FFI RAPPORT

INFORMASJONSINFRASTRUKTUR FOR NBF

HEDENSTAD, Ole-Erik

FFI/RAPPORT-2002/03973

FFIE/855/134

Godkjent
Kjeller 30. oktober 2002

Vidar S Andersen
Forskningssjef

INFORMASJONSINFRASTRUKTUR FOR NBF

HEDENSTAD, Ole-Erik

FFI/RAPPORT-2002/03973

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2002/03973	UNCLASSIFIED	32
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFIE/855/134	-	

4) TITLE

INFORMASJONSINFRASTRUKTUR FOR NBF

INFORMATION INFRASTRUCTURE FOR NETWORK CENTRIC WARFARE

5) NAMES OF AUTHOR(S) IN FULL (surname first)

HEDENSTAD, Ole-Erik

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Information infrastructure	a) Informasjonsinfrastruktur
b) Network Centric Warfare	b) Nettverksbasert Forsvar
c) Information system	c) Informasjonssystem
d) Communication infrastructure	d) Kommunikasjonsinfrastruktur
e) Service infrastructure	e) Tjenesteinfrastruktur

THESAURUS REFERENCE:

8) ABSTRACT

This report is part of a report series that describes central technology areas for the future defence. The topic presented is information infrastructure for Network Centric Warfare (NCW). The future defence will move in the direction of Network Centric Warfare, and a capable information infrastructure is needed to achieve this.

The purpose of the report is to elaborate on the information infrastructure needed in Network Centric Warfare. The information infrastructure consists of a service infrastructure (traditionally called information system) and a communication infrastructure. Essential characteristics of the information infrastructure are described. We also discuss the operational benefit and cost implications of implementing such an infrastructure.

9) DATE	AUTHORIZED BY	POSITION
	This page only	
30. October 2002	Vidar S Andersen	Director of Research

ISBN 82-464-0655-8

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

INFORMASJONSINFRASTRUKTUR FOR NBF

1 INNLEDNING

Denne rapporten er en av flere teknologirapporter i en temaserie som har som fellestrekk at det tas opp sentrale teknologiområder for fremtidens forsvar. Formålet med rapportserien er å sette disse temaene på dagsorden og få konkretisert teknologiområdene slik at de kan inngå i den pågående langtidsplanleggingen i Forsvaret. Dette vil således være bidrag inn i både Forsvarssjefens militærfaglige utredning 2003 (FSJ MFU03) i FO og langtidsplanleggingen (LTD04) i FD. Rapportserien koordineres av FFI-prosjekt 845 "Terrorisme og teknologi".

Tema for denne rapporten er informasjonsinfrastruktur for Nettverksbasert Forsvar (NbF). Fremtidens forsvar skal utvikle seg i nettverksbasert retning, og en forutsetning for å få til dette er en godt utbygget informasjonsinfrastruktur som kan understøtte NbF.

Formålet med rapporten er å klargjøre hvilken informasjonsinfrastruktur som er egnet for et Nettverksbasert Forsvar. De nødvendige egenskaper ved infrastrukturen blir beskrevet, samt at muligheter som teknologiområdet åpner for og nytteverdien for Forsvaret blir behandlet. Også kostnadsaspekter blir berørt. Det må spesielt nevnes at mange ulike teknologier inngår i informasjonsinfrastrukturen. Eksempelvis finnes det et utall av kommunikasjonsteknologier for trådløs kommunikasjon, hvor hver enkelt er optimalisert for spesielle anvendelser.

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. Begrepet *informasjonsgrid* har også vært brukt i forbindelse med NbF. Dette begrepet er å betrakte som synonymt med *informasjonsinfrastruktur*.

Rapporten er bygd opp som følger:

- Overordnede egenskaper og definisjon av informasjonsinfrastruktur (kapittel 2).
- Hvilken militær nytte en slike informasjonsinfrastruktur kan gi (kapittel 3).
- De ulike komponenter som inngår i infrastrukturen (kapittel 4).
- Komponentene tjeneste- og kommunikasjonsinfrastruktur blir behandlet spesielt (henholdsvis kapittel 5 og 6).
- Kostnadseksempler (kapittel 7).

En viktig egenskap ved en informasjonsinfrastruktur er at den er en *felles* ressurs som brukes av

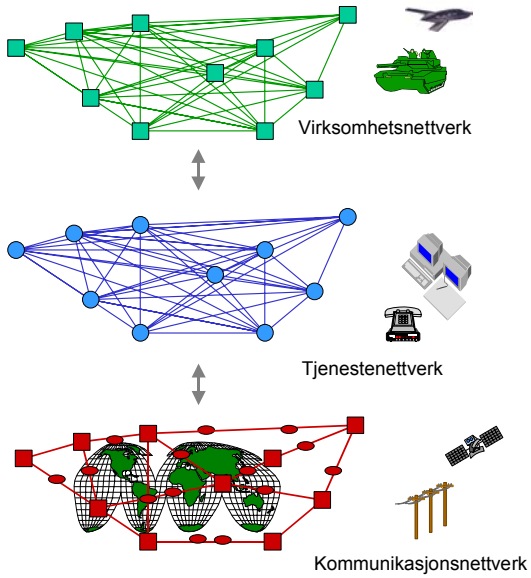
flere aktører. Rapporten omhandler ikke infrastrukturelementer som er av mer personlig karakter, slik som kommunikasjonsutrustning på soldatnivå.

2 EGENSKAPER VED INFORMASJONSINFRASTRUKTUREN

I dette kapitlet beskriver vi i stort hva en informasjonsinfrastruktur for NbF er. For enkelthets skyld blir informasjonsinfrastruktur omtalt som *infostruktur*. Det fokuseres på hva infostrukturen gir brukerne, dvs egenskaper ved infostrukturen sett fra virksomhetsnivå.

2.1 Nettverkene i NbF

I et Nettverksbasert Forsvar (NbF) har man nettverk på flere nivåer, som illustrert i figur 2.1. På øverste nivå har vi *virksomhetsnett* som gir en logisk kopling mellom ulike militære avdelinger og styrker. Disse enhetene kalles aktører (komponenter), og det er i hovedsak tre typer; beslutnings-, effektor- (våpensystem) og sensoraktører. Man kan si at virksomhetsnettet gir de nødvendige relasjoner mellom disse aktørene og dermed representerer behovet sett fra virksomheten. Dette kan for eksempel være relasjoner som er nødvendige for å foreta koordinering og informasjonsutveksling for at aktørene skal kunne utføre sine oppgaver.



Figur 2.1 De ulike nettverkene i NbF.

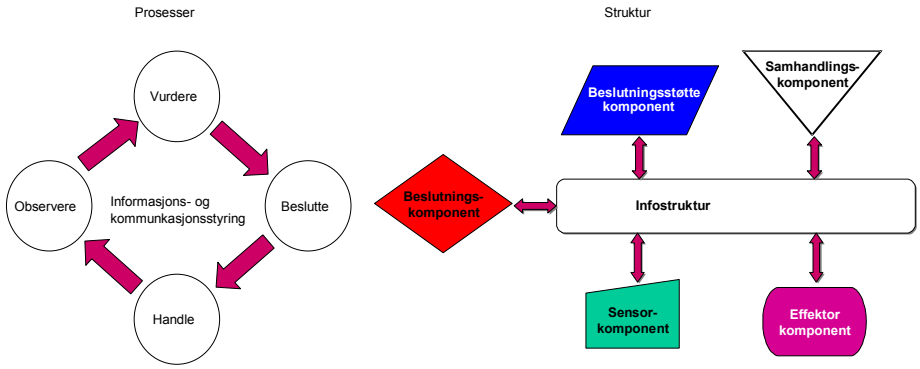
Aktørene er brukere av et underliggende *tjenestenett*, se det midterste nivået i figuren. Noen av brukerne har rollen som tjenesteprodusenter og gjør informasjon tilgjengelig ved å legge den ut på nettet. Andre brukere har rollen som tjenesteforbrukere og henter informasjon ut fra de oppgaver som skal gjennomføres. Dette tjenestenettet er igjen avhengig av godt utbygde kommunikasjonssystemer, vist som *kommunikasjonsnett* på laveste nivå i figuren.

Både tjenestenett og kommunikasjonsnett er tekniske systemer, i motsetning til virksomhetsnett som representerer behovene for virksomheten.

2.2 Relasjoner til grunnlagsdokumenter

I MFU03 er det utviklet et konsept for *nettverksbasert anvendelse av militærmakt* i Norge. Dette NbF-konseptet (1) beskriver hvordan militære operasjoner kan gjennomføres ved å knytte sammen militære kapasiteter i nettverk ved bruk av informasjonsteknologi. Det er følgelig relatert til virksomhetsnivået som er beskrevet tidligere (se figur 2.1). Videre bruker (1) begrepet *komponent* om det som i denne rapporten er kalt *aktør*. De tre komponentkategoriene blir således beslutnings-, effektor- (våpensystem) og sensorkomponenter.

