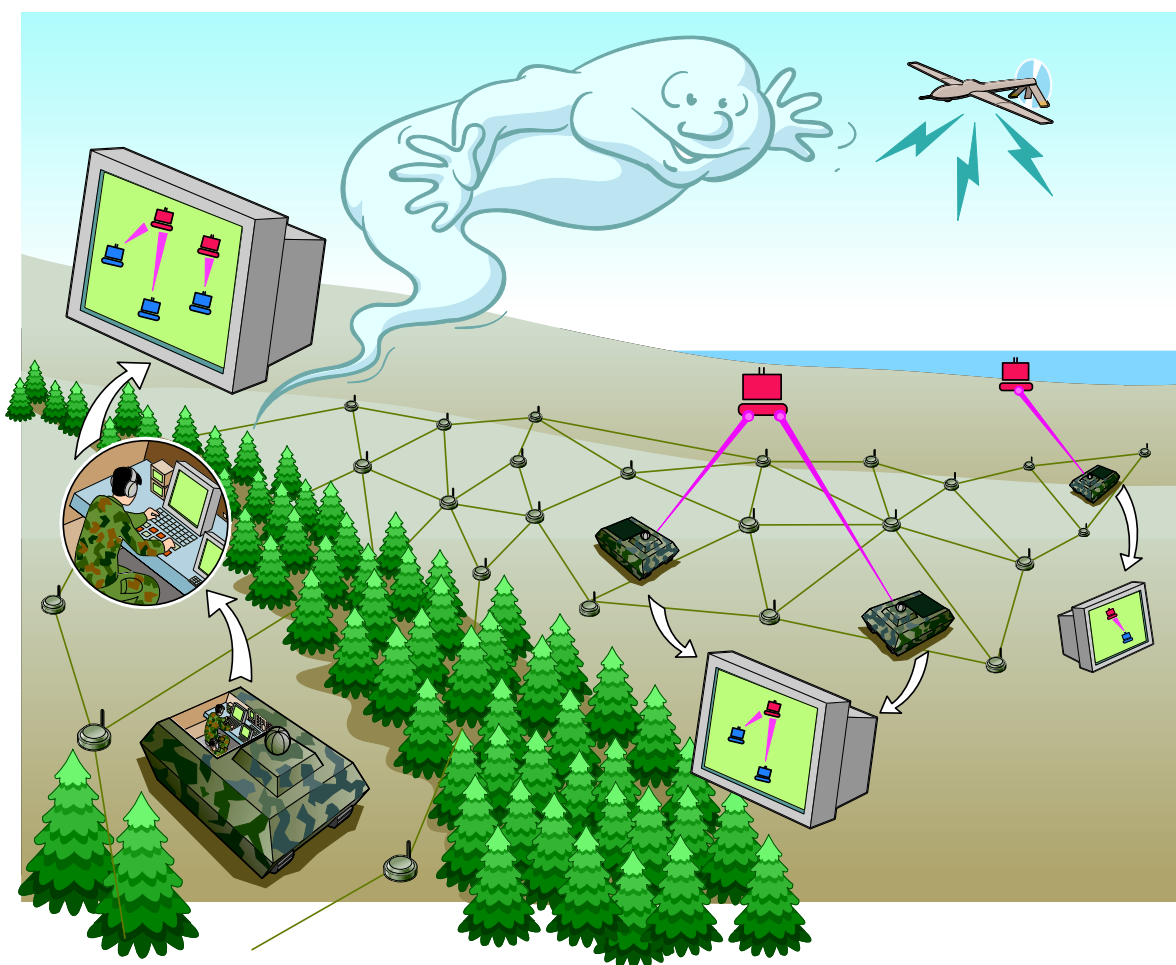


Redaktör: Lisa Alsér

Värdering av nätverksorienterad krigföring – Förstudie

Underlagsrapport i FoRMA



TOTALFÖRSVARETS FORSKNINGSPINSTITUT

Systemteknik

172 90 Stockholm

FOI-R--0338--SE

Januari 2002

ISSN 1650-1942

Metodrapport

Lisa Alsér (red)

Värdering av nätverksorienterad krigföring – Förstudie

Underlagsrapport i FoRMA

SAMMANFATTNING

Vid FOI, tidigare FOA, pågår studier kring nätverksbaserad krigföring i projektet FoRMA. Nätverksbaserad krigföring, eller dess amerikanska beteckning Network Centric Warfare, NCW, betecknar ett system för krigföring där funktionerna kan vara uppdelade på olika plattformar och samtidigt arbeta tillsammans genom ett nätverk, vilket är realiserat av informationsteknologi.

Arbetsgruppen Nätverksstrid bildades i maj 2001 och gruppens uppgift är att ta fram metoder och tillämpa dessa för att bedöma och värdera väpnad strid i nätverk. Frågeställningar vid analys av nätverksbaserad strid bör vara huruvida nätverksbaserad strid är möjlig, vad som är gränssättande samt vilka mervärden nätverksbaserad krigföring tillför framför plattformsbaserad. Särskilt ska studeras hur modeller för att representera och värdera nätverksbaserad strid kan utvecklas.

I denna förstudierapport diskuteras olika nätverksstrukturer för krigföring och olika typer av ledningsfunktioner, såsom centraliserad och distribuerad. Viktigt vid nätverksbaserad krigföring är förmågan att upprätta en lägesbild. Troligt är att man på olika nivåer i systemet vill ha tillgång till olika grad av detaljrikedom. Det är tänkbart att en sammanställd lägesbild som håller fullt tillräcklig kvalitet för att användas vid genomförandeledning, inte har detaljeringsgrad eller uppdateringshastighet som är tillräcklig för vapeninsats, varför ett ”subnät” måste dedicerats för genomförande av aktuella vapeninsatser.

Ett antal typfall har tagits fram, med vars hjälp man senare vill undersöka möjligheterna att utnyttja nätverksbaserad krigföring. Scenarierna beskriver typfallen fast mål, stridsvagn, stridsflyg, ytstridsfartyg samt ett undervattensfall. Triviala nätverk mellan ledning, sensorer och vapen för de olika scenarierna presenteras. För att studera egenskaper och effekter av ett samlat nätverk bestående av en mängd olika komponenter beskrivs också en tänkbar struktur för ett generellt nätverk.

I rapporten lyfts även några kända modelleringsmetoder fram som kan få betydelse när man ska finna en metodik och systematik vid modellering av de scenarier som beskriver nätverksbaserad krigföring.

Innehållsförteckning

SAMMANFATTNING	3
1 BAKGRUND OCH UPPGIFT	7
1.1 Uppgift och arbetsgrupp	7
1.2 Läsanvisning.....	8
2 NÄTVERKSBASERAD KRIGFÖRING	9
2.1 Aktörer i nätverket	9
2.2 Ledningens roll i nätverksförvar	9
2.2.1 Ledningens funktioner.....	9
2.3 Spaning, sensorer och ledning.....	10
2.3.1 Spaning	10
2.3.2 Sensorledning och -datafusion.....	10
2.3.3 Prognoser	11
2.4 Ledning - olika filosofier	11
2.4.1 Centraliserad	11
2.4.2 Distribuerad	11
2.4.3 Ledning i nätverket	12
2.4.4 Samverkansförmåga.....	12
2.4.5 Kommunikationsstruktur	12
2.5 Metoder för att upprätta en lägesbild	13
2.5.1 Central bild.....	14
2.5.2 Lokal bild.....	14
2.5.3 Uppgiftsspecifik bild.....	14
2.5.4 Kvalitetsmått på lägesbilden.....	14
3 METODBESKRIVNING.....	16
3.1 Definition.....	16
3.2 Trivialt och generellt nätverk.....	18
3.3 Modelleringsansats.....	19
4 TYPFALL OCH NÄTVERK	20
4.1 Scenarier	20
4.1.1 Fast mål	20
4.1.2 Stridsvagn.....	20
4.1.3 Stridsflyg.....	20
4.1.4 Ytstridsfartyg	20

4.1.5	Undervatten	21
4.2	Nätverk	21
4.2.1	Triviala nätverk.....	21
4.2.2	Generellt nätverk	27
5	MODELLERINGSMETODER	29
5.1	Modelleringsparadigmer	29
5.1.1	Ramverktyg	29
5.1.2	Generella verktyg	29
5.1.3	Distribuerad simulering.....	30
5.2	Analysmetoder	30
5.2.1	CMMS.....	30
5.2.2	Objektorienterad analys & design	31
5.2.3	Verifiering, validering och ackreditering	31
5.2.4	Fedep	31
5.3	Angränsande områden.....	31
5.3.1	Datorgenererade styrkor.....	31
5.3.2	Data- och Informationsfusion	31
6	BIBLIOGRAFI.....	33
6.1	Böcker.....	33
6.2	Rapporter	34
6.3	Tidskriftsartiklar	37
6.4	Konferensbidrag	39
BILAGA 1	- TYPFALL FAST MÅL.....	40
BILAGA 2	- TYPFALL STRIDSVAGN	43
BILAGA 3	- TYPFALL STRIDSFLYG.....	46
BILAGA 4	- TYPFALL YTSTRIDSFARTYG.....	53
BILAGA 5	- TYPFALL UNDERVATTEN.....	57
BILAGA 6	– KRAVSTÄLLARE PÅ NÄTVERKET	60

1 BAKGRUND OCH UPPGIFT

Sedan ett antal år tillbaka pågår en förändring av förutsättningarna för väpnad strid. Denna förändring möjliggörs av den snabba teknikutvecklingen, framförallt utvecklingen på informationsteknologiområdet, men också sådant som nanoteknik och miniatyrisering.

Det som är karaktäristiskt för de pågående förändringarna är att man mer och mer går över från att tänka i termer av plattformar till att tänka funktionsuppdelat och i nätverk. Förmågan som erhålls genom att medvetet och strukturerat nyttja ny teknik är så mycket större än tidigare att detta kallats en ”Revolution in Military Affairs”, RMA¹. Genom historien har vi sett ett antal tillfällen då ny teknik introducerats på ett sådant sätt att krigföringen revolutionerats.² Denna senaste RMA har ofta kommit att kallas Nätverksbaserad krigföring, eller med dess amerikanska beteckning Network Centric Warfare, NCW.

1.1 Uppgift och arbetsgrupp

Vid FOI, tidigare FOA, pågår studier kring nätverksbaserad krigföring i projektet FoRMA (Forskning om RMA). Inom ramen för FoRMA-projektet arbetar en delstudiegrupp med att utveckla och tillämpa metoder för att värdera väpnad strid i ett nätverksbaserat försvar, nätverksstrid.

Ett stringent svenskt språkbruk avseende nätverksstrid saknas fortfarande och ett antal olika formuleringar cirkulerar. I detta arbete kommer, om inget annat anges, uttryck som nätverksstrid, nätverksbaserad krigföring, nätverksstödd strid, strid i nätverk m fl användas synonymt för att beteckna ett system för väpnad strid där funktioner kan vara uppdelade på olika plattformar och samtidigt arbeta tillsammans genom ett nätverk, realiserat av informationsteknologi.

Arbetsgruppen Nätverksstrid bildades i maj 2001. Arbetsgruppens uppgift är att ta fram metoder och tillämpa dessa för att bedöma och värdera nätverksbaserad väpnad strid. De centrala frågeställningarna vid en analys av nätverksbaserad strid bör vara:

- I vilka fall är nätverksbaserad strid möjlig?
- Vad är gränssättande?
- Vilka mervärden tillför nätverksbaserad krigföring framför traditionell plattformsbaserad?

Särskilt skall studeras hur modeller för att representera och värdera nätverksbaserad strid kan utvecklas.

Arbetet rapporteras som en förstudierapport (denna rapport), en lägesrapport avseende årets arbete vid slutet av 2001 och en slutrapport avseende allt arbete andra halvåret 2002. Vidare bör projektet leverera resultat i form av en eller flera ”modellritningar”. Dessa leveranser planeras till andra kvartalet 2002.

Arbetet bedrivs av en projektgrupp bestående av kompetenser avseende analys, sensorer, vapen samt modellering och simulering. Gruppen sätts samman av personal från FOI och FMV. Till stöd för arbetet föreslås att en kontaktgrupp bestående av personer från Försvarsmakten, FMV, FOI och industrin skapas. Syftet med kontaktgruppen är att under arbetet stämma av projektets inriktning mot dels Försvarsmaktens mål och behov, dels mot industrins möjligheter att bidra.

Arbetet avgränsas till att gälla enbart väpnad strid. Explicit gäller att vi inte avser att behandla det som brukar kallas informationskrigföring, IW. Inte heller tar vi upp frågan om sårbarhet i olika nätverkskonfigurationer då detta hanteras i andra projekt vid FOI³.

1.2 Läsanvisning

Syftet med denna förstudierapport är att beskriva arbetssättet och redovisa resultatet av förstudien samtidigt som den ska fungera som en gemensam grund för det fortsatta arbetet i gruppen. Rapporten är, förutom denna inledning, uppdelad i fem avsnitt.

Avsnittet Nätverksbaserad krigföring beskriver närmare några förutsättningar och möjligheter kring nätverksstrid, speciellt med avseende på ledning.

Avsnittet metodbeskrivning innehåller en närmare redogörelse för arbetssättet och den metod man föreslår för fortsatt arbete. Eftersom arbetet har ett uttalat iterativt inslag kommer dessa metoder att förfinas och vidareutvecklas vartefter arbetet fortskrider. En slutlig redogörelse för metod och erfarenheter kan presenteras i arbetsgruppens slutrapport.

Det avsnitt som kallas Typfall och nätverk beskriver de fem typfall vi arbetar med och de olika nätverkskonfigurationerna vi avser att pröva typfallen mot. De beskrivningar som återfinns i förstudierapporten gör inga anspråk på att vara fullständiga, utan återger typfall och nätverksalternativ så långt de hunnit beskrivas då förstudiefasen avslutas.

Modelleringsmetoder är det avsnitt som översiktligt beskriver olika metoder för att modellera nätverksstrid. Här presenteras några intressanta tekniker som antas vara betydelsefulla för att finna metodik och systematik vid modellering av scenarier som beskriver nätverksstödd krigföring.

Slutligen finns ett avsnitt kallat bibliografi som utgör en uppräkningslista av böcker, rapporter, tidskriftsartiklar och konferensbidrag som behandlar nätverkskrigföring. För varje skrift som listas finns också en kort presentation. Tanken är att denna lista skall fungera som en slags litteraturlista för arbetsgruppen.

¹ RMA-begreppet har i svenska dokument ofta kopplats till de tre begreppen Dominant Battlespace Awareness, DBA, Precision Engagement, PE och Decision Support DS.

² Se till exempel FOI-tidningen Framsyn nr 2 2001, sid. 40-41.

³ Analys av nätverkskonfigurationer kommer t ex att behandlas i det kommande projektet Metoder för analys av nätverk, METANET med start 2002.

2 NÄTVERKSBASERAD KRIGFÖRING

2.1 Aktörer i nätverket

En av grundteserna när det gäller nätverksbaserad krigföring är att förmågan hos systemet är större än hos ett plattformsbaserat system beroende på att många, till form och förmåga olika aktörer, intressenter, tjänster och funktioner finns representerade i samma nätverk. Detta leder i sin tur att det finns många olika "kravställare" på nätverkets förmåga. I denna förstudierapport har vi inte haft ambitionen att identifiera alla dessa kravställare och till dem associerade krav, men en sammanställning över tänkbara kravställare redovisas i bilaga 6. I avsnitt 2.2 till 2.4 nedan diskuteras några kravställare och till dem knutna intressen och krav.

2.2 Ledningens roll i nätverksförvar

Tanken med nätverksbaserad krigföring har sin förebild i den dynamik i tillväxt och konkurrens som har utvecklat sig i den moderna ekonomin. Denna förväntar sig ökande utdelning på investeringen, utmärks av tävling inom och mellan näringsgrenar (ecosystems) och är ständigt utsatt för/utsätter konkurrenterna för tidspress. Detta har t ex lett till utveckling av analysmetoder för att analysera stora datamängder. Viktiga förmågor är t ex strukturanalys, nätverksanalys, prognostisering, kundprofiler med t ex beteendemönsteranalyser som används för att hitta kreditkortsbedrägerier etc.

När teorierna överförs till militära behov är det sådant som att metoderna för sensoranalys förbättrats, ofta inom civila industrin, till att kunna ge automatisk analys och igenkänning av objekt eller händelser som skapar nya möjligheter. Denna teknik skapar förutsättningar för att bygga upp komplexa beslutsstödssystem inom försvaret på samma sätt som man idag gör inom den ekonomiska sektorn.

Potentialen med nätverksbaserad krigföring ligger framför allt i dynamiken; snabbare och säkrare informationsinhämtning genom samverkan av sensorer, bättre förmåga att ta beslut (med delvis automatiserad beslutsförmåga och beslutsstöd) och en förmåga till samlad insats utan att behöva ha resurserna samlade och utan att behöva göra tidsödande förflyttningar och omflyttningar. Detta kan också göra krigföringen mindre sårbar.

Förebilden för det är den potentiella förmågan som finns i konceptet att knyta samman sensornätverk, ledning och vapen i ett nätverk som givit namnet åt NCW. NCW emanerar från begreppet "Network Centric Computing" vilket använts framförallt för kommersiella ändamål av företrädare på framkant i sektorer som industri och banker. Detta begrepp kallas också NCO, Network Centric Operations.

2.2.1 Ledningens funktioner

Ett ledningssystem består av ett antal informationsflöden i olika riktningar, både uppåt och nedåt i ledningshierarkin. Flödet i riktning uppåt kan vara att förse ledningscentraler med data från sensorer och egna enheter för att kunna bearbeta dessa till en sammanhållen och om möjligt entydig lägesbild som beslutsunderlag för hotprognoser och resursfördelning. I riktning nedåt

kan flödet syfta till att förmedla order och distribuera fusionerade lägesbilder från ledningscentraler till den lokala nivån.

En presenterad lägesbild kan vara av flera olika typer, t ex fusionerad lägesbild som anger upptäckta mål och hotprognoser eller fusionerad lägesbild som anger sensortäckning och förmåga mot olika mål för ett område. Kommunikationens täckning och tillförlitlighet är också viktig i detta sammanhang. Sådan information är viktig för att kunna bedöma tillförlitligheten hos de presenterade lägesbilderna.

2.3 Spaning, sensorer och ledning

2.3.1 Spaning

Spaning är medel för informationsinhämtning och kan delas in i två huvudtyper:

Kontinuerlig och yttäckande spaning

Syftet med den kontinuerliga spaningen är att ge en kontinuerligt uppdaterad lägesbild (gärna fusionerad) som t ex anger sensortäckning och upptäckta mål. Yttäckande kontinuerlig spaning kan också vara ett medel för att kartlägga och följa fiendens aktiviteter. Detta kan gälla både fordonsrörelser och t ex störning.

Reaktiv spaning

Den reaktiva spaningen är behovsstyrd och sätts in för att öka informationsmängd och kvalitet i ett område eller mot ett mål som upptäckts av den kontinuerliga spaningen. Syftet kan vara klassificering eller identifiering av målet eller målföljning och noggrannare inmätning av mål som ett led vid vapeninsats. Vid reaktiv spaning måste sensor väljas för att klara den för uppgiften specificerade informationskvaliteten och lämplig plattform placeras ut i målets närhet (inom täckningsområdet).

2.3.2 Sensorledning och -datafusion

För att korrekta beslut ska kunna fattas är det viktigt att inte bara kunna beskriva läget i nutid utan också hur det har förändrats under en längre tidsperiod för att kunna upptäcka att "något är på gång" innan det har hänt. Det är viktigt att ha så god information som möjligt vid planering av en insats eftersom detta kan inverka på val av insatsmedel, ledningsfilosofi och riskbedömningar vilket på ett avgörande sätt kan påverka utgången och resultatet vid insatsen. Detta leder till kontinuerliga behov av sensorledning och sensordatafusion

Sensorledning

Sensorledning är en viktig funktion i ett nätverksorganiserat ledningssystem med tillgång till många sensorer. Sensorledningens uppgift är att planera och övervaka den kontinuerliga spaningen så att den kontinuerligt anpassas till hotprognoser och tillgodoser önskade krav på prestanda för lägesbildsgenerering. Uppgiften sensorledning för reaktiv spaning kan antingen tilldelas centrala sensorledningen eller vara utlokaliserad till lokala nivåer i samband med delegerat insatsansvar.

Sensordatafusion

Syftet med sensordatafusion är att kunna sammanställa information från flera olika typer av sensorer men också flera av samma typ för att kunna presentera en sammanhållen lägesbild. Ett annat syfte är att kunna producera högre informationskvalitet genom att förstärka t ex klassificerings-, identifierings- och målföljningsförmåga genom att kunna kombinera data från flera sensorer gällande ett och samma mål.

Svårigheter finns dock att använda denna typ av teknik. Samtidigt som informationen om ett visst mål kan öka genom att fusionera information så kan osäkerheten i lägesbilden öka vad gäller t ex antal mål, målvägar etc.

2.3.3 Prognoser

En intressant aspekt på sensordatafusion och beslutsstödsförmåga är möjligheten att producera prognoser utifrån kontinuerlig uppdatering av stora mängder sensordata tillsammans med erfarenhetsdatabaser. En situation kan jämföras med tidigare lagrade situationer vilket innebär att även mindre förändringar (tendenser) som sker fortlöpande under en längre tid kan upptäckas. Prognoser kan t ex förutsäga kommande händelseutveckling eller ändrade resursbehov utifrån förändringar av komplexa samband i lägesbilden, exempelvis trafikflödesstruktur i ett område.

2.4 Ledning - olika filosofier

2.4.1 Centraliserad

Centraliserad ledning innebär att man lokalt utför order uppifrån med litet utrymme för egna initiativ. Detta kan vara en lämplig lösning när den bästa lägesbilden finns i t ex en ledningscentral. Förmågan kan dock förbättras genom lokalt informationsbidrag från lokala enheter.

Ett exempel på centraliserad ledning är flygledning där ansvaret för en uppgifts utförande i allmänhet ligger på en ledningscentral och där den utförande enheten är ett instrument för detta. Denna strategi bygger på ett antagande att den bästa scenarioinformationen och analysförmågan för framtagande av lägesinformationen för att leda och invisa en insats finns på en central nivå. Ett flygplans egna sensorer har kortare räckvidd och är främst avsedd för slutfasstyrning. Dessutom är piloternas analysresurser i form av data och utrustning begränsad.

2.4.2 Distribuerad

Distribuerad ledning kan innebära att uppgiften utlokaliseras som lokala uppdrag med stort utrymme för självständig utformning. Behov av att kunna rekvirera resurser uppifrån för att kunna utföra uppgiften finns. Kontrollen från den centrala ledningen är liten avseende exakt var, hur och när uppgiften utförs.

Distribuerad ledning har den största fördelen när man i den centrala ledningen har knapphändig lägesinformation på detaljnivå och förutsättningarna är bättre lokalt att besluta hur verksamheten ska bedrivas.

Uppdragstaktik är en form av distribuerad ledning och har traditionellt varit ett viktigt begrepp i markledning och markstridssammanhang. Lägesuppfattningen är i ledningscentralerna ofta diffus

vad gäller detaljer. Detta innebär att beslut om insats och insatsorder blir diffusa vad gäller om, var och hur en insats ska genomföras och antar snarast formen av diskussion mellan olika beslutsnivåer och de som ska utföra uppdraget.

Ledning av sjöstrid karaktäriseras av att stridsledningen i många fall ger insatsorder av mer allmän karaktär där det konkreta insatsbeslutet utlokaliseras till lägre nivåer. Detta kan t ex grunda sig på hotbild och handlingsregler som resulterar i mer generella insatsbeslut, t ex insats sätts in när främmande ubåt lokaliseras. Detta lämnar stort lokalt utrymme att tolka och bedöma de potentiella hot som lokaliseras och relatera dessa till rådande beslutsramar. Detta innebär att stort och självständigt ansvar för insats ges till den lokala ledningen på t ex ett fartyg.

2.4.3 Ledning i nätverket

Nätverksstrukturen har behov av både centraliserad och decentraliserad förmåga, samt möjlighet att optimera växelverkan mellan dessa. En viktig funktion i detta sammanhang är ett beslutstöds-system som kan utvärdera informationssituationen på olika nivåer och avgöra var den lämpligaste beslutsnivån är och vilken grad av självständighet som ska tillåtas vid olika uppdrag.

Ett specialfall i detta sammanhang är sensor- till- verkanskedjan där det kan vara väsentligt för tids- och rumsprecision att en snabb och väl kontrollerad process uppnås. I detta fall kan, om tillräckliga resurser föreligger vad gäller information, spaningsmedel och insatsmedel, en centraliserad ledning av förloppet vara att föredra. Detta speciellt ur ett tidsoptimeringsperspektiv eftersom flera beslutsprocesser innebär ökad tidsfördröjning i kedjan.

Som en följd av nätverksorganisering och ökat användande av sensorer med tillhörande autonomitet och analysförmåga ökar möjligheten att ändra och förbättra beslutsläget på olika ledningsnivåer. Detta kan t ex innebära att i bästa fall finns samma information tillgänglig i ledningscentralen som ute på fältet, t ex i ett flygplan, fartyg och ett markfordon. Detta kommer i sin tur att i olika utsträckning medge en större möjlighet att välja ledningsstruktur och beslutsnivå för olika situationer. Ett sådant val kan till exempel vara hur man vill optimera insatsen med avseende på tid eller säkerhet.

2.4.4 Samverkansförmåga

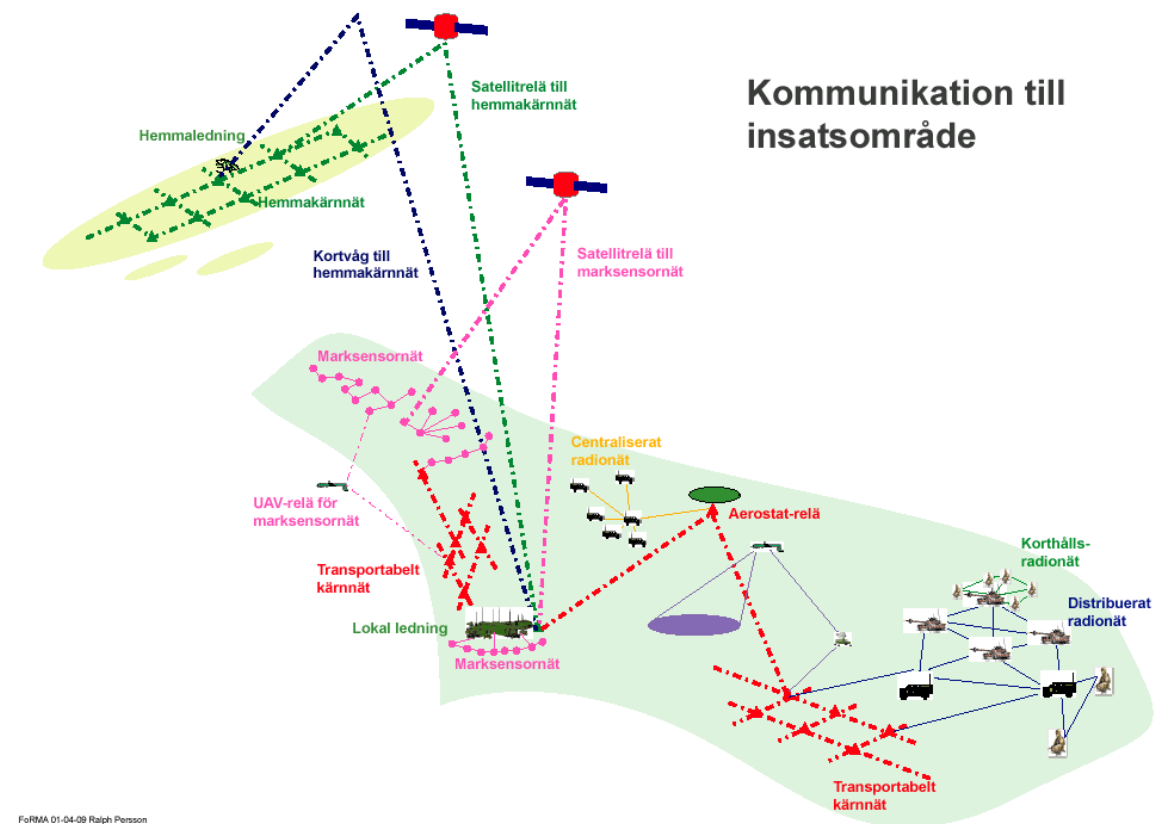
Som ett resultat av de olika förutsättningarna för ledning så har olika kulturer och språk för ordergivning utvecklats. Förståelsen för order i de olika verksamhetsgrenarna är beroende av kännedom om hur denna kultur ser ut.

För att kunna skapa en god och flexibel samverkansförmåga så är det nödvändigt att kunna hantera de olika behoven av ledning och ha ett gemensamt lednings- och orderspråk samt kunskap om hur man leder i andra delar. Med tillgång till de möjligheter som en nätverksorienterad ledningsstruktur kan ge kan det vara möjligt att skapa en flexibel och situationsanpassad ledning med skraddarsydd besluts- och ledningsfilosofi med samverkan mellan olika försvarsgrenar.

2.4.5 Kommunikationsstruktur

För alla nätverksanslutna resurser behövs kommunikation för att förmedla information och för att vid behov möjliggöra snabb insats. Detta inkluderar möjligheter till talsamband inom lokala

ledningsplatser och mellan lokala ledningsplatser och den centrala ledningen. För all denna kommunikation behövs en kombination av fasta och mobila kommunikationskomponenter.



Figur 1. Exempel på beskrivning av kommunikationsstruktur.

2.5 Metoder för att upprätta en lägesbild

Under diskussioner i arbetsgruppen har det framkommit att det finns ett behov av att definiera vad vi menar med en lägesbild och hur en sådan kan upprättas. En extrem tolkning av informationsöverläge för nätverksstrid skulle kunna vara att en lägesbild upprättas med sådan detaljnoggrannhet att den i sig är tillräcklig för att leda en vapeninsats och att denna lägesbild alltid finns tillgänglig på alla nivåer i systemet.

En mer nyanserad tolkning är sannolikt att man på olika nivåer i systemet har tillgång till lägesbilder som förvisso bygger på samma information men som presenteras med olika grad av detaljrikedom. Vidare är det fullt tänkbart att den sammanställda lägesbilden håller fullt tillräcklig kvalitet för att användas vid genomförandedledning men att detaljeringsgrad eller uppdateringshastighet inte är tillräcklig för vapeninsats varför ett "subnät" av sensorer måste dedicerats enbart för genomförande av insatsen. Dessa sensorer skulle då mer eller mindre direkt mata skjutande enhet/vapnet med information om målet.

Alberts m fl¹ talar om vad man kallar "Mission Specific Sensor Network", d v s för uppgiften särskilt sammansatta nätverk av sensorer. Deras argument är att man för vissa uppgifter kräver en hög detaljeringsgrad (High Level of Battlespace Awareness). Detta uppnås bäst genom att man tilldelar en "sensor network commander" rätten att nyttja tilldelade sensorer såsom det bäst

passar för uppgiften. Ett sådant nyttjande kan vara att en specifik sensor direkt matar en skjutande enhet eller ett vapen med målläge i realtid.

För att ha en lägesbild att utgå ifrån måste information från ett flertal källor sammanställas på något sätt. Förutom att samla information från sensorsystem som radar, sonarer eller spanings-UAV:er handlar det om att hämta data ur databaser, t ex i syfte att identifiera fartyg och flygplan som syns på sensorerna. Vi har preliminärt identifierat tre olika sätt att skapa en lägesbild:

2.5.1 Central bild

Data/information från alla relevanta sensorer samlas centralt och en lägesbild sammanställs. Denna lägesbild distribueras sedan till alla som ska eller vill ha den. Detta kan lösas antingen genom "broadcasting" där bilden skickas ut blint och alla som är intresserade tar emot den eller genom ett prenumerationsförfarande där den som är intresserad av en viss bild anmäler detta i ledningssystemet och sedan får bilden skickad till sig. Fördelen är att alla får samma information, nackdelen är att bilden sannolikt tar viss tid att sammanställa.

2.5.2 Lokal bild

Lägesbilden byggs upp lokalt hos alla enheter som vill ha den genom att man prenumererar på sensordata/information som man själv sammanställer. Om man i ett sådant system kan välja vilka sensorer i nätet man vill nyttja finns ingen garanti för att alla har samma bild. Å andra sidan garanteras man att alltid få en bild som passar för de egna behoven, givet att sensorresurserna är tillräckliga.

2.5.3 Uppgiftsspecifik bild

Den tredje modellen innebär att en uppgiftsspecifik bild skapas i likhet med idén om "Mission Specific Sensor Network" som beskrivs ovan. Det skulle kunna innebära t ex att man under en begränsad tid i ett begränsat området dedicerar ett antal sensorer till en specifik uppgift. Från dessa byggs sedan en lägesbild upp hos eller distribueras till en entydigt definierad grupp av mottagare.

Det fortsatta arbetet får visa vilken typ av lägesbild som är lämplig vid vilka situationer. Sannolikt måste olika sätt användas beroende på vilka förutsättningarna är. Det som kommer att vara avgörande för hur lägesbilden byggs upp och används är den kvalitet i lägesbilden som kan uppnås.

2.5.4 Kvalitetsmått på lägesbilden

För att kunna bestämma hur bra en lägesbild är, d v s vilken kvalitet den har bör ett antal kvalitetsmått på lägesbilden definieras. Dessa bör sedan relateras till vilken kvalitet som krävs på olika nivåer. Exempel på sådana mått kan vara:

- Uppdateringstid – Hur "gammal" informationen som presenteras i genomsnitt är. Detta blir i sin tur en summa av hur lång tid det tar att skapa lägesbilden och hur ofta en ny bild sänds ut.

- Lägesfel – Det genomsnittliga felet i mållägen beroende på tidsfördröjningar i överföring och onoggrannhet i sensorsystemen.
- Gemensamhet – Grad av gemensamhet i bilden hos olika enheter.

I det fortsatta arbetet bör relevant mått identifieras och definieras liksom krav på olika nivåer relaterade till dessa mått.

¹ Se Alberts, Garstka, Stein, Network Centric Warfare: Developing and Leveraging Information Superiority, 2nd Edition, CCRP, 2000.

3 METODBESKRIVNING

Arbetsmässigt delas uppgiften i fyra delmoment kallade Definition (1), ”Trivialt” nätverk (2), ”Generellt” nätverk (3) och Modelleringsansats (4). De fyra momenten beskrivs mer ingående nedan.

Under hela arbetets gång planeras att använda fem olika typfall för att analysera förmågan till nätverksstrid. De fem typfallen har valts efter att de har olika karaktär och förväntas därför kunna belysa olika problemställningar. De fem typfallen har kallats Fast mål, Stridsvagn, Ytstridsfartyg, Stridsflyg och Undervattensmål. De beskrivs närmare i avsnittet Typfall och nätverk nedan.

Tidsmässigt genomförs arbetet i två faser, en förstudiefas och en huvudstudiefas. Under förstudien planeras arbetet, grundläggande definitioner och avgränsningar görs samtidigt som kunskap om värdering av nätverksstrid inventeras. Arbetsmodellen löps igenom översiktligt i syfte att identifiera svagheter och utvecklingsbehov. I och med denna rapport avslutas förstudiefasen. En stor del av momentet Definition sker under förstudiefasen.

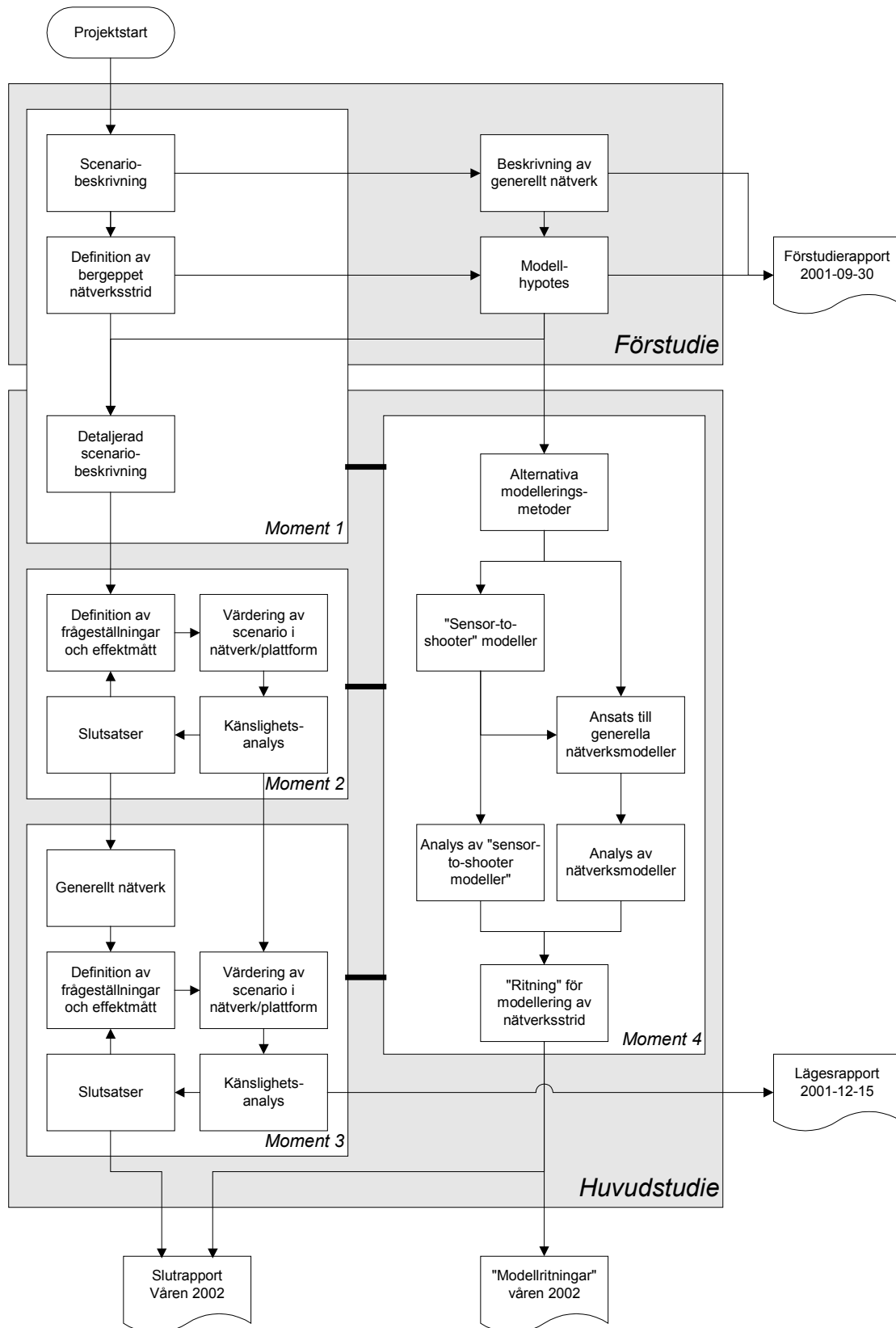
Under huvudstudiefasen slutförs Definitionsmomentet. Därefter genomförs först momentet Trivialt nätverk och därefter momentet Generellt nätverk. Parallellt med att dessa två moment pågår startas och drivs arbetet i momentet Modelleringsansats. Tanken är att momenten ska dra nytta av varandra såtillvida att analysmetoder som utvecklas i momenten (2) och (3) skall kunna läggas in i de modellidéer som utvecklas i moment (4). Modellidéerna skall sedan kunna användas i värderingen under momentet (2) och (3).

3.1 Definition

Momentet Definition (1) är centralt för det fortsatta arbetet. Under detta moment samlas grundläggande kunskap in samtidigt som förutsättningarna för analys av nätverksstödd strid formuleras. Det viktigaste arbetet som görs under definitionsmomentet är att de fem typfallen vi avser att arbeta med formuleras. Typfallen presenteras längre fram i rapporten.

Vidare skall under definitionsmomentet begreppet ”nätverk” och ”nätverksstrid” undersökas i den meningen att olika sätt att organisera och nyttja nätverket skall identifieras. Detta är en förutsättning för att kunskap om teknik, t ex sensorer och vapen, skall kunna analyseras i det vidare arbetet. Inriktningen är att inte begränsa oss till en formulering utan i arbetet pröva olika alternativa sätt att organisera nätverket.

En av grundtankarna är att processen till del skall vara iterativ såtillvida att såväl beskrivningen av typfallen som nätverket hela tiden förfinas vartefter arbetet fortskrider. Särskild vikt skall läggas vid att hela tiden dokumentera de förändringar som sker och att för varje moment som genomförs tydligt dokumentera den version av typfall respektive nätverk som används.



Figur 2. Arbetschema som beskriver de fyra delmomentet och indelningen i en förstudiefas och en huvudstudiefas, samt de leveranser som planeras 2001-2002.

3.2 Trivialt och generellt nätverk

De två momenten trivialt respektive generellt nätverk följer bägge i princip samma arbetsprocess. Utgående från de nätverksbeskrivningar som tagits fram i definitionsmomentet identifieras de frågeställningar som är kritiska. För att kunna jämföra nätverksstrid med traditionell plattformstrid definieras ett eller flera effektmått. Effektmåtten bör vara sådana att de kan användas i samtliga typfall. Exempel på effektmått kan vara:

- Tid från målupptäckt till bekämpning
- Grad av precision i bekämpningen
- Kostnad (i tid, pengar eller personal) för att bekämpa med sannolikhet P.

En värdering sker för varje typfall med hjälp av de framtagna effektmåtten och för varje fall görs en känslighetsanalys i avsikt att bedöma hur känsligt systemet är för förändringar i indata. Ur denna känslighetsanalys bör det gå att få fram en bild av vilka parametrar som är gränssättande. Denna del av processen har ett tydligt iterativt inslag då det är mycket troligt att slutsatserna av värderingen och känslighetsanalysen leder till att de framtagna effektmåtten behöver förändras.

Skillnaden mellan de två momenten trivialt respektive generellt nätverk ligger i vilken nätverkskonfiguration vi arbetar med. Ett trivialt nätverk anses vara den enklaste tänkbara kombinationen sensor-beslutsfattare-vapen (sensor-to-shooter) som analyseras för vart och ett av typfallen.

Vi behöver inte använda någon exakt modell av sensorer, plattformar eller vapensystem utan kan använda "generiska" system, såsom radar, stridsflygplan eller sjömålsrobot utan angivande av typ eller nationalitet. Dock är det av spårbarhetsskäl vettigt att då det är möjligt nyttja de spelkort som finns tillgängliga. Det triviala nätverket bör analyseras m a p:

- Tidsfördröjningar
- Skjuttider
- Måldynamik
- Positionsnoggrannhet

Syftet är att identifiera vilka faktorer som är eller kan vara gränssättande. Genom att jämföra respektive typfall mot en traditionell plattformorienterad organisation fås en idé om vilka mervärden som ett nätverksbaserat försvar kan tillföra.

För nästa arbetsmoment utvidgas det triviala nätverket till ett generellt nätverk med n stycken noder. Inledningsvis görs analysen av de enkla typfallen i detta utvidgade nätverk. Detta bör sedan utvecklas till att även omfatta nätverkets förmåga till att hantera flera samtidiga fall. Särskilt skall studeras huruvida nätverkets funktion degraderar vid flera samtidiga uppgifter. Förutom de fyra parametrar som nämns ovan bör nätverket analyseras m a p datamängder och kommunikationskapacitet. Särskilt skall studeras om den så kallade Metcalfs lag¹ är tillämplig för nätverksstrid.

3.3 Modelleringsansats

Parallellt med analyserna i moment 2 och 3 ovan bör olika metoder för att modellera nätverksstrid studeras. En tydlig ansats för modellering av nätverksstrid bör genomföras som ett separat moment. I detta moment skall ingå att välja modelleringsmetod. Två ”huvudmetoder” som bör studeras är ”traditionell” modellering i något ramverktyg, t ex Flames, respektive System Dynamics genom t ex iThink. Under definitionsmomentet identifieras ytterligare alternativ till modelleringsmetoder. Resultatet av detta bör inte vara en fullständig modell av nätverksstrid, enbart en prototyp eller ”modellritning” som sedan kan vidareutvecklas i ett separat arbete. Utdata från sådana modeller skall knyta an till de analytiska mått som definierats i moment två och tre ovan.

Frågan om en fullständig modell skall utvecklas bör tas upp till beslut i särskild ordning då samtliga arbetsmoment är genomförda.

¹ Metcalfs lag säger att förmågan i nätverket ökar som kvadraten på antalet noder.

4 TYPFALL OCH NÄTVERK

Här beskrivs kortfattat de fem olika scenarierna som ska studeras. En omfattande redogörelse för varje scenario finns i bilaga 1-5.

4.1 Scenarier

4.1.1 Fast mål

I typfallet fast mål har en artillerikanon beskjutit en civil by. Beskjutningen upptäcktes av våra sensorer som medgav beräkning av kanonens position. Ett av våra attackflygplan som var i luften blir beordrat att bekämpa den upptäckta kanonen. Anfallet försvåras av att artillerikanonen är placerad intill ett sjukhus där flyktingar passerar på en närliggande väg. Typfallet fast mål beskrivs närmare i bilaga 1.

4.1.2 Stridsvagn

I det typfallet stridsvagn föreligger höjd beredskap men ingen direkt krigssituation. Den höjda beredskapen föranleder våra styrkor att upprätthålla en allmän yttäckande luft- och markbaserad spaning samt ökad övervakning av hamnar och flygplatser för incidentberedskap och upprätthållande av territoriell integritet. I anslutning till ett hamnområde har en främmande stridsvagn observerats.

De svenska styrkornas uppgift är att upptäcka och lokalisera stridsvagnen för att sedan följa denna och genomföra en vapeninsats. Reaktiv spaning bedrivs med en liten UAV och stridsvagnen bekämpas med en fiberoptisk robot. Typfallet stridsvagn beskrivs närmare i bilaga 2.

4.1.3 Stridsflyg

Typfallet stridsflyg består av ett läge med viss höjd beredskap. Våra styrkor har bl a som uppgift att skydda ett viktigt fast markmål samt övervaka och hävda ett territorium som avgränsas av en bestämd gräns t ex en territorialvattengräns. Målet anfalls utan särskild förvarning av motståndarens attackföretag bestående av fyra attackflygplan och två eskorterande jaktflygplan. Vår sida har en flygande spaningsradar, en kustkorvett samt en fast radarstation alternativt en aerostat med radar som sensorer. Vår sida har som vapen luftvärnsrobotar på kustkorvetten, luftvärnsrobotar vid målet samt jaktflyg. Vår sida har även ett nätverksbaserat ledningssystem med en central beslutsfattare. Typfallet stridsflyg beskrivs närmare i bilaga 3.

4.1.4 Ytstridsfartyg

En fregatt från stormakt A som vägrar lyda order från sin egen försvarsmakt närmar sig en svensk konvoj på väg ut från Göteborg mot engelska kanalen. Konvojen transporterar svensk trupp på väg mot en internationell operation som stormakt A har intresse av att fördröja. När fregatten bedöms utgöra ett hot mot den svenska konvojen och alla försök att få den att vända misslyckats beslutar den svenska operativa insatsledningen att den skall sänkas med sjömålsrobot eller styrda bomber. Uppgiften faller på den insatsstyrka som skapats för att skydda konvojen. Typfallet ytstridsfartyg beskrivs närmare i bilaga 4.

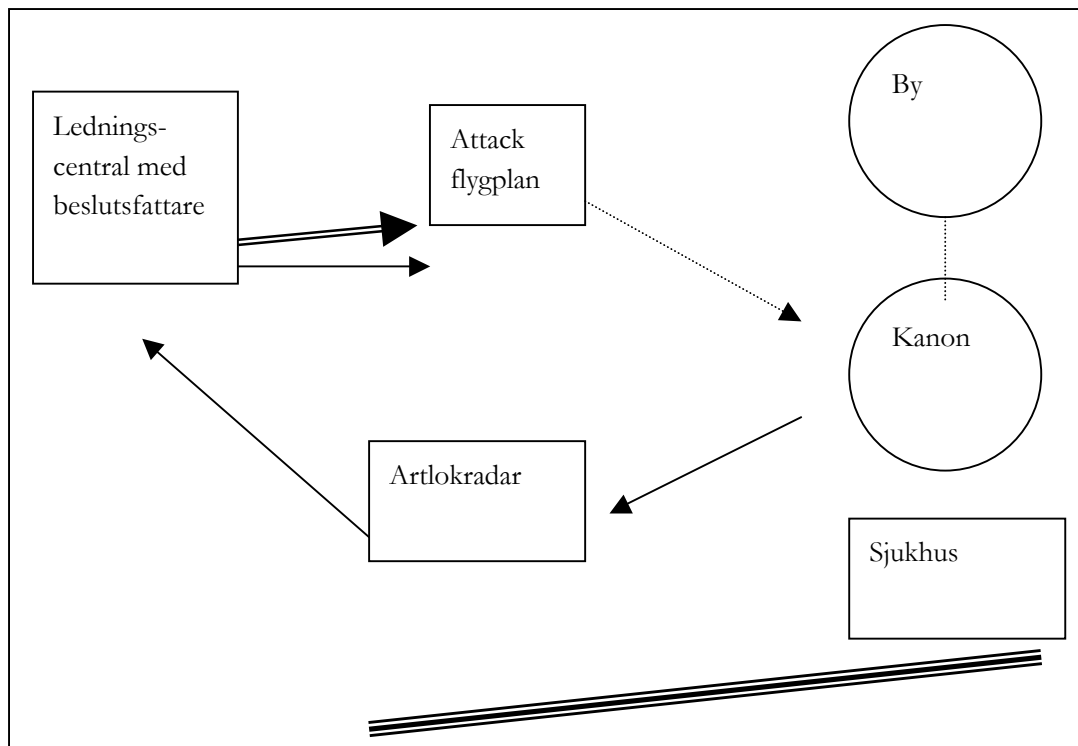
4.1.5 Undervatten

Under ett uppdrag att skydda fartyg i en konvoj upptäcker vår spaning en fientlig ubåt. Vår ubåt som finns i närheten får order att bekämpa motståndarens ubåt med hjälp av information erhållen via en fiberoptisk kabel. Med hjälp av målinformation från utplacerade spaningssensorer får vår ubåt tillräcklig målinformation för att kunna skjuta torped mot målet. Målet bekämpas och verkansvärdering sker via spaningssensorerna. Typfallet undervatten beskrivs närmare i bilaga 5.

4.2 Nätverk

I denna studie är arbetet tänkt att delas upp genom att ett trivialt nätverk först studeras, vilket innefattar olika enheter i ett och samma scenario. Med ett trivialt nätverk menas här att minsta antal noder i nätverket som krävs för att realisera kedjan sensor-beslutsfattare-vapen tas med i värderingen. Med generellt nätverk menas ett "komplett" nät med ett flertal, redundanta, noder och alternativa kommunikationsvägar. Inom ramen för det generella nätverket kan enheter och händelser från alla typfallen läggas samman i ett gemensamt scenario.

4.2.1 Triviala nätverk



Figur 3. Schematisk beskrivning av ett trivialt nätverk för typfallet fast mål.

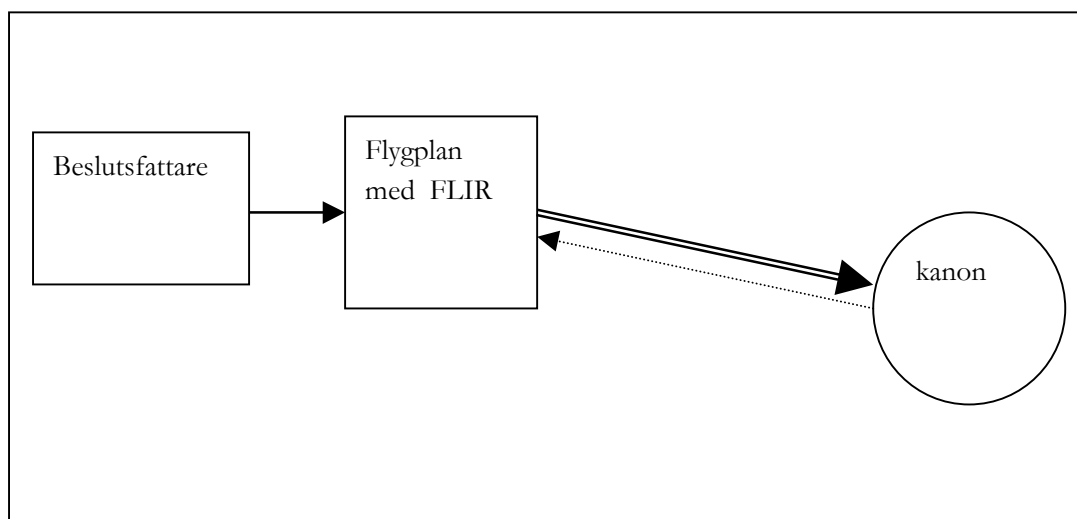
Fast mål - nätverk

I ett trivialt nätverk för fast mål upptäcktes en skjutande kanon (figur 3) av vår artillerilokaliseringsskärmar som sänder sin information till en beslutsfattare placerad i en ledningscentral.

Beslutsfattaren beordrar ett attackflygplan att bekämpa kanonen med en robot. Verkan av insatsen kontrolleras med hjälp av en UAV som sänds in över målet efter att anfallet utförts.

Fast mål - Plattformsorienterat alternativ

I det plattformorienterade nätverket i typfall fast mål upptäcker attackflygplanet en skjutande kanon med hjälp av sin FLIR. Piloten avfyra en robot mot kanonen.



Figur 4. Schematisk beskrivning av ett plattformorienterat alternativ för typfallet fast mål.

Stridsvagn - nätverk

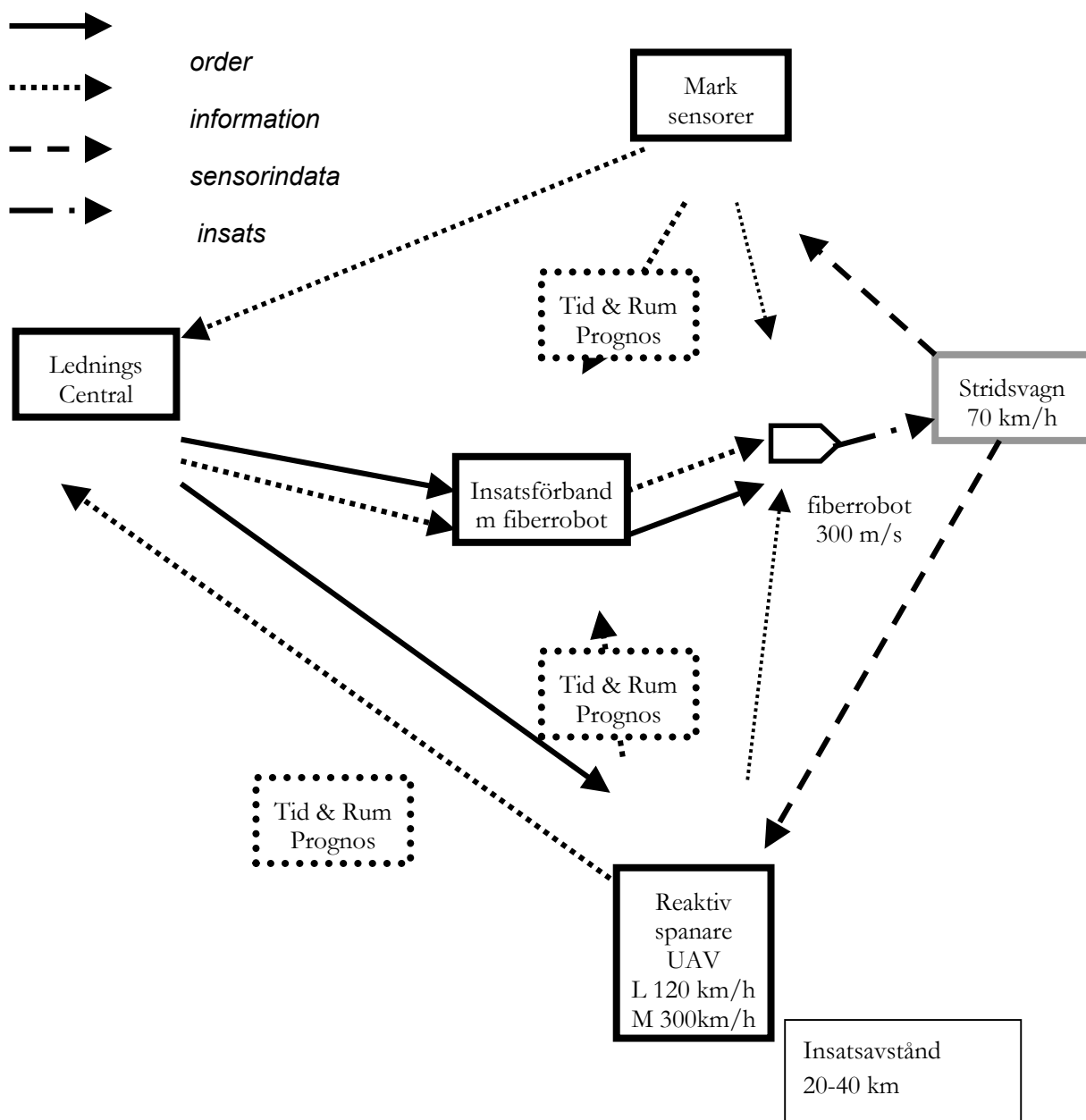
Stridsvagn i rörelse upptäcks av marksensorer placerad med 5 km avstånd längs en väg. Ett larm sänds till ledningscentralen. Ledningsfunktionen tar beslut om möjlig insats kombinerad med reaktiv spaning för att identifiera det upptäckta målet. Order om reaktiv spaning med en liten UAV skickas till en spaningsenhet.

Information från den reaktiva spaningen skickas till ledningscentralen som beslutar om insats med fiberoptisk robot. Roboten har GPS och uppdateras kontinuerligt under insatsen med prognoser om målets koordinater vid träfftilfället. Dessa koordinater erhålls via data från marksensornät och reaktiv spaning som bevakar målet kontinuerligt.

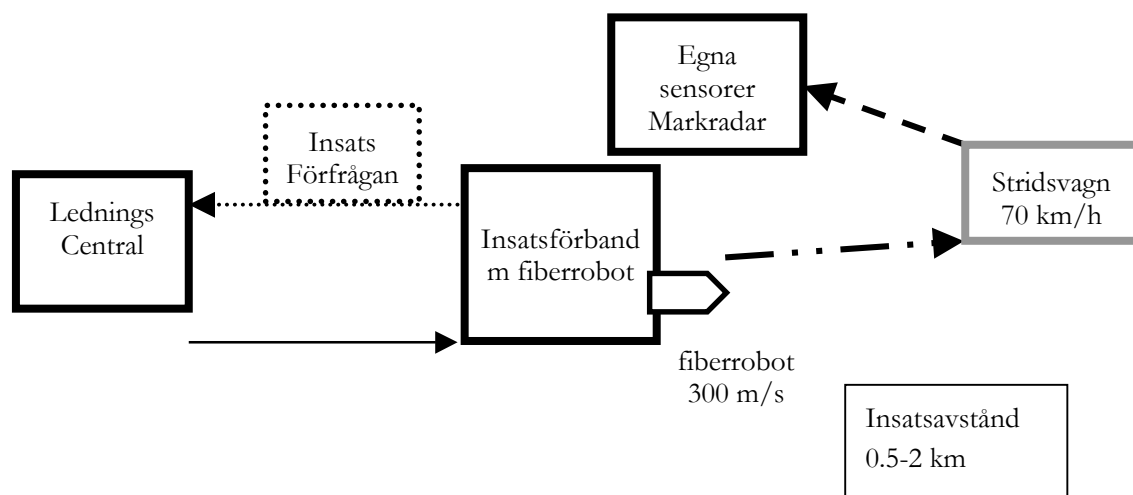
Roboten träffar målet och verifiering av insatsens verkan erhålls genom analys av data från marksensorer och reaktiv spanare som hänger kvar över målet.

Stridsvagn - Plattformsorienterat alternativ

I det plattformorienterade alternativet kan inte insats mot stridsvagnen ske förrän den upptäcks visuellt. Det kan ske från t ex attackhelikopter. Val av vapen i det plattformorienterade fallet blir då sannolikt inte en fiberoptisk robot utan något vapen som kräver "line-of-sight" till målet, t ex en laser- eller trådstyrd robot



Figur 5. Schematisk beskrivning av ett trivalt nätverk för typfallet stridsvagn.



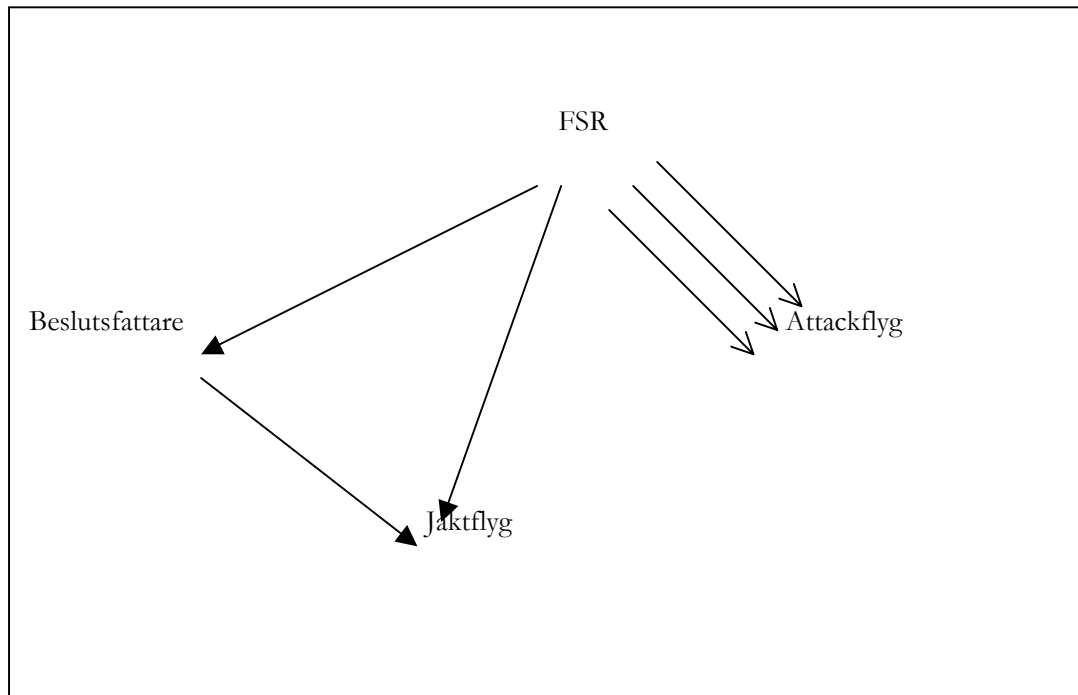
Figur 6. Schematisk bild över traditionell plattformorienterad sensor-till-verkanskedja för stridsvagn.

Stridsflyg - nätverk

I ett triviale nätverk för stridsflyg används spaningsradar som upptäcker mål på ett visst avstånd och kan identifiera mål på ett annat mindre avstånd. Sensornära signalbehandling sker av radarbilden. Från FSR skickas behandlad målinformation till beslutsfattaren. Information skall för varje mål innehålla position inklusive noggrannhet, måltyp, bana, hastighet m m. Hos beslutsfattaren sammanställs inkommen information till en lägesbild. Med stöd av denna ger beslutsfattaren order om anfall till jaktflyget. Jaktflyget leds mot målet från beslutsfattaren. När jaktflyget har kommit tillräckligt nära målet tar jaktrotens chef över ansvaret. Målinformation skickas då direkt från FSR till jaktflygplanen. Jaktflygplanen avfyrar radarrobotar med ledning av målinformationen från FSR utan att slå på egen radar. Robotens radar slås på när roboten är nära målet.

Stridsflyg - Plattformsorienterat alternativ

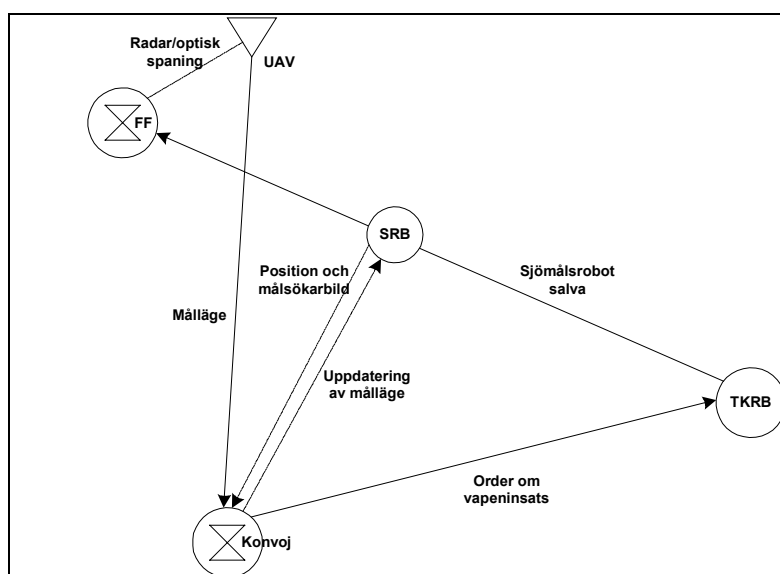
Skillnaden jämfört med triviale nätverk är att idag används inte FSR för att skjuta och leda robotar mot målet.



Figur 7. Schematisk beskrivning av ett triviale nätverk för typfallet stridsflyg.

Ytstridsfartyg - nätverk

Det triviala nätverket för ytstridsfallet börjar i den reaktiva spaningen från en UAV.



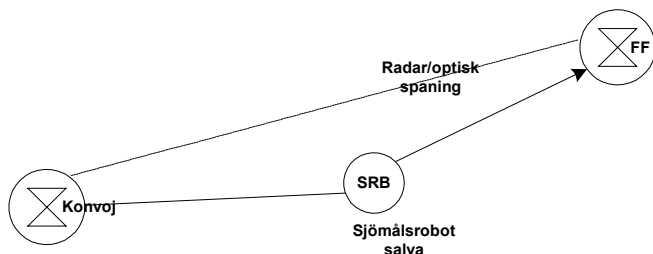
Figur 8. Schematisk beskrivning av ett triviale nätverk för typfallet ytstridsfartyg.

Målläget skickas kontinuerligt av UAV:n till den plattform där insatsen leds, i detta fall en korvett typ Visby. Här skapas en lokal, detaljerad lägesbild. Från ledningsplattformen skickas en order till det tunga kustrobotbatteriet (TKRB) att avfira en salva med sjömålsrobotar mot mål nr Z i position X,Y.

Efter det att robotarna preparerats avfyras en salva. Om robotarna har förmåga att kommunicera under gång uppdateras målläget för robotarna kontinuerligt, antingen från skjutande enhet eller direkt från ledningsplattformen. Är kommunikationen med robotarna dubbelriktad uppdateras även lägesbilden med robotarnas verkliga läge och målsökarinformation.

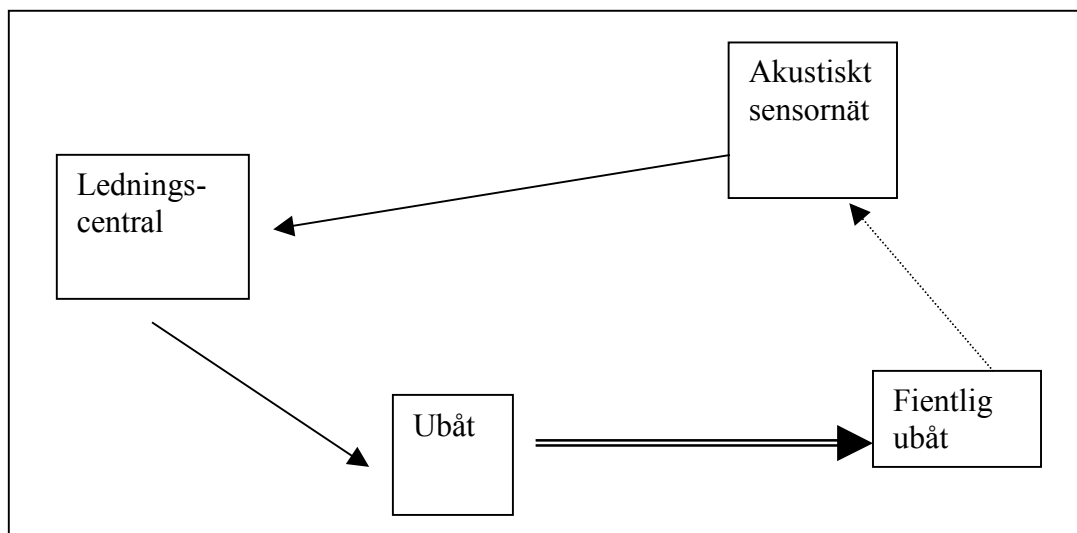
Ytstridsfartyg - Plattformsorienterat alternativ

I det klassiska ytstridsfallet upptäcker den skjutande plattformen målet med egna sensorer, t ex radar eller SIS. Vapeninsats med sjömålsrobot sker med egna robotar.



Figur 9. Schematisk beskrivning av ett plattformsorienterat alternativ för typfallet ytstridsfartyg.

Undervatten - nätverk

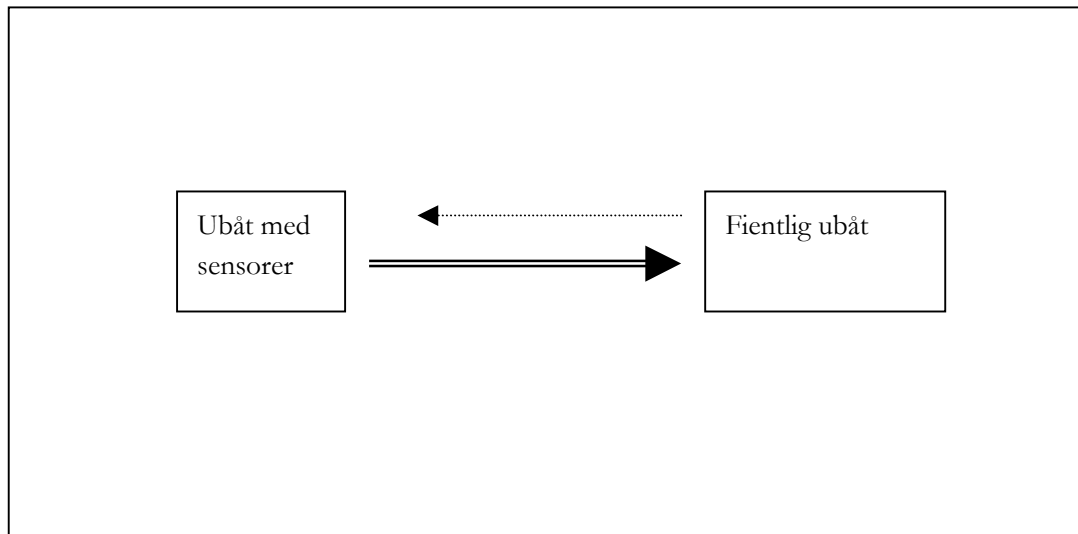


Figur 10. Schematisk beskrivning av ett triviellt nätverk för typfallet undervatten.

I det triviala nätverket för undervattensfallet upptäcks den fientliga ubåten av det i förväg utplacerade sensornätet. Från en lokal bearbetnings- och sammantälningscentral sänds målposition till en ledningscentral på land, där en beslutsfattare och informationschef är placerad. Beslutsfattaren skickar en order till en egen ubåt att bekämpa den fientliga ubåten. Den egna ubåten skickar en torped mot den anvisade målpunkten. Verkan av insatsen registreras både av det utlagda sensornätet och passiva sensorer ombord på den egna ubåten.

Undervatten - Plattformsorienterat alternativ

Vår ubåt upptäcker en fientlig ubåt med sin sonar. Ubåten avfyrar en torped mot målet. Ubåten registrerar verkan med hjälp av sin sonar.



Figur 11. Schematisk beskrivning av ett plattformsorienterat alternativ för typfallet undervatten.

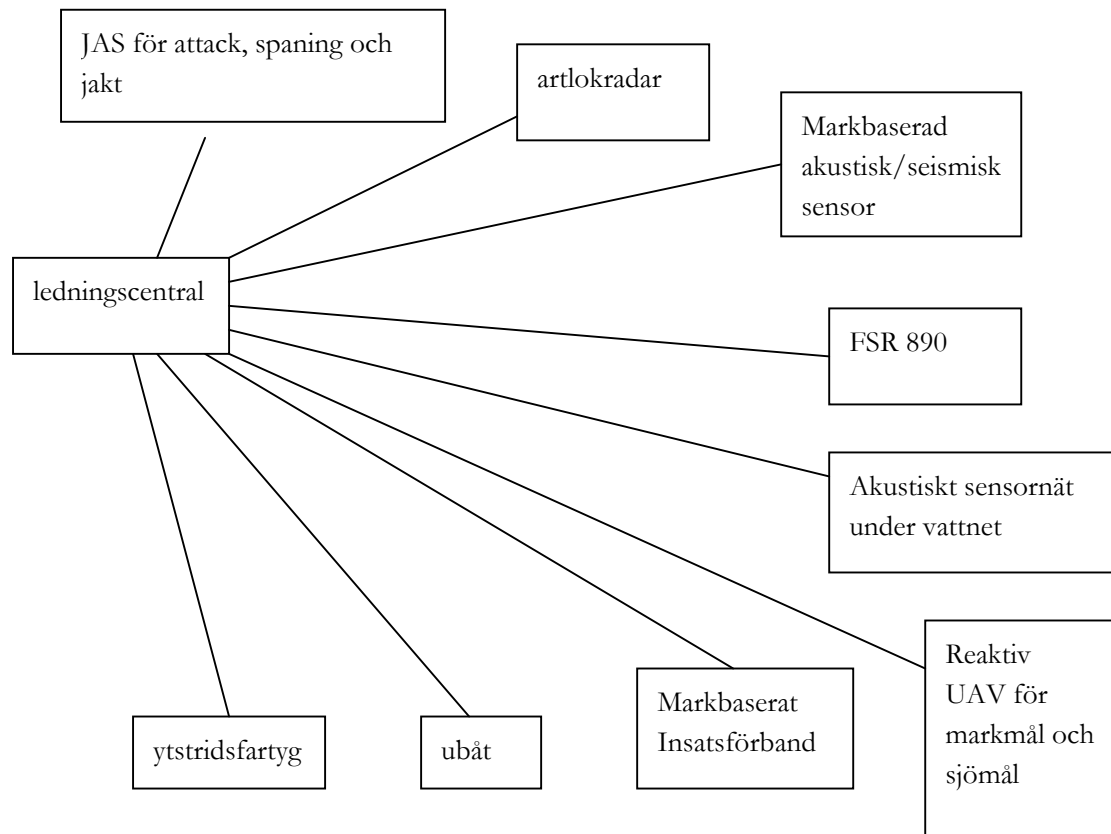
4.2.2 Generellt nätverk

De nät som beskrivits i de triviala nätverken för respektive scenario medger studier av vilka faktorer som är väsentliga i de enskilda fallen. För att studera egenskaperna och effekterna av ett samlat nätverk bestående av en mängd olika komponenter, beskrivs nedan en tänkbar struktur för ett generellt nätverk, sammansatt med de i scenarierna använda enheterna.

Den centrala beslutsfattaren skall när som helst kunna ersättas av annan beslutsfattare på någon av de övriga ledningscentralerna eller plattformarna. Om den centrala beslutsfattaren eller delar av nätverket slås ut skall varje vapenbärare ha "rules of engagement" så att den kan agera mer eller mindre autonomt med hjälp av information från de sensorer som är tillgängliga i nätverket.

All lägesinformation från samtliga sensorer kan presenteras i den ledningscentral där beslutsfattaren sitter. Denna information förs vidare i realtid till alla plattformar som kan ha intresse av den, t ex skall de egna jaktflygplanen kunna få kontinuerlig målinformation från flygande spaningsradar och aerostatburen radar. I normalfallet ges alla skjutorder från beslutsfattaren. Som alternativ till den centrala beslutsfattaren skall det finnas möjlighet att flytta beslutsfattarfunktionen till en annan plattform, t ex flygande spaningsradar, baksits på en JAS39 B, markcentral eller korvett. Detta ska kunna ske utan tidsfördröjning om den centrala

beslutsfattaren eller delar av nätverket slås ut eller om det av annat skäl är lämpligare att beslutsfunktionen finns på annat ställe.



Figur 12. Det är viktigt att alla olika typer av noder i ett lokalt nätverk för en specifik insats kan kommunicera med samma ledningscentral. Vidare är det också viktigt att de kan fortsätta att kommunicera med varandra även om ledningscentralen skulle bli utslagen.

5 MODELLERINGSMETODER

Modellering och simulering är ett snabbt växande område, med en omfattande spännvidd från metodik för analys och design, till verifiering och validering. Att ta fram en översiktlig bild av vilka metoder och verktyg som finns tillgängliga låter sig inte göras, då den skulle bli alltför omfattande. I denna förstudierapport lyfts några intressanta och kända tekniker fram, som antas kan komma att få betydelse för att finna metodik och systematik vid modellering av scenarier som beskriver nätverksstödd krigföring.

5.1 Modelleringsparadigmer

Utformning av modeller kan ske på ett stort antal sätt, allt från att själv konstruera dem från grunden, till att koppla samman färdiga modellkomponenter i en HLA-federation. Olika angreppssätt är också förenade med skilda tekniker för analys och design. Att finna ett tillvägagångssätt som lämpar sig för den aktuella uppgiften är inte trivialt, det är en process där en rad olika frågeställningar bör bedömas. Nedan ges en kort sammanfattning av några kända paradigmer som kan vara av intresse att studera närmare.

5.1.1 Ramverktyg

Simuleringsramverk är verktyg för att bygga modeller och genomföra simuleringar, utan att verktygen i sig innehåller några specifika modeller. Fördelar med simuleringsramverk är att de ger möjlighet till besparingar i tid och kostnad genom att tillhandahålla hela den infrastruktur som behövs för att genomföra en simulering i form av verktyg för scenariogenerering och analys, simuleringsmotor, grafik, tidshantering. Genom att tillhandahålla dessa tjänster är det då möjligt att enkelt ta fram komplicerade scenarier och återanvändbara modeller utifrån enkla standardmoduler.

FLAMES och STAGE är kommersiella produkter som kan kategoriseras som simuleringsramverk, med tyngdpunkt på modellering av taktiska och stridstekniska förlopp på systemnivå. Många av fördelarna med att använda simuleringsramverk kan beskrivas i generella termer, medan nackdelarna ofta kan härröra sig till implementeringsspecifika detaljer, och kan variera kraftigt mellan olika produkter, exempelvis begränsningar i hur modellen måste anpassas för att passa in i ramverket.

Ett intressant angreppssätt kan vara att utröna vilka speciella krav som är specifika för nätverksstödd krigföring, och utreda om tekniken med simuleringsramverk är applicerbar på problemområdet. Det är värt att notera att dessa ramverk är utvecklade med ett traditionellt synsätt på krigföring, det är inte givet att det är möjligt att på ett enkelt sätt inkorporera ett nytt synsätt i dem.

5.1.2 Generella verktyg

Det finns idag en stor mängd kommersiell programvara för att lösa matematiskt formulerade problem, några exempel på sådan programvara är MATLAB, MatrixX, Dymola, Extend, iThink, med flera. Dessa produkter spänner över oerhört skilda tillämpningsområden, och är ofta lämpliga för att studera väldefinierade delproblem, men kan bli svårhanterliga på en systemnivå

med en betydligt högre abstraktionsnivå, där man exempelvis vill studera taktiska för- och nackdelar. Trots dessa begränsningar kan det finnas skäl till att se närmare på delar av detta område:

Det är alltid intressant att undersöka om problematiken kan formaliseras; en matematisk definition av en problemställning är i många fall att föredra framför resultat av antaganden som gjorts i modeller efter att de specificeras. Det är troligt att delproblem som formuleras i projektet med fördel kan studeras med något av dessa verktyg.

Till grund för modellering av nätverksbaserad krigföring, ligger som namnet antyder, möjligheterna att modellera nätverket. För många frågor på taktisk och operativ nivå behöver kanske inte nätverket modelleras alls, medan det för frågor på sensor-to-shooter nivå kan vara av stor betydelse. Datornätverk förekommer så gott som överallt i samhället, och följaktligen finns det gott om kända tekniker för att modellera datornätverk med avseende på olika aspekter så som sårbarhet, känslighet för lastvariationer mm inom denna paradigm.

Denna typ av modelleringsverktyg är i många fall lämplig som en första ansats till att lösa ett delproblem, framförallt då man kan göra större avgränsningar och inte behöver ta hänsyn till alla detaljer som formar helheten.

Utöver kommersiella modellerings- och simuleringsverktyg, finns även mer eller mindre allmänt tillgängliga språk för att uttrycka dynamiska modeller, exempel på dessa är acsl och modelica.

5.1.3 *Distribuerad simulering*

En modell behöver inte exekveras fristående, den kan mycket väl konstrueras så att den interagerar med andra modeller som exekverar antingen på samma dator, eller över ett nätverk. Det är en intressant tanke att man skulle kunna bygga nätverksbaserade modeller av nätverksbaserade krigförande enheter, men det är inte givet att det i alla fall är den bästa lösningen.

5.2 Analysmetoder

Att bygga datormodeller för simulering av händelseförlopp kan göras på en mängd olika sätt; att välja en metod som lämpar sig för ändamålet, är främst en fråga om att definiera de frågeställningar som simuleringar med modellen skall kunna besvara, och utifrån detta välja bäst metodik.

För problem av mindre komplex natur kan det ofta vara effektivt att ha en högre grad av specialisering, medan för mer komplexa problemställningar kan det vara önskvärt att generalisera problematiken och använda sig av mer generella lösningar.

5.2.1 *CMMS*

Att ha en för alla gemensam begreppsapparat och uppfattning om vad som skall representeras är avgörande för att åstadkomma teknisk och kunskapsmässig interoperabilitet¹. Ett omfattande arbete bedrivs internationellt för att åstadkomma metoder för och innehåll i konceptuella

modeller, (*Conceptual Model of Mission Space*, CMMS). En förstudie inom området genomförs vid FOI under 2001.

Även om det i dag inte existerar någon fullt utvecklad metodik för CMMS, kan *mission space models* i termer av standarder, format, verktyg, mm vara mycket intressant för detta område, där frågeställningarna ännu inte är givna.

5.2.2 Objektorienterad analys & design

Objektorienterad analys och design (OOA&D) har under 1990-talet kommit att bli en dominerande metod för beskrivning av programvarusystem. Det är en generell och väl beprövad metodik för att beskriva ett system, och applicerbart inom många områden.

5.2.3 Verifiering, validering och ackreditering

Verifiering och validering och ackreditering (VV&A) av modeller är ett ämne som otvivelaktigt kommer att bli intressant, om det idag är besvärligt att på ett systematiskt sätt verifiera och validera modeller som används för modellering av traditionell krigföring, kommer det inte att bli enklare att systematisera VV&A för modeller av nätverksstrid, då frågeställningarna kan bli mer komplexa.

5.2.4 Fedep

Federation Development and Execution Process (FEDEP) är som namnet antyder mer en process än metodik, som vuxit fram i och med utvecklingen inom området distribuerad simulering. Det huvudsakliga syftet med FEDEP är att systematisera utvecklingen av distribuerade simuleringsmodeller, men processen är så pass generell att den är applicerbar även i andra modellutvecklingsprojekt. De aktiviteter som definieras i "HLA Federation Development and Execution Process Model V1.5"² kan med fördel ingå i detta projekt.

5.3 Angränsande områden

Nätverksbaserad krigföring är ett komplext område, och det finns idag inget självklart val bland metoder och verktyg. Den uppräknade av kända tekniker och verktyg som här gjorts gör ej anspråk på att vara fullständig, den har gjorts i syfte att belysa vikten av att ha ett väl definierat problemområde, samt visa på behovet och svårigheterna med modellering på olika detaljeringsnivåer.

5.3.1 Datorgenererade styrkor

Datorgenererade styrkor (Computer Generated Forces, CGF:er) är en metod för att befolka bemannade distribuerade simuleringar med aktörer. I en förlängning av projektet kan det vara av intresse att närmare studera möjligheterna att använda tekniker för CGF:er.

5.3.2 Data- och Informationsfusion

Ett område som angränsar till nätverksbaserad krigföring på *sensor-to-shooter* nivå, är data och informationsfusion, framför allt möjligheterna att fusionera sensordata. Även om datafusion

ligger utanför ramarna för detta projekt, kan det kan finnas goda skäl till att åtminstone definiera gränstorna.

¹ Löf S, Utlandsrapport Modellering och simulering, 1997, ISSN 1100-2999.

² DMSO: HLA Federation Development and Execution Process Model V1.5, 1999.

6 BIBLIOGRAFI

Efter varje litteraturförslag finns en kort beskrivning kring innehållet i litteraturen.
Nätverksbaserad krigsföring, *Network Centric Warfare*, förkortas oftast som NCW.

6.1 Böcker

J. Adams, *The Next World War*. Hutchinson, 1998.

"Boken beskriver hur krig kan komma att utkämpas i framtiden och hur planerarna i Pentagon och på andra ställen håller på att ta fram en metod kallad Information Warfare, IW, där modern teknik används för att identifiera, demoralisera och förstöra en motståndare utan att binda upp militära styrkor i fält."

D.S. Alberts, J.J. Garstka och F.P. Stein, *Network Centric Warfare – Developing and Leveraging Information Superiority*. Center for Advanced Concepts and Technology, 2000.

"Bok som går igenom tankar och grunder kring nätverksbaserad krigsföring."

G & M Friedman, *The Future of War*, ST. Martin Griffin, 1996.

"Författarna hävdar att vi lämnat 'The age of Ballistics' och går in i 'The age of precision-guided munitions'. Denna fundamentala förändring kräver förändringar av strategier."

N. Friedman, *Seapower and Space*, Naval Institute Press, 2000.

"Norman Friedmans bok handlar huvudsakligen om den amerikanska flottan och olika system kopplade till satelliter som nu eller inom en snar framtid finns i tjänst. Dessutom görs kopplingar från systemen till hur de fungera i en nätverksorienterad miljö."

R.R Leonhard, *The Principles of War For The Information Age*, Presidio Press, 1998.

"Författaren marknadsför sin syn på att krigets principer, formulerade under bondesamhället, är föråldrade och att nya principer krävs för att uppnå seger på dagens komplexa slagfält."

M. O'Hanlon, *Technological Change and the future of War*, Brookings Institution Press, 2000.

"O'Hanlon intar en kritisk hållning till den mest entusiastiska förespråkaren för RMA-koncepten. Samtidigt görs en strukturering av trender och policy och en värdering sensor och vapensystem inom ramen för dessa nya koncept."

W. Owens och E. Offley, *Lifting The Fog Of War*. FSG, 2000.

"Admiral William Owens redogör mot bakgrund av sina erfarenheter som chef för 6:e flottan i Medelhavet och som Deputy JCS för sin syn på hur det amerikanska försvaret måste omvandlas och hur IT kan nyttjas i detta."

6.2 Rapporter

A. Adler, *DARPA Technologies for Future Combat Systems*. DARPA Tactical Technology Office, January 2001.

“Future Combat Systems, FCS, ska vara ett system av system vilket är nätverkscentrerat, inte plattformscentrerat. Beskrivning finns av vad som anses behövas i detta system och teknik som kan behövas nämnas. Finns även information om detta i rapporten; Why a Future Combat Systems Program.”

S.W. Askins, *The Black Box Conundrum of Network Centric Warfare*. Naval War College Newport RI, Joint Military Operations Dept, February 2000.

“En revolution inom affärsvärlden har applicerats till NCW. Kan användas för att nå ökad medvetenhet samt tidskomprimering för att överbygga ett gap mellan medvetenhet om situationen på slagfältet och informationsöverlägsenhet.”

J.D. Beck, *Preventing Network Centric Overload*. Naval War College Newport RI, Joint Military Operations Dept, February 2001.

R.A. Borchert, *Organizational Fitness of a Proposed Network Centric Organization*. Naval Postgraduate School Monterey Ca., December 1998.

“Snabbhet vid kommandogivning samt självsynkronisering är viktiga begrepp vid NCW. En organisation tänkt att användas vid NCW föreslås. Den består av stridsledaren och ledare för situationsmedvetande, resurser, effekter samt operationer. Hur organisationsmodellen fungerar studeras både för planeringsprocessen och för utförandeprocessen. Resonemanget fungerar om man gör planeringsprocessen mycket centraliserad och utförandeprocessen decentraliserad.”

M. Burke, *Thought Systems and Network Centric Warfare*. Defence Science and Technology Organisation Salisbury, July 2000.

“TWA – Thought Warfare and Anti-Warfare innefattar den dynamiska interaktionen mellan allierades och motståndares tänkta system. Ett system av idéer för tänkta system presenteras.”

A.K. Cebrowski, *Network-Centric Warfare: An Emerging Military Response to the Information Age*. Naval War College, June 1999.

“Innebörden av NCW samt olika komponenter som begreppet innefattar beskrivs. Vanliga missförstånd kring innebörden av att använda NCW utreds.”

A.K. Cebrowski, *Network-Centric Warfare: Its Origin and Future*. U.S Naval Institute, December 2000.

“Innebörden av NCW och hur det kan vara uppbyggt med informationsnät, sensornät och vapennät beskrivs. Att informationstekniken går från plattformscentrering till nätverkscentrering diskuteras.”

R.D. Critchlow, *Weaving the Net: Linking Space Systems to Theater Operations*. Naval War College Newport RI.

“NCW:s grund är ett informationsnät som fungerar som ett nervsystem vilket länkar ihop sensorer och vapen. Informationsnätet som krävs kan uppnås endast med hjälp av rymdbaserade hjälpmedel såsom satelliter. Det är sällan kommenderkaptenen har tid att etablera markbaserad kommunikation då snabbhet är viktigt inom NCW. Tyvärr råder tekniska begränsningar hos existerande satellitsystem, de måste vidareutvecklas.”

M.M. Eagen, *Advanced C4I and Operational Decision Making: Panacea or Pandora's Box?* NASA no. 19980237720; AD-A351761.

“RMA innefattar teknik som kommando och kontroll, kommunikation, datorer och intelligens. Fördelar och svaga punkter samt samverkan mellan systemet och framtidens soldat diskuteras. Även hur RMA förändrar beslutsfattandeprocessen tas upp.”

D.L. Eubanks, *Application of Network Centric Warfare to J-SEAD*. Naval War College Newport RI, Joint Military Operations Dept., February 2000.

“Fördelar med NCW vid flygstrider för att undertrycka fiendens försvar beskrivs. Det viktigaste verktyget är tiden – man vill störa i fiendens beslutsöversikt.”

S.G. Fox, *The Dimming of Joint Vision 2020: A Concern That the Lack of Military Satellite Communications Will Impede the Future Force*. Army War College Carlisle Barracks PA, February 2001.

“För att uppnå informationsöverlägsenhet är det viktigt att ha omfattande kommunikationsmöjligheter för att flytta information när och vart det behövs. Historiskt har kraven på kommunikation inte överensstämmt med tillgänglig satellitkommunikation.”

C.R. Fralick, *Navigation in the Age of Network Centric Warfare*. Naval War College Newport RI, Joint Military Operations Dept., February 2000.

“Hela vapensystem litar nu på GPS för sin precisionskapacitet, men GPS är sårbart vid asymmetriska attacker i form av störningssändare. Detta ska förbättras vid användning av NCW.”

J.A. Freebersyser, *Future Combat Systems Communications*. DARPA/ATO, September 2000.

“Future Combat Systems, FCS, ska vara ett system av system vilket är nätverkscentrerat, inte plattformscentrerat. Vad som behövs i detta system beskrivs.”

J.C. Horne, *Information Superiority as an American Center of Gravity: Concepts for Change in the 21st Century*. Army War College Carlisle Barracks PA, April 2000.

“Diskuterar informationshot, undersöker specifika fiendliga anfall och utvecklar koncept för försvar av militära informationsnätverk. Ger strategiska rekommendationer för fortsatta försök att uppnå informationsöverlägsenhet.”

H.H. Hultgren, F.E. White, J.A. Roese och J.V. Simmons, *A Network-Centric Framework for Engineering Future Naval Platforms*. Naval Undersea Warfare Center Newport Div. RI, Mars 2000.

“De element som behövs inom ramen för information i ett system med NCW-koncept beskrivs. Ett specifikt exempel ges som beskriver vikten av precision gällande upptäckt, tolkning, beslut och åtgärd.”

Joint Vision 2010 samt *Joint Vision 2020*

"Är en modell för hur man ska leverera tekniska möjligheter för att uppnå bra effektivitet inom gemensam krigsföring. Det ska göras genom att utveckla fyra koncept för militära operationer; Dominant Maneuver, Precision Engagement, Full Dimensional Protection och Focused Logistics."

T.F. Keeley, *Network Centric Warfare – Wiring Joint Forces for Battle: Are Operational Leaders Really Plugged In*, Naval War College Newport RI, Joint Military Operations Dept., May 2000.

"NCW är ett exempel på Metcalfs lag som säger att värdet av ett nätverk växer proportionellt med kvadratroten ur dess noder. Detta uppfylls inte då man ser till en viktig nod i informationsnätverket - ledarna. De måste förstå både nätverket och informationen om deras agerande ska vara optimalt."

S.L. McLennan, *Battlespace Awareness: Solutions for a Multinational Problem*. Naval War College Newport RI, Joint Military Operations, February 2001.

"Diskuterar de ökade krav som NCW ställer på informationsöverlägsenhet samt de möjligheter som finns att skapa 'Shared Awareness' och ökat tempo vid operationer."

F.J. Olmo, *Command and Control in Joint Vision 2010: Flexible, Adaptive and Networked*. Naval War College RI, Joint Military Operations Dept, February 1999.

"Ny teknik utvecklas för att stödja Joint Vision 2010. Viktigt är att konceptet "Command and Control" ger kommandören flexibilitet och möjlighet att använda snabbare informationsteknologier för att utöka kunskapen om slagfältet och uppfattningen om situationen."

M.S. Paulk, *Fortifying the Foundation of Combat Power: Centric Warfare and Principles of Logistics*, Naval War College Newport RI, Joint Military Operations Dept., February 2000.

"Utvärderar fyra logistikprinciper samt applicerar en nätverkslösning vid NCW. Påvisar fördelar med NCW."

C.A. Richard, *Network Centric Warfare and the Bandwidth Limited Platform: Beyond the Engagement*, Naval War College Newport RI, May 2000.

"NCW behöver stor bandbredd, men det finns alltid enheter som är begränsade i sin förmåga att kommunicera. Styrkan hos NCW är att bäst utnyttja de tillgängliga kommunikationsmöjligheterna för varje element."

Sensor to Shooter 3: Precision Engagement C4ISR Architecture Analysis, Final Report. National Defence University Press, Washington, DC, 1998.

M.R. Sickert, *Network-Centric Warfare and the Operational Concepts of War: A Synergetic Effect*. Naval War College Newport RI, May 2000.

"NCW ökar handlingsfriheten på strategisk, operationell och taktisk nivå då man får större kontroll gällande områden, tid och stridsstyrkor. Största fördelen med NCW är ökad 'Battlespace Awareness'. Man vill kunna operera i fiendens beslutscykel samt bättre disponera tillgängliga styrkor."

T.A. Slais, *Some Principles of Network-Centric Warfare: A Look at how Network-Centric Warfare Applies to the Principles of War*, Naval War College Newport RI, February 1999.

“Beskriver NCW och hur det ger fördelar gällande masseffekter, bra offensiv och ökad säkerhet vid krigföring. NCW ska syfta till att strida snabbare, billigare och bättre. Man vill uppnå en masseffekt av skilda system genom att koordinera läge, identifikation och finna mål för att göra en gemensam aktion. Bra offensiv uppnås då NCW ger dominans med avseende på tidsfaktorn. Säkerheten ökas genom dominans på slagfältet tack vare informationsöverlägsenhet.”

F.P. Stein, *Network-Centric Warfare: Impact on Army Operations*, IEEE Piscataway, NJ USA.

“Beskriver de fem koncept som ska vara grunden för framgångsrika strider; Dominant Maneuver, Precision Engagement, Focused Logistics, Full-dimensional Protection samt Information Superiority vilket ska möjliggöra de fyra andra. Informationsöverlägsenhet uppnås med tre matriser; sensorer, vapen och informationssystem. Exempel ges från tester som visar att sättet strider utkämpas på förändras på grund av informationsöverlägsenhet.”

F.P. Stein, *Observations on the Emergence of Network Centric Warfare*, Evidence Based Research, Spring Hill Road Vienna, December 2000.

“Bra genomgång av grunderna för hur ett NCW-system är uppbyggt av informationsnät, sensornät och vapennät.”

P.J. Szczepankiewicz, *Authentication in SAAM Routers*, Naval Postgraduate School Monterey Ca., June 2000.

“Verifiering är mycket viktigt i ett SAAM-system (Server and Agent Based Active Network Management). SAAM med verifiering kan användas som teknisk nätverksinfrastruktur för att stödja NCW. Lösning på detta presenteras.”

I.V. Vatet, *Can Network-Centric Warfare Save Undersea Warfare?* Naval War College Newport RI, February 2000.

“Undervattensförsvaret med ubåtar kan bli en sårbar länk vid NCW och man uppnår då inte ökad säkerhet och överraskningsmoment hos fienden. Man saknar den teknik som krävs för att få den tidsprecision och exakthet i position som krävs vid NCW.”

W.T. William, *Network-Centric Warfare and the Command and Control of Amphibious Operations*. Naval War College Newport RI, Joint Military Operations Dept, February 2000.

“Full spektrumdominans kräver att man uppnår informationsöverlägsenhet på slagfältet. Här diskuteras hur man inkluderar NCW-konceptet gällande framtida landstigningsoperationer.”

6.3 Tidskriftsartiklar

Y. Atamna, “NETWARS: Toward the Definition of a Unified Framework for Modelling and Simulation of Joint Communication Systems,” *Spie International Society for Optical*, Issue 3393, 1998.

A.R. Garrett, “Information Superiority and the Future of Mission Orders,” *Military Review*, vol. 79, no. 6, 1999.

L.H. Green och E.B. Raff, “Net-Centric Undersea Warfare,” *Sea Technology*, vol.40, no. 11, 1999.

“NCW ska förbättra flottans arbete genom att ge rätt information till rätt person i rätt format vid rätt tid. De element som krävs för att bygga upp en nätverksbaserad miljö nämns.”

M. Kelley och R. Pei, "C412WS System of Systems Integration for the Future Army," *Society of Photo-Optical Instrumentation Engineers*, vol. 3694, 1999.

"I framtiden då man har en mängd olika sensor- och vapensystem ska de kunna länkas ihop till ett system av system m b a ett informationsnät i realtid. Man måste utveckla en robust och flexibel miljö för att stödja integrationen av olika system. Här redovisas förslag på ett möjligt koncept."

Lewis, "Impact of Network Centric Warfare on Sub Operations," *Submarine Review*, January 1999.

E. Mårtensson och M. Nordin, "Marinen i en omdanad försvarsmakt," *Marinnytt*, vol. 4, 2000.

"Kort om Joint Vision 2010. Visar på den teknikutveckling som möjliggör utvecklingen av NCW och även exempel på hur viss teknik måste förändras för ändamålet."

E.C. Shek, "Intelligent Information Dissemination Services in Hybrid Satellite-Wireless Networks," *Mobile Networks and Applications*, vol. 5, no. 4, 2000.

"Förslag på användning av infrastruktur med satellit och trådlöst nätverk för att uppnå hög 'Situation Awareness'. Hjälpmedel är IIDS, Intelligent Information Dissemination Service, som b l a ska hantera karaktäristikskillnader mellan satellit och det markbundna trådlösa nätverket, möjliggöra effektiv användning av bandbredd samt se till att realtidsinformation snabbt kommer fram."

M.A. Simard, J. Couture och E. Bosse, "Data Fusion of Multiple-Sensors Attribute Information for Target-Identity Estimation Using a Dempster-Shafer Evidential Combination Algorithm," *Spie International Society for Optical*, Issue 2759, 1996.

Thomppson, "Attack Subs & Network-Centric Warfare," *Submarine Review*, no. OCT, 2000.

E.J. Walsh, "Exercise Demonstrates Benefits of Military's Network-Centric Warfare," *Signal*, vol. 52, no.3, 1997.

F.J. West, "Ring of Fire. Ring of Smoke?" *Proceedings*, November 1998.

"Krav finns på högre kapacitet för att kunna genomföra NCW. T ex får fartyg många fler anrop om eld då anropen kan komma från många olika sensorer. Snabb information krävs så att beslutsfattarna agerar innan motståndaren flyttar sig, kapaciteten för beslutsfattande måste ökas."

E.C. Whitman, "Submarines in Network Centric Warfare," *Sea Power*, vol.42, no.7, 1999.

"Diskuterar många fördelar men också nackdelar gällande planerna kring NCW"

A.D. Zimm, "Human-Centric Warfare," *Proceedings*, May 1999.

"Hur passar människan in i NCW-bilden – hur fungerar vi och hur mycket information krävs för att man ska uppfatta en situation? Faktorer som stress, tid och beslutsfattande tas upp."

6.4 Konferensbidrag

J. Brand, A. Brodeen, R. Coleman, M. Lopez, D. Meyer och K. Preston, "Virtual Reality C3 Network Battle Management and Analysis Tool," från *IEEE Military Communications Conference MILCOM*, Atlantic City NJ, Oct 31 – Nov 3 1999.

"Mjukvara är utvecklad för att förbättra medvetande om situationen genom att samla in slagfältstatus från skilda källor och visa informationen i form av text och bild."

B.J. Jansen, J.A. Hamilton och U.W. Pooch, "Modelling and Simulating an Army Information Support Structure," från *Multiconference*, Atlanta: Society for Computer Simulation International, April 1997.

S. Julier, R. King, B. Colbert, J. Durbin och L. Rosenblum. "Software Architecture of a Real-time Battlefield Visualization Virtual Environment", från *Virtual Reality Annual International Symposium*, Houston, 1999.

"Beskriver DRAGON, en virtuell miljö som visualiserar slagfält för att uppnå 'Situational Awareness' i realtid."

N.H. Lu, "Network Interface to Tactical Communications," från *IEEE Military Communications Conference MILCOM*, Monterey CA USA, 3-5 November 1997.

"Olika användare och heterogena nätverk ska kunna kommunicera. Problem finns relaterade till bl a interoperabilitet mellan nätverken och effektivt utnyttjande av bandbredd. De problemen undersöks och ett koncept för att lösa dem identifieras."

C.W. Noyes, "Network Centric Warfare Operational Impact on Land Warfare," från *Defence systems & equipment international DSEi 99 conference*, Chertsey, September 1999.

D.A. White, L. Young och G.R. Kelsch, "Modelling and Simulation of Situational Awareness in the Tactical Internet," från *IEEE Military Communications Conference MILCOM*, Bedford, MA USA, 19-21 October 1998.

"Viktigt vid 'Situational Awareness' att veta position för både allierade och fiende. 'Situational Awareness' grundar sig på information från de allierades nätverk och det krävs ett komplext kommunikationssystem vilket ska ge pålitlighet och effektiv dataöverföring."

BILAGA 1 - TYPFALL FAST MÅL

Sammanfattning

I typfallet fast mål har en artillerikanon beskjutit en civil by. Beskjutningen upptäcktes av våra sensorer som medgav beräkning av kanonens position. Ett av våra attackflygplan som var i luften blir beordrat att bekämpa den upptäckta kanonen. Anfallet försvåras av att artillerikanonen är placerad intill ett sjukhus där flyktingar passerar på en närliggande väg.

Ingående verksamheter och objekt

Vår trupp har fått i uppgift att skydda ett antal byar i en dal där de ständigt har fått utstå artilleribeskjutning. På grund av beskjutningen flyr de som kan via den stora vägen som löper genom området. Vägen löper bredvid ett gammalt sjukhus som båda sidor i konflikten använder för att vårda sina sårade. Vår artillerilokaliseringsradar upptäcker att den senaste beskjutningen har kommit från en plats inte långt från sjukhuset och befälhavaren i ledningscentralen begär insats från attackflygplan i luften mot den beräknade målpositionen.

Aktiviteter

Anflygning

Anflygning sker på låg höjd med avslagen radar och radiotystnad för att visa så liten signatur som möjligt.

Spaning

En artillerilokaliseringsradar upptäcker och beräknar positionen för en skjutande artillerikanon.

Positionen skickas in till en central ledningscentral som sammanställer och värderar informationen.

Underrättelsevärdering

Den information som kommer in till underrättelsecentralen sammanställs, bearbetas och infogas i den lägesbild som presenteras för beslutsfattare.

Ledningscentral

I ledningscentralen finns beslutsfattare med stabsmedlemmar. Varje beslutsfattare kan sätta ihop sin egen lägesbild. Beslutsfattare anger vilka mål som skall bekämpas och vilken vapenplattform som skall användas.

Insats

När flygplanet närmar sig målet skall piloten kontrollera att Rules of Engagement (ROE) är uppfyllda. Vid positivt svar avskjuter piloten attackroboten mot målet.

Värdera verkan av insatsen.

Spanings-UAV som följer attackflygplanet genomför överflygning för att ta ett foto för analys av insatsens verkan.

Objekt

Ledningscentral

En central där beslutfattaren är placerad.

Informationscentral

Plats där den information som kommer in från sensorerna sammanställs och bearbetas vidare.

JAS39

Attackflygplanet har prestanda som Fpl 39 delserie 3.

Attackrobot

Attackroboten på flygplanet är en KEPD 350.

Artillerikanon

Den fientliga artillerikanonen har samma prestanda som dagens 15,2 cm haubits.

Spanings-UAV

Spanings-UAV har samma prestanda som Hunter (amerikansk UAV).

Spaningssensor

Artillerilokaliseringsradar av typ Arthur.

Samband

Sambandet består av en universalradio som kan upprätta samband mellan alla i typfallet ingående enheter.

Geografiska områden och förutsättningar

Uppdraget skall kunna utföras på vilken plats var som helst i hela Europa. I närheten av målet finns ett sjukhus och en väg där flyktingar färdas.

Storlek och utformning på militära resurser

Våra

1 ledningscentral

1 fpl 39 ur delserie 3 med 2 attackrobotar

1 mål ca 3 m x 3 m

Universalradio

Motståndaren

Motståndarens artilleri består av en 15 cm haubitskanon.

Övriga objekt

I närheten av sjukhuset finns en väg som är asfalterad och ca 7 m bred. Flyktingar rör sig på vägen och intill sjukhuset. Sjukhuset är en 4-våningsbyggnad ca 100 m lång och 30 m bred.

Tid och miljö

Artillerikanonen är placerad 100 m från civil huvudväg. Vägen trafikeras av flyktingströmmar. Anfallet skall endast kunna genomföras under dager.

Scenariot utspelar sig under ca 2 timmar. 1 timmes anflygning och därefter vapeninsats. Insatsen tidslängd ca 20 minuter.

Startläge och avslutningsvillkor

Situationen börjar med flygplanet i luften beväpnade med 2 attackrobotar. Typfallet slutar när verkansvärdering av anfallet blivit utfört.

BILAGA 2 - TYPFALL STRIDSVAGN

Sammanfattning

I det typfallet stridsvagn föreligger höjd beredskap men ingen direkt krigssituation. Den höjda beredskapen föranleder våra styrkor att upprätthålla en allmän yttäckande luft- och markbaserad spaning samt ökad övervakning av hamnar och flygplatser för incidentberedskap och upprätthållande av territoriell integritet. I anslutning till ett hamnområde har en främmande stridsvagn observerats.

De svenska styrkornas uppgift är att upptäcka och lokalisera stridsvagnen för att sedan följa denna och genomföra en vapeninsats. Reaktiv spaning bedrivs med en liten UAV och stridsvagnen bekämpas med en fiberoptisk robot.

Ingående verksamheter och objekt

Situationen har föregåtts av ett antal terroristangrepp mot svensk infrastruktur t ex el- och telekommunikationer. Dessutom har det förekommit en ökad militär verksamhet i gränsområden och i anslutning till svenska territorialvattengränser.

En fientlig stridsvagn har kränkt den svenska territoriella integriteten och befinner sig under rörelse mot tätort. Detta innebär en färdväg på omkring 100 km som företas både i terräng och på väg. Eld kan avfyras under gång eller i stillastående. Stridsvagnen har under gång och eldgivning hög signatur. Under gruppering, stillastående så är signaturerna låga då stridsvagnen gömmer sig genom maskering i terräng under träd etc. eller genom att gömma sig i närheten av eller i byggnader (exempelvis lador).

Marksensorsystem består av akustiska, seismiska, magnetiska och optiska sensorer finns utplacerade på strategiska platser längs vägar och gränser. Dessa kan upptäcka, klassificera och målfölja fiendens enheter. Dessa kompletteras av civila övervakningssystem, t ex trafikövervakningssystem. Dessa system kan operera i särskilda moder där larmtröskeln är lägre eller larmkriterierna är annorlunda än vid vanlig civil användning.

Efter indikationer från marksensornätet informeras hemvärnet som lokaliserar och identifierar målet som befinner sig under rörelse på väg och rapporterar typ av mål, tidpunkt, rörelseriktning, hastighet och koordinater till stridsledningen. I syftet att kontinuerligt erhålla måldata genomförs reaktiv spaning med en liten UAV. Denna levererar måldata till den gemensamma lägesbilden. Lägesbilden finns sedan tillgänglig dels hos den centrala ledningen, OPIL, dels hos de förband som befinner sig i området.

När den främmande stridsvagnen dolt närmar sig tätorten utan att svara på anrop beslutas om vapeninsats. Det vapen som väljs är en fiberoptiskt kontrollerbar robot.

Aktiviteter

Lägesbild

En marklägesbild byggs upp av en kombination av särskilt utplacerade marksensorer, civila övervakningssystem (trafikkameror) och rapporter från t ex hemvärnet. De utplacerade marksensorerna är av sådan typ att de snabbt kan placeras ut i ett område där det förväntas främmande aktivitet. För att erhålla måldata av sådan kvalitet att vapeninsats kan ske används en mindre spanings-UAV.

Ledning

Den överordnade ledningen sker från den operativa insatsledningen, OPIL. Lokal ledning sker vid brigadledning. Beslut om vapeninsats tas av OPIL. Brigadledningen väljer vapensystem, planerar och genomför vapeninsatsen.

Vapeninsats

Vapeninsatsen sker med en fiberoptiskt styrd robot med prestanda ungefär motsvarande Polyphem¹.

Objekt

Marksensornät

Marksensorsystem består av akustiska, seismiska, magnetiska och optiska sensorer. Marksensorsystem används genom att de placeras ut på strategiska platser längs vägar och gränser. Dessa kan upptäcka, klassificera och målfölja fiendens enheter och leda in insatser mot dessa. De kan också upptäcka och lokalisera eldgivning. Det finns således ett tämligen stort antal sensorer som kan övervaka den fientliga framryckningen. I viss utsträckning är informationen tillräcklig för att sätta in långräckviddiga vapensystem för att hejda framryckningen eller sänka hastigheten.

Fientlig stridsvagn

Den fientliga stridsvagnen är av en äldre modell som saknar avancerade motverkanssystem som sensoraktiverat skydd eller aktivt pansar. Den kräver regelbunden påfyllning av drivmedel vilket sker genom att till synes civila tankbilar, som framförs av agenter för främmande makt, möter stridsvagnen på förutbestämda platser för tankning.

Fiberoptiskt styrd robot

Roboten har en räckvidd på upp till 60 km. Roboten styrs via en optofiber som dels skickar styr signaler från operatören till missilen, dels skickar bilden från missilens IR-kamera till operatören för analys. Vapensystemet (missil och operatör) har därmed förmåga att ”se” målet innan det bekämpas och kan på så sätt vara säker på att det är rätt mål.

Geografiska områden och förutsättningar

Terrängen utmärks av blandad terräng med skog, småbruten, vägar och mindre samhällen samt spridda jordbruk.

Storlek och utformning på militära resurser

Våra

I området finns följande egna förband:

- Brigadstab
- Delar av en divundbataljon (UAV, markspaning)
- Del av en SIS- bataljon (1-2 SIS- komp och bataljonsledningen) (ungefär samma område)
- En amfibiebataljon
- Del av en lätt mekbataljon under utbildning (begränsat användbar)
- Flygbasförband, inklusive säkförband
- Luftvärn
- Det fasta radarsystemet (aerostater, markbaserad radar av olika typ).

Motståndaren

Fiendens resurser består av spridda autonoma enheter som i förväg fått instruktioner om mål färdvägar etc. Enheterna upprätthåller viss kommunikation med sin bas.

Tid och miljö

Typefallet utspelar sig i oktober månad med ett väder bestående av växlande molnighet och tidvis regnskurar. Tidsperioden för scenariot är ca 6 timmar till ett dygn.

Startläge och avslutningsvillkor

Scenariot startar när informationer om fientlig verksamhet, fordon och personal inkommer till ledningscentralen.

Yttäckande spaningssystem ger larm om utökad ej klassificerad verksamhet inom olika områden, t e x utökad trafik med stora fordon. Utrustning för övervakning av hamn och gränsområden ger larm om ökad aktivitet och även klassificering av tunga bandfordon. Reaktiv spaning initieras som sedan leder till insats med vapen.

Scenariot avslutas när bekämpning är utförd och verifierad.

¹ Polyphem är en fiberoptiskt styrd robot med en IR-kamera. Se till exempel <http://www.army-technology.com/projects/polyphem/> för mer information.

BILAGA 3 - TYPFALL STRIDSFLYG

Allmänna kommentarer till typfallet

Robotar i typfallet är tagna ur en källa som har valt väsentligt högre prestanda än dagens robotar. För att matcha detta har prestanda på framför allt radar också satts högre än dagens. Problemet som är tydligt redan vid första anblicken är att typfallet blir oerhört känsligt för små variationer i upptäcktsavstånd. Det är inte helt osannolikt att modellerna måste göras mycket noggrannare och mer verklighetstroga för att det skall gå att få ut meningsfulla resultat. Det är framför allt radarprestanda där bara ett schablonmässigt upptäcktsavstånd kanske inte räcker. Dessa radarprestanda är dock nödvändiga för att i det här skedet se att typfallet har en rimlig möjlighet att fungera på den stora känsligheten. Övriga kompletteringar är träffsannolikheter, P_{kill} , prestanda på motmedel m m.

Typfallet måste kanske kompletteras med en höghöjds-UAV med infraröd sensor som kan upptäcka en inkommande robot i M3 i vissa fall. Även våra jaktflygplan bör eventuellt kompletteras med infraröd sensor.

Sammanfattning

Typfallet stridsflyg består av ett läge med viss höjd beredskap. Våra styrkor har bl a som uppgift att skydda ett viktigt fast markmål samt övervaka och hävda ett territorium som avgränsas av en bestämd gräns t ex en territorialvattengräns. Målet anfalls utan särskild förvarning av motståndarens attackföretag bestående av fyra attackflygplan och två eskorterande jaktflygplan. Vår sida har en flygande spaningsradar, en kustkorvett samt en fast radarstation alternativt en aerostat med radar som sensorer. Vår sida har som vapen luftvärnsrobotar på kustkorvetten, luftvärnsrobotar vid målet samt jaktflyg. Vår sida har även ett nätverksbaserat ledningssystem med en central beslutsfattare.

Ingående verksamheter och objekt

Beskrivs under rubriken "Aktiviteter".

Aktiviteter

Flygattack mot mål som utgörs av en viktig anläggning

Motståndarens flygplan startar från flygbasen 1000 km från målet vinkelrätt mot vår kust och flyger på rak bana i riktning mot målet. Flyghöjden är 10000 m. Motståndarens flygplan kommer att fullfölja uppdraget oavsett hur stora förluster de drabbas av. Efter utfört uppdrag återvänder samtliga motståndarens flygplan.

Flygande spaningsradar och aerostatburen radar är i funktion och övervakar området. Korvetten övervakar också sin omgivning kontinuerligt med radar. När något av dessa system har upptäckt motståndarens anfallande flygplan kommer Beslutsfattaren att beordra våra jaktflygplan att starta för att kunna avvisa dessa flygplan. Motståndarens flygplan svarar inte på kontaktförsök via radio. Motståndarens anfallande jaktflygplan kommer att avfira först samtliga radarrobotar och sedan

samtliga IR-robotar mot vår flygande spaningsradar och våra jaktflygplan tills dessa mål har bekämpats. Våra flygplan anfalls i den ordning som de upptäcks och kommer inom skjutavstånd. Motståndarens attackflygplan kommer vardera att avfira en robot mot korvetten, en mot flygbasen och två robotar mot målet. Dessa anfalls i den ordning som de kommer inom skjutavstånd. Målet anses bekämpat om minst en robot träffar. Om minst en robot träffar flygbasen kommer inget jaktflygplan att kunna starta under resten av typfallet. Om minst en robot träffar korvetten kommer alla system på korvetten att vara utslagna under resten av typfallet. Motståndarens attackflygplan kommer att avfira IR-robotar mot våra jaktflygplan om dessa kommer inom skjutavstånd. När attackrobotarna är avfyrade kommer samtliga motståndarens flygplan att återvända.

När motståndaren har avfyrat den första roboten och vår sida har upptäckt det får våra jaktflygplan order att avfira jaktrobotar mot i första hand motståndarens attackflygplan men även mot motståndarens jaktflygplan om det inte är möjligt att nå attackflygplanen på annat sätt.

Om motståndarens flygplan i stället utan att skjuta passerar den gräns som vår styrka skall övervaka, t ex en territorialvattengräns får våra flygplan order att avfira jaktrobotar mot i första hand motståndarens attackflygplan men även mot motståndarens jaktflygplan om det inte är möjligt att nå attackflygplanen på annat sätt, dock skall våra flygplan inte avfira robotar mot de av motståndarens flygplan som ännu inte har passerat den övervakade gränsen.

Objekt

Motståndaren

Attackflygplan, Attackrobotar¹

Fyra st tunga attackflygplan med vardera 4 st attackrobotar och 4 st IR-robotar för närstrid. Motmedelskapslar. Multimodradar med upptäcktsavstånd 100 km mot ett mål med 1 m² radarmålärea. Radarmålärea 1 m². Aktionsradie 1500 km. Fart 1000 km/h.

Medeltung långräckviddig attackrobot avsedd mot fasta mål. Roboten uppträder autonomt efter fällning. Roboten är försedd med ramjetmotor. Medelfart M3. Räckvidd 300 km. Radarmålärea 0,1 m².

Eskorterande jaktflygplan, Jaktrobotar

Två st eskorterande jaktflygplan med vardera 6 st långräckviddiga radarjaktrobotar och 4 st IR-robotar för närstrid. Motmedelskapslar. Multimodradar med upptäcktsavstånd 100 km mot ett mål med 1 m² radarmålärea. Signaturdämpande åtgärder har vidtagits. Radarmålärea 0,1 m². Aktionsradie 2000 km. Fart 1200 km/h (supercruise). Farten är 1000 km/h i normalfallet.

Långräckviddig radarjaktrobot med aktiv målsökare. Roboten är försedd med ramjetmotor. Medelfart M3. Räckvidd 100 km

Våra

Markbundet mål

Viktig anläggning som utgör mål för attacken. För civilbefolkningen i närheten av målet finns någon form av skyddsrum eller möjlighet till evakuering inom 10 minuter från att order ges.

Korvett²

Korvett utrustad med radar, luftvärnsrobotar samt Telemotmedel. Radar med upptäcktsavstånd 40 km för ett luftmål med 1m² radarmålärea. luftvärnsrobotens räckvidd 10 km. Fart vid patrullering 25 km/h. Radarmålärea 1000 m². Oändlig uthållighet.

Flygande spaningsradar³

Radar med upptäcktsavstånd 250 km för ett luftmål med 1m² radarmålärea. Fart vid patrullering 500 km/h. Oändlig uthållighet tills flygplanet har bekämpats av motståndarens flygplan (Flera fpl förutsätts kunna delta i uppdraget och därmed kan ett fpl alltid vara i luften). Efter bekämpning kan flygplanet inte ersättas av annat inom den tid som typfallet pågår.

Aerostat med spaningsradar⁴

Radar med upptäcktsavstånd 250 km för ett luftmål med 1m² radarmålärea. (Denna radar kan eventuellt ersättas med en fast spaningsradar liknande PS 860)

Luftvärnsrobotbatteri med tillhörande radar⁵

Luftvärnsrobotens räckvidd 10 km. Radar med upptäcktsavstånd 30 km för ett luftmål med 0,1m² radarmålärea (inkommande robot).

Jaktflygplan

JAS 39 vilket har skrov där signaturdämpande åtgärder har vidtagits. Radarmålärea 0,1 m². Aktionsradie 500 km. Fart 1000 km/h. Fpl kan starta 10 min efter order.

Gripen kan utrustas med en mängd olika robotar och missiler. Man kan även hänga på en extra tank på undersidan för att öka räckvidden. Gripen har alltid en grund beväpning oavsett uppdrag. Den består av en AIM-9 Sidewinder i varje vingspets och en automatkanon från Tyskland av märket Mauser-Werke typ Akan m/85.

Kulorna har en kaliber av 27 mm. Sedan kan Gripen utrustas beroende av vilket uppdrag den ska utföra. Sex olika robotar och missiler inklusive en bombkapsel kan bäras av JAS 39. I typfallet har jaktflygplanet 4 radarjaktrobotar Rb2000 och 2 st AIM9 samt en motmedelskapsel

Jaktrobotar

- *Rb 2000*AMRAAM Radarjaktrobot
- *AIM-9 Sidewinder*Huvudfunktion: Luftstridsmissil

Leverantör: Naval Weapons Center

Raket motorn: Hercules och Bermite Mk 36 Mod 71, 8

Längd: 2.87 meter

Diameter: 0.13 meter

Stridshuvud: Annular blast fragmentation

Vikt : 85.5 kilo

Navigeringsystem: Infrarött

Enhetskostnad: \$84,000

Radar

Multimodradar med upptäcktsavstånd 100 km mot ett luftmål med 1m² radarmålarea.

Långräckviddig radarjaktrobot med aktiv målsökare. Roboten är försedd med ramjetmotor.
Medelfart M3. Räckvidd 100 km

Nätverket

All lägesinformation från samtliga sensorer presenteras i realtid i den ledningscentral där Beslutsfattaren sitter. Denna information förs vidare i realtid till alla plattformar som kan ha intresse av den, t ex skall våra jaktflygplan kunna få kontinuerlig målinformation från flygande spaningsradar och aerostatburen radar. I normalfallet ges alla skjutorder från Beslutsfattaren. Som alternativ till den centrala beslutsfattaren skall det finnas möjlighet att flytta beslutsfattarfunktionen till en annan plattform, t ex flygande spaningsradar, baksits på en JAS39 B eller korvett. Detta ska kunna ske utan tidsfördröjning om den centrala beslutsfattaren eller delar av nätverket slås ut.

Geografiska områden och förutsättningar

Vår styrka är stationerad i en stat med rak kust i den riktning som anfallet kommer. Därefter är det 500 km vatten till motståndarstatens kust. Territorialvattengränsen går 250 km utanför kusten. Samtliga våra fasta objekt utom aerostat är samgrupperade 100 km innanför kusten. Det inbördes avståndet är dock så stort att om ett av målen bekämpas kommer övriga inte att skadas. Aerostat finns 100 km från de övriga objekten och 100 km innanför kusten.

Storlek och utformning på militära resurser

Våra

En division består av 4 jaktflygplan med 4 långräckviddiga och 2 AIM 9.

Motståndaren

Resurser framgår under rubriken "Objekt". Attackföretaget har fått uppdraget definierat i förväg och varje ingående flygplan antas följa det oavsett vad som händer. Uppdraget framgår under rubriken "Aktiviteter".

Tid och miljö

Totalt omfattar typfallet tiden från en tidpunkt då viss höjd beredskap har införts i vårt försvar tills hela anfallet är över. Totalt kan anfallet beräknas ta mindre än en timme.

Startläge och avslutningsvillkor

Scenariot börjar med att motståndarens flygplan startar från en flygbas 100 mil från målet som de ska anfalla. Våra jaktflygplan står i beredskapsläge på flygbas med 10 minuters startberedskap efter order, luftvärnet är i beredskapsläge. En flygande spaningsradar patrullerar en 400 km lång sträcka 200 km utanför kusten. Korvett patrullerar en 400 km lång sträcka 50 km utanför kusten. Samtliga sensorer på flygande spaningsradar, aerostat och korvett är igång. Försvaret har vid typfallets början vidtagit vissa åtgärder för att kunna agera mot ett överraskande flyganfall.

Scenariot avslutas när samtliga motståndarens flygplan har upptäckts och bekämpats alternativt när eget mål har utsatts för bekämpning och motståndarens flygplan har vänt tillbaka.

Idéer om fortsatt analys

Grundfrågan som skall besvaras är vilka fördelar kan man uppnå med ett nätverk i stället för med dagens ledningssystem.

Lämpliga analyser

Redan nu kan man se att det rör sig om mycket korta tider från förvarning till verkställt anfall. Det verkar rimligt att anta att just tiden för att beslutsfattare skall få relevant information och tiden för att få ut skjutorder är avgörande faktorer. Man kan också anta att en stor tidsvinst kan göras genom att om möjligt exkludera ”onödiga” steg i loopen. I vissa fall kan det kanske vara realistiskt att beslut om anfall tas av rotechefen i en av våra jaktrotar baserad direkt på lägesinformation från flygande spaningsradar. Jämför även med dagens ledningssystem och titta på hur olika tider i hela ledningsloopen påverkas om man har ett nätverk i stället.

Man bör undersöka ett antal olika fall där olika delar av nätverket är utslaget eller vissa sensorer är utslagna för att få en uppfattning om hur känsligt nätverket är för störningar.

Nätverkets funktion bör varieras lite med t ex beslutsfattare placerade på olika ställen för att se hur sårbarheten påverkas. Man kan ha flera alternativa beslutsfattare på olika plattformar. Beroende på om delar av nätverket är utslaget kan uppgiften tas över av annan beslutsfattare.

Ytterligare en möjlighet är att variera beredskapsläget. Tiden det tar för fpl att starta efter order är förmodligen mycket avgörande för utfallet. På samma sätt kan tiden för att få luftvärnsrobotbatteriet skjutklart ha mycket stor inverkan på utfallet under förutsättning att luftvärnsrobotarna kan bekämpa inkommande attackrobotar.

Steg två kan vara att titta närmare på hur nödvändiga funktioner kan realiseras tekniskt och var i nätverket informationen ska behandlas innan den skickas iväg och presenteras för berörda.

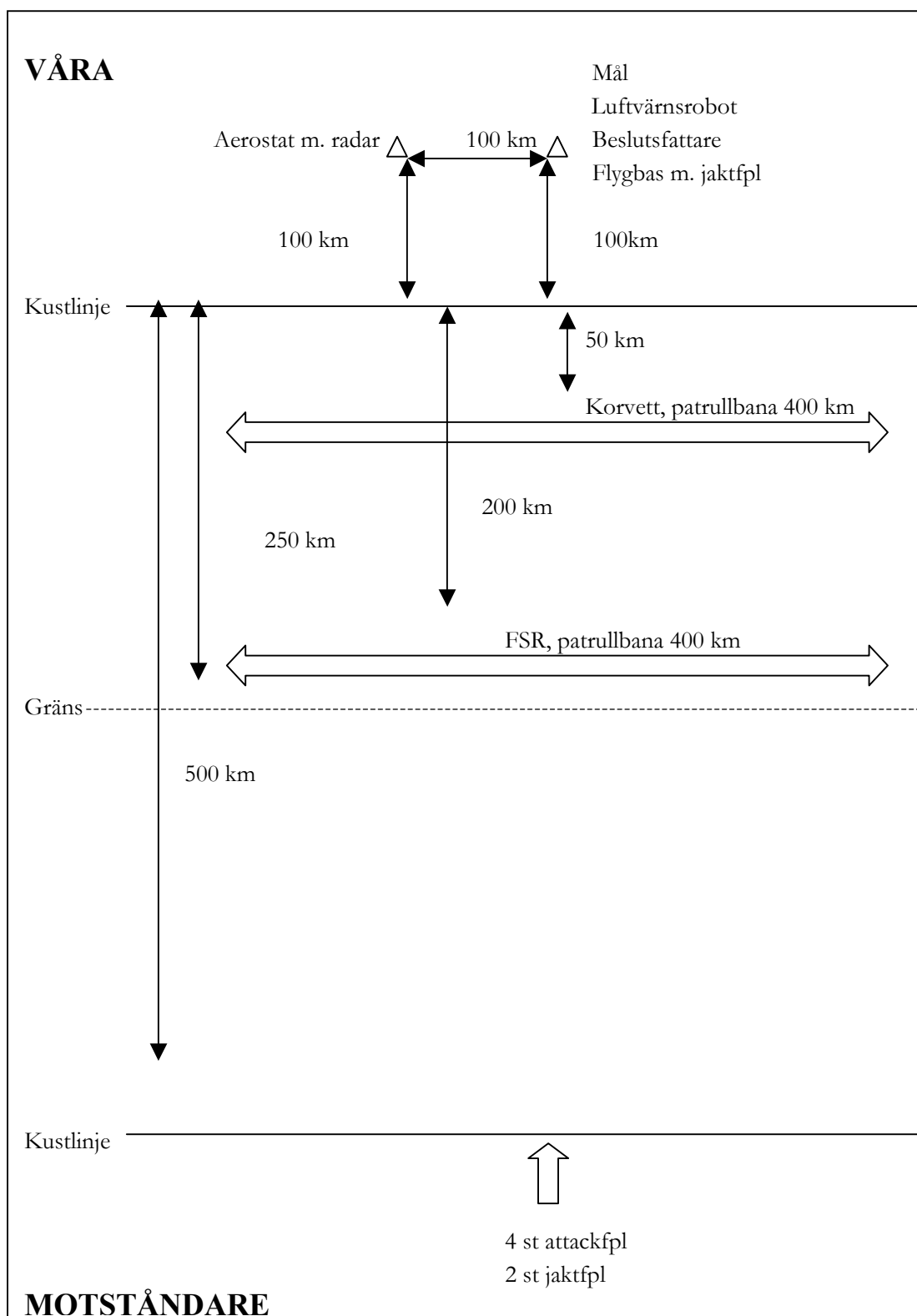
Analytiska mått som kan vara relevanta.

Sannolikhet att målet bekämpas.

Sannolikhet att civilbefolkning runt målet kan skyddas eller evakueras. Detta kan även mätas som tid som finns till förfogande till evakuering.

Tidsvinst för viktiga beslut jämfört med dagens ledningssystem.

Något mått för att mäta vinsten med att kunna flytta beslutsfattarfunktionen mellan olika platser.



Figur 13. Schematisk bild av typfall stridsflyg.

¹ Fpl och robotar baseras på rapport FOI d nr H2001/203. Radarmålareor är erfarenhetsvärden från FOI Försvarsanalys personal. Radarprestanda motsvarar bedömningar av vad som kan vara rimlig utveckling till 2002 gjorda av Rolf Kaddik, FOI Försvarsanalys.

² Generisk modell som baseras på korvetterna I Visby-serien med LV-robot typ Bamse. Radarmålarean är schablonmässigt beräknad som en tiondel av vad fartyg i motsvarande storlek har idag. Radarprestanda motsvarar bedömningar av vad som kan vara rimlig utveckling till 2020 gjorda av Rolf Kaddik, FOI Försvarsanalys.

³ FSR890 enligt Jane's all the worlds aircraft 1995-96. Radarprestanda motsvarar bedömningar av vad som kan vara rimlig utveckling till 2020 gjorda av Rolf Kaddik, FOI Försvarsanalys.

⁴ Radarprestanda som FSR890 ovan.

⁵ Generisk modell liknande LV-robot typ Bamse. Radarprestanda motsvarar bedömningar av vad som kan vara rimlig utveckling till 2020 gjorda av Rolf Kaddik, FOI Försvarsanalys.

BILAGA 4 - TYPFALL YTSTRIDSFARTYG

Sammanfattning

En fregatt från stormakt A som vägrar lyda order från sin egen försvarsmakt närmar sig i typfallet ytstridsfartyg en svensk konvoj på väg ut från Göteborg mot engelska kanalen. Konvojen transporterar svensk trupp på väg mot en internationell operation som stormakt A har intresse av att fördröja. När fregatten bedöms utgöra ett hot mot den svenska konvojen och alla försök att få den att vända misslyckats beslutar den svenska operativa insatsledningen att den skall sänkas med sjömålsrobot eller styrda bomber. Uppgiften faller på den insatsstyrka som skapats för att skydda konvojen.

Ingående verksamheter och objekt

Sverige har åtagit sig att inom ramen för en internationell operation bidra med en fullt utrustad amfibiebataljon till en internationell styrka i Asien. Bataljonen lastas ombord på tre större fartyg i Göteborgs hamn för att skeppas sjövägen till operationsområdet. I engelska kanalen skall de svenska fartygen möta en internationell konvoj som eskorteras av brittiska och amerikanska örlogsfartyg. Fram till engelska kanalen skall svenska marinen skydda de tre transportfartygen. En insatsstyrka bestående av ytstridsfartyg, helikoptrar, flygplan och kustrobotbatteri sätts ihop för att lösa uppgiften.

Stormakt A har intressen i krisområdet och vill på olika sätt fördröja den internationella styrkan. I syfte att fördröja sjötransporten har stormakt A skickat en flottstyrka till Nordatlanten och Nordsjön. Sammanstötningar har tidigare förekommit och det anses föreligga en risk för att stormakt A:s flottstyrka skall angripa de svenska transportfartygen på vägen till samlingspunkten. En grupp på tre fregatter har siktats söder om Norge på östlig kurs.

I samband med att de svenska fartygen lämnar Göteborgs hamn delar sig gruppen av fregatter och en främmande fregatt (FF) går med hög fart i riktning mot den svenska konvojen. Fartyget ignorera alla försök till kontakt via radio och beskjuter ett JAS-plan på spaningsuppdrag med en semiaktiv radarmålsökande luftvärnsrobot. Svenska diplomatiska kontakter med stormakt A leder inte till att fartyget stoppas. Tvärtom försäkrar stormakt A att de inte längre har kontroll över fartyget, dess besättning med befälhavaren i spetsen agerar på eget initiativ och fartyget vägrar lyda order om att vända. I Sverige bestämmer det Marintaktiska kommandot att det främmande fartyget skall stoppas. Med hänsyn till tidsfaktorer och risker för svensk personal och utrustning beslutar man att fartyget skall sänkas med sjömålsrobot eller styrda bomber.

När ordern kommer om att FF skall sänkas faller ansvaret på den taktiske ledare (TAL) som har ansvaret för att skydda konvojen. TAL leder ombord på korvetten HMS Karlstad till sjöss med konvojen. Insatsen försvåras av den omfattande civila sjötrafiken i området.

I första hand skall FF bekämpas med robotinsats från landbaserat kustrobotbatteri, TKRB¹, grupperat mellan Uddevalla och Munkedal. Om detta inte bedöms som möjligt på grund av riskerna för civil sjöfart skall bekämpningen ske genom insats med styrda bomber från en rote JAS från F7 i Såtenäs. Efter genomfört anfall sker bedömning av effekt genom spaning med en rote JAS.

Aktiviteter

Lägesbild

Befintliga sensorsystem används för att kontinuerligt bygga upp en lägesbild där FF kan följas. Om detaljeringsgraden i lägesbilden inte är tillräcklig nyttjas reaktiv spaning med spanings-UAV. Lägesbilden finns tillgänglig hos såväl eskortfartygen som kustrobotbatteri och JAS-flottiljen.

Ledning

TAL har underställt alla relevanta förband i området. Det innebär att TAL har befälsrätt över såväl fartyg i konvojen, kustrobotbatterier samt en rote JAS för attackuppdrag och en rote JAS för spaningsuppdrag. För att lösa sin uppgift har TAL ombord på HMS Karlstad sådana kommunikationssystem att han kan stå i direkt kontakt med JAS-divisionen på Sätenäs.

Vapeninsats, alternativ 1

TAL beordrar insats med fyra SRB mot mål FF enligt den gemensamma lägesbilden. Ordern tas emot hos TKRB som preparerar fyra SRB och fyrar av dem. SRB prepareras för att ankomma till målet vid samma tid, +/- 5 sekunder. En angriper uppifrån och tre på låg höjd ur tre olika riktningar.

Vapeninsats, alternativ 2

TAL beordrar insats med styrda bomber från två JAS-plan mot mål FF enligt den gemensamma lägesbilden. Flygplanen är, när ordern kommer, klargjorda och startar snarast möjligt. De flyger på direkt kurs mot FF och faller de laserstyrda bomberna på 12 km avstånd.

FF egenskydd

FF är utrustad med luftvärnssystem som kan användas för att bekämpa inkommande SRB eller flygplan. Dessa system nyttjas i bägge vapeninsatsalternativen.

Objekt

Främmande Fregatt - FF

FF är en fregatt för i första hand ytattackuppdrag. Displacementet är ca 2 200 ton. Den är bestyckad med två 100 mm eldrör i dubbelmontage för bekämpning av sjömål, en luftvärnskanal med semiaktiv radarmålsökande luftvärnsrobot för fjärrskydd (upp till 10 km), två luftvärnskanaler med vardera två tvillingmonterade 37 mm lvakan. Utöver dessa vapensystem har fartyget också aktiva och passiva telekrigssystem.²

HMS Karlstad

Korvett i Visbyklassen, rustad för eskortuppdrag med ubåtsjaksutrustning. I eskorten ingår även två korvetter typ Göteborg utrustade med SRB. De svenska fartygen har i detta scenario ingen annan funktion än att utgöra ledningsplattform för operationen.

Spanings-UAV

Spanings-UAV:n är landbaserad. Den är utrustad med SAR och utrustning för optisk spaning som i realtid sänder bearbetade data tillbaka till markstationen via radio. Med en laserlänk finns också förmågan att sända rådata till markstationen. UAV kan hålla sig i luften i 6-8 timmar. Spanings-UAV är samgrupperad med helikopterdivisionen på Säve.

Tung kustrobot

Den tunga kustroboten har en räckvidd på mer än 200 km och kan prepareras för att flyga mot målet helt enligt operatörens önskemål. Den är utrustad med dubbla målsökare, radar och IR, och har återattackförmåga.³

JAS-plan

JAS-plan ur delserie tre.

Styrda bomber

Laserstyrda bomber för precisionsinsats med pansarbrytande förmåga.

Geografiska områden och förutsättningar

Typfallet utspelar sig till sjöss i september månad. Platsen är västerhavet med de miljöparametrar som gäller för den tiden och platsen.

Storlek och utformning på militära resurser

Våra

C OPIL leder den operativa verksamheten. En insatsstyrka bestående av ytstridsfartyg, HKP, JAS-plan och TKRB har satts ihop för att skydda den planerade konvojen. Chefen för insatsstyrkan är taktisk ledare (TAL). Insatsstyrkan är delad i fyra stridsgrupper, 1) Ytstridsfartyg, 2) Helikoptrar 3) TKRB och 4) JAS-plan. SjöBevC (motsvarande) är ansvarig för att upprätta en lägesbild. UAV-förband lyder under SjöBevC.

Motståndaren

Motståndaren i detta fall är ett fristående fartyg.

Tid och miljö

Totalt omfattar typfallet från det att stormakt A:s stridsgrupp upptäcks till vapeninsats ca två dygn. Under denna tid skall lägesbilden upprätthållas och nödvändiga förberedelser göras, t ex gruppering av TKRB och förberedelse av JAS-plan. Momentet då FF går mot svenska fartyg pågår ca en timme.

Startläge och avslutningsvillkor

Typfallet startar då en stridsgrupp om tre främmande fregatter upptäcks söder om Norge. Då pågår redan ilastning av en amfibiebataljon i Göteborgs hamn. I hamnen ligger de fyra korvetter

som avses utgöra eskort till transportfartygen. TKRB befinner sig på övning i Karlskronaområdet och beordras vid momentets början gå mot gruppering i Uddevallaområdet. Spanings-UAV står i normal beredskap på Säve.

Spaningsresurserna i området är vid moments start de som normalt används för att bestämma sjölägesbilden.

Momentet avslutas då OPIL fått bekräftelse från egna spaningsresurser på att målet är bekämpat.



Figur 14. Schematisk bild av typfall ytstridsfartyg.

¹ Organisatoriskt har Tungt kustrobotbatteri (sannolikt) utgått ur den svenska militära organisationen. I detta scenario har det tagits med i syfte att förstärka nätverkskaraktären av den insatsstyrka som skapats.

² Den främmande fregatten är modellerad på en kinesisk Jiangwei-fregatt såsom den beskrivs i Jane's fighting Ships 2001-2002. Viss frihet avseende LV-kanalerna har utnyttjats så informationen i Jane's inte är fullständig.

³ Detta är en "generisk" SRB som i mycket liknar en RB 15 men som lika gärna kan vara en Harpoon eller liknande. De dubbla målsökarna är inlagda för att degradera verkan av FF:s telekrigsinsatser.

BILAGA 5 - TYPFALL UNDERVATTEN

Sammanfattning

Under ett uppdrag att skydda fartyg i en konvoj upptäcker i typfallet undervatten vår spaning en fientlig ubåt. Vår ubåt som finns i närheten får order att bekämpa motståndarens ubåt med hjälp av information erhållen via en fiberoptisk kabel. Med hjälp av målinformation från utplacerade spaningssensorer får vår ubåt tillräcklig målinformation för att kunna skjuta torped mot målet. Målet bekämpas och verkansvärdering sker via spaningssensorerna.

Ingående verksamheter och objekt

Vår ubåt är ute på patrulleringsuppdrag i Östersjön. Uppgiften är att tillsammans med en ytfartygsstyrka skydda handelsflottans fartyg från attack från ubåt. Vår ubåt är uppkopplad i det svenska nätverket med hjälp av en fiberoptisk kabel som rullas ut allt eftersom ubåten förflyttar sig. Den lägesbild som ubåten får erhålls från både ytövervakningsfartygens sensorer, utlagda akustiska bojar och UAV-sensorer utrustade med blågrön laser ev. också från egna utsända UUV. Ubåtens beväpning är en trådstyrd torped som styrs mot målet från vår ubåt. Efter bekämpning sker verkansvärdering med hjälp av en utskickad UUV.

Aktiviteter

Patrullering med ubåt

Ett ubåtsuppdrag kan pågå i en månad med flera ingående aktiviteter. Ett patrulluppdrag kan pågå under högst en vecka. Den skall kunna verka både i svenska farvatten och vid internationella insatser. Ubåten får i regel sig tilldelat ett spaningsområde inom vilket den skall genomföra sin uppgift.

Sammanställning av lägesbild

Sammanställning av inkommen sensorinformation sker i en underrättelsecentral i land.

Insats med torped

Torpeden skjuts från ubåten som sedan styr den mot angiven målposition.

Verkansbedömning av torpedinsats

Verkansbedömning sker med hjälp av tillgängliga sensorer.

Objekt

Våra

Ubåt

Av typen Gotland

Fart 20 knop i undervattensläge

Torped

Trådstyrd, det finns två varianter; tunga torpeder motsvarande typ 63 och lätta torpeder typ 431/451

Hydroakustisk sonar med cirkulär täckning och FAS.

UAV-buren sensor med blågrön laser

UUV med CCD-kamera och akustisk sensor

Ytstridsfartyg

Visby med sonarer

Handelsfartyg

Fartyg med vikt ca 30000 ton

Motståndaren***Ubåt***

Ubåt av typen Kilo

Torped

- *Torped TEST-71MKE TV*, en målsökarstyrd torped med aktiv sonar med TV där operatören kan välja mål under slutfasen. Vikt 1800 kg 1,820 kg med a 200 kg stridsdel.
- *Torped TEST 72*, en kölvattenstorped. Vikt 2,200 kg med 200 kg stridsdel och räckvidd 40 km.

Sonar

MGK-400EM digital sonar. Upptäcker mål i en sektor +/- 30 grader

Radar

Ubåtens radar finns i periskopet och kan detektera både ytmål och luftmål.

Geografiska områden och förutsättningar

Typfallet är förlagt i Östersjön. Räckvidden på torpeden är ca 10 mil. Spaningsområdet är en ruta 30 x5 mil.

Storlek och utformning på militära resurser

Vi har 3 ubåtar till förfogande för att täcka Östersjön. Som yttäckande skydd finns 2 korvetter. Ett heltäckande nätverk av hydroakustiska bojar är utlagda mellan svenska och finska fastlanden.

Motståndaren har 2 ubåtar som är stationerade i Östersjön. Ubåtarna är utrustade med torpeden Skvall.

Tid och miljö

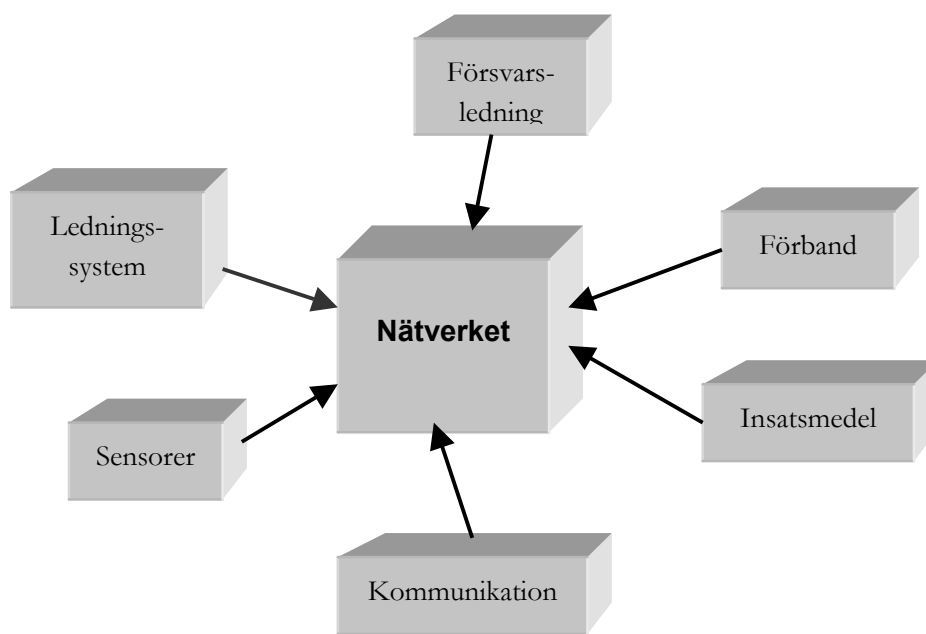
Ett ubåtsuppdrag kan pågå i en månad med flera ingående aktiviteter. Ett patrulluppdrag kan pågå under högst en vecka. Den skall kunna verka både i Östersjön, längs västkusten och även kunna skickas ut på internationella uppdrag. I det aktuella fallet är primärtområdet Östersjön. Tidpunkten är tidig höst.

Startläge och avslutningsvillkor

Typfallet startar med ett tillstånd då vår ubåt varit ute på ett spaningsuppdrag under 3 veckor. Som en sista aktivitet skall ubåten patrullera längs med en av handelsflottans leder. Vid starten av typfallet befinner sig ubåten ost Gotland och skall gå längs med en led mellan Nynäshamn och Helsingfors. Simuleringen avslutas då den fientliga ubåten sänkts eller bedömts vänt tillbaka på grund av skada eller annat uppdrag. Typfallet slutar när konvojen nått Nynäshamn.

BILAGA 6 – KRAVSTÄLLARE PÅ NÄTVERKET

Ett nätverk för försvarsmaktens behov behöver uppfylla ett antal krav på olika funktioner från en mängd kravställare. Exempel på tänkbara kravställare visas i figur 15 och exempel på deras respektive krav anges i tabellen nedan.



Figur 15. Kravställare på nätverket.

Kravställare	Behov av nätverksfunktioner
Försvarsledningen	Kommunikation, ordergivning Information, lägesbild Beslutsstöd Verifiering
Ledningssystemet	Information från sensorer egna enheter ledning förband insatsmedel Kommunikation Analysförmåga

	Sammanställningsförmåga Planeringsförmåga
Kommunikation	Transport och fördelning av information Ledning
Förband	Information, lägesbild Beslutsstöd Kommunikation Ledning, order Styra insatsmedel
Sensorer	Kommunikation Information, order Ledning Sammanställningsförmåga
Insatsmedel	Information Mållägesuppdatering Order Verifiering av verkan

Nätverkets funktioner

För att kunna tillmötesgå de krav som ställs på nätverket, måste detta kunna tillhandahålla ett antal tjänster eller funktioner. Dessa funktioner kan delas in i några huvudgrupper:

- Kommunikation
- Ledning för sensorer
- Ledningsplanering
- Beslutsstöd
- Information om
- Data från sensorer och egna enheter
- Sammanställningar

- Prognoser
- Verifiering av
 - Verkan
 - Prognoser
 - Måldata
 - Kommunikation
 - Funktion

Kraven på tillgänglighet, säkerhet och tidsfördröjning kan variera olika uppgifter ställer på nätverket kan skilja väsentligt mellan olika användare och olika uppgifter. Där kan t ex insatser vara tidskritiska vid utförandet men informationskritiska vid planeringen.

Utgivare Totalförsvarets Forskningsinstitut - FOI Systemteknik 172 90 Stockholm	Rapportnummer, ISRN FOI-R--0338--SE	Klassificering Metodrapport
	Forskningsområde Operationsanalys, modellering och simulering	
	Månad, år Januari 2002	Projektnummer E1791
	Verksamhetsgren Uppdragsfinansierad verksamhet	
	Delområde Metod och utredningsstöd	
Författare/redaktör Lisa Alsér (red) Johan Pelo Jan Aksberg Karina Waldemark Lars Höstbeck Leif Lundgren Sten-Åke Nilsson	Projektledare Olof Söderqvist	
	Godkänd av	
	Uppdragsgivare/kundbeteckning Försvarmakten	
	Tekniskt och/eller vetenskapligt ansvarig	
Rapportens titel Värdering av nätverksorienterad krigföring – Förstudie		
Sammanfattning (högst 200 ord) Vid FOI pågår studier kring nätverksbaserad krigföring i projektet FoRMA. Nätverksbaserad krigföring (Network Centric Warfare, NCW) betecknar ett system för krigföring där funktionerna kan vara uppdelade på olika plattformar och samtidigt arbeta tillsammans genom ett nätverk vilket är realiserat av informationsteknologi. Arbetsgruppen Nätverksstrid bildades i maj 2001 och gruppens uppgift är att ta fram metoder och tillämpa dessa för att bedöma och värdera väpnad strid i nätverk. Frågeställningar vid analys av nätverksbaserad strid bör vara huruvida den är möjlig, vad som är gränssättande samt vilka mervärden nätverksbaserad krigföring tillför jämfört med plattformsbaserad. Syftet med denna förstudierapport är att beskriva arbetssättet och redovisa resultatet av förstudien samtidigt som den ska fungera som en gemensam grund för det fortsatta arbetet i gruppen. Intressanta scenarier studeras för vilka man senare vill undersöka möjligheterna att utnyttja nätverksbaserad krigföring. Scenarier beskrivs för typfallen fast mål, stridsvagn, stridsflyg, ytstridsfartyg samt för ett undervattensfall. Även triviala nätverk mellan ledning, sensorer och vapen för de olika scenarierna presenteras. För att studera egenskaper och effekter av ett samlat nätverk bestående av en mängd olika komponenter beskrivs också en tänkbar struktur för ett generellt nätverk. I rapporten lyfts några kända modelleringsmetoder fram som kan få betydelse när man ska finna en metodik och systematik vid modellering av de scenarier som beskriver NCW.		
Nyckelord		
Övriga bibliografiska uppgifter	Språk Svenska	
ISSN 1650-1942	Antal sidor: 64 s.	
Distribution enligt missiv	Pris: Enligt prislista Sekretess	

Issuing organization FOI – Swedish Defence Research Agency Systems Technology SE-172 90 Stockholm	Report number, ISRN FOI-R--0338--SE	Report type Methodology report
	Research area code Operational Research, Modelling and Simulation	
	Month year January 2002	Project no. E1791
	Customers code Commissioned Research	
	Sub area code Operational Analysis and Support	
Author/s (editor/s) Lisa Alsér (red) Johan Pelo Jan Aksberg Karina Waldemark Lars Höstbeck Leif Lundgren Sten-Åke Nilsson	Project manager Olof Söderqvist	
	Approved by	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible	
Report title (In translation) Network Centric Warfare Assessment - Preliminary Study		
Abstract (not more than 200 words) Studies about Network Centric Warfare, NCW, are in progress in the project FoRMA at FOI. