger til grunn for NBF; deres syn på hvilket problem NBF skal løse og hvordan det løser det. Det teoretiske grunnlaget bak NBF er imidlertid i stor grad basert på amerikansk grunnlagslitteratur for NCW. Ved en del tilfeller var det nødvendig å referere denne litteraturen for å klargjøre forhold som ikke fremgikk eksplisitt i den norske.

Del av CLD	Kriterier
Tilsiktet effekt	1. Offisielle dokumenter utgitt av Forsvaret eller politiske myndigheter som beskriver bakgrunn for NBF, hva NBF er og/eller forventet effekt av NBF 2. Teoretisk grunnlag for dokumenter som tilfredsstiller ovenstående krav
Utilsiktet effekt	1. Offisielle dokumenter utgitt av Forsvaret eller politiske myndigheter som beskriver informasjonsinfrastruktur for NBF 2. Beskrivelser av sårbarheter i datamaskinbaserte informasjonssystemer fra pålitelige kilder 3. Beskrivelser av trusler mot datamaskinbaserte informasjonssystemer fra pålitelige kilder

Tabell 1: Kriterier for utvalg av dokumenter

Kriteriene for utvalg av dokumenter for utilsiktet effekt er relatert til avgrensningen i vår oppgave som tilsier at vi vurderer endringer i risikobildet for informasjonssystemer ved overgang til NBF. Risiko eksisterer der verdi, sårbarhet og trussel overlapper hverandre. Verdien til informasjonsinfrastrukturen er knyttet til hvordan den understøtter utførelsen av militære operasjoner. Dette er direkte relatert til tilsiktet effekt ved NBF og fremgår følgelig av denne. Utviklingen av sårbarheter er knyttet til egenskapene ved informsasjonsinfrastrukturen i NBF og til drivere for sårbarhet i slike systemer. Norge har etter den kalde krigen ingen fast definerte fiender og en trusselvurdering må følgelig baseres på generelle globale trender.

Den initiale CLD-modellen ble diskutert med eksperter fra Forsvaret. Utvalget av eksperter var basert på at de skulle inneha god kunnskap innen minimum et av følgende kompetansefelt;

1. Nettverksbasert Forsvar
2. Informasjonssikkerhet/risikoanalyse
3. Systemdynamikk

Tabell 2 gir en oversikt over organisasjonsmessig tilhørighet og kompetanseprofil for ekspertene som ble benyttet i begge fasene. Forkortelser i kolonne “Avdeling”: FSA/FSKI = Forsvarets sikkerhetsavdeling / Senter for beskyttelse av kritisk infrastruktur, FSS = Forsvarets skolesenter/Forsvarets Institutt for ledelse, FFI = Forsvarets Forskningsinstitutt, FSA led = Forsvarets sikkerhetsavdeling ledelse og INI FS07 = spesialutredning informasjonsinfrastruktur for Forsvarstudien 07. Forkortelser i kolonner under “Kompetanse”: NBF = Nettverksbasert Forsvar, IS/R = Informasjonssikkerhet/Risikoanalyse og SD = Systemdynamikk

Diskusjonene i fase 1 ble gjennomført som uformelle og semistrukturerte intervjuer med en og en ekspert. For eksperter som ikke hadde kjennskap til systemdynamiske metoder ble det gitt en beskrivelse av hva systemdynamikk er og en kort opplæring i CLD-modellering. Deretter ble eksperten presentert for modellen og en begrunnelse for alle variabler, kausale forhold og feedbackløkker i denne. Ekspertene ble så bedt om å kommentere modellen. Det overordene målet var å validere om modellen var sammenfallende med ekspertenes syn på hvordan forholdene relatert til problemstillingen ville

Fase	Avdeling	Kompetanse		
		NBF	IS/R	SD
1	FSA/FSKI	X	X	
	FSS/FIL	X		X
	FFI	X	X	
2	FSA led	X	X	
	INI FS07	X		

Tabell 2: Oversikt over organisasjonsmessig tilhørighet og kompetanseprofil for eksperter.

utvikle seg over tid. I forkant av diskusjonene var det utarbeidet noen spørsmål som var styrende for innholdet i samtalene:

1. Representerer de valgte dokumentene pålitelige/gode kilder for informasjon relatert til problemstillingen?
2. Kan du identifisere noen forhold i denne informasjonen som er feil tolket av forfatteren?
3. Er du enig i de påståtte kausale forholdene mellom variablene i modellen?
4. Er feedbackstrukturen i modellen sammenfallende med din oppfatning av forholdene i problemstillingen?
5. Kan du identifisere noen feil eller mangler i modellen?

Tilbakemeldinger fra ekspertene ble benyttet til å korrigere den initiale modellen (illustrert som "Korrigering 1" i figur 7). Denne korrigerte modellen ble så benyttet i fase 2 hvor den ble forelagt for en annen gruppe eksperter fra Forsvaret. I denne fasen ble det gjennomført en presentasjon av modellen for hele gruppen med en påfølgende diskusjon styrt etter samme spørsmål som ble benyttet i fase 1. Tilbakemeldingene ble benyttet til å korrigere modellen fra fase 1 (illustrert som "Korrigering 2" i figur 7). I begge fasene medførte tilbakemeldingen bare små justeringer av den initiale modellen. Det ble identifisert noen uklarheter i forbindelse med kausale påstander og variabler. Forfatteren endret modellen for å forbedre dens nøyaktighet relatert til disse forholdene. Hovedlinjene i feedbackstrukturen forble imidlertid uendret gjennom begge fasene.

3.3 Analyse av CLD-modell og forslag til intervensjon for å håndtere uønsket atferdsmønster

Målet med analysen var å vurdere om feedbackstrukturen i systemet avslørte forhold som over tid kan forringe eller forpurre oppnåelse av tilsiktet effekt for NBF. Analysen ble utført etter samme modell som utviklingen av CLD-modellen; forfatteren identifiserte systemarketyper i systemets struktur og benyttet disse til en prediksjon av systemets utvikling. Systemarketypene ble her brukt som et verktøy for å identifisere generiske strukturer i systemet som medfører kjente atferdsmønstre. Disse generiske problemstrukturene ble relatert til konteksten og det ble utviklet et forslag for intervensjon som skulle motvirke eller minimalisere den uønskede atferden. Analysen og forslag for intervensjon ble forelagt de samme gruppene av eksperter i to omganger sammenfallende med de to fasene i figur 7. Forfatterens analyse av modellen og forslag til intervensjon ble bifalt av ekspertene i begge fasene.

3.4 Verktøy

Alle systemdynamiske modeller i denne oppgaven ble utviklet ved hjelp av programmet Vensim® DSS for Windows Version 5.5d fra Ventana Systems Inc [64].

3.5 Reliabilitet og validitet

Vurdering av en oppgavens reliabilitet og validitet medfører implisitt en vurdering av oppgavens kvalitet. Validiteten forteller oss om oppgavens gyldighet; analyserer vi det som vår problemstilling skal avklare? [65]. Med reliabilitet mener man hvor pålitelig en undersøkelse er; Hvordan er den gjennomført og hvor nøyaktig man behandler dataene [65]. I kvalitativ forskning blir gjerne reliabilitet sammenfallende med validitet og kan derfor vanskelig studeres separat. I tillegg er ofte begrepsbruken i kvalitative studier noe anderledes enn i kvantitative studier (se tabell 3) [66]. Siden denne oppgaven er basert på et kvalitativt forskningsopplegg, vil vi i det følgende benytte det kvalitative begrepsapparatet.

Kvantitativt	Kvalitativt	Betydning av kvalitativt begrep
Reliabilitet	Troverdighet	En vurdering av om fremgangsmåten inngir troverdighet i forhold til konklusjonen
Validitet	Bekreftbarhet	Forståelsen forskeren kommer frem til skal kunne bekreftes
Generalisering	Overførbarhet	Kan forståelsen også gjelde i andre sammenhenger?

Tabell 3: Forskjeller i begrepsbruk for kvantitativ og kvalitativ metode

I utviklingen av systemdynamiske modeller er troverdighet knyttet til i hvor stor grad modellen gjenspeiler virkeligheten. En modell vil alltid være en begrenset og forenklet representasjon av virkeligheten og således aldri være fullstendig komplett, men noen modeller er "mer riktige enn andre"[67]. For at en systemdynamisk modell skal gi oss riktig innsikt som leder til god forståelse med påfølgende robuste beslutninger, må den vise en tilnærmet riktig gjengivelse av de dynamiske kreftene som virker innenfor det aktuelle problemområdet i den virkelige verden.

Våre primære virkemiddel for å oppnå en modell som i størst mulig grad gjenspeiler virkeligheten er baser på to forhold; utvikling av modeller på bakgrunn av relevant litteratur og validering av modellen og dokumentene av strategisk utvalgte fageksperter (se liste over krav for valg av eksperter i kapittel 3.2). Fremgangsmåten for modellutviklingen var som følger:

1. Det ble utarbeidet initiale kriterier for utvalg av dokumenter som skulle anvendes for utarbeidelse av de første utkastene til modeller (se tabell 1)
2. Et første utkast av modeller og en analyse av dem (kommunisert via systemarketyper) ble utviklet av forfatteren på bakgrunn av de utvalgte dokumentene. Valg av variabler og kausale linker ble i denne prosessen utelukkend basert på informasjon fra den utvalgte dokumentasjonen.
3. De første utkastene for både CLD-modeller og deres analyse i form av systemarketyper ble presentert og forklart for en gruppe fageksperter i en iterativ prosess (flere gjentakende møter over en lengre tidsperiode). Ekspertene ble bedt om å vurdere troverdigheten til både den underliggende litteraturen og selve modellene ut fra

en forhåndsdefinert liste med spørsmål (se kapittel 3.2)

4. Deretter ble de "validerte" modellene og deres analyse (systemarketyper) presentert og for en ny gruppe eksperter. Disse ble også bedt om å vurdere troverdigheten til både den underliggende litteraturen og selve modellene ut fra en forhåndsdefinert liste med spørsmål (se kapittel 3.2)

Denne fremgangsmåten sikrer at modellene ikke bare er et resultat av forfatterens tolkning av dokumenter avgrenset av hans kunnskap om litteratur innen problemområdet. Fagekspertene har bidratt til økt troverdighet gjennom sin kompetanse realtert både til utvalget av dokumenter og en validering av hvor godt forfatterens modeller sammenfaller med deres oppfatning av den virkelige verden. Deres innspill medførte justeringer av modellene fram til den formen de fremstår med i denne oppgaven. Modellene er således et produkt skapt ved en kombinasjon av mange ulike informasjonskilder.

For å sikre bekreftbarhet er det lagt stor vekt på å utarbeide en tekstlig beskrivelse av alle variabler, kausale linker og kausale løkker som benyttes i modellene. Det samme gjelder for de identifiserte systemarketypene med tilhørende BOT grafer som ble anvendt i analysen. Denne fremgangsmåten tilsier at det er god mulighet for utenforstående å vurdere grunnlaget for og tolkningen av modellene i oppgaven.

Som vi allerede har bemerket, er det ikke et mål for denne oppgaven å produsere forståelse som kan anvendes i andre sammenhenger. Forskningsopplegget er designet for å gi dybdekunnskap om problemområdet for Forsvaret. Det er imidlertid mulig at andre entiteter som kan sammenligne seg med Forsvaret og Forsvarets situasjon, kan anvende innsikten fra modellene som et utgangspunkt for egne studier. Det er trolig mange organisasjoner som befinner seg i en lignende situasjon som Forsvaret med tanke på at de ønkser å omstille seg for å kunne skape mer effekt gjennom kreativ anvendelse av IKT. Dersom disse organisasjonene i tillegg har et relativt likt trusselbilde som Forsvaret, er det sannsynlig at de vil oppleve å bli påvirket av de samme dynamiske forholdene som identifiseres i denne oppgaven.

4 Tilsiktet effekt for NBF konseptet

I dette kapittelet vil vi, med bakgrunn i dokumentstudier, utlede grunnlaget for at NBF skal være et sentralt konsept i utviklingen av Forsvaret og hvilken effekt en forventer at konseptet skal gi.

De mest dyptgående beskrivelser av bakgrunnen for NBF og den forventede effekten av konseptet vi har identifisert er stadfestet i et sett overordende strategiske dokumenter utviklet i forbindelse med Forsvarssjefens Militærfaglige Utredning 2003 (MFU03) og et dokument som beskriver fokus for Forsvarsstudie 2007 (FS07). Det er i tillegg benyttet et forprosjekt utarbeidet ved Forsvarets stabsskole som ble utarbeidet for å bygge opp kompetanse innen NBF.

Sluttrapporten i MFU03 bygger på innspill fra et sett med delutredninger og representerer Forsvarssjefens fagmilitære syn og anbefaling for hvordan Forsvaret bør innrettes for perioden 2005-2008 innenfor rammen av de overordnede politiske føringer som ble gitt. Den var i så måte et sentralt innspill til St.prp nr.42(2003-2004) Den videre moderniseringen av Forsvaret 2005-2008 [23] med tilhørende iverksettingsbrev[35]. Disse dokumentene regulerer på et overordnet nivå hvordan Forsvaret skal utvikle seg i den angitte tidsperioden. Her er transformasjon av Forsvaret med overgang til et nettverksbasert konsept et sentralt tema.

FS07 er forsvarssjefens fagmilitære innspill til hvordan Forsvaret skal utvikles i perioden 2009-2012. Studien skal munne ut i et helhetlig militærfaglig råd til forsvarsministeren og regjeringen høsten 2007. Forsvarssjefens anbefalinger vil bli vurdert politisk innenfor en større helhet, som et ledd i utarbeidelsen av regjeringens neste langtidsplan for Forsvaret i perioden 2009-2012. Hovedfokuset i dette studiet vil være å å kartlegge og anbefale tiltak for å utvikle et forsvar i langsiktig balanse når det gjelder sammenhengene mellom ambisjonsnivå og budsjetter. Arbeidet omfatter blant annet en vurdering av Forsvarets fremtidige struktur. Det er angitt at det i denne sammenhengen skal legges vekt på å utnytte ny teknologi og nettverksbaserte løsninger maksimalt. Altså ser vi en videreføring av tankene om NBF fra MFU03.

Alle dokumentene vi har hentet informasjonen om NBF fra er utarbeidet og publisert av sentrale aktører i Forsvarets militære organisasjon (FMO), Forsvarets forskningsinstitutt (FFI) og Forsvarsdepartementet, og utgjør således Forsvarets offisielle syn på konseptet. Tabell 4 gir en oversikt over de mest sentrale dokumentene i denne sammenhengen. Siden de fleste av disse dokumentene bygger på et teoretisk grunnlag for nettverksbasert krigføring som er utviklet i USA, vil det også benyttes dokumenter som beskriver dette teoretiske grunnlaget. Disse er omtalt i kapittel 4.5.1 og referert til der de benyttes i teksten.

Vi vil omsette informasjonen fra disse dokumentene til en kausal struktur i form av en CLD-modell som beskriver sentrale variabler og dynamikken mellom de impliserte variablene. Modellen vil vise hvilke krefter som driver overgangen til et nettverksbasert forsvar i Norge og hvilke tilsiktede effekter en forventer å oppnå. Den vil i neste omgang benyttes som utgangspunkt for å vurdere eventuelle utilsiktede effekter konseptet kan ha for risiko relatert til informasjonssikkerhet.

Årstall	Tittel	Beskrivelse
2001	Introduksjon til Nettverksbasert forsvar [21]	Forprosjekt fra Forsvarets stabsskole
2003	Forsvarssjefens militærfaglige utredning 2003 [39]	Sluttrapport for MFU03
2003	Konsept for nettverksbasert anvendelse av militærmakt [38]	Delutredning for MFU03
2003	Kommandokonsept i Nettverksbasert Forsvar [6]	Delutredning for MFU03
2003	Utnyttelse av vedtatt struktur i realiseringen av et nettverksbasert Forsvar [43]	Delutredning for MFU03
2003	Det nye Forsvaret [40]	Informasjonsmateriale ifbm MFU03
2003	Et nytt Forsvar for en ny tid [41]	Informasjonsmateriale ifbm MFU03
2003	Mot et nettverksbasert Forsvar [42]	Informasjonsmateriale ifbm MFU03
2003	Forsvarets konsept for nettverkssentrisk krigføring [5]	Foredrag av Forsvarssjef Sverre Diesen i Oslo Militære Samfund
2004	St.prp 42 (2003-2004) [23]	Politiske føringer for modernisering av Forsvaret i perioden 2005 til 2008
2004	Strategisk konsept for forsvaret i perioden 2005-2008 [36]	Angir det sikkerhets- og forsvarspolitiske grunnlaget for Forsvarets operative virksomhet i den angitte perioden
2005	Nettverksbasert forsvar (NBF) eller nettverkstilpasset forsvar (NTF)? [12]	Rapport fra arbeidsgruppe NBF: revisjon forsvarets felleoperative doktrine
2006	Derfor fornyer vi Forsvaret [34]	Informasjonsmateriale ifbm FS07

Tabell 4: Oversikt over litteratur for bakgrunn og forventet effekt av NBF

4.1 Bakgrunn: behov for militær effekt under endrede rammebetingelser

NBF og NCW er konsepter. De er beskrevet ved samlinger av hypoteser som angir hva konseptene går ut på og hvordan en mener de kan gi økt militær effekt. Vårt fokus er å identifisere hvilken effekt Forsvaret forventer av NBF og hvordan de mener denne effekten skal oppstå. Med andre ord ønsker vi å synliggjøre den mentale modellen Forsvaret legger til grunn for konseptet; deres tanker om hvilket problem NBF skal løse og hvordan NBF kan være en løsning på dette problemet.

Siden tidlig på 1990-tallet har det i Norge vært et sterkt fokus på et behov for transformasjon, en endring, av Forsvaret. Den viktigste bakenforliggende drivkraften til behovet for endring var slutten på den kalde krigen. Etter Sovjetunionens og Warsawapaktens fall var Forsvaret, på mange måter, "en løsning på et problem som ikke lengre eksisterte". Forsvaret var på denne tiden dimensjonert og organisert for å møte trusselen fra øst. Dersom man sammenholder informasjonskildene som er anvendt i dette studiet (se tabell 4) fremgår det fire sentrale argumenter for hvorfor en transformasjon må finne sted og hvordan dette gir nye rammebetingelser for "det nye Forsvaret ";

1. Sikkerhetspolitisk endring
2. Endring i det strategiske konseptet for NATO
3. Økonomiske bevilgninger til Forsvaret
4. Teknologisk utvikling innen IKT

De tre øverste argumentene henger, etter vår mening, tett sammen. De har alle hovedsakelig rotfeste i den senere tids endrede sikkerhetspolitiske rammebetingelser for hele

den vestlige verden. Fra andre verdenskrig og frem til Sovjetunionens og Warszawapaktens oppløsning tidlig på 90-tallet har dimensjonering, oppbygning og organisering av Forsvaret vært sterkt preget av den kalde krigen mellom øst og vest. Resultatet var en investering i et invasjonsforsvar som var relativt stort i volum og baserte seg på en mindre kjerne av fulltids yrkesoffiserer, verneplikt og mobilisering ved kriser hvor norsk territorie var truet. I dag er trusselbildet sterkt endret [68];

> Under den kalde krigen var trusselbildet klart definert. Trusselen var i hovedsak knyttet til en annen stats mulige vilje og evne til et angrep. I dag er trusselbildet mye mer sammensatt og uforutsigbart. Skillet mellom nasjonal og internasjonal sikkerhet er i ferd med å viskes ut, og kriser kan oppstå i glidende overganger mellom fred og krig. Trusselen kan like gjerne være en enkelt terrorist eller en spesiell interessegruppe som en stat. Vi står overfor såkalt asymmetriske trusler. Allerede lenge før 11. september 2001 hadde dette bildet begynt å avtegne seg. Terrorangrepene denne dagen bekreftet den nye virkeligheten med ekstrem tydelighet. Terrorisme, spredning av masseødeleggelsesvåpen, nye former for organisert kriminalitet og angrep på informasjonssystemene som styrer viktige samfunnsfunksjoner, er sikkerhetsutfordringer også for Norge. Det betyr at å beskytte Norge og norske interesser går ut over ensidig å verne om vårt territorium

Samtidig som det forutsigbare trusselbildet fra den kalde krigen er borte, har altså nye sikkerhetspolitiske utfordringer vokst frem. Konflikter med utgangspunkt i bl.a etniske, sosiale eller religiøse spenninger, samt terrorisme og andre typer asymmetriske trusler representerer en alvorlig utfordring for internasjonal stabilitet og sikkerhet. Det bærende prinsippet er at trusler mot Norge og norske interesser kan skapes av forhold og hendelser som i utgangspunktet har sitt utspring langt utenfor våre egne grenser. I følge norske sikkerhetspolitiske vurderinger kan slike utfordringer bare møtes gjennom felles innsats og et bredt internasjonalt samarbeid [69].

Denne endringen i trusselbildet gjør at Norge i dag har behov for et anderledes Forsvar enn det som var designet for den kalde krigen. De nye sannsynlige trusler og utfordringer vil normalt være av mindre omfang, men kan til gjengjeld utvikle seg svært raskt. og konsekvensene kan være store for Norges befolkning og norske interesser. Dette krever at utviklingen fra et statisk mobiliseringsforsvar i retning av et mindre forsvar som kan reagere raskere og med høy kvalitet.

For NATO har denne endringen i trusselbilde ført til samme behov for endring som vi ser for Forsvaret. Alliansen er utvidet fra å være et redskap mot fullskala krig til et mer generelt sikkerhetsmessig felleskap med en rekke nye utfordringer. Dette innebærer at NATO må være i stand til å stabilisere forholdene i sitt til en hver tid gjeldende interesseområde gjennom å forebygge eller intervenere i en rekke mindre situasjoner. Som for Norge innebærer dette at en endrer sitt strategiske konsept til å fokusere på å kunne utføre hurtige og fleksible deployeringer av stryker, også utenfor området som er geografisk avgrenset av medlemslandene. Dette innebærer at det er et mindre behov for at hvert medlemsland opprettholder store styrker som ikke lett kan flyttes.

Bortfallet av den massive og statiske trusselen fra den kalde krigen er også en driver for reduserte økonomiske rammer for Forsvaret. Tildelingene vil i fremtiden trolig økes noe per år, men Forsvarets ressursbruk som andel av bruttonasjonalprodukt (BNP) har sunket betraktelig de siste 10-15 årene [70]. Forsvarets økonomi presses gjennom både endret operasjonsmønster og en kostnadsvekst i virksomheten. Den nye uforutsigbare trusselen som fordrer fleksible, gripbare og deployerbare styrker krever en større andel

stående avdelinger og modernisering av Forsvarets materiell. Andre kostnadsdrivere er reallønnsveksten i samfunnet og en prisøkning for nytt forsvarsmateriell utover inflasjon [70].

Reduksjon av den forutsigbare trusselen for Norge og NATO, samt strammere økonomiske rammer gjør at Forsvaret er nødt til å reduseres i volum. Dette betyr at det i fremtiden vil bestå av færre enheter (personell og materiell). Dersom dette er den eneste endringe som foretas, vil det resultere i at Forsvarets militære effekt reduseres. Selv om denne påstanden er relativt intuitivt, har vi i her et behov for å beskrive en definisjon for militær effekt. Dette for å eksplisitt vise hvordan en reduksjon i antall enheter direkte kan påvirke Forsvarets militære effekt. I en delutredning for MFU03 [71] defineres militær effekt som:

> Dersom den opprinnelige effektivitet av en gitt del av organisasjonen (E_{total}) kan beskrives som antall våpensystemer (n) den kan sette inn mot motstanderen, multiplisert med den midlere virkning av hvert enkelt system ($V_{midlere}$), dividert på den tiden det tar å utløse engasjementet fra beslutning tas til ilden er effektiv (t), fremkommer følgende uttrykk;
>
> $$E_{total} = \frac{n \cdot V_{midlere}}{t}$$

Siden formelen angir militær effekt på en gitt del av organisasjonen, vil den kunne benyttes som et uttrykk for Forsvaret som helhet dersom man velger "den gitte delen"til å omfatte alle enheter i Forsvaret. Ut fra denne definisjonen ser vi at en reduksjon av antall enheter totalt i Forsvaret, vil påvirke en av variablene i ligningen direkte; antall våpensystemer som kan settes inn mot motstanderen (n). Dersom antall enheter totalt da reduseres, betyr dette at den totale effekten Forsvaret er i stand til å levere (E_{total}) vil reduseres.

Situasjonen vi da vil stå ovenfor er at en reduksjon i den statiske og oversiktlige trusselen fra den kalde krigen medfører tiltak som leder til et Forsvar som er mindre i volum og følgelig har lavere militær effekt. Dersom dette var den eneste endringen i det globale sikkerhetspolitiske bildet, hadde dette vært en tilfredsstillende situasjon. Den anvendte litteraturen slår imidlertid fast at vi ikke nødvendigvis ser en reduksjon i den totale trusselen mot Norge, men heller en endring i trusselbildet. Endringen er drevet av en rekke globale utviklingstrekk [72]:

Slutten på den kalde krigen Den kalde krigen hadde en intern kontrollerende funksjon på den måten at den virket samlende mot en ytre, felles fiende. Det var ikke rom for strid internt i medlemslandene eller mellom medlemslandene. Etter at denne kontrollen er borte, har det blusset opp en rekke stridigheter som følge av nasjonale, etniske, kulturelle og religiøse konflikter. Mange av disse har dype historiske røtter som har fått en renessanse i maktvakuumet etter den kalde krigen.

Økt globalisering Globalisering i form av en mer integrert verdensøkonomi og gjensidig økonomisk avhengighet har vokst i styrke de senere år. På grunn av nasjonenes ulike evne til å tilpasse seg denne nye situasjonen, oppstår det tapere og vinnere. Slike motstridende utviklingstrekk kan bidra til destabilisering, rivalisering og konflikt mellom og innenfor stater. Globaliseringen påvirker også kulturelle, ideologiske og religiøse forhold. Den voldsomme økningen i utvikling og spredning av

informasjon kan gi tilgang til nye ideer og ny kunnskap til samfunn som tidligere var relativt skjermet fra omfattende påvirkning. Dette kan oppfattes som en trussel mot nasjonens levestett, egenart og normative verdier. Følgelig kan aktørene som oppfattes som de sterkeste bidragsytere til globaliseringen fremstå som en trussel. Mottiltak mot disse vil kunne omfatte internasjonal terrorisme.

Begrensede ressurser Den stadige befolkningsveksten i verden fører til at det i en del geografiske områder oppstår knapphet på ressurser. Som følge av dette kan det oppstå kamper om livsnødvendige midler som mat, vann og lignende. Demografisk skjevhet medfører at det oppstår et økt skille mellom fattige og rike i verden. Befolkningsveksten er helt klart størst i utviklingsland, det gir knapphet av ressurser i land som i utgangspunktet er dårlig stilt fra før. Denne urettferdigheten i ulike levevilkår vil kunne medføre en økt trussel for at fattige land er villige til å bruke militær makt for å utjevne forholdene.

Utvikling og spredning av ny teknologi Spredning av informasjonsteknologi, missilteknologi og masseødeleggelsesvåpen har økt dramatisk de siste 30 årene. Dette innebærer at de ikke lengre er forbeholdt et begrenset antall ressursterke land. Mange av de land og ikke-statlige aktører som ønsker tilgang til masseødeleggelsesvåpen og deres leveringsmidler, har et til dels anstrengt forhold til internasjonale forpliktelser og de verdier og prinsipper som er nedtegnet i FN-pakten og folkeretten. Dette medfører at det globale sikkerhetsbildet påvirkes i negativ retning.

På bakgrunn av disse utviklingstrekkene har en i Norge utviklet et sett med fire alternative utviklingstrender over hvordan en mener det er mulig at risikobildet vil utvikle seg i fremtiden. De fire mulige utviklingstrendene er [36]:

1. At omfanget av risikoer og trusler mot den kollektive sikkerhet og internasjonal fred og stabilitet gradvis reduseres (en positiv utviklingsretning)
2. At omfanget av sikkerhetsutfordringer som må håndteres på kort og midlere sikt vedvarer eller øker i antall og eventuelt intensitet, men uten at den mer langsiktige utviklingen dreier i en negativ retning (en usikker utviklingsretning)
3. At omfanget av sikkerhetsutfordringer øker i så stor grad i antall og intensitet, at den kollektive sikkerhet og internasjonal fred og stabilitet blir klart svekket også på lengre sikt (en negativ utviklingsretning)
4. At Norge og NATO igjen blir utsatt for en konvensjonell trussel som krever bruk av større militære styrker for å ivareta militær avskrekking og kollektivt forsvar, eller at Norge og NATO blir utsatt for en kjernefysisk trussel (en dyster utviklingsretning)

I Norge har man kommet frem til, etter en samlet vurdering av de globale utviklingstrekkene, at en vil legge til grunn en usikker utviklingsretning (alternativ 2) for deres sikkerhetspolitikk. Dette medfører at militærmakt, på kort eller midlere sikt, fortsatt vil være et viktig sikkerhetspolitisk virkemiddel for Norge. Denne erkjennelsen kan stå i konflikt med en reduksjon av Forsvarets reduksjon av militær effekt. Det har ikke vært mulig for oss å identifisere om en vurderer det slik at den samlede effekten fra de dynamiske og uoversiktlige truslene som har vokst frem vurderes likt med det omfanget den statiske og oversiktlige trusselen fra den kalde krigen representerte. Med andre ord er det vanskelig å identifisere om en mener at størrelsen av trusselen mot Norge er lik det den var

under den kalde krigen og at den eneste endringen som har skjedd er at trusselen har endret form. Det virker imidlertid som om det er politisk enighet om at trusselen mot Norge er av en slik karakter at det fremdeles er behov for at Forsvaret må kunne levere en betydelig militær effekt [36];

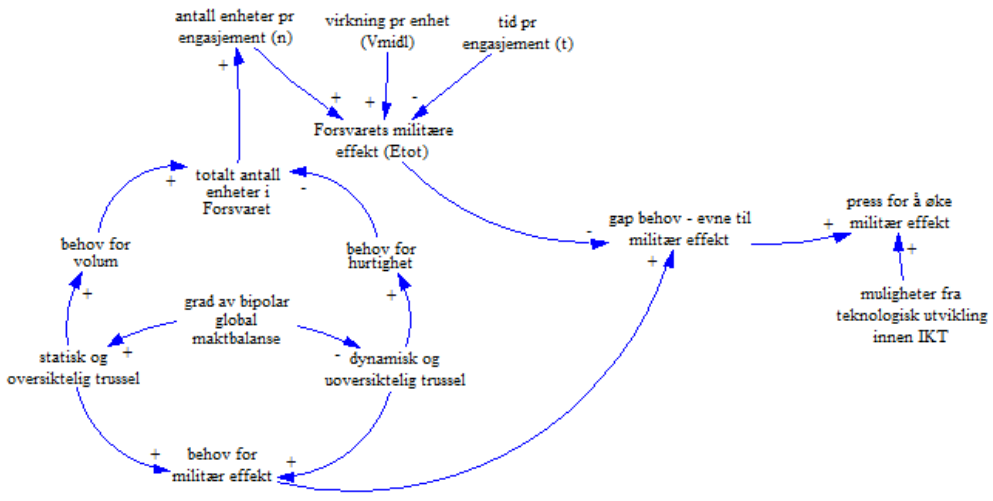
> På kortere og midlere sikt vil alle utviklingsretninger kreve et internasjonalt militært engasjement av et omfang som neppe blir mindre enn det som har vært tilfelle de senere år.

Problemstillingen en da står ovenfor i Norge er at en ønsker å redusere Forsvarets volum (som vi tidligere har vist medfører redusert militær effekt), samtidig som det eksisterer en betydelig trussel som krever et Forsvar som kan levere høy grad av militær effekt. Altså trenger Forsvaret et konsept som gjør det mulig å levere en like høy militær effekt med færre enheter.

Det siste argumentet for behovet for en transformasjon av Forsvaret er knyttet til den teknologiske utviklingen inne IKT. Dette argumentet bygger på en observasjon av hvilke endringer IKT har ført til i det sivile samfunnet. Det private næringslivet og offentlige institusjoner over store deler av verden har i de senere år benyttet IKT som middel for å øke effektivitet og inntjening. IKT fremstår alstå som en attraktiv teknologi med tanke på effektivitetsøkning. Forsvaret ser et behov for å identifisere hvordan også de kan benytte denne teknologien for å øke effekten av sin egen organisasjon.

4.2 CLD-modell av drivere for anvendelse av NBF konseptet

I dette kapittelet har vil omsatt informasjonen som ble identifisert i forrige kapittel til en kvalitativ kausal struktur i form av en CLD-modell. Denne viser årsak-virkningssammenhenger i den den aktuelle problemstillingen. Modellen (se figur 8) tar utgangspunkt i argumentene for hvorfor en ønsker å innføre NBF i Norge og viser hvilke konsekvenser det vil få for Forsvaret.



Figur 8: Drivere for anvendelse av NBF konseptet

I forrige kapittel viste vi at det er en nær sammenheng mellom de tre første argumentene for hvorfor vi trenger en transformasjon av Forsvaret. Kjernen til disse argu-

mentene ligger i en endring i trusselbildet for Norge. Endringen er preget av en reduksjon av en global bipolar maktbalanse. Den statiske og oversiktlige trusselen som den kalde krigen representerte reduseres, samtidig som det vokser frem en ny dynamisk og uoversiktlig trussel som følge av en rekke globale utviklingstrekk. En del av de den nye trusselen oppstår som en følge av at gamle trusselen forsvinner. Denne dynamikken oppstår som en følge av at balansen mellom de to sidene i den kalde krigen la lokk på mange latente stridigheter innenfor egne områder. Da den kalde krigen tok slutt, oppstod det et maktvakuum som gav rom for at mange av disse blusset opp til krig [73];

> Når denne situasjonen (slutten på den kalde krigen) forandret seg, ble også spenningsnivået senket flerfoldige hakk. Men samtidig kom et mangfold av konflikter opp til overflaten, som tidligere enten var blitt holdt i sjakk av terrorbalansen, var blitt feilaktig tolket i lys av den, eller på annen måte var direkte influert av den. Paradoksalt nok førte den kalde krigens slutt til ny usikkerhet på den internasjonale arena.

Denne sammenhengen vises i modellen ved en positiv kausalitet mellom variabelen *"grad av bipolar maktbalanse"* og variabelen *"statisk og oversiktlig trussel"*. På samme tid oppstår det en negativ kausalitet mellom variabelen variabelen *"grad av bipolar maktbalanse"* og variabelen *"dynamisk og uoversiktlig trussel"*. Disse samtidige kausale sammenhengene betyr at når graden av bipolaritet i den globale maktbalansen reduseres som et resultat av slutten på den kalde krigen, skjer det en endring av trusselbildet for Norge. Den statiske og oversiktlige trusselen reduseres samtidig som den dynamiske og uoversiktlige trusselen øker. Denne dynamikken påvirker igjen to andre sentrale variabler; *"totalt antall enheter i forsvaret"* og *"behov for militær effekt"*. Den første variabelen reduseres som en følge av at variablene *"behov for volum "* og *"behov for hurtighet"* henholdsvis reduseres og økes. Dynamikken i disse variablene er knyttet til dreiningen av fokus i Norges sikkerhetspolitikk som oppstod etter den kalde krigen. Det tradisjonelle fokuset var statssikkerhet hvor sikkerhetspolitikkens formål var knyttet til forsvar av statsmakten og dens grunnleggende interesser. Et slikt invasjonsforsvar var basert på den statiske trusselen fra Warszawapaktlandene generelt og Sovjet spesielt. Norges tilnærming til denne trusselen var å opprettholde et Forsvar med stort volum som var sikret gjennom obligatorisk førstegangstjeneste og mobilisering dersom Norges suverenitet var truet. Siden denne trusselen nå er redusert, ser vi følgelig et redusert behov for å opprettholde Forsvarets volum. I modellen vises dette som en positiv kausalitet mellom variablene *"statisk og oversiktlig trussel "* og *"behov for volum "*. En reduksjon i den siste variabelen tilsier at vi i fremtiden skal ha et Forsvar med færre enheter. Dette fremgår av modellen som en positiv kausalitet mellom variabelen *"behov for volum"* og *"totalt antall enheter i Forsvaret"*.

De nye sikkerhetsutfordingene etter den kalde krigen har ført til økt vekt på samfunssikkerhet og menneskelig sikkerhet. Samfunnssikkerhet dreier seg om å ivareta sivilbefolkningens trygghet og beskytte sentrale samfunnsfunksjoner og viktig infrastruktur mot angrep og annen skade i situasjoner der statens eksistens som sådan ikke er truet. Menneskelig sikkerhet omhandler beskyttelse av enkeltmennesket, der menneskerettighetene og ikke minst retten til liv og personlig trygghet står i sentrum. Det nye trusselbildet består av elementer som terrorisme, spredning av masseødeleggelsesvåpen, borgerkriger med store lidelser for landets sivilbefolkning og angrep på infrastrukturer som styrer viktige samfunnsfunksjoner. Da disse truslene kan oppstå hurtig og utenfor Norges grenser, har man et økt behov for et Forsvar som på kort tid kan deployeres til innsats der det

trengs, uavhengig av geografisk lokasjon. Dette betyr at vi ser et økt behov for hurtig reaksjon. En slik lav reaksjonstid kan vanskelig realiseres ved hjelp av et Forsvar basert på mobilisering og stort volum. Den nye tiden tilsier med andre ord behov for en økning i evne til hurtig reaksjon. I modellen vises dette ved en positiv kausalitet mellom *"dynamisk og uoversiktlig trussel"* og *"behov for hurtighet"*. Siden nødvendig hurtighet ikke kan oppnås med dagens volum, tilsier en økning i behov for hurtig reaksjon at antall enheter i Forsvaret bør reduseres i fremtiden. Derav den negative kausaliteten mellom mellom *"behov for hurtighet "* og *"totalt antall enheter i Forsvaret"*.

En oppsummering av de to siste avsnittene viser at endringen i trusselbildet medfører at vi i framtiden har behov for et Forsvar som er mindre i volum og har større evne til hurtig reaksjon. Dette medfører at Forsvaret vil reduseres i antall enheter. Med utgangspunkt i definisjonen for militær effekt som vi benyttet i forrige kapittel, ser vi at om dette er den eneste endringen som foretas, vil det bety at Forsvaret i fremtiden vil få redusert evne til å levere militær kapasitet. Årsaken er at dersom man reduserer det totale antallet enheter i Forsvaret, vil det være færre tilgjengelig for anvendelse i engasjement.

Modellen viser en kausal fremstilling av definisjonen i samspillet mellom variablene *"antall enheter pr engasjement (n) "*, *"tid pr engasjement (t) "*, *"virkning pr enhet ($V_{midlere}$)"* og *"Forsvarets militære effekt (E_{total})"*. I følge definisjonen kan den militære effekten økes dersom antall enheter som benyttes pr engasjement og/eller den midlere virkningen av disse enhetene økes. På samme måte vil en økning kunne realiseres gjennom å redusere tiden en bruker på å gjennomføre et engasjement. Følgelig har de to første variablene en positiv kausalitet og den siste en negativ kausalitet med variabelen *"Forsvarets militære effekt (E_{total})"*.

På samme tid som Forsvarets evne til å levere militær effekt reduseres, skjer det en endring i trusselbildet for Norge. Endringen er trolig ikke i størrelse, men heller i form. Vi har tidligere vist at samtidig som den statiske og oversiktlige trusselen fra den kalde krigens tid forsvinner, oppstår det en økning i den dynamiske og uoversiktlige trusselen. Det er tilnærmet umulig å måle disse formene for trussel opp mot hverandre med tanke på om den samlede trusselen mot Norge øker eller minker. Det som imidlertid er klart er at en forventer at det i fremtiden fortsatt vil eksistere en reell trussel mot Norge. For å oppnå sikkerhetspolitisk balanse er Norge til enhver tid nødt til å dimensjonere Forsvarets evne til å levere militær effekt slik at det kan håndtere den eksisterende trusselen. Med andre ord vil Norges behov for militær effekt som sikkerhetspolitisk virkemiddel kunne endres over tid. Siden den dynamiske trusselen mot Norge øker samtidig med at den statiske trusselen reduseres, antar vi at den totale trusselen er noen lunde lik i størrelse. Følgelig vil Norges behov for militær effekt også holdes relativt konstant. I modellen fremgår dette ved henholdsvis positiv og negativ kausalitet mellom variablene *"statisk og oversiktlig trussel"*, *"dynamisk og uoversiktlig trussel"* og *"behov for militær effekt"*.

Situasjonen vi da står ovenfor er at endringen i Norges trusselbilde fører til to motstridende forhold. På den ene siden resulterer det i en redusert evne for Forsvaret til å levere militær effekt gjennom at Forsvaret reduseres i antall enheter. På den andre siden ser vi at behovet for å kunne levere militær effekt holder seg konstant gjennom at den totale trusselen mot Norge trolig ikke vil endres. Behovet for sikkerhetspolitisk balanse fører til at uoverensstemmelsen gir et politisk press for å øke den militære effekten på tross av at Forsvaret skal bestå av færre enheter. I modellen fremgår dette av at en reduksjon i variabelen *"Forsvarets militære effekt"* samtidig som variabelen *"behov for militær effekt"*

holder seg konstant, vil gi en økning av variabelen *"gap behov - evne til militær effekt"*, som igjen bidrar til en økning av variabelen *"press for å øke militær effekt"*.

Den siste variabelen i modellen er relatert til argumentet som omhandler IKT som en attraktiv kilde for effekt-forbedringer i Forsvaret. Som vi viste i forrige kapittel har en registrert at utviklingen innen IKT har gitt opphav til radikale effekt-forbedringer innen privat og offentlig sektor. En regner følgelig med at utviklingene innen IKT også vil kunne være en sterk kilde for en forbedring av Forsvaret. Denne muligheten vil være med på å drive presset for økning av militær effekt. Følgelig har variabelen *"muligheter fra teknologisk utvikling innen IKT "* en positiv kausalitet med *"press for å øke militær effekt "*. Utvikling i IKT bidrar altså til økning av presset fordi en mener at det innehar potensiale for økning av effekt.