Det er også utviklet et kommandokonsept for nettverksbasert forsvar. Dette konseptet (2) definerer et kommandosystem som *de strukturer og de prosesser som etableres for å omgjøre intensjon til handling* (2). Kommandosystemet er framstilt som et sett med egenskaper som karakteriserer prosessene og en struktur av komponenter og relasjoner mellom disse (se modell i figur 2.2). Også kommandokonseptet er relatert til virksomhetsnivået.



Figur 2.2 Kommandosystemets prosess og strukturmodell.

I kommandokonseptet introduseres to nye komponenter i forhold til NbF-konseptet (1). Disse er beslutningsstøtte- og samhandlingskomponentene, se modellen i figur 2.2:

- *Beslutningsstøttekomponenten* (2) omfatter i hovedsak den kapabilitet som tilsvarer ren informasjonsbehandling og formidling. Eksempler er etterretning og militær funksjonell ekspertise innen operasjoner, logistikk (og styrkeproduksjon).
- *Samhandlingskomponenten* (2) kan forstås som liaisonelementer i utvidet forstand.

Strukturmodellen legger til grunn at ønsket om en fleksibel komponering av styrker fører til økende behov for samhandling, spesielt horisontalt i organisasjonen.

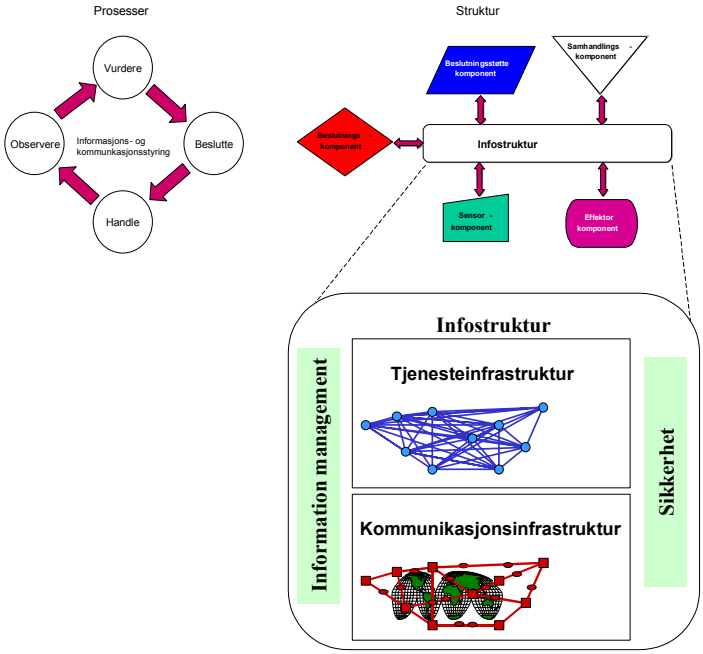
Disse to komponentene kan betraktes som spesialiserte komponenter under hovedklassen beslutningskomponent.

2.3 Definisjon

Informasjonsinfrastruktur (infostruktur) for NbF defineres som *en sammenkopling (netting) av ressurser for å muliggjøre innsamling, prosessering, lagring og distribusjon av informasjon etter aktørenes behov*. Man kan se på infostrukturen 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.

Infostrukturen består av to hovedkomponenter (se figur 2.3):

- *Kommunikasjonsinfrastrukturen* omfatter de elementer som sørger for formidling av lyd, bilde, video og data.
- *Tjenesteinfrastrukturen* omfatter de elementer som gjør informasjonstjenester tilgjengelig for brukere og applikasjoner over nettet.



Figur 2.3 Komponenter i infostrukturen.

2.4 Essensielle egenskaper ved infostrukturen

Viktige ressurser i infostrukturen vil være programvare på ulike tjenestenoder (datasystemer/servere). Denne programvaren, kalt *applikasjoner*, utfører spesifikke funksjoner og tilbyr tjenester direkte overfor brukeren. Sluttbrukeren anvender programvaren for å få støtte til å utføre de oppgaver han har ansvaret for. Videre kan den enkelte applikasjon hente databehandlingstjenester på nettet og den kan også tilby tjenester på nettet som så i neste omgang forbrukes av andre. For å få til et effektivt samvirke mellom disse distribuerte applikasjonene kreves det *sømløs deling av informasjon*. Dette innebærer at det er en *felles* forståelse av hva informasjonen betyr og ikke minst at informasjonen kan "forstås" av datamaskiner. Dette er interoperabilitet på høyeste nivå og tilsvarer interoperabilitetgrad 4 i NIMP (NATO C3 Interoperability Management Plan) (4).

Innenfor bruksområdet *bildeoppbygging* kan infostrukturen brukes til å nette alle tilgjengelige og relevante informasjonskilder for å produsere et mest mulig helhetlig og oppdatert bilde av stridssituasjonen. I den sammenheng vil infostrukturen ha distribuerte applikasjoner som tilbyr tjenester for å etablere og vedlikeholde situasjonsbilder, samt tjenester for å distribuere og presentere disse til operative beslutningstakere. Distribuert datafusjon vil være en del av dette tjenestespekteret.

Et annet bruksområde er *kommando* hvor aktører i kommandoorganisasjonen kan nettes for å få et effektivt samvirke mellom disse. De distribuerte applikasjonene vil nå ha et tjenestespekter som omfatter beslutningsfatning, operativ planlegging, oppdrag/ordeformidling og rapportering i kommandosystemet.

I stor grad vil infostruktur-ressursene være applikasjoner på ulike tjenestenoder som lagrer og prosesserer informasjon. Det vil imidlertid også være andre kommunikasjonsformer som benyttes. Eksempelvis vil det tilbys tradisjonelle tjenester som tale, video/videokonferanser og meldinger. Ideelt sett vil det være muligheter for dynamisk å kople opp forbindelser mellom hvilke som helst aktører som man ønsker. Et viktig bruksområde i denne sammenheng er å opprette koplinger direkte mellom sensor og våpensystemer for sanntids overføring av data.

Infostrukturen vil ha den egenskapen at den gir samvirke mellom alle aktører internt i FMO (Forsvarets Militære Organisasjon). Den vil også gi interoperabilitet mot allierte styrker og mot relevante offentlige etater. De mobile deler av nettet vil kunne benyttes utenfor landets grenser og fungere sammen med NATO-styrker i forbindelse med internasjonale operasjoner. Dessuten vil det nasjonale nettet kunne fungere sammen med NATO-styrker når disse er i landet. Det er ønskelig med interoperabilitet på høyeste nivå mellom alle disse aktørene. Men spesielt mot NATO og sivile etater vil det være store utfordringer forbundet med å realisere en slik *sømløs deling av informasjon*.

Informasjonsinfrastrukturen er beskrevet som et *felles* nett hvor all informasjon er tilgjengelig for aktørene som er koplet på nettet. Dette innebærer imidlertid ikke en fullstendig *fri* informasjonsflyt mellom aktørene. Det vil være en sikkerhetsrelatert kontroll knyttet til hvilken

informasjon man får tilgang til. Dette innebærer at informasjonstilgang og flyt styres gjennom informasjonens gradering og av aktørenes autorisasjon. Det er store utfordringer forbundet med realisering av informasjonssikkerhet i infostrukturen, og utfordringene øker i forhold til dagens situasjon.

En annen viktig egenskap er at nettet vil understøtte både stasjonære og mobile brukere. En stasjonær bruker vil typisk tilkoples via et fastnett (trådbundet kommunikasjon), mens en mobil bruker vil benytte trådløse kommunikasjonsnett. Infostrukturen vil ha den egenskap at det kan etableres forbindelser på tvers av de underliggende kommunikasjonssystemene, det vil si at det er fullt mulig å opprette en forbindelse mellom en mobil bruker og en stasjonær bruker. I utgangspunktet gis det gjennomgående tjenester både over trådløse og trådbundne kommunikasjonssystemer. Kvaliteten på tjenesten vil imidlertid kunne være noe dårligere når det benyttes trådløs kommunikasjon.

Infostrukturen vil ha mobile elementer som kan understøtte både nasjonale og internasjonale operasjoner. Disse mobile elementene vil ha egenskaper som er tilpasset mobiliteten i de militære operasjoner de skal understøtte (elementene vil ikke begrense mobiliteten i operasjonene de understøtter).

Infostrukturen gir også økt båndbredde. I forhold til dagens kommunikasjonssystemer forventes det at infostrukturen vil gi økt båndbredde til aktørene. Dette er fullt mulig å få til, også på taktisk nivå. Det er først og fremst et kostnadsspørsmål. Kostnadene vil være avhengig av krav til båndbredde, mobilitet og dekning.

Dessuten er det viktig at infostrukturen har egenskaper som gir god *tjenestetilgjengelighet*. Dette innebærer funksjoner for å motstå overbelastninger, feil eller ødeleggelser (omtales gjerne som robusthet). Tjenester fra nettet må være tilgjengelig når det virkelig er behov for dem.

3 NYTTEVERDI

I dette avsnittet vil vi belyse hvilken militær nytte man kan ha av informasjonsinfrastrukturen (infostrukturen) med de egenskaper som er skissert i forrige kapittel. Også en del utfordringer ved å etablere en slik infostruktur vil bli diskutert. Den militære nytten vil kunne variere noe avhengig av hvilket ambisjonsnivå man velger når det gjelder realisering.

