FOI-R--1037--SE
December 2003
ISSN 1650-1942
Underlagsrapport

Christian Carling, Rickard Enander, Jörgen Lindström, Ulf Palmqvist, Johan Tofte

FoRMA 2003: Nätverksstrukturer

Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--1037--SE
December 2003
ISSN 1650-1942
Underlagsrapport

Christian Carling, Rickard Enander, Jörgen Lindström, Ulf Palmqvist, Johan Tofte

FoRMA 2003: Nätverksstrukturer

Totalförsvarets Forskningsinstitut - FOI
Försvarsanalys
172 90 Stockholm

Rapportnummer, ISRN
FOI-R--1037--SE

Klassificering
Underlagsrapport

Forskningsområde
2. Operationsanalys, modellering och simulering

Månad, år
December 2003

Projektnummer
E1850

Verksamhetsgren
5. Uppdragsfinansierad verksamhet

Delområde
22. Metod- och utredningsstöd

Författare/redaktör
Christian Carling
Rickard Enander
Jörgen Lindström
Ulf Palmqvist
Johan Tofte

Projektledare
Olof Söderqvist

Godkänd av
E. Anders Eriksson

Uppdragsgivare/kundbeteckning
Försvarsmakten

Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel
FoRMA 2003: Nätverksstrukturer

Sammanfattning (högst 200 ord)
Nätverksgruppen inom FoRMA har under 2003 arbetat med att stödja perspektivplaneringen med underlag inför FB 2004. Uppgiften har varit att utveckla och värdera alternativa nätverksstrukturer kopplade till olika försvarsmaktsinriktningar. Tyngdpunkten i arbetet har legat på att beskriva och grovt kostnadsuppskatta de nödvändiga delarna i en försvarsmaktsgemensam nätverksstruktur. Arbetet har bedrivits både internt och genom direktmedverkan vid särskilda PerP-arbetsveckor. Gruppen har även deltagit i delar av den genomförda spelverksamheten och genom efteranalyser till PerP-spelen undersökt hur olika situationer i spelen ställer krav på nätverket. Kompletterande underlag i särskilda frågor har tagits fram genom uppdrag till industrier och konsulter.

Nyckelord
FoRMA, Nätverk, PerP, Nätverksbaserat försvar, NBF, kostnadsuppskattning

Övriga bibliografiska uppgifter

Språk Svenska

ISSN 1650-1942

Antal sidor: 48 s.

Distribution enligt missiv

Pris: Enligt prislista

Issuing organization FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	**Report number, ISRN** FOI-R--1037--SE	**Report type** Base data report
	Programme Areas 2. Operational Research, Modelling & Simulation	
	Month year December 2003	**Project no.** E1850
	General Research Areas 5. Commissioned Research	
	Subcategories 22 Operational Analysis and Support	
Author/s (editor/s) Christian Carling Rickard Enander Jörgen Lindström Ulf Palmqvist Johan Tofte	**Project manager** Olof Söderqvist	
	Approved by E. Anders Eriksson	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible	
Report title (In translation) FoRMA 2003: Network Structures		

Abstract (not more than 200 words)

The network group within FoRMA has during 2003 supported the long-term planning process within the Swedish Armed Forces Headquarters, providing analysis in support of the parliamentary defence decision 2004. The group was tasked with developing and providing coarse cost estimates of alternative network structures, coupled to different force structures. The main emphasis has been on the network components necessary to ensure a joint networking capability.

Keywords	
Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 48 p.
	Price acc. to pricelist

INNEHÅLLSFÖRTECKNING

1 Sammanfattning

Nätverksgruppen inom FoRMA har under 2003 arbetat med att stödja perspektivplaneringen med underlag inför FB 2004. Uppgiften har varit att utveckla och värdera alternativa nätverksstrukturer kopplade till olika försvarsmaktsinriktningar. Tyngdpunkten i arbetet har legat på att beskriva och grovt kostnadsuppskatta de nödvändiga delarna i en försvarsmakts-gemensam nätverksstruktur. Arbetet har bedrivits både internt och genom direktmedverkan vid särskilda PerP-arbetsveckor. Gruppen har även deltagit i delar av den genomförda spelverksamheten och genom efteranalyser till PerP-spelen undersökt hur olika situationer i spelen ställer krav på nätverket. Kompletterande underlag i särskilda frågor har tagits fram genom uppdrag till industrier och konsulter.

2 Inledning

2.1 Bakgrund

Frågan om utformning av nätverk inom det framtida försvaret har funnits med ända sedan starten av FoRMA-projektet. Redan DBA-studien[1] som SAIC genomförde åt Försvarsmakten 1998 innehåll kostnadsposter för nätverk och datafusion. Fokus i denna studie låg dock på sensorstrukturen. Även de första årens arbete inom FoRMA fokuserades, naturligt nog, på enskilda tekniska system, såsom sensorer och vapen, och inte på nätverket som skall knyta samman dem. Först under 2001 bildades en särskild grupp inom FoRMA, som arbetade med nätverksstrid. Gruppens uppgift var att ta fram metoder för att beskriva och värdera väpnad strid när den bedrivs med och utan stöd av ett nätverk. I huvudsak studerade gruppen *sensor-to-shooter*-kedjan, det vill säga den del av nätverket som tar hand om sensordata och förmedlar den till ett vapensystem. Inom ramen för den kedjan tog gruppen också hänsyn till ledningsfunktionen och vapenoperatören. Arbetet under 2001 finns avrapporterat i två rapporter.[2]
Under 2002 utökades uppgiften för arbetsgruppen till att ha en helhetssyn på det nätverksbaserade försvaret (NBF) med avseende på ledning, doktriner (det vill säga metoder), organisation, personal och system. Gruppen fick också i uppgift att ta fram alternativa nätverksstrukturer och värdera dessa på tre ekonomiska nivåer: 1, 2 och 3 miljarder kr per år mellan 2004 och 2020. Detta arbete finns beskrivet i förra årets rapport från nätverksgruppen.[3]

Om arbetet med nätverksfrågan de första åren hade en dragning åt funktionskedjor av typen *sensor-to-shooter*, så kan det sägas att arbetet under 2003 varit ”ledningsfokuserat”. Detta är en naturlig pendling mellan olika ytterlägen, men återspeglar även arbetsgruppens sammansättning.

2.2 Uppgift

Uppgiften för nätverksgruppen inom FORMA har under 2003 i huvudsak varit att stödja perspektivplanprocessen (PerP) genom att utveckla och värdera olika nätverksalternativ med tillhörande komponenter, kopplat till olika FM-inriktningar. Två olika angreppssätt har

[1] DBA: Dominant Battlespace Awareness.
[2] FOI-R—0338--SE, 2002, *Värdering av nätverksorienterad krigföring – förstudie*, samt FOI-R--0671—SE, 2003, *Metoder för värdering av nätverksbaserad strid – Underlagsrapport i FoRMA.*
[3] FOI-R--0943—SE, 2003, *FoRMA Nätverk- Sammanfattning av arbetet 2002*

använts, dels helhetsperspektivet, dels förbands- och systemperspektivet, för att belysa olika typer av krav/behov på nätverket.
Under 2003 har tre huvudaktiviteter genomförts inom Nätverksgruppen:

- Utveckling av nätverksstrukturer kopplade till målbildsalternativen
- Systemnära nätverksanalyser för att belysa krav på nätverk på taktisk nivå
- Underlagsframtagning genom uppdrag till industri

2.3 Avgränsningar

Det är inte trivialt att avgränsa vad som skall innefattas inom begreppet nätverksstruktur. Till en viss del avses vidmakthållande och vidareutveckling av befintlig infrastruktur, till exempel delar av Försvarets Telenät (FTN). Till en viss del innefattar den system som Försvarsmakten (FM) sannolikt hade anskaffat oavsett utvecklingen mot ett nätverksbaserat försvar. Därutöver ligger specifika satsningar på gemensam infrastruktur motiverat av utvecklingen av NBF.

Inom Försvarsmakten finns redan idag många olika system som är sammankopplade i nätverk. Dessa är alla designade för att lösa avgränsade uppgifter och möjligheten att utbyta information med andra system är högst begränsad. Vi har valt att fokusera på att beskriva vad som krävs för att realisera ett *försvarsmaktsgemensamt* nätverk, i hög grad baserat på öppna standarder och kommersiellt tillgängliga system. Utgångspunkten för denna fokusering står att finna i den särskilda redovisning som Försvarsmakten lämnade till Regeringen den 1 mars 2003:

> ”För att uppnå nationell och internationell interoperabilitet ställer anskaffningsstrategin krav på bland annat följande:
>
> - Öppen arkitektur, innebärande publicerade, tillgängliga och ej företagsägda metoder, datastrukturer, gränssnitt mm för hur arkitekturen är utformad och hur komponenter interagerar med varandra.
> - Tekniska lösningar inom ramen för öppna arkitekturer skall prioriteras. Vid teknikval skall följande grundprioritering tillämpas
>
> | | |
> |---|---|
> | Prio 1 | Civila lösningar och civil teknik |
> | Prio 2 | Anpassade civila lösningar och civil teknik |
> | Prio 3 | Försvarsunika lösningar” |

Även om vi fullt ut delar synsättet att tillgänglig civil teknik skall utnyttjas i första hand, så ställer användningen av sådana system i militär verksamhet ofta krav som inte kan tillgodoses direkt av den civila tekniken. Vi har alltså sett det som vår främsta uppgift att försöka uppskatta omfattningen av de anpassningar som måste göras för att ”fylla igen gapen” mellan civila produkter och de militära särkraven. Samtidigt tror vi att vissa uppgifter, framförallt inom bekämpningsfunktionerna, ställer så höga krav relativt prestanda i kommersiella systemlösningar, att de även i framtiden kommer att kräva unika lösningar.[4]

Konsekvensen av detta är att vi ser framför oss en försvarsmakt som kommer att innehålla en bred flora av heterogena system, och system som är sammankopplade i dedicerade nätverk. Vi vill fokusera på hur man kan åstadkomma väsentligt förbättrad samverkan, genom att beskriva en struktur som inte ersätter alla existerande system och nätverk, men länkar samman alla dessa i ett försvarsmaktsgemensamt nätverk och i förlängningen ger bättre

[4] Försvarsunika får dock inte tolkas som försvarsmaktsunika, i snäv svensk avgränsning.

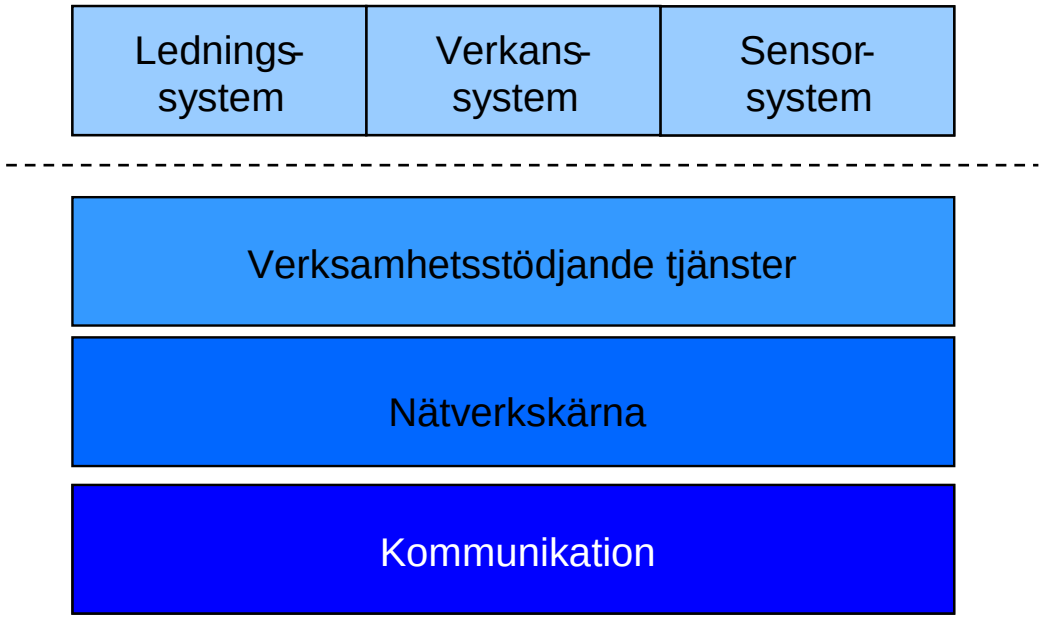
förutsättningar att införa nya system som redan i utvecklingsfasen utnyttjar detta gemensamma nätverk.

Den stora bredden i vårt uppdrag innebär att vi har rört oss över områden som överlappar med eller gränsar mot ett flertal andra aktiviteter. Främst gäller detta LedSyst- och speciellt Demo-verksamheten. Det är då viktigt att hålla isär de olika rollerna. Skillnaden ligger framförallt i tidsperspektiv. Syftet med vårt arbete är att stödja PerP i framtagningen av underlag för försvarsbeslutet 2004, främst genom att beskriva nätverkssatsningar som en integrerad del av olika försvarsmaktsstrukturer i målbildsperspektivet (2014). Vi har bemödat oss om att hela tiden orientera oss om vad som sker i angränsande verksamheter. Samordningen underlättas genom att personer i nätverksgruppen även deltar direkt i olika LedSyst-aktiviteter.

2.4 Definition av nätverksstruktur

Namnet *nätversstruktur* är valt för att peka på att det vi beskriver utgör en del av de försvars-maktsstrukturer som övervägs inom PerP-arbetet. Detta är alltså styrande både för avgränsningen av och detaljeringsgraden i vårt arbete. Tidigt under våren genomfördes ett internt arbete med begreppsanalys kring nätverk. Syftet var framförallt att skapa en gemensam bild av gruppens ansvarsområde och att avgränsa uppgiften genom att definiera vad vi uppfattar med begreppet ”nätverksstruktur”. Ett resultat av detta arbete är att en komplett beskrivning av en nätverksstruktur även omfattar delar som faller inom andra gruppers ansvarsområden, framförallt de systemarbetsgrupper inom Försvarets materielverk (FMV) som hanterar Kommunikation och Ledningskomponenter. Den tolkning vi gjort innebär att nätverksgruppen

- beskriver en kärna av centrala nätverkstjänster,
- i samverkan med andra grupper beskriver gemensamma verksamhetsstödjande tjänster
- med stöd av andra grupper sammanställer ovanstående med relevanta förbands- och systemspelkort till en komplett nätverksstruktur enligt nedanstående bild.



Nätverksstrukturen definieras i detta arbete som de tre undre skikten i bilden ovan. Den innehåller både fysiska och logiska komponenter. De tre översta boxarna representerar de system som länkas samman av nätverksstrukturen. De ingår alltså enligt denna definition inte

i nätverksstrukturen, men är ytterst det som kravställer alla delarna i strukturen. Bilden ovan skall inte tolkas alltför hårt som en formell arkitekturmodell. Den är helt enkelt ett naturligt sätt att dela vårt ansvarsområde i mindre delar. Gränsdragningen mellan de mellersta skikten och mot det översta skiktet är i praktiken svår att göra knivskarp.