4.3 Oppsummering av drivere for NBF-konseptet

Den kausale modellen i forrige kapittel er utledet fra informasjon om hvordan politiske og fagmilitære autoriteter i Norge mener at endringer i rammevilkår medfører et behov for transformasjon av Forsvaret. Modellen tar utgangspunkt i at det, på et høyt aggregeringsnivå, er hovedsakelig to rammevilkår som er endret: trusselbildet og potensiale for effekt-forbedring i anvendelse av IKT.

Endringen i trusselbildet medfører en uoverensstemmelse mellom hvilken militær effekt Forsvaret kan levere og hvilket behov Norge har for militær effekt for å oppnå sikkerhetspolitisk balanse. Uoverensstemmelsen oppstår som et resultat av at den militære effekten som kan leveres reduseres samtidig som behovet for militær effekt holder seg konstant.

Den senere tids utvikling innen IKT representerer en mulighet for effektforbedring. En ser at dette er utnyttet i privat og statlig sektor, og forventer at det samme vil være mulig for Forsvaret dersom en finner en adekvat anvendelse av teknologien.

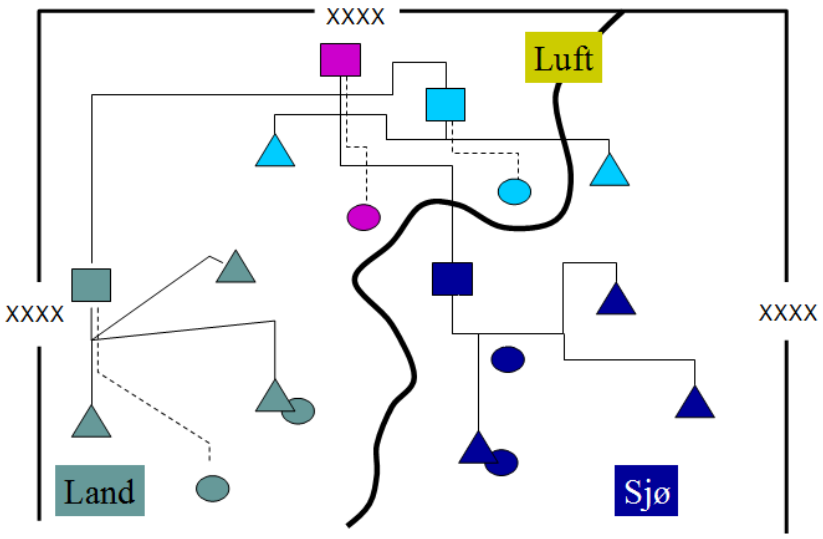
Disse to forholdene vil sammen virke for å øke det politiske presset for å øke militær effekt som kan leveres på tross av at det skjer en reduksjon av antall enheter i Forsvaret. Gapet mellom militær effekt som kan leveres og behovet for militær effekt utgjør en sikkerhetspolitisk utfordring. Potensialet for effektforbedring som ligger i anvendelse av IKT fremstår som en sterk kandidat for å løse denne utfordringen.

4.4 Hvilke endringer nettverksbasert konsept medfører

Utfordingen Forsvaret står ovenfor er altså at de har mindre evne til å levere militær effekt enn det den sikkerhetspolitiske tilstanden tilsier at det er behov for. I følge norsk syn er det her den teknologiske utviklingen innen IKT, operasjonalisert gjennom konseptet NBF har sitt virke. Konseptet skal gjøre det mulig å hente ut mer effekt per enhet enn hva en kunne tidligere. En kan med andre ord si at konseptet er en konkretisering av hvordan en kan anvende teknologiske fremskritt innen IKT for å tette gapet mellom behovet for militær effekt og den effekten som kan leveres av et forsvar med redusert antall enheter.

4.4.1 Tradisjonell organisering av forsvaret: plattformbasert forsvar

I den tradisjonelle organiseringen av Forsvaret opererer styrkene etter en modell hvor man har avgrenset ansvarsområde relatert til hvilken forsvarsgren en tilhører og hvilket geografisk område en er tildelt. Dette kan illustreres ved hjelp av et forenklet operasjonskart som vist i figur 9.



Figur 9: Plattformbasert organisering med statisk inndeling i rom (ansvarsteiger) og grenvis ansvarstildeling [5]

Operasjonskartet viser den tradisjonelle måten å organisere seg på i Forsvaret og dette konseptet benevnes plattformbasert forsvar. Rektanglene representerer kommandoplasser (ledelseselementer), ellipsene sensorer og trekantene våpenplattformer. Fargene viser hvilken forsvarsgren (hæren, sjøforsvaret og luftforsvaret) de ulike komponentene tilhører. Linjene mellom elementene viser kommando- og kommunikasjonsstrukturer.

I et plattformbasert konsept er våpenplattformene (for eksempel en stridsvogn, en fregatt eller et jagerfly) basis for den operative tenkningen. Her "eier" plattformene sitt eget våpen, og våpnene har ofte sine egne integrerte sensorer. I tillegg har hver forsvarsgren noen dedikerte sensorer, ledelseselementer med tilhørende kommando og kommunikasjonsstrukturer. Radio er ofte det primære kommunikasjonsmiddelet for å formidle situasjonsbildet og utføre ledelse av våpenplattformene. Integrasjon av av informasjon og koordinering av oppdrag på tvers av forsvarsgrenene utføres høyt oppe i organisasjonshierarkiet (markert i figuren ved et lilla ledelseselement som "eier" en egen sensor og er knyttet til et ledelseselement i hver forsvarsgren. I dette konseptet er forsvarets operative struktur basert på at hver forsvarsgren er tilpasset for å understøtte sine egne våpenplattformer. Dette medfører at hver forsvarsgren har et begrenset situasjonsbilde og typer våpenplattformer de kan sette inn mot fienden.

Situasjonsbildet er avgrenset til det behovet en har for å lede egne våpenplattformer. Et eksempel på dette kan være at Luftforsvaret har en kjede av radarer som genererer et situasjonsbilde av det som foregår i luften innen deres geografiske ansvarsområde. Dersom deres domene (luftrommet) i det geografiske området befinner seg over landjord eller sjøen, har de få eller ingen sensorer som samler inn situasjonsinformasjon fra disse domenene.

Typen våpenplattformer de kan sette inn er avgrenset til plattformer som er optimalisert for det domenet de skal håndtere. Disse plattformene er ikke alltid optimale i forhold til de fiendtlige målene de trenger å bekjempe. Dette kan eksemplifiseres med en situasjon hvor det er behov for å ta ut en liten patrulje av soldater til fots på landjorda

innenfor et geografisk område hvor Luftforsvaret er tildelt ansvar. Det er sannsynligvis ikke mest hensiktsmessige å benytte et jagerfly i denne settingen, men det kan hende det er det eneste alternativet dersom man har behov for å håndtere situasjonen raskt.

Det plattformbaserte konseptet innebærer også en statisk inndeling i rom (ansvarsteiger). Dette betyr at dersom en fiende benytter store deler av sin styrke til å angripe innenfor en ansvarsteig, kan en oppleve en situasjon hvor vi lokalt sett er "underbemannet " innenfor denne teigen, mens man samtidig har uvirksom kapasitet i en annen teig. En tilsvarende utfordring kan oppstå innenfor en ansvarsteig, men på tvers av forsvarsgrenene. Det er selvfølgelig ikke slik at det ikke er mulig å flytte styrker mellom teiger i dette konseptet, men det er en tidkrevende prosess. I forrige kapittel så vi at Forsvaret skal reduseres i antall enheter, altså vil det bli færre enheter fra hver forsvarsgren (og totalt) for å møte fienden innenfor hver ansvarsteig.

Selv om antall enheter en militær sjef råder over har direkte innvirkning på hvilken militær effekt han er i stand til å generere, er det også av avgjørende betydning hvordan disse enhetene benyttes for å oppnå høyest mulig effekt. Ledelse av militærmakt benevnes å føre kommando. Kommando kan defineres som [6]:

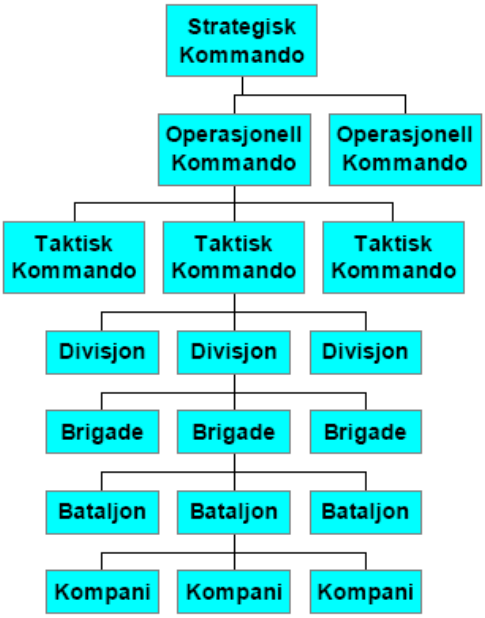
> Kommando er den myndigheten og det tilhørende ansvar en militær sjef tildeles til å skape en felles intensjon og å omgjøre denne til synkroniserte handlinger med involverte militære styrker.

Kommando utøves gjennom et kommandosystem, som er de strukturer og prosesser som etableres for å omgjøre intensjon til handling. Hensikten med et kommandosystem er å muliggjøre effektiv kommando. Systemet består av både en struktur og prosesser, altså noe vi gjør og noe som eksisterer. Det sentrale i prosessen er å fatte beslutninger; bestemme hvordan vi vil håndtere innsatsrommet.

Informasjonsteknologi har vist seg å ha en sterk innvirkning på hvilke løsninger vi kan velge innen kommandosystem og beslutningsprosesser. I det tradisjonelle Forsvaret har man begrenset kommunikasjon mellom aktørene i organisasjonen. Dette medfører at man har valgt å lage en struktur med et hierarki av ledere med kommunikasjon seg i mellom som leder underlagte enheter direkte. På denne måten utfører sjefen kommando over plattformene i de ulike forsvarsgrenene gjennom hierarkier av mellomledere. Strukturen er nødvendig for å koordinere situasjonsbildet fra aktørene og for å lede dem gjennom utførelsen av beslutningene som fattes. Resultatet er at det plattformbaserte forsvaret i Norge ledes gjennom en sterkt hierarkisk kommandostruktur. Dette fremgår av figur 10 som er et eksempel på et typisk organisasjonskart for en tradisjonell militær organisasjon.

Dersom en benytter organisasjonsteoretikeren Mintzbergs organisasjonsformer som beskrivelsesgrunnlag, kan organiseringen i det plattformbaserte forsvaret betegnes et maskinbyråkrati. Dette er en organisasjonsform som gir lite rom for hurtighet og fleksibilitet [6]:

> I maskinbyråkratiet er mellomlederne bindeleddet mellom den strategiske topp og utøverne. Mellomlederne koordinerer aktiviteten til utøverne. Utøvelsen er standardisert rundt arbeidsprosessene og koordineringen krever direkte tilsyn med virksomheten. Dette resulterer i at antallet underlagte ledd som en mellomleder makter å følge opp, er relativt få. Mellomlederen har da et lite kontrollspenn. Dette forholdet fører til at antallet vertikale organisasjonsnivåer øker, og ledelsesformen blir sterkt sentralisert.



Figur 10: Eksempel på tradisjonell kommandostruktur [6]

> Regler, prosedyrer og kontroll gjennomsyrer organisasjonen og mellomlederne er gitt avgrenset myndighet i forhold til disse faktorene.

Siden kommunikasjonen i slike organisasjoner er formell og følger hovedsakelig de vertikale linjene (kommandonivåene), medfører det at hurtigheten i beslutningsprosessen (informasjonsformidling, distribusjon av oppdrag, ordre og intensjoner) blir lav.

4.4.2 Fremtidens organisering av forsvaret: nettverksbasert forsvar

Den senere tids utvikling innen informasjonsteknologi har muliggjort en ny tilnærming til hvordan vi kan organisere og gjennomføre militære operasjoner. Den sentrale tanken i NBF er å benytte de økte mulighetene og kapasiteten i datamaskinbaserte informasjonssystemer til å overkomme en del av utfordingene i den tradisjonelle måten å organisere og lede militære styrker på [38, 21]

> Det norske begrepet NBF er en norsk tilpasning av det amerikanske “Network-Centric Warfare” (NCW) som er et konsept, en ide, for hvordan militære operasjoner kan gjennomføres ved å knytte sammen militære kapasiteter i nettverk ved bruk av informasjonsteknologi.
>
> Alle konseptene som er knyttet til NCW forutsetter nettverk eller en informasjonsinfrastruktur (infostruktur). Nettverkene er altså ikke en del av “Network-Centric Warfare”, men en forutsetning for å tale om denne type konsepter. Det som er den konseptuelle utfordringen er altså et Forsvar som skal utvikles på basis av en nettverksstruktur i motsetning til i dag hvor plattformene er basis for vår operative tenkning. Nettverket gir like lite som plattformene stridseffekt - det er de kapasiteter som knyttes opp i nettverket eller, som i dag, plasseres på plattformene som skal gi denne. Derfor mener vi at en rimelig norsk oversettelse vil være Nettverksbasert Forsvar som er en annen konseptuel modell å bygge Forsvaret på enn et plattformsbasert Forsvar.

I et nettverksbasert forsvar fokuserer en ikke på plattformenes forsvarsgrenvise tilhørighet, men ser på alle enheter i Forsvaret som komponenter som opererer i hele innsatsrommet og et sett med forbindelser mellom dem. Komponentene er inndelt etter sin hovedfunksjon i tre kategorier:

Sensorer Komponenter med sansing som hovedfunksjon. Sensorer omfatter alle komponenter som bidrar til bevissthet om innsatsrommet. Dette kan være en radar eller observasjoner utført av menneskelige aktører.

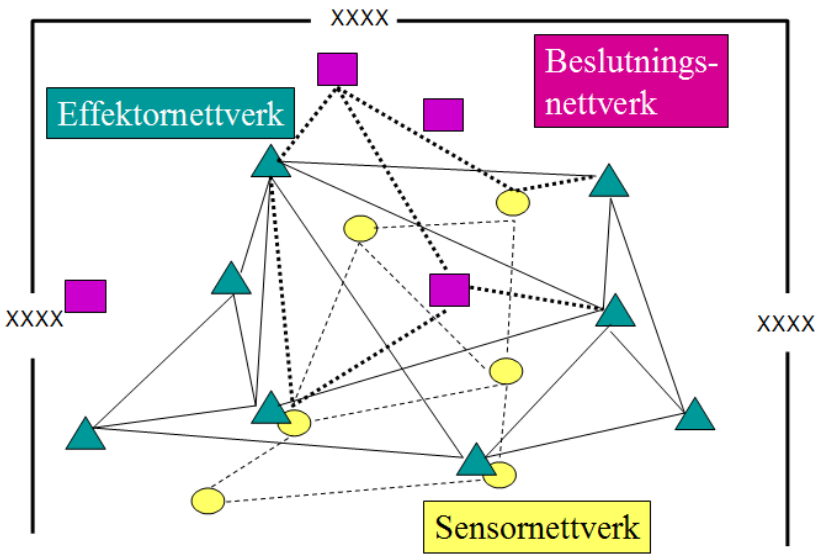
Beslutningstakere Komponenter med beslutning som hovedfunksjon. Sentrale oppgaver for disse vil være beslutning om rekonfigurering av organisasjonen, prioriteringer og allokering av ressurser til bekjempelse av mål

Effektorer Komponenter med oppnåelse av en våpenvirkning eller annen effekt med stridsverdi som hovedfunksjon.

Forbindelsen mellom disse komponentene skal realiseres av en høyteknologisk informasjonsinfrastruktur (INI) med stor kapasitet for å samle inn, behandle og distribuere informasjon. Sensorene samler inn informasjon om hele innsatsrommet (på tvers av de tidligere separerte domenene land, sjø og luft) som korreleres og distribueres til beslutningstakere og effektorer. Alle beslutningstakere får dermed forbedret informasjonsgrunnlag for sine valg av handlinger. Ordre om utførelse av handlingene kan hurtig distribueres til de effektorene en mener er best skikket for et aktuelt engasjement (uavhengig av hvilken forsvarsgren de tilhører). Effektorene har allerede de data de trenger for å utføre engasjementet gjennom informasjonen de har fått fra sensorene. Etter engasjementet er gjennomført kan effektorene rapportere hvor vellykket det var tilbake til beslutningstakeren som igjen tilpasser sine planer i henhold til dette. Som vi ser innebærer konseptet en tanke om opphevelse av statisk inndeling i rom (ansvarsteiger) og grenvis ansvarstildeling (land, sjø, luft). Forsvarets organisasjon fremstår dermed som en samling av komponenter som kan anvendes slik det til enhver tid vurderes mest hensiktsmessig i forhold til situasjonen. Dette fremgår av figur 11, som er en visuell fremstilling av hvordan komponentene er spredt ut i hele innsatsrommet og knyttet sammen ved hjelp av INI.

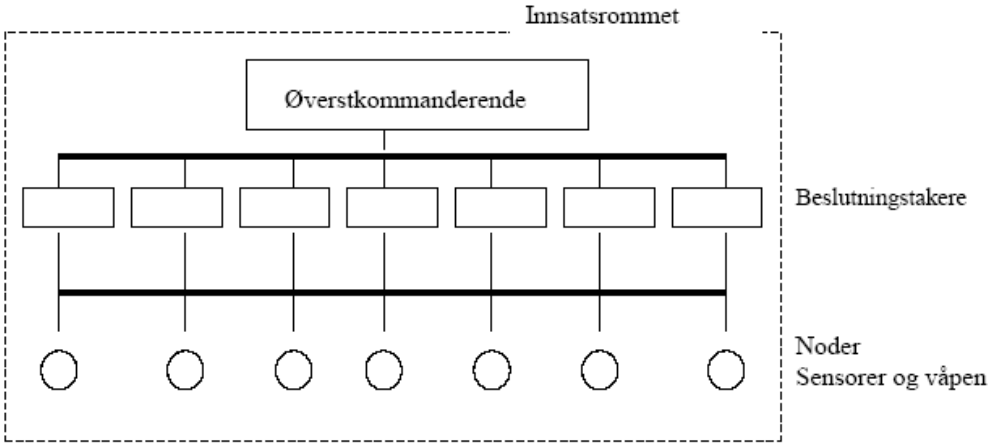
Denne måten å disponere de militære enhetene på skal kombineres med et økt innslag av avstandsleverte presisjonsvåpen (effektorene). Kombinasjonen av et forbedret situasjonsbilde over hele innsatsrommet og slike våpen, er en viktig faktor i hvordan NBF skal levere økt militær effekt i forhold til et plattformbasert forsvar. Effekten skal oppstå ved at man kan utføre prioriteringer av mål på tvers av hele innsatsrommet og kraftsamle den mengde og sammensetning av effektorer som vil gi størst virkning. Siden både beslutninger om engasjement og effektuering av beslutningen vil gå raskere som en følge av forbedret situasjonsbevissthet og evne til å spre informasjon, vil organisasjonen som en helhet også være i stand til å gjennomføre flere engasjement per tidsenhet enn tidligere. Det skal med andre ord bli mulig å gjennomføre flere engasjement med høyere militær effekt per tidsenhet.

Den store økningen i muligheter for kommunikasjon mellom de ulike aktørene i NBF, muliggjør et nytt kommandosystem og raskere prosesser. Siden alle aktørene har tilgang til et felles oppdatert situasjonsbilde (generert fra sensornettverket) og alle kan raskt kommunisere med hverandre, kan en øke beslutningskomponentenes kontrollspenn og



Figur 11: Nettverksbasert organisering med helhetlig fokus på hele innsatsområdet [5]

eliminere mange kommandonivåer. Beslutningstakerne mottar sjefens intensjon og samhandler om å benytte nodene som er tilgjengelige i innsatsrommet for å realisere denne. Dette gir en betraktelig flatere organisasjon med mulighet for raskere beslutningsprosesser. Et eksempel for hvordan en kan utforme organisasjonen er illustrert i figur 12.



Figur 12: Eksempel på mulig kommandostruktur i NBF[6]

Vi ser at denne er betraktelig flatere enn den organisasjonsformen som er fremtredende i et plattformbasert forsvar og det er mulig med direkte kommunikasjon mellom sjefen og beslutningskomponentene. Denne måten å organisere seg på, gir igjen mulighet for raskere og bedre beslutningsprosesser [6]

> Det er et nettet informasjonssystem, som omfatter og støtter alle prosessene, som vil muliggjøre synkroniserte handlinger og dermed synkroniserte effekter. Det er dette

> som bidrar til å øke kvaliteten og tempoet i beslutningsprosessen og som bidrar til synkronisering i utførelsen av beslutningene. Det muliggjør også større kontrollspenn og dermed færre nivåer, som igjen betyr raskere vertikale prosesser, og dermed høyere tempo.

Av dette sitatet ser vi at endringene innen organisering og beslutningsprosesser er basert på endringer i hvordan en kan samle inn, behandle og distribuere informasjon. Informasjon og informasjonsinfrastrukturen i NBF er med andre ord svært sentral for utviklingen av økt militær effekt.

4.5 Utvidelse 1 av CLD-modell: Tilsiktede effekter ved NBF

4.5.1 Kilder for kunnskap om teoretisk grunnlag for NBF

NBF lanseres i den anvendte litteraturen som et konsept for hvordan en kan utføre militære operasjoner. Et konsept defineres i FFOD som en grunnleggende idé eller skisse til hvordan et problem eller en oppgave kan løses [74]. Det er altså snakk om en alternativ metode for utførelse av militære operasjoner. Behovet for en ny metode har oppstått (ref figur 8) som et resultat av at Forsvaret skal redusere sitt totale antall enheter. En slik reduksjon vil, basert på opprettholdelse av det tradisjonelle konseptet for utførelse av militære operasjoner (plattformbasert forsvar), resultere i en mindre evne til å levere militær effekt. Da behovet for militær effekt ikke antas å reduseres, oppstår det et gap som må dekkes for å oppnå sikkerhetspolitisk balanse. Siden NBF lanseres som en metode for å møte denne utfordringen, betyr det at den nye måten å utføre militære operasjoner på, må muliggjøre en økt effekt per enhet i Forsvaret (ref ligning om militær effekt). I et systemdynamisk perspektiv skal NBF altså være det tilsiktede tiltaket som skal lukke gapet mellom behov og evne til å lever militær effekt. For å modellere dette i en CLD-modell må vi identifisere hvilke variabler som påvirkes ved innføringen av NBF og hvordan den kausale sammenhengen mellom disse medfører en feedback-sløyfe som gir den ønskede effekten.

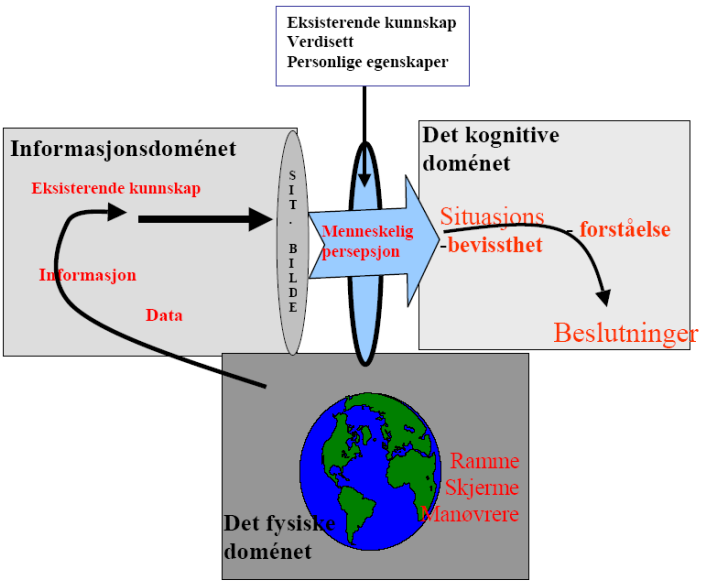
Det norske begrepet NBF har en nær tilknytning til det amerikanske konseptet Network Centric Warfare (NCW) [38]. Den teoretiske forankringen som legges til grunn for effektskapningen i NBF er hovedsakelig basert på forskning med tilhørende litteratur utført av institusjoner underlagt det amerikanske forsvarsdepartementet. En spesielt sentral aktør innenfor feltet er Command and Control Research Program. Litteratur om NCW er benyttet som sentral referanselitteratur i de viktigste dokumentene som beskriver NBF. Relasjonen mellom NBF og NCW er noe uklar. Noen av de norske grunnlagsdokumentene beskriver NBF som en direkte oversettelse av det amerikanske begrepet NCW [21], mens andre omtaler NBF som en tilpasning av det amerikanske begrepet [38]. Det har imidlertid ikke vært mulig å identifisere en beskrivelse av hva denne tilpasningen innebærer. Det eksisterer ingen beskrivelser av hva som eventuelt skiller NBF fra NCW. For den videre diskusjonen innebærer dette at NBF og NCW antas å bygge på det samme teoretiske grunnlaget og være identiske begreper.

4.5.2 Militær effekt som resultat av tilstand i tre domener

NBF er et relativt nytt begrep. Vi kjenner i dag ikke til noen nasjon eller koalisjon av nasjoner som fullt ut har realisert konseptet ved å organisere hele sin forsvarsmakt etter en nettverksbasert modell. På dette stadium i utviklingen av konseptet, eksisterer nettverksbasert tenkning hovedsakelig som et lenket sett av hypoteser om hvordan

en nettverksorganisering av styrker vil resultere i mer effektiv utførelse av militære operasjoner. Hypotesene representerer altså det teoretiske grunnlaget for hvordan nettverksorganisering forventes å gi økt militær effekt.

Alle hypotesene tar utgangspunkt i betydningen av informasjon i krigføring. Tradisjonelle sammenligninger av evne til å skape militær effekt har ofte vært basert på antall enheter på hver side i en konflikt. Det antas at dette er et for snevert syn på hvilke momenter som styrer en forsvarsmakts evne til å skape militær effekt. Grad av effekt kan trolig utledes av en syntese av relative fortrinn innen flere arenaer [7]. Eksempler på elementer som kan virke på dette forholdet er; informasjon, kunnskap, ledelse og moral. Teorien som ligger til grunn for nettverkstenkningen tar utgangspunkt i betydningen av informasjon i krigføring. Hvordan informasjon påvirker ens evne til å utføre militære operasjoner, forklares med en modell som knytter sammen tre domener (se figur13).



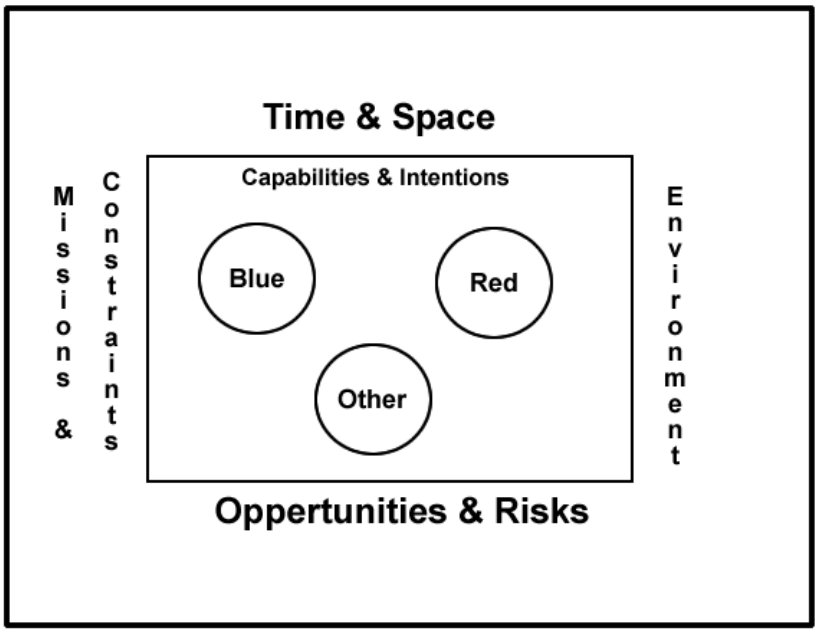
Figur 13: De tre domener for militære operasjoner [6]

Det fysiske domenet er hvor den aktuelle situasjonen som forsvarsmakten søker å påvirke eksisterer. Det er hvor de fysiske plattformene og informasjonssystemene som binder dem sammen oppholder seg. Domenet spenner over alle tradisjonelle miljøer for krigføring; land, sjø og luft. Hendelser i dette domenet ansees som virkeligheten.

Informasjonsdomenet er hvor informasjon skapes, manipuleres og deles. I dette domenet skapes og distribueres informasjon om hendelser og tilstander i det fysiske domenet. Foruten direkte observasjoner, påvirker vår interaksjon med dette domenet all vår informasjon om forhold i det fysiske domenet, det er med andre ord grunnlaget for vårt situasjonsbilde. Denne informasjonen kan ha ulike grader av riktighet. En annen viktig egenskap ved dette domenet er at her utføres kommunikasjonen som er påkrevd for kommando og kontroll av alle enhetene som deltar i operasjonene. Et sentralt element i denne sammenhengen er spredning av sjefens intensjon; hva han ønsker at enhetene skal oppnå.

Det kognitive domenet omfattes av alle beslutningstakernes kognitive prosesser. Her

eksisterer fenomener som persepsjon, bevissthet, forståelse, tro/overbevisning og verdier. Disse fenomenene spiller en viktig rolle i vår tolkning av informasjonen fra informasjonsdomenet. Dersom en definerer begrepet situasjonen som en tilstad som eksisterer i hele eller deler av innsatsrommet på et gitt tidspunkt, beskriver begrepet situasjonsbevissthet bevissthet om denne tilstanden. I en militær setting består situasjonen av en rekke komponenter (se figur 14): Oppdrag og begrensninger i oppdraget legger rammen for hva



Figur 14: Situasjonen er definert av tilstanden for en rekke komponenter i innsatsrommet [7]

som skal utføres og eventuelle begrensninger i hvordan en skal gå frem. Kapabiliteter og intensjoner for egne (blå) og fiendens (rød) styrker, samt viktige attributter i miljøet (for eksempel terreng og vær) er svært sentrale for vurderingen av muligheter og risiko. Forholdet mellom tid og rom kan også spille en sentral rolle. Dette kan for eksempel være relatert til rekkevidde av våpen eller hastighet en kan forflytte seg med i ulike typer terreng.

Situasjonsbevisstheten oppstår ved at situasjonsbildet som presenteres fra informasjonsdomenet vil tolkes individuelt av hver beslutningstaker (persepsjon er hvordan du oppfatter, tolker og bearbeider det du sanser). På denne måten oppstår det en forståelse for situasjonen som igjen vil legges til grunn for hvilke beslutninger en tar for hvordan en vil håndtere den aktuelle situasjonen. Resultatet av de kognitive prosessene er altså beslutninger; valg om hvordan vi vil forholde oss til tilstanden i det fysiske domenet. Disse beslutningene vil så omsettes til handlinger som iverksettes i det fysiske domenet.

Dersom en aksepterer at krigføring påvirkes av forhold i disse domenene, innebærer det et syn om at økt militær effekt kan oppnås gjennom forbedringer innen alle disse domene. Dette skiller seg fra det tradisjonelle synet om at militær effekt er hovedsakelig et resultat av styrkeforhold i det fysiske domenet.

4.5.3 Historiske utfordringer og mulige løsninger i informasjonsalderen

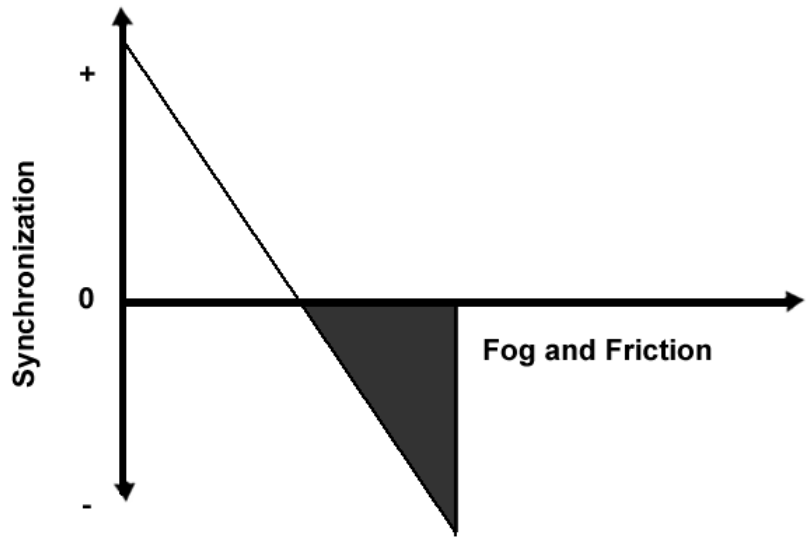
Selv om styrkeforhold tradisjonelt sett har vært vurdert ut fra forhold i det fysiske domenet, har informasjon alltid spilt en sentral rolle i krigføring. To av historiens mest sentrale personer innen militærteori, adresserer dette på følgende måte;

> Know the enemy and know yourself; in a hundred battles you wil never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or loosing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril.[75]

> War is the realm of uncertainty; three quarters of the factors on which action is based are wrapped in a fog of greater or lesser uncertainty [76]

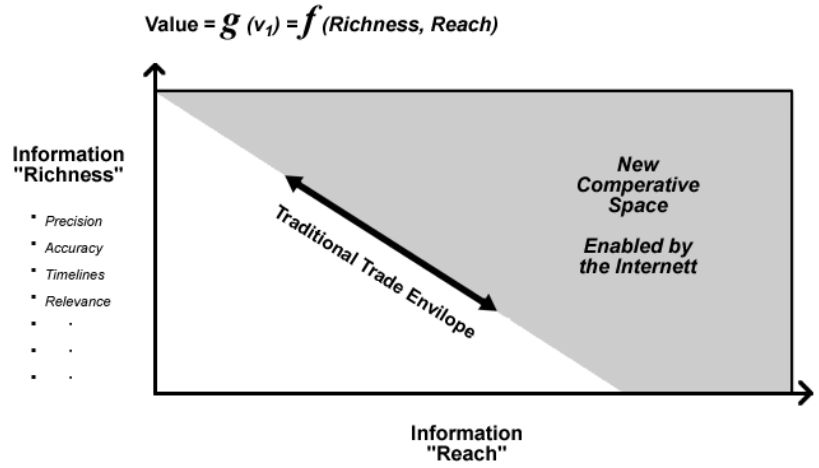
Det første sitatet er hentet fra Sun Tzu's "The Art of War". Han peker på behovet for kunnskap relatert til to av de mest sentrale komponentene av vår tidligere definisjon av situasjonen (se figur 14); egne styrker og fiendens styrker. Implisitt i dette utsagnet ligger det et syn på at kunnskap om disse komponentene vil gi deg mulighet til å treffe kvalitativt gode beslutninger som vil lede til bedre ytelse i det fysiske domenet.

Det andre sitatet er hentet fra Carl von Clausewitz' "Vom Kriege". Sitatet har gitt opphavet til begrepet "Fog of War", som beskriver tradisjonell usikkerhet relatert til situasjonsbevisstheten som oppleves av beslutningstakerne i krigføring. Usikkerheten oppstår som et resultat av liten tilgjengelighet til informasjon om situasjonen. Denne usikkerheten har nær tilknytning til et annet sentralt begrep i Clausewitz' lære; friksjon. Friksjon er relatert til problemer med utførelse av militære operasjoner; forhold som forpurrer utførelsen planen. Dårlige beslutninger som følge av lite informasjon kan være en sentral driver i dette forholdet. Det er sannsynlig at grad av "Fog of War" og friksjon er omvendt proporsjonalt korrelert med evne til å oppnå synkronisering av utførelse i militære operasjoner. Det vil igjen resultere i lavere effektivitet (se figur 15)



Figur 15: Forholdet mellom grad av "fog ", friksjon og evne til synkronisering i utførelse av militære operasjoner [7]

Historisk sett har forsvarsmakter måtte operere i det mørke området av figuren (figur 15). Årsaken var lav evne til å samle inn og distribuere informasjon om situasjonen (fog i forhold til planlegging), samt begrensede muligheter for kommunikasjon under utførelse (friksjon i forhold til koordinering av utførelsen av planen). Den senere tids utvikling innen informasjonsteknologi har skapt et mulighetsrom for å redusere disse utfordringene. Resultatet av denne utviklingen kan beskrives ved hjelp av begreper utviklet av forskerne Evans og Wurster. I sin bok "Blown to Bits: How the New Economics of Information Transforms Strategy" [77] har de utviklet en teori hvor overføring av informasjon defineres som en byttehandel mellom "richness" og "reach". Reach defineres som en aggregert verdi for grad av deling av informasjon og richness er definert som en aggregert verdi for informasjonskvalitet [7]. Teorien sier at tradisjonelt har man måtte velge mellom disse to variablene når man ønsket å distribuere informasjon. Jo høyere reach, jo lavere richness og omvendt. Et eksempel på dette kan være reklame for et produkt. En avisartikkel vil ha relativt god reach; den vil kunne nå mange mennesker. Den vil derimot bestå av en statisk tekst som gir liten richness. I den andre ytterenden av skalaen kan promotering av produktet utføres av en selger direkte til en potensiell kunde. I dette tilfelle vil en ha høy grad av richness (kunden kan interaktivt kommunisere med selgeren), men reach vil være lav; den når kun denne ene kunden. Utviklingen innen informasjonsteknologi (prosesseringskraft, båndbredde, lagringskapasitet, osv) har medført at man nå kan oppnå høy grad av richness og reach samtidig. Evans og Wurster hevder at et informasjonsmiljø's potensielle evne til å skape verdi er en funksjon av både richness og reach (se figur 16)



Figur 16: Forholdet mellom richness, reach og potensiell evne til å skape verdi[7]

På grunn av begrensede faktorer i tradisjonell informasjonsmiljøer, var man tidligere tvungen til å velge mellom richness og reach ved distribusjon av informasjon. Dette forholdet fremgår av modellen som det hvite området merket "Traditional Business Space". Med dagens teknologi er det mulig å skape informasjonsmiljøer (som for eksempel Internett) som gjør det mulig å samtidig oppnå høy grad av både richness og reach. Dette nye mulighetsrommet vises som det grå feltet i modellen merket "New Competitive Space". Jo lengre opp og til høyre et gitt informasjonsmiljø befinner seg, jo bedre informasjon-

sposisjon kan det sies å ha.

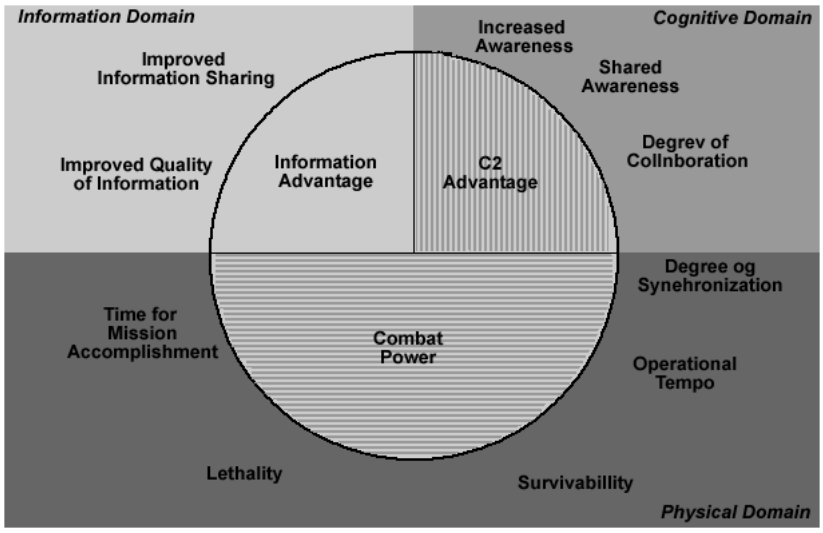
En forbedring i informasjonsposisjon tilsier et potensiale for økt verdi fra informasjonsmiljøet/informasjonssystemet. Realisering av potensiale krever at forbedringen relateres til en kontekst. For nettverkssentriske operasjoner har man identifisert følgende kontekst for å forklare hvordan forbedringene i nettverkene kan omsettes til økt verdi [7];

Økt richness gjennom økt reach Nettverk muliggjør en forbedring av informasjonskvalitet (richness) ved at man kan dele, korrelere, sette sammen og aksessere informasjon fra flere kilder.

Økt delt bevissthet Nettverk bidrar til å skape en delt bevissthet gjennom at det muliggjør deling av den økte informasjonskvaliteten.

Forbedret samarbeid Nettverk muliggjør deling av informasjon som omdanner delt bevissthet til felles planlegging og synkronisering som igjen skaper et konkurransefortrinn.