3.1 Netting av aktører for fremskaffing av situasjonsbilder

Infostrukturen kan brukes til å knytte sammen alle tilgjengelige og relevante informasjonskilder og produsere et bilde av stridssituasjonen som er mest mulig helhetlig og oppdatert. Dette bildet gjøres tilgjengelig for operative beslutningstakere (beslutningsaktører) for å sikre disse egnet og rettidig informasjon. Som et viktig element i produksjonsprosessen benyttes det teknikker for å foreta integrasjon av sensordata, et felt som omtales som datafusjon.

En av de store fordelene med bruk av infostrukturen for *fremskaffing av situasjonsbilder* er den fleksibiliteten som ligger i at man i en gitt situasjon kan nette sammen alle informasjonskilder som er tilgjengelige og relevante. I dagens systemer er det ofte rigide prosesser for informasjonsinnhenting og bildeoppbygging. Det er på forhånd gitt hvilke informasjonskilder som skal inngå og hvordan data skal flyte i produksjonskjeden. Den nye infostrukturen kan brukes til raskt å tilpasse bildeoppbyggingen til behovet, og sammen med avanserte funksjoner for datafusjon vil dette gi økt kvalitet på situasjonsbildene (nøyaktighet, tidsriktighet, kompletthet, etc).

Infostrukturen har også fleksibilitet til raskt å kunne tilpasses ulike kommandostrukturer ved at situasjonsdata lett kan gjøres tilgjengelig for beslutningsaktører. Det vil eksempelvis i visse situasjoner være ønskelig at militære ledere på høyt nivå har en detaljert innsikt i hva som foregår. Disse lederne kan gis tilgang til situasjonsdata i tilnærmet sann tid via infostrukturen.

Bildeoppbyggingen i infostrukturen vil foregå i et enhetlig system som muliggjør samordning av bildeoppbyggingen over flere nivåer. Systemet vil også muliggjøre en *horisontal* samordning av bildeoppbyggingen på taktisk nivå, både mellom forsvarsgrener og internt mellom avdelinger i samme forsvarsgren. Applikasjoner for distribuert bildeoppbygging vil være viktig for å realisere denne samordningen på tvers av organisasjonen. Dette innebærer blant annet at de ulike avdelinger/nivåer ikke bare utveksler ”ferdige” produserte situasjonsbilder, men også utveksler ulike grunnlagsdata. Situasjonsbildene som benyttes av de ulike beslutningsaktører vil være tilpasset de ulike oppgavene den enkelte aktør har. På de ulike nivåene vil situasjons-bildene ha forskjellig detaljeringsgrad, men de vil likevel være konsistente og basert på det samme datagrunnlaget. Dette vil gi en bedret felles situasjonsbevissthet i kommandoorganisasjonen som er et viktig grunnlag for å kunne drive effektiv ledelse.

Datafusjon er et felt med store utfordringer. Faget kan karakteriseres som modent når det anvendes for ildledning i avgrensede våpensystemer (f eks luftvernsystemene på en fregatt hvor man har dedikerte sensorer knyttet sammen i et lokalnett). Det er imidlertid større utfordringer i forbindelse med stridsledelse på høyere nivåer. Skal man få full nytte av det nye informasjonsnettet vil man således måtte utvikle nye applikasjoner som gir avansert datafusjon.

Informasjonssikkerhet er en annen stor utfordring forbundet med realisering av infostrukturen. Dette temaet er diskutert i avsnitt 3.7.

3.2 Beslutningsstøtte

Den nye teknologien kan også benyttes til å nette beslutningsaktører i kommandosystemet for å få en rask planleggings-, beslutnings- og iverksettingsprosess. For å få til dette vil beslutnings-aktørene ha tilgang til distribuerte applikasjoner som støtter beslutningsfatning, operativ planlegging, formidling av intensjon/oppdrag/ordre og rapportering i kommandoorganisasjonen.

Applikasjonene innen dette bruksområdet vil ha tjenester som blant annet gir støtte for:

- Formidling av sjefens intensjon.

- Vurdering av handlemåter og utforming av planer, f eks fremskriving av stridssituasjoner under ulike forutsetninger.
- Oppnåelse av samsvar mellom planer i ulike beslutningsledd.
- Utarbeidelse av oppdrag og ordre basert på etablerte planer.
- Dynamisk re-planlegging etter hvert som operasjonen utvikler seg.
- Formidling og mottak over infostrukturen.

I dagens system er det en arbeidskrevende prosess å utarbeide planer. I infostrukturen vil man kunne representere planer, oppdrag og rapporter på en enhetlig måte hos de ulike beslutnings-aktørene. Aktørene kan dermed få datastøttet hjelp til å sikre at det er nødvendig samsvar mellom planene i de ulike ledd. Dette vil gi en betydelig raskere planleggingsprosess enn i dagens system.

Man vil ytterligere kunne redusere planleggingstiden ved at relasjoner mellom situasjonsbilder og planer er representert på en enhetlig måte i infostrukturen. Gevinsten oppnås ved at aktørene dermed kan få datastøttet hjelp til re-planlegging etter hvert som operasjonen utvikler seg.

3.3 Netting av aktører for ildledelse

Det er tidligere beskrevet hvilken nytte man har av å nette ulike aktører for å få et mest mulig helhetlig bilde av stridssituasjonen. På samme måte kan beslutningsaktører, sensorer og våpensystemer (effektorer) nettes sammen i et ildledningsnett for å bruke langtrekkende våpen for bekjempelse av tidskritiske sjø/land/luftmål (”sensor-to-shooter”).

Infostrukturen gir god konnektivitet ved at det dynamisk kan koples opp forbindelser mellom aktørene som er tilknyttet infostrukturen, uavhengig av om aktørene er mobile eller stasjonære. Dessuten gir infostrukturen tilnærmet sann tids overføring og behandling av måldata. Disse egenskapene gjør det mulig å utnytte langtrekkende våpen med måldatagivere som er lokalisert på helt andre steder enn der våpenplattformen befinner seg. På denne måten vil en få en bedret evne til å utnytte langtrekkende våpen med ulike måldatagivere. Og vi får en vesentlig reduksjon i beslutningssykluser i forbindelse med våpenengasjement.

3.4 Dynamisk organisering og selvorganisering

En fordel med bruk av infostrukturen er den fleksibiliteten som ligger i at man raskt kan nette sammen aktører på en ny måte ved endrede situasjoner og styrkesammensetninger. Denne *dynamiske* organiseringen innebærer ikke nødvendigvis fysiske forflytninger av aktørene. Ideelt sett innebærer det kun en endring av kommandoforholdene og organiseringen kan således betegnes som virtuell.

Det er beslutningsaktørenes oppgave å styre bruk av effektorer (våpensystemer) mot nærmere angitte mål. Det kan være aktuelt å dedikere beslutningstakere på lavere nivå til å lede og koordinere styrkeinnsatsen. Eksempelvis kan én av enhetene i styrken få rollen som beslutningstaker og ellers kan styrken organisere seg selv for å løse oppdraget uten styring fra

overordnet nivå. I denne sammenheng vil vi nevne at den enkelte styrkeenhet (plattform) kan ha flere roller. Enkelte styrkeenheter kan ha kapasitet til å fylle alle tre roller (sensor, effektor og beslutning), mens andre kanskje bare har kapasitet til å fylle to av rollene. I eksemplet som er beskrevet foran kan nå styrken vente lengst mulig med å bestemme intern organisering for de styrkeenhetene som skal inngå i oppdraget. Etter hvert som stridssituasjonen utvikler seg og man får oppdatert informasjon om den lokale situasjonen gjennom et felles situasjonsbilde, vil det tydeligere kunne avtegne seg hvilke roller de enkelte styrkeenheter bør ha. Først da bestemmes for eksempel hvilken enhet som skal ha sensorrollen og hvilken enhet som skal ha effektorrollen mot et gitt mål. På denne måten kan man styrke den samlede stridsevnen.

3.5 Automatisering

I infostrukturen kan deler av informasjonsbehandlingen tenkes helt eller delvis automatisert ved spesielle beslutningsstøttekomponenter kalt *agenter*. En sentral egenskap ved en agent er at den er autonom og selv kan ta initiativet til aksjoner (proaktiv). Den eksisterer på en måte uavhengig av andre agenter og arbeider aktivt mot å nå sine egne mål. Hvilke mål den arbeider mot er selvfølgelig styrt av mennesker.

Et agentsystem kan utføre utvalgte oppgaver for aktørene. Dette kan gi gevinst i form av økt tempo i stridsledelsen. Oppgavene kan for eksempel være innsamling av tilleggsinformasjon som trengs i den aktuelle situasjonen, og det kan være understøttelse av datafusjon og presentasjon av situasjonsbilder. Det kan også være samordning av bildeoppbyggingen slik at man får et felles konsistent situasjonsbilde, og omfatter oppgaver som identifisering og løsing av inkonsistens i felles situasjonsbilde.

3.6 Alle tjenester på samme nett

Som en integrert del av infostrukturen vil man ha tradisjonelle tjenester som tale, video/videokonferanser og meldinger. Dette vil være i tillegg til de mer skreddersydde informasjonstjenestene som er tilgjengelig på infostrukturen. Alt dette vil gå over det *samme* kommunikasjonsnettet, noe som betyr at brukerens tilgjengelige båndbredde fleksibelt kan fordeles mellom de ulike typer tjenester. Om ønskelig kan all båndbredde i en periode benyttes til tale, eller alt kan benyttes til data. Spesielt i forbindelse med taktiske systemer hvor man er avhengig av et underliggende trådløst kommunikasjonsnett med relativt lav båndbredde, vil dette gi stor fleksibilitet for brukerne.

At alle aktører er på *samme* nett betyr også at tradisjonelle tjenester (f eks tale) kan opprettes direkte mellom aktørene. Dette er en stor forbedring sett i forhold til dagens situasjon med mange lukkede systemer på taktisk nivå. Ved at det opprettes en gjennomgående forbindelse over de ulike underliggende kommunikasjonsnett, vil man dermed slippe manuelle mellomledd. Infostrukturen gjør det også mulig å tilby en videotjeneste direkte mellom taktisk nivå og militære ledere på høyt nivå.

3.7 Sikkerhet og tjenestetilgjengelighet

Etablering av infostrukturen vil gi store sikkerhetsmessige utfordringer. For å understøtte NbF ønsker man i utgangspunktet at informasjonssikkerheten skal ivaretas uten at det går på bekostning av funksjonalitet og fleksibilitet. Man ønsker at alle aktører skal kunne være tilknyttet den samme infostrukturen og at infostrukturen skal kunne ha informasjon på flere graderingsnivåer (fra ugradert til hemmelig). Dessuten skal aktører med forskjellig klarering kunne bruke infostrukturen. Dette krever at aktørenes informasjonstilgang vil måtte kontrolleres basert på informasjonens gradering, brukernes klarering og autorisasjon. Dette stiller store krav til informasjonssystemenes tiltro, både til operativsystem og applikasjoner. Ulike sikkerhetstjenester og -mekanismer vil være viktige elementer for å sikre informasjonen i denne sammenheng.

For å realisere den ønskede funksjonalitet og fleksibilitet krever gjeldende IT sikkerhetspolicy at infostrukturen har flernivå sikkerhetsfunksjonalitet og operasjon (MLS – Multi Level Security). Videre kreves høytillits brannmursystemer for tilkobling til aktører utenfor Forsvaret; mot offentlige etater og åpne systemer som Internett.

Flernivå operasjon vil kreve tilgang på sertifiserte operativsystemer og applikasjoner med MLS-funksjonalitet. Disse systemene må også samtidig tilfredsstille krav til funksjonalitet og fleksibilitet. Slike produkter er ikke tilgjengelige i dag, og fremtidig tilgjengelighet er avhengig av kommersiell utvikling. Forsvaret har neppe ressurser til å påvirke denne i særlig grad.

Sikkerhet i betydningen tjenestetilgjengelighet og robusthet er også et viktig aspekt. I et NbF vil det være en økt avhengighet av at infrastrukturen er tilgjengelig når aktørene trenger den. Infrastrukturen vil bli en så viktig del av Forsvaret at infrastrukturen i seg selv vil bli mål og ønskes degradert av en motstander. Infrastrukturen må sikres deretter.

Tjenestetilgjengelighet innebærer at infostrukturen har funksjoner for å motstå overbelastninger, feil eller ødeleggelser. Slike funksjoner omtales gjerne som robusthet. For å oppnå akseptabel informasjonstilgjengelighet vil det være redundant lagring (databasereplikasjon) av informasjon, d v s at informasjon distribueres slik at det finnes flere informasjonsnoder som har lagret samme informasjon. For tilgjengelighet til databehandlingstjenester betyr det tilsvarende at de samme databehandlingsressurser må være tilgjengelig fra flere noder.

3.8 Informasjonstilgang og metning

Infostrukturen har egenskaper som radikalt forenkler tilgangen til informasjon. Dette gjør det mulig for operative ledere og andre aktører til selv å finne fram til den informasjon de trenger ut fra sin situasjon og behov.

Denne forenklede informasjonstilgangen gir samtidig muligheter for at mye tid og ressurser brukes til unyttig informasjonsinnsamling. Ikke all informasjon som er tilgjengelig vil være relevant i en gitt situasjon, og det kan bli mer informasjon enn man er i stand til å fordøye. Man

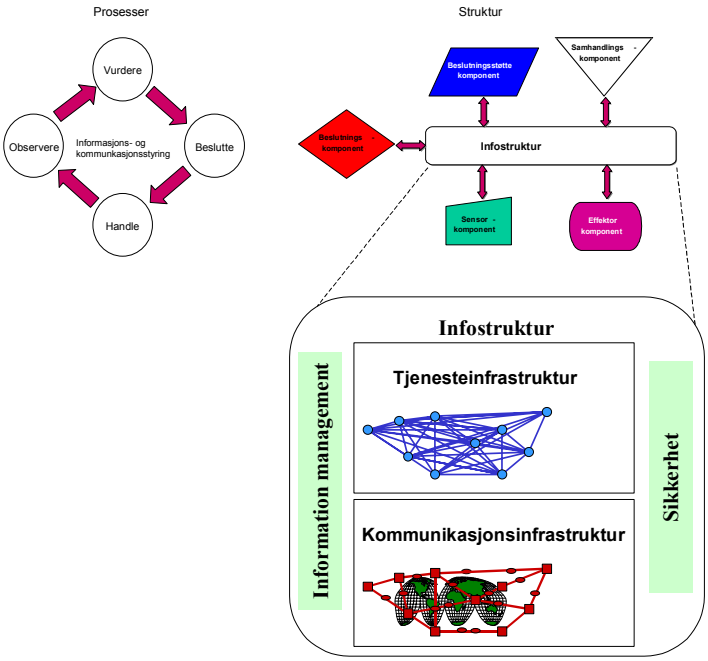
kan også få unødvendig mye trafikk på nettet. Båndbredde på taktisk nivå vil også i fremtiden som oftest være en knapp ressurs. Det vil derfor i mange situasjoner måtte legges begrensinger på bruken av nettet. Utfordringene er å etablere prosesser som sikrer tilgang til *riktig* informasjon og samtidig hindrer informasjonsmetning og unødvendig nettrafikk. Dette inngår i informasjonsstyring (*information management*), som blant annet omfatter prosesser for å lage, innhente, behandle, fordele og styre informasjon gjennom hele dets livssyklus.

Tilgang til relevant informasjon kan tenkes styrt ved at en beslutningsaktør har en stab som foretar de nødvendige operasjoner på nettet for raskt å finne frem til den informasjon beslutningstakeren trenger. Det er altså ikke fritt opp til den enkelte person å gjøre dette. Staben vil ha aksess til ulike hjelpemidler for å fremskaffe opplysninger om hvilke informasjons-tjenester som er tilgjengelig. Staben vil typisk også ha som oppgave å kontinuerlig sørge for at informasjonstilgangen er optimal.

4 KOMPONENTER I INFOSTRUKTUREN

I dette kapitlet vil vi beskrive og karakterisere de viktigste komponentene som infostrukturen består av. Figur 4.1 nedenfor viser fire komponenter:

- Tjenesteinfrastruktur
- Kommunikasjonsinfrastruktur
- Informasjonsstyring (*Information management*)
- Sikkerhet



Figur 4.1 Komponenter i infostrukturen

Tjenesteinfrastrukturen omfatter de elementer som gjør informasjonstjenester (inklusive tradisjonelle tjenester som tale) tilgjengelig for brukere og applikasjoner over nettet. Mens kommunikasjonsinfrastrukturen omfatter de elementer som sørger for formidling av lyd, bilde, video og data. Tjeneste- og kommunikasjonsinfrastrukturen er nærmere beskrevet i henholdsvis kapittel 5 og 6. Innholdet i disse kapitlene er i stor grad hentet fra (3) som forfatteren har vært med på å utarbeide.

I det følgende blir de to andre komponentene (sikkerhet og informasjonsstyring) og integrasjon av datalinker kort beskrevet.

4.1 Sikkerhet

Ulike tjenester og mekanismer for sikkerhet vil være viktige elementer i infostrukturen, og en forutsetning for samvirke mellom systemer og nasjoner. Sikkerhet i denne sammenheng er *informasjonssikkerhet* som går ut på å sikre informasjonen med hensyn på:

- Konfidensialitet (data beskyttes mot uautorisert tilgang)
- Integritet (data beskyttes mot uautorisert endring)
- Tilgjengelighet (data beskyttes mot *Denial of Service* angrep)
- Autentisitet (ekthet, data beskyttes mot forfalskning)
- Ansvarlighet (tilgang til data registreres mot brukeridentifikasjon)

Sikkerhetskonseptet må være tilpasset NbF og er avhengig av hvordan NbF realiseres. Sikkerhetskonseptet i NbF involverer alle nivåer i informasjonsinfrastrukturen.

4.2 Informasjonsstyring

Informasjonsstyring er definert som *planlegging, budsjettering, håndtering og kontrollering av informasjon gjennom hele dets livssyklus*. Som beskrevet i (1) er informasjonsstyring et *virkemiddel* for å:

- Sikre relevant informasjon til egne beslutningsprosesser.
- Spre informasjon om beslutninger og intensjoner.
- Sikre at underlagte ledd har tilgang til informasjon som gir grunnlag for rasjonell og effektiv virksomhet.

Informasjonsstyringen innvirker på infostrukturen på den måten at den setter rammene for hvilken informasjon som skal inn i infostrukturen og hvordan informasjonen behandles og fordeles. Dette betyr blant annet at det å fremskaffe og tilrettelegge de nødvendige ressurser i tjeneste- og kommunikasjonsinfrastrukturen er en del av informasjonsstyringen.

4.3 Integrasjon av datalinker

Det forutsettes at taktiske datalinker som link16 og link22 vil integreres i infostrukturen. Imidlertid har datalinker mangler i forhold til enkelte essensielle egenskaper som infostrukturen vil ha. Datalinker har blant annet en egen spesiell adresseringsstruktur. Dette gir liten fleksibilitet når datalinken skal integreres i infostrukturen. Videre er en taktisk datalink særegen

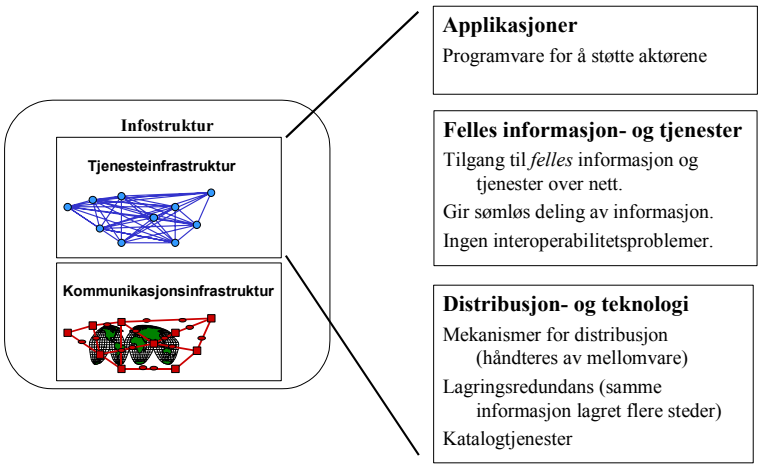
på den måten at den både er et kommunikasjonssystem (link-radio) og et informasjonssystem. Dagens datalinker må dermed integreres på begge nivåer.

I fremtiden vil man dessuten kunne introdusere helt nye løsninger slik at en aktør kan være deltager på et link-nett uten å ha en egen skreddersydd og dyr link-radio. Dette kan man få til ved at aktørene bruker infostrukturens kommunikasjonssystemer og kopler seg til ved en ny datalink-terminal som bare inneholder informasjonssystemdelen av datalinken (hvilket betyr at den gamle link-radioen er tatt ut). Eksempelvis kan en kystjeger bruke en slik terminal for å være deltager på samme link16-nett som fregatter og jagerfly. Kystjegeren bruker infostrukturens mobile kommunikasjonssystem og har en billigere utgave av link16-terminalen.

5 TJENESTEINFRASTRUKTUR

De tre hovedelementene i tjenesteinfrastrukturen er (se figur 5.1):

1. *Applikasjoner.* En applikasjon er et program som utfører en spesifikk funksjon direkte overfor brukeren. Den består av tjenester som sluttbrukeren anvender for å løse et bestemt problem.
2. *Informasjons- og tjenestenivå.* Dette nivået omfatter hvilken informasjon og hvilke tjenester som applikasjoner kan benytte. Applikasjoner kan hente noen av ressursene via informasjonsnettet, mens andre ressurser bare er tilgjengelig lokalt.
3. *Distribusjons- og teknologinivå.* Dette nivået omfatter konkrete mekanismer som benyttes for å distribuere informasjon og for å få tilgang til tjenester over informasjonsnettet.



Figur 5.1 Tjenesteinfrastruktur

Som vi ser i figuren kan disse tre hovedelementene betraktes som lagdelte elementer som understøtter hverandre. Applikasjonene (øverste element) får tilgang til informasjon og databehandlingsressurser over nettet via elementet under. Dette informasjons- og tjenestenivået

benytter igjen distribusjons- og teknologinivået (laveste element) for å få distribusjonstjenester og oppnå teknologiuavhengighet.

Egenskaper ved tjenesteinfrastrukturen som vil bli belyst i dette avsnittet er:
- Interoperabilitet på informasjons- og tjenestenivå
- Teknologiuavhengighet
- Tjenestetilgjengelighet
- Tilpasning for trådløse systemer
- Katalogtjenester

Det drøftes kort hvorvidt dagens systemer har de ønskede egenskaper og utfordringer forbundet med å realisere nye systemer som oppfyller kravene. Videre diskuteres også tilgjengelig sivil teknologi.

5.1 Interoperabilitet på informasjons- og tjenestenivå

I NIMP (NATO C3 Interoperability Management Plan) er det definert ulike interoperabilitets-grader som representerer økende grad av interaksjon mellom informasjonssystemene. Høyeste ambisjon (grad 4) er kalt *sømløs deling av informasjon*. Et nettverksbasert konsept hvor informasjon og tjenester gjøres tilgjengelig på nettet, forutsetter høyeste ambisjonsnivå.

De forskjellige gradene i NIMP-modellen (4) er kort som følger:
- *Grad 0: Ingen direkte utveksling.* Dette innebærer at det ikke er noen fysisk forbindelse mellom systemene, utveksling kan bare skje manuelt.
- *Grad 1: Ustrukturert datautveksling.* Dette innebærer utveksling av menneskelesbar ustrukturerte data som f eks friteksten man finner i operasjonsanalyser.
- *Grad 2: Strukturert datautveksling.* Dette innebærer utveksling av menneskelesbar strukturerte data som er tilrettelagt for manuell og/eller automatisk behandling, men som krever manuell sammenstilling, mottak og/eller sending av meldinger.
- *Grad 3: Sømløs deling av data.* Dette innebærer en automatisk deling av data mellom systemer som er basert på en felles utvekslingsmodell.
- *Grad 4: Sømløs deling av informasjon.* Dette er en utvidelse av grad 3 for å oppnå en universell forståelse av informasjon basert på samvirkende applikasjoner, d v s at applikasjonene bruker databehandlingstjenester som er tilgjengelig over nettet.

Interoperabilitetsgrad 3 innebærer ideelt sett at det finnes én felles utvekslingsmodell som benyttes innenfor alle funksjonsområder. Realistisk sett vil det måtte brukes et mindre antall datamodeller også i NbF. I så måte er det viktig at det er definert entydige konverteringer (mappinger) mellom de modeller som benyttes, slik at man kan få en god informasjonsutveksling også på tvers av funksjonsområder.

Merk at selv om NbF krever interoperabilitetsgrad 4, vil det også i fremtiden være informasjons-utveksling på lavere nivåer. Eksempelvis vil Web-browsing, meldingstjeneste (MIF - Meldingstjensten i Forsvaret) og elektronisk post også være aktuelt i NbF.

Dagens operative systemer gir i hovedsak interoperabiliet på nivå 2, innenfor enkelte områder også nivå 3. De viktigste mekanismene som er i bruk er formaterte meldinger (som sendes via et militært meldingshåndteringssystem) og taktiske datalinker (5). Utfordringen videre for å realisere en tjenesteinfrastruktur for NbF vil være å ta i bruk nye mekanismer som muliggjør samvirke på høyeste nivå. I tillegg bør man ha fokus på utvikling av *felles informasjonsmodeller* slik at nivå 3 samvirke i større grad blir tatt i bruk.

5.2 Teknologiuavhengighet/Mellomvare

På distribusjons- og teknologinivå benyttes det konkrete mekanismer (mellomvareteknologi) for å få tilgang til tjenester over informasjonsnettet. De forskjellige delsystemer og komponenter som realiserer disse tjenestene vil være utviklet i forskjellige programmeringsspråk. Dessuten vil delsystemene/komponentene være deployert på forskjellige maskinplattformer (maskinvarearkitekturer/ operativsystemer, o s v). Valgt mellomvareteknologi må gi uavhengighet av både programmeringsspråk og maskinplattform.

I dagens operative systemer benyttes det ikke mellomvare for **ekstern** kommunikasjon mellom systemer for å oppnå interoperabilitetsgrad 4 (som innebærer tilgang til databehandlingstjenester over nettet).