En komplett beskrivning av en nätverksstruktur omfattar som nämnts ovan många delar, varav vissa faller utanför nätverksgruppens egentliga arbetsområde: Den samlade kommunikationsinfrastrukturen sammanställs från befintliga system- och förbandsspelkort och det arbete som görs inom FMV:s systemarbetsgrupp för kommunikation. Den givna sensorstrukturen måste stödjas prestandamässigt av kommunikationsinfrastrukturen och funktionsmässigt av verksamhetstjänster, implementerade i olika ledningssystem. Vissa plattformsspelkort behöver dessutom kompletteras med en beskrivning av vad som krävs för att de skall kunna samverka via nätverket.

Arbetet med att ta fram en avvägd nätverksstruktur kopplad till grundalternativet är alltså i hög grad en sammanställning och värdering av befintligt underlag, med vissa återstående kompletteringar. Andra alternativ kan sedan skapas genom variationer av denna. Vi har i tidigare arbeten pekat på övergripande parametrar som kan användas för dessa variationer: ett exempel är balansen mellan internationell förmåga och försvarsförmåga; ett annat kopplat till detta är art och grad av interoperabilitet; andra kan vara total kostnad eller införandehastighet.

2.5 Läsanvisning

Nästa kapitel redogör kort för de aktiviteter som nätverksgruppen genomfört under 2003. Arbetet med nätverksanalyser redovisas i en separat rapport.[5] Resten av denna rapport är helt ägnad åt arbetet med nätverksstrukturer: Kapitel fyra redogör för det angreppssätt vi valt för att kunna beskriva och kostnadsuppskatta de olika delarna i nätverksstrukturen och diskuterar vad som är styrande för utformningen av de olika delarna.

De följande tre kapitlen redogör sedan för de tre olika nivåerna i nätverksstrukturen: kapitel fem om kommunikationslagret är mer kortfattat än de två följande, vilket återspeglar en medveten prioritering i arbetet: flera aktörer arbetar inom detta område och vi har i princip bara sammanställt underlag som tagits fram av andra. Beskrivningen av nätverkskärnan i kapitel sex och av gemensamma verksamhetstjänster i kapitel 7 är mer omfattande och representerar huvuddelen av vårt eget arbete.

Kostnadsuppskattning av nätverksstrukturer behandlas mycket kortfattat i kapitel åtta. Detta är den del av arbetet som har genomförts närmast i dialog med PerP-gruppen och med nära medverkan från FMV och övrig FM-personal. Resultaten har underhand lämnats direkt till PerP och inarbetats i deras ekonomiberäkningar. Av sekretessskäl redovisas i denna rapport inga siffror, utan endast en översiktlig diskussion om metoder för att genomföra kostnadsberäkningar, samt några internationella jämförelseobjekt.

Kapitel nio ger en bakgrund till hur man kan konstruera alternativa nätverksstrukturer anpassade till olika försvarsmaktsinriktningar. Detta är en del av arbetet som inte är genomfört fullt ut i förhållande till ursprunglig plan. Orsaken är delvis att andra delar tagit längre tid än planerat, delvis att vi i slutskedet inte fått förnyat underlag som beskriver de alternativa försvarsmaktsinriktningar som kan kopplas till de olika ekonomiska nivåer som övervägts inom PerP-arbetet.

[5] FOI-R—1038—SE, December 2003, FoRMA 2003 Nätverksanalyser

Kapitel tio, som är något fristående i förhållande till övriga, presenterar några principiella utgångspunkter för framtida systemutveckling, som skiljer sig från etablerad praxis på många punkter. Detta kapitel har framförallt utarbetats av FMVs deltagare.

Rapporttexten avslutas med kapitel 11 som sammanfattar slutsatser av det genomförda arbetet, identifierar uppgifter som enligt vår mening kräver fortsatt arbete, samt möjliga nya uppgifter.

3 Genomförande

3.1 Gruppens sammansättning

Under året har ett relativt stort antal personer varit aktiva i nätverksgruppens arbete. Från FOI Försvarsanalys har följande personer medverkat: Eva Andersson, Rickard Enander, Thomas Ekström, Martin Hamrin, Mats Lindberg, Jörgen Lindström, Karin Mossberg samt Patrik Thoren. Rickard Enander och Jörgen Lindström har haft ett särskilt ansvar för beskrivningen av nätverkskärnan respektive verksamhetsstödjande tjänster. Patrik Thoren och Mats Lindberg har ansvarat för att sammanställa arbetet med systemnära nätverksanalyser. Johan Tofte, avdelningen för Ledningssystem, har haft en dubbel roll som ansvarig för kontakter med övriga avdelningar samt för kommunikationsdelarna i strukturarbetet. Ledare för gruppens arbete har varit Christian Carling.

Göran Skogsberg från FMV har tillsammans med Ulf Palmqvist haft en stor roll i arbetet med strukturbeskrivningen, och framförallt i arbetet med kostnadsuppskattningar. Göran Skogsberg har även haft ett särskilt ansvar för industribeställningarna.

Gruppen har även fått stöd av FoRMAs PerP-ekonomigrupp, i diskussionerna kring metoder för kostnadsuppskattningar och den kalkylmodell (EBV) som används av PerP för strukturberäkningar.

3.2 FoRMA-gemensamma aktiviteter

Arbetet i nätverksgruppen under våren dominerades av informationsinsatser och uppstart av nya uppdrag och arbetsområden. Utgångspunkten var projektledningens avsikt att nätverks-frågorna under 2003 skulle vara en viktig uppgift för FoRMA som helhet.

För att skapa en gemensam grund för detta arbete arrangerade nätverksgruppen i mars en särskild nätverksdag. Syftet med dagen var att alla verksamma inom FoRMA skulle få en gemensam förståelse för vad nätverket kan innebära i den framtida Försvarsmakten. Dagen skulle även tjäna som en start för ett samarbete mellan spelgrupperna och nätverksgruppen med fokus på de uppgifter som skulle lösas inom FoRMA under året 2003. Nätverksdagen genomfördes i form av ett antal presentationer med interna och externa föreläsare och avslutades med en diskussion, som också blev inledningen på det gemensamma arbetet med nätverksfrågor inom FoRMA.

3.3 Nätverksstrukturer

Inför vårens spelomgångar genomförde gruppen i samverkan med FMV:s Systemarbetsgrupp för ledningskomponenter ett arbete för att identifiera och mycket grovt uppskatta de dominerande kostnadsposter som kan knytas till utveckling och vidmakthållande av en försvarsmaktsgemensam informationsinfrastruktur. Detta har sammanfattats och lämnats underhand i form av spelkort (”skivor”) till PerP-gruppen.

Inom ramen för nätverksgruppens direktstöd till PerP:s fördjupningsområde NBF genomfördes i maj en föredragning för Försvarsmaktens direktion.

Denna del av arbetet har kontinuerligt bedrivits internt inom gruppen, genom direkt medverkan i de gemensamma PerP-arbetsveckorna under året och vid särskilda möten med företrädare för PerP och andra delar ur HKV.

3.4 Nätverksanalyser

I flera tidigare studier inom FoRMA har fokus naturligt nog legat på enskilda tekniska system, såsom sensorer och vapen, och inte på nätverket som skall knyta samman dem. I vissa fall har man explicit antagit att detta nätverk har obegränsad kapacitet och tillgänglighet. Ännu vanligare har varit att man inte alls berört vilka krav de enskilda systemen ställer på nätverket. Detta är en naturlig arbetsgång, men förr eller senare måste givetvis kraven på nätverket preciseras. För att komma åt dessa krav har vi under året bedrivit vad vi kallar systemnära nätverksanalyser, med syfte att i dialog med FoRMA:s övriga grupper skapa en bättre bild av vilka krav olika funktioner ställer på det gemensamma nätverket. Denna del av arbetet redovisas i en separat rapport[6]

3.5 Industristöd

Under 2000 och 2001 deltog ett flertal industriföretag direkt och indirekt i arbetet, framförallt genom att genomföra underlagsstudier. Denna medverkan fortsatte in i 2002 men under senare delen av 2002 deltog inga industrikonsulter i arbetet. Arbetet med att utforma nya uppdrag till industrin och att sätta in dem i det nuvarande arbetsläget har varit mer omfattande än beräknat. Samtidigt har industrimedverkan breddats, genom att två nya uppdrag lagts utanför gruppen av försvarsindustriföretag som tidigare varit inblandade i arbetet. På grund av den utdragna upphandlingsprocessen och återkommande osäkerheter om tillgänglig ekonomisk ram för genomförande, kommer uppdragen att slutredovisas till FoRMA först efter denna rapports färdigställande. Här ges en kort översikt över de uppdrag som lagts ut:

3.5.1 AerotechTelub

För att fördjupa beskrivningen av vad som kan vara exempel på gemensamma, verksamhetsstödjande tjänster har ett mindre tilläggsuppdrag lagts på AerotechTelub. Uppdraget genomförs av samma personal som medverkar i det större uppdraget från FMV:s Systemarbetsgrupper för ledningskomponenter och ledningsplatser. Syftet med detta uppdrag är att ytterligare belysa vilka verksamhetstjänster som är mest fundamentala enligt kriterierna:

- Används av många
- Bidrar till att möta grundläggande militära behov
- Utgör förutsättning för realisering av andra användartjänster

Syftet är att kunna identifiera vad som bör göras först, vad som kan vara kostnadsdrivande och vilka krav dessa grundläggande tjänster ställer på de underliggande delarna av nätverksstrukturen. Uppdraget genomförs under december till januari och redovisas i februari 2004.

3.5.2 Cap Gemini Ernst & Young

En återkommande erfarenhet från organisationer med stort beroende av informationssystem är att drift- och vidmakthållandekostnader ofta underskattas i den långsiktiga planeringen. När det som i vårt fall är frågan om att bedöma kostnaderna för framtida system som bygger på kontinuerlig vidareutveckling och införande av nya funktioner, i växlande konfigurationer, blir problemet komplext. Den organisation som krävs för att leda en sådan utveckling ser

[6] FOI-R—1038—SE, December 2003, FoRMA 2003 Nätverksanalyser

förmodligen helt annorlunda ut än den nuvarande. Situationen liknar dock i grova drag den som större internationella koncerner befinner sig i. Företagsköp och sammanslagningar skapar en mycket heterogen och snabbt föränderlig IT-miljö, samtidigt som konkurrensen kräver att samverkansfördelar hela tiden uppnås över hela verksamheten. För att öka förståelsen för denna organisatoriska dimension har Cap Gemini Ernst & Young fått i uppdrag att beskriva denna problematik. I en första fas gjordes en snabb översikt över vilka faktorer som styr utformningen av, och indirekt kostnaderna för, en sådan organisation. På grund av försenad och minskad finansiering har vi inte kunnat gå vidare med den avsedda fortsättningen i full omfattning, utan genomför i fas två en mindre case-study av NCW-utvecklingen inom den nederländska försvarsmakten, utifrån detta perspektiv. Uppdraget redovisas i januari 2004.

3.5.3 Ericsson Microwave Systems (EMW)

Flera av de underlagsstudier som genomförts under tidigare år beskriver hur olika situationer på stridsteknisk nivå kan beskrivas i termer av funktionskedjor och värderar kraven på de ingående systemen. Exempel på tillämpningssituationer har varit bekämpning av kryssningsmissiler och upprättande av konnektivitet i ett operationsområde. Nästa naturliga steg är att på högre systemnivåer undersöka komplexare situationer, med fler ingående förband och system. EMW genomför på vårt uppdrag en scenariobaserad system-av-system-studie för att värdera hur den föreslagna nätverksstrukturen kan hantera ett flertal samtidiga, temporära funktionskedjor i en dynamisk miljö, med många ingående delsystem.

3.5.4 SaabTech Systems

Även om man inom NBF-utvecklingen knyter stora förhoppningar till att i framtiden kunna ersätta gamla, slutna system med nya flexibla lösningar, byggda på öppna standarder, kommer den framtida försvarsmakten i varje skede att innehålla en stor mängd system som utgör ”arv” från tidigare teknologigenerationer. SaabTech Systems genomför därför en inledande studie för att belysa hur befintliga ledningssystem i relativ närtid kan integreras i ett försvarsmakts-gemensamt nätverk, byggt på den gemensamma nätverksstruktur vi beskrivit.

3.5.5 Swedish Institute of Computer Science (SICS)

Ett fruktbart sätt att se på informationsnätverken i den framtida Försvarsmakten är som ett distribuerat informationssystem, med stor dynamik och ständigt växlande struktur. Swedish Institute of Computer Science (SICS) har från FoRMA:s nätverksgrupp fått i uppdrag att i en rapport beskriva kunskapsläget inom forskningsområdet distribuerade system, främst med inriktning mot helt decentraliserade arkitekturer (*Peer-to-Peer-system*). Arbetet kommer att redovisas i mars 2004.

3.6 Övrigt

Medlemmar i gruppen har vid två tillfällen tillsammans med representanter från Högkvarteret (HKV), FMV, Försvarshögskolan (FHS) deltagit i tvådagars arbetsmöten med DSTL, Storbritannien, om utvecklingen av NBF respektive NEC-konceptet. Arbetet har under året även föredragits för representanter från DSO (Singapore), CAD (Frankrike), RAND (USA/Europe) samt vid ett kontaktmöte med FFI i Norge.

Under förra hösten lades ett uppdrag på RAND, som syftade till att ta fram ett ramverk för att beräkna kostnader för nätverkssatsningar, kopplade till olika uppgifter. Uppdraget är genomfört och arbetet är kvalitetsmässigt granskat och godkänt. Resultatet har föredragits för FOI och dokumentation överlämnats. Rapporten (Perry et al, 2003) kommer att publiceras av RAND och kommer i början av 2004 att finnas tillgänglig via RAND:s hemsida.

4 Nätverksstrukturer

För att närma oss en struktur (eller modell) av nätverket som vi kan fortsätta diskutera kring finns det ett antal steg vi måste genomlöpa. Dessa steg är a) kravbilden på NBF, b) avgränsningar som vi gör och c) vissa antaganden. Vi kommer att genomlöpa dessa steg i detta kapitel för att till slut komma fram till en modell av nätverket som används för den fortsatta diskussionen.

4.1 Kravbilden på NBF

Kravdrivande på den nätverksstruktur vi söker är ytterst vad som förväntas av NBF. Alla som har varit involverade i diskussioner och arbetsgrupper vet att förväntningarna på NBF dels är höga och dels är ganska olika. Ibland förekommer redan gjorda ”taktiska inteckningar” på NBF och nätet av typen ”den informationen får jag från nätet”. Det är därför viktigt att ett arbete som detta tidigt klargör (så långt som det är möjligt idag) vilka källor vi anser vara kravdrivande:

- NBF-konceptet som det framställs till exempel i presentationer från Försvarsmakten
- De dokument som styr LedSyst verksamhet mot FMLS2010
- Spel och scenarier i olika former
- Civil teknikutveckling och trender
- Andra källor, till exempel FMA

Dessa kravkällor diskuteras i mer detalj längre ner. Det skall dock tydligt påpekas att kravbilden på NBF, och därmed på nätverksstrukturer för att stödja konceptet, idag är otydlig. Detta är i sig inget fel; NBF är i ett konceptstadium och dessutom under snabb utveckling i Sverige såväl som på andra håll. I ett sådant skede kan kraven inte vara väldigt tydliga, det skulle bara motverka kreativiteten i utvecklingen. Dock blir precisionen i föreslagna nätverksstrukturer och teknikförslag av naturliga skäl lägre. Precisionen i kostnadsuppskattningar blir naturligtvis också låg.