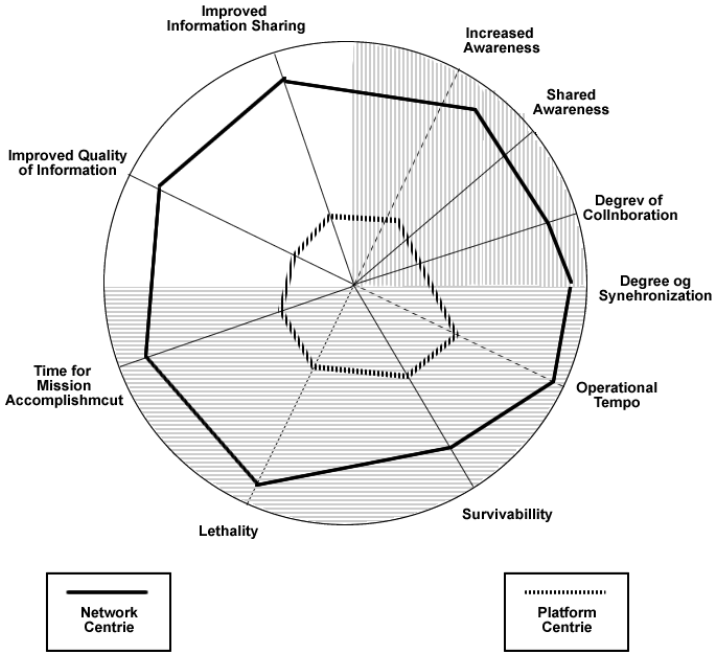
En verdikjede kategoriserer generiske aktiviteter en organisasjon utfører for å skape verdi. Dersom vi antar at domene-modellen representerer en militær verdikjede, kan hypotesen om sentrale sammenhenger mellom informasjonsposisjon, kommando og kontroll og verdi for militære operasjoner beskrives med følgende diagram;



Figur 17: Verdikjede for militære operasjoner[7]

I diagrammet benyttes richness og reach for å beskrive en forbedret informasjonsposisjon (information advantage). Kommando og kontroll (C2) beskriver forbedringer i kvalitet for interaksjon mellom enhetene og verdi (value) representerer effekt i militære operasjoner. Hypotesen er at en nettverksorganisert styrke vil ha en bedre informasjonsposisjon enn en plattformbasert styrke. Dette forholdet er et resultat av at nettverket som knytter alle nodene sammen gir samtidig forbedring i richness og reach (informasjonsdomenet). Forbedringen i informasjonsposisjon gir enhetene som deltar i striden informasjon om situasjonen som er kvalitativt bedre og kan deles i hele organisasjonen. Resultatet er en bedre og delt situasjonsbevissthet og forbedret mulighet for samarbeid

(det kognitive domenet). Dette vil igjen gi bedre og synkroniserte beslutninger som fører til synkronisering av utførelsen av operasjonene i det fysiske domenet. Hypotesen er med andre ord at nettverksbasering fører til økte verdier for sentrale variabler i informasjonsdomenet og det kognitive domenet, samt at dette vil gi økte verdier for viktige variabler i det fysiske domenet. Dette er visualisert i figur 18.



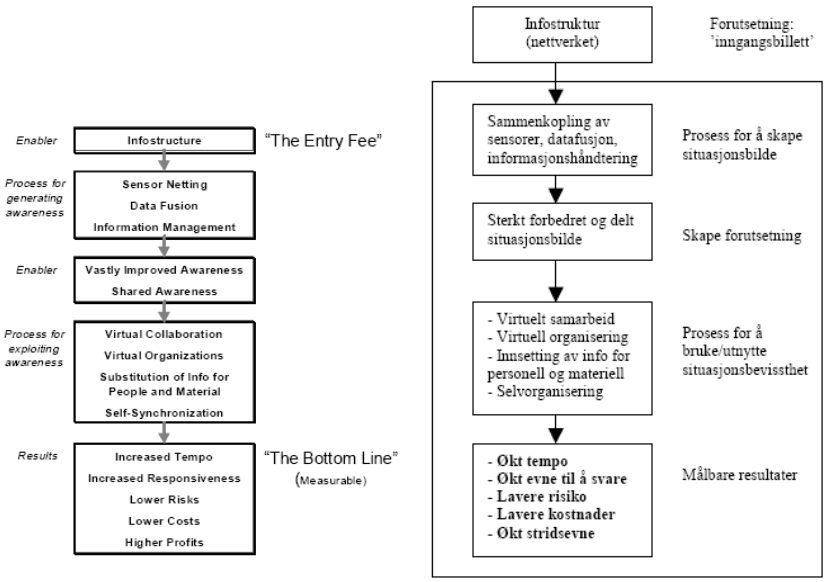
Figur 18: Forbedringer i informasjonsdomenet og det kognitive domenet gir økt effekt i det fysiske domenet[7]

4.5.4 Forholdet mellom økt kapasitet i informasjonsdomenet og militær effekt

Begrepet NCW ble introdusert til et bredt publikum i 1998 gjennom artikkelen "Network Centric Warfare: Its Origins and Future" [47]. Hypotesen om hvordan NCW skaper økt militær effekt ble først presentert på en helhetlig og gjennomarbeidet måte i 1999. Den ble fremsatt i en boken "Network Centric Operation Developing and Leveraging Information Superiority" [46]. Her er hypotesen presentert som en verdikjede som starter med realiseringen av en informasjonsinfrastruktur og ender i en beskrivelse av forventede effekter i forhold til utførelsen av militære operasjoner (se figur 19 (a)). Kjeden viser antatte kausale sammenhenger mellom variabler som påvirkes dersom en samler alle enhetene i forsvarsmakten i en felles informasjonsinfrastruktur. "Drivkraften" i kjeden er å utnytte en forbedret informasjonsposisjon til å skape felles situasjonsbevissthet for så å omsette denne til stridseffekt.

Verdikjeden i figur 19 (b) er hentet fra "Introduksjon til Nettverksbasert Forsvar" [21] fra mars 2001. Dette dokumentet er utarbeidet av Forsvarets stabsskole og er det første norske dokumentet som behandler NBF konseptet utførlig. Kjeden fremstår som en, mer eller mindre, avskrift av den amerikanske. Dette anser vi som en bekreftelse på at det teoretiske grunnlaget for de to konseptene er identiske.

Domenemodellen (se figur 13) ble introdusert i boken "Understanding Information



(a) NCW verdikjede [7] (b) NBF verdikjede [21]

Figur 19: Verdikjeder fra "Network Centric Warfare Developing and Leveraging Information Superiority" og "Introduksjon til Nettversbasert Forsvar"

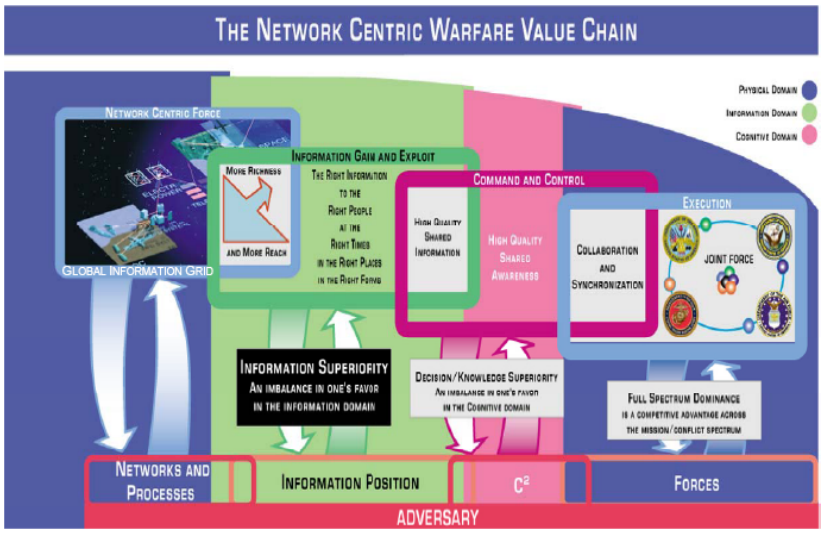
Age Warfare" i august 2001 [7]. Modellen beskriver betydningen av informasjon i krigføring. Den representerer en mer helhetlig tilnærming for å vurdere en forsvarsmakts evne til å skape militær effekt. Hypotesen er at en forbedring i informasjonsdomenet og det kognitive domenet vil medføre kvalitativt bedre beslutninger som igjen gir en bedre utnyttelse av eksisterende enheter. Informasjon og kognitive prosesser fremstår med andre ord som en svært viktige styrkemultiplikatorer. Stilt ovenfor en fiende, betyr dette at seier kan skapes gjennom evne til å samtidig skape relative fortrinn innen alle tre domenene.

I informasjonsdomenet benevnes et slik relativt fortrinn informasjonsoverlegenhet. Dette er en tilstand av ubalanse i informasjonsdomenet i egen favør. En slik tilstand er avhengig av at vi er relativt bedre enn våre fiender til å dekke størst mulig grad av vårt informasjonsbehov. Informasjonsbehovet er definert som den mengden informasjon en trenger for å planlegge og/eller utføre et oppdrag eller en oppgave.

I det kognitive domenet er det beslutningsoverlegenhet som er målet på et relativt fortrinn. Beslutningsoverlegenhet er en tilstand av ubalanse i det kognitive domenet i egen favør. Det innebærer at en er relativt bedre enn sin fiende til å fatte beslutninger (mer riktige/hensiktsmessige i forhold til situasjonen) og implementere dem raskere. Informasjonsoverlegenhet er en nødvendig forutsetning for beslutningsoverlegenhet. Det er imidlertid ikke slik at det første automatisk fører til det andre. For å realisere beslutningsoverlegenhet er det like nødvendig med tilpasning av organisasjonsstruktur, doktriner, utdanning og system for kommando og kontroll slik at de utnytter de nye mulighetene i informasjonssystemene.

Beslutningsoverlegenhet vil føre til et relativt fortrinn i det fysiske domenet. Bedre, raskere og synkroniserte beslutninger er grunnlaget for synkronisering og økt hurtighet i utførelsen av de militære operasjonene.

Videreutviklingen av det teoretiske grunnlaget for NCW er drivkraften for den utvidede verdikjeden som presenteres i boken (se figur 20). Denne versjonen relaterer grunnleggende begreper til hvordan de virker i prosessen med å skape relative fortrinn i de ulike ulike domenene. Den sentrale hypotesen er imidlertid den samme som tidligere; bedre informasjonsposisjon gir økt delt situasjonsbevissthet som leder til bedre beslutninger som til slutt medfører bedre utførelse av operasjoner.



Figur 20: Utvidet verdikjede fra "Understanding Information Age Warfare"[7]

I juli 2001 leverte det amerikanske forsvarsdepartementet en rapport om NCW til Kongressen. I denne finner vi "NCW's fire dogmer" (se figur 21).

The tenets of NCW are:

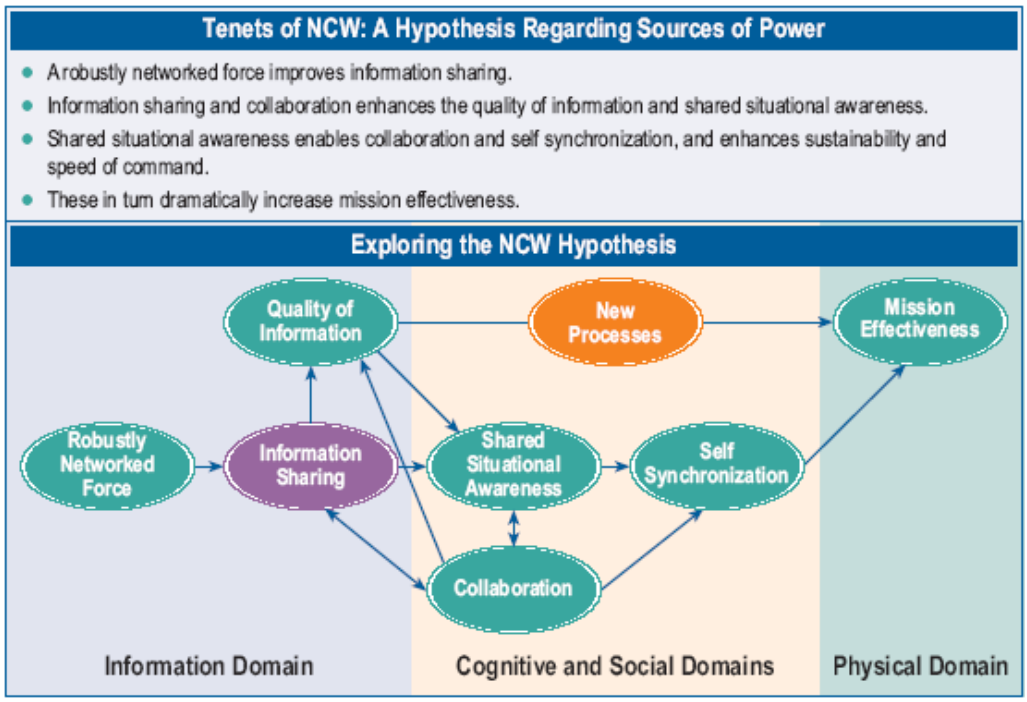
- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness

Figur 21: De fire dogmene i NCW[8]

Dogmene er utviklet av forskerne i CCRP og er en forenklet fremstilling av hypotesene fra verdikjedene vi har behandlet tidligere i dette kapittelet. De er en tekstlig, enkel beskrivelse av prinsippene som legges til grunn for den antatte effektøkningen en forventer av konseptet. Den enkle formen gjør den lett tilgjengelig for et bredt publikum, noe som trolig er en viktig årsak til at disse dogmene er mye brukt i dokumenter om NCW. Dersom vi ser nærmere på begrepene og de påståtte kausalitetene i dogmene, ser vi at de ikke introduserer noen nye elementer til verdikjeden. Det sentrale argumentet er fortsatt at en nettverksorganisering av en forsvarsmakt forbedrer informasjonsposisjonen (resultat av samtidig økt information sharing og quality), som igjen gir bedre ytelse

i det kognitive domenet (shared situational awareness, self-synchronization og speed of command). Disse forholdene resulterer til slutt i økt effekt i det fysiske domenet (sustainability og mission effectiveness).

De fire dogmene inneholder implisitte betraktninger om kausaliteten mellom de sentrale variablene i NCW konseptet. Figur 22 viser hvordan dogmene kan modelleres som en relasjon mellom variablene.

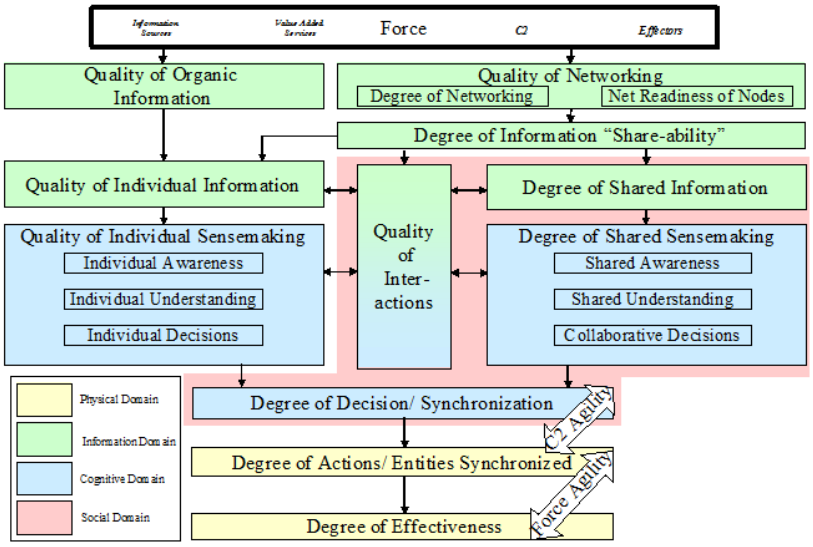


Figur 22: Dogmer omsatt til modell[9]

Modellen relaterer også de ulike variablene til hvilket domene de tilhører. Her ser vi at det er introdusert et nytt domene; det sosiale domenet. Dette tillegget er et resultat av utviklingen av et metrikk-rammeverk utviklet for Department of Defence/Office of Force transformation i 2003; Network Centric Operations Conceptual Framework (NCO CF) [10]. Det nye domenet overlapper med informasjonsdomenet og det kognitive domenet, og beskrives som; hvor entitetene i forsvarsmakten samhandler, utveksler informasjon, forståelse og utvikler beslutninger i samarbeid med hverandre. Behovet for dette nye domenet har sin bakgrunn i en erkjennelse av at kognitive aktiviteter er individualistisk i sin natur; det finner sted i hodet til hvert enkelt individ. Prosessen med å omsette delt bevissthet til delt forståelse og endelig til felles beslutninger betraktes her som en sosio-kognitiv aktivitet hvor individuelle kognitive prosesser er direkte påvirket av det sosiale miljøet det finner sted i og motsatt. Felles bevissthet, forståelse og beslutninger krever med andre ord interaksjon mellom entitetene som skaper disse tilstandene.

NCO CF er en videreutvikling av dogmene som ligger til grunn for NCW. Rammeverket knytter sammen hypotesene fra NCW konseptet på et høyt aggregeringsnivå (se figur 23) og tilbyr et sett attributter med tilhørende metrikker for hver sentral komponent i hypotesene. Målet er å gi et rammeverk for innsamling og analyse av empiriske data som

kan bekrefte eller avkrefte NCW hypotesene. Rammeverket gir også en høyere grad av presisjon enn tidligere modeller i forhold til viktige aspekter ved NWC hypotesene.



Figur 23: NCW verdikjede fra NCO CF[10]

NCO CF representerer den siste og mest utviklede verdikjeden for NCW/NBF vi har identifisere i eksisterende litteratur. Den historiske utviklingen av NCW verdikjeder vitner om en stadig økning i presisjon og oppløsning for begreper, variabler og kausale sammenhenger mellom dem. Kjernen i hypotesene er imidlertid den samme gjennom hele utviklingen; Nettverksorganisering av en forsvarsmakt vil gi økt militær effekt.

4.5.5 Sentrale variabler og kausale sammenhenger

CLD-modellen vi utviklet i kapittel 4.2 resulterer i et åpent problem; gapet mellom behov og evne til å skape militær effekt. Dette gapet medfører et politisk press for å øke den militære effekten. I norske øyne vil en nettverksorganisering av Forsvaret lukke gapet og redusere presset. Dette innebærer at den tilsiktede effekten av nettverksorganisering er å fjerne gapet mellom behov og evne til å skape militær effekt. Siden dette skal skje i en tilstand hvor Forsvaret består av færre enheter enn tidligere, må NBF resultere i en endring av de to andre variablene som styrer E total; midlere effekt per enhet og tid for gjennomføring av et engasjement.

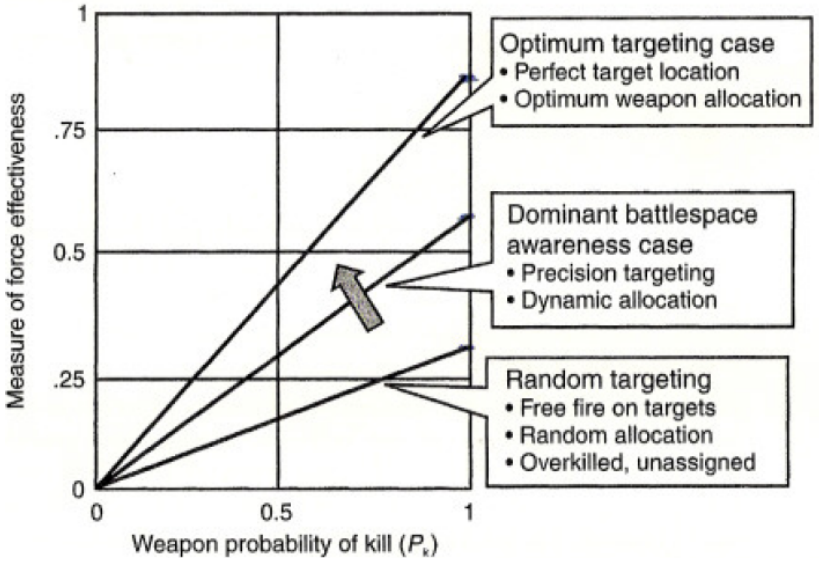
For å modellere hypotesen om hvordan en mener NBF vil lukke gapet, må vi lage en kausal struktur mellom variabler som påvirkes ved overgang til NBF og knytte denne til militær effekt. Her er de fire dogmene for NCW/NBF et godt utgangspunkt. Disse identifiserer den teoretiske hypotesen om hvordan nettverksorganisering av Forsvaret vil resultere i økt militær effekt. De opererer med relativt få variabler på et høyt aggregert nivå i forhold til verdikjeden fra "Network Centric Operation Conceptual Framework". Dette er ønskelig da det holder antall variabler i CLD-modellen på et oversiktlig nivå. Modellen av dogmene i figur 22 inneholder alle de sentrale variabler i hypotesen og relasjonen mellom dem. Det gjør at man kan utvikle en presis kausal struktur av dem.

I dogme-modellen er det ikke angitt hvordan den militære effekten vil materialisere seg. Her er det bare angitt at økning i informasjonskvalitet og selvsynkronisering medfør-

er en økning i militær effekt (Mission Effectiveness). I to dokumenter om NBF produsert av Forsvaret [38, 12] er det eksplisitt angitt en hypotese om hvilke forhold i det fysiske domenet som gir den økte effekten;

> Konseptets sentrale hypotese er at en nettverksorganisert militær styrke vil være i stand til å generere økt stridsevne ved:
>
> - større mulighet for innsetting av flere stridsmidler av ulik type mot mål i hele innsatsrommet, på tvers av tradisjonelle organisasjonsmessige og geografiske grenser
> - bedre styrkeøkonomisering ved bekjempelse av det enkelte mål, fordi man pga bedre situasjonsbevissthet ikke setter inn flere stridsmidler enn det som kreves for å ødelegge målet
> - større mulighet for innsetting av de riktige typer stridsmidler i forhold til målenes art, dvs en mer optimal utnyttelse av stridsmidlenes ulike egenskaper og dermed bedre virkning i målet
> - bedre synkronisering av stridsmidlene i tid og rom
> - mulighet for økt tempo i stridsledelsen og dermed i operasjonene som helhet

Dersom vi ser nærmere på denne hypotesen, ser vi at de tre første punktene er relatert til en forbedring i allokering av mål. Den økte kvaliteten av informasjonen om situasjonen i hele innsatsområdet og distribusjon av denne til alle enheter vil kunne resultere i kvalitativt bedre avgjørelser for valg av hvilke typer og mengde effektorer (stridsmidler) som skal benyttes for å bekjempe de ulike målene. Disse punktene kan derfor samles til en variabel på et høyere aggregeringsnivå som vi velger å kalle *"kvalitet for allokering av effektorer mot mål"*. Dersom kvaliteten til effektorene (P_k i figur 24) er konstant, vil en forbedring i allokering av mål øke den gjennomsnittlige virkningen av hvert våpen (Meassure of force effectiveness i figur 24). Ergo har en en økning av variabelen *"kvalitet for allokering av effektorer mot mål"* en positivt kausalitet med variabelen *"*$V_{midlere}$*"* fra formelen for militær effekt.



Figur 24: Økt virkning ved økt kvalitet for allokering av mål[11]

Det fjerde punktet er relatert til synkronisert innsetting av effektorer (stridsmidlene) i tid og rom. Dette kan defineres som den mest effektive form for samhandling i utførelse av militære operasjoner [6]:

> Målet med bruk av militær makt, og altså det endelige resultatet av det å føre kommando, er alltid en eller annen form for påvirkning. Størst effekt i påvirkningen oppnås dersom man er i stand til å synkronisere egne virkemidler. Ledelse av militære operasjoner vil derfor ha som høyeste ambisjon å synkronisere militære effekter mot målsettingen om å påvirke en annen aktør.
>
> På et lavere samhandlingsnivå finner vi koordinering og samvirke, der koordinering defineres som det å påse at handlinger og virksomheter til forskjellige, egne enheter ikke påvirker hverandre negativt (unngå konflikter), mens samvirke innebærer en aktiv handling av flere aktører mot et felles mål.
>
> Synkronisering blir da høyeste grad av samhandling i tid og rom for å oppnå synergieffekter i påvirkningen. Samlet er disse tre begreper gradering av samhandlingen mellom de militære komponenter

Synkronisering i bruk av effektorer er altså en driver for synergieffekter. Dette innebærer at dersom man synkroniserer innsetting av effektorer som utfyller hverandre, vil de oppnå høyere virkning enn hver for seg. Et eksempel på dette kan være synkronisert innsetting av bakkestyrker og jagerfly i angrep mot en flystasjon. Bakkestyrkene vil da kunne nøytralisere luftvernsystemene som beskytter flystasjonen. Da vil jagerflyene kunne angripe mål på bakken uten å måtte beskytte seg selv mot fiendtlig ild. Dersom jagerflyene bekjemper fiendens fly på bakken, vil ikke disse kunne settes inn mot våre bakkestyrker. Siden dette medfører at både bakkestyrker og jagerfly kan angripe uten å samtidig måtte beskytte seg selv, er det sannsynlig at de vil oppnå økt presisjon og derigjennom økt virkning. Ergo har en en økning av variabelen "*grad av synkronisering av effektorer*" en positivt kausalitet med variabelen *"*$V_{\mathtt{midlere}}$*"* fra formelen for militær effekt.

Det femte og siste punktet er relatert til hastighet i ledelse av militære operasjoner. Forsvarets Fellesoperative Doktrine benytter begrepet handlingssløyfen for en overordnet beskrivelse av hvilke aktiviteter som må gjennomføres for å utøve stridsledelse [74]:

> En handlingssløyfe består av fire klart identifiserbare elementer som utgjør en kontinuerlig mental prosess: observasjon, vurdering, beslutning og handling. Evnen til å gjennomføre denne prosessen hurtigere enn en motstander er avgjørende for suksess i fremtidige konflikter. Sløyfen består egentlig av tre seksjoner, hvor den ene er knyttet til informasjon (observasjon og vurdering = hva er det egentlig som skjer?), den andre er knyttet til beslutning (beslutning = hva kan jeg eller hva bør jeg gjøre med det?), og den tredje er knyttet til handling (handling = hvordan og med hva noe utføres).

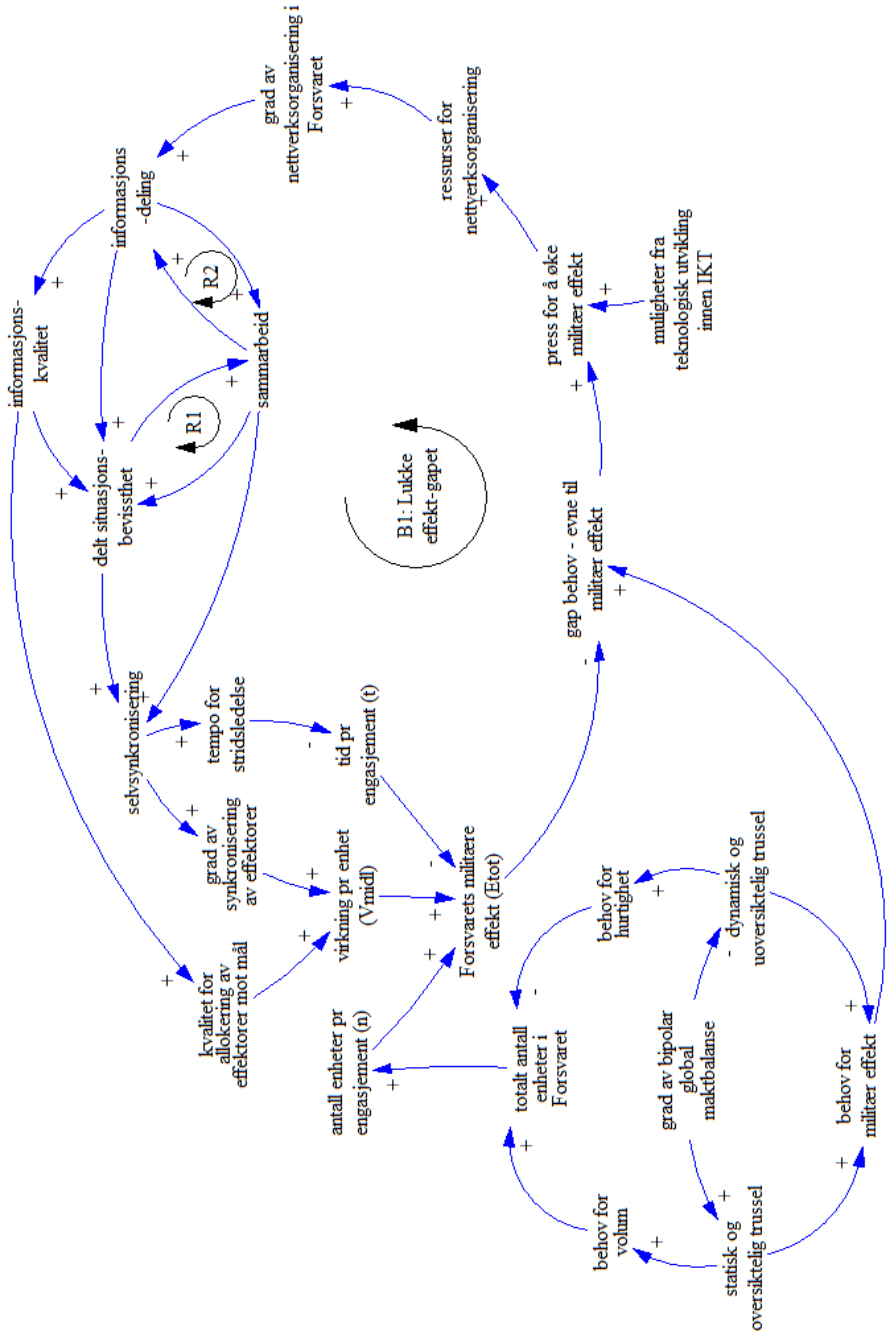
Handlingssløyfen er en sekvensiell prosess. De tre første elementene innebærer å fatte en beslutning om når og hvordan et engasjement skal gjennomføres. Dersom denne tiden reduseres, vil det innebære at den totale tiden for gjennomføringen av et engasjement vil reduseres. Ergo har en en økning av variabelen *"tempo for stridsledelse"* en negativ kausalitet med variabelen *"tid per engasjement (*t*)"* fra formelen for militær effekt.

Den tekstlige beskrivelsen av sentrale variabler og kausale sammenhenger mellom dem kan omsettes til å utvide CLD-modellen fra kapittel 4.2 som viser bakgrunnen for hvorfor man ønsker å benytte NBF-konseptet i Forsvaret. Den utvidede modellen viser

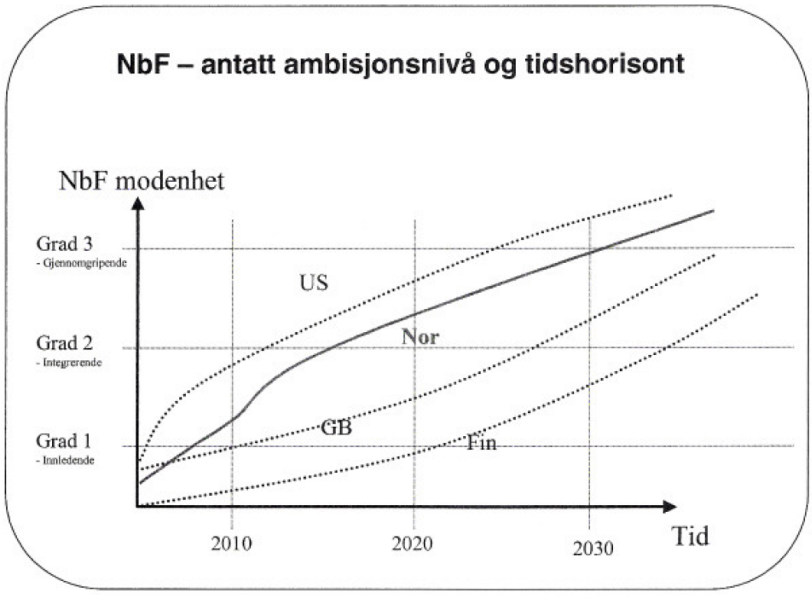
hypotesen om hvordan en nettverksorganisering av Forsvaret skal bidra til å lukke gapet mellom behovet for militær effekt og den effekten man kan levere med et plattformbasert forsvar som har redusert antall enheter (se figur 25).

Den tilsiktede effekten av NBF fremkommer i modellen som en balanserende sløyfe (B1: lukke effektgapet) som starter i variabelen *"press for å øke militær effekt"*. Denne variabelen vil øke som et resultat av økningen i gapet mellom effektbehov og evne til å levere effekt. Norske fagmilitære og politiske myndighetspersoner har uttalt at dette gapet skal lukkes som ved at en nettverksorganisering av Forsvaret vil resultere i økt effekt per enhet. For å nettverksorganisere Forsvaret er man nødt til å bruke ressurser for en omorganisering. Dette innebærerer en positiv kausalitet med variabelen *"ressurser for nettverksorganisering"* som kan måles ut fra en monetær verdi. Det vil være en økt andel av forsvarsbudsjettet som må benyttes for, blant annet å realisere en informasjonsinfrastruktur samt utvikle og tilpasse enheter som har et adekvat grensesnitt mot denne. Dette vil drive variablene *"grad av nettverksorganisering av Forsvaret"* i en positiv retning; jo mer ressursser vi benytter til nettverksorganisering, jo flere av enhetene i Forsvaret vil tilknyttes informasjonsinfrastrukturen og samvirke med de andre enhetene via denne. I en rapport fra arbeidsgruppe NBF for revisjon av Forsvarets Fellesoperative Doktrine (FFOD) [12] måles denne variabelen etter en skala for *"NBF modenhetsgrad"*. Overgangen fra plattformbasert konsept til nettverksorganisering vil være en lang prosess som vil gå over mange år. NBF modenhetsgrad er delt inn i tre ulike nivåer og angir en tilstandsbeskrivelse for hvor langt Forsvaret er kommet i denne prosessen. Arbeidsgruppen har også stipulert en mulig tidshorisont for hvor lang tid det vil ta Forsvaret å nå den tredje og øverste NBF modenhetsgrad. Med andre ord en tidshorisont for hvor lang tid en må regne før Forsvaret fullt ut er nettverksorganisert. Som vi ser av figur 26 (kurve merket med NOR) antas denne prosessen å ta ca 25 år. Tidsforsinkelsen mellom innsetting av ressurser og NBF modenhetsnivå er et resultat av tiden for design, utvikling og integrasjon av informasjonsinfrastrukturen og enheter som er kompatible med denne. Av figur 26 ser vi at det er 10-15 år mellom oppnåelse av hvert modenhetsnivå. Det vil altså være slik at etter oppnåelsen av et nivå, starter en å benytte ressurser for å videreutvikle seg til neste nivå som en regner med å nå i løpet av en tidsperiode på 10-15 år. Vi vil ikke markere denne forsinkelsen i CLD-modellen, men kommer tilbake til den når vi utvikler arketyper i kapittel 6.

De påfølgende fem variablene i modellen og det kausale forholdet mellom dem, er hentet fra modellen over de fire dogmene for NCW/NBF. De viser hvordan en forbedring i informasjonsposisjonen vil kunne bidra til økt militær effekt. Denne effekten startes av den positive kausaliteten fra *"grad av nettverksorganisering av Forsvaret"* til *"informasjonsdeling"*. Den viser at jo større andel av forsvarets enheter som er nettverksorganisert (knyttet sammen gjennom en informasjonsinfrastruktur med høy kapasitet), jo høyere grad av informasjonsutveksling vil skje mellom enhetene. Dette medfører en økning av *"informasjonskvalitet"*, *"delt situasjonsbevissthet"* og *"samarbeid"*. Et eksempel på hvordan informasjonskvaliteten øker kan være sammenknytningen av alle sensorer i Forsvaret. Dette vil bidra til et mer komplett situasjonsbilde. Dette eksemplet fungerer også som en forklaring på økt *"delt situasjonsbevissthet"* ved at det kvalitativt bedre situasjonsbildet kan distribueres til alle beslutningstakere. I henhold til dogmene viser modellen to små selvforsterkende løkker mellom *"samarbeid"* og to av de andre variablene. Den første kan forklares med at en økt kapasitet i informasjonsdeling medfører



Figur 25: Modell for tilsiktet effekt av NBF konseptet



Figur 26: Tidshorisont for fullstendig nettverksorganisering av Forsvaret [12]

en økning i samarbeid mellom enhetene ved økt mulighet for mengde og form for kommunikasjon mellom dem. Samarbeid innebærer å dele informasjon mellom enhetene i nettverket, ergo vil det medføre en feedbacksløyfe som øker informasjonsdeling. Den andre løkken kan forklares med at en økning av samarbeid vil gi økt delt situasjonsbevissthet ved at enhetene gjennom samarbeidet utvikler en økt felles situasjonsbevissthet. Denne tilstanden vil igjen kunne resultere i mer og bedre samarbeid gjennom en felles forståelse for den aktuelle situasjonen. Den siste variabelen fra dogmene er *"selvsynkronisering"*. Dette er en slags automatisk synkronisering av enhetene som oppstår som et resultat av at alle enhetene deler den samme økte situasjonsbevisstheten og kunnskap om sjefens intensjon for den militære operasjonen som utføres.

Dogmene for NCW/NBF tilsier at en økning av variablene *"informasjonskvalitet"* og *"selvsynkronisering"* vil resultere i økt militær effekt. I modellen har vi lenket disse til variablene fra de norske hypotesene om hvordan denne effekten vil oppstå. En økning av *"informasjonskvalitet"* vil medføre en økt kvalitet i allokeringen av effektorer til bekjempelse av fiendtlige mål og variabelen har følgelig positiv kausalitet med *"kvalitet for allokering av effektorer mot mål"*. Årsaken er relatert til at beslutningstakere har en helhetsoversikt over alt som skjer i innsatsrommet og tilgjengelige effektorer. De kan da utføre en helhetlig vurdering av hvilke og hvor mange effektorer som bør settes inn mot hvert enkelt mål. Disse valgene kan gjøres på tvers av effektorenes tilhørighet til en forsvarsgren og fysiske sektorinndelinger av innsatsrommet.

Økningen av variabelen *"selvsynkronisering"* vil medføre en økning av både *"grad av synkronisering av effektorer"* og *"tempo for stridsledelse"*. Selvsynkronisering kan defineres som [6];

> En form for stilltiende interaksjon mellom to eller flere aktører. To eller flere aktører som er knyttet til et nettverk og har tilgang på et felles situasjonsbilde og et sett interaksjonsregler som skal øke stridseffekten er forutsetningene for selvsynkronisering.

Den tradisjonelle metoden for synkronisering i militære operasjoner er en sekvensiell, strukturert og toppstyrt planprosess. Selvsynkronisering skjer nærmere "kanten av organisasjonen" ved samarbeid mellom beslutningstakere på lavere nivå. Man forventer at denne tilnærmingen til synkronisering er både raskere og kvalitativt bedre (oppnår høyere grad av synkronisering) enn den tradisjonelle, samt at den vil gå raskere.

Kausaliteten mellom variablene *"kvalitet for allokering av effektorer mot mål"*, *"grad av synkronisering av effektorer"* og *"tempo for stridsledelse"* med variablene *"virkning på enhet"* og *"tid per engasjement"* er beskrevet tidligere i dette kapitlet. Den er av en slik karakter at variabelen *"Forsvarets militære effekt"* vil øke. Siden dette igjen medfører en reduksjon av variabelen *"gap behov - evne til militær effekt"*, ser vi at løkken B1 er balanserende siden den til slutt reduserer variabelen *"press for å møte militær effekt"*. Den mest sentrale variabelen i løkken er *"Forsvarets militære effekt"*. Hypotesen er at en nettverksorganisering av Forsvaret vil øke denne variabelen, slik at gapet mellom behov og faktisk militær effekt lukkes. Dette skjer ved at kjeden av kausaliteter mellom sentrale variabler som endres når Forsvaret nettverksorganiseres medfører en økt effekt per enhet og redusert tid per engasjement.

4.6 Delkonklusjon - tilsiktet effekt av NBF

Modellen i forrige kapittel er utviklet fra informasjon i sentrale norske dokumenter om NBF og deres amerikanske grunnlagsdokumenter. Modellen viser at den tilsiktede effekten av en nettveksorganisering av Forsvaret er å lukke et gap mellom behov for militær effekt og evne til å skape denne. Gapet oppstår som et resultat av en endring i Norges sikkerhetspolitiske situasjon. Den tidligere sterkt bipolare globale maktbalansen mellom øst og vest, med en statisk og oversiktlig trussel, blir erstattet av en dynamisk og uoversiktlig trussel. Det nye trusselbildet tilsier et behov for et Forsvar som er mindre i volum (antall enheter) slik at det raskt kan utføre militære operasjoner der det trengs, uavhengig av geografisk lokasjon. Selv om den globale trusselen har endret karakter, er den trolig ikke redusert i omfang. Forsvaret må altså kunne levere samme mengde militær effekt som tidligere, men med færre enheter.

NBF-konseptet bygger på en hypotese om at en forbedring i informasjonsdomenet og det kognitive domenet vil sette Forsvaret i stand til å lever økt militær effekt i det fysiske domenet. Forbedringene skal realiseres ved å utnytte muligheter de senere års utvikling innen IKT har skapt. Det er nå mulig å knytte sammen alle Forsvarets enheter i en felles informasjonsinfrastruktur som gir radikale forbedringer av informasjonsdeling, informasjonskvalitet, samarbeid og felles situasjonsbevissthet. Disse forbedringene skal muliggjøre bedre synkronisering, allokering og tempo i militære operasjoner. Den militære effekten økes ved at en oppnår mer effekt per enhet gjennom at midlere virkning per enhet øker samtidig som tiden det vil ta å sette inn enheter mot fiendtlige mål reduseres.

På denne måten regner en med at en nettverksorganisering av et Forsvar som reduseres i antall enheter, gradvis vil sikre en fremtidig evne til å skape militær effekt som tilfredsstiller det sikkerhetspolitiske behovet. Dette besvarer vårt første forskningsspørsmål (Hva er den forventede effekten av NBF og hvordan skal denne realiseres?); Økt bruk av ressurser for NBF-organisering gradvis gi høyere NBF modenhetsnivå som igjen medfører bedre evne til å skape militær effekt. Etter en implementeringsperiode for NBF på ca 25 år, vil gapet mellom behov og evne til å levere militær effekt lukkes.

I USA er det gjennomført en rekke studier for å undersøke validiteten i NCW-hypotesen. Mange av disse har benyttet NCO CF som vitenskapelig rammeverk for innsamling og analyse av empiriske data (tabell 5 inneholder et utvalg av undersøkelser basert på NCO CF). Målet for undersøkelsene har vært å påvise kausale sammenhenger mellom nettverksorganisering og militær effekt.

Årstall	Undersøkelse	Kort beskrivelse
2005	Network-Centric Operations Case Study Air-to-Air Combat With and Without Link 16 [78]	Øvelse luft-til-luft kamp
2005	A Network-Centric Operations Case Study: US/UK Coalition Combat Operations during Operation Iraqi Freedom (OIF)[79]	Bruk av sporingssystem for egne styrker i strid under OIF
2005	Network-Centric Operations Case Study: The Stryker Brigade Combat Team [80]	Øvelse for sertifisering av stridsdyktighet før strid

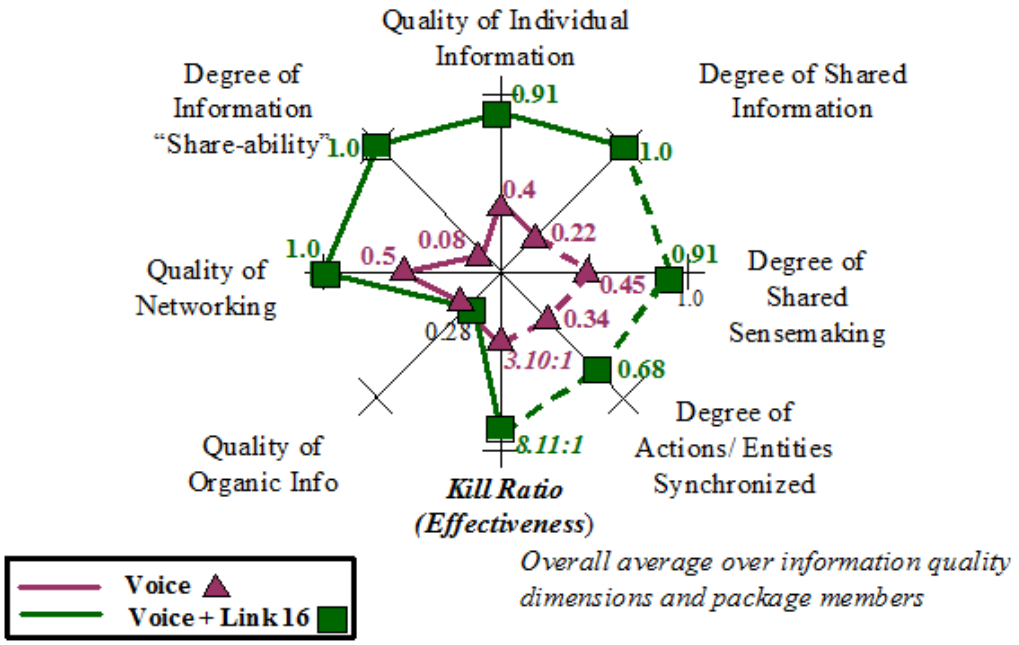
Tabell 5: Undersøkelser for validering av NCW hypotese

Undersøkelsene indikerer at NCW-hypotesen er valid og at en nettverksorganisering av militære enheter medfører en dramatisk økt militær effekt [10]:

> Preliminary insights gained from the research reported in this document demonstrate that investments aimed at enhancing NCO capabilities have a dramatic impact on force effectiveness. Each of the case studies provides evidence of the improved force effectiveness that resulted from investments in NCO capabilities across the DOTML-PF (Doctrine, Organization, Training, Materiel, Leadership, Education, Personnel and Facilities) lines of development.

Den første av undersøkelsene i tabell 5 er en av de mest anvendte i litteratur som forfekter verdien av NCW. Undersøkelsen ble gjennomført for å evaluere resultatene fra over 12000 luft-til-luft treningstokter utført under en militær øvelse i USA. Det eneste som skilte partene som utførte lut-til-luft kampene var hvilke informasjonssystemer de benyttet. Den ene siden hadde bare tale over radio, mens den andre siden hadde tale over radio og et informasjonssystem som betegnes Link16. Den siste gruppen ansees som en representant for en nettverksorganisert styrke, siden deres informasjonssystem muliggjorde delt tale og data mellom alle tilknyttede aktører. Resultatene fra øvelsen viste at den nettverksorganiserte siden hadde en kill-ratio som var over to og en halv ganger bedre enn den andre siden. Dette innebærer at for hvert jagerfly den nettverksorganiserte styrken mistet, skjøt de ned to og et halvt (i snitt) jagerfly fra den andre styrken. Undersøkelsen forklarer denne dramatiske forskjellen i militær effektivitet ved hjelp av empiriske data relatert til metrikkene i NCO CF. Den eneste variabelen som hadde lik verdi var "kvalitet for organisk informasjon". Denne variabelen representerer kvaliteten til informasjonen som hvert enkelt jagerfly kunne skape gjennom egne sensorer (i all hovedsak radar). Den nettverksorganiserte styrken hadde høyere verdier for alle de andre variablene (se figur 27).

Selv om undersøkelsen er utført på taktisk nivå og således ikke omfatter en hel forsvarsmakt, er den en sterk indikator på at nettverksorganisering av militære styrker medfører en dramatisk økning av militær effekt. Dette medfører en styrket validitet



Figur 27: Sammenligning av variabler for styrker med og uten Link16

for realiseringen av den tilsiktede effekten av NBF i Norge.

5 Utilsiktet effekt ved implementering av NBF konseptet

I dette kapitlet vil vi vurdere om implementeringen av NBF kan medføre sideeffekter knyttet til risikobildet for informasjonssystemet som skal muliggjøre konseptet. Dersom en slik sideeffekt identifiseres, vil vi vurdere hvordan denne kan påvirke realiseringen av tilsiktet effekt for NBF. Fremgangsmåten vi har valgt er å først beskrive informasjonssystemet som skal muliggjøre NBF, samt hvilke momenter som inngår i en risikoanalyse av slike informasjonssystemer. Deretter vil vi vurdere hvordan risikobildet for informasjonssystemet kan utvikle seg som en følge av faktorer relatert til den tilsiktede effekten av NBF. I relasjon til avgrensningen av oppgaven innebærer dette en vurdering av utviklingen for risiko knyttet til villede logiske angrep mot INI som en følge av endringer ved implementering av NBF. Til slutt vil vi benytte denne vurderingen til å videreutvikle CLD-modellen fra forrige kapittel for å identifisere forholdet mellom tilsiktet og utilsiktet effekt.

I dette kapitlet er er det benyttet en rekke ulike dokumenter fra ulike kilder. Tabell 6 viser en oversikt over de mest sentrale og i hvilken sammenheng de er benyttet. I tabellen er; I=Beskrivelse av INI, R=Risikodefinisjon, V=Verdi, T=Trussel og S=Sårbarhet

5.1 Informasjonssystemet i NBF

5.1.1 Informasjonsinfrastrukturen (INI)

Informasjonssystemet som skal muliggjøre NBF er gitt benevnelsen Informasjonsinfrastrukturen (INI). Begrepet informasjonsinfrastruktur har de senere år i økende grad blitt benyttet for å beskrive integrerte løsninger ved informasjonsbehandling. Informasjonsinfrastruktur brukes for å beskrive informasjons- og kommunikasjonsteknologi; fra nasjonale og globale nettverk som Internett, og ned til de mer lokale og spesialiserte løsninger for kommunikasjon, eksempelvis taktisk militær kommunikasjon. I begrepet informasjonsinfrastruktur inngår både kommunikasjons- og informasjonssystemer [13].

Et nettverksorganisert Forsvar vil bestå av nettverk på tre ulike nivåer slik det er illustrert i figur 28.

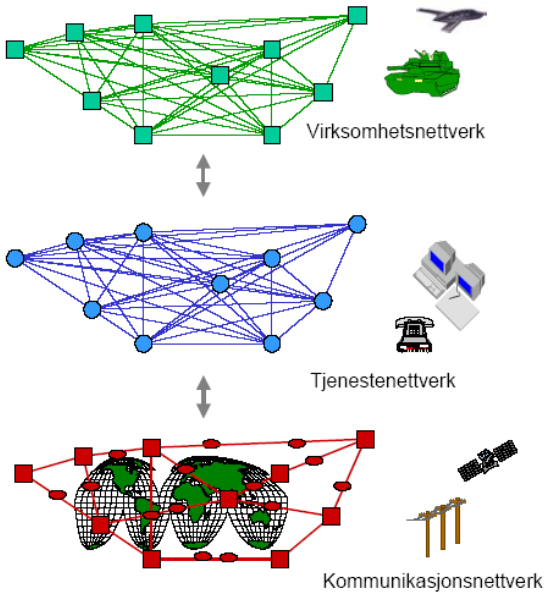
Det øverste nivået er et virksomhetsnettverk som representerer den logiske koplingen mellom enhetene i Forsvaret (enhetene i NBF benevnes noder; sensorer, beslutningstakere og effektorer). Dette er ikke et teknisk nettverk, men en illustrasjon av hvilket behov de to nederste nettverkene skal dekke; sammenkopling av alle nodene i Forsvaret. De to nederste nettverkene er av teknisk natur og utgjør til sammen INI. Kommunikasjonsinfrastrukturen (merket Kommunikasjonsnettverk i figur 28) sørger for forbindelse mellom entitetene i tjenesteinfrastrukturen (merket Tjenestenettverk i figur 28) samt koblingen mellom disse og de ulike beslutnings-, effektor- og sensorkomponentene. Nodene er brukere av tjenesteinfrastrukturen. Noen av nodene har rollen som tjenesteprodusenter og gjør informasjon tilgjengelig ved å legge den ut på nettet. Andre noder har rollen som tjenesteforbrukere og henter informasjon ut fra de oppgaver som skal gjennomføres.

INI er med andre ord systemet som kopler sammen (netting) ressurser for å mulig-

Årstall	Tittel	Hvor benyttet				
		I	R	V	T	S
2000	Forsvarets fellesoperative doktrine DelA - Grunnlag [74]			X		
2000	Samfunnets sårbarhet som følge av avhengighet til IT [30]		X		X	
2001	Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. [17]		X			
2002	FFI/Rapport-2002/03973 Informasjonsinfrastruktur for NBF [13]	X				X
2002	Identification of a method for the calculation of threat in an information environment. [81]				X	
2003	Konsept for nettverksbasert anvendelse av militærmakt. [38]			X		
2004	FFI/Rapport-2004/01561 Network Architecture for Network Centric Warfare Operations [16]	X				X
2004	Styrke og relevans: Strategisk konsept for forsvaret i perioden 2005-2008. [36]				X	
2004	Risk management of information systems in dynamic environments - a case study of the norwegian defence and the process of approving classified information systems [82]		X			
2005	Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i forsvaret. [14]	X				X
2005	Konsept for styring av elektronisk informasjon i forsvaret. [37]	X				
2005	Network-centric operations case study air-to-air combat with and without link 16. [78]			X		
2005	Risk Management for Computer Security - Protecting Your Network and Information Assets. [83]				X	
2005	Sårbarheter og trusler mot informasjonssystemer. [84]				X	X
2006	Beskrivelse av programområde informasjonsinfrastruktur - plan for perioden 2006-2009+. [15]	X				X

Tabell 6: Oversikt over sentral litteratur for analyse av utilsiktet effekt.

gjøre innsamling, prosessering, lagring og distribusjon av informasjon etter aktørenes behov. Man kan se på INI som en felles infrastruktur som muliggjør deling av informasjon og samarbeid mellom aktørene som har tilgang til nettet. Produsenter av tjenester legger informasjon ut på en eller flere ressurser i nettet. Brukere på sin side finner hvilke tjenester som er tilgjengelige ved å gjøre oppslag i kataloger, hvoretter tjenestene kan hentes og forbrukes. Som en integrert del av infostrukturen vil man også ha tradisjonelle tjenester som tale, video/ videokonferanser og meldinger. Målsettingen er at INI skal muliggjøre organisering av Forsvarets ressurser i samvirkende nettverk, fra strategisk til stridsteknisk nivå, både nasjonalt, med allierte styrker og koalisjonspartnere samt med

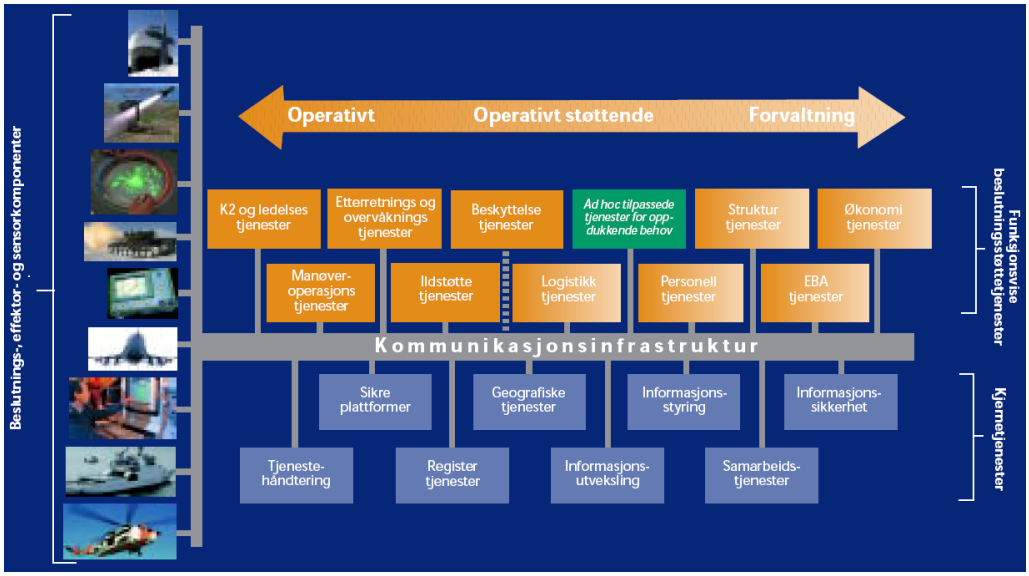


Figur 28: De ulike nettverkene i NBF [13]

relevante sivile instanser. I de påfølgende to kapitlene vil vi se nærmere på hovedkomponentene i INI; Tjenesteinfrastrukturen og Kommunikasjonsinfrastrukturen.

5.1.2 Tjenesteinfrastrukturen

Tjenesteinfrastrukturen omfatter de elementene i INI som gjør informasjonstjenester tilgjengelig for brukere og applikasjoner over nettet. Informasjonstjenestene er igjen delt opp i to hovedkategorier etter hvilken type tjeneste de leverer; funksjonsvise beslutningsstøttetjenester og kjernetjenester. De funksjonsvise beslutningsstøttetjenestene understøtter grupper av brukere med felles informasjonsbehov og prosesstøtte. Disse tjenestene skal benytte felles kjernetjenestene. Kjernetjenestene er felles, og angir hvilken grunnleggende informasjons og prosesstøtte som kan leveres av INI. At tjenestene er felles betyr ikke at alle har alt, men at tjenestene er standardiserte for hele Forsvaret. Til sammen utgjør disse to settene av tjenester det behovet som er identifisert for informasjonstjenester i realiseringen av NBF. Referansemodellen for INI [14] i figur 29 gir en visuell forestilling av informasjonstjenestene og deres relasjon til den underliggende kommunikasjonsinfrastrukturen. Tabellene 7 og 8 gir en kort beskrivelse av de ulike informasjonstjenestene [37].



Figur 29: Referansemodell for NBF [14]

5.1.3 Kommunikasjonsinfrastruktur

Kommunikasjonsinfrastrukturen tilbyr kvalitetssikrede mekanismer for forbindelse mellom beslutningsstøtte- og kjernetjenestene, samt koblingen mellom disse og de ulike beslutnings-, effektor- og sensorkomponentene. Den omfatter de elementer som sørger for formidling av lyd, bilde, video og data. I grensesnittet mot tjenesteinfrastrukturen fungerer den som et felles integrerende kommunikasjonslag basert på IP-teknologi. I figur 30 benevnes dette grensesnittet "Kommunikasjonstjenester". Eksisterende løsninger, som skal videreføres, skal i fremtiden migreres over til en infrastruktur basert på IP-teknologi når og hvis det er økonomisk hensiktsmessig ut fra levetidskostnader. Nye tjenester og plattformer skal støtte IP-teknologi når disse innføres.

Figur 30: Komponenter i kommunikasjonsinfrastrukturen for NBF [15]

Transmisjonstjenestene i kommunikasjonsinfrastrukturen må kunne fremskaffe tilgang til IP-nettverket i alle mulige geografiske områder hvor Forsvaret skal utføre militære operasjoner. I tråd med de nye sikkerhetspolitiske retningslinjene skissert i kapittel 4 betyr dette at INI må gi mulighet for global dekning. Nettverkstopologien som skal

Funksjonsvise beslutningsstøttetjenester	
Kommando, kontroll og ledelsestjenester	Tjenester for å planlegge, lede og kontrollere Forsvarets virksomhet. Eksempelvis tjenester for utvikling av planer, ordre og oppdrag samt for simulering og analyse.
Manøveroperasjonstjenester	Tjenester for gjennomføring av militær virksomhet, dvs til støtte for de ulike typene operasjonsformer (landoperasjoner, luft operasjoner, maritime operasjoner, amfibieoperasjoner, luft- og missilvern, informasjonsoperasjoner, spesialoperasjoner samt krisehåndtering).
Etterretnings- og overvåkningstjenester	Tjenester for å bygge situasjonsbilder. Eksempelvis tjenester for etterretning, rekognosering, overvåkning og sensorstyring.
Ildstøttetjenester	Tjenester for å styre og synkronisere ulike typer ild. Eksempelvis tjenester for lokalisering og målprosessering, målengasjement, valg av effektor og virkningsanalyse.
Beskyttelsestjenester	Tjenester for ARBC, fortifikasjon og andre beskyttelsestiltak.
Logistikktjenester	Tjenester for fremskaffe og opprettholde materiell stridsevne.
Personelltjenester	Tjenester for rekruttering, utvikling, anvendelse og avvikling av personell.
Strukturtjenester	Tjenester for å planlegge, realisere og evaluere strukturer.
EBA-tjenester	Tjenester for håndtering av eiendom, bygg og anlegg. Eksempelvis tjenester som støtter etablering og nedrigging av camp.
Økonomitjenester	Tjenester for lønn og regnskap.
Ad hoc tilpassede tjenester	Denne typen tjenester er tatt med for å indikere at man vil ha fleksibilitet til å kunne lage spesialtilpassede samlinger av tjenester tilpasset et oppdukkende operativt behov.

Tabell 7: Beskrivelse av funksjonsvise beslutningsstøttetjenester i INI

understøtte dette vil bli implementert i en klassisk struktur med tre nivåer; et stasjonært strategisk stamnett i Norge samt deployerbare og mobile taktiske nettverk i operasjonsområdene [16](se figur 31).

Det stasjonære strategiske nettverket i Norge skal knytte sammen alle militære enheter i Forsvaret, samt gi mulighet for sammenkobling med andre nasjoners militære nettverk, sivile etater og kommersielle tjenesteleverandører. Nettverket vil benytte ulike typer transmisjonsteknologier og det vil være designet for stabilitet og robusthet gjennom transmisjonsmessig redundans. Deler av nettverket vil trolig realiseres gjennom å anskaffe kommersielle tjenester. Målet er å øke fleksibiliteten og robustheten samt redusere kostnader forbundet med det økte kapasitetsbehovet i fremtiden.

Deployerbare taktiske nettverk skal etableres som en del av internasjonale eller nasjonale militære operasjoner. Disse vil lokaliseres til det geografiske området hvor operasjonen skal utføres. All kommunikasjon mellom enheter i det samme operasjonsområdet skal

Felles kjernetjenester	
Tjenestehåndtering	Tjenester for eksempelvis systemovervåkning, sikring av tilgjengelighet og ulike typer callsentre (helpdesk).
Sikre plattformer	Sikre kjøremiljøer med standard støtteverktøy (FISBasis Hemmelig/NATO Secret og FISBasis Begrenset/Ugradert).
Registertjenester	Forvaltning og formidlig av tjenestene i informasjonsinfrastrukturen, eksempelvis en oppslagstjeneste
Geografiske tjenester	Tjenester for forvaltning og bruk av geografisk informasjon. Eksempelvis kartmotor med evne til å vise militær symbolikk, overlegghåndtering og grunnleggende tracking.
Informasjonsutveksling	Standarder og løsninger for informasjonsutveksling nasjonalt, med allierte styrker og koalisjonspartnere samt med relevante nasjonale instanser. Eksempler på denne typen tjenester er militær meldingshåndtering, epost, datalinker og replikering.
Informasjonsstyring	Tjenester for fangst, lagring, fusjonering og korrelering, gjenfinning og utnyttelse av informasjon.
Samarbeidstjenester	Tjenester for lyd- og videotelefoni og annen online samhandling.
Informasjonssikkerhet	PKI, IP kryptering og andre typer tjenester for sikring av konfidensialitet, integritet og tilgjengelighet.

Tabell 8: Beskrivelse av felles kjernetjenester i INI

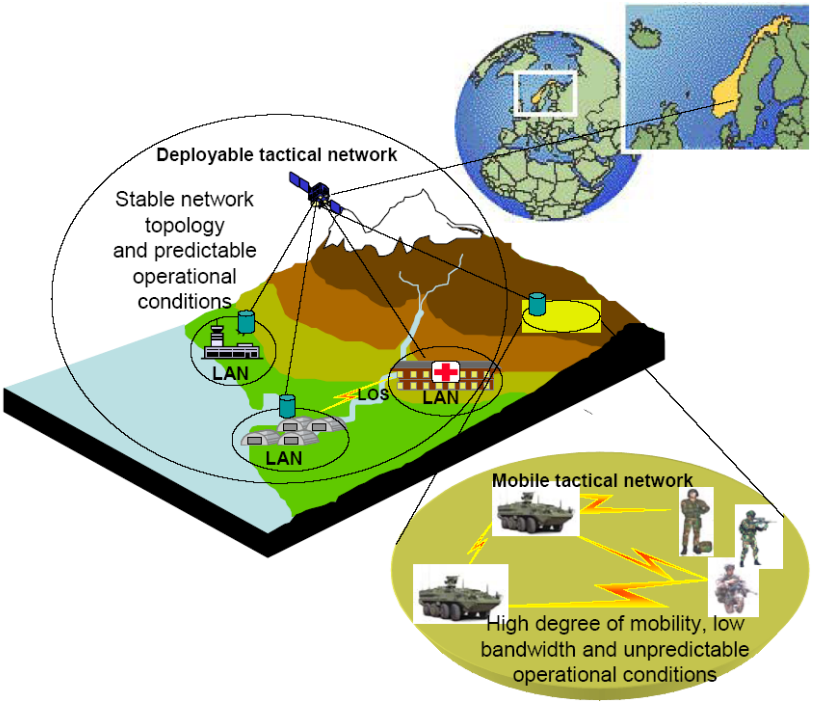
gå gjennom dette nettverket. Enhetene kan være koblet direkte til dette nettverket eller via mindre mobile nettverk. Hovedfunksjonen til de deployerbare nettverkene vil følgelig være;

- Fremskaffe lokal tilknytning til INI for enheter i operasjonsområdet
- Aggregering av trafikk til og fra enheter i operasjonsområdet.
- Muliggjøre lokal tilknytning til andre nasjoners militære nettverk (siden Norge ofte vil operere som en del av en multinasjonal styrke).
- Fremskaffe aksess til det strategiske stamnettet med de tjenester som finnes der.

Kommunikasjonen mellom de globalt deployerte enhetene og det strategiske stamnettet skal realiseres ved bruk av satellitt, tuneller gjennom andre nasjoners militære nettverk, sivile Virtual Private Network tjenester (VPN-tjenester) eller leide linjer.

Mobile taktiske nettverk skal også kunne deployeres som en del av internasjonale eller nasjonale militære operasjoner. Dette er nettverk som skal understøttet enheter og brukerer med krav til høy grad av mobilitet. Eksempler er; kjøretøy, skip og fly. Nettverkene vil benytte seg av radiokommunikasjon som transmisjonsbærer hvor hver node må kunne fungere både som endepunkt og reléstasjon. Enhetene må også kunne benytte seg av ulike typer kommunikasjonsteknologi for å knytte seg til det deployerbare taktiske nettverket som er etablert i området de opererer i.

Den totale kommunikasjonsinfrastrukturen er altså en løsning for å fremskaffe en felles plattform for kommunikasjon mellom alle enhetene i Forsvaret uavhengig av hvor



Figur 31: Topologi for kommunikasjonsinfrastrukturen i NBF [16]

de er deployert. Den felles plattformen er et "Internett-type" nettverk basert på IP-teknologi.

5.2 Faktorer som inngår i risikoanalyse av INI

Det eksisterer en rekke ulike metoder og prinsipper for fastsettelse av risiko og sikkerhetsnivå for informasjonssystemer. Den tradisjonelle og sannsynligvis mest kjente beskrivelsen av risiko uttrykkes som forholdet mellom sannsynlighet for en uønsket hendelse og konsekvensen dersom det skjer:

Risiko = Sannsynlighet x Konsekvens

Norsk Standard 5814 omfatter elementer som ideelt sett inngår i totale risikoanalyser. Standarden benytter den tradisjonelle tilnærmingen til risiko. Risiko defineres som et uttrykk for den fare som uønskede hendelser representerer for mennesker, miljø eller verdier. Risikoen uttrykkes ved sannsynligheten for og konsekvensene av de uønskede hendelsene [85]. Standarden definerer videre en risikoanalyse som en systematisk framgangsmåte for å kartlegge uønskede hendelser og beskrive risiko. Akseptkriterier indikerer sikkerhetsnivået, og det skal iverksettes sikkerhetstiltak for å møte uakseptabel risiko. For informasjonssystemer er en uønsket hendelse noe som påvirker informasjonen eller informasjonssystemets konfidensialitet, integritet eller tilgjengelighet.

Nærings- og handelsdepartementet benytter også den tradisjonelle definisjonen av risiko ved analyse av ikke-villede (tilfeldige) hendelser [30]:

Risiko = Sannsynlighet for svikt x Konsekvensen av en eventuell svikt

der sannsynlighet for svikt er en kombinasjon av hvilke sviktsituasjoner som teoretisk vil kunne oppstå, kunnskap om tidligere hendelser og hvor utsatt og sårbart systemet som

helhet er overfor disse situasjonene. For de fleste komplekse systemer vil det være mulig med bakgrunn i erfaringer å anslå en repetisjonsrate eller sviktintensitet som grunnlag for et sannsynlighetsmål.

ROS (Risiko og Sårbarhetsanalyse) metoden fra 2000 er et tredje eksempel på risikoanalyse som benytter seg av den tradisjonelle definisjonen av risiko [86]. Metoden er utviklet i et samarbeid mellom Sikkerhetsstaben i Forsvarets overkommando (FO/S), Norges teknisk-naturvitenskapelige universitet (NTNU) og direktoratet for sivilt beredskap (DSB). Metoden ble videreutviklet i et samarbeid mellom Nasjonal sikkerhetsmyndighet (NSM) og NTNU i 2004 [87]. Også denne videreutviklede metoden benytter en tradisjonell tilnærming til risiko.

Den tradisjonelle definisjonen av risiko fungerer bra i forhold til safety-relaterte risikoanalyser. Det kan imidlertid være problematisk å benytte denne for security-relaterte risikoanalyser. Problemet er knyttet til anvendelsen av sannsynlighet. Holm beskriver dette på følgende måte i sin Masteroppgave fra HiG (2004)[82]:

> Tilstedeværelse av tilfeldighet er et krav som må innfris før en kan gjøre sannsynlighetsberegninger og statistiske undersøkelser. I safety scenarier kan det antas at hendelser inntreffer tilfeldig, og bruk av stokastiske metoder med estimater for sannsynlighet vil følgelig være gyldige. Men i et security perspektiv hvor det er snakk om tilsiktede handlinger som ikke er tilfeldige, vil sannsynlighetsberegninger kunne medføre gyldighetsproblemer. For eksempel vil sannsynligheten være lik 1 og ikke en statistisk verdi fremkommet av erfaringsdata, når en motstander har bestemt seg for å gjennomføre et angrep.

Nærings- og handelsdepartementet anerkjenner også dette problemet. De benytter derfor en annen tilnærming for analyse av villede handlinger enn den som tidligere ble skissert for tilfeldige hendelser [30]:

> Villede angrep kan være utført av et vidt spekter med aktører fra enkeltpersoner til grupperinger, organisasjoner, virksomheter og stater. Det er imidlertid ikke lenger hensiktsmessig å snakke om sannsynlighet for svikt i tradisjonell forstand, ei heller kan en snakke om sannsynlighet for at en hendelse vil finne sted. Det finnes svært lite empiri på omfattende angrep mot IKT-systemer, særlig når det gjelder logiske virkemidler av nyere dato. Det er mer hensiktsmessig å se på hva som er mulig med bakgrunn i en teknisk vurdering. Mulighet for svikt som følge av en villet handling kan uttrykkes som:
>
> Mulighet for svikt = Angripers motiv og intensjon x Angripers kapasitet x Sårbarhet
>
> Et angrep må være fundert i et motiv og en intensjon om å utrette skade. Dette kan dekke hele spekteret fra ren underholdningsverdi for angriperen, via økonomisk vinning til et ønske om å skade en fremmed makts interesser. Dette er imidlertid ikke tilstrekkelig. En angriper med en gitt intensjon må også samtidig ha kapasitet til å gjennomføre angrepet gjennom å beherske de nødvendige fysiske, elektroniske, logiske og sosiale virkemidler. Systemet som angripes må også være sårbart overfor den kapasitet en angriper innehar. Med denne definisjonen kan en studere et spekter av mulige aktører og hvilke motiv og intensjon disse vil kunne ha for et eventuelt angrep. Dette kan så vurderes opp mot hvilken kapasitet disse vil kunne forventes å ha i dag og i fremtiden. Hvorvidt de virkelig noen gang vil gjennomføre et angrep er svært usikkert og vil være helt avhengig av den videre utviklingen. Det sentrale spørsmålet blir til slutt om vi kun skal sikre oss mot det som er sannsynlig, eller om vi også bør sikre oss mot det som er mindre sannsynlig, men likevel mulig.

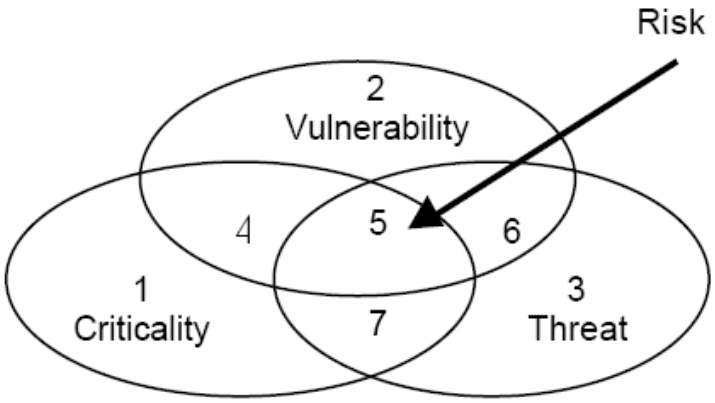
Flere andre metodiske tilnærminger til risikoanalyse benytter seg av et relativt likt syn på risiko, men utvider det til også å omfatte informasjonens verdi[88, 17, 89]. I disse metodene defineres risiko som et resultat av verdi, trussel og sårbarhet [88]:

Verdi Med verdi menes den betydning eller viktighet en virksomhet, objekt eller person representerer. Mao: hvor kritisk er informasjonen for organisasjonens virksomhet?

Trussel Trusselen representerer eksterne krefter som har til hensikt å skade, kompromittere eller stjele de angitte verdiene, som er utledet ved en verdivurdering.

Sårbarhet Sårbarhet er tekniske, organisatoriske, menneskelige eller rutinemessige feil og mangler som gjør at trusselaktøren kan fullbyrde sin hensikt.

Med en slik tilnærming toner man ned sannsynlighetsbegrepet og vurderer i stedet hva som er mulig med bakgrunn i en vurdering av faktorene verdi, trussel og sårbarhet for det aktuelle informasjonssystemet. I dette scenariet eksisterer risiko der de tre faktorene overlapper hverandre;



Figur 32: Risiko eksisterer der kritisk informasjon (verdi), trussel og sårbarhet overlapper [17]

Sirklene i figur 32 omfatter den totale mengden av informasjon, systemer, programmer, mennesker, materiell og fasiliteter som utgjør det aktuelle informasjonssystemet. Den følgende listen beskriver delmengdene som utgjør helheten (tallene i listen korresponderer med tallene som identifiserer hver delmengde i figur 32) ;

1. Kritiske objekter (informasjon, systemer, programmer, mennesker, utstyr eller fasiliteter) som ikke har noen kjente sårbarheter eller trusler.
2. Sårbarheter i systemer, programmer, mennesker, utstyr eller fasiliteter som ikke er assosiert med kritiske objekter og som ikke har kjente trusler.
3. Trussel hvor det ikke eksisterer utnyttbare sårbarheter i kritiske objekter.
4. Kritiske objekter som har kjente sårbarheter men ingen kjente trusler.
5. **Kritiske objekter som har kjente sårbarheter og trusler. Dette er det mest sensitive området og utgjør risiko.**
6. En trussel eller et antall trusler har tilegnet seg kunnskap og/eller kapasitet til å utnytte en sårbarhet men ikke til et kritisk objekt.

7. Kritisk objekt som har ingen kjente sårbarheter, men det er eksponert for en spesifisert trussel.

En fordel ved en slik tilnærming til å analysere risiko er at det virker konsistent og gyldig relatert til security. Det kan være en svakhet ved denne metoden at den kan bli for overordnet og generell til å kunne foreta en grundig analyse av informasjonssystemer. I denne oppgaven vil vi gjennomføre en overordnet analyse av hvordan implementeringen av NBF kan medføre endringer innen risikobildet. Det innebærer at vi ikke har behov for stor grad av detaljer i vår vurdering, følgelig er denne risikomodellen egnet for vår oppgave. I de påfølgende kapitlene vil vi derfor vurdere hvordan faktorer som endres ved implementeringen av NBF kan påvirke verdi, trussel og sårbarhet for INI. Det er med andre ord et dynamisk syn som legges til grunn; hvordan faktorene som definerer risikoen vil endres over tid som et resultat av implementeringen av NBF. I henhold til oppgavens avgrensning, vil vi fokusere på villede logiske hendelser.

5.3 INI's verdi

5.3.1 INI's verdi for Forsvaret

Den første faktoren vi vil vurdere i vår risikoanalyse er verdi. Siden INI er informasjonssystemet som skal muliggjøre NBF, vil vurderingen fokuseres mot INI's fremtidige verdi for Forsvaret. Dersom vi rekapitulerer begrepet verdi fra definisjonen i forrige kapittel, husker vi at den var som følger:

> Med verdi menes den betydning eller viktighet en virksomhet, objekt eller person representerer. Mao: hvor kritisk er informasjonen/informasjonssystemet for organisasjonens virksomhet?

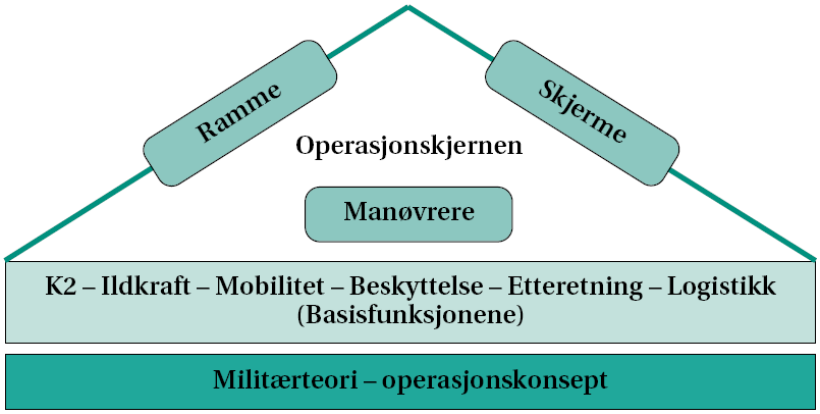
Kritisk informasjon og informasjonssystemer understøtter prosesser som er kritiske for en gitt organisasjon. Dette er prosesser som organisasjonen er avhengig av for å skape de produktene de produserer. Produkttyper kan i denne sammenhengen spenne over et vidt spekter fra tjenester, som for eksempel militær effekt, til rene råvarer, som for eksempel biler. For å avgjøre hvor stor grad av verdi INI vil representere for Forsvaret, må vi derfor vurdere følgende;

1. Hva er kritisk informasjon og informasjonssystemer for Forsvaret?
2. Vil INI understøtte kritisk informasjon og kritiske funksjoner?
3. Hvilken konsekvens vil det kunne medføre dersom denne kritiske informasjonen angripes?

Kritisk informasjon for Forsvaret er informasjon som er knyttet til de viktigste prosessene som Forsvaret må kunne utføre for å produsere sitt produkt; militær effekt. Forsvarets fellesoperative doktrine (FFOD), del A Grunnlag [18]gir en oversikt over funksjoner som er kritiske for Forsvaret i det som kalles "Den indre doktrinesløyfen"(se figur 33).

Den indre doktrinesløyfen viser sammenhengen mellom operasjonskjernen, de militære basisfunksjonene og operasjonskonseptet:

> Den indre doktrinesløyfen virker på følgende måte: Militærteorien og operasjonskonseptet som er avledet fra den, vil på kort sikt føre til endringer eller justeringer i utdanning, trening, øvelser og operasjonsmønstre. Operasjonskonseptet vil samtidig kreve endringer av militære kapasiteter og av forsvarsstruktur. Det gjør konseptet ved å stille "krav "til utvikling av basisfunksjonene.



Figur 33: "Den indre doktrinesløyfen"[18]

Operasjonskjernen beskriver tre grunnleggende faktorer som alltid skal utgjøre kjernen i planlegging og gjennomføring av militære operasjoner. Dette er prinsipper som legges til grunn ved bruk av militære stryker (operativ planlegging) og kan følgelig ansees som grunnleggende forutsetninger for å utkjempe en kamp:

Ramme kunne angripe motstanderen

Manøvrere kunne bevege seg for å komme i en posisjon hvor du kan angripe vitale punkt hos motstanderen eller for å skjerme seg mot angrep fra motstanderen (ergo: både for å ramme og skjerme)

Skjerme kunne beskytte seg selv mot angrep fra motstanderen

De militære basisfunksjoner er rettet mot utvikling av militære styrker og defineres som grunnleggende funksjoner som militære avdelinger/enheter må kunne utøve for å være effektive. Effektivitet er i denne sammenhengen relatert til å kunne levere militær effekt gjennom utførelsen av militære operasjoner. Disse basisfunksjonene regnes derfor som kritiske for Forsvarets evne til å utføre militære operasjoner etter prinsippene gitt av operasjonskjernen:

Kommando og kontroll - for å lede og koordinere

Ildkraft - for å ramme

Mobilitet - for å manøvrere

Beskyttelse - til egensikring

Etterretning - for å danne seg et bilde av hva som skjer (situasjonen)

Logistikk - for utholdenhet og transport

Siden dette er kritiske funksjoner for Forsvaret, kan vi utlede at informasjon og informasjonssystemer som understøtter disse også vil være kritiske verdier for utførelse av militære operasjoner. Referansemodellen for INI (se figur 29) viser at alle disse kritiske funksjonene skal understøttes av hver sin funksjonsvise beslutningsstøttetjeneste.

Dette innebærer at INI på lengre sikt skal inneholde tjenester som understøtter alle de funksjoner som regnes som kritiske for Forsvaret (se tabell 9). INI vil følgelig inneholde tjenester som er av svært høy verdi for gjennomføring av militære operasjoner.

Militær basisfunksjon	**Tjeneste i INI**
Kommando og kontroll (K2)	K2 og ledelsestjenester
Ildkraft	Ildstøttetjenester
Mobilitet	Manøveroperasjonstjenester
Beskyttelse	Beskyttelsetjenester
Etterretning	Etterretnings- og overvåkningstjenester
Logistikk	Logistikktjenester

Tabell 9: Militære basisfunksjoner og deres korresponderende tjenester i INI

NBF konseptet er etter vår mening en materialisering av Business Process Reengineering (BPR) for Forsvaret. Når BPR er nært knyttet sammen med innovativ anvendelse av informasjonsteknologi, kan det defineres som [90];

> Omforming av virksomhetsprosesser gjennom kreativ bruk av informasjonsteknologi.

BPR kalles gjerne radikal prosessforbedring på norsk og det refererer seg til innovativ fornying av større eller mindre deler av virksomheten til en organisasjon. Med fornying menes en omfattende forandring av virksomhetsprosesser, rutiner og måter å utføre arbeid på. Målet er å oppnå en radikal forbedring for organisasjonens funksjoner [91];

> ...en fundamental og radikal omforming av virksomhetsprosesser i den hensikt å oppnå dramatiske forbedringer som gir målbare resultater på kriterier som kostnad, kvalitet, service og (lede)tid.

I BPR-sammenheng er altså målet å oppnå dramatiske resultatforbedringer. Her snakker man ikke om prosentvise forbedringer, men heller flere ganger forbedring. Man kan si at mottoet for BPR er; “10x, ikke 10% ”.

Informasjonsteknologi fungerer som sagt ofte som en muliggjørende faktor (katalysator) i BPR. INI er den konkrete informasjonsteknologien (informasjonssystemet) som skal muliggjøre NBF konseptet (“BPR for Forsvaret ”). Resultatet som skal forbedres dramatisk er evne til å skape militær effekt (med færre enheter). I “Konsept for nettverksbasert anvendelse av militærmakt”[71], antydes det en forventing om at NBF vil medføre en seksdobling av militær effekt. Undersøkelser fra USA basert på NCO CF indikerer at dette muligens er et noe høyt tall. Et eksempel på dette er “Network-Centric Operations Case Study Air-to-Air Combat With and Without Link 16”[78] som vi har omtalt tidligere. Forsøket viste at enhetene med den beste informasjonsposisjonen kunne skape 2,5 ganger mer militær effekt enn sine opponenter. Uavhengig av det nøyaktige tallet for hvor stor effektforbedring INI kommer til å skape, uttaler de fleste norske dokumenter som omhandler NBF at INI trolig kommer til å være den største styrkemultiplikatoren for Forsvaret i fremtiden. Dette forutsetter en sikker funksjon av INI med tanke på informasjonens konfidensialitet, integritet og tilgjengelighet. Vi kan derfor utlede at vellykkede logiske angrep mot INI vil kunne få dramatisk konsekvens for Forsvarets evne til å skape militær effekt gjennom militære operasjoner. I sin ytterste konsekvens kan det føre til flere ganger redusert evne til å levere militær effekt.

5.3.2 Dynamisk utvikling av INI's verdi

Implementasjonen av NBF vil gå over flere år (se estimat av tidsramme i figur 26). Graden av nettverksorganisering for Forsvaret angis av tre ulike nivåer for NBF modenhetsgrad. INI vil følge en tilsvarende gradvis utvikling og vil være på et gitt utviklingsnivå korrelert med NBF modenhetsgrad. Alle tjenestene i INI som skal understøtte Forsvarets kritiske virksomhetsprosesser (militær basisfunksjon) vil ikke implementeres simultant. Dette betyr at de vil gradvis innlemmes i INI på ulike trinn i dens utviklingsnivå. Med andre ord vil det være slik at flere og flere av de militære basisfunksjonene vil over tid understøttes av tjenester i INI.

Realiseringen av NBF omfatter mye mer enn å bygge ut et INI. NBF krever en fundamental og radikal omforming av virksomhetsprosesser gjennom kreativ bruk av informasjonsteknologien som INI representerer. Denne omleggingen av virksomhetsprosesser vil også gjennomføres gradvis over tid og være korrelert med NBF modenhetsgrad. Dette vil medføre en stadig økning i avhengighet av en fungerende INI for effektiv utførelse av militære operasjoner. Vi vil med andre ord se en gradvis radikal omforming av militære basisfunksjoner slik at de blir stadig mer avhengige av INI for å fungere effektivt. Et enkelt eksempel som kan illustrere en slik utviklingen er en overgang fra bruk av kart og kompass til databaserte kart med GPS for navigasjon. Overgangen vil, ettersom brukerne opparbeider erfaring med det nye systemet, medføre en bedre evne til navigering. Samtidig vil det medføre en forringelse av kunnskap om navigering ved hjelp av kart og kompass. Dersom det etter en stund oppstår en feil med GPS systemet slik at brukerne er nødt til å returnere til kart og kompass igjen, er det trolig at de vil være enda dårligere til å navigere ved hjelp av disse verktøyene enn det de var før de fikk det nye elektroniske navigasjonssystemet. Årsaken ligger i at de ikke lengre har trening i bruk av kart og kompass. Resultatet vil med andre ord være at de en periode (til de får tilegnet seg ny eller oppfrisket kompetanse) vil være mindre effektive til å navigere.

Som vi så i kapitlet om tilsiktet effekt for NBF vil en nettverksorganisering av Forsvaret blant annet omfatte en ny kommandostruktur og organisasjonsform enn den vi benytter i dag. Denne endringen er basert på muligheter skapt av INI. Dersom INI kompromitteres (bortfall av konfidensialitet, integritet eller tilgjengelighet) etter en slik omorganisering og omlegging av virksomhetskritiske prosesser, vil det trolig få store konsekvenser for Forsvarets evne til å utføre militære oppdrag. Det er sannsynlig at Forsvaret evne til å skape militær effekt med et gitt antall enheter vil være enda dårligere enn det den var før innføringen av INI. Årsaken er at Forsvaret ikke lengre har den kompetansen som kreves for å operere etter de organisasjonsformene, kommandostrukturene og prosesser som må benyttes i en "ikke-nettverksorganisert organisasjon ".

INI er entiteten som muliggjør en radikal forbedring av Forsvarets informasjonsposisjon. INI's verdi er med andre ord direkte korrelert med Forsvarets evne til å skape militær effekt (ref. kapitlet om tilsiktet effekt for NBF). Denne evnen vil øke med hvilken NBF modenhetsgrad Forsvaret befinner seg på. En overgang fra en modenhetsgrad til en annen innebærer at stadig flere av de militære basistjenestene vil være avhengige av tjenester i INI og en større grad av tilpasning av disse militære basistjenestene slik at de utnytter mulighetene INI gir. Resultatet er en økt evne til å skape militær effekt. Verdiøkningen for INI er derfor sammenfallende med CLD-modellen vi utviklet i kapitlet om tilsiktet effekt for NBF og drives av NBF modenhetsgrad.

5.4 Trussel mot INI

Den andre faktoren vi vil vurdere i vår risikoanalyse er trusselen. I begynnelsen av kapitlet definerte vi trussel som:

> Trusselen representerer eksterne krefter som har til hensikt å skade, kompromittere eller stjele de angitte verdiene, som er utledet ved en verdivurdering.

En trussel mot INI er i denne sammenhengen altså en entitet som har til hensikt å angripe integriteten, tilgjengeligheten eller konfidensialiteten til tjenestene som understøtter de militære basisfunksjonene vi identifiserte i forrige kapittel. Selv om definisjonen inneholder en pressisering om at det er eksterne krefter det fokuseres mot, betyr dette ikke at et logisk angrep ikke kan implementeres av noen som har autorisert tilgang til systemet. Dette kan for eksempel skje ved at en ekstern entitet verver eller tvinger en autorisert bruker til å utføre angrepet.

Med eksterne krefter menes trusselagenter. En trusselagent er et individ eller en gruppe individer som vil implementere trusselen. Norges sikkerhetspolitiske situasjon gjør det vanskelig å peke på konkrete trusselagenter i denne sammenhengen. Dette fremgår av den globale sikkerhetspolitiske utviklingsretningen som legges til grunn for norsk sikkerhetspolitikk [36]

> **Om forventet sikkerhetspolitisk utvikling:** At omfanget av sikkerhetsutfordringer (risikoer og trusler mot den kollektive sikkerhet og internasjonal fred og stabilitet) som må håndteres på kort og midlere sikt vedvarer eller øker i antall og eventuelt intensitet, men uten at den mer langsiktige utviklingen dreier i en negativ retning (en usikker utviklingsretning)
>
> **Om forventet trusselbilde:** Trusler kan oppstå og utvikle seg raskt og uten særlig forvarsel, blant annet fordi også ikke-statlige aktører kan true sikkerheten. Mulighetene for at Norge kan bli trukket inn i konflikter - både direkte og indirekte - er reelle. Det er sannsynlig at flere mindre konflikter kan opptre samtidig. Større internasjonale væpnede konflikter, inkludert omfattende krig mellom stater, kan heller ikke utelukkes.

Det eksisterer med andre ord ingen eksplisitt utpekte trusselagenter mot Norge eller det norske Forsvaret. Det identifiseres imidlertid et svært dynamisk trusselbilde som tilsier at konkrete trusselagenter raskt kan oppstå på bakgrunn av sikkerhetspolitiske endringer. Et eksempel i denne sammenhengen kan være at Norge deltar i en fredsopprettende styrke for å påtvinge fred i en nasjon eller et geografisk område. Alle parter som rammes negativt av denne hendelsen vil da fremstå som potensielle trusselagenter.

Siden det ikke er mulig å identifisere spesifikke trusselagenter, kan det være mer hensiktsmessig å se på ulike aktørgrupper av potensielle trusselagenter og vurdere hvilke av disse som er mest sannsynlige for Forsvaret. En oversikt over mulige aktørgrupper for logiske angrep mot Norges nasjonale infrastruktur er presenter i “Samfunnets sårbarhet som følge av avhengighet til IT ”[30];

1. Inkompetent
2. Underholdningshacker
3. Forulempet ansatt
4. Kjeltring
5. Organisert kriminalitet

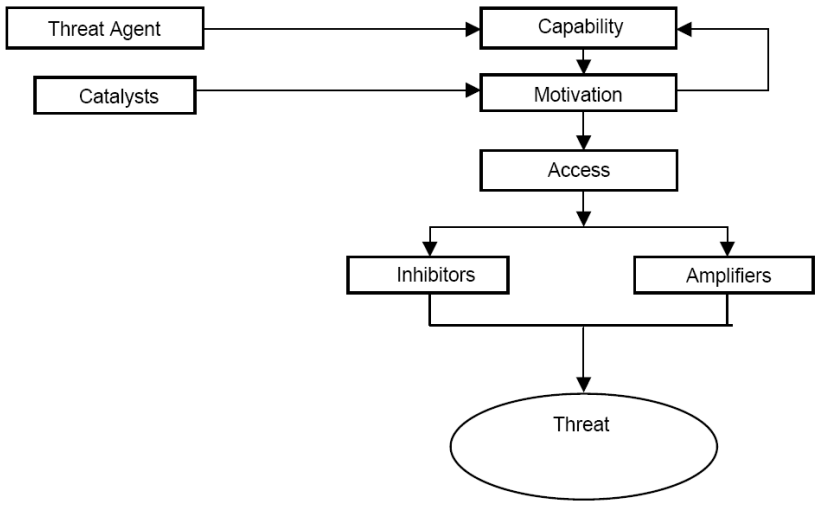
6. Terroristgruppering
7. Nasjonalstatlig

Av disse aktørgruppene er det nasjonalstater og terroristgrupperinger som fremstår som de mest sannsynlige trusselagentene mot INI. Dette begrunnes med at dette er aktører som vil kunne befinne seg i direkte konfrontasjon med Forsvaret. Det dynamiske trusselbildet tilsier at konkrete trusselagenter vil variere over tid. I det følgende vil vi derfor legge til grunn en generisk vurdering av globale trender relatert til faktorer som er sentrale i en trusselvurdering.

Andrew Jones har utviklet en modell som beskriver hvilke elementer som definerer en trussel mot informasjonssystemer [81, 83] (se figur 34). I følge modellen eksisterer det to ulike typer trusselagenter;

Naturlige trusler og uhell Denne gruppen består av ufrivillige trusselagenter og omfatter uhell forårsaket av mennesker eller naturlige hendelser som brann eller jordskjelv.

Ondsinnede Denne gruppen består av de trusselagentene som utfører sine handlinger med overlegg.



Figur 34: Elementer som definerer trussel mot et informasjonssystem

I vår avgrensning av denne oppgaven har vi valgt å bare fokusere på villede logiske angrep. Dette medfører at vi bare vil inkludere den siste gruppen trusselagenter i vår analyse. Ondsinnede trusselagenter har følgende egenskaper (se figur 34):

Motivasjon En årsak som gjør at trusselagenten vil angripe et informasjonssystem. Med andre ord et bevisst mål de ønsker å oppnå.

Evne En evne/kapasitet til å utføre et angrep mot informasjonssystemet. Dette innebærer faktorer som; personell, kunnskap, ferdigheter og teknologi.

Katalysator En årsaksfaktor som styrer om og når en trusselagent implementerer et angrep mot et informasjonssystem. Dette kan være en hendelse som for eksempel

starten av en væpnet konflikt mellom trusselagentens hjemland (eller en han sympatiserer med) og en opponent.

Hemmere/forsterkere Et sett av faktorer som kan enten undertrykke eller fremme en trusselagents evne til å utføre vellykkede angrep mot et informasjonssystem. Avhengig av konteksten kan en og samme faktor virke enten undertrykkende eller fremmende på potensialet for et vellykket angrep. Et eksempel kan være hvilket sikkerhetsnivå som eksisterer i målet. Dersom sikkerheten er ivaretatt på en god måte, kan det virke som en hemmende faktor. Dersom sikkerheten er dårlig ivaretatt, kan den virke som en fremmende faktor.

Aksess En trusselagent er avhengig av aksess til informasjonssystemet dersom han skal være i stand til å implementere et angrep mot det. Aksess kan være enten direkte fysisk tilgang til komponentene i informasjonssystemet, eller elektronisk via det nettverket komponentene er tilkoblet.

Et vellykket angrep er også avhengig av to egenskaper ved informasjonssystemet som skal angripes. For det første må det eksistere en eller flere sårbarheter i det som trusselagenten kan utnytte. I tillegg må systemet ha høy verdi for organisasjonen som eier det. Dette innebærer at tap eller degradering av konfidensialitet, integritet og/eller tilgjengelighet vil ha stor nok påvirkning på organisasjonens virksomhetsprosesser til at angriperen anser angrepet som en vellykket.

Som en oppsummering av denne modellen kan vi si at for at en ondsinnet trusselagent skal utgjøre en reell trussel mot INI, må følgende faktorer være tilstede:

1. Trusselagenten må ha motivasjon for å gjennomføre et logisk angrep.
2. Trusselagenten må ha evne til å gjennomføre et logisk angrep.
3. Trusselagenten må ha mulighet til å gjennomføre et logisk angrep (han må ha aksess til INI og INI må inneholde sårbarheter som han kan utnytte)

5.4.1 Motivasjon for logiske angrep mot INI

Økt anvendelse av IKT for å skape militær effekt er ikke spesifikt for Norge. Globalt ser man en økende grad av IKT-integrering i moderne militære organisasjoner. Dette medfører at militære planleggere har begynt å anse IKT som både et våpen og et mål på lik linje med andre komponenter. Resultatet er at enheter med evne til logiske angrep kommer til å bli en integrert del av framtidens militære operasjoner [92];

> Countries around the world are developing and implementing cyber strategies designed to impact an enemy's command and control structure, logistics, transportation, early warning and other critical, military functions. In addition, nations are increasingly aware that the use of cyber strategies can be a major force multiplier and equaliser. Smaller countries that could never compete in a conventional military sense with their larger neighbours can develop a capability that gives them a strategic advantage, if properly utilised. As a RAND Corporation study pointed out in the mid-1990s, the entry costs for conducting cyber war are extremely modest. Therefore, countries that are not as dependent on high technology within their military establishment consider such dependence a potential "Achilles heel " for their enemies.

Kombinasjonen av potensiale for å gi stor effekt og en lav inngangskostnad motiverer altså både høyteknologiske og andre aktører til å utvikle evne til logiske angrep. Logiske

angrep ansees ofte som både et strategisk og operasjonelt middel for krigføring. Det eksisterer ingen felles global terminologi innen dette feltet enda, men de fleste skiller mellom bruk av logiske angrep mot nasjonale (NII) og militære informasjonsinfrastrukturer (DII). Den første kategorien kan benyttes som et frittstående alternativ eller i kombinasjon med angrep med konvensjonelle styrker. Den andre kategorien benyttes i væpneden konflikter som en del av en militær operasjon. Forskere fra CERT ved Carnegie Mellon University har utviklet følgende klassifisering av hvordan logiske angrep kan benyttes i krigføring [92]:

Cyber war as an adjunct to military operations The aim, in Clausewitzian terms, is to increase the "fog of war" for the enemy and to reduce it for one's own forces. This can be achieved through direct military strikes designed to degrade the enemys information-processing and communications systems or by attacking the systems internally to achieve, not denial of service, but a denial of capability. In effect, this form of cyber warfare focuses almost exclusively on military cyber targets.

Limited cyber war In a limited cyber war, the information infrastructure is the medium, target and weapon of attack, with little or no real-world action accompanying the attack. Limited cyber war of this kind could be designed to slow an adversary's preparations for military intervention, as part of an economic warfare campaign, or as part of the manoeuvring that typically accompanies a crisis or confrontation between states.

Unrestricted cyber war A form of warfare that has three major characteristics. First, it is comprehensive in scope and target coverage with no distinctions between military and civilian targets or between the home front and the fighting front. Second, unrestricted cyber war has physical consequences and casualties, some of which would result from attacks deliberately intended to create mayhem and destruction, and some of which would result from the erosion of what might be termed civilian command and control capabilities in areas such as air-traffic control, emergency-service management, waterresource management and power generation. Third, the economic and social impact (in addition to the loss of life) could be profound. An unrestricted cyber campaign would almost certainly be directed primarily against the target countrys critical national infrastructure: energy, transportation, finance, water, communications, emergency services and the information infrastructure itself. It would likely cross boundaries between government and private sectors, and, if sophisticated and coordinated, would have both immediate impact and delayed consequences. Ultimately, an unrestricted cyber attack would likely result in significant loss of life, as well as economic and social degradation.

Siden INI er en del av norsk DII (og i fremtiden kanskje utgjør hele den norske DII), er det hovedsakelig angrep med motiver fra den første klassen som er aktuelle for INI; i forbindelse med væpnede konflikter. En væpnet konflikt kan kort beskrives som et voldelig sammenstøt mellom to viljer eller interesser, hvor formålet er å påtvinge motstanderen ens egen vilje [74]. Slike sammenstøt kan skje mellom nasjonalstater, men også innenfor andre rammer. Et eksempel på dette kan være borgerkriger og ikke-statlige aktører som terrorister. I væpnede konflikter er de stridende parters evne til å utøve fysisk makt (skape militær effekt) være av avgjørende betydning for utfallet av konflikten.

INI er en muliggjører for NBF-konseptet som skal øke Forsvarets evne til å skape militær effekt i de fysiske domenene (land, sjø og luft). Den er en styrkemultiplikator som setter Forsvaret i stand til å levere mer militær effekt per enhet. Konsekvensen er at Forsvaret totalt sett vil øke sin relative militære effekt i forhold til en motpart i en væpnet konflikt. Motparten kan i hovedsak velge to ulike metoder eller kombinasjoner av disse for å imøtegå en slik utvikling:

1. Øke sin egen kapasitet i de fysiske domenene ved å anskaffe flere og/eller bedre enheter.
2. Redusere Forsvarets evne til å skape økt militær effekt per enhet gjennom å angripe styrkemultiplikatoren.

De to alternativene relaterer seg til to grunnleggende ulike syn på krigføring; utmattelseskrigføring og manøverkrigføring [74]. Kjennetegnet ved utmattelseskrigføring er at man søker seier gjennom en kumulativ ødeleggelse av fiendens materielle aktiva ved bruk av overlegen ildkraft, muliggjort ved en betydelig industriell basis og teknologisk overlegenhet. En tilhenger av utmattelseskrigføring betrakter fienden som et angrepsmål som skal engasjeres og ødelegges systematisk . Dersom vi vurderer dette alternativet i lys av undersøkelsene som indikerer at forbedret informasjonsposisjon kan gi flere ganger økt militær effekt, ser vi at denne løsningen kan være svært ressurskrevende. Et eksempel som illustrerer hvor ressurskrevnede det kan være er undersøkelsen som viste at jagerfly med radio og Link16 hadde en kill-ratio på 2,5:1 i forhold til jagerfly som bare hadde radio. Dersom vil legger denne observasjonen til grunn, innebærer det at motparten må anskaffe og bemanne 2,5 ganger så mange enheter som Forsvaret for å utjevne ubalansen i evne til å skape militær effekt.

Manøverkrigføring forutsetter at det er mulig å omgå et problem og angripe det fra en “fordelaktig posisjon ” i stedet for å gå direkte på det. Teorien legger vekt på å unngå en motstanders hovedstyrker og i stedet kraftsamle mot utvalgte, relativt sett svakere mål. To begreper i manøverteorien er sentrale i forhold til valg av hvilke mål en skal angripe; tyngdepunkt og vitale punkter. Clausewitz innførte begrepet tyngdepunkt (Center of Gravity) og definerte det som “et sentrum av kraft og bevegelse som alt avhenger av” [76]. En motstanders tyngdepunkt hviler på et eller flere vitale punkter. Formålet med en tyngdepunktbetraktning er å avdekke hvorfra en motstander får sin handlefrihet, fysiske styrke eller vilje til motstand. På det operasjonelle nivået vil det ved militære operasjoner være naturlig å konsentrere tyngdepunktbetraktningene om en motstanders militære styrke, om hans evne til å gjennomføre militære operasjoner og mer indirekte om de faktorer som understøtter motstanderens evne til å bruke militær makt. Siden en forventer at INI skal bli den største styrkemultiplikatoren i det nettverksbaserte Forsvaret, er det logisk å anta at INI vil betraktes som et operasjonelt tyngdepunkt av Forsvarets fremtidige motstandere. Gjennom logiske angrep mot INI kan en motstander potensielt angripe konfidensialiteten, integriteten og tilgjengeligheten til alle tjenestene som understøtter de militære basistjenestene. Motivasjonen er at angrep i det virtuelle domenet har potensiale for å gi svært store fordeler i de fysiske domenene. Denne tilnærmingen vil trolig også være langt mer kosteffektiv enn å øke antall militære enheter.

5.4.2 Evne til logiske angrep mot INI

I tillegg til motivasjon, må en motstander ha evne til å gjennomføre logiske angrep mot INI for å utgjøre en reell trussel. På et overordnet nivå innebærer dette at trusselagenten må ha tilgang til virkemidler for logiske angrep og evne til å bruke disse innenfor rammene av en koordinert operasjon.

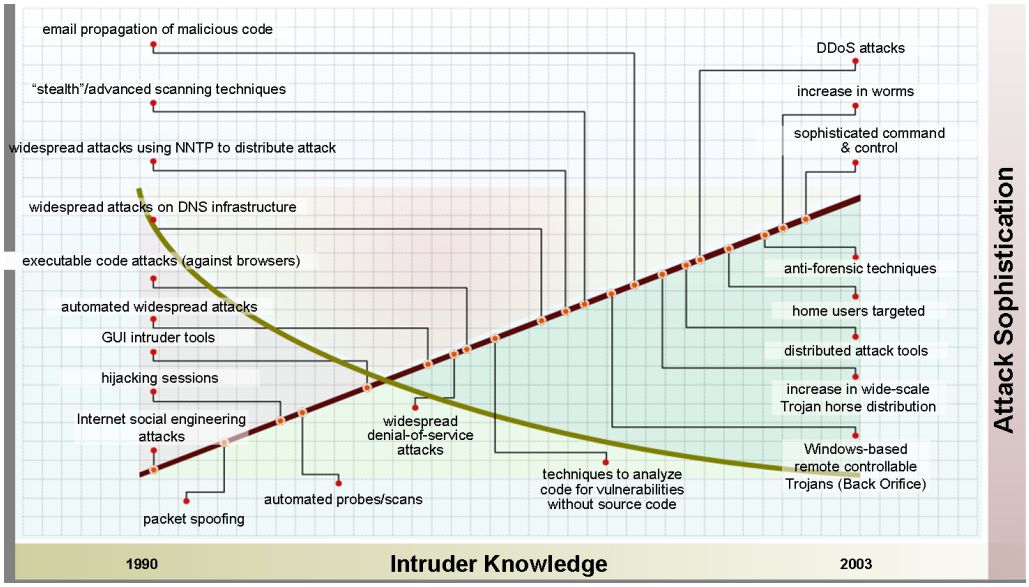
Teknologiske virkemidler for logiske angrep mot informasjonssystemer skiller seg fra tradisjonelle virkemidler for krigføring ved at de er langt letter å anskaffe og/eller utvikle (relativt til for eksempel å utvikle eller anskaffe et jagerfly). På Internett eksisterer det en stor mengde fritt tilgjengelige programmer som kan benyttes for logiske angrep. Disse kan vanligvis lastes ned anonymt av enhver med tilgang til Internett. Listen i figur 35, som er utviklet av Nasjonal sikkerhetsmyndighet i 2006 [84], viser en oversikt over teknologiske virkemidler som kan benyttes for å utnytte sårbarheter i informasjonssystemer. De aller fleste av disse er rene logiske virkemidler (programvare) og kan anskaffes gratis fra Internett. Listen viser at det eksisterer virkemidler som kan angripe alle typer sikkerhetsmessige egenskaper i et informasjonssystem (konfidensialitet, integritet og tilgjengelighet).

Uønskede konsekvenser / Virkemidler	Data på avveie	Modifisering av data	Sletting av data	Reduksjon/eliminasjon av datatilgjengelighet
Ondsinnet kode				
Virus	X	X	X	X
Ormer	X	X	X	X
Mobil ondsinnet kode	X	X	X	X
Trojaner	X	X	X	X
Bakdører	X	X	X	X
Spionprogramvare	X	X	X	X
Rootkit	X	X	X	X
Tjenestenektangrep				
Botnet	X	X	X	X
Søppelpost			X	X
Elektromagnetisk jamming/destruksjon			X	X
Svindel				
Phishing/pharming	X			
Avtitting				
Skjult kamera	X			
Mobilkamera	X			
Avlytting				
Nettverkssniffing	X			
Mikrofoner	X			
Smugling av stjålne data				
Trådløse bærbare terminaler	X			
Minnebrikker og mobile disker	X			

Figur 35: Virkemidler for logiske angrep korrelert med hvilke sikkerhetsegenskaper de angriper

Utviklingstrenden innen logiske midler for angrep går mot stadig mer sofistikerte angrepsverktøy. Når angrep automatiseres gjennom utvikling av programvare, kreves det stadig mindre kunnskap for å implementere angrepene. Forholdet mellom hvor sofistikerte angrepene er og hvor stor teknisk ferdighet som trengs for å implementere dem fremgår av trendanalysen i figur 36 som er utviklet av CERT. Den røde streken indikerer økt grad av sofistikerthet i logiske midler for angrep. Den Grønne linjen indikerer redusert behov for tekniske ferdigheter for å kunne implementere angrepene. De aller fleste av slike logiske midler for angrep krever relativt lite maskinvare (prosesseringskraft, minne og lagring) og båndbredde. Et eksempel i denne sammenhengen er et program som heter Metasploit [93]. Dette er et rammeverk for gjennomføring av logiske angrep. Programmet har en hel rekke ferdig utviklede angrep som en bruker kan anvende

gjennom et enkelt GUI. Programmet gir også mulighet for utvikling av egne angrep. Slike rammeverk gjør det mulig for mange å implementere angrep utviklet av noen få spesialister. En meget alvorlig situasjon kan oppstå i denne sammenhengen dersom noen finner en alvorlig sårbarhet og i tillegg gjør en grundig planlegging av hvordan den skal utnyttes før den oppdages og korrigeres (Et såkalt Zero-Day Attack) [94]. Det er svært sannsynlig at trusselagenter relatert til nasjonalstater og terroristorganisasjoner vil ha kapasitet til å utvikle slike angrep. I tillegg eksisterer det et økende svartebørsmarked for kjøp og salg tilsvarende typer logiske angrep [95]. Trusselagenter som ikke har kompetanse til å utvikle egne Zero-Day Attacks kan altså kjøpe dem av andre.



Figur 36: Økt grad av sofistikerthet for logiske midler for angrep vs behov for teknisk ferdighet for å implementere dem [19]

Kombinasjonen av lav kostnad og lett tilgjengelighet gjør at trusselagenter med relativt stor grad av letthet kan tilegne seg logiske midler for angrep mot INI.

Målrettede angrep mot komplekse informasjonssystemer som INI krever mer enn tilgang til logiske virkemidler for å oppnå signinfikant effekt i forbindelse med militære operasjoner. Frittstående, tilfeldige angrep mot INI vil trolig ikke kunne utvikle mer enn en forstyrrende effekt. For å være i stand til systematisk å ramme tjenestene som understøtter de militære basisfunksjonene, må trusselagenten kunne opptre på en koordinert måte. Dette innebærer at han må kunne formulere konsepter og doktriner for anvendelse av logiske virkemidler, identifisere mål han ønsker å oppnå, tilegne seg detaljert informasjon om INI, kunne identifisere sammenhengen mellom tjenester i INI og de militære basistjenestene, identifisere sårbarheter som kan utnyttes for å ramme de identifiserte tjenestene, koordinere de logiske angrepene med operasjoner i de fysiske domenene, evne til å opprettholde effekten over tid, osv.

I følge Rattray [96] viser analyser at organisasjonsmessig tilpasning av ny teknologi for løsning av oppgaver ikke skjer over natten. Trusselagentens implementasjon av de logiske virkemidlene vil altså kreve en bevisst satsing og bruk av ressurser for å tilegne seg organisasjonsmessig teknologisk kapasitet til logiske angrep mot INI. Det eksisterer

indikasjoner på at en rekke nasjoner jorden rundt er i ferd med å implementere en slik egenskap i sine militære organisasjoner. Under følger noen eksempler for dette. Eksemplene er hentet fra en rapport utarbeidet av Institute for Security Technology Studies ved Dartmouth college [97] og en CRS Report for congress [98]:

China Within the framework of an integrated national plan, the People's Liberation Army (PLA) has formulated an official cyber warfare doctrine, implemented appropriate training for its officers, and conducted cyber warfare simulations and military exercises.

China is pursuing the concept of a Net Force (battalion size), which would consist of a strong reserve force of computer experts trained at a number of universities, academies, and training centers. Several large annual training exercises have already taken place since 1997. The Chinese have placed significant emphasis on training younger persons for these tasks.

India The Indian authorities announced a shift in military doctrine in 1998 to embrace electronic warfare and information operations. A new National Defense University and Defense Intelligence Agency (DIA) have been established. According to journalistic accounts, the armed forces plan to establish an information warfare agency within the DIA with responsibility for cyber war, psychological operations, and electromagnetic and sound wave technologies.

Iran U.S. national security experts have included Iran on a published list of countries said to be training elements of the population in cyber warfare. This is illustrated in two ways: first, the armed forces and technical universities have joined in an effort to create independent cyber R & D centers and train personnel in IT skills; and second, Tehran actively seeks to buy IT and military related technical assistance and training from both Russia and India.

North Korea We believe it is possible North Korea is experimenting with offensive cyber attack capabilities, based on Pyongyang's track record of priority resource allocations to the military, its evident endowment of scientists and engineers, and its documented achievements in missile and related military technologies.

Pakistan Well-documented hacker activity in Pakistan and possible ties between the hacker community and Pakistani intelligence services indicate that Pakistan appears to possess a cyber attack capability.

Russia Russia's armed forces, collaborating with experts in the IT sector and academic community, have developed a robust cyber warfare doctrine. The authors of Russia's cyber warfare doctrine have disclosed discussions and debates concerning Moscow's official policy. "Information weaponry," i.e., weapons based on programming code, receives paramount attention in official cyber warfare doctrine.

Other Russians see a military role for cyberwarfare activities, where the goal is for competing sides to gain and hold information advantages over the other. This is accomplished by using specific information technology capabilities to affect an adversary's information systems, decision making processes, command and control

system, and even populace. Some Russians believe that after conflict begins, "combat viruses and other information related weapons" can be used as powerful force multipliers.

United Kingdom (UK) The UK view toward cyberwarfare is similar to that of the United States. Basically, it notes that information warfare refers to actions affecting others' information systems while defending one's own systems in support of national objectives.

Germany For the most part, the German perspective toward cyberwarfare is comparable to that of the United States and the UK. It recognizes a legitimate role for offensive and defensive information warfare in pursuit of national objectives.

USA er trolig den nasjonen som har kommet lengst i å realisere en organisatorisk teknisk kapasitet til å gjennomføre logiske angrep innefor rammen av en militær operasjon. De har hatt en offisiell doktrine for informasjonsoperasjoner siden 1996 [99, 100, 101] som omfatter mål både innen forsvarsstyrkers og nasjoners informasjonsinfrastruktur. I den siste versjonen er angrep og forsvar i datamaskinbaserte informasjonsinfrastrukturer definert gjennom en kapasitet som benevnes Computer Network Operations (CNO). USA anerkjenner det virtuelle domenet (cyberspace) som den femte dimensjonen for krigføring (de fire andre er; land, sjø, luft og verdensromme), og skal opprette en egen kommando for operasjoner i denne dimensjonen som skal være operativ i 2009 [102, 103];

> On Dec. 7, 2005, cyberspace became an official Air Force domain after Secretary of the Air Force Michael W. Wynne and Chief of Staff of the Air Force Gen. T. Michael Moseley introduced a new mission statement. The statement informed Air Force personnel that their new mission was to "deliver sovereign options for the defense of the United States of America and its global interests - to fly and fight in air, space and cyberspace".
>
> Air Force officials will work on plans for the new command throughout 2007, with the goal of going operational in 2009. The Cyber Command will be part of the 8th Air Force.
>
> The Air Force will form the Cyber Command using the 8th Air Force, based at Barksdale Air Force Base, La. About 25,000 of the unit's 40,000 employees are involved in cyber operations, an Air Force spokesman said
>
> The Cyber Command will apply the Laws of Armed Conflict, which include having rules of engagement, delivering proportional responses to attacks and observing distinctions between combatants and civilians.

Det ser altså ut som om en rekke nasjoner har eller er i ferd med å tilegne seg en reell evne for logiske angrep mot informasjonssystemer. Denne oppstår som et resultat av stor tilgjengelighet av logiske virkemidler og bruk av ressurser for å skape organisatorisk teknologisk kapasitet til å anvende disse innenfor rammene av militære operasjoner. Utviklingen viser at nasjonalstater tar det virtuelle domenet på alvor og det er i ferd med å bli en ny dimensjon for krigføring. Det er derfor logisk å anta at jo større motivasjon en trusselagent har for å angripe motpartens informasjonssystemer (som INI), jo mer ressurser vil han benytte for å skaffe seg reell evne til logiske angrep.

5.4.3 Mulighet for logiske angrep mot INI

Den siste faktoren som inngår i vår analyse av trusselen mot INI omhandler en trusselagents mulighet til å gjennomføre logiske angrep mot denne. Det er to faktorer som må være tilstede for at muligheten skal eksistere: det må eksistere sårbarheter i INI og trusselagenten må kunne skaffe seg fysisk eller logisk (via fra et annet nettverk) aksess til INI. Disse to faktorene er i all hovedsak knyttet til egenskaper ved INI og vil behandles i kapittel 5.5.

5.4.4 Dynamisk utvikling av trussel mot INI

INI vil over tid gradvis inneholde stadig flere tjenester som understøtter de militære basistjenestene. Forsvaret vil i takt med dette omstille sine virksomhetsprosesser slik at de blir stadig mer avhengige av en sikker funksjon av disse tjenestene. Den gradvise økningen er korrelert med NBF modenhetsgrad hvor tilsiktet effekt er å øke Forsvarets evne til å skape militær effekt i de fysiske domenene (land, sjø og luft) til et nivå som er flere ganger høyere enn dagens. INI er muliggjøreren for denne effektøkningen og det vil følgelig være et stadig høyere potensiale for å ramme Forsvarets evne til å skape militær effekt gjennom logiske angrep mot INI. Resultatet er at trusselagenters motivasjon for å angripe INI vil øke med den militære effekten Forsvaret kan skape. Motivasjonen for logiske angrep mot INI vil medføre at trusselagenter benytter stadig mer ressurser for å tilegne seg evne til å gjennomføre slike angrep. Det er lite ressurskrevende å tilegne seg logiske virkemidler, mens det vil kreve noe mer ressurser å skape en organisatorisk teknologisk kapasitet til å benytte dem innenfor rammen av militære operasjoner. Det er likevell trolig en kosteffektiv tilnærming i relasjon til det å øke sin egen kapasitet i de fysiske domenene.

Trusselen for logiske angrep mot INI vil altså øke over tid og være korrelert med Forsvarets evne til å skape militær effekt i de fysiske domenene gjennom overgang til NBF. Den økte trusselen vil materialisere seg i flere og kvalitativt bedre logiske angrep mot INI.

5.5 Sårbarhet i INI

Den siste faktoren i vår risikoanalyse er en vurdering av sårbarheter i INI. I begynnelsen av kapitlet definerte vi sårbarhet som:

> Sårbarhet er tekniske, organisatoriske, menneskelige eller rutinemessige feil og mangler som gjør at trusselaktøren kan fullbyrde sin hensikt.

Denne definisjonen anerkjenner at sårbarheter oppstår som et resultat av design, implementering (tekniske) og konfigurering/bruk (organisatoriske, menneskelige, rutinemessige) av IKT. Dette er et vanlig syn på hva sårbarheter er og hvordan de oppstår [104]:

Vulnerability a weakness in a system allowing unauthorized action

Design vulnerability a vulnerability inherent in the design or specification of hardware or software whereby even a perfect implementation will result in a vulnerability.

Implementation vulnerability a vulnerability resulting from an error made in the software or hardware implementation of a satisfactory design.

Configuration vulnerability a vulnerability resulting from an error in the configuration of a system, such as having system accounts with default passwords, having “world write ” permission for new files, or having vulnerable services enabled

Det er en rekke ulike faktorer som påvirker hvor sårbart et informasjonssystem er (grad av tilstedeværelse av sårbarheter). Nasjonal sikkerhetsmyndighet (NSM) har utgitt en rapport som identifiserer de mest sentrale bakenforliggende drivere for sårbarhetsutvikling i informasjonssystemer [84]. Rapporten inneholder et sett faktorer relatert til teknologisk utvikling som medfører både økt antall og økt utbredelse av sårbarheter i informasjonssystemer. Vi vil benytte denne som et utgangspunkt for å identifisere faktorer som fører til økt sårbarhet i informasjonssystemer. Deretter vil vi sammenligne disse faktorene med egenskaper for INI for å vurdere en sannsynlig utvikling av sårbarhetstilstanden for INI.

5.5.1 Sårbarhetsskapende faktorer for informasjonssystemer

Bruk av hyllevareprodukter

Det meste av programvare (operativsystemer og applikasjoner) som benyttes av dagens organisasjoner er det som kalles kommersielle hyllevareprodukter (engelsk: Commercial off-the-shelf; COTS). Dette er programvare som er utviklet for et størst mulig publikum og er følgelig drevet av kommersielle krefter. Programvaremarkedet preges av meget sterk konkurranse hvor fokuset er å tilegne seg og opprettholde markedsandeler gjennom å levere produkter med stadig større grad av funksjonalitet på stadig kortere tid. Det kommersielle presset fører altså til at utviklingen av programvareprodukter kreves utført raskere, billigere og kun med “god nok kvalitet”, samt at programvareprodukter øker i volum (flere linjer programkode). Fokuset er med andre ord ikke å levere sikker programvare, men rask nok leveranse av programvare med omfattende funksjonalitet.

Presset for hurtig produksjon medfører større sannsynlighet for at det gjøres feil i forbindelse med utviklingen av programkoden. Gjennomsnittlig feilfrekvens er 5 til 50 feil per tusen linjer kode [105]. En del av disse feilene vil medføre tilstander som kompromitterer informasjonssikkerhet sikkerhet (tap av konfidensialitet, integritet og/eller tilgjengelighet). Et eksempel i denne sammenhengen kan være såkalte “Buffer Overflows”. Dette er en type feil som gjør det mulig for en trusselagent å overskrive minneområdet som er avsatt for programmet og således få kjørt den koden han ønsker.

Presset for økt funksjonalitet medfører at programmene vokser i volum og kompleksitet. Siden programmene er laget for å kunne selges til et bredest mulig gruppe av kjøpere, innholder de ofte funksjonalitet som ikke er påkrevd for spesifikke brukere. I tillegg har man i den senere tid sett en tendens til at lesbare data og kjørbare instruksjoner blandes i stadig større grad sammen for å øke graden av opplevelse, fleksibilitet og effektivitet (eks: makroer i tekst- og regnearkdokumenter, skript på web-sider osv). Sammenblanding av data og kjørbar kode har medført større åpning for bruk av ondsinnet kode ved at all informasjonen på en datamaskin kan være ispedd ondsinnet kode. Resultatet er at programvaren totalt sett inneholder større antall feil (totalt antall feil i et program = gjennomsnittlig feil per kodelinje x antall linjer kode).

Dagens PC’er opererer oftest i komplekse miljøer; det er mange programmer og kombinasjoner av maskinvare som kjører samtidig med forskjellige versjoner av operativsystemer, BIOS og enhetsdrivere. Maskinene opererer i parallell og i samhandling. Programmene kan kjøres samtidig, dele data og er sårbare overfor uforutsette samhan-

dlinger seg i mellom. Totalt sett betyr dette at det er tilnærmet uendelig mange feilsituasjoner som kan oppstå i eksekveringen av et program. I praksis er det sjelden mulig å avdekke alle feil og mangler før programmene tas i bruk. Dette fordi eksekvering av kode i slike koplekse miljøer medfører enormt mange mulig tilstander som hver og en representere en mulig feilsituasjon. Dagens operativsystemer er så omfattende og komplekse at det er tilnærmet umulig å gjennomføre en formell verifikasjon av om de utfører sine funksjoner på en sikker måte. Det vil uansett være en svært tidkrevende oppgave og den vil bare ha eksplisitt gyldighet inntil operativsystemet oppdateres.

Kompleksitet

I forrige avsnitt fokuserte vi på hvordan kompleksitet internt i et program kan medføre en økning i antall feil og sårbarheter. Dagens informasjonsinfrastrukturer blir også stadig større og mer komplekse gjennom at flere og flere relaterte systemer vil kunne kommunisere med hverandre og med eksterne systemer. Tjenestetilbudet mellom nettverkene øker også. Nye tjenester benytter komplekse applikasjonsprotokoller og dynamiske datastrømmer som vanskeligere lar seg kontrollere sikkerhetsmessig. Samtidig øker automatisering og fjendrift. Kompleks funksjonalitet i informasjonsinfrastrukturer medfører;

a) Økt sannsynlighet for feil bruk, feilkonfigurasjon og uforutsette og uønskede avhengigheter og sideeffekter

b) Økt forekomst av høypriviligert kode i applikasjoner og applikasjonsprotokoller.

c) Redusert mulighet for sanntidsanalyse av overførte data (feks søke etter ondsinnet kode, uønsket eksekverbar kode eller skjulte data) på grunn av rikt innhold og komplekse dataformater.

Omfang/størrelse

En annen trend i utviklingen er at informasjonssystemer vokser i volum; de består av stadig økende antall noder som er spredt over stadig større geografiske områder. Økning i omfang medfører;

a) Redusert oversikt over systemet.

b) Økt sannsynlighet for at det finnes autoriserte brukere som ønsker å begå sikkerhetsbrudd.

c) Flere komponenter som kan feile og flere brukere som kan bli rammet av feil.

d) Mer brukerdata som kan bli kompromittert eller gå tapt i forbindelse med et sikkerhetsbrudd.

e) Økt bruk av fjerndrift og større avstand mellom driftspersonell og brukere.

f) Stor geografisk utbredelse gir flere vektorer for fysisk aksess.

Tilgjengelighet

Økt krav til effektivitet og tilgjengelighet har ført til behov for tjeneste og informasjonstilgjengelighet “alltid og overalt”. Dette er en stor sikkerhetsmessig utfordring siden økt antall av eksterne tilkoblinger gjør det vanskelig å definere et systems grenser;

a) Redusert kontroll med eksterne brukere (hvem de er og hvilke regler de er underlagt).

b) Mulighet for uforutsette og uønskede tilknytninger via eksterne systemer.

c) Mulighet for angrep fra eksterne systemer med påfølgende kompromittering av ressurser.

d) Mulighet for datalekasjer som bare er begrenset av båndbredden til ekstern linje.

e) Redusert mulighet for oppfølging av sikkerhetsrelevante hendelser utenfor nasjonal informasjonsinfrastruktur.

I tillegg ser man at behovet for mobilitet medfører en økt anvendelse av trådløse kommunikasjonsbærere (radio/sattelitt/WLAN/GSM/GPRS/EDGE/UMTS). Sikkerhetsrisikoen knyttet til dette ligger først og fremst i at overføringsmediet og dataene som overføres er lettere tilgjengelig for en trusselagent. Det medfører at trusselagenten ofte ikke må tilegne seg fysisk aksess til lokaler hvor nettverket eksisterer for å kunne angripe det. Nye angrepsvektorer som oppstår er; angrep på tilgjengelighet gjennom jamming av radiosignalene og/eller angripe konfidensialitet/integritet gjennom å avlytte radiosignalene eller koble seg til det trådløse nettverket. Et annet sårbarhetsaspekt som er knyttet til det elektromagnetiske spektrum er at alle elektroniske komponenter og metalliske kabler alltid har en viss elektromagnetisk utstråling (TEMPEST). Ved hjelp av radiomottakere og riktig demoduleringsutstyr kan denne utstrålingen utnyttes til avlytting av informasjon. Etter NSM's vurdering må en trusselagent da befinne seg mindre enn 100 meter fra den elektroniske komponenten for å kunne avlytte signaler i luft. Dersom signalet transporteres over metallisk leder (kabel) kan avstanden bli vesentlig lengre.

Et siste moment er at ved stor geografisk utbredelse av et informasjonssystem, er det sannsynlig at organisasjonen ikke selv eier hele kommunikasjonsinfrastrukturen som er påkrevd. I slike situasjoner benyttes ofte Internett som bærenett enten ved kryptert trafikk eller klartekst. Den sikkerhetsmessige utfordringen ved dette er at man ikke har noen garanti for hvem som har tilgang til kommunikasjonen (ikke egen kontroll over alle komponentene mellom pkt A og B). Altså vil mange eksterne aktører ha tilgang til dataene som overføres.

Homogenitet

Økt grad av standardisering av maskinvare, programvare og kommunikasjonsprotokoller medfører homogene miljøer i informasjonssystemer. I økende grad kan ulike typer programvare og maskinvare kommunisere med hverandre og utstyret blir mer og mer homogent. For bare få år siden var det et utstrakt antall protokoller, operativsystemer, prosessorer, osv. Nå kjører de fleste instruksjoner på Linux/Unix eller Windows (evt Cisco IOS), man kommuniserer over TCP/IP og prosessorene er i all hovedsak basert på Intel (evt AMD). Homogene miljøer betyr at en enkeltstående ondsinnet programkode element kan infisere store deler av det som finnes av datamiljøer.

Konsolidering

Et slagord i en tidlig fase av ARPANET (nettverket som siden har utviklet seg til Internett) var; "IP over Everything ". Bakgrunnen var at man hadde en målsetning om at IP-protokollen (den mest grunnleggende protokollen på Internett. Gir mulighet til forbindelsesløs transport av data mellom to noder) skulle kunne benyttes over enhver kommunikasjonsteknologi. De senere årene har dette slagordet endret seg til; "Everything over IP". Årsaken er at utviklingen går mot en konvergens mellom ulike typer nettverk med tanke på hvilke tjenester de kan tilby. Det som tidligere ble transportert over sepparate nettverkstyper samles nå mer og mer i en type nettverk og IP fremstår

som en vinner i denne konkurransen. Tidligere ble IP-nettverk bare benyttet til å frakte data. Nå ser vi en økende tendens til at de frakter annen type informasjon som tale og video. Med denne konvergeringen oppstår det nye typer farer. Et eksempel i denne sammenhengen er IP-telefoni som er en konvergens mellom tale og data; det muliggjør tradisjonell telefoni og datakommunikasjon i samme nettverk. Resultatet er at telefonsamtaler nå står ovenfor trusselen fra "to verdener"; fra telefoniverden med avlytting, missbruk og stjeling av tellerskritt, og fra dataverden med hacking, man in the midle, uautoriserte klienter, ondsinnet kode, tjenestenektangrep, spam, sårbarheter i programvare osv.

En annen utfording ved konvergens er at en nå i større grad "legger alle eggene i samme kurv". Dersom vi fortsetter å benytte IP-telefoni som eksempel, ser vi at dette medfører økt fare for samtidig tap av alle kommunikasjonstjenester. Dersom en ønsket å utføre et tjenestenektangrep mot en organisasjon, måtte en tidligere "ta ut" både telefonsystemet og datasystemet deres. Ved implementeringen av IP-telefoni, trenger en bare å angripe datasystemet for å oppnå samme effekt.

Generell trend

Det er en vanlig oppfatning at den viktigste kilden til økt sårbarhet i informasjonssystemer er bruk av kommersielle programmer [83, 106, 19, 107]. CERT har ført statistikk over den generelle utviklingen av antall sårbarheter i systemer tilknyttet Internett siden 1995 (se figur 37).

1995-1999

Year	1995	1996	1997	1998	1999
Vulnerabilities	171	345	311	262	417

2000-2006

Year	2000	2001	2002	2003	2004	2005	Q1-Q3,2006
Vulnerabilities	1,090	2,437	4,129	3,784	3,780	5,990	5,340

Total vulnerabilities reported (1995-Q3,2006): **28,056**

Figur 37: Økt grad av sofistikerthet for logiske midler for angrep vs behov for teknisk ferdighet for å implementere dem [20]

Som vi ser av tallene har antall sårbarheter økt betraktelig hvert år siden CERT iverksatte denne trendanalysen. Selv om dette er statistikk fra Internett, er det verdt å merke seg at de fleste databaserte nettverk i dag baserer seg på samme teknologi som den som anvendes på Internett. Dette gjelder også for INI.

5.5.2 Sentrale egenskaper for INI

Bruk av hyllevareprodukter

For bare få år siden ble militært materiell i all hovedsak spesialutviklet for formålet. Denne trenden har i den senere tid vært på vikende front, ikke minst innenfor IKT-systemer. Tidligere utviklet Forsvaret programvaren sin selv eller kjøpte generisk programvare og modifiserte den slik at den passet for deres spesifikke behov (som regel

gjennom kontrakter med tiltrodde bedrifter). På denne tiden var informasjonssystemene ofte sepparate systemer som ikke kommuniserte med hverandre. Ettersom IKT-verden etter hvert har dreid seg mot nettverksorganisering, har behovet for interoperabilitet mellom systemer vokst. Med denne utviklingen har det vokst frem et stadig økende behov for at alle systemene skal kunne kommunisere med hverandre og ha kompatibel funskjonalitet. Behov for sammenkobling av systemer og interoperabilitet fremtvinger programvare som kan samarbeide. Denne utviklingen, sammen med en eksplosiv økning i utnyttelse av IKT i privat og offentlig sektor, har medført en stor fremvekst av kommersielle programvareleverandører de senere år. Dette har også medført en endring av maktbalansen innenfor utvikling av programvare. Tidligere var Forsvaret en sentral aktør for innovasjon og nytenkning innen IKT-feltet. I de senere år har den kommersielle utnyttelsen av denne type teknologi medført at Forsvarets rolle er overtatt av kommersielle aktører. Forsvaret har med andre ord gått fra å være en sentral premissleverandør for utviklingen til å bli en kunde på lik linje med mange andre sterke aktører som også gir føringer for utviklingen av programvare. Det faktum at utviklingen av programvare nå er styrt av markedskreftene har medført noen sentrale fordeler [108];

Redusert kostnad Hyllevareprodukter gir ofte mye funksjonalitet til en lav kostnad. Årsaken er at siden markedet for slik programvare er stor, vil utviklingskostnadene fordeles på flere.

Redusert utviklingstid Hyllevareprodukter oppgraderes og utgis i nye versjoner med stadig kortere intervaller. Oppgraderingsfrekvenser for henholdsvis programvare og maskinvare var i 2002 ca 18 og 9 måneder.

Forsvarsdepartementet har besluttet at alle delene av INI skal baseres på hyllevare i så stor grad det er mulig [14]:

> Militær tilpasning med påfølgende anvendelse skal gis prioritet fremfor utvikling av egne løsninger. Informasjonsinfrastrukturen skal således i størst mulig grad baseres på eksisterende teknologi, tilpasset og anvendt for å dekke Forsvarets behov. Forsvarets prosesser skal om nødvendig tilpasses slik at standardprosesser og standard programvare kan benyttes der dette er mulig.

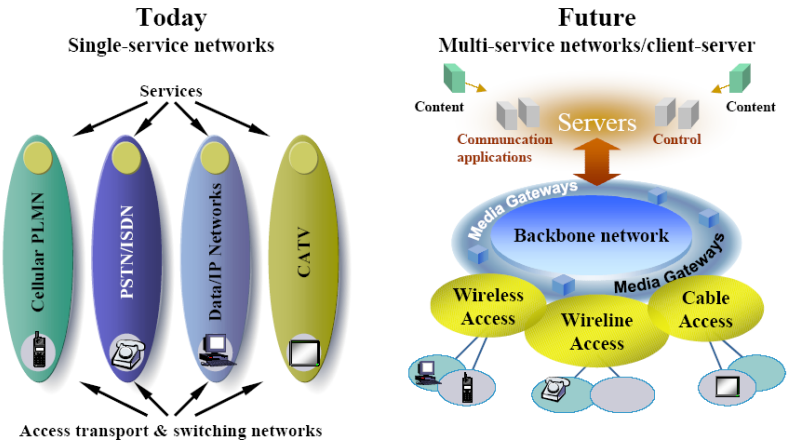
Denne regelen gjelder for alle komponenter i INI og medfører at etterhvert som INI utvikles over tid, vil den inneholde en stadig større andel av hyllevareprodukter.

Homogenitet og konsolidering

Kostnader relatert til anskaffelse og drift av INI, samt behovet for interoperabilitet (både internt i Forsvaret og mot samarbeidspartnere) har ledet til en beslutning om reduksjon i variasjon av IKT-løsninger som skal benyttes i fremtiden. Det er gitt overordnede føringer fra Forsvarsdepartementet for å sikre at variasjonen reduseres [15, 14];

> Det skal tilstrebes en utvikling der typen og antallet av IKT løsninger reduseres og samordnes bedre både innenfor og på tvers av graderingsnivåer.
>
> Det skal fokuseres på åpne industri- og alliansestandarder som har en minimum kritisk masse av brukere.
>
> Det er viktig at alle typer kommunikasjon kan brukes effektivt og sømløst, både på tvers av forsvarsgrener og uavhengig av geografisk plassering. Føringen om variantbegrensning gjelder også for kommunikasjonsinfrastrukturen. Alternative løsninger skal derfor reduseres og standardiseres.

Variasjonsbegrensningen gjelder for alle delene av INI. Utviklingen av kommunikasjonsinfrastrukturen i INI medfører at vi erstatter entjeneste eller dedikerte nettverk med en mer åpen kommunikasjonsinfrastruktur hvor det er mulig å formidle en rekke forskjellige tjenester (se figur 38).



Figur 38: Overgang til et felles nettverk basert på IP-teknologi som bærer for ulike tjenester [21]

Utviklingen av kommunikasjonsinfrastrukturen medfører en overgang til et integrerende kommunikasjonslag basert på IP-teknologi. Eksisterende løsninger, som skal videreføres, skal migreres over til en infrastruktur basert på IP-teknologi. Nye tjenester og plattformer skal støtte IP-teknologi når disse innføres.

For tjenesteinfrastrukturen medfører variasjonsreduksjonen en mest mulig enhetlig bruk av operativsystem, applikasjoner og nettverksprotokoller. Det er sannsynlig at de fleste instruksjonene vil kjøres enten på Windows- eller Unix-maskiner, kommunikasjonen vil gå over TCP/IP og prosessorene i stor grad vil være basert på Intels x86 instruksjonssett. Denne utviklingen medfører at INI over tid vil utvikle seg i en retning av stadig større grad av homogenitet, samt at alle informasjonstjenester vil gå over et og samme nettverk.

Omfang

Implementering av NBF i Forsvaret vil gjennomføres over en lang tidsperiode. Vi har tidligere i oppgaven estimert at det vil ta ca 25 år før Forsvaret er på det øverste modenhetsnivået for NBF. Den samme utviklingstiden må antas å gjelde for INI. I denne perioden vil vi se at en stadig økende andel av Forsvarets enheter tilkobles INI. De eksisterende enhetene i Forsvaret må tilpasses slik at de får et kommunikasjonsmessig grensesnitt som gjør det mulig for dem å utveksle data med andre enheter i INI. Nye systemer må utvikles med et grensesnitt som understøtter det samme. Ettersom stadig flere enheter blir kompatible med INI, vil vi se en jevn økning av INI's volum (enheter og brukere i nettverket) frem til det endelige modenhetsnivået hvor mer eller mindre alle enhetene i Forsvaret er koblet sammen i en felles INI. Denne utviklingen medfører at INI over tid vil utvikle seg i volum med stadig flere noder og brukere.

Tilgjengelighet og geografisk utbredelse

INI skal i fremtiden gi tilkoblingsmuligheter for enheter i alle geografiske områder hvor Forsvaret utfører militære operasjoner. I tråd med gjeldende sikkerhetspolitiske retningslinjene medfører dette at INI vil få en global utbredelse med fysisk tilstedeværelse i stadig flere områder. Nettverk, noder og brukere skal kunne aksessere INI hvor som helst i verden. USA planlegger å bygge et eget globalt nettverk som skal understøtte en slik kapasitet for sine militære styrker [109]. Dette vil ikke være økonomisk mulig for Norge. Global aksess til INI må derfor realiseres gjennom å anskaffe aksess av kommersielle aktører, eller gjennom avtaler med de nasjonene vi samarbeider med. Dette kan løses gjennom satellitt, tuneller gjennom andre nasjoners militære nettverk eller over Internett og leide linjer. FFI anbefaler at Forsvaret bør vurdere å benytte kommersielle tjenestetilbydere også i realisering av deler av det strategiske stasjonære stamnettet i Norge [16].

Det vil i fremtiden også eksistere et behov for sammenkobling av INI med eksterne nettverk. De mest aktuelle aktørene i denne sammenhengen vil være sivile myndigheter og samarbeidspartnere, militære koalisjonsstyrker og tilbydere av kommersielle tjenester [16]. Det er også mulig at nettverket må kunne tilby tilknytning til Internett [13].

For å oppnå den mobiliteten Forsvaret trenger for å implementere NBF, er man også avhengig av at deler av INI baseres på trådløse kommunikasjonssystemer. Den mest utbredte bruken av trådløs kommunikasjon vil vi finne i det mobile taktiske nettverkene som etableres i ulike operasjonsområder. Disse nettverkene vil etableres både ved hjelp av bakkebaserte og luftbårne radio-relé nettverk [16].

Samlet sett betyr denne utviklingen av INI i fremtiden vil medføre en stadig utvidelse i geografisk omfang, et økende bruk av eksternt eide og kontrollerte kommunikasjonsmidler, økt antall eksterne tilkoblingspunkter og et økt innslag av trådløs kommunikasjonsteknologi.

Kompleksitet

Operativsystemer og applikasjoner har de senere år utviklet seg i retning av økende funksjonalitet. Denne trenden er drevet av markedskrefter og utviklingen innen maskinvare [108]. Dagens marked forventer at nye versjoner av operativsystemer og applikasjoner skal inneholde mer funksjonalitet enn sine forgjengere. Programvareleverandørene prøver å tilfredsstille en størst mulig del av det totale markedet. Resultatet er programvare som totalt sett inneholder svært mye funksjonalitet. Denne utviklingen er korrelert med utviklingen innen maskinvare; utviklingen innen CPU-hastighet, RAM- og harddiskstørrelse gjør det i dag mulig å kjøre svært store programvareløsninger. Det kan nevnes som et eksempel at Windows 95 inneholdt mindre enn 5 millioner linjer kode, mens Windows XP som ble utgitt i 2002 inneholdt ca 40 milioner linjer kode [105]. I slike store systemer er det mange komponenter som skal fungere sammen. Dette skaper komplekse miljøer for programkoden. INI vil inneholde flere slike enkeltstående systemer bestående av komplekse operativsystemer og applikasjoner.

Mange av disse systemene som hver for seg er komplekse skal samhandle i INI. De funksjonsvise beslutningsstøttetjenestene skal for eksempel benytte seg av tjenester levert av felles kjernetjenester. Som et konkret eksempel kan vi nevne at K2 og ledelsestjenester samt manøveroperasjonstjenester må kunne samhandler med geografiske karttjenester. Den sist nevnte tjenesten vil levere kartdata til de to første. Når flere komplekse

systemer skal kunne samhandle med hverandre oppstår det et enda høyere nivå av kompleksitet for INI som helhet.

I tillegg skal INI kunne sørge for dynamisk allokering av kapasitet og autorisasjon mellom de ulike brukerne og enhetene i nettverket etter operativt behov. Det skal være mulig å hurtig kunne omstille bruken av INI slik at den understøtter den organisasjonen som skal løse en gitt militær operasjon. Konkret kan dette bety at rettighetene til å motta data fra et sett av sensorer og styring av et sett av effektorer tildeles et sett av beslutningstakere for en gitt tidsperiode. Ved periodens utløp skal det være mulig å omkonfigurere disse rettighetene for å tilpasse dem til behovet for utførelsen av et nytt oppdrag som kanskje krever en annen konfigurasjon.

Man ønsker at alle aktører i Forsvaret skal kunne være tilknyttet INI og at INI skal kunne ha informasjon på flere graderingsnivåer (fra ugradert til hemmelig). Dessuten skal aktører autorisert for forskjellige sikkerhetsgraderinger kunne bruke INI. Dette krever at aktørenes informasjonstilgang vil måtte kontrolleres basert på informasjonens gradering, brukernes sikkerhetsklarering og autorisasjon. [13]

Alle tjenester, graderingsnivåer og evne til dynamisk styring vil ikke innføres på samme tidspunkt i INI. Vi vil trolig se en gradvis innføring av tjenester ettersom et økende antall enheter tilknyttes INI. Dette medfører at INI's grad av kompleksitet vil øke over tid fra systemets start og frem til en når det høyeste modenhetsnivået for NBF. Det endelige systemet vil inneholde et stort antall teknisk komplekse og samvirkende funksjoner.

Dynamisk

INI vil være et informasjonssystem i en tilstand av konstant endring. Endringene skjer både som et resultat av kontinuerlig videreutvikling av INI og som en kontinuerlig prosess for å konfigurere nettverket slik at det understøtter endringer i operative behov.

Videreutviklingen av INI skal utføres for å møte nye behov og utnytte nye teknologiske muligheter [14];

> Nye løsninger skal utvikles med mulighet for kontinuerlig tilpasning og oppgradering, ikke bare for total utskifting. Fleksibilitet skal være et bærende prinsipp, blant annet gjennom en løpende evaluering av nye løsninger. Informasjonsinfrastrukturen utvikles over en lengre tidsperiode, i form av utvidelser, forlengelser og forbedringer av den eksisterende infrastrukturen. Det betyr at videreutvikling av en stor infrastruktur er en kontinuerlig prosess.
>
> Funksjonsvise beslutningsstøttetjenester; Ad hoc tilpassede tjenester - Denne typen tjenester er tatt med for å indikere at vi må ha fleksibilitet til å kunne lage spesialtilpassede samlinger av tjenester tilpasset et oppdukkende operativt behov.

NBF skal gi rom for virtuell organisering og selvsynkronisering av enhetene i Forsvaret. Dette innebærer at en skal kunne utpeke et sett med enheter og tildele et oppdrag og en tidsramme for utførelse til disse. INI må i disse situasjonene gi mulighet for hurtig konfigurasjon som gir dette settet av enheter de informasjonsressurser og autorisajon til bruk av ressurser de behøver for å gjennomføre oppdraget. Det er derfor et krav at INI skal kunne understøtte [16]:

> Dynamisk autorisasjon: autorisasjon til å bruke ulike ressurser vil endres dynamisk. Tidsvindu vil kunne ligge innenfor sekunder.
>
> Policy-driven auto-configuration: INI fungerer i et svært dynamisk miljø hvor tilgjengeligheten til nettverkdriftspersonell vil variere sterkt. Konfigurering av rutere, server og systemer bør derfor gjøres mest mulig automatisk.

Fleksibilitet: nettverket må kunne tilpasses ulike operative konsepter, protokoller og metoder. Samarbeid med ulike internasjonale partnere vil være et vanlig scenario.

Ad hoc nettverk: midlertidige trådløse nettverk som kan organisere og konfigurerer seg selv automatisk er påkrevd.

Endringer i operasjonsporteføljen Forsvaret til enhver tid skal utføre vil medføre endringer i INI av noe lengre varighet. Siden de to nederste lagene av INI (deployerbare og mobile taktiske nett) skal lokaliseres geografisk til Forsvarets operasjonsområder, vil nettverket måtte endres i tråd med disse føringene. Det betyr at INI i en tidsperiode vil lokaliseres til et geografisk område så lenge Forsvaret utfører militære operasjoner der. Ved endringer i det globale sikkerhetspolitiske bildet som medfører at Forsvaret skal utføre operasjoner i et annet geografisk område, må INI omkonfigureres slik at det kan understøtte enhetene i den nye lokasjonen.

Dette dynamiske miljøet innebærer at INI vil være et svært levende nett med kontinuerlige endringer av kort eller lengre varighet. Det er sannsynlig at behovet for stor endringshastighet vil øke over tid ettersom Forsvaret som organisasjon tilpasser seg nettverkssentriske operasjonskonsepter. Dette vil skje som en naturlig følge av at Forsvaret over tid oppnår høyere NBF modenhetsgrad. Den økte graden av endring bidrar til å øke INIs totale kompleksitet.

5.5.3 Dynamisk utvikling av sårbarhet i INI

INI vil bli et svært komplekst og omfattende informasjonssystem som det vil ta mange år å utvikle. Omorganiseringen av Forsvaret til en nettverksorganisert styrke vil være en gradvis prosess hvor de egenskapene vi har beskrevet for INI vil utvikle seg over tid. NBF modenhetsgradene beskriver hvordan Forsvaret vil se ut ved de ulike tilstandene. Innlemmet i disse er også beskrivelser av forventet tilstand for INI [12]

Innledende NBF (Modenhetsgrad 1) Eksisterende informasjon er blitt tilgjengelig for flere enn i dag. Et felles nettverk for utvalgte plattformer og komponenter er opprettet, der man har tilgang på et felles situasjonsgrunnlag. Interoperabilitet er fokusert på samarbeidende avdelinger i militære operasjoner. Organisasjonens IKT-bruk er motivert mer ut fra et rasjonaliseringssynspunkt enn fra et "muliggjørende" synspunkt.

Integrerende NBF (Modenhetsgrad 2) Alt eksisterende materiell og nyanskaffelser er "Net-ready ", 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 nødvendigvis kan forstås og nyttiggjøres av alle brukere. Interoperabilitet er gjennomgående internt og også til dels mot eksterne aktører. Fremdeles fokus på militær interoperabilitet. Innovativ bruk av IKT blir stadig viktigere i forhold til IKT som rasjonaliseringsverktøy.

Gjennomgripende NBF (Modenhetsgrad 3) En gjennomgripende informasjonsstyring sørger for at all informasjon i nettverket er tilgjengelig, forståelig og utnyttbar for enhver med behov. Interoperabilitet (teknologisk, prosessmessig og organisatorisk) er gjennomgripende internt og mot prioriterte eksterne aktører, og sees på som

svært viktig også utover det militære domenet. En høy grad av teknologisk modenhet muliggjør en effektiv utnyttelse av nettverket. IKT blir sett på som "muliggjørende" for å bidra til å forbedre eksisterende prosesser eller etablere nye (innovasjon, i motsetning til automatisering).

Disse beskrivelsene viser at INI vil utvikle seg over tid og at utviklingen er korrelert med NBF modenhetsgrad. Det betyr at en høyere NBF modenhetsgrad vil medføre et høyere utviklingsnivå for INI med følgende endringer innen de identifiserte egenskapene;

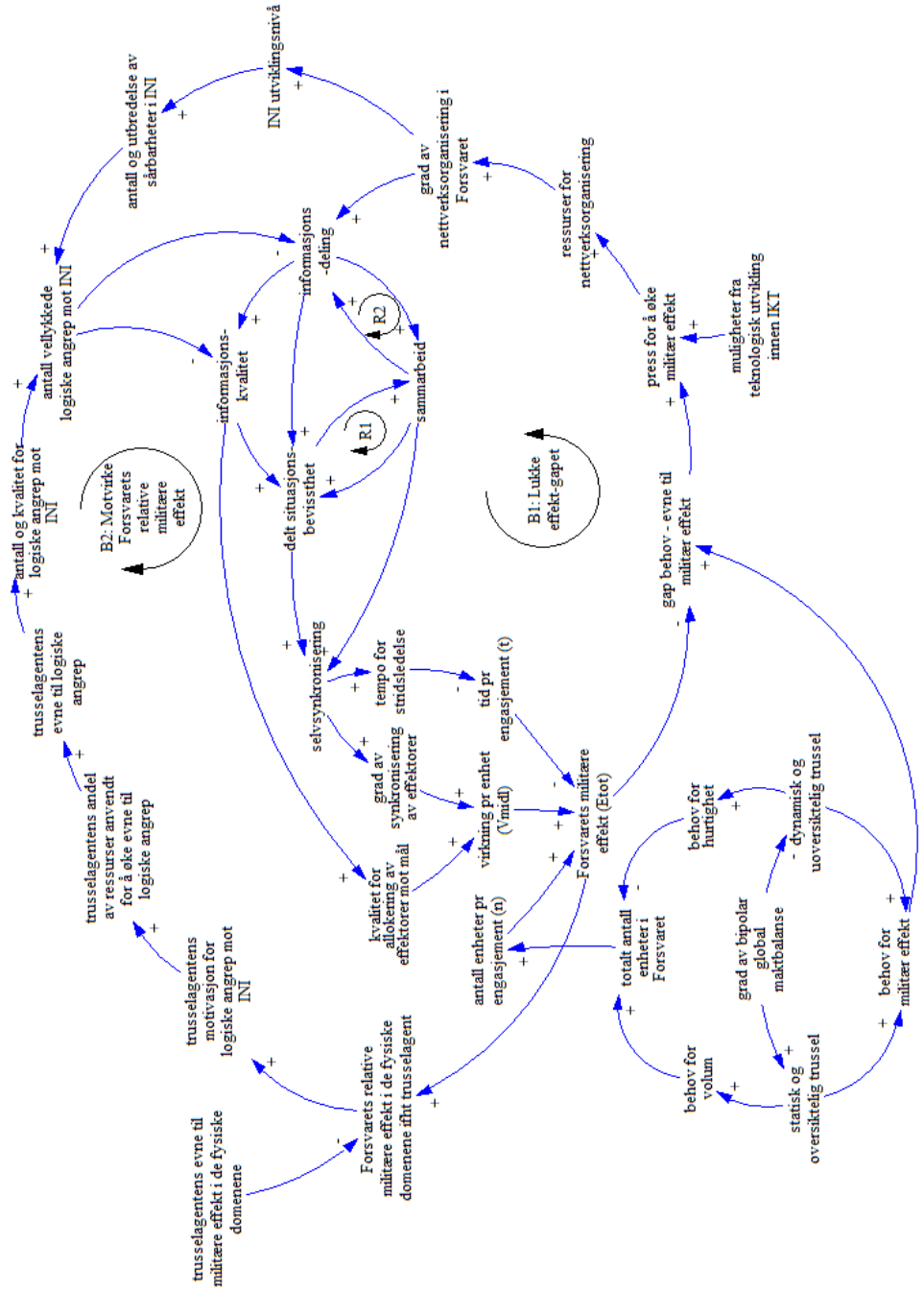
- Økt bruk av hyllevareprodukter
- Økt grad av teknologisk homogenitet og konsolidering av ulike informasjonssystemer til et felles system basert på IP-teknologi.
- Økt omfang (flere noder og brukere)
- Økt grad av geografisk utbredelse og tilgjengelighet
- Økt grad av kompleksitet
- Økt grad av dynamikk (endring)

Disse egenskapene er sammenfallende med de sårbarhetsskapende faktorene vi identifiserte i forrige kapittel. Det vil si, egenskapen dynamisk er ikke eksplisitt uttalt som en sårbarhetsskapende faktor. Den kan imidlertid ansees som en underkategori av kompleksitet. Siden utviklingen av INI over tid medfører en økning innen alle de identifiserte egenskapene, og disse er sårbarhetsskapende faktorer i et informasjonssystem, konkluderer vi med at antall og utbredelse av sårbarheter i INI vil øke over tid og være korrelert med INI utviklingsnivå.

5.6 Utvidelse 2 av CLD-modell: Utilsiktet effekt av NBF implementering

Utilsiktet effekt er en form for sideeffekt som oppstår som følge av endringene forårsaket av tilsiktet effekt. For å modellere hvordan utilsiktet effekt relatert til informasjonssikkerhet oppstår som en følge av implementeringen av NBF, må vi ta utgangspunkt i hvordan endringer påvirker de tre faktorene som utgjør risiko for INI; verdi, trussel og sårbarhet. Modellen i figur 39 viser både tilsiktet og utilsiktet effekt ved implementasjon av NBF. Resten av dette kapitlet beskriver de sentrale variablene og kausale sammenhengene relatert til utilsiktet effekt.

NBF er et konsept om hvordan en kan utøve militære operasjoner på en slik måte at en oppnår økt evne til å skape militær effekt med et gitt antall enheter. Den økte effekten oppstår som et resultat av forbedret evne til informasjonsdeling og informasjonskvalitet. INI er den entiteten som gjør det mulig å forbedre disse informasjonsegenskapene. INI's verdi drives derfor av og er sammenfallende med variablene relatert til tilsiktet effekt av NBF. Dette fremgår av modellen i figur 39. INI vil derfor øke i verdi i et kausalt forhold med variabelen *"grad av nettverksorganisering av Forsvaret"*. Verdien er uttrykt ved at variabelen *"Forsvarets militære effekt"* øker som en følge av de kausale lenkene mellom disse to variablene. Resultatet er at jo høyere verdi *"grad av nettverksorganisering av Forsvaret"* har (som måles i NBF modenhetsgrad), jo større negativ innvirkning vil vellykkede logiske angrep mot INI ha på Forsvarets evne til å skape militær effekt. Sagt på en enklere måte; i fremtiden vil INI muliggjøre stadig større evne til å skape militær



Figur 39: Utilsiktet effekt ved implementering av NBF

effekt. INI får derfor stadig større verdi for Forsvaret og logiske angrep som hindrer dens funksjon vil gi stadig større negativt utslag.

Endringen for trussel er, som vi utledet i kapittel 5.4.4, positivt kausalt knyttet til variabelen *"Forsvarets militære effekt (*E_{tot}*)"*. Den militære effekten som oppstår er knyttet til de fysiske domenene (land, sjø og luft). Dersom Forsvaret øker sin evne på dette området, vil det medføre at Forsvaret vil øke sin relative effekt relatert til en trusselagent. Dette fremgår av den positive kausaliteten mellom *"Forsvarets militære effekt"* og *"Forsvarets relative militære effekt i de fysiske domenene ifht trusselagent"* (en måleenhet for denne variabelen kan være kill-ratio; hvor mange av trusselagentens enheter ifht hvor mange av våre enheter han bekjemper). Dette forutsetter en statisk evne for trusselagenten i disse domenene, som er uttrykt ved variabelen *"trusselagentens evne til militær effekt i de fysiske domenene"*. Trusselagentens reduserte relative effekt i de fysiske domenene, sammen med kunnskap om INI's verdi og derav et stadig høyere potensiale for å ramme Forsvarets evne til å skape militær effekt gjennom logiske angrep mot denne, vil være en sterk motivator for å skifte sitt angrepsfokus til informasjonsdomenet (her representert ved INI). Motivasjonen for logiske angrep mot INI vil medføre at trusselagenter benytter stadig mer ressurser for å tilegne seg evne til å gjennomføre slike angrep. Den økte ressursbruken vil igjen medføre økt evne, både med tanke på tilegnelse av logiske virkemidler og utvikling av organisatorisk kapasitet, til logiske angrep. Resultatet vil være en økning i antall og kvalitet av logiske angrep mot INI. Denne kjeden av positive kausale forhold er uttrykt i modellen ved variablene; *"trusselagentens andel av ressurser anvendt for å øke evne til logiske angrep"*, *"trusselagentens evne til logiske angrep"* og *"antall og kvalitet for logiske angrep mot INI"*. Modellen kunne inneholdt en negativ kausal lenke mellom *"trusselagentens andel av ressurser anvendt for å øke evne til logiske angrep"* og *"trusselagentens evne til militær effekt i de fysiske domenene"* siden man må regne med at han ikke har en ubegrenset mengde ressurser han kan sette inn i konflikten. Dette tilsier at dersom han har brukt mer ressurser på striden i informasjonsdomenet, vil hans ressurser (og følgelig evne) i de fysiske domenene reduseres. På grunn av at evne til logiske angrep er svært lite ressurskrevende å utvikle, har vil valgt å ikke ta med denne kausaliteten.

INI vil bli et svært komplekst og omfattende informasjonssystem som det vil ta mange år å utvikle. Som vi viste i kapittel 5.5.3 vil INI utvikle seg i en positiv kausal relasjon til variabelen *"grad av nettverksorganisering i Forsvaret "* på en slik måte at en økning i NBF modenhetsgrad vil medføre et økt *"INI utviklingsnivå "*. Når INI utviklingsnivå øker, vil det medføre en økning innen sentrale egenskaper for INI som vi har vist er drivere for økt antall og utbredelse av sårbarheter. Derav den positive kasuale linken til *"antall og utbredelse av sårbarheter i INI "*

Den situasjonen som da oppstår er at egenskapene som beskriver reell trussel fra en ondsinnet trusselagent blir "fullbyrdet". Når den økte graden av trusselagentens motivasjon og evne til logiske angrep kombineres med muligheten, representert ved økt sårbarhet og mulighet for aksess (økt geografisk utbredelse av INI), vil den økte risikoen materialisere seg ved at variabelen *"antall vellykkede logiske angrep mot INI "* øker. Logiske angrep er rettet mot tilgjengelighet, integritet og/eller konfidensialitet. Dette medfører at de logiske angrepene vil ha en negativ kausal relasjon med de to mest sentrale driverne for økt militær effekt i NBF; *"informasjonsdeling "* og *"informasjonskvalitet"*.

Det sist omtalte kausale forholdet gjør at en ny balanserende løkke trer frem i mod-

ellen vår: B2 - Motvirke Forsvarets relative militære effekt. Løkken er balanserende fordi kreftene i den virker for å "utligne" den effekten Forsvarets økte evne til å skape militær effekt har på det relative maktforholdet i de fysiske domenene mellom Forsvaret og en trusselagent. Når Forsvaret bruker ressurser for å oppnå et nytt nivå i NBF modenhetsgrad (variabelen *"grad av nettverksorganisering i Forsvaret"*), tilsier de kasuale relasjonene i modellen at *"Forsvarets militære effekt (*E_{tot}*)"* vil øke. En økning av denne variabelen vil igjen medføre en økning av *"Forsvarets relative militære effekt i de fysiske domenene ifht trusselagent"*. Dette er starten på kreftene som virker i løkke B2, siden det gjennom kausale forhold vi tidligere har omtalt medfører en økning av variabelen *"antall vellykkede logiske angrep mot INI "* med påfølgende reduksjon av variablene *"informasjonsdeling "* og *"informasjonskvalitet"*. En reduksjon av disse medfører, via reduksjon i en rekke variabler en reduksjon av *"Forvarets militære effekt (*E_{tot}*)"*. Dersom denne reduksjonen er stor nok, vil den utligne forskyvningen i maktbalansen mellom Forsvaret og trusselagenten representert ved variabelen *"Forsvarets relative militære effekt i de fysiske domenene ifht trusselagent"*.

5.7 Delkonklusjon - utilsiktet effekt av NBF

Det andre forskningsspørsmålet vårt var; Kan implementeringen av NBF medføre utilsiktet effekt relatert til informasjonssytemsikkerhet og hvordan påvirker eventuelt denne realiseringen av den tilsiktede effekten?

Svaret på dette spørsmålet fremgår av modellen med tilhørende beskrivelse som vi presenterte i forrige kapittel. Modellen viser at implementering av NBF medfører endringer i variablene *"grad av nettverksorganisering i Forsvaret"* (målt i NBF modenhetsgrad) og *"Forsvarets militære effekt (*E_{tot}*)"* som igjen gir en økning av vellykkede logiske angrep mot INI, representert ved variabelen *"antall vellykkede logiske angrep mot INI"*. Økningen av denne variabelen virker negativt tilbake på to variabler som er avgjørende for realiseringen av effekten i NBF; *"informasjonsdeling "* og *"informasjonskvalitet"*. Gjennom en serie kausale sammenhenger medfører dette at den tilsiktede økningen av variabelen *"Forsvarets militære effekt (*E_{tot}*)"* reduseres eller oppheves. Om effekten forsvinner eller bare reduseres, er avhengig av styrkeforholdet mellom B1 og B2 (se figur 39). Dette er ikke mulig å fastslå ut fra vår kvalitative modell. Vi vil imidlertid bemerke at et intelligent utformet og strukturert utført logisk angrep mot INI har et stort potensiale for å skape vedvarende effekt som alvorlig kan degradere systemets, og derigjennom Forsvarets evne til effektiv utførelse av militære operasjoner [110];

> Even a single penetration can be extremely damaging, particularly in a richly connected information system. Obviously, some data (such as concepts of operations, planning documents, and orders) are extremely sensitive. A well-crafted "worm"or computer virus can spread literally with the speed of light once inside a complex system. Moreover, knowing that databases have been penetrated and may be corrupted can be expected to greatly inhibit decisive and effective decision making.

Tilsiktet effekt ved implementering av NBF er identifisert ved den balanserende løkken B1. Målet for denne løkken er å lukke gapet mellom behov og evne til å skape militær effekt effekt gjennom å øke evnen. Siden utilsiktet effekt, representert ved den balanserende løkken B2 motvirker eller opphever evne til å øke mil effekt, konkluderer vi med at utilsiktet effekt eksisterer og virker reduserende eller opphevende på tilsiktet effekt. Siden løkke B1 viser at Forsvarets svar på et økt gap er å ytterligere øke sin grad

av nettverksorganisering, vil virkningen mellom de to balaserende løkkene gjenta seg etter mønsteret vi nettopp har beskrevet; økt NBF modenhetsgrad medfører ytterligere økt militær effekt som igjen medfører ytterligere økning av logiske angrep som igjen motvirker økning i militær effekt og følgelig motvirker lukking av gapet mellom behov for effekt og evne til effekt. Med andre ord; utilsiktet effekt relatert til informasjonssikkerhet nuller ut eller reduserer tilsiktet effekt for NBF.

Ingen av NCP CF undersøkelsene vi kjenner til (se tabell 5) har tatt høyde for logiske angrep mot informasjonssystemene (forsøkene forutsetter med andre ord “en sikker ” informasjonsinfrastruktur). Ergo er resultatene oppnådd i fravær av logiske angrep. Dette gir trolig en unaturlig høy evne til å skape militær effekt for den parten som har det beste, og er mest avhengig av sitt informasjonssystem. Det bør derfor gjennomføres undersøkelser for å samle inn empiriske data hvor man angriper informasjonssystemene med logiske virkemidler. Dette vil kunne gi en indikasjon på virkningsforholdet mellom B1 og B2.

6 Tiltak for minimalisering av utilsiktet effekt

I kapittel 5.7 så vi at det eksisterer utilsiktet effekt som påvirker tilsiktet effekt ved implementering av NBF. Dette forholdet kan forårsake det som kalles en policy resistance; tendensen til at intervensjoner blir forsinket, utvannet eller forpurret av systemets respons på den opprinnelige intervensjonen. For å unngå en slik situasjon, må vi vurdere alternative tiltak som kan redusere virkningen av den utilsiktede effekten. Dersom vårt forslag til løsning skal ha mulighet for å gi en "varig" virkning, må vi anvende vår innsikt i de dynamiske kreftene som virker i systemet vi har utledet i modellen i figur 39. Vi må identifisere de mest fremtredende egenskapene til systemet som kan lede til policy resistance og velge en løsning som motvirker disse best mulig.

Dersom vi rekapitulerer Coyle's prosess for et systemdynamisk prosjekt (se figur 1), husker vi at denne innebar utvikling av flere modeller med ulik grad av oppløsning. Vi har gjennomført arbeidet på nivå 2 og 3 (utviklet en relativt omfattende CLD-modell av problemstillingen) og skal nå anvende vår innsikt til å utlede hvilke underliggende krefter som kan forårsake policy resistance. Vi skal altså bevege oss opp til nivå 1 i modellhierarkiet for å identifisere de viktigste egenskaper og innsikt vi har utviklet om systemet. Målet er å benytte denne på en slik måte at vi kan foreslå en policy som kan motvirke policy resistance ved implementering av NBF.