Det finnes en rekke mellomvareteknologier tilgjengelig på markedet. Objektorientert mellomvare som er i utstrakt bruk er OMGs CORBA (Common Object Request Broker Architecture) og Microsoft DCOM (Distributed Component Object Modell). Også Java-basert mellomvare som Java RMI (Remote Method Invocation) og JINI har oppnådd stor interesse. Ingen av disse teknologiene er enerådende slik at det finnes ikke bare én standard. Dessuten utvikles det stadig nye teknologier, og det antas at denne utviklingen vil fortsette. Det er derfor også viktig at applikasjonene utvikles etter metoder som gjør dem mest mulig uavhengig av spesifikke typer mellomvare. Applikasjoner kan dermed enkelt tilpasses implementering mot en mellomvareløsning.

Utfordringen for å realisere tjenesteinfrastrukturen for NbF vil være å håndtere et system hvor flere mellomvareteknologier benyttes. Til enhver tid bør Forsvaret ha en formening om hvilken teknologi som skal benyttes til ulike formål, slik at alle prosjekter som utvikler ny funksjonalitet kan forholde seg til dette valget. Men over tid forventes det at anbefalt teknologi(er) vil endres. Hvilket betyr at man også må forvente at normaltilstanden vil være at flere teknologier til enhver tid er i bruk i de ulike delsystemene, og i en slik situasjon vil det måtte defineres en entydig konvertering (mapping) mellom disse.

5.3 Tjenestetilgjengelighet.

Tjenestetilgjengelighet innebærer at tjenesteinfrastrukturen har funksjoner for å motstå overbelastninger, feil eller ødeleggelser. Slike funksjoner omtales gjerne som robusthet. I dette avsnittet beskrives tilgjengelighet som kan oppnås ved *redundans* og *prioritetsmekanismer*.

Tjenestetilgjengeligheten på dette nivået (tjenesteinfrastruktur) er dessuten avhengig av tjenestetilgjengeligheten på nivået under (d v s kommunikasjonsnettene).

Tjenesteinfrastrukturen tilbyr informasjons- og databehandlingstjenester til applikasjoner. For å oppnå akseptabel informasjonstilgjengelighet må det være redundant lagring (database-replikasjon) av informasjon, d v s at informasjon distribueres slik at det finnes flere tjenestenoder som har lagret samme informasjon. For tilgjengelighet til databehandlingstjenester betyr det tilsvarende at de samme databehandlingsressurser må være tilgjengelig fra flere noder.

På samme måte som at redundans i kommunikasjonsnettene er usynlig for brukerne av nettet, vil redundans i tjenesteinfrastrukturen være usynlig for applikasjonene og informasjons-/tjenestenivået (se figur 5.1). Nødvendig styring av redundansfunksjonene vil håndteres som en del av et *management*-system for tjenesteinfrastrukturen.

I de tilfeller at kommunikasjonsnettene degraderes og får mindre båndbredde og dermed ikke klarer å opprettholde all kommunikasjon, vil prioritetsmekanismer måtte benyttes. Applikasjonene og informasjons- og databehandlingsnoder i informasjonsnettet må kunne angi prioritet/viktighet på de ulike kommunikasjonsbehovene slik at kommunikasjonsnettene kan opprettholde prioritert kommunikasjon i de situasjoner at nettet degraderes.

I dagens operative systemer benyttes hovedsaklig formaterte meldinger og datalinker for ekstern informasjonsutveksling. Lagringsredundans oppnås dermed ved at meldingsmottakerne lagrer mottatt informasjon. Dagens metoder skjuler derimot ikke lagringsredundans for applikasjons- og tjenestenivå.

5.4 Tilpasning for trådløse/mobile systemer

Trådløse kommunikasjonssystemer vil ha båndbreddebegrensinger sammenliknet med trådbundne systemer. I utgangspunktet skal de mobile systemene kunne tilby de samme tjenestene som systemene i fastnettet, men de mobile systemene må ta hensyn til båndbreddebegrensingene som finnes i de underliggende kommunikasjonssystemene. Dette betyr blant annet at det benyttes spesielle mobil-tilpassede mekanismer for informasjons-distribusjon (på distribusjons- og teknologinivå). Til en viss grad aksepteres det også at tjenestene i den mobile infrastrukturen har noe lavere kvalitet enn i fastnettet.

I dagens systemer skjer tilpasningen for trådløse systemer ved at det brukes taktiske datalinker for trådløs datakommunikasjon. En datalink har typisk et skreddersydd meldingsformat som gjør meldingene svært korte (tilpasningen skjer på bit-nivå og kalles derfor bit-orienterte). Dette gir en effektiv bruk av båndbredde i kommunikasjonssystemene.

Taktiske datalinker vil fortsatt være i bruk i 2014. Det vil imidlertid også være behov for annen type kommunikasjon, som for eksempel sanntids data som ikke kan gå over datalinker, bilder og Web-tjenester. Det finnes ingen egnede mekanismer for å håndtere disse i dagens mobile systemer.

På sivil side skjer det en utvikling for å ta frem teknologi som kan minske gapet mellom trådløse og trådbundne tjenester. WAP (Wireless Application Protocol) er en slik teknologi. Formålet med WAP er å forlenge Internet-teknologier ut til trådløse nett og brukerterminaler.

5.5 Katalogtjenester

Innføring av standardiserte katalogtjenester vil være en forutsetning for innføring av et NbF. Kataloger vil bli benyttet på alle nivåer i informasjonsinfrastrukturen. Det vil være kataloger over brukere, brukerprofiler, ressurser av alle slag i nettverket etc. Management- og sikkerhetsinfrastrukturen vil benytte katalogtjenester. Kataloginformasjonen er viktig for å kunne operere de ulike infrastrukturer. Den må derfor være distribuert, slik at kopier finnes flere steder i nettet. Videre vil mye av kataloginformasjonen være gradert, og må sikres mot uautorisert tilgang.

For å understøtte NIMP interoperabilitetsgrad 4 (tjenester gjøres tilgjengelig over nettet) vil katalogtjenester bl a brukes til følgende:

- Av applikasjonene for å få oversikt over (også oppdage) hvilke tjenester som er på nettet.
- Av applikasjonene/mellomvare for å få lokalisert hvilke(n) noder som tilbyr aktuell tjeneste.
- Av systemet for å holde oversikt over lagrings- og tjenesteredundans.

Katalogtjenester vil bli tatt i bruk på stadig nye områder. Utfordringen i forhold til realisering av infostrukturen vil være å håndtere alle katalogtjenester på en mest mulig kosteffektiv måte.

6 KOMMUNIKASJONSINFRASTRUKTUR

Kommunikasjonsinfrastruktur dekker alle former for kommunikasjon, *fast* og *mobilt,* militære og/eller sivile ressurser (3). *Mobilitetsegenskapene* for et nettverk karakteriseres ved to aspekter; grad av mobilitet for brukernes terminaler og grad av mobilitet for nettverksinfrastrukturen. Både terminalmobilitet og infrastrukturmobilitet beskrives under ved tre alternativer:

- Fast
- Flyttbar
- Mobil

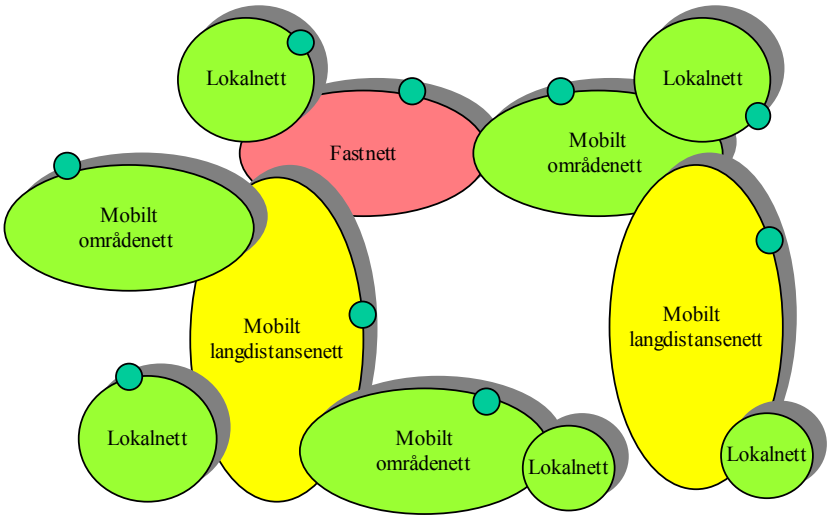
Fast er selvforklarende, flyttbar vil f eks være utstyr installert i mobil plattform eller deployerbare kommunikasjonsmoduler, og mobil vil si at utstyret er operativt under forflytning.

Fastnett brukes om systemer hvor både brukerutstyr og nettinfrastruktur er fast montert. *Mobilnett* kan brukes om systemer hvor enten brukerutstyr eller nettutstyr ikke er fast montert, dvs med mobilitetsgradene flyttbart eller mobilt.

Manøverkrigføring og operasjoner i NbF vil kreve *økt* mobilitet, både for terminaler og

infrastruktur. Mobil kommunikasjonsinfrastruktur forventes derfor å bli sentralt for Forsvaret i tiden fremover. Følgende inndeling av nettyper er gjort:

1. Et *langdistansenett* gir kommunikasjonstjenester over store avstander, for eksempel mellom aktører i forskjellige regioner av landet. Et slikt nett kan eksempelvis tenkes realisert ved satellitt- og HF-kommunikasjon, via fastnett, eller ved kombinasjoner av disse.
2. Et *områdenett* gir kommunikasjonstjenester til brukere innenfor et avgrenset geografisk område. Området kan for eksempel være en brigadeteig. Eksisterende systemer av denne typen er TADKOM og MRR i Hæren, UHF- og VHF-radio i Sjøforsvaret og Luftforsvaret.
3. Et *lokalnett* gir kommunikasjonstjenester til brukere innenfor et mindre område, for eksempel en kommandoplass. Området er betydelig mindre i utstrekning enn et områdenett. Et slikt nett kan tenkes realisert ved WLAN (Wireless LAN) eller trådbundet LAN.



Figur 6.1 Eksempel på sammenkopling av ulike nett, med aksesspunkter

I dette avsnittet vil viktige egenskaper for kommunikasjonsinfrastrukturen i NbF bli belyst:

- Tjenesteintegrert nett/full service nett
- Skalerbarhet/fleksibilitet/endringsevne
- Global dekning
- Konnektivitet mellom ulike aktører
- Større mobilitet i operasjoner
- Tjenester
- Tjenestetilgjengelighet

6.1 Tjenesteintegrert nett

Et nettverksbasert konsept krever tjenesteintegrasjon hvor brukeren får tilgang til alle tjenester via ett og samme tjenestegrensesnitt. Dette oppnås ved å realisere et *Full Service Network* (FSN) som tilbyr alle typer tjenester i ett og samme nett. FSN beskriver det samme som

tjenesteintegrasjon, men sett fra nettet som ståsted.

De to viktigste egenskapene ved et *Full Service Network* vil være:

- *Felles nett*. Et FSN vil ha et felles svitsjet nett som brukes for både tale, video og data. Dette nettet vil høyst sannsynlig være et pakkesvitsjet nett hvor det er lagt inn mekanismer for å ivareta tjenestekvalitet for sanntidskommunikasjon slik som tale.
- *Felles tjenester over flere domener*. Et FSN vil tilby tjenester som er uavhengig av om brukeren har mobil eller fast tilknytning til tjenestenettet. Et FSN vil også tilby tjenester som integrerer tale, video og data (multimedia tjenester).

Tjenesteintegrasjon gir fleksibilitet på flere måter. Nettet har automatikk (ruting) for å sette opp logiske kommunikasjonslinjer mellom ønskede aktører og gir dermed fleksibilitet i form av automatisk oppsett for ønsket konnektivitet. Nettet gir også tilgang til alle tjenester over samme grensesnitt og gir på den måten fleksibilitet ved at fordelingen mellom for eksempel tale og data kan tilpasses situasjonen. Man får også en bedre utnyttelse av den fysiske infrastrukturen.

Ingen av dagens militære kommunikasjonssystemer oppfyller denne egenskapen fullt ut. De systemer som ligger best an i så måte er FDN, TADKOM og MRR.

6.2 Skalerbarhet/endringsevne

Kommunikasjonsinfrastrukturen må være skalerbar. Blant annet må kapasiteten i ulike typer nett kunne bygges ut for å møte økninger i båndbreddebehov. Det enkelte nett må også være skalerbart på den måten at nye komponenter kan inkorporeres i nettet for å gi geografisk dekning over et større område eller for raskt å understøtte endrede situasjoner og styrkesammensetninger. Eksempelvis må komponenter kunne tas ut av et nett som skal nedkoples eller nedskaleres, for å settes sammen i et nytt nett sammen med andre komponenter, og raskt kunne konfigureres og settes i drift.

Infrastrukturen må i stor grad være selvkonfigurerende og ha egenskaper som muliggjør AdHoc-nettverk med ”plug-and-play” muligheter for brukerne.

6.3 Global dekning

Operasjoner kan i prinsippet gjennomføres hvor som helst. Dette betyr at nødvendig kommunikasjonsinfrastruktur for å understøtte styrkene må kunne transporteres til det aktuelle operasjonsområde. Dette gir krav til alle mobile og flyttbare elementer i kommunikasjonsinfrastrukturen.

6.4 Konnektivitet mellom ulike aktører

Det skal være konnektivitet mellom ulike aktører:

- Vertikalt og horisontalt på alle nivå internt i FMO.
- Mellom alle typer aktører (beslutnings-, sensor- og effektoraktør).

- Operere integrert med (utvalgte) allierte.
- Interoperabilitet mot relevante offentlige etater.

I et nettverksbasert konsept er det essensielt at kommunikasjonsinfrastrukturen kan gi både *vertikal* og *horisontal interoperabilitet* mellom ulike aktører på alle nivå internt i FMO. Interoperabilitet kan i denne sammenheng beskrives som *konnektivitet* fordi infrastrukturen setter opp logiske ende-til-ende kommunikasjonslinjer mellom de aktører som skal kommunisere. Kravet om horisontal konnektivitet innebærer en flat struktur hvor kommunikasjonslinjene ikke bare følger den tradisjonelle kommandostrukturen.

Konnektivitet skal kunne realiseres uavhengig av hvilket subnett den enkelte aktør faktisk er tilkoplet, enten subnettet er av typen fastnett, mobilt langdistansenett, mobilt områdenett eller mobilt lokalnett. Dette krever at de ulike subnett må ha en felles adresseringstruktur og ruting, det vil si krav som er relatert til nettlaget i OSI (Open Systems Interconnection) Referanse-modellen. Konnektivitet på nettlaget betyr at det opprettes logiske kommunikasjonslinjer som går over flere subnett via koplinger på nettlaget. Det kreves koplinger mellom alle typer nett. I tillegg kreves det at disse nettene kan koples sammen i *kjeder*.

Den eksisterende militære kommunikasjonsinfrastrukturen har flere mangler innen dette området.

6.5 Mobilitet / Større mobilitet i operasjoner

Et overordnet krav i forbindelse med mobilitet er at samme kommunikasjonsinfrastruktur skal kunne støtte både nasjonale og internasjonale operasjoner. Dessuten skal infrastrukturen ikke begrense mobiliteten i operasjonene de understøtter.

Lokalnett vil omfatte mobilitetsgradene *mobil* (operative under forflytning) og *flyttbar* (installert i mobil plattform). Et kjøretøysbasert lokalnett (dvs flyttbart) vil for eksempel kunne benyttes for trådløs kommunikasjon innenfor en kommandoplass. Aktuelle sivil teknologi for denne type nett er trådløs LAN (WLAN – Wireless LAN).

Områdenett vil også omfatte mobilitetsgradene *mobilt* og *flyttbart*. Et mobilt områdenett vil for eksempel kunne installeres i kjøretøy på bakken, og avhengig av implementasjon vil et slikt nett enten være på *flyttbart* eller *mobilt* nivå. Dagens TADKOM-system i Hæren er et eksempel på et bakkebasert områdenett som er flyttbart. Et mobilt områdenett vil også kunne realiseres med eleverte plattformer (fly-rele, UAV-rele, aerostat). Et eksempel på et elevert system er et sivilt konsept (HALO Network) fra Angel Technology Corporation. Dette konseptet er basert på fly som flyr i opptil 20 km høyde. Dekningsområdet er en sirkel på ca 40 km i diameter med en totalkapasitet på 10-15 Gbit/s. Systemet er i utgangspunktet laget for brukere i faste installasjoner på bakken. Men systemer av denne typen vurderes å kunne utvides til mobilt terminalutstyr på bakken.

For langdistansenett er løsninger basert på satellittkommunikasjon aktuelle. Områdenett kan

også realiseres ved satellittkommunikasjon.

6.6 Overføringstjenester

Tjenestetilbudet er kategorisert i fire hovedkategorier:

- Sanntids lav båndbredde (tale, datalink)
- Sanntids høy båndbredde (video/videokonferanse, sensordata)
- Ikke-sanntid lav båndbredde (tekst/formatterte meldinger, data)
- Ikke-sanntid høy båndbredde (data)

Aktører som er tilknyttet et mobilt lokalnett skal kunne benytte samtlige av de overnevnte tjenestekategoriene. Det samme gjelder aktører som er tilknyttet de andre typer mobilnett (langdistansenett og områdenett) og fastnett. Dessuten må tjenestene være gjennomgående slik at de ulike tjenester (for eksempel videokonferanse) kan realiseres på tvers av de ulike subnettene. Man må imidlertid akseptere at tjenester som bildeoverføring og video/videokonferanser vil komprimeres så sterkt i mobile/trådløse systemer at vi får en dårligere kvalitet i disse systemer enn i fastnettet.

6.7 Tjenestetilgjengelighet

Tjenestetilgjengelighet innebærer at kommunikasjonssystemet har funksjoner for å motstå overbelastninger, feil eller ødeleggelser. I dette avsnittet diskuteres tilgjengelighet innenfor ulike områder som redundans i infrastrukturen, objektsikring og prioritetsmekanismer.

Redundans i infrastrukturen betyr at det finnes flere fysiske kommunikasjonsveier (primær- og sekundærveier) mellom to geografiske punkter. Objektsikring omfatter både fysisk sikring og EMP-sikring av kommunikasjonsinstallasjoner. Krav til fysisk sikring gjelder først og fremst fastnett. For mobile systemer vil fysisk sikring kunne være aktuelt når de er i statisk bruk (d v s at de tas inn i fjellanlegg eller sikrede bygninger).

Forsvarets behov for fastnettjenester vil kunne dekkes som en kombinasjon av både sivile og militære fastnett. Dersom Forsvaret stiller krav til objektsikring av egen infrastruktur som overgår de som stilles til Totalforsvaret generelt, betyr det at Forsvarets egen kjernekapasitet må bygges ut for å dekke primærkommunikasjon for alle viktige/vitale stasjonære militære brukersteder (for å få en balansert objektsikring).

Når det gjelder krav til objektsikring i Totalforsvaret er trenden at det stilles strengere krav enn tidligere. Forsvaret bør utrede konsekvensene av denne utviklingen. Skal man for eksempel opprettholde kravene til objektsikring, skal man øke kravene, eller skal man gå inn for samme krav til objektsikring av egen kommunikasjonsinfrastruktur som for Totalforsvaret forøvrig.

Når det gjelder krav til prioritetsmekanismer, må applikasjonene kunne angi prioritet/viktighet på det som skal overføres, slik at kommunikasjonsnettene kan opprettholde prioritert kommunikasjon i de situasjoner at nettet degraderes og får mindre båndbredde.

7 KOSTNADSEKSEMPLER

Kostnadene ved å etablere en infostruktur slik den er skissert i denne rapporten vil være sterkt avhengig av flere faktorer. Dette gjelder for det første antallet aktører som er tilkoplet infostrukturen og deres *trafikkbehov*. Jo flere aktører samtidig på nettet, desto mer trafikk vil bli generert. Kommunikasjonsnettet må ha en ytelse (mht båndbredde, tidsforsinkelse med mer) som er tilpasset aktørenes trafikkbehov. Videre vil kostnadene øke med *graden av mobilitet* i infostrukturen. Et mobilnett hvor også nettutstyr (som basestasjoner) skal være operative når de forflyttes, koster vesentlig mer enn et mobilnett hvor nettutstyret kan forflyttes uten at de samtidig skal være operative. Dessuten vil kostnadene generelt øke jo større det geografiske *dekningsområdet* som skal understøttes samtidig er.

Det vil i denne rapporten gis grove kostnadsoverslag for noen få utvalgte komponenter i infostrukturen for å illustrere hvordan mobilitetsgrad og dekningsområde påvirker kostnadene. Kostnadsoverslagene er knyttet til mobile områdenett i kommunikasjonsinfrastrukturen. Ellers er estimatene basert på anskaffelse av nye systemer. Mulighetene for å oppgradere dagens systemer slik at de tilfredsstiller nødvendige egenskaper (som skissert i kap. 6), er ikke studert. Estimatene for tre eksempler er vist i tabellen nedenfor.

Eksempel		Investeringskostnader (i milliarder kr)
Bakkebasert områdenett	Neste generasjons TADKOM type nett. Mobilitetsgrad: flyttbart.	1-2
Elevert områdenett – High Altitude Platform	System med fire fly. Videreutvikling av sivilt konsept. Dekning: ett område på 40 km i diameter. Operativt under forflytning (mobilt).	1,5-2,5
Elevert områdenett – To systemer	To system á fire fly. Dekning: to områder, hver på 40 km i diameter.	3-5

Tabell 7.1 Kostnadseksempler

Det er i skrivende stund vanskelig å gi noe overslag på hva totalkostnaden på infostrukturen vil kunne bli. Dette har sin bakgrunn i de betraktninger som er gjort innledningsvis i dette kapitlet. For å kunne lage estimater på totalkostnaden vil man først måtte konkretisere hvordan det fremtidige operative Nettverksbaserte Forsvar skal være i form av strukturbeskrivelser. Det pågår arbeid i forbindelse med MFU03 for å ta frem slike strukturer.

Litteratur

(1) Forsvarets overkommando (2002): Forsvarssjefens militærfaglige utredning 2003 – Konsept for nettverksbasert anvendelse av militærmakt - Grunnlag.

(2) Forsvarets overkommando (2002): Forsvarssjefens militærfaglige utredning 2003 – Kommandokonsept i Nettverksbasert Forsvar - Grunnlag.

(3) Forsvarets overkommando (2002): Konsept for videreutvikling av Forsvarets informasjonssystemer/infrastruktur (Program FIS/I).

(4) NATO C3 Board Interoperability Sub-Committee (2001): NATO C3 Interoperability Management Plan (NIMP), Volume II, draft version 0.8, 16 February 2001.

(5) Winjum Eli, Hedenstad Ole-Erik, Sletten Geir (2000): Kartlegging av operative informasjonssystemer, FFI/RAPPORT-2000/02034, Forsvarets forskningsinstitutt, Begrenset

FORDELINGSLISTE

FFIE **Dato:** 30. oktober 2002

RAPPORTTYPE (KRYSS AV)	RAPPORT NR.	REFERANSE	RAPPORTENS DATO
X RAPP ☐ NOTAT ☐ RR	2002/03973	FFIE/855/134	30. oktober 2002
RAPPORTENS BESKYTTELSESGRAD		ANTALL EKS UTSTEDT	ANTALL SIDER
UGRADERT		62	32
RAPPORTENS TITTEL		FORFATTER(E)	
INFORMASJONSINFRASTRUKTUR FOR NBF		HEDENSTAD, Ole-Erik	
FORDELING GODKJENT AV FORSKNINGSSJEF		FORDELING GODKJENT AV AVDELINGSSJEF:	
Vidar S Andersen		Johnny Bardal	

EKSTERN FORDELING

ANTALL	EKS NR	TIL
2		FD II
2		FD IV
1		v/ Annette Hurum
1		v/ Bård Bredrup Knudsen
1		v/ Nils Espen Skjelland
1		v/ Erling Alvestad
1		v/ Torbjørn Svensgård
1		v/ Beate Lübeck
1		v/ Bjørn Tore Solberg
1		Landsdelskommando Nord
1		v/Kom Arne M Grønningsæter
1		KNMT
1		v/KK Stein Otto Hole
1		FO/E
1		v/ Tom Grønlien
1		v/ Audun Strandnæs
1		v/ Karsten Haaheim
1		v/ Runar Jørgensen
1		v/ Hans Rostrup
1		FO/FST
1		v/ Stener Olstad
1		v/ Paul Torvund
1		v/ B H T Hals
1		v/ J A Nyland
1		v/ T J Melien
1		v/ A Klevberg
1		FO/I
1		v/ Tor Einar Wivelstad
1		v/ Per Trygve Gundersen

INTERN FORDELING

ANTALL	EKS NR	TIL
14		FFI-Bibl
1		Adm direktør/stabssjef
1		FFIE
1		FFISYS
1		FFIBM
1		FFIN
3		Restopplag til Bibliotek
		ELEKTRONISK FORDELING:
		Vidar S Andersen (VSA)
		Torleiv Maseng (TMa)
		Terje Wahl (TeW)
		Richard Olsen (ROl)
		Bjørn T Narheim (BTN)
		Torkild Eriksen (ToE)
		Gudrun Høye (GKH)
		Kjell Viken (KOV)
		Dan Weydahl (DJW)
		Knut Eldhuset (KnE)
		Johan H Aas (Jaa)
		Pål Bjerke (PBj)
		Karsten Bråthen (KaB)
		Ole M Mevassvik (OMM)
		Stein Kristoffersen (SKr)
		Nils A Sæthermoen (NAS)
		Svein-Erik Hamran (SEH)
		Jonny Otterlei (JMO)
		Bjørn Olav Knutsen (BOK)
		Tore Nyhamar (TNy)
		Ragnvald H Solstrand (RHS)
		Else Helene Feet (ElF)
		Fredrik Dahl (FAD)
		Bent Erik Bakken (BEB)
		Ole-Erik Hedenstad (OEH)
		Hans Christian Gran (HCG)

FFI-K1 Retningslinjer for fordeling og forsendelse er gitt i Oraklet, Bind I, Bestemmelser om publikasjoner for Forsvarets forskningsinstitutt, pkt 2 og 5. Benytt ny side om nødvendig.

EKSTERN FORDELING

ANTALL	EKS NR	TIL
1		FLO/IKT
2		FMGT
3		UD
1		v/ Odd Inge Kvalheim
		Forsvarets skolesenter FSS
1		v/ FHS
1		v/ FSTS

INTERN FORDELING

ANTALL	EKS NR	TIL
		Stein Grinaker (SGr)
		Per Espen Hagen (PEH)
		Nils Størkersen (NJS)
		Halvor Ajer (Haj)
		Stig Lødøen (SEL)
		Robert Macdonald (RHM)
		John-Mikal Størdal (JMS)
		Stein Malerud (SMa)
		Halvor Bjordal (HBj)
		Rune Lausund (RLa)
		FFI-veven