4.1.1 NBF-konceptet

Om vi börjar med konceptet NBF som sådant så är den grundläggande idén att kunna formera situationsanpassade styrkor för olika insatser[7]. Tekniskt sett så innebär detta att olika förband och system skall kunna utbyta information (tjänster[8]) med varandra. Nätet skall möjliggöra kommunikation mellan noder i nätet oberoende av organisatoriskt tillhörighet. Nätet skall ur en brukares synpunkt vara sömlöst, brukaren skall inte se eventuella tekniska skarvar i nätet. Några kommentarer:

- Nätet skall/kan ses som ett **nät av nät**. Det finns flera skäl till detta bland annat att vissa teknikövergångar inte i sig är sömlösa och att åtkomsten av en viss nod i vissa fall är begränsad utanför det egna nätet. Detta innebär att ”det totala nätet” inte nödvändigtvis är identiskt för alla noder utan beror av om man befinner sig innanför eller utanför ett visst subnät.

[7] Redan här gör vi en avgränsning genom att betrakta insatser och inte “normal verksamhet”. Skälet är att vi tror att insatser är en mer krävande situation.
[8] Med begreppet tjänst menar vi här förmågan att kunna kommunicera information med varandra, inte själva effekten av en given order.

- Ordet **situationsanpassat** ska också tolkas i ganska vid bemärkelse. Den omedelbara tolkningen är att man ”konfigurerar upp” en insatsstyrka. Dessutom – på en kortare tidsskala – kommer noder att utgå och tillkomma i snabb takt.
- **Konfigureringen** i sin tur bör vara så enkel som möjlig. För det mesta ska den vara automatisk (en sensor faller ur). I andra fall styrs den av doktrin och reglemente (lydnadsförhållande). Sådana fall är troligen förberedda i de applikationer som ingår i nätet. Ytterligare andra fall kan kräva manuell konfiguration.

Vidare så kommer de ingående noderna/systemen i nätet att vara av olika typer:

- Arvssystem (det vill säga system som fanns inom Försvarsmakten innan NBF) som inte i sig är NBF-fäiga
- Nybyggda system som vi bygger som vi vill.
- Nya inköpta system som inte följer våra riktlinjer. Dessa kan i vissa avseenden likställas med ärvda system.

Nätet i NBF framställs på olika sätt av olika aktörer:

- **Källan för information**
  Nätet beskrivs ofta som källan till den information (i vid bemärkelse) som en befattningshavare behöver. Detta synsätt kan liknas med det amerikanska *Global Information Grid* (GIG). Synsättet liknar mycket Internet som det används av privatpersoner idag.
- **Källan för resurser**
  Ett något annorlunda sätt att se på nätet är som hemvisten för olika resurser, typiskt ledningsresurser. En användare tänks kombinera ihop olika tjänster till en fungerande enhet. Var dessa tjänster är lokaliserade är oftast oväsentligt för användaren.
- **Förutsättning för integration**
  Ett kanske mer handgripligt sätt att se på nätet är som medlet för att integrera system och noder. Värdet ligger mer i noderna och deras samverkan än i nätet i sig. Integrationsproblematiken är i sig ett klassiskt problem.

Inget enskilt sätt att beskriva nätet kan göra anspråk på att vara sanningen, istället kompletterar de olika beskrivningssätten varandra. Att se nätet som en resurspool är kanske det mest avancerade synsättet men förutsätter i sig en förmåga att kunna integrera.
Vi har valt att lägga mer fokus på integration än på de två övriga aspekterna.

4.1.2 FMLS 2010

Den källa som idag har den tydligaste kravbilden är planen för LedSyst-utvecklingen mot FMLS 2010. Många av dessa krav och målsättningar hamnar utanför de nätverksstrukturer som vi diskuterar här[9]. Det finns dock en hel del tydliga krav på nätverket, exempelvis:

- Öppen lösning
- Enkelt att ansluta och konfigurera objekt/system
- Kommersiella standarder
- Oberoende av transmissionsteknologi
- Åtkomst oberoende av organisationstillhörighet

[9] Exempel på detta är antagandet att man utifrån gemensam information kan uppnå en gemensam lägesförståelse. Detta antagande berör mer doktrin och metodutveckling än själva nätet.

- Driftsäkerhet i olika former
- Stödja distribuerat arbetssätt
- Teknisk interoperabilitet
- Medge simulering
- Säkerhet
- Rollbaserad åtkomst

Ovanstående krav är inte alltför ovanliga. Intressantare är den funktionalitet som LedSyst avser att demonstrera vid olika tidpunkter:

- Att skapa gemensam lägesinformation[10] genom att samla in data från sensorer, egna förband och andra källor.
- Att rollbaserat kunna distribuera denna gemensamma lägesbild till alla som vill ha den (och är behöriga).
- Att ledningsmässigt kunna arbeta parallellt och distribuerat.
- Att baserat på den information som finns kunna verka effektivt och med rätt insats.

4.1.3 Spel och Scenarier

Scenarier[11] är en teknik som används för att generera krav när IT-lösningar skall utformas. Scenarier och spel är också ett traditionellt sätt att kravsätta militära enheter kvalitativt och kvantitativt. De spelaktiviteter som har förekommit i PerP:s regi och som FoRMA-nät har deltagit i, är en källa till vår kravuppfattning. Genom analyser av dessa spel har vi hittat en mängd olika krav och mönster som:

- Kvantitativa mått som intensitet i kommunikation i olika faser av en operation.
- Mönster på vilka enheter som har behov att kommunicera med varandra i olika skeden.
- Krav och förslag på tjänster.

Dock skall det sägas att dessa spel inte har haft som syfte att belysa nätverksmässiga aspekter. Som komplement har gruppen använt sig av andra ”artificiella” scenarier mer avsedda för att fånga nätverksfrågor. Exempel på sådana är:

Etablera insatsstyrka	Belysa situationen då nod efter nod slås på utan att central information finns tillhands.
Övervaka och bekämpa	Belysa situationen då en insatsledare behöver veta vilka noder som finns, vilka som tillkommer och vilka som försvinner.
Den gotländske fiskaren	Belysa problematiken med att använda källor utanför den egna organisationen.
Plutonen som bytte sida	Belysa situationen då det egna nätet används i fientligt syfte.
Återgruppering av stab	Belysa situationen då man ska återuppbygga en

[10] Notera att gemensam lägesinformation inte är målet i sig utan ett medel för att nå en gemensam lägesuppfattning som i sin tur är en förutsättning för självsynkronisering. Tekniskt sett är skapandet och distribueringen av gemensam lägesinformation dock central.
[11] Tekniken går under olika namn som *use cases* eller *user stories*. Oavsett benämning är avsikten att beskriva konkreta situationer i vilket systemet är tänkt att användas och utifrån detta hitta krav.

	infrastruktur och återta ”befälet”.
Skogsbranden	Belysa en situation med interoperabilitet med civila myndigheter.

4.1.4 Civil teknikutveckling

Att ta till vara civil teknik och utveckling är ett explicit krav som satts upp av statsmakterna. Aven frånsett det formella så ser vi det som omöjligt att inte ta starkt intryck av vad som händer på den civila marknaden inom många olika områden. Det finns många olika tekniker och standarder som kan nämnas. Dock vill vi speciellt nämna den allmänna utvecklingen mot att integrera fler och fler system med varandra, både inom och mellan företag och myndigheter. Ett ganska grundläggande antagande är att NBF-konceptet har många likheter med de integrationssträvanden man kan finna på många civila håll.

De kommersiellt tillgängliga tekniker och produkter som idag finns representerar dels tiotals år av erfarenhet och dels enorma investeringar i produkter. Att inte ta hänsyn till vad som faktiskt görs och finns skulle göra en diskussion som denna ganska akademisk och sannolikt ge dyrbara konsekvenser.

4.1.5 Andra källor

Det finns ett antal andra källor att nämna i detta sammanhang, exempelvis erfarenheter från LedSystT och kanske framför allt FMA. I skrivande stund är dock FMA:s ställning oklar. Eftersom FMA ändå har fått genomslag nomenklaturmässigt har vi valt att i vissa fall använda oss av begrepp och koncept därifrån. Exempel på detta är:

- **Tjänstebegreppet**
  Vi tror starkt på att tjänster kommer att vara ett mycket centralt begrepp i NBF. Tjänst (eller service) är ett centralt tankesätt när man vill uppnå integrationsmöjligheter mellan system på kort och lång sikt.
- **LOVENTP**
  Vi använder oss flitigt av denna modell för att avgränsa vad vi diskuterar i detta dokument.

4.2 Antaganden

Vårt grundläggande antagande om NBF-konceptet är att frågeställningarna inte är speciellt olika de man kan finna i vissa civila situationer. Ett exempel på en sådan situation är ett större företag som verkar inom en bransch under omstrukturering. Företaget köper andra företag som måste integreras IT-mässigt och på andra sätt. Mer eller mindre heliga affärsallianser uppstår och avslutas i rask takt. Den grundläggande likheten mellan NBF och ett sådant civilt scenario är att ett stort antal heterogena system måste kunna integreras och information kunna bytas fritt mellan olika delar i detta intranät. Vidare kommer nya, idag okända, system att behöva integreras.

Vi tror det finns många viktiga likheter mellan NBF och civila frågeställningar men man ska naturligtvis inte dra alltför förhastade slutsatser. Det finns också stora skillnader som måste tas i beaktande, exempelvis:

- **Typen av applikationer**
  De applikationer som integreras i NBF-konceptet kommer av naturliga skäl inte att vara desamma som i det civila scenariet. Vi tror dock att typen av applikationer i de flesta fall är av mindre betydelse, den avgörande egenskapen som eftersträvas är att kunna utbyta information så flexibelt och säkert som möjligt.
- **Takten och arten av förändring**
  I det civila exemplet ”köper och integrerar” man företag. Förhoppningsvis får man några dagar på sig att integrera de nya systemen. På den militära sidan kan man i vissa situationer förvänta sig mycket snabba förändringar av vad som finns i nätet och vilka tjänster som kan levereras. Enheter kommer att röra sig in och ut i områden och därmed in och ut ur olika nät, sensorer kommer att snabbt behöva kopplas samman med verkansenheter och så vidare.
- **Säkerhet**
  På den militära sidan kommer säkerhetskraven troligen att behöva vara högre än på den civila sidan. Det kommer också att finnas andra militärspecifika lösningar. Vi tror dock att dessa skillnader inte skall överdrivas, många civila verksamheter har också höga krav på säkerhet.
- **Tålighet mot degradering**
  Civilt kan man acceptera att svarstider blir långa eller att man exempelvis inte kan autentisera en användare mitt i natten om en revokeringsserver är nere. Militärt måste man kunna hantera sådan degradering av systemprestanda mer handgripligt. Exempel är att vissa tjänster kan användas trots att normal autentisering inte kan utföras[12]. Ett annat exempel är om bandbredd, CPU-kraft eller annan prestanda inte räcker till så måste man kunna prioritera trafik och resursutnyttjande.

Vi ser dock inte skillnaderna som dramatiska och gör antagandet att om vi idag skulle välja teknologier för NBF skulle en stor del baseras på civila produkter och standarder. Många produkter behöver sannolikt modifieras för att möta militärspecifika krav men vi ser att utvecklingen är snabb och att gapet mellan de militära kraven och och prestanda i civil teknologi kommer att vara än mindre om ett par år. Vidare ser vi att den typ av teknologi som är tillämplig har många andra goda egenskaper inbyggda som skalbarhet, *fail over*[13], redundans med mera. Detta är egenskaper som kommer att vara viktiga då riktiga applikationer skall byggas i NBF. Till dags dato har dessa egenskaper på nodnivå inte fått så stort utrymme i kravdiskussionen, kanske beroende på att de tillämpningar som har diskuterats är ganska enkla.

Den stora brasklappen i antagandet om att civil teknologi är tillämplig är naturligtvis den oklara kravbilden enligt tidigare.

4.3 Avgränsningar

Den största avgränsningen vi gjort är att vi koncentrerar oss till vad vi kallar nätverksstrukturen och i viss mån på ledningstjänster. Övriga verksamhetstjänster (Omvärld, Verkan och E-bryggor i FMA-termer) har vi inte explicit betraktat annat än i vissa scenarier. Vidare har vi gjort vissa avgränsningar (eller antaganden) kring hur vi tror att NBF kommer att användas initialt. Exempel på detta är:

[12] Någon får helt enkelt ta risken baserat på annan information man har tillgänglig. Detta är både en teknisk och doktrinmässig fråga.
[13] *Fail over* innebär att funktionalitet automatiskt kan flyttas över till en annan dator om en dator skulle fallera.

- Många existerande system, exempelvis ledningssystem, kommer att ”livstidsförlängas” och integreras in i ett NBF-sammanhang som arv. Vi tror inte på en massiv initial utveckling av nya ledningskomponenter som kan komponeras ihop fritt.
- Majoriteten av tillämpningarna kommer att bestå av förberedda informationskedjor och inte i att nätet automatiskt kopplar samman lämpliga delar för en uppkommen situation.
- Nätet i sig kommer inledningsvis inte att ha mycket egen intelligens av typen ”tjänstebroker”, replikerad datalagring, semantiska sökningar etc. Istället kommer den mesta upplevda intelligensen att ligga i specifika noder.

Vi vill inte med dessa avgränsningar säga att användningen för all framtid kommer att vara begränsad på det sätt som beskrivs. Vi tror dock mer på en trend där man går från att integrera existerande system genom att kapsla in dem till att senare gradvis växa in i bilden med distribuerade generella och ihopkopplingsbara komponenter.

Vidare kan man nog inte räkna med att ”nätet” kommer att lösa alla kommunikationsbehov inom försvaret. Vissa tillämpningar kan ha så höga realtidskrav att hårt kopplade lösningar blir nödvändiga; exempel kan vara närförsvar av ett ytstridsfartyg eller taktisk kommunikation mellan JAS-plan. Gränsen mellan vad NBF-nätet kan klara av och var speciallösningar behövs är inte helt klar. Gränsen kommer också att flyttas dels beroende på teknikutvecklingen och dels beroende på nya krav. Den viktiga poängen är att inse såväl vinsterna som begränsningarna med ”nätet”.

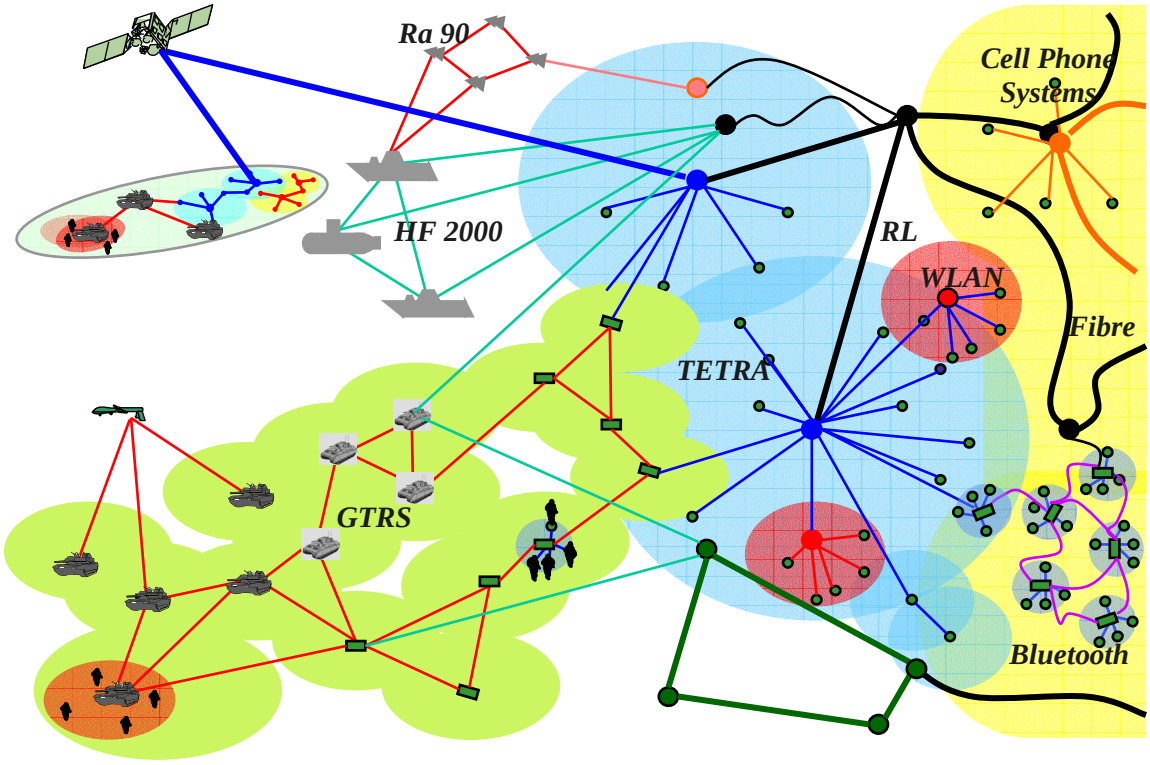
5 Kommunikationslagret

I detta kapitel beskrivs förutsättningarna och möjligheterna till realisering för det vi kallar kommunikationslagret. Notera att FoRMA under innevarande år inte bedrivit egna studier inom kommunikationsområdet. Därför bygger texten nedan mycket på tidigare arbete och andra källor.[14]

5.1 Försvarets framtida kommunikationsnät

Ett nätverksbaserat insatsförsvar ställer ökade krav på informationsutbyte vilket innebär stora utmaningar för kommunikationssystemen. Flera av dessa krav omfattar funktionalitet och prestanda såsom kapacitet, konnektivitet, säkerhet, gemensamma standardiserade protokoll, smygförmåga och mobilitet. Vissa krav står i motsatsförhållande till varandra och då måste avvägningar göras. Förmåga måste finnas till att anpassa funktion efter rådande förutsättningar. Dessutom skall framtidens militära kommunikationssystem vara interoperabla både med system från andra länder Sverige vill kunna samverka med och med civila system. För att hålla nere kostnader utnyttjas civilt utvecklad kommersiell teknik i största möjliga utsträckning. Utveckling och anskaffning av kommunikationsnät och delsystem sker evolutionärt vilket innebär att komponenter kan uppgraderas och bytas ut.

Kommunikationsnäten är en förutsättning för de generella nätverkstjänster som vi beskriver längre fram. Vi behöver ett kommunikationsnät som hanterar gemensamma protokoll för överföring, antingen direkt eller via *gateways*. Nätet byggs upp som ett sammanhängande nät av nät med olika system som är anpassade för behoven hos respektive nod. Mobila enheter utnyttjar trådlösa system och även i framtiden kommer radioteknik att vara det dominerande alternativet. För vissa tillämpningar kan det vara tillräckligt med enkla, billiga kommersiella system men i många fall krävs militärspecifika lösningar.



[14] Bland annat FMV:s rapport ”Försvarets Framtida Taktiska Kommunikationer” (UO Led 3195:61837/03).

5.2 Fasta kärnnät

Ett fast kärnnät är uppbyggt med fast installerade transmissionssystem, till exempel fiberoptiska kablar eller radiolänk, och fasta noder i fast byggda materielskydd. Användarna erbjuds generellt hög kapacitet och tillförlitlig konnektivitet, men rörligheten inskränks.

Det viktigaste fasta kärnnätet är den fasta delen av Försvarsmaktens Telenät (FTN), som utgör ett nationellt fast kärnnät byggt för Försvarsmaktens ändamål. Det har full geografisk täckning (även glest befolkade områden täcks) med fortifikatoriskt skyddade noder och med säkerställd kraftförsörjning.

Andra fasta kärnnät utgörs av de civila nät som finns, både inom landet och utomlands. Tillgången till dessa nät regleras genom avtal. Kontrollen är dock alltid nätägarens vilket kan vara svårt att hantera. Näten är inte byggda efter militära krav och täckningen är bättre i tättbefolkade områden än i glesbygd.

Standardiserade gränssnitt och protokoll gör det möjligt att utnyttja kommersiellt utvecklade system och applikationer.

5.3 Mjukvarudefinierad radio

Rörliga förband behöver trådlös kommunikation och i princip betyder detta någon form av radiosystem. Trenden för framtida radiosystem är att implementera mer av funktionaliteten i mjukvara. Terminalerna realiseras med en kombination av programvara och hårdvara i enlighet med en vedertagen internationell standard som kallas *Software Communications Architecture* (SCA). I ett mjukvarubaserat radiosystem finns möjligheter både att snabbt anpassa funktion efter rådande omständigheter och till evolutionär och modulär utveckling och anskaffning.

Radiosystemen kommer att finnas i olika utföranden för att passa olika behov. USA leder utvecklingen och där har man inom programmet *Joint Tactical Radio System* (JTRS) delat in terminalerna i fem typer (*cluster*):

- fordonsmonterad
- bärbar
- handhållen
- luftburen
- inbäddad (små enheter)

Radions funktionalitet kallas vågform och en terminal kan, beroende på typ, innehålla en eller flera samtidiga vågformer. Med flera vågformer kan terminalen utgöra *gateway* mellan olika nät via så kallad *crossbanding*. Genom att ta fram vågformer för arvet kan bakåtkompabilitet garanteras så att äldre system kan kommunicera med nya system. En vågform med namnet *Wideband Networking Waveform* (WNW) är under framtagning för att möjliggöra taktisk kommunikation med dynamisk överföringshastighet i mobila ad hoc-nät. Dessutom utvecklas vågformer för att ge störskydd och smygegenskaper.

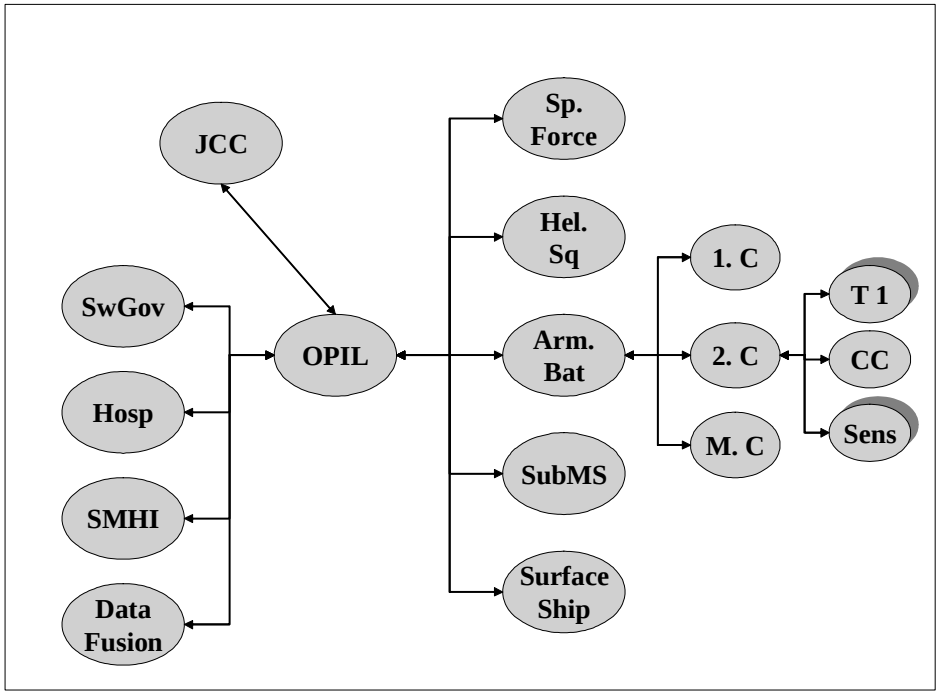
En rad problem återstår dock fortfarande att lösa. Det gäller främst analoga komponenter som filter, förstärkarsteg och framför allt antenner. Men också regelverk avseende frekvensutnyttjande och certifierande av radiosystem måste utvecklas för att kunna ta tillvara på möjligheterna med mjukvarubaserade system.

6 Nätverkskärnan

I detta avsnitt ska vi diskutera nätverkskärnan närmare. Det kommer att framgå att kärnan inte är en entydig ”produkt” som enkelt kan placeras in en lagermodell. De noder som kommer att ingå i NBF är av olika typ och komplexitet beroende på var noden verkar och med vilka den utbyter information. Nätverkskärnan kommer på olika sätt att vara inbäddad i olika produkter och kommer att se lite olika ut. Kärnans uppgift är dock att uppträda på samma sätt utåt oberoende i vilken typ av nod den sitter.

6.1 Ett inledande exempel

Låt oss utgå från ett exempel i figuren nedan:



Figuren beskriver ett urval förbandsenheter och andra aktörer och resurser som tillsammans genomför en svensk insats. Noderna i figuren är:

- **OPIL**,
  Kontingenten består av
  - **Special Force Platoon**
  - **Helicopter Squadron**
  - **Heavy Armored Battalion (stridsvagnsbataljon)**
  - **Submarine Ship**
  - **Surface Ship**
- **JCC**, Joint Commanding Chief, till exempel FN eller NATO.
- **SwGov**, Svenska regeringen.
- **Hosp**, Ett svenskt sjukhus som används som experter
- **SMHI,** För väder.
- **Data Fusion**, placerad i en specialdator på KTH.

I figuren så har vi också ”öppnat upp” stridsvagnsbataljonen till en del. Figuren är naturligtvis bara ett utsnitt av alla enheter som kan tänkas finnas men vissa principer och antaganden framgår förhoppningsvis:

- Själva insatsstyrkan sträcker sig från OPIL och till höger i bilden.
- OPIL samverkar med svenska myndigheter och med NATO eller FN.
- Det finns ett antagande om att ”hierarkiska strukturer” finns kvar. En bataljon ”består av” ett antal kompanier som i sin tur ”består av” och så vidare.
- Nätet består av ett antal subnät som använder olika transmissionsteknologier. En enhet i en del av nätet kan principiellt kommunicera med vilken annan enhet som helst, oberoende av subnät. Åtkomsten kan dock begränsas av doktrinmässiga, säkerhetsmässiga, tekniska och taktiska skäl.
- Vissa noder finns i flera subnät och fungerar också som ”bryggor” mellan dessa subnät. Dessa bryggor kan tekniskt tänkas ligga i transmissionslagret (routrar) eller i applikationslagret.
- Alla enheter i nätet vet också ”hur nätet ser ut”, dock begränsat av sina rättigheter.
- Situationen i figuren är en ögonblicksbild, nättopologin kan (snabbt) ändras av olika orsaker.
- Nätet kan också i vissa situationer vara osammanhängande så att autonoma öar uppstår.

Figuren är en ganska tekniknära representation av nätet. Man skulle också kunna illustrera nätet utan subnät, ungefär som Internet ibland avbildas. I en sådan representation så når alla uppkopplade varandra förutsatt att nätet hänger ihop. Om nätet inte är sammanhängande så finns isolerade (autonoma) öar där varje ö är ”Internet-lik”.

Båda sätten att illustrera nätet äger sin giltighet i olika situationer. En slutanvändare ser troligen nätet som ett Internet oavsett hur trafiken går. Å andra sidan så vill en slutanvändare troligen inte få upp en lista med alla 3,000 Markus-soldater i sin applikation. I de applikationer han använder vill han kunna ”känna igen” en familjär organisation när han skall söka sig fram till en viss enhet eller enskild soldat.

En annan viktig sak att inse i bilden ovan är att varje nod i nätet är en kommunicerande dator i någon form. Dessa datorer har applikationer av olika karaktär och med vitt skilda krav. Exempel på ett antal olika NBF-noder med stegrande komplexitetsgrad kan vara:

- En Markussoldat har en ”enkel” utrustning. Idag skulle vi likna den med en modern mobiltelefon. Denna utrustning har troligen inte krav på redundans. Antalet tjänster som andra noder kan utnyttja är begränsat.
- I en stridsvagn sitter kanske en PC-lik dator som samlar in data från stridsvagnen för internt bruk och för att rapportera uppåt till den gemensamma lägesbilden. Vidare finns en applikation som hämtar den gemensamma lägesbilden så att olika befattningshavare i vagnen kan se den på sina displayer. Man kan också tänka sig att en dator i en vagn kan ta över vissa funktioner från en annan stridsvagn, till exempel närbevakning.
- I en bataljonsstab har man behov av ett ledningssystem i vilket flera befattningshavare kan arbeta samtidigt. Staben kommer att arbeta delat eller mer distribuerat än så. Man kommer då in på begrepp som arbetsflöden och processer (eller WorkFlow). Man kan också tänka sig analys- och beslutsstödsapplikationer som är krävande. Troligen kommer bataljonsstabens nod att bestå av ett flertal samverkande datorer med icke-funktionella krav som redundans, *fail over*, skalbarhet, distribuerbarhet och så vidare. Vidare kommer bataljonsstaben (kanske) att hantera icke öppen information vilket också ger krav på systemet, exempelvis inloggning.

- I OPIL:s stab kommer datorstödet av naturliga skäl att bli än mer komplicerat. Bara storleken på staben och antalet befattningshavare inblandade är en faktor i sig. Det kommer också att finnas en hel del avancerade stödsystem (logistiksystem) som kan betraktas som *back-office*-funktionalitet. IT-stödet i en stab av denna dignitet kanske också har en egen intern integrationsteknologi.

Observera att exemplen inte nödvändigtvis är riktiga utan avsikten är att belysa den stora spännvidd som kommer att finnas mellan olika typer av noder i ett NBF-nätverk.

6.2 Baskrav på kärnan

Situationen som beskrivs ovan är en tämligen klassisk bild av ett (stort) antal olika system som ska integreras. En grundbult är att definiera hur kommunikationen mellan de olika systemen skall ske. En inledande definition på nätverkskärnan är:

> *Nätverkskärnan beskriver och implementerar mekanismer för att möjliggöra ett säkert informationsutbyte mellan noder i ett NBF-perspektiv. Nätverkskärnan handlar endast om konsten att utbyta information, inte om vilken information som faktiskt utbyts.*

Nätverkskärnan förutsätter naturligtvis transmission, i vårt fall IP-trafik med hjälp av olika transmissionsteknologier. Det grundläggande kravet är att olika noder skall prata samma språk[15]. För att kommunikation noder emellan överhuvudtaget ska fungera krävs dels att en nod kan hitta andra noder och dels också att den kan ta reda på vilka tjänster andra noder kan bistå med. En annan grundläggande egenskap är att informationsutbytet skall vara säkert. Säkerhet innebär bland annat att en nod kan avgöra vem som åberopar tjänster och att informationsutbytet kan ske skyddat mot insyn. Det kan synas som tämligen triviala krav på kärnan att en nod skall kunna upptäcka och kommunicera med andra noder. Man ska dock komma ihåg att den omgivning som en nod kommer att verka i kan vara synnerligen dynamisk med nya och bortkopplade noder i en snabb takt.

Förutom att kunna hitta noder och kunna kommunicera säkert måste en nod i ett NBF-sammanhang följa vissa andra regler. Olika noder behöver ta hänsyn till olika mycket av sådana regler. Exempel är:

- **Intensitet**
  I vissa lägen kommer prestandan i nätet att vara begränsad. Det kan gälla både bandbredd och ren CPU-kraft. Noder måste kunna ”styras” så att de går ner i intensitet för att inte överbelasta transmissionen eller andra noder. Detta kan till exempel ske genom att en nod anropar en annan nod för uppdateringar mindre ofta.
- **Sessioner**
  Tjänster kommer att anropas i en följd och ett sådant sammanhang måste kunna identifieras. Begreppet för detta är att noder måste kunna ”hålla” en session. Hur sessioner etableras och hålls måste vara överenskommet i förväg.
- **Quality of Service (QoS)**
  Olika exempel på vad man brukar kalla ”Quality of Service” är tillgänglighet, redundans, skalbarhet och ”fail over”. Olika noder kommer att behöva olika grader av

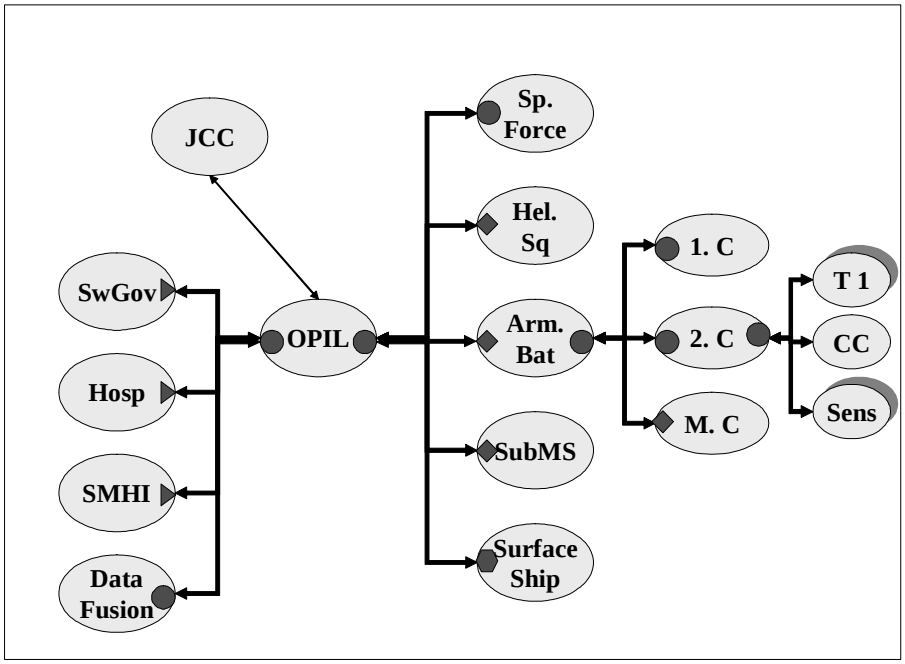
[15] Språk ska här ses i pluralis. Det bör finnas ett språk som alla kan prata. Andra språk kan behövas i speciella situationer. Ett konkret exempel är att alla ska kunna prata SOAP över http men att i vissa situationer är CORBA eller MQ-series mer lämpliga.

QoS. Exempelvis kan funktionaliteten hos en viss typ av nod behöva vara fysiskt separerad på flera datorer för att öka graden av tillgänglighet. Vissa typer av noder måste kunna klara stor belastning och vara förberedda för att skala upp på ett enkelt sätt.

6.3 Kärnans omfattning

Praktiskt sett är det möjligt att dra gränsen för vad nätverkskärnan skall omfatta lite olika. En möjlighet är att vara minimalistisk och argumentera för att egenskaper som skalbarhet inte skall omfattas av kärnan. Ett annat synsätt är att definitionen av kärnan lämpligen följer av vilka teknologier och produkter som till slut väljs. Klart är dock att den verksamhetslogik som finns i noderna inte hör till nätverkskärnan.

Noteras skall dock att kärnan inte är "någon server någonstans" utan kommer att vara en integrerad del av alla noder som ingår i en NBF-situation, illustrerat som små "klickar" i figuren nedan.



Instanserna av nätverkskärnan i bilden ovan har olika form för att indikera att det troligen kommer att vara olika implementationer i olika noder. Alla kommer dock att ha en minsta gemensamma nämnare; att kunna hitta, autentisera och kommunicera med varandra. Vissa kärnor kommer att kunna "prata andra språk" och ha högre grad av avancerade egenskaper.

Ovanstående bild skall dock inte tas alltför bokstavligt. Det kan i vissa fall finnas funktionalitet som tillhör kärnan placerad på en eller flera dedicerade noder någonstans. Ett sådant exempel är en namn- eller katalogtjänst. Man ska dock vara väldigt försiktig med sådana lösningar eftersom det är lätt att bygga in oönskade beroenden. Ett grundkrav är att två autonoma Markussoldater skall kunna utbyta tjänster med varandra oberoende av någon tredje part. Specifika servrar kan dock effektivisera en del funktionalitet men det bör då finnas ett autonomt reservförfarande.

Olika implementationer av kärnan kommer också att användas på lite olika sätt av tjänste- och applikationsutvecklare. I det enklaste fallet är kärnan något som används för kommunikation.[16] I andra fall kommer en utvecklare att implementera en funktionalitet i form av en komponent. Denna komponent kommer sedan att dels kunna exekvera i en avancerad omgivning och dels kan ett kommunikationsgränssnitt automatisk skapas ”ovanpå” komponenten[17].

[16] Detta kan (mycket förenklat) liknas med att man använder sig av ”sockets” eller ”connections” i en programmeringssituation.

[17] Ett konkret exempel på detta är att man implementerar någon ledningsfunktionalitet i form av en Enterprise Java Bean. För denna komponent skapar man sedan genom verktyg den kommunikationsfasad som behövs, exempelvis Web Services. Komponenten kan sedan exekvera i mer eller mindre avancerade applikationsservrar.

7 Verksamhetsstödjande tjänster

Detta kapitel behandlar det översta lagret i den presenterade modellen för en nätverksstruktur, de verksamhetsstödjande tjänsterna. Det innehåller först en kort diskussion om vad verksamhetsstödjande tjänster egentligen är för något, för att därefter behandla framför allt en möjlig princip för hur dessa tjänster kan realiseras i ett NBF-sammanhang och vilka avvägningar denna princip medför.

7.1 Olika typer av verksamhetsstödjande tjänster

Den grova definitionen av verksamhetsstödjande tjänster är – naturligtvis – att de på något sätt stödjer den verksamhet som bedrivs, i det här fallet militär verksamhet i vid mening. På sätt och vis stödjer också de funktioner och tjänster som finns i nätverksstrukturens underliggande två lager den militära verksamheten men på ett mer indirekt sätt. De är mer att betrakta som generella tekniska funktioner som ser likadana ut oavsett vilket nät de ytterst ingår i och vilken verksamhet de ytterst stödjer.

Med detta som bas kan sedan en ytterligare distinktion göras mellan två olika typer av verksamhetsstödjande tjänster. Det finns för det första de tjänster som innehåller logik byggd kring militära objekt (till exempel mål, plan, order). Det handlar om tre övergripande typer av tjänster; Ledningstjänster (beslutsstöd, stabsstöd, uppdragsplanering med mera), Omvärldsbeskrivande tjänster (såsom sensorinformation och måldatafusion) samt Verkanstjänster (exempelvis vapenverkan, informationsattacker och underhåll). Några exempel på denna typ av tjänster har utvecklats[18].

En annan typ av verksamhetsstödjande tjänster är de som mer liknar civila applikationer men i vårt fall används i ett militärt sammanhang. Här finns för det första sådant som kan hjälpa enskilda individer och grupper i deras (oftast stabs-) arbete. Det kan handla om sökmotorer, stöd för grupparbete, distribuerat *workflow* med mera. För det andra finns i den här gruppen sådant som mer syftar till att få organisationen och verksamheten att fungera. Det är sådant som logistikstöd och ekonomisystem.

I ett första skede på vägen mot en fullt utbyggd NBF-vision kan det vara värdefullt att vara medveten om denna skillnad mellan olika typer av verksamhetsstödjande tjänster. Den princip för hur dessa tjänster kan realiseras som beskrivs nedan fungerar i och för sig för båda typerna av tjänster men det kan finnas en skillnad på andra plan, till exempel avseende vilka typer av tjänster som kan stödjas med kommersiellt tillgängliga produkter.

I en situation som mer närmar sig den vision som NBF beskriver (i en mer avlägsen framtid) kan skillnaden mellan de två typerna av verksamhetsstödjande tjänster eventuellt komma att vara mindre intressant. Detta kan till exempel bli fallet om vi får en situation där alla tjänster erbjuds i form av små ”paket” som kan plockas ut från en stor tjänstedepå och byggas ihop efter önskemål. Men det ligger bortom den tidshorisont som är aktuell i den här rapporten och lämnas därför till diskussion på annan plats.

7.2 Möjliga realiseringsprinciper

Det finns ett antal möjliga principer för hur nya (typer av) verksamhetsstödjande tjänster kan realiseras i ett NBF-sammanhang. För att generera ett antal sådana principer – och för att kunna prioritera mellan dem – har utgångspunkterna här varit att de:

[18] FOI-R--1038—SE, FoRMA 2003: Nätverksanalyser

- Ska ta hänsyn till existerande system (det som blir ”arvet” i en NBF-värld), helst så att dessa snabbt och kostnadseffektivt kan föras in i ett NBF-sammanhang,
- Ska vara förenliga – eller i alla fall inte uppenbart oförenliga – med andra initiativ såsom FM A,
- Ska hänga ihop med de andra två nivåerna i den nätverksstruktur som utgör grunden för detta arbete,
- Ska vara rimliga i förhållande till den teknik och de koncept som finns idag, samtidigt som
- De ska vara framtidssäkra, det vill säga bygga på principer och metoder som är sådana att de kan antas leva under lång tid framöver.

Med dessa utgångspunkter som grund kan tre realiseringsprinciper identifieras. En av dessa bygger, populärt uttryckt, på att existerande system förses med ett extra lager som möjliggör kommunikation med andra system via en applikation som så att säga läggs ovanpå de existerande systemen.

En annan möjlig princip är att gå in i de existerande systemen och bygga om dessa enligt vissa gemensamma principer så att de kan kommunicera mer direkt med varandra utan en överliggande applikation. Ytterligare ett alternativ är att lämna de existerande systemen orörda och nöja sig med att bygga nya system enligt vissa NBF-kompatibla principer. Allt eftersom nya system ersätter existerande så blir helheten allt mer NBF-liknande.

Av dessa möjliga alternativ har den första principen valts och den diskuteras utförligare nedan. Alternativ två har valts bort eftersom det antas vara en betydligt besvärligare och dyrare väg att gå medan den tredje principen har valts bort på grunden att det skulle ta väldigt lång tid att komma till NBF den vägen.

7.3 Kompositapplikationer

Den princip som skissades och valdes ovan utvecklas i detta avsnitt. Utgångspunkten har varit det som i alla fall i affärssystemvärlden ibland går under benämningen *Composite Applications*[19].

Grundtanken där är i korta drag att det i ett företag – eller för den delen i ett nätverk av samverkande företag – finns ett flertal olika applikationer/system som alla innehåller information som för vissa arbetsuppgifter behöver samordnas. Ett exempel kan vara kundinformation; det finns exempelvis ett kundregister med adress- och kontaktuppgifter, ett ekonomisystem med de finansiella transaktionerna med kunderna, ett system för produktionen som kan ge uppgifter om var kundens produkter befinner sig i tillverkningsprocessen, ett system för service- och supportcentret med kundernas supportärenden och hur dessa hanterats, och så vidare. Samtliga dessa system kan dessutom i verkligheten vara uppdelade på ett antal system.

I stället för att bygga in all denna information i ett nytt system – eller bygga ut ett av de existerande systemen och låta det bli överordnat de andra – är tanken med en *composite application* (hädanefter kompositapplikation) att all information ska ligga kvar i och ägas av de idag existerande systemen. På dessa lägger man väl definierade gränssnitt och kommunikationsformat så att de kan kommunicera med en kompositapplikation som sköter

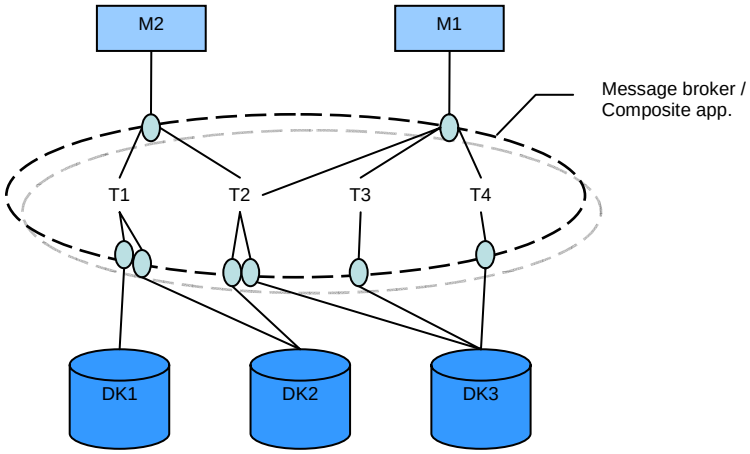
[19] Jämför till exempel med vad SAP kallar *xApps.* Se SAP, 2003 i referenslistan.

all bearbetning och presentation av information som kräver data från fler än ett av de underliggande systemen.
Notera att inte all integration mellan samtliga system sköts via en enda kompositapplikation. Dessa byggs tvärtom förhållandevis uppgiftsspecifika och det blir i stället frågan om en uppsättning kompositapplikationer.

I det följande diskuteras fyra olika aspekter på kompositapplikationer. Dessa är i tur och ordning hur dessa applikationer är uppbyggda ur logisk respektive teknisk synvinkel, vilka krav en lösning med kompositapplikationer ställer samt vilka effekter en sådan lösning ger upphov till.

7.3.1 Logiskt

Om denna tanke tillämpas på nätverksstrukturen och de verksamhetsstödjande tjänsterna som de definieras i detta dokument får man en principbild som den nedan:



I denna bild finns det mottagare (M) som är antingen applikationer eller individer i behov av en eller flera verksamhetsstödjande tjänster (T). För att dessa tjänster ska kunna leverera behöver de i sin tur indata från en eller flera datakällor (DK) – eller en eller flera andra, underliggande tjänster men detta är inte illustrerat i bilden. Dessa underliggande datakällor har alla sina egna dataformat och informationsmodeller och kommunicerar med kompositapplikationen som också innehåller en ”översättningsfunktion”.[20]

Kompositapplikationen sköter sedan all databearbetning som är nödvändig för att kunna leverera de efterfrågade tjänsterna till mottagarna. Även den leveransen går via en översättningsfunktion vilket möjliggör att även mottagarna kan ha sina egna dataformat och informationsmodeller.

Med detta minskar komplexiteten drastiskt jämfört med alternativen. Alla system är enbart kopplade till kompositapplikationen och en ändring i ett av systemen – eller ett byte av system – påverkar enbart det aktuella systemet och kompositapplikationen. Ändringar blir därmed lätta och billiga att genomföra och de gamla systemen kan leva kvar och anpassas eller bytas ut i den takt som är tekniskt och ekonomiskt motiverat. Varje delsystem kan dessutom fortsätta att vara optimerat för sin uppgift/funktion och därmed vinner man i effektivitet.

[20] Jämför till exempel med Microsoft BizTalk Server. Se Microsoft, 2003, i referenslistan.

7.3.2 Fysiskt

Beskrivningen ovan är en logisk representation av hur verksamhetsstödjande tjänster kan produceras och levereras. Fysiskt kan kompositapplikationen antingen ligga separat i en egen enhet/server eller i anslutning till en eller flera datakällor/mottagare. I ett extremfall är alla datakällor, mottagare och själva kompositapplikationen fysiskt åtskilda, dvs de ligger i olika servrar som alla kan befinna sig på olika och geografiskt åtskilda plattformar. Men flera andra modeller kan också tänkas.

Ett exempel på en annan modell är *Cooperative Engagement Capability* (CEC). Detta är ett amerikanskt system för att skapa en gemensam lägesbild på ett antal sjöstridsenheter.[21] Genom att koppla ihop de olika enheternas sensorer skapar man större räckvidd och en bättre målföljning än vad varje separat enhet kan åstadkomma på egen hand.

I princip fungerar detta genom att det finns en kontinuerlig kommunikation mellan samtliga enheter i systemet via parvis kommunikationskanaler där en enhet sänder sina data (rådata, ej spår) till en annan enhet i korta datapulser. De olika enheterna har sedan samma logik installerad och eftersom de alla opererar med samma indata ger de olika enheternas individuella bearbetning av informationen samma resultat.

I de termer som använts ovan är de olika sjöstridsenheternas sensorer de datakällor som används. Kompositapplikationen är den logik som tar ingångsvärdena från de olika sensorerna och genererar en lägesbild utifrån dessa data. Mottagare är de olika sjöstridsenheternas verkansfunktioner. Kompositapplikationen finns i flera instanser; en i anslutning till varje sensor. På varje sjöstridsenhet (plattform) finns både en datakälla, en instans av kompositapplikationen och en mottagare.

7.3.3 Krav

För att den lösning som har beskrivits ovan ska fungera krävs flera saker. För det första måste det finnas en informationsmodell för varje kompositapplikation och en beskrivning som visar hur denna förhåller sig till de underliggande systemen. Notera dock att det inte alls krävs att de underliggande systemen har samma informationsmodell som kompositapplikationen – det räcker att definiera hur de förhåller sig till varandra i de dimensioner som berörs.

Vidare måste det finnas en kärna som definierar vilka grundläggande protokoll och tekniker som ska användas. För att få full effekt måste både kärnan och de olika kompositapplikationerna vara byggda så att nya protokoll och tekniker lätt kan inkorporeras i kärnan.

Kärnan måste också stödja realtidskommunikation eftersom det i många fall sannolikt kommer vara så att kompositapplikationerna efterfrågar data från de underliggande systemen när de så behöver – alternativet att bygga upp stora databaser där kompositapplikationerna hämtar information är knappast realistiskt i alla fall.

Med den mängd integrationer det kan bli fråga om i en fullt utbyggd NBF-värld så måste priset per integration vara så lågt som möjligt. Dessutom bör nya integrationer kunna byggas rimligt snabbt, både mot egna system och mot system från andra. Båda dessa skäl talar för att öppna och kommersiellt tillgängliga standarder bör användas i så stor utsträckning som möjligt.

[21] För en beskrivning av CEC, se till exempel Federation of American Scientists, 2003, i referenslistan.

7.3.4 Effekter

Det finns flera fördelar med att realisera de verksamhetsstödjande tjänsterna inom NBF med hjälp av en kompositapplikationsprincip. Dessa är till exempel:

- Man behöver inte riva ut eller bygga om arvet – det räcker med att kapsla in de olika arvssystemen så att de kan kommunicera med en eller flera olika kompositapplikationer. Detta torde vara rimligt enkelt och billigt att göra jämfört med alternativen att bygga nytt eller att drastiskt bygga om existerande applikationer.
- Det medger att existerande – och inte minst framtida! – system kan byggas så att de blir optimalt funktionella för en given uppgift samtidigt som de via ett gränssnitt mot en kompositapplikation kan såväl erbjuda tjänster till som efterfråga tjänster från andra system. Självklart kommer det att kräva mer utvecklingsresurser om de framtida systemen både ska innehålla funktionalitet för sin egen uppgift och vara NBF-kompatibla så att de kan kommunicera med andra system. Men detta är fallet oavsett vilken realiseringsprincip som väljs och den här beskrivna principen är sannolikt den minst resurskrävande.
- Ändringar och anpassningar av system kommer att bli förhållandevis lätta, snabba och enkla att genomföra eftersom det bara finns ett gränssnitt att ta hänsyn till – nämligen mellan kompositapplikationen och systemet i fråga. Vidare kan all utveckling och alla ändringar göras i form av flera mindre steg, snarare än i en stor insats, vilket är både säkrare och i de flesta fall billigare.
- Genom att bygga Försvarsmaktens system efter en kompositapplikationsprincip ökas också möjligheterna att ta in utomstående parter – till exempel civila myndigheter eller utländska enheter vid internationella insatser. Det enda som krävs är ett NBF-kompatibelt skal på de aktuella systemen, precis på det sätt som används för att integrera Försvarsmaktens arvssystem. Det är inte alldeles enkelt att bygga ett sådant skal men igen – det är den enklaste vägen som finns. Det bör också noteras att om de aktuella systemägarna inte vill bygga ett skal på sina system kan motsvarande funktionalitet lika gärna läggas i kompositapplikationen, under förutsättning att gränssnitten (de tjänster som levereras) från/till de ”främmande” systemen är väl definierade.

7.4 Avvägningar

Det finns flera dimensioner där den ovan beskrivna realiseringsprincipen inte föreskriver en specifik lösning. I stället finns där en skala där olika utfall kan tänkas, beroende på situation och vilken tjänst det är frågan om.

7.4.1 En eller flera instanser av kompositapplikationen?

En uppenbar diskussionspunkt – illustrerad av CEC-exemplet ovan – är hur många instanser man ska ha av kompositapplikationen och var denna/dessa ska ligga någonstans rent fysiskt. Att ha endast en separat instans av kompositapplikationen har den fördelen att det är bandbreddsbesparande eftersom endast ett litet antal kommunikationslänkar behöver upprättas. Man slipper situationen att alla mottagare kontaktar alla datakällor hela tiden. Å andra sidan blir hela lösningen känslig för utslagning eftersom man skapar en ”single point of failure”.

Om kompositapplikationen i stället finns i flera instanser – till exempel en på varje samverkande enhet – uppnås en ökad robusthet. Detta kommer dock som regel att ske till en högre kostnad; en sådan lösning kräver sannolikt fler och mer avancerade kontrollfunktioner för att säkerställa att de olika enheterna verkligen arbetar med exakt samma indata (till exempel tidsdimensionen), att de ger de olika målen samma nummer (i CEC och liknande fall), och så vidare. Därmed blir också utvecklingsinsatsen svårare, längre och dyrare.

7.4.2 Principen med system-av-system påverkar

En annan dimension som man kan spela med är hur ”tydligt” varje enhet ska veta vilka andra enheter som finns i dess närhet. I en lösning som bygger på system-av-system-tanken är det möjligt men inte helt säkert att flera av de tänkbara kompositapplikationerna kommer att finnas inom ett väl definierat sub-system. Detta har sannolikt viss betydelse för hur kompositapplikationerna ska byggas men huvudsakligen är de krav denna dynamik ställer en fråga för nätverkskärnan.

En annan implikation av system-av-system-tanken är att det kan bli fråga om flera nivåer där en kompositapplikation hämtar information från andra kompositapplikationer och därefter levererar sitt resultat till ytterligare en eller annan kompositapplikation. Det är sannolikt inte särskilt praktiskt att bygga en lösning i alltför många nivåer men det finns inget i principen med kompositapplikationer som hindrar det.

7.4.3 Central eller distribuerad lösning

Ytterligare en avvägning där principen med kompositapplikationer lämnar fältet öppet för olika val är den mellan central och distribuerad lösning. Bland kommersiella system har länge funnits en trend att lägga så mycket som möjligt av ett givet system på en central server och därefter bygga vad som kallas tunna klienter, det vill säga med liten mängd kod på användarens sida. Idealfallet har många gånger varit att det räcker med en webbläsare.

För vissa militära tillämpningar kan det tänkas att detta är långt ifrån en ideal situation. Det kan finnas tjänster där en viss mängd logik på klienten är nödvändig, till exempel för att säkerställa överlevnad även om kommunikationen mot en central server skulle försvinna. Andra faktorer där det militära sammanhanget kan sätta gränser och/eller ställa krav rör exempelvis tillgänglig bandbredd och processorkraft på olika ställen i nätverket.

8 Kostnadsuppskattning

8.1 Metodik

Det finns flera olika metoder för att göra kostnadsuppskattningar av utvecklingsprojekt rörande informationsteknik och informationssystem. Exempelvis har RAND i en rapport till FOI identifierat tre olika metoder (Perry et al, 2003):

- *The Bottom-up Approach*
- *The Analogy Approach*
- *The Parametric Approach*

Den första av dessa metoder innebär att man utifrån en detaljerad bild av det framtida systemet uppskattar kostnaden för varje enskild del (på en ”låg” nivå) och därefter adderar alla dessa till en slutsumma. Detta tillvägagångssätt kräver en stor arbetsinsats och är inte ens då möjligt att genomföra fullt ut utan en detaljerad bild av det som ska byggas och en djup kunskap om kostnaden för alla dessa enskilda delar.

Att uppskatta kostnaden med hjälp av analogier innebär enligt RAND att man söker efter ett redan existerande system som är så likt det som ska kostnadsuppskattas som möjligt. Om kostnaden för det redan existerande systemet är känd räcker det då med att göra en uppskattning av avvikelserna mellan det och det nya systemet. En variant av att använda analogier är att låta en eller flera experter göra en uppskattning baserad på egen erfarenhet. Inte heller detta är problemfritt – bland annat finns risker kring subjektivitet och föråldrad erfarenhet – men i vissa fall är detta ändå det bästa alternativet.

The Parametric Approach, slutligen, innebär att man letar efter relationer mellan faktorer av betydelse för systemet och kostnader. För mjukvara kan det t ex handla om antal rader kod som systemet omfattar, hur mycket data det ska hantera eller något liknande. Med hjälp av historiska nyckeltal kan därefter – om samma nyckeltal antas gälla – kostnaden för det nya systemet uppskattas.

8.1.1 Att kostnadsuppskatta nätverksstrukturen

I dagsläget erbjuder alla de tre metoderna ovan stora svårigheter i uppskattningen av kostnaden för nätverksstrukturen. Exempelvis så saknas den detaljerade kunskap om vad som ska utvecklas för att det ska vara möjligt att fullt ut tillämpa vare sig *the bottom-up approach* eller den parametriska ansatsen. Vi vet helt enkelt inte vad som ska byggas och utan den kunskapen är det naturligtvis omöjligt att göra kostnadsuppskattningar med någon säkerhet.

Analogiresonemang är generellt sett svåra eftersom även små skillnader i vad som ska utvecklas eller i de miljöer där utvecklingen ska ske kan resultera i stora kostnadsskillnader. Vad gäller NBF finns heller inga motsvarande system utvecklade tidigare varför eventuella analogier skulle få sökas ganska långt bort, så att säga. Det blir då naturligtvis än svårare att få till stånd en rimlig jämförelse. Till viss del kan detta bero på att det tycks finnas en mer eller mindre uttalad vilja från svensk sida att ligga på *the bleeding edge* när det gäller utvecklingen av NBF. Med detta avses att man ligger allra längst fram i teknikutvecklingen och tar alla kostnader och misslyckanden själv. Även en moderat skillnad i inställning – att det räckte med att ligga på *the leading edge* – skulle kunna underlätta ett analogiresonemang i framtiden när fler nationer hunnit längre i sin utveckling av koncept och teknik.

Till dessa svårigheter som är direkt kopplade till den ena eller andra metoden för att genomföra kostnadsuppskattningar bör också läggas ett antal mer generella svårigheter som gäller NBF i nuvarande skede. En av dessa är att projektet ännu får anses vara i en initieringsfas. Med den terminologi som används i *Rational Unified Process* (RUP) – den mest kända och använda metoden för mjukvaruutveckling – kan NBF sägas vara i ett tidigt skede av *Inception*, den första fasen av fyra i RUP. För att man ska kunna göra en rimlig kostnadsuppskattning ska helst hela den andra fasen vara genomförd och dit är det ännu långt för NBF.[22]

Vidare utvecklas NBF med ett evolutionärt angreppssätt vilket innebär att konceptet, metoderna, tekniken etc. utvecklas parallellt och i flera iterationer. Syftet med detta angreppssätt är att man ska kunna bygga bättre system. Men det är inte ägnat att vare sig minska kostnaden eller underlätta en kostnadsuppskattning, effekten blir snarare den omvända i dessa dimensioner.

NBF är också ett långsiktigt projekt som med all sannolikhet involverar teknik som inte finns att köpa kommersiellt, vare sig idag eller vid aktuell tidpunkt i framtiden och därför måste utvecklas. Detta involverar då

- dels en uppskattning idag av hur långt den kommersiella utvecklingen kommer att ha kommit vid en tidpunkt flera år framåt i tiden, och
- dels en uppskattning av de utvecklingsresurser som kommer att krävas för det som fattas.

Trots dessa svårigheter – och det förtjänar att påpekas att flera av dem kommer att minska i betydelse med tiden och i takt med att arbetet med NBF fortskrider – vill vi försöka visa på storleksordningen för de kostnader det sannolikt kommer att bli fråga om. Vårt primära intresse i denna uppskattning är kostnaderna för utveckling och andra investeringar. Vi bortser tills vidare från kostnader förknippade med exempelvis utbildning och framtida drift och underhåll av den lösning som så småningom tas i bruk. Vi för heller inget resonemang om kostnadseffektiviteten (det vill säga mängden ”pang för pengarna”) i olika lösningar.

8.2 Paralleller till NBF

Det finns egentligen inga tillgängliga siffror från andra länder kring kostnaderna för NBF-liknande initiativ, framför allt inte från sådana som är jämförbara med Sverige. Det finns en del tillgängligt framför allt från USA vilket redovisas nedan. Men de har naturligtvis en helt annan budget och andra ambitioner än vad som är aktuellt för Sverige vilket man bör hålla i minnet.

8.2.1 Global Information Grid

USA:s motsvarighet till det svenska begreppet Nätverksbaserat försvar är *Network Centric Warfare* (NCW). Det finns också ett begrepp *Global Information Grid* (GIG) som är själva den tekniska infrastrukturen för att man ska kunna agera nätverksbaserat. I tabellen nedan redovisas de investeringar som USA redan beslutat om för att kunna bygga GIG (Frankel, 2003). Notera att detta alltså inte är totalkostnaden för dessa delar utan enbart redan beslutade projekt.

[22] De fyra faserna är *Inception*, *Elaboration*, *Construction* och *Transition*.

Kalkylen omfattar vad det verkar en del hårdvara (bland annat några satelliter) men ingen mjukvaruanpassning av existerande system. Detta betyder att det huvudsakligen svarar mot det vi i den här rapporten kallar för kommunikationslager respektive nätverkskärna men inte det vi kallar verksamhetsstödjande tjänster. Som framgår av tabellen ligger investeringarna på drygt 250 miljarder svenska kronor fram till och med 2009.

	DoD Investments ($ Million)		
GIG Area	**2003**	**2004-2009**	
GIG Bandwidth Expansion	500	300	
Transformational SATCOM	120	9 850	
Joint Tactical Radio System	200	5 750	
Net-Centric Enterprise Services		380	
Horizontal Fusion	75	1 220	
Dist. Common Ground Station	513	6 573	
Global C2 System	23	305	
Crypto Transformation Program	977	6 152	
Total	**2 408**	**30 530**	**32 938**
USD/SEK Exchange Rate	7,67		
Miljarder SEK			**252,63**

8.2.2 Cooperative Engagement Capability

Ett annat exempel från USA – det ovan beskrivna CEC – är förmodligen det system av någon slags NBF-karaktär som utvecklats längst och som därmed erbjuder det bästa jämförelseobjektet idag. Det är två saker som bör noteras om detta system i relation till den nätverksstruktur som den här rapporten handlar om: för det första är det ett system som är till för att lösa en enda, väldigt tydligt definierad uppgift. Det är därför inte omedelbart överförbart till en allomfattande nätverksstruktur. Dock, och för det andra, den uppgift systemet ska lösa är helautomatiserad och kräver realtidskommunikation. Det är alltså svårt att tänka sig ett fall där kraven är högre på ett system än detta.

Totalkostnaden för utvecklingen av CEC kan antas hamna någonstans runt $3 miljarder (Sherman, 2003). Enligt Perry et al (2003) är fördelningen av dessa utvecklingskostnader drygt 20 % på integration i existerande plattformar, 10 % på testning och resten på ny mjukvara. Man kan notera att utvecklingskostnaden för hårdvaran var närmast obefintlig eftersom man använde kommersiellt tillgänglig teknik. Vad gäller drift och underhåll så beräknas hälften av den kostnaden avse underhåll och support av mjukvara.

8.2.3 Bowman

Det brittiska försvaret fattade under 2001 ett inköpsbeslut kring ett digitalt röst- och datakommunikationssystem kallat Bowman.[23] Syftet med detta system är främst att tillhandahålla effektiv kommunikation för att stödja ledning på lägre taktiska nivåer. Det ska dock vara integrerat med andra kommunikationssystem för att möjliggöra snabb kommunikation på alla nivåer, från den taktiska till den strategiska. Ett annat krav är att systemet ska kunna utvecklas till ett mer avancerat digitalt system, i riktning mot ett ”taktiskt Internet”. Bowman ska omfatta alla tre grenar av det brittiska försvaret, börja införas under 2004 och fungera minst till 2026.

[23] Global-Defence.com (2001) och General Dynamics (2001).

Kontraktet var på 1,8 miljarder pund, det vill säga i dagens penningvärde ungefär 23 miljarder SKr. Detta omfattar omkring 48 000 radioapparater och 30 000 datorer. Mer än 30 000 fordon och andra plattformar kommer att modifieras och omkring 100 000 individer ska utbildas på de nya apparaterna. Dessutom ingår support under de första fem åren.
I de termer vi använder i den här rapporten återfinns Bowman i kommunikationslagret i nätverksstrukturen. Det bör dock noteras att det dels inte på något sätt utgör hela kommunikationslagret, dels att det är minst en generation äldre än det radiosystem vi har diskuterat tidigare i rapporten.

9 Variationer

Så här långt i arbetet har vi medvetet valt att inte formulera distinkta alternativ inom ramen för den generella beskrivningen av vad en nätverksstruktur består av. Detta ligger i linje med att det vi beskriver är *gemensamma* satsningar, där standardisering är det avgörande för framgång, och de hinder vi vill övervinna alla har sin grund i inkompatibla system.

För att kunna bedöma konsekvenserna av olika ekonomiska nivåer på nätverkssatsningar måste ett resonemang föras om vilka faktorer som påverkar hur man kan *rikta* dessa satsningar, för att svara mot de allmänna inriktningarna som knyts till de olika nivåerna.

En första hypotes är att större delen av variationen kommer att slå igenom i nätverkets ”perifera delar”, framförallt i kommunikationsinfrastrukturen, genom att olika delnät kan uteslutas eller byggas ut i varierande omfattning. Mängden verksamhetsstödjande tjänster som behöver utvecklas i olika alternativ kan variera, beroende på vilka sensor-, lednings- och verkanssystem som skall stödjas. Den centrala kärnan av nätverkstjänster påverkas däremot inte, *by design*. Däremot kan den faktiska implementeringen och driften av dessa nätverkstjänster i någon mån påverkas av varierande krav på skydd och säkerhet.

9.1 Variationsdimensioner

Detta avsnitt försöker svara på frågorna:

- Vilka parametrar behövs för att beskriva alternativa utformningar av en framtida nätverksbaserad försvarsmakt?
- Hur påverkar dessa parametrar utformningen av nätverksstrukturen?
- Vilka av dessa är särskilt kostnadsdrivande?

Nedan redovisas ett antal parametrar som kan ha stor inverkan på vilka krav som ställs på nätverksstrukturen. De flesta är mer eller mindre kopplade till varandra, vilket starkt begränsar det möjliga utfallsrummet av lösningar.

Uppgifter, förmågor och delförmågor

Beskrivningen av alternativa utformningar av nätverket bör på något sätt knytas till vilka grundläggande förmågor det skall understödja.

Insatsmiljö

Bortom Europa, Europa, närområde, nationellt.
Det är naturligt att kraven på nätverket och hur man bäst tillfredställer dessa varierar inte bara med uppgiften utan även med det geografiska område där verksamheten skall genomföras. Dessutom kan man dela in den operativa miljön i domänerna *luft*, *mark*, *sjö* och ytterligare förfina beskrivningen genom att ange om speciella lokala förhållanden föreligger (exempel kan vara olika klimatologiska zoner, svår signalmiljö, NBC-hot med mera).

Kommunikationsinfrastruktur

God, dålig, obefintlig
Med detta avses den infrastruktur för kommunikation som finns på plats i operationsområdet före insats. Detta är nära kopplat till den operativa miljön, men det är inte självklart att insatser ”långt bort” alltid innebär att vi måste stå för hela uppbyggnaden av denna infrastruktur. Inom ramen för koalitionsoperationer kan någon annan aktör ansvara för att

tillhandahålla eller komplettera grundläggande kommunikationskapacitet (exempelvis utbyggda stomnät, mobila system och satellitlänkar). Problemet blir då mer att garantera interoperabilitet med dessa system.

Interoperabilitet

Höga krav på interoperabilitet med andra försvarsmakter eller andra aktörer kan komma att ställa mycket långtgående krav på det tekniska nätverket. Avgörande är formen för samverkan, på vilken nivå den sker och uppgiften. Om samverkan skall ske så att enskilda farkoster eller små förbandsenheter deltar sida vid sida med andra parter, och om uppgiften kräver samverkan i realtid, ställs mycket långtgående krav på samordning av både kommunikations- och ledningssystem. Större förbandsenheter som underställs en annan part, med egna uppgifter inom ett avgränsat operationsområde ställer inte lika långtgående krav på samordning av tekniska system, vilket skapar större utrymme för egna lösningar.

Interoperabilitet har både tekniska och organisatoriska aspekter. På det tekniska planet krävs givetvis att samverkande system är anpassade till en gemensam standard, allt från frekvenser, vågformer, protokoll, till kablar och kontakter. Dessutom krävs att den information som utbyts är uttryckt i en enhetlig form, från system för koordinatangivelser till utformningen av ordergivningar. På den organisatoriska nivån krävs givetvis att samverkande personal har en god kännedom om sina respektive organisationer, ledningsmetodik och taktisk uppträdande. Vi bedömer dock att detta inte är ställer särskilda krav på utformningen av nätverksstrukturen.

Designprinciper

Detta är ett sätt att försöka sammanfatta många olika faktorer. Enkelt uttryckt handlar det om traditionella respektive visionära strukturer. I termer av teknik handlar det framförallt om balansen mellan traditionella integrerade plattformssystem och innovativa distribuerade systemlösningar. Att bygga upp ett nätverksbaserat försvar på ett arv av traditionella plattformssystem är i praktiken det enda sättet att inleda en transformation mot en mer visionär utformning av försvarsmakten. Även mycket visionära strukturer kommer realistiskt sett att innehålla traditionella plattformssystem.

Sammanlänkning av befintliga plattformsbaserade system innebär merkostnader för att tillföra de gränssnitt som medger att information kan utbytas mellan separata, dedicerade system.

I det längre perspektivet, när nya system kan designas utifrån ett fullt utvecklat nätverkstänkande, sjunker dessa gränssnittskostnader. Visserligen ökar då de gemensamma kostnaderna när mer och mer funktionalitet flyttar ”ut från plattformarna och in i den gemensamma infrastrukturen”, men ett grundantagande bakom idéerna om nätverksbaserat försvar är att totaleffekten blir ökad funktionalitet och flexibilitet till samma eller lägre kostnad.

Doktrin och ledningsmetodik

Nya tekniska systemlösningar ger sällan stor effekt utan utvecklade principer och metoder för hur de skall utnyttjas. Eftersom många av grundtankarna bakom det nätverksbaserade försvaret är visioner om effektivare sätt att leda och genomföra insatser, oberoende av enskilda tekniska lösningar, borde man snarast utgå från dessa och överväga hur det systemtekniska nätverket bör utformas för att stödja dessa visioner.

Att flexibelt kunna skifta mellan decentraliserade och centraliserade ledningsprinciper ställer direkta prestandakrav på kommunikations- och ledningssystem. Vad gäller ledningsmetod kan man överväga komplement till uppdragstaktik, exempelvis självsynkronisering, initiativtaktik eller annat. Även sådana val kan ha konsekvenser för utformningen av nätverket. Utvecklade former av manöverkrigföring, såsom svärmning, kan komma att ställa speciella krav på utformningen av det systemtekniska nätverket.

Personal och organisering

Aspekter på personal och organisering i ett nätverksperspektiv har berhandlats översiktligt i förra årets arbete inom FoRMA:s nätverksgrupp. Det finns några förhållanden som kan komma att ställa specifika krav på utformningen av nätverksstrukturen. Karaktäristiskt för personer som agerar i en nätverksorganisation är att de kan ha flera olika roller samtidigt eller skifta mellan olika roller. Att bygga in sådan flexibilitet, prestanda och säkerhet i nätverket att man kan styra informationsflöden till aktörer som skall kunna agera i skiftande roller kan medföra höga systemkostnader.

Materielförsörjning och tjänsteupphandling

Kostnaden för att bygga upp ett nätverk beror även på *hur* man väljer att realisera kraven. I de fall man kan bygga på kommersiellt utvecklad teknologi och standarder kan kostnaderna bli lägre än om man av olika skäl måste utveckla dedicerade system. En avgörande faktor är om man köper färdiga, utprovade system, utvecklar själv eller i samverkan med andra. Dessutom finns ibland möjligheten att avväga mellan egenproduktion och tjänsteupphandling. Grundläggande fredstida kommunikationstjänster kan förstås i hög grad realiseras genom tjänsteupphandling, men även vissa temporära behov vid genomförande av operationer kan lösas genom upphandling, exempelvis genom inhyrning av satellitlänkar.

Volym och utvecklingstakt

I alla tänkbara försvarsmaktstrukturer kan man, inom vissa gränser, variera totalvolymen mätt i antal förband, system, personal med mera. En annan faktor man har att spela med är i vilken takt man inför nya system, och om man strävar efter införande på bredden eller väljer att prioritera vissa förband.

10 Metoder för systemframtagning

10.1 Bakgrund

Dagens fokus i försvarssfären finns till stor del inom nätverkssatsningarna för att åstadkomma visionen om det nätverksbaserade försvaret (NBF). Det syfte som oftast framställs som det primära är eftersträvandet av en bättre lägesuppfattning. En minst lika stor nytta (och kanhända i många fall till och med den bakomliggande drivkraften) är möjligheten till flexibilitet. Den bättre lägesuppfattningen kan sägas utgöra ”i princip ett resultat (en output) från de i NBF ingående systemen”, medan delen som berör flexibilitet i större utsträckning framstår som även avhängig andra faktorer. För att närma sig visionen bör fokus dessutom inriktas även mot nyss nämnda ”andra faktorer”.

Möjligheten till ett flexibelt upplägg i (genomförande och planering av) verksamheten, förutsätter naturligtvis att de system som används i arbetet utformas för att stödja denna flexibilitet. Dessutom krävs att arbetssätt och metoder vid framtagande av system anpassas, så att inte dessa arbetssätt och metoder istället övertar rollen av ”skapare av trång sektor” vad avser graden av flexibilitet. Ty en strävan som bland annat innebär att arbetet i det vidaste perspektivet ska bedrivas mer snabbfotat kan ju knappast bygga på utvecklingsprocesser – både avseende teknik och metod – vilka tar så lång tid, att chansen till det övertag som ett flexibelt systemstöd ger, ändå försitts på grund av den långa tid det tar att skapa systemet och den tillhörande metoden för användande (reglemente eller motsvarande).

10.2 Tjänstekonceptet

Förknippat med nätverkssatsningarna är tjänstekonceptet, vars grundläggande tanke är att en nytta skall av producenten exponeras som en avropningsbar tjänst. Trots att inte tjänste-konceptet i sig är en förutsättning för att arbeta i ett nätverk, har den modularisering av funktionalitet, vilken blir följden vid en nedbrytning i tjänster, en positiv inverkan på den eftersträvade flexibiliteten. En stor andel tjänster kommer att realiseras i form av program-varukomponenter som levererar en viss nytta. Låt oss ta ett exempel: tjänsten ”samman-ställning av invärden inför lämnande av upplysning om väderförhållanden”. Låt oss säga att denna tjänst bearbetar data från mänskliga eller maskinella vädersensorer för att sedan låta andra brukare i nätverket avropa resultatet. Många individer och system kan komma att interagera med denna tjänst – både i egenskap av brukare och som leverantörer av indata. Aktörer kommer att interagera med tjänsten oberoende av förbandstillhörighet och oberoende av i vilket materielsystem vederbörande för tillfället arbetar. Att börja tänka i nya banor samt att börja bygga system som separerar funktioner från plattformar – som den här nämnda vädertjänsten –är ett steg som för oss närmare visionen.

10.3 Förändrade tillvägagångssätt

Tittar vi mer konkret på följderna av synsättsförändringarna, framstår det som naturligt att även ett antal tillvägagångssätt på en övergripande nivå sannolikt kommer att behöva förändras. Ett exempel kan vara att i budgetarbetet avseende utveckling och vidmakthållande av den tilltagande mängden gemensamma komponenter (programvarukomponenter), som instrument för kostnadsuppskattningar inte använda sig av fördelandet av kostnader på förband och/eller materielsystem, vilket kan vara tillämpligt då vi från början känner antalet förband samt tillhörande (i princip förbandsskräddarsydda) materiel. Under de förmodade nya omständigheterna framstår detta tillvägagångssätt som ett trubbigt och inexakt redskap – ett redskap som inriktar nyttjaren mot att börja i fel ände. (En fördelning på kostnadsbärare kan

naturligtvis, om så önskas, göras som en efterkonstruktion, då vi vet svaret. Det är tanken att använda denna metod som instrument för att ta reda på svaret som inte är tillfyllest.)

Kan medlet för att uppnå detta vara hårdare och striktare samordning? Emellertid finns det alltid ett behov av att göra en avvägning mellan ”hela världen ska samordnas” (innebärande att arbetet går i stå) och ”ett begränsande av antalet kockar” (innebärande ökat inslag av så kallat stuprörstänkande – förordandet av dedikerade, speciella, lösningar för varje användningsområde – men även, med stor sannolikhet, ett mer lätthanterligt projekt).

Vi tror att budskapet istället ska formuleras med avseende på ansvarsområden. Och då inte i termer av ansvaret för samordningen i sig, utan snarare genom (inrättandet av) befattningar med ansvar för att få grepp om fundamentet för samordning – ställa sig frågan ”vad måste göras av fler än en”? Mer konkret: En befattningsinriktning med fokus på att se gemensamma beröringspunkter avseende metodik och behov av systemstöd. Detta arbete ska tillåtas kosta pengar och personalen ska utbildas i syfte att bemanna dessa befattningar. Samtliga av dem (inom statsmakternas rådandesfär) som är inblandande i kedjan ”idé till nätorienterat system med tillhörande reglemente” ska komma i åtnjutande av dylika befattningar.

10.4 Tilltagande föränderlighet

Då ett större system med lång utvecklingstid tas fram finns alltid faran att tekniken utvecklas, så att den valda lösningen är föråldrad redan då systemet tas i bruk. Om vi antar att den hittillsvarande trenden håller i sig, kommer teknikutvecklingen att i ännu högre grad accelerera. Detta är speciellt påtagligt för programvaruintensiva lösningar, det vill säga den typ av lösningar som i ökande utsträckning antas ingå i Försvarsmaktens framtida system. Vad kan vi då göra för att inte bli frånsprungna av utvecklingen?

Önskvärt är att kontinuerligt ha grepp på kraven på systemet, vilka svarar mot den metod vi vill använda. Detta arbete sker, som tidigare antytts, parallellt med metodutvecklingen. Hela denna process med att ta fram adekvat systemstöd, kan inte helt och hållet bedrivas som en skrivbordsövning, utan vid ett antal tillfällen bör systemet materialiseras i en försöksplattform/testrigg. Möjligen skulle en sådan kunna liknas vid de demonstratorer och illustratorer vi känner idag och inget hindrar att testriggen skulle kunna spela en dubbelroll. Emellertid är det skillnad. Skillnaden i upplägget mellan denna testrigg och demonstratorer och illustratorer, är att vid de tillfällen vi tycker att den inslagna vägen verkar lovande, så förfinar vi iterativt programvarukomponenterna i så stor utsträckning att de blir fäiga för användning i ett skarpt system. Själva testriggen däremot, behöver inte på något sätt vara fältmässig, ackrediterad eller svara upp mot stridens krav. Med detta upplägg vinner vi möjligheten att vara snabbfotade inom de områden där det finns störst behov av att pröva och känna sig för – metod inklusive systemstöd, samtidigt som möjligheten bjuds att avvakta med att beställa materielens mer rigida strukturer (oftast hysaren – plattformen). Vi kan, i traditionell bemärkelse, gå i produktion med en plattform, först när den behövs – men vi vet hur vi ska använda vår materiel.

Det är inte bara takten för den tekniska utvecklingen som förändras i allt högre grad. Även vår omvärld verkar i nuläget bli mer och mer oförutsägbar. Ovanstående resonemang – ”plattform först när det behövs” – är även i högsta grad tillämpligt för denna mer oförutsägbara situation.

Vem är det då som ska utföra arbetet med att pröva och känna sig för? Tanken är här att detta är en del av den normala taktikutvecklingen och de som har till uppgift att bedriva denna har också till uppgift att anlägga ett systemperspektiv. Det går också att tänka sig att deltagande i

nyss nämnda arbete sker som ett led i kompetensutvecklingen och kanske är en del i karriärvägen. Arbetet skulle sannolikt genom en sådan åtgärd kunna få rätt status. Oavsett detaljerna spelar i detta arbete även de tidigare nämnda befattningarna – vilka hade att bevaka systemsamordning – en central roll. Vidare, för att komma så nära en fullständig genomlysning av det studerade området som möjligt, bör representanter från alla tillämpliga försvarsmyndigheter delta.

I dessa sammanhang, då vi sysslar med nätsatsningar, innebärande att vi arbetar med komponenter och innebärande att vi försöker skjuta upp besluten avseende de rigida strukturerna så länge som möjligt, kommer färre av oss att få möjligheten att se systemen som helheter. Det kan till och med tänkas bli så att det inte är eftersträvansvärt att målet definieras som arbete mot den traditionella helheten – normalt materielsystemen. I detta läge uppstår ett stort behov av gemensamma referensramar – ett ramverk som ger svar på vanliga, övergripande designfrågor, i form av grundläggande riktlinjer. Dettta rättesnöre utgörs av den valda arkitekturen – en övergripande planritning för hur byggklossarna kan passa ihop.

11 Slutsatser

Den metod vi valt för att beskriva nätverksstrukturer innebär att vi utgår från idag kända industristandarder och *best practice* för distribuerade informationssystem, kompletterat med utvecklingstrender inom detta område. Utgångspunkten är att vi måste studera konkreta system, standarder och produkter för att kunna uppskatta kostnader och värdera kapacitet i förhållande till verksamhetens krav. Avgörande för om denna metod är framgångsrik är inte att vi väljer ”rätt” system som referenspunkt, utan att våra val inte kommer att avvika markant i kostnad och kapacitet från den teknologi, som slutligen kommer att väljas[24].

Omfattningen på de nätverkssatsningar som kan göras i grundalternativet (en försvarsmakt med oförändrad anslagsram på c:a 40 mdr kr/år) ger enligt vår bedömning rimliga förutsättningar att realisera huvuddelen av nu gällande målsättningar som styr inriktningen mot ett nätverksbaserat försvar, framförallt inom funktionerna Ledning och Informationshantering.

De reducerade nätverkssatsningar som kan genomföras i planeringsalternativet –3 Mdr kr/år gör det fortfarande möjligt att realisera grundläggande delar av den nödvändiga gemensamma nätverksstrukturen. Däremot kommer man inte i denna ekonomiska nivå att kunna ersätta existerande ”arvssystem” eller att tillföra nya verksamhetstjänster i någon större omfattning. Satsningen blir till stor del ett renodlat integrationsprojekt, som syftar till att länka samman och möjliggöra samverkan mellan existerande system, och till betydligt mindre del att utveckla nya tjänster. Det är nätverksgruppens bedömning att även detta är en meningsfull nivå för nätverkssatsningar. Det är dock viktigt att här framhålla att detta skulle innebära en delvis förändrad strategi för Försvarsmaktens nätverkssatsningar:

- Fokusering på närtida effekter, optimering mot kortsiktig nytta. Sådant som är svårt och därmed kostnadsdrivande väljs bort till förmån för det som bidrar till grundläggande förmågor i närtid.
- Existerande större system, t.ex. StriC ersätts inte inom perioden. Arvsystemens nytta exponeras via inkapsling. Systemens livslängd förlängs genom olika tekniska åtgärder.
- Komponenter byggs uppgiftsorienterat och inte generellt.

De slutsatser vi här formulerar och de synsätt som ligger bakom dessa avvägningar kan synas ligga långt bort från de visioner som kommit till uttryck i tidigare års FoRMA-arbete. Detta är fullt naturligt, eftersom vi först nu har satt nätverkssatsningarna i ett sammanhang, och diskuterat vad som är välavvägda nätverkssatsningar inom ramen för en komplett försvarsmaktstruktur, med givna budgetramar.

11.1 Framtida arbete

Årets arbete har resulterat i en samlad beskrivning av nödvändiga och för övrigt önskvärda komponenter i en nätverksstruktur. Fokus har mer kommit att ligga på att beskriva den infrastruktur, såväl fysisk som logisk, som möjliggör enskilda tillämpningar, än att ge exempel på sådana tillämpningar. Framförallt har vi koncentrerat arbetet på att beskriva de delar som vi uppfattar som icke valbara. För att kunna fullfölja uppgiften med att utveckla alternativa nätverksstrukturer som stöder olika försvarsmaktsinriktningar, krävs under inledningen av nästa år ett fortsatt arbete med att skapa valbara, kostnadsuppskattade

[24] Å andra sidan är vi, efter diskussioner med många olika aktörer, övertygade om att våra teknikval vore rimliga, om man idag skulle inleda utvecklingen.

tilläggspaket som kan ingå eller utgå i olika alternativa strukturer. Som nämnts ovan kommer dessa variationer framförallt att beröra kommunikationsdelarna i strukturen samt olika steg i ambitionsgrad för utveckling av nya lednings- och omvärldsuppfattningstjänster.

Interoperabilitet är en komplex fråga som vi inte kunnat ägna stor uppmärksamhet under detta år. Försvarsmakten har på central nivå slagit fast att alla nya system skall vara interoperabla, men detta kan åstadkommas på flera olika sätt, med olika ambitionsgrad och tidsplan. Många svåra avvägningar kommer att behöva göras framöver: Skall man satsa på att direkt göra utvalda plattformar eller vapensystem interoperabla med andra länder, eller skall man först satsa på förbättrad samverkan inom Försvarsmakten, eller med andra svenska civila myndigheter? Skall man i standardiseringsarbete välja att snabbt adoptera gällande, men snart obsoleta NATO-standarder, avvakta, eller ta en ledande roll i utvecklingen av nästa generation standarder? För att skapa underlag för dessa avvägningar krävs ett gemensamt arbete med internationellt deltagande för att bättre förstå i vilken nätverksmiljö framtida koalitionsoperationer kommer att genomföras.

När det gäller spel och metodutveckling för att bättre kunna värdera nyttan med olika nätverkssatsningar, så måste detta ses i ett långsiktigt perspektiv. I år gjordes ett första försök att koppla nätverksfrågorna till spelverksamheten, men verksamheten kunde inte fullföljas på grund av successiva omprioriteringar. Om spelverksamhet skall vara en fortsatt stor del av FoRMA under 2004 bör man noga överväga hur nätverksfrågorna kan integreras ännu mer i spelen, redan på planeringsstadiet.

Förkortningar

CEC: *Cooperative Engagement Capability*

CORBA: *Common Object Request Broker Architecture*

COTS: *Commercial of the Shelf*

CPU: *Central Processing Unit*

DSTL: *Defence Science and Technology Laboratory*, en forskningsorganisation tillhörande Storbritanniens försvarsdepartment.

FHS: Förvarshögskolan

FM: Försvarsmakten

FM A: Försvarsmaktens arkitektur

FMLS 2010: Försvarsmaktens ledningssystem 2010

FMV: Försvarets materielverk

FoRMA: FOI-projektet Forskningsområde *Revolution in Military Affairs*.

FTN: Försvarets Telenät

GIG: *Global Information Grid*

GTRS: Gemensamt Taktiskt Radiosystem

HKV: Högkvarteret

http: *HyperText Transfer Protocol*

KRI/LED: En avdelning inom Krigsförbandsledningen

LedSyst: Försvarsmaktens arbete med att utveckla ett nytt ledningssystem går under beteckningen LedSyst och bedrivs inom fem delprojekt; T (teknik), M (metod), P (personal), O (organisation) och GRU (gruppen för utvärdering).

LOVENTP: En samlande beteckning för de sju olika tjänstekategorier som finns i FM A; Ledning (L), Omvärldsbeskrivning (O), Verkan (V), Extern samverkan (E), Informationsinfrastruktur (N för Nätet), Transmission (T) och Plattform (P).

MOM: *Message Oriented Middleware*

NBC: *Nuclear, Biological, and Chemical* (nukleära, biologiska och kemiska)

NBF: Nätverksbaserat försvar

NCW: *Network Centric Warfare*

NEC: *Network Enabled Capability*, det brittiska begrepp som närmast liknar det svenska NBF

OPIL: Operativa insatsledningen

PerP: Perspektivplanering

QoS: *Quality of Service*

RPC: *Remote Procedure Call*

RUP: *Rational Unified Process*

SICS: *Swedish Institute for Computer Science*

SOA: *Service Oriented Architecure*

SOAP: *Simple Object Access Protocol*

WS: *Web Services*

Referenser

Alsér, Lisa (red), ”*Värdering av nätverksorienterad krigföring – förstudie*”, FOI-R— 0338—SE, FOI Systemteknik 2002.

Carling, C., Hamrin, M., Mossberg, K., Tofte J. (red), ”*FoRMA Nätverk- Sammanfattning av arbetet 2002*”, FOI-R--0943--SE, FOI Försvarsanalys 2003.

Federation of American Scientists (2003), “Cooperative Engagement Capability (CEC)”, http://www.fas.org/man/dod-101/sys/ship/weaps/cec.htm, läst 2003-11-24

Frankel, M.S. (2003), "Implementing the Global Information Grid (GIG): A Foundation For 2010 Net Centric Warfare (NCW)", Presented at the 8th International Command and Control Research and Technology Symposium, National Defense University, Washington, DC, 17-19 June 2003

Försvarsmakten (2003), *Särskild redovisning rörande Försvarsmaktens utveckling mot NBF, SR 79. HKV 2003-02-21 23 383, Underbilaga 8.2*

General Dynamics (2001), ”Geoff Hoon announces Bowman”, http://www.gdcanada.com/company_info/articles/body_art2001jul20rk6.html, läst 2003-11-27

Global-Defence.com (2001), ”Bowman misses the target”, http://www.global-defence.com/2001/CSpart1.html, last 2003-11-27

Höstbeck, L., ”*Metoder för värdering av nätverksbaserad strid – Underlagsrapport i FoRMA*”, FOI-R--0671--SE, FOI Systemteknik 2003.

Lindberg, M. & Thorén, P. (2003) ”FoRMA 2003: Nätverksanalyser”, FOI-R--1038--SE

Microsoft (2003), ”Microsoft BizTalk Server”, http://www.microsoft.com/biztalk/, läst 2003-11-24

Perry, W.; Gordon IV, J.; Boito, M. & Kingston, G. (2003), “Network-Based Operations for the Swedish Defence Forces: An Assesment Methodology”, Report No. MR-1754-Sweden, June 2003, RAND

SAP (2003), ”SAP xApps”, http://www.sap.com/solutions/xapps/, läst 2003-11-24

Sherman, J. (2003), “U.S. Navy Shifts Course on CEC”, Defence News, Vol. 18, No. 32.