I denne fasen kan vi få stor hjelp av Wolstenholme's problemarketyper (se kapittel 3.1). De kan benyttes som hjelpemiddel både for å identifisere og forklare de grunnleggende årsakene til policy resistance i CLD-modellen vi har utviklet. Deretter kan vi benytte den tilhørende løsningsarketypen som et utgangspunkt for å identifisere tiltak som kan motvirke utilsiktet effekt. Fremgangsmåten i resten av dette kapittelet vil derfor være som følger:

1. Vi vil identifisere systemets grunnleggende dynamiske problem gjennom å beskrive en problemarketype og benyttet denne til en prediksjon av systemets utvikling (dynamisk hypotese).
2. Vurdere tilhørende løsningsarketype med utgangspunkt i konteksten den skal virke i og utlede en generisk policy for hvordan en kan motvirke utilsiktet effekt.
3. Konkretisere den generiske policyen gjennom en vurdering av konteksten den skal virke i. Målet er å oppnå noe høyere grad av presisjon for tiltak som skal motvirke utilsiktet effekt.

Dette kapitlet er i mye mindre grad basert på dokumentundersøkelser enn de to foregående. Vi gir likevell en oversikt over sentral litteratur for noen av vurderingene som er gjort i figur 10. I tabellen er; P=Problemarketype og L=Løsningsarketype med konkretisering.

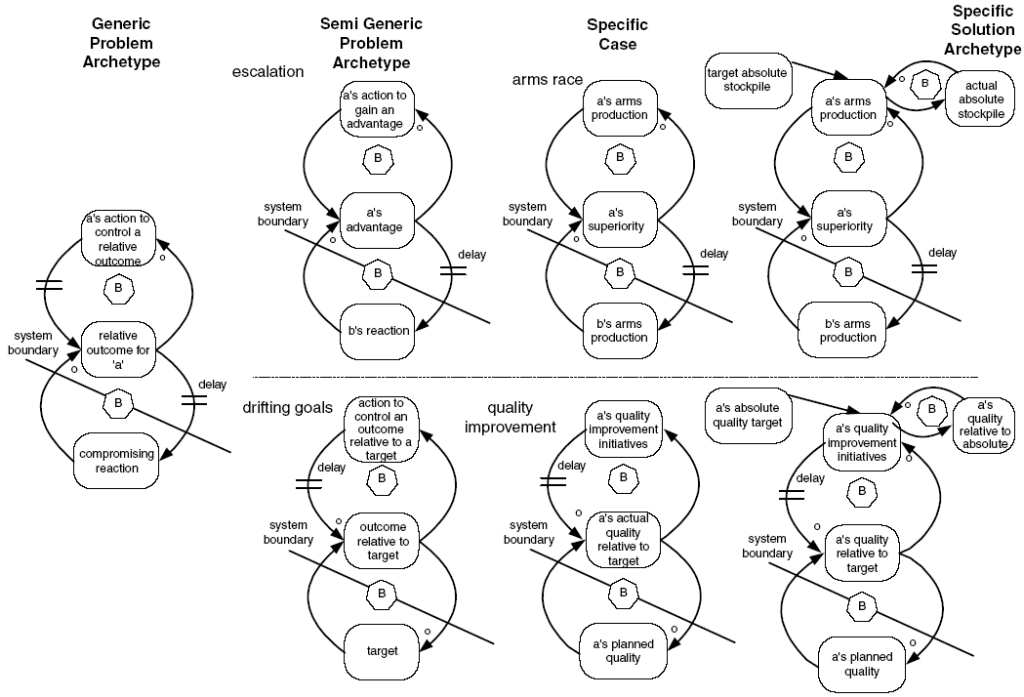
6.1 Problemarketype

CLD-modellen vi har utviklet (se figur 39) består av to balanserende løkker (B1 og B2) som har flere sammenfallende variabler de virker over. De beskriver en dynamisk situ-

Årstall	Tittel	Hvor benyttet	
		P	L
2000	Secrets & Lies - Digital Security in a Networked World [111]		X
2000	Cyber Defence Protection Methods [112]		X
2001	Defense-In-Depth Revisited: Qualitative Risk Analysis Methodology for Complex Network-Centric Operations [17]		X
2003	Towards the definition and use of a core set of archetypal structures in system dynamics [4]	X	X

Tabell 10: Oversikt over sentral litteratur for minimalisering av utilsiktet effekt.

asjon hvor både Forsvaret og en vilkårlig trusselagent søker å oppnå en balanse som er fordelaktig relativt til motparten. Dette tilsier at de omhandler en problemstilling som er sammenfallende med problemarketypen “relative control”(se figur 40).



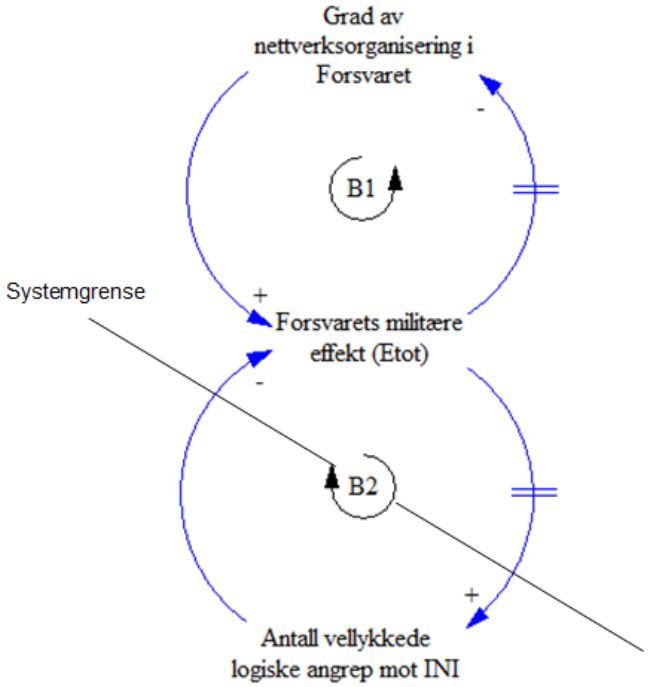
Figur 40: Den generiske problemarketypen Relative control med de tilhørende semi-generiske arketypene Escalation og Drifting goals [4]

De tradisjonelle arketypene “escalation” og “drifting goals” faller inn under denne generiske arketypen og kan ansees som semi-generiske tilfeller av denne. I vårt tilfelle er det den spesifikke instansen “arms race” av arketypen “escalation” som fremstår som mest lik vår dynamiske situasjon [4]:

> In the escalation case the ic loop is a balancing loop where action is taken by one sector of an organisation to control an outcome relative to another organisation, for example arms production by one country to achieve weapon superiority. However, the reaction of another country is to mirror this action by increasing the target for

their own arms stockpile. Each attempts to gain relative control, but the net result is escalation in the total stockpile.

Med bakgrunn i denne har vi utviklet en problemarketype som beskriver den grunnleggende dynamiske problemstillingen i vår CLD-modell (se figur 41).



Figur 41: Problemarketype

De to balanserende løkkene i arketypen er en forenkling av løkkene i CLD-modellen fra figur 39 hvor løkken B1 representerer tilsiktet effekt og løkken B2 representerer utilsiktet effekt som en reaksjon på endringen B1 medfører. B1's mål er å redusere variabelen *"gap behov - evne til militær effekt"*, mens B2's mål er å redusere variabelen *"Forsvarets relative militære effekt i de fysiske domenene ifht trusselagent"*. Begge løkkene er avhengige av å påvirke variabelen *"Forsvarets militære effekt (Etot)"* for å oppfylle sine mål. Forsvarets policy for å oppnå balanse mellom evne og behov for militær effekt er økt grad av nettverksorganisering, mens trusselagenten søker å oppnå balanse gjennom å utvikle økt evne til logiske angrep. Den opprinnelige CLD-modellen inneholder ingen vurderinger av eventuelle tidsforsinkelser i systemet. Hverken Forsvaret eller trusselagenten vil imidlertid oppdage forskyvelsen i variabelen *"Forsvarets militære effekt (Etot)"* umiddelbart etter at motparten har iverksatt tiltak for å påvirke den. Det vil derfor være en tidsforsinkelse mellom faktisk reduksjon av denne variabelen og Forsvarets registrering av at *"gap behov - evne til militær effekt"* øker . På samme måte vil det være en tidsforsinkelse mellom faktisk økning av variabelen og trusselagentens registrering av at *"Forsvarets relative militære effekt i de fysiske domenene ifht trusselagent "* øker. Størrelsen på tidsforsinkelsene bestemmes av den totale tiden en trenger for å gjennomføre alle faktorene som inngår i en klassisk handlingssløyfe [74] (forklart i kapittel 4.5.5);obser-

vasjon, vurdering, beslutning og handling. Disse tidsforsinkelsene endrer ikke modellens dynamiske oppførsel i vesentlig grad, men vil trolig bidra til større svingninger i variabelen *"Forsvarets militære effekt (Etot)"* over tid.

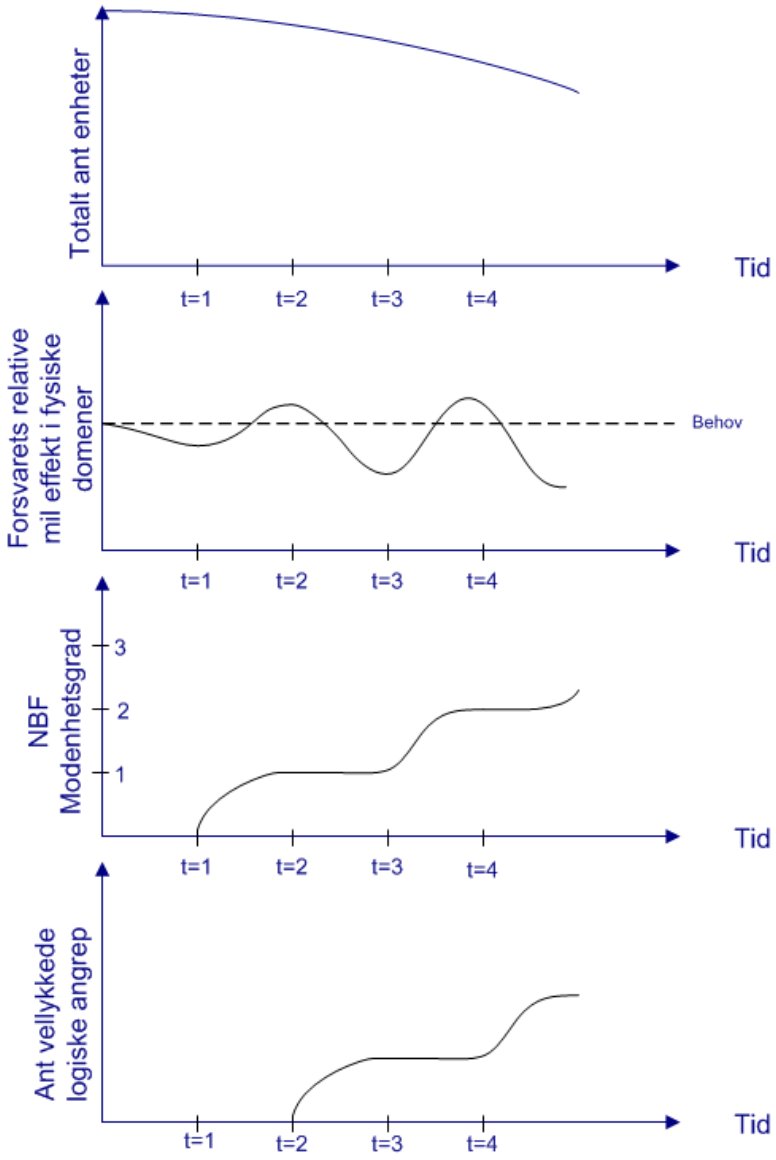
Figur 42 består av fire Behaviour Over Time (BOT) grafer som viser vår dynamiske hypotese for hvordan variablene i problemarketypen vil utvikle seg over tid. BOT'en som er merket med teksten Forsvarets militære effekt (Etot) viser også en linje som markerer behov for militær effekt. Grafen i denne BOT'en indikerer evnen til å skape militær effekt. Når denne ikke er sammenfallende med behov-linjen, betyr det at man har et gap mellom Forsvarets behov og evne til å skape militær effekt. I tillegg har vi tatt med variabelen *"totalt antall enheter i Forsvaret"* siden den er viktig for den helhetlige forståelsen av arketypens utvikling. Alle BOT'ene har tid som måleenhet for x-aksen. På denne representerer t=x et tidspunkt i utviklingen. Under følger en beskrivelse av utviklingen i systemet for økende verdier av x;

t=1: *"totalt antall enheter i Forsvaret"* reduseres som en følge av at *"grad av bipolar global maktbalanse"* reduseres. Dette medfører at *"Forsvarets militære effekt (Etot)"* med påfølgende økning av gap mellom behov og evne til militær effekt. Jo mer variabelen *"totalt antall enheter i Forsvaret"* synker, jo mer vil Forsvarets evne til å skape militær effekt være avhengig av INI.

t=2: Etter en tidsforsinkelse (tiden Forsvaret trenger for å registrere økning av *"gap behov - evne til militær effekt"*) vil økningen av gapet registreres av Forsvaret og de svarer med økt bruk av ressurser for nettverksorganisering. Tiltakene medfører at *"Forsvarets militære effekt (Etot)"* vil endre retning og øke (korrelert med at man oppnår en ny NBF modenhetsgrad). På grunn av det store effektforbedringspotensialet som ligger i NBF konseptet (ref NCO CF undersøkelser 5) er det sannsynlig at *"Forsvarets militære effekt (Etot)"* vil returnere til behovet og muligens overkompensere noe, slik at variabelen faktisk øker over fastsatt behov.

t=3: Utviklingen av *"Forsvarets militære effekt (Etot)"* vil etter en stund registreres av trusselagenten (tiden trusselagenten trenger for å observerer at variabelen *"Forsvarets relative militære effekt i de fysiske domenene"* øker) og svare med å benytte mer ressurser for utvikling av evne til logiske angrep. Dette medfører igjen at variabelen *"antall vellykkede logiske angrep mot INI"* øker med påfølgende reduksjon av *"Forsvarets militære effekt (Etot)"*. På dette tidspunktet er *"totalt antall enheter i Forsvaret"* ytterligere redusert og Forsvarets avhengighet av INI for å skape militær effekt har økt. Resultatet er at *"Forsvarets militære effekt (Etot)"* får et enda større negativt utslag i forhold til behovet en det ville fått ved t=1 og t=2 (siden de da hadde flere enheter totalt og følgelig ikke var like avhengig av INI for å skape militær effekt). Som et resultat av dette vil også variabelen gap behov - evne til militær effekt øke igjen.

t=4: Etter en tidsforsinkelse registreres økningen i *"gap behov - evne til militær effekt"* igjen av Forsvaret. På dette tidspunktet vil også *"totalt antall enheter i Forsvaret"* være ytterligere redusert og bidra til økningen. Forsvarets svar på en slik situasjon er å igjen øke bruken av ressurser for nettveksorganisering, siden dette er deres policy for hvordan gapet mellom behov og evne til å skape militær effekt skal håndteres. Deretter vil handlingene og resultatene i t=1 og t=2 gjenta seg (ikke med i figuren;



Figur 42: Behaviour Over Time (BOT) grafer for sentrale variabler

vil skje i forlengelsen av tidsaksene), men utslaget for variabelen variabelen *"gap behov - evne til militær effekt"* vil øke i størrelse for hver gang trusselagenten øker sin ressursbruk for å skape evne til logiske angrep. Årsaken til dette er at Forsvaret vil bli stadig mer avhengig av INI for å skape militær effekt ettersom *"totalt antall enheter i Forsvaret"* reduseres.

Resultatet i denne dynamikken er altså at Forsvaret eskalerer stadig sin bruk av ressurser for å oppnå nye NBF modenhetsgrader (fremgår av BOT merket *"Grad av nettverksorganisering i Forsvaret"*). Fienden vil følge opp med å stadig eskalere sin evne til logiske angrep (fremgår av BOT merket *"Ant vellykkede logiske angrep mot INI"*). Effektgapet (når evne ligger over eller under behov-linjen for BOT merket *"Forsvarets militære effekt (Etot)"*) vil imidlertid oscillere etter hvilken part som til enhver tid "har overtaket". Utslaget vil øke i negativ retning for Forsvaret over tid (gapet vil bli større) siden de vil bli stadig mer avhengig av INI for å skape militær effekt (fremgår av BOT *"Totalt antall enheter i Forsvaret"*). Av denne beskrivelsen fremgår det klart at dersom man ikke håndterer utilsiktet effekt ved implementering av NBF, ligger det til rette for en policy resistance situasjon; Forventet effekt av NBF (tilsiktet effekt) er at gapet mellom behov og evne for militær effekt skal lukkes.

Hypotesen over viser at utilsiktede effekter vil kunne påvirke evne til realisering av effektpotensialet i NBF. I hvor stor grad er vanskelig å si ut fra en kvalitativ modell. Det er ikke mulig å fastsette styrkeforholdet mellom løkkene B1 og B2 uten å gjennomføre en kvantitativ analyse, men vi har noen indikatorer på at det vil virke relativt sterke krefter i begge løkkene. Det eksisterer empiriske undersøkelser som tyder på at nettverksorganisering gir en flerdoblet evne til å skape militær effekt (se tabell 5). Dette medfører at B1 vil ha evne til å gir store positive utslag for *"Forsvarets militære effekt (Etot)"*. Det eksisterer også gode indikasjoner på at B2 er mye billigere å realisere enn B1 (se kapittel 5.4.2) og det finnes mange eksempler på at angrep mot en organisasjons informasjonsinfrastruktur kan medføre stor reduksjon i evne til å utføre dens virksomhetskritiske prosesser. Dette medfører at B2 vil ha evne til å gir store negative utslag for *"Forsvarets militære effekt (Etot)"*.

Vi har ikke eksplisitt innhentet data som kan forklare en eventuelt "organizational boundary" (merket "systemgrense" i figur 41) som forårsaker at de som implementerer tiltak for å realisere tilsiktet effekt ved NBF er "blinde" for den utilsiktede effekten som oppstår. Det er imidlertid en kjensgjerning at i mange organisasjoner fokuserer den øverste ledelsen ofte på håndgripelige og primære mål, mens IKT-systemer og deres sikkerhet blir ansett som "en teknisk greie" som teknisk personell skal håndtere [113];

> To many directors and managers, it tends to mean something they don't understand and that the IT manager has to deal with

Det er naturlig å anta at dette i en eller annen grad også gjelder for Forsvaret. Mange av de øverste lederne i Forsvaret har trolig sitt fokus på hvilken effekt de kan skape i de fysiske domenene. Dette er de tradisjonelle domenene for krigføring og det er følgelig langt enklere å forholde seg til hvilken effekt NBF kan skape i disse. Reaksjonen på tiltakene som bedrer effekten i de fysiske domenene kommer i det virtuelle domenet/informasjonsdomenet i form av logiske angrep (fokuset i vår oppgave). Forståelsen for slike angrep ligger som regel et godt stykke utenfor kjerneområdet i tradisjonell fagmilitær kompetanse. På den andre siden kan det også være slik at personell med teknisk

innsikt i slike angrep ikke har dyp forståelse for utførelse av militære operasjoner. Det er altså slik at et helhetlig bilde på den dynamiske situasjonene i vår problemstilling krever innsikt i både fagmilitære emner og informasjonssystemsikkerhet. En helhetlig løsning av denne utfordringen vil derfor kreve nært samarbeid mellom ulike fagmiljøer i Forsvarets organisasjon.

6.2 Løsningsarketype

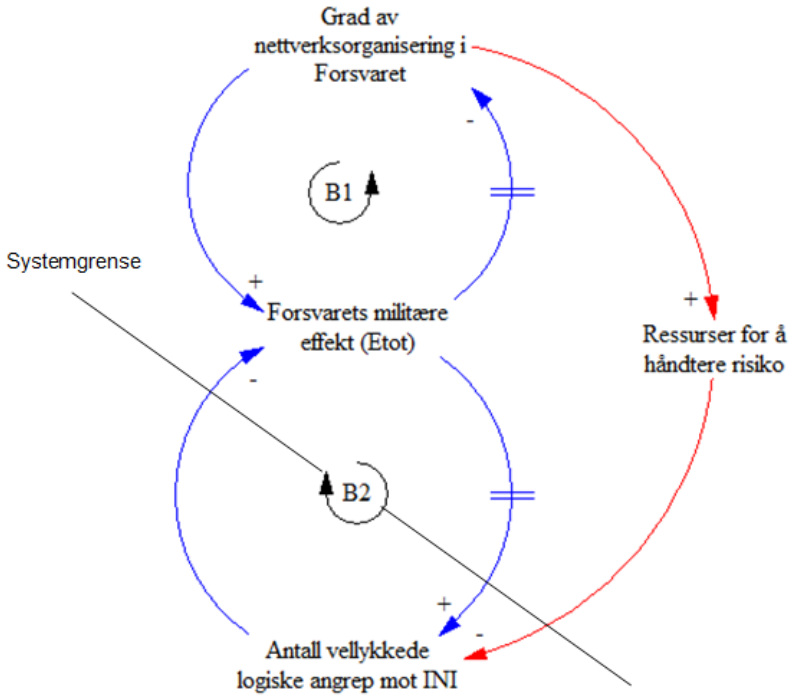
Wolstenholmes forslag til generisk løsningsarketype for "arms race" problemarketypen (se øvre høyre hjørne i figur 40) innebærer å stanse den "evige" eskaleringen gjennom en avtale mellom de to opponentene om et maksimalt nivå for begge sider. Et eksempel på dette kan være en avtale mellom to motstandere i et atomvåpenkappløp om en felles grense for maksimalt antall atomvåpen på hver side. En slik avtale forutsetter kommunikasjon mellom to rasjonell parter og at det må oppleves som om avtalen medfører fordeler for begge aktørene. Dette mener vi tilsier at denne generiske løsningen ikke vil være gyldig i vårt tilfelle. Det er flere årsaker til dette. For det første tilsier den dynamiske sikkerhetspolitiske situasjonen Norge befinner seg i at hvem den spesifikke trusselagenten er raskt kan endres. Det vil derfor være svært vanskelig å identifisere hvem vi skal inngå en slik avtale med. For det andre, dersom vi var i stand til å identifisere en gruppe trusselagenter, er det ikke sikkert at de vil oppfatte det som om en slik avtale vil være fordelaktig for dem. Det er en utbredt oppfatning at det er svært billig å utvikle evne til logiske angrep i forhold til å skaffe seg evne til militær effekt i de fysiske domenene. En slik vurdering taler for at våre motstandere kan tilegne seg et viktig fortrinn ved ikke å inngå en slik avtale.

Vi ønsker derfor å utlede vårt eget forslag til løsningsarketype basert på konteksten i vår problemstilling. Den utilsiktede effekten oppstår som et resultat av at implementering av NBF medfører en økning i verdi, trussel og sårbarhet for INI. Tilstanden for disse variablene utgjør i henhold til vår definisjon risikobildet for INI (se kapittel 5.2). Siden alle variablene øker med NBF modenhetsgrad, fastslår vi at risikoen (muligheten for logiske angrep og konsekvensen av dem) for INI øker korrelert med denne verdien. I følge Schneier [111] kan man håndtere risiko på tre måter;

> After you've identified a risk, you can do one of three things with it: You can accept it, you can reduce it, or you can insure yourself against it.

For Forsvaret er det trolig bare det andre alternativet som er reelt. Dersom de aksepterer risikoen vi har identifisert, vil de oppleve at utilsiktet effekt relatert til informasjonssikkerhet vil redusere eller oppheve den tilsiktede effekten av NBF dersom de møter en trusselagent med evne til logiske angrep. Med tanke på utviklingen vi viste i kapittel 5.4 er det svært sannsynlig at det vil kunne skje. Det tredje alternativet, forsikring, er i hovedsak tenkt på som en mulighet for organisasjoner som beskytter monetære verdier. Det finnes ingen forsikringsløsninger for tap av nasjonal suverenitet. Her kan man kanskje tenke på allianser med andre nasjoner som en slags forsikring; dersom vårt Forsvar (som et resultat av manglende evne til å håndtere risiko i informasjonssystemene sine) feiler, vil de andre nasjonenes militære enheter "ta over". Dette er trolig ingen holdbar tilnærming for de nasjonene vi er i allianse med. Norges alliansepartnere vil nok forvente at Forsvaret skal være i stand til å forsvare sine egne informasjonssystemer for å kunne levere den effekten som forventes av dem. Dette innebærer at det

alternativet vi står igjen med er å håndtere risikoen knyttet til logiske angrep mot INI. Problemarketypen viser at risikoen for vellykkede logiske angrep mot INI har en positiv kausal relasjon til grad av nettverksorganisering i Forsvaret. En grunnleggende løsning på dette må derfor følge denne utviklingen dynamisk. Det innebærer at vi parallelt med økt bruk av ressurser for nettverksorganisering, må øke bruken av ressurser for å håndtere risikoen. Av dette kan en utlede løsningsarketypen som fremgår av figur 43.



Figur 43: Løsningsarketype

Ressursene for risikohåndtering må altså benyttes parallelt med at en benytter ressurser for å øke "grad av nettverksorganisering". Variabelen "Ressurser for å håndtere risiko" må kunne motvirke trusselagentens økte evne til logiske angrep, på tross av at han anvender mer ressurser for å øke denne evnen. Som vi har vist i CLD-modellen vil dette være nødvendig for å realisere det effektpotensialet som NBF representerer. Målet er å redusere svingningene i variabelen *"Forsvarets militære effekt (Etot)"* mest mulig slik at vi oppnår en situasjon som er fordelaktig for Forsvaret. Dersom vi klarer dette, vil vi kunne hente ut den forbedrede militære effekten som NBF skaper i de fysiske domenene. Vi har derfor følgende forslag for en generisk policy som skal motvirke utilsiktet effekt og sikre realisering av effektpotensialet som ligger i NBF-konseptet;

> For å sikre realisering av effektpotensialet i NBF, skal økt bruk av ressurser for nettverksorganisering av Forsvaret medføre parallelt økt bruk av ressurser for håndtering av risiko for logiske angrep mot INI.

Denne policyen kan virke som en selvfølgelighet, men den bygger på en argumentasjonsrekke som er radikalt ulik den som vanligvis er rådende i Forsvaret. De fleste

informasjonssystemer i Forsvaret inneholder informasjon som er gradert i henhold til Lov om forebyggende sikkerhetstjeneste med tilhørende forskrifter [114]. Sikkerhetsloven med forskrifter stiller konkrete krav til forutsetninger som må innfris før et informasjonssystem kan gis sikkerhetsmessig godkjenning. Nasjonal sikkerhetsmyndighet (NSM) eller virksomhetens leder er godkjenningsansvarlig, avhengig av informasjonssystemets sikkerhetsgradering og valgt operasjonsmåte. Drivkraften bak implementeringen av risikohåndtering for informasjonssystemer i Forsvaret er altså i stor utstrekning ønsket om å oppfylle kravene i Sikkerhetsloven. Resultatet er at det i Forsvaret eksisterer et utbredt syn på informasjonssystemsikkerhet som; "noe vi må ha for å oppfylle kravene i Sikkerhetsloven". Dette forholdet underbygges av en uttalelse fra en sikkerhetsekspert ansatt hos NSM [82];

> Mange tror at de utarbeider dokumentasjon (kommentar; dokumentasjon som viser at kravene i Sikkerhetsloven er tilfredsstilt) for å tilfredsstille NSM. Da blir jeg litt provosert. Hensikten med dokumentasjonen er å sørge for at systemet er sikkert, ikke å tilfredsstille NSM.

Vår dynamiske innsikt anerkjenner at risikohåndtering for INI medfører tiltak som må gjennomføres for å sikre evne til å skape militær effekt. Håndtering av økt risiko for INI blir altså en forutsetning for effektiv gjennomføring av militære operasjoner og må derfor være et fokusområde for operative ledere i Forsvaret [112]:

> As the military operations keep evolving towards a network enabled capability (NEC), the integration between the actual operations and the communications and informations systems (CIS) increase. In order to achieve NEC operations, the dependancy on the CIS must increase, meaning that the network itself becomes an integral part of the operations.

Operative ledere bør med andre ord i fremtiden ha sitt fokus på informasjonsdomenet på lik linje med de fysiske domenene (land, sjø og luft) og inkludere det i sine operative planer.

Dersom en skal redusere risikoen knyttet til logiske angrep mot INI, må man redusere en eller flere av variablene som definerer risikobildet:

Redusere verdi for INI Den økte verdien til INI er et direkte resultat av den økte militære effekten en oppnår gjennom nettverksorganisering av Forsvaret. Den er altså direkte korrelert med tilsiktet effekt og en reduksjon av denne er ingen reell opsjon.

Redusere trussel mot INI Trusselen utvikles som et resultat av at Forsvarets militære effekt i de fysiske domenene øker. Siden økning av militær effekt (dvs; opprettholde samme evne til militær effekt, men med færre enheter) er selve målet for nettverksorganiseringen, er det (som beskrevet i avsnittet over) ikke ønskelig å redusere denne. I tillegg er det slik at en trusselagents bruk av ressurser for utvikling av kapasiteter for logiske angrep er i all hovedsak utenfor vår påvirkningsevne. Det vi imidlertid kan påvirke er graden av virkning vellykkede logiske angrep vil få i INI. Virkningen kan svekkes ved å redusere angrepenes utbredelse i tid og rom.

Redusere sårbarhet i INI Sårbarheten utvikles som et resultat av økende INI utviklingsnivå (som inneholder verdier for størrelsen, kompleksiteten, geografiske utbredelsen, osv for INI). Økningen av denne variabelen er en nødvendighet for å realisere NBF,

men det eksistere en rekke mulig tiltak for å redusere sårbarheten og virkningen av logiske angrep mot INI. Implementering av slike tiltak er innenfor vårt påvirkningsområde og fremstår derfor som et godt alternativ for reduksjon av risiko.

Som vi ser av vurderingen for de ulike variablene, er det bare reduksjon av sårbarhet og virkningen av vellykkede logiske angrep som er et reelt alternativ. Dette innebærer at vårt valg av tiltak for risikohåndtering i INI bør fokuseres mot å redusere trusselagentens mulighet for gjennomføring av vellykkede logiske angrep mot INI. Det er en utbredt oppfatning at det eksisterer tre mulige typer tiltak som kan benyttes i denne sammenhengen [17, 111, 112]:

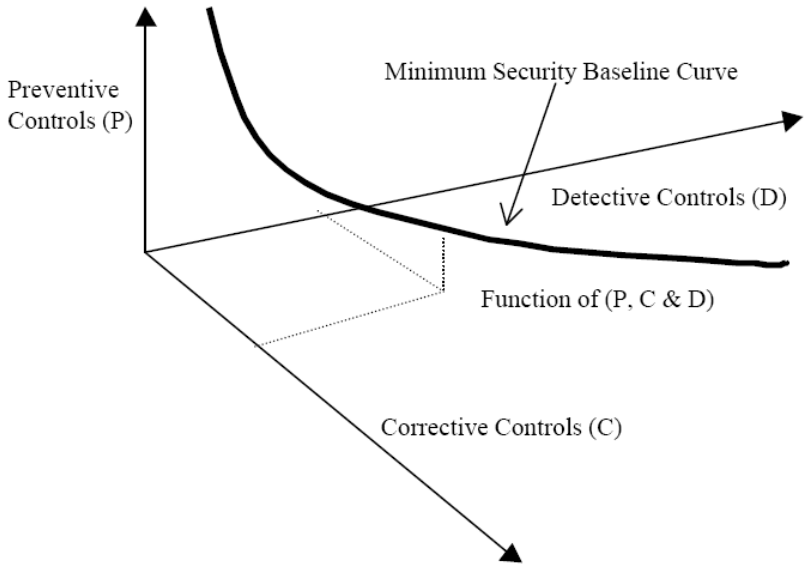
Protection/Preventive Controls Protection is a term that includes measures to protect your network, not only in a preventive manner, but also protection in the form of e.g. fault tolerance. Prevention, one area of protection measures, is the traditional security area where one fortifies the network defense against outsiders that have malicious intent. Prevention in the cyber domain has been around for quite a while and there are quite a few tools available in this area, e.g. firewalls and security protocols. However, areas such as survivability, deception and containment also fall into the protection category, but there are far fewer products and tool available in this area. Still, in order to have good cyber defense, these areas should be well covered.

Detection/Detective Controls In order to improve on the pure preventive approach to security, one of the most useful capabilities is the detection of errors or attacks. Without such detection, one cannot know when it would be good to do a system check, nor where to begin. With sensors that are able to detect both intentional and unintentional errors, one at least has a starting point. After such a detection one can use the reaction tools to, hopefully, prevent damage.

Reaction/Corrective Controls With detection tools, it is possible to react to a given number of events. Not all events might turn out to be problematic, however, they should be responded to. Different reaction measures might include event verification, damage assessment, impact analysis, attribution, eradication, containment, forensics, and response. After an incident has occurred with possible reaction and damage, it is necessary to restore the system to a well known, working, state. This might not always be easy and might have impact on the continous operation of the system. This could include restoring system backup, replacing systems with spare parts etc. The more prepared one is for the fact that recover will be necessary at some point, the easier it will be.

Det er mulig å oppnå samme kvalitative nivå av sikkerhet i et informasjonssystem gjennom anvendelse av et utall ulike kombinasjoner av disse tre tiltakene. Hvert punkt på kurven i figur 44 representerer det samme kvalitative nivå av sikkerhet gjennom ulike kombinasjoner av forebyggende, detekterende og reagerende tiltak.

Hvert tiltak som anvendes har en kostnad. Den totale kostnaden for et gitt nivå av sikkerhet vil derfor være lik summen av kostnaden knyttet til hvert enkelt tiltak. Gitt at en har et begrenset budsjett, vil altså en intelligent kombinasjon av de ulike typene tiltak gi størst mulig grad av kosteffektivitet. Fra et matematisk standpunkt vil det være



Figur 44: Ulike kombinasjoner av forebyggende, detekterende og reagerende tiltak kan gi samme kvalitative nivå av sikkerhet (alle punkter på kurven representerer samme kvalitative nivå av sikkerhet) i et informasjonssystem [17]

mulig å identifisere den optimale kombinasjonen av tiltak gjennom å beregne et minimumspunkt for grafen. Det forutsetter imidlertid eksplisitt kunnskap om kostnad knyttet til hvert tiltak og kombinasjonen av dem. Dette er trolig vanskelig å gjennomføre i praksis, men modellen kommuniserer likevell en viktig innsikt; samme nivå av sikkerhet kan oppnås gjennom ulike kombinasjoner av de tre tiltakene og hver kombinasjon har en gitt kostnad. På bakgrunn av denne innsikten, har vi viderutviklet vårt forslag til en generisk policy. Den nye versjonen tar i større grad hensyn til konteksten den skal anvendes i (redusere vellykkede logiske angrep mot INI);

> For å sikre realisering av effektpotensialet i NBF, skal økt bruk av ressurser for nettverksorganisering av Forsvaret medføre parallelt økt bruk av ressurser for håndtering av risiko for logiske angrep mot INI. Bruken av ressurser skal baseres på en intelligent og kosteffektiv kombinasjon av forebyggende, detekterende og reagerende tiltak.

Tradisjonelt sett har informasjonssikkerhetsmiljøer hatt størst fokus på forebyggende tiltak. Dette kan også sies å gjelde for Forsvaret. Et slikt ensidig fokus på forebyggende tiltak kan være lite formålstjenelig av både tekniske og operative hensyn. I følge Bruce Schneier er dette en lite konstruktiv løsning på dagens tekniske utfordringer innen informasjonssystemsikkerheten [111];

> Digital security's singular reliance on protection mechanisms is wrong, and is the primary reason we see attack after attack against digital systems today. Protection mechanisms alone can only work if the technologies are perfect. In the real world, we've never fielded any of those products without vulnerabilities.

Hoglund og McGraw har i sin bok, "Exploiting Software - How to Break Code"[105], laget et hypotetisk regnestykke som eksemplifiserer utfordringen en står ovenfor i et

middels stort informasjonssystem (30000 maskiner) dersom en ønsker å identifisere og fjerne alle sårbarheter (med andre ord forebygge ved å fjerne alle sårbarheter før noen kan utnytte dem). Regnestykket innehoder en del forutsetninger;

- Programvaren som benyttes er underlagt strenge kvalitetskontroller. (Programvare som er underlagt strenge kvalitetskontroller inneholder i gjennomsnitt 5 feil per tusen linjer kode (KLOC = Kilo Lines of Code). Dette er et lavt tall. Programkode som ikke er testet like systematisk inneholder ofte opp til 50 feil per KLOC).
- Hver maskin inneholder 3000 eksekverbare moduler (kjørbare programmer i form av EXE-filer eller biblioteker)
- Hver modul består av 100K byte kode
- En LOC er i gjennomsnitt 10 bytes

Disse forutsetningene tilsier at hver eksekverbare modul vil inneholde ca 50 feil, altså vil hver maskin i nettverket inneholde 150000 unike programmeringsfeil. Siden de samme 150000 feilene befinner seg på alle de 30000 maskinene i nettverket (homogent miljø), betyr dette at det eksisterer 4.5 milliarder instanser av disse programmeringsfeilene totalt. Dersom 10% av disse programmeringsfeilene kan resultere i en sikkerhetsfeil (feil som kan føre til tap av konfidensialitet, integritet eller tilgjengelighet) og at bare 10% av disse igjen kan nås over nettverket, eksisterer det 45 millioner programvaresårbarheter som kan utnyttes ved nettverksbaserte logiske angrep! Disse tallene viser at forsvar og angrep av informasjonssystemer er en asymmetrisk situasjon som gir en klar fordel til angriperen; han trenger i utgangspunktet bare å identifisere og utvikle et angrep mot en av disse sikkerhetsfeilene for å kunne gjennomføre et logisk angrep mot hele nettverket. Tallene indikerer også at det vil være tilnærmet umulig for en forsvarer å til enhver tid identifisere og fjerne alle disse feilene. Dette underbygger at et ensidig fokus på forebyggende tiltak trolig ikke er en fullgod eller kosteffektiv løsning.

Forsvaret håndhever et sikkerhetsregime som er basert på en sikkerhetsmessig godkjenning av informasjonssystemer før de tas i bruk. Prosessen for sikkerhetsgodkjenninger er delt i to faser [82]:

Godkjenning av referanseløsning: Først gjennomføres det en godkjenning av en såkalt referanseløsning. Referanseløsningen er en prototyp av informasjonssystemet som består av de nettverkskomponentene som skal benyttes. Komponentene blir utsatt for en grundig sikkerhetstest hver for seg og sammen som et system. Dersom komponentene består testen, utstedes en godkjenning av referanseløsning av informasjonssystemet.

Godkjenning for operativt bruk: Når godkjenning av referanseløsningen foreligger, gjennomføres det en godkjenning for operativt bruk for hver lokasjon systemet skal installeres. Denne fasen av godkjenningsarbeidet skal kontrollere at informasjonssystemet konfigureres og brukes i henhold til forutsetningene som er gjort i forbindelse med godkjenning av referanseløsning. Det legges spesiell vekt på å kontrollere administrative rutiner rundt informasjonssystemet, slik at ikke nye trusler og sårbarheter introduseres som følge av feil konfigurering og bruk.

Som vi ser av disse beskrivelsene er det en forebyggende filosofi som legges til grunn. Den godkjente referanseløsningen består av en sikkerhetsmessig test som skal fjerne

alle sårbarheter som er kjente på godkjenningstidspunktet. Godkjenningen for operativt bruk skal sørge for administrative rutiner som skal motvirke fremtidig introduksjon av sårbarheter. Slike godkjenningsregimer er svært tid- og ressurskrevende. Dette vil ikke nødvendigvis være sammenfallende med de operative behovene som NBF medfører. NBF vil trolig kreve en svært dynamisk og fleksibelt INI (se kap 5.5.2). Eksempler på dette kan være behov for tilkobling til nye aliansepartnere, flytting til nye geografiske områder, omkonfigurering av organisasjonen for å løse et oppdrag, implementering av stadig ny funksjonalitet, osv. I mange tilfeller kan en være avhengig av raske endringer for å utnytte operative mulighetsrom. Dynamisk bruk av INI vil trolig også kreve en dynamisk håndtering av sikkerheten. Dette kan tilsi at tiden det tar å gjennomføre komplette sikkerhetsmessige godkjenninger med teknisk testing og verifikasjon av alle forebyggende tiltak ikke alltid er sammenfallende med de operative behovene. Altså må man prioritere mellom muligheten til å utnytte et operativt mulighetsrom og en verifisert sikker informasjonsinfrastruktur for å realisere muligheten. I slike situasjoner kan det være fordelaktig å raskt implementere forebyggende tiltak basert på "best practice" (ikke 100% verifisert av oss selv ved testing og godkjenning) og håndtere rest-risikoen ved å kunne detektere og håndtere eventuelle logiske angrep som bryter gjennom de forebyggende tiltakene. En slik tilnærming tilsier at en må endre fokuset fra risikounngåelse til risikohåndtering. Det medfører også at man må se på risikohåndtering som en kontinuerlig prosess og ikke noe som utelukkende håndteres i forbindelse med sikkerhetsmessig godkjenning av et system. Et annet forhold som taler for en slik tilnærming til risikohåndtering er den globale trenden som går mot at datanettverk er i ferd med å bli et eget domene for krigføring. En anerkjennelse av dette forholdet innebærer at vi må ha soldater som kan utkjempe strid også i dette domenet. Slike soldater må gis kunnskap, ferdigheter og doktriner for hvordan de skal forsvare datanettverk. De må med andre ord trenes i deteksjon og håndtering av logiske angrep. Vårt fokus bør i fremtiden altså være risikohåndtering ved bruk av alle tre mulige tiltakstyper, ikke risikounngåelse ved utelukkende satsing på forebyggende tiltak. En grad av forebyggend tiltak må imidlertid alltid implementeres, men det er ikke alltid hverken den eneste eller den beste løsningen [111];

> Computer insecurity is inevitable. Technology can foil most casual attackers. Laws can deter, or at least prosecute, most criminals. But attacks will fall through the cracks. Networks will be hacked. Fraud will be committed. Money will be lost. People will die. Technology alone cannot save us. Products have problems, and they are getting worse. The only thing reasonable to do is to create processes that accept this reality, and allow us to go about our lives in the best we can.
>
> Business is about taking risks, which is why in the real world much more focus is put on detection and reaction than on prevention. Once you start thinking of security this way, everything else falls into place. If security is about avoiding threats, then it is a cost center. If security is about managing risk, it becomes a way to create revenue.

6.3 Utvidelse 3 av CLD-modell: Risikohåndtering for militær effekt

I forrige kapittel utledet vi fra løsningsarketypen et forslag til en generisk policy og utvidet den siden ved å vurdere konteksten den skal brukes i. Den utvidede policyen foreslår tiltak som skal iverksettes parallelt med implementeringen av NBF for å motvirke utilsiktet effekt. Målet er å unngå policy resistance og sikre realisering av effektpotensialet som ligger i NBF. De røde objektene i figur 45 viser tiltakene som skal redusere

utilsiktet effekt og kan ansees som en konkretisering av den generiske løsningsarketypen i forrige kapittel.

For å motvirke utilsiktet effekt, må tiltakene vi velger å bruke motvirke økningen av variabelen *"antall vellykkede logiske angrep mot INI"*. Ut fra resonnementet i forrige kapittel tilsier dette bruk av ressurser for risikohåndtering. Disse ressursene, identifisert ved variabel *"ressurser for å håndtere risiko"*, må økes dynamisk med variabelen *"ressurser for nettverksorganisering"*. Ressursene skal fordeles på tre ulike typer tiltak; forebyggende, detekterende og reagerende. De to siste tiltakstypene er svært tett knyttet til hverandre; det har liten hensikt å snakke om deteksjon uten reaksjon siden det å ikke gjøre noe også kan ansees som en reaksjon. Det betyr at ressursene for risikohåndtering skal fordeles på to ulike typer tiltak (variablene *"forebyggende tiltak"* og *"detekterende og reagerende tiltak"*):

Forebyggende tiltak Denne typen tiltak er fokusert mot å redusere antall og utbredelse av sårbarheter som trusselagenten kan utnytte til logiske angrep. Spesifikke tiltak i denne sammenhengen kan være organisert system for hurtig sikkerhetsmessig oppdatering av kjente sårbarheter, herde maskiner gjennom å fjerne unødvendige tjenester, redusere tilgang til tjenester gjennom brannmurer, osv.

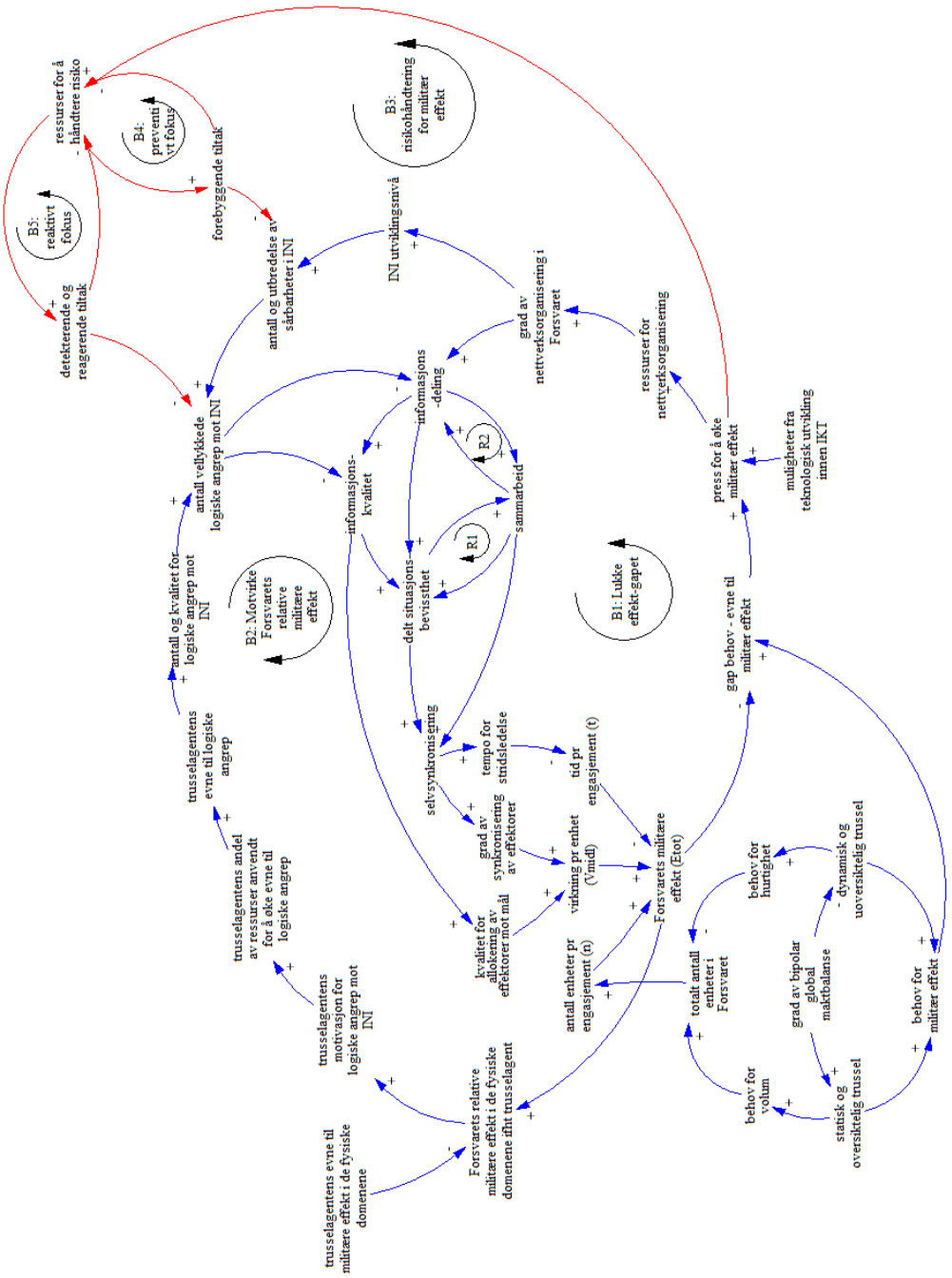
Detekterende/reagerende tiltak Denne typen tiltak er fokusert mot å redusere utbredelse i tid og rom for vellykkede logiske angrep som trusselagenten klarer å gjennomføre på tross av de forebyggende tiltakene. Spesifikke tiltak i denne sammenhengen kan være bruk av ulike overvåkningssystemer for å detektere logiske angrep, kartlegging av kjente sårbarheter for å bedre nøyaktighet i deteksjon av angrep, dataetterforskning for å fastslå effekt av vellykkede logiske angrep, prosedyrer for å begrense virkningen av et logisk angrep, osv.

På grunn av virkningen disse tiltakene har, vil de redusere variablene *"antall og utbredelse av sårbarheter i INI"* og *"antall vellykkede logiske angrep mot INI"*. Denne virkningen gir opphavet til den balanserende løkken B3: risikohåndtering for militær effekt. Siden den medfører en reduksjon i de to sist nevnte variablene, vil den virke balanserende ved at den bidrar til å redusere variabelen (gjennom en kjede variabler som fremgår av CLD-modellen) *"gap behov - evne til militær effekt"*, som igjen vil redusere variabelen *"press for å øke militær effekt"*.

De to balanserende løkkene B4: preventivt fokus og B5: reaktivt fokus oppstår som et resultat av at både *"forebyggende tiltak"* og *"detekterende og reaerende tiltak"* har sitt utspring i variabelen *"ressurser for nettverksorganisering"* som er av en gitt størrelse. Det innebærer at en her må prioritere bruken av ressurser på en intelligent måte slik at en oppnår høyest mulig grad av kosteffektivitet for den totale risikohåndteringen (se figur 44). En lignende prioritering må gjøres mellom variablene *"ressurser for nettverksorganisering"* og *"ressurser for å håndtere risiko"*. Økning av disse variablene bidrar til oppnåelse av tilsiktet effekt, men de er begge avhengig av en avgrenset mengde ressurser som i sin ytterste konsekvens er tilsvarenede forsvarsbudsjettet.

6.4 Delkonklusjon - tiltak for minimalisering av utilsiktet effekt

Det siste forskninsspørsmålet i denne rapporten var; Hvordan kan eventuell utilsiktet effekt minimaliseres?



Figur 45: Risikohåndtering for militær effekt

I kapittel 5 utledet vi at det vil oppstå utilsiktet effekt ved implementering av NBF og at den vil motvirke tilsiktet effekt. I kapittel 6 utledet vi et forslag til en policy som skal motvirke den utilsiktede effekten. Denne policyen ble utviklet på bakgrunn av vår innsikt i den dynamiske problemstillingen og konkretisert gjennom en vurdering av konteksten;

> For å sikre realisering av effektpotensialet i NBF, skal økt bruk av ressurser for nettverksorganisering av Forsvaret medføre parallelt økt bruk av ressurser for håndtering av risiko for logiske angrep mot INI. Bruken av ressurser skal baseres på en intelligent og kosteffektiv kombinasjon av forebyggende, detekterende og reagerende tiltak.

Denne policyen viser hvilke tiltak en bør anvende for å minimalisere utilsiktet effekt. Utvidelse 3 av CLD-modellen viser hvordan tiltakene vil redusere utilsiktet effekt gjennom reduksjon av antall vellykkede logiske angrep mot INI. Ved implementering av NBF vil det altså være et behov for å parallelt benytte ressurser for risikohåndtering i INI og utvikling av NBF modenhetsgrad. Begge disse faktorene vil bidra til å realisere effektpotensialet i NBF. Dette medfører, for mange, et radikalt endret syn på hvorfor en må benytte ressurser for å sikre INI. I en fremtidig verden hvor NBF medfører at Forsvaret blir stadig mer avhengig av sine IKT-systemer for å levere militær effekt, må militære ledere anerkjenne at forsvar av INI vil ha direkte innvirkning på deres evne til å gjennomføre militære operasjoner. Risikohåndtering for INI er ikke noe vi må realisere fordi det blir "en stor beholder av gradert informasjon". Risikohåndtering av INI må realiseres for å sikre Forsvarets evne til å produsere sitt viktigste produkt: evne til å skape militær effekt!

7 Konklusjon og diskusjon

7.1 Konklusjon

Implementeringen av NBF avhenger av realiseringen av en informasjonsinfrastruktur som skal knytte sammen tilnærmet alle enheter i Forsvaret. Den tilsiktede effekten er en økt evne til å skape militær effekt som en følge av at bedre informasjonskvalitet og informasjonsdeling gir bedre virkning per enhet og redusert tid per engasjement. En vellykket implementering vil således motvirke effekten av at Forsvaret reduseres i antall enheter (en balanserende løkke som lukker gapet mellom behov og evne til å skape militær effekt).

Den utilsiktede effekten av overgangen til et nettverksorganisert Forsvar er en økning av verdi, trussel og sårbarhet for den underliggende informasjonsinfrastrukturen. Med andre ord er det slik at risikobildet for informasjonsinfrastrukturen øker dynamisk med graden av nettverksorganisering Forsvaret oppnår. Realiseringen av denne risikoen innebærer økt antall vellykkede logiske angrep mot informasjonsifrastrukturen. Den forventede effekten av NBF er å gi Forsvaret et relativt fortrinn i de fysiske domenene. Denne fordelen vil dermed effektivt kunne motvirkes av våre trusselagenter gjennom logiske angrep mot informasjonsinfrastrukturen. En trusselagent som utvikler forbedret evne til logiske angrep vil således ha mulighet til å motvirke den relative ujevnheten som oppstår mellom hans og Forsvarets evne til å skape militær effekt i de fysiske domenene (en balanserende løkke som lukker gapet mellom Forsvarets og trusselagentens evne til å skape militær effekt i de fysiske domenene).

Den kombinerte virkningen av tilsiktet og utilsiktet effekt vil medføre en stadig eskalering av henholdsvis grad av nettverksorganisering for Forsvaret og evne til logiske angrep for trusselagentene. Den relative fordelen i de fysiske domenene vil imidlertid oscillere mellom Forsvaret og trusselagenten ut fra hvem som til enhver tid klarer å skape mest effekt av sine konsepter (en situasjon som kjennetegnes av en “relative control” systemarketype).

En systemdynamisk løsning på denne situasjonen i Forsvarets favør innebærerer økt bruk av ressurser for å motvirke logiske angrep mot informasjonsinfrastrukturen parallelt med økningen av ressursbruk for nettverksorganisering. Dersom økningen i antall og virkningen av vellykkede logiske angrep kan motvirkes i tide og i nødvendig utstrekning samtidig som man implementerer NBF, vil det være mulig å oppnå den potensielle effektforbedringen som forventes av en nettverksorganisering av Forsvaret.

Siden Forsvaret i all hovedsak bare kan påvirke økningen av vellykkede logiske angrep gjennom en reduksjon av sårbarheter (reduserer muligheten til logiske angrep) og virkningen av logiske angrep (det er tilnærmet umulig å identifisere alle sårbarheter og ofte ikke kosteffektivt å utelukkende anvende forebyggende tiltak), foreslås følgende policy for Forsvarets transformasjon til NBF;

> **For å sikre realisering av effektpotensialet i NBF, skal økt bruk av ressurser for nettverksorganisering av Forsvaret medføre parallelt økt bruk av ressurser for håndtering av risiko for logiske angrep mot informasjonsinfrastrukturen. Bruken**

av ressurser skal baseres på en intelligent og kosteffektiv kombinasjon av forebyggende, detekterende og reagerende tiltak.

7.2 Begrensninger ved undersøkelsen

Siden det ikke ble identifisert noen andre risikoanalyser for NBF i forbindelse med kartlegging av relatert litteratur, må denne oppgaven regnes som et innledende studie for den aktuelle problemstillingen. Det har derfor vært viktigst for oss å påvise de mest sentrale kausale sammenhengene og vi har valgt vekk arbeid som vil være viktig for en dypere systemdynamisk studie av problemstillingen. Det betyr ikke at vår oppgave er unøyaktig eller har lav verdi, tvert imot; det er etter vår mening både en viktig og en riktig start! På tross av dette har arbeidet noen begrensninger.

For det første har vi kun utviklet kvalitative modeller. Slike modeller kan ikke med stor grad av presisjon eksplisitt påvise styrkeforholdet mellom de påviste kausale løkkene. Dette medfører at det er mulig å oppnå høyere grad av nøyaktighet gjennom utvikling av simulerbare kvantitative modeller for forholdet mellom tilsiktet og utilsiktet effekt, robust fordeling av ressursbruk mellom NBF organisering og risikohåndtering, robust fordeling mellom ressursbruken for forebyggende tiltak og detekterende/reagerende tiltak og størrelsen til påviste forsinkelser.

For det andre har vi ikke fokusert mye på identifisering av forsinkelser i CLD-modellene våre. Selv om vi inkluderte forsinkelser i arketypene, kan vi ha oversett forsinkelser som eksisterer på lavere nivå "modell-hierarkiet" (se Coyle's modell for en systemdynamisk prosess i kapittel 1.2). Det eksisterer i hovedsak to ulike årsaker til dynamiske forsinkelser. Den første er relatert til materiellflyt (personer, fysiske gjenstander, osv) og den andre er relatert til informasjonsflyt (observasjon av en endring, orientere seg, fatte en beslutning og iverksette valgt handling). Slike forsinkelser kan medføre en rekke problemer i et system og bør derfor kartlegges nøye. Det er ikke mulig å eksakt vurdere virkningen av disse uten å utvikle en simulerbar modell, men påvisning vil være et første steg på veien.

For det tredje har vi ikke eksplisitt identifisert måleenheter for alle variablene i modellen. Flere av variablene er myke, noe som kan medføre at man derfor må utlede indirekte måleenheter for disse. En eksplisitt angivelse av måleenheter for alle variablene i en CLD-modell, øker modellens validitet. Dette vil også være påkrevd dersom man skal utvikle en kvantitativ simulerbar modell for problemstillingen.

En fjerde faktor som kan virke begrensende på undersøkelsen er utvalget av fageksperter. Som vi tidligere har nevnt, ble fagekspertene valgt på bakgrunn av deres kjennskap til et eller flere av fagområdene oppgaven berører. Det hadde vært ønskelig å identifisere aktører for alle interessenter (stakeholders) for NBF i Forsvaret for så å gjennomføre en gruppemodelleringsprosess med disse. En slik tilnærming har ikke vært mulig for oss siden vi ikke har nok innflytelse i Forsvaret til å samle alle interessenter til et felles møte. Et slik møte ville økt validiteten til modellene ved at man hadde forsikret seg mot at viktige synspunkter er utelatt.

Den siste faktoren vi vil bemerke er at modellen for tilsiktet effekt er basert på hypotesen om hvordan NBF vil medføre økt militær effekt. Dette er imidlertid den eneste informasjonen som finnes for NBF i en hel forsvarsmakt. Det eksisterer som nevnt en del empiriske undersøkelser som indikerer at nettverksorganisering kan gi en radikal økning av effekt på taktisk nivå (se kapittel 4.6), men vi har ikke identifisert noen empiriske

bevis for at dette er tilfelle ved nettverksorganisering av en hel forsvarsmakt.

7.3 Videre arbeid

For fremtiden er det ønskelig å fortsette det systemdynamiske arbeidet for å øke innsikten i problemstillingen fremsatt i denne undersøkelsen. Vi ser for oss to ulike retninger som kan bidra i denne prosessen. Disse er ikke innbyrdes ekskluderende.

Den første retningen innebærer å videreutvikle presisjonen til de kvalitative modellene som er utviklet i denne oppgave. For det første er det ønskelig å identifisere eventuelle forsinkelser i de to balanserende løkkene for tilsiktet og utilsiktet effekt. Forsinkelser kan medføre store utslag i oscilleringen mellom dem og er således viktig informasjon for å øke innsikten i problemstillingen.

Det er også av stor interesse å utvide modellen med variabler relatert til menneskelige aspekter ved en økning i logiske angrep mot INI. Hva skjer dersom brukerne av INI opplever at fienden til stadighet lykkes i å trenge inn i informasjonssystemet de er så avhengige av for å gjøre jobben sin? La oss gjøre et lite tanke-ekspiriment... Tenk deg at en offiser (beslutningstaker) mottar måldata fra en radar over INI i form av en posisjonsangivelse. Han benytter denne informasjonen til å utløse beskytning av fiendtlige enheter ved å sende en elektronisk ildordre, bestående av koordinater for den fiendtlige enheten, til en effektor som automatisk effektuerer denne ordren. På samme tid har fienden gjennomført et vellykket logisk angrep mot INI som setter han i stand til å endre koordinatene i ildordren slik at resultatet blir at effektoren beskyter egne styrker. La oss så si at offiseren opplever dette to ganger på rad. Er det sannsynlig at han vil stole på INI i fremtiden? Vår hypotese er at dette vil medføre en situasjon hvor brukerne ikke tørr å benytte seg av INI lengre og at han heller vil returnere til gamle, velkjente metoder for krigføring. Dersom dette skjer i en større del av organisasjonen, vil det kunne resultere i en dramatisk reduksjon i Forsvarets evne til å skape militær effekt siden den er basert på bruken av INI. Fra et systemdynamisk synspunkt innebærer det at den balanserende løkken for utilsiktet effekt kan øke dramatisk (virkningen skapes ikke bare av de tekniske følgene av det logiske angrepet, men også ved at brukerne "vender seg vekk" fra systemet som er muliggjøreren i NBF) og således medføre enda større negative utslag for relativt fortrinn i de fysiske domenene.

En annen side ved det menneskelige aspektet som kan påvirke risikoutviklingen for INI er knyttet til den dynamiske relasjonen mellom innføring av nye prosesser og behovet for ny kunnskap. Dersom det innføres nye prosesser uten at menneskene i Forsvaret har den kunnskapen som kreves for å virke i de nye miljøene, kan dette medføre økt risiko. Her er det tidligere utført kvantitativ systemdynamisk forskning i forbindelse med innføringen av eDrift i oljenæringen som kan legge grunnlaget for lignende undersøkelser for transformasjonen i Forsvaret [28, 48, 49]

Et siste forslag til arbeid som kan øke presisjonen til den kvalitative modellen er å gjennomføre en gruppemodelleringsprosess med representanter fra alle grupper av interessenter for NBF i Forsvaret. En slik prosess kan enten gjøres "helt fra bunnen av", eller en kan anvende modellene vi har utviklet i denne undersøkelsen som et utgangspunkt for diskusjon. En slik kritisk gjennomgang av modellen kan medføre økt validitet for modellen og samtidig at den kan integreres med sentrale aktørers mentale modeller om hva som er viktig for en vellykket realisering av NBF.

Den andre retningen for videre systemdynamisk arbeid vi ser for oss, er en utvikling

av en kvantitativ simulerbar modell som tilsvarer hele eller deler av den kvalitative modellen vi har utviklet. I denne sammenhengen, mener vi at følgende områder er av spesiell interesse;

- Modell som undersøker hvordan en mest effektivt kan påvirke graden av virkning mellom tilsiktet og utilsiktet effekt.
- Modell som undersøker hvordan prioritering mellom ressurser for nettverksorganisering og risikohåndtering påvirker systemets robusthet. Her eksisterer det kvantitativ systemdynamisk forskning som fokuserer på et systems robusthet relatert til prioritering av ressurser mellom optimalisering av produksjon og sikkerhet [115]. Innsikten fra denne forskningen kan være et godt utgangspunkt for lignenede undersøkelser for Forsvarets transformasjon til NBF.
- Modell som undersøker hvordan prioriteringer av ressurser mellom forebyggende og detekterende/reagerende tiltak påvirker systemets robusthet.

Et siste forhold vi vil nevne er relatert til fremveksten av "cyber space" som et nytt domene for krigføring i fremtidens konflikter. Dersom Forsvaret skal kunne aktivt beskytte sin informasjonsinfrastruktur på en effektiv måte, trenger man et konsept som beskriver hva det innebærer, hvilke kapabiliteter man trenger og hvordan disse skal ledes og integreres i operativ planlegging. Relatert til vår oppgave, handler det om hvordan man konkret skal implementere detekterende og reagerende tiltak for å håndtere vellykkede logiske angrep mot INI. Det amerikanske forsvaret har utviklet et begrepsapparat for angrep og forsvar av datanettverk [116, 101]. Der benevnes akivt forsvar av datanettverk (relatert til vår CLD-modell er dette det samme som kombinasjonen av tiltakene deteksjon og reaksjon) Computer Network Defense (CND). Dette begrepet er adoptert av Forsvaret [117]. CND-enheter er ofte implementert etter samme rammeverk som Computer Security Incident Respons Team (CSIRT) [118]. Et utbredt problem blant CSIRT-enheter er at antall ansatte og tilgjengelige ressurser ofte er langt mindre enn det som kreves for å håndtere en stadig økende mengde sikkerhetsbrudd i informasjonssystemene de har ansvar for. I denne sammenhengen eksisterer det kvantitativ systemdynamisk forskning som undersøker hvordan en best kan oppnå økt effektivitet for CSIRT-enheter [119, 120]. Siden det ikke vil eksistere ubegrenset med ressurser for CND i Forsvare, vil denne forskningen kunne gi viktig innsikt og eventuelt fungere som et utgangspunkt for lignende undersøkelser.

Bibliografi

[1] Department of Defense/Office of the Under Secretary of Defense. Februar 2006. Quadrennial defense review report.

[2] China View. 2006. Chinese army holds "vanguard-206b"drill in e. china. http://news.xinhuanet.com/english/2006-11/19/content5349105.htm. Besøkt: 20.11.2006.

[3] Coyle, G. 1998. The practice of system dynamics: milestones, lessons and ideas from 30 years experience. *System Dynamics Review*, 14(4), 343–365.

[4] Wolstenholme, E. F. 2003. Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review*, 19(1), 7–26.

[5] Diesen, S. april 2003. Forsvarets konsept for nettverkssentrisk krigføring. Foredrag i Oslo Militære Samfund.

[6] Forsvarsstaben. 2003. Kommandokonsept i nettverksbasert forsvar.

[7] Alberts, D. S., Gartska, J. J., Hayes, R. E., & A., S. D. august 2001. *Understanding Information Age Warfare*. CCRP Press.

[8] Alberts, D. S. & Gartska, J. J. Network centric warfare - department of defense report to congress. Technical report, US Department of Defense (DoD), 2001.

[9] Department of Defence/Office of Force Transformation. 2005. The implementation of network-centric warfare.

[10] Garstka, J. & Alberts, D. Network centric operations conceptual framework version 2.0. Technical report, Office of Force Transformation, juni 2004.

[11] Waltz, E. *Information Warfare - Principles and Operations*, chapter 4, 111. Artech House, 1 edition, 1998.

[12] Brevick, J. e. a. Nettverksbasert forsvar (nbf) eller nettverkstilpasset forsvar (ntf)? rapport fra arbeidsgruppe nbf: revisjon forsvarets felleoperative doktrine. Technical report, Forsvarets stabsskole, 2005.

[13] Hedenstad, O.-E. FFI/Rapport-2002/03973 informasjonsinfrastruktur for nbf. Technical report, Forsvarets Forsknings Institutt, Oktober 2002.

[14] Forsvarsdepartementet. Policy for militær tilpasning og anvendelse av informasjons- og kommunikasjonsteknologi i forsvaret. Technical report, Forsvarsdepartementet, September 2005.

[15] Forsvarsdepartementet. Beskrivelse av programområde informasjonsinfrastruktur - plan for perioden 2006-2009+. Technical report, Forsvarsdepartementet, 2006.

[16] Kure, i. & Sorteberg, I. FFI/Rapport- 2004/01561 network architecture for network centric warfare operations. Technical report, Forsvarets Forskningsinstitutt, januar 2004.

[17] Bass, T. & Robichaux, R. 2001. Defense-in-depth revisited: Qualitative risk analysis methodology for complex network-centric operations. *IEEE MILCOM 2001 Communications For Network-centric Operations: Creating The Information Force*, 2, 28–31.

[18] Forsvarets overkommando. *Forsvarets fellesoperative doktrine DelA - Grunnlag*, chapter 2.10.3, 42. Forsvarets overkommando, 1 edition, Februar 2000.

[19] Carpenter, J. J. Computer security issues that affect federal, state, and local governments and the code red worm. Technical report, CERT Coordination Center, 2002.

[20] CERT. 2006. CERT/CC Statistics 1988-2006. http://www.cert.org/stats/cert_stats.html. Besøkt: 14.11.2006.

[21] Tjøstheim, I., Innset, B., Haaberg, J., & Håvoll, H. Mars 2001. Introduksjon til nettverksbasert forsvar. *Militærteoretisk skriftserie*, 1, 1–75.

[22] Krepinevich, A. F. september 1994. Cavalry to computers: The patterns of military revolutions. *The National Interest*, 30–43.

[23] Forsvarsdepartementet. mars 2004. St.prp 42 (2003-2004) den videre moderniseringen av forsvaret i perioden 2005-2008. Stortingsproposisjon.

[24] Forsvarsdepartementet. September 2003. St.prp 1 for budsjettåret 2004.

[25] Sterman, J. D. 2000. *Business Dynamics - System Thinking and Modeling for a Complex Worl*. Irwin McGraw-Hill.

[26] A.Jones, G.L.Kovacich, & P.G.Luzwick. *Global Information Warfare*, chapter 1, 55. Auerbach, 1 edition, 2002.

[27] A.Jones, G.L.Kovacich, & P.G.Luzwick. *Global Information Warfare*, chapter 1, 56–59. Auerbach, 1 edition, 2002.

[28] Sveen, F. O., Qian, Y., Hillen, S., Radianti, J., & Gonzalez, J. J. 2006. A dynamic approach to vulnerability and risk analysis of the transition to eoperations. In *The 24th International Conference of the System Dynamics Society*. System Dynamics Society.

[29] Daler, T., Guldbrandsen, R., Høie, T. A., Melgård, B., & Sjølstad, T. *Håndbok i datasikkerhet - informasjonsteknologi og risikostyring*, 121. Tapir akademisk forlag, 2002.

[30] Olsen, V., Olsen, S. R., & Nystuen, K. O. Samfunnets sårbarhet som følge av avhengighet til it. Technical report, Nærings- og handelsdepartementet, oktober 2000.

[31] Wolstenholme, E. F. 1990. *System Enquiry: A System Dynamics Approach*. John Wiley & Sons.

[32] Coyle, R. G. 1996. *System Dynamics Modelling: a Practical Approach*. Chapmann & Hall/CRC.

[33] Kim, D. H. 1992. Guidelines for drawing causal loop diagrams. *The Systems Thinker*, 3(1).

[34] Forsvarsdepartementet. Derfor fornyer vi forsvaret, 2006.

[35] Forsvarsdepartementet. september 2004. Den videre moderniseringen av forsvaret 2005-2008 iverksettingsbrev for forsvarssektoren.

[36] Forsvarsdepartementet. oktober 2004. Styrke og relevans: Strategisk konsept for forsvaret i perioden 2005-2008.

[37] Forsvarsdepartementet. Konsept for styring av elektronisk informasjon i forsvaret. Technical report, Forsvarsdepartementet, september 2005.

[38] Forsvarsstaben. Konsept for nettverksbasert anvendelse av militærmakt. Delutredning for militærsjefens militærfaglige utredning 2003 (mfu03), Forsvarsstaben, 18.02 2003.

[39] Forsvarsstaben. desember 2003. Forsvarssjefens miitærfaglige utredning 2003.

[40] Forsvarsstaben. 2003. Det nye forsvaret.

[41] Forsvarsstaben. Et nytt forsvar for en ny tid, 2003.

[42] Forsvarsstaben. Mot et nettverksbasert forsvar, 2003.

[43] Forsvarsstaben. mars 2003. Utnyttelse av vedtatt struktur i realiseringen av et nettverksbasert forsvar.

[44] Forsvarsstaben. Strukturvisjon 2014+. Technical report, Forsvarsstaben, 2003.

[45] Reitan, B. K. & Pålhaugen, L. FFI/Rapport-2004/04004: Forventningene til nettverksbasert forsvar - 6 tema. Technical report, Forsvarets forskningsinstitutt (FFI), 2004.

[46] Alberts, D. S., Garstka, J. J., & Stein, F. P. August 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Press, 2nd edition.

[47] Cebrowski, A. K. & Garstka, J. J. 1998. Network centric warfare: Its origin and future. *Proceedings of the Naval Institute*, 124:1(January), 28–35.

[48] Gonzalez, J. J., Qian, Y., Sveen, F. O., & Rich, E. 2005. Helping prevent information security risks in the transition to integrated operations. *Telektronikk*, (1).

[49] Rich, E. & Gonzalez, J. J. 2006. Maintaining security and safety in high-threat e-operations transitions. In *39th Hawaii International Conference on System Science*, Sprague Jr., R. H., ed. IEEE Press.

[50] Jacobsen, D. I. *Hvordan gjennomføre undersøkelser - Innføring i samfunnsvitenskapelig metode*, chapter 4, 52–70. Høyskoleforlaget, 1 edition, 2000.

[51] Jacobsen, D. I. *Hvordan gjennomføre undersøkelser - Innføring i samfunnsvitenskapelig metode*, chapter 5, 73–107. Høyskoleforlaget, 1 edition, 2000.

[52] Jacobsen, D. I. *Hvordan gjennomføre undersøkelser - Innføring i samfunnsvitenskapelig metode*, chapter 6, 112–117. Høyskoleforlaget, 1 edition, 2000.

[53] Forrester, J. W. Designing the future. Technical report, Massachusetts Institute of Technology (MIT), 1998.

[54] Aronson, D. 2001. Targeted innovation: Using systems thinking to increase the benefits of innovation efforts. *Innovative Leader*, 6(2), 31–33.

[55] Dokumentasjonsprosjektet. 2006. Bokmålsordboka. http://www.dokpro.uio.no/ordboksoek.html. Besøkt: 07.03.2006.

[56] Wolstenholme, E. F. 1999. Qualitative vs quantitative modelling: the evolving balance. *Journal of the Operational Research Society*, 50(4), 422–428.

[57] Maani, K. E. & Cavana, R. Y. *System Thinking and Modelling: Understanding Change and Complexity*, chapter 2, 17. Pearson Education, 2000.

[58] Coyle, G. 2000. Qualitative and quantitative modelling in system dynamics: some research questions. In *System Dynamics Review*, volume 16, 225–244.

[59] Braun, W. The system archetypes. Technical report, 2002.

[60] Wolstenholme, E. F. 2004. Using generic system archetypes to support thinking and modelling. *System Dynamics Review*, 20(4), 341–356.

[61] Mostashari, A. & Sussman, J. 2004. Engaging stakeholders in engineering systems representation and modeling. In *The Engineering Systems Symposium*. MIT Engineering Systems Division.

[62] Vennix, J. A. M. 1996. *Group Model Building: Facilitating Team Learning Using System Dynamics*. John Wiley and Sons Ltd.

[63] Rouwette, E. A. J. A., Vennix, J. A. M., & van Mullekom, T. 2002. Group model building effectiveness: a review of assessment studies. *System Dynamics Review*, 18(1), 5–45.

[64] 2006. Ventana systems. http://www.vensim.com/. Besøkt: 10.04.2006.

[65] Kvale, S. 1997. *Det kvalitative forskningsintervju*. Ad Notam Gyldendal forlag.

[66] Lilledahl, G. & Hegnes, A. W. 2000. Kvalitativ metode. http://www.giaever.com/sosiologi/KM.htm_Toc496898516. Besøkt:03.03.2006.

[67] Burns, J. R. 2001. Structural validation of causal loop diagrams. In *Proceedings of the 19th International Conference of the System Dynamics Society*.

[68] Forsvarsdepartementet. Derfor fornyer vi forsvaret, 2006. side 6.

[69] Forsvarsstaben. desember 2003. Forsvarssjefens miitærfaglige utredning 2003. side 3.

[70] Forsvarsstaben. desember 2003. Forsvarssjefens miitærfaglige utredning 2003. side 6.

[71] Forsvarsstaben. Konsept for nettverksbasert anvendelse av militærmakt. Delutredning for militærsjefens militærfaglige utredning 2003 (mfu03), Forsvarsstaben, 18.02 2003. side 50.

[72] Forsvarsdepartementet. oktober 2004. Styrke og relevans: Strategisk konsept for forsvaret i perioden 2005-2008. side 26.

[73] Stålsett, S. J. 1998. Fredsetikk etter den kalde krigen. *PACEM - Militært tidsskrift for etisk og teologisk refleksjon*, 1, 10–30.

[74] Forsvarsdepartementet. 2000. *Forsvarets fellesoperative doktrine DelA - Grunnlag*. Forsvarets overkommando.

[75] Sun Tzu. *The Art of War - The New Illustrated Edition*, chapter 3, 125. Duncain Baird Publishers, 2005.

[76] Clausewitz, C. V. 1832. *Vom Kriege*. Dümmlers Verlag.

[77] Evans, P. & Wurster, T. S. 2000. *Blown to Bits: How the New Economics of Information Transforms Strategy*. Harvard Business School Press.

[78] Gonzales, D., Hollywood, J., Kingston, G., & Signori, D. Network-centric operations case study air-to-air combat with and without link 16. Technical report, RAND, 2005.

[79] Mawby, D., McDougal, I., & Boehmer, G. A network-centric operations case study: US/UK coalition combat operations during operation iraqi freedom. Technical report, Office of Force Transformation, 2005.

[80] Gonzales, D., Johnson, M., McEver, J., Leedom, D., Kingston, G., & Tseng, M. Network-centric operations case study: The stryker brigade combat team. Technical report, RAND, 2005.

[81] Jones, A. Identification of a method for the calculation of threat in an information environment. Technical report, QinetiQ, 2002.

[82] Holm, O. Risk management of information systems in dynamic environments - a case study of the norwegian defence and the process of approving classified information systems. Master's thesis, Høgskolen i Gjøvik, 2004.

[83] Jones, A. & Ashenden, D. *Risk Management for Computer Security - Protecting Your Network and Information Assets*, chapter 4, 37–53. Elsevier Butterworth Heinemann, 2005.

[84] Onerød, J. T. Sårbarheter og trusler mot informasjonssystemer. Technical report, Nasjonal sikkerhetsmyndighet, 2006.

[85] Norges standardiseringsforbund. Norsk standard: Risikoanalyse ns 5814. Technical report, Norges standardiseringsforbund (NSF), 1991.

[86] Skavland, E. I. & Jakobsen, y. M. Objekt- og informasjonssikkerhet: metode for risiko- og sårbarhetsanalyse. Technical report, Norges teknisk-naturvitenskapelige universitet (NTNU), 2000.

[87] Øksne, A. & Furuseth, H. R. Risikohåndtering: Bruk av risikoanalyser i det kontinuerlige sikkerhetsarbeidet. Technical report, Norges teknisk-naturvitenskapelige universitet (NTNU), 2004.

[88] Nasjonal sikkerhetsmyndighet. Veiledning i verdivurdering. Technical report, Nasjonal sikkerhetsmyndighet (NSM), 2005.

[89] Joint Chief of Staff. januar 1997. *Joint Pub 3-54 Joint Doctrine for Operations Security*. Joint Chief of Staff.

[90] Christensen, G. E., Grønland, S. E., & Methlie, L. B. *Informasjonsteknologi - Strategi, organisasjon, styring*, chapter 2.4, 51. Cappelen Akademisk Forlag, 3. edition, 1999.

[91] Christensen, G. E., Grønland, S. E., & Methlie, L. B. *Informasjonsteknologi - Strategi, organisasjon, styring*, chapter 2.4, 50. Cappelen Akademisk Forlag, 3. edition, 1999.

[92] Shimeall, T., Williams, P., & Dunlevy, C. 2002. Countering cyber war. *NATO review*, 49, 16–18.

[93] The Metasploit Project. http://www.metasploit.com/. Besøkt 01.11.2006.

[94] Justis- og politidepartementet. Nou 2006:6 når sikkerheten er viktigst - beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. Technical report, Justis- og politidepartementet, 2006.

[95] Radianti, J. & Gonzalez, J. J. 2006. Toward a dynamic modeling of the vulnerability black market. The Workshop on the Economics of Securing the Information Infrastructure.

[96] Rattray, G. J. *Strategic Warfare in Cyberspace*, chapter 3, 163–234. The MIT Press, 2001.

[97] Billo, C. G. & Chang, W. Cyber warfare - an analysis of the means and motivations of selected nation states. Technical report, Institute for Security Technology Studies at Dartmouth College, 2004.

[98] Hildreth, S. A. Cyberwarfare. Technical report, CRS Report for Congress, 2001.

[99] Joint Chief of Staff. februar 1996. *Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare (C2W)*. Joint Chief of Staff.

[100] Joint Chief of Staff. oktober 1998. *Joint Pub 3-13 Joint Doctrine for Information Operations*. Joint Chief of Staff.

[101] Joint Chief of Staff. februar 2006. *Joint Pub 3-13 Joint Doctrine for Information Operations*. Joint Chief of Staff.

[102] Federal Computer Week. november 2006. Air force leaders hold cyber summit. http://www.fcw.com/article96881-11-17-06-Web. Besøkt 18.11.2006.

[103] Federal Computer Week. november 2006. Air force to create cyber command. http://www.fcw.com/article96791-11-13-06-Print. Besøkt: 15.11.2006.

[104] Howard, J. D. & Longstaff, T. A. A common language for computer security incidents. Technical report, Sandia National Laboratories, 1998.

[105] Hoglund, G. & McGraw, G. 2004. *Exploiting Software - How to Break Code*. Addison Wesley.

[106] A.Jones, G.L.Kovacich, & P.G.Luzwick. *Global Information Warfare*, chapter 6, 131–155. Auerbach, 1 edition, 2002.

[107] Pethia, R. D. Cyber security - growing risk from growing vulnerability. Technical report, CERT, 2003.

[108] A.Jones, G.L.Kovacich, & P.G.Luzwick. 2002. *Global Information Warfare*. Auerbach.

[109] of Defense (DoD), D. Dod chief information officer (cio) guidance and policy memorandum (g&pm) no. 11-8450, department of defense (dod) global information grid (gig) computing. Technical report, Department of Defense (DoD), 2001.

[110] Alberts, D. S. 1996. *The Unintended Consequences of Information Age Technologies*. National Defense University Press.

[111] Schneier, B. 2000. *Secrets & Lies - Digital Security in a Networked World*. John Wiley & Sons, Inc.

[112] Hallingstad, G. & Eckstein, K. Cyber defence protection methods. Technical report, NATO Consultation, Command and Control Agency (NC3A), 2005.

[113] Calder, A. & Watkins, S. 2004. *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO 17799*. Kogan Page Ltd., 2 edition.

[114] 2005. *Lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven) med endringer, sist ved lov av 17. juni 2005 nr.81 (i kraft 1. januar 2006) samt forskrifter*. Cappelen Akademisk Forlag Lovdata, 2 edition.

[115] Rydzak, F., Breistrand, L. S., Sveen, F. O., Qian, Y., & Gonzalez, J. J. 2006. Exploring resilience towards risks in eoperations in the oil and gas industry. In *SAFECOMP*, 57–70.

[116] Joint Chief of Staff. CJCSI 6510.01D information assurance (ia) and computer network defense (cnd). Technical report, Joint Chief of Staff, 2004.

[117] Forsvarsstaben. Militære informasjonsoperasjoner. Delutredning for militærsjefens militærfaglige utredning 2003 (mfu03), Forsvarsstaben, 2003.

[118] Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. Defining incident management processes for csirts: A work in progress. Technical report, CERT, 2004. side 9.

[119] Wiik, J., Gonzalez, J. J., & Kossakowski, K.-P. 2005. Limits to effectiveness of Computer Security Incident Response Teams (CSIRTs). In *Proceedings of the 23rd International Conference of the System Dynamics Society*.

[120] Wiik, J., Gonzalez, J., & Kossakowski, K.-P. 2006. Effectiveness of proactive csirt services. In *18th Annual FIRST Conference on Computer Security Incident Handling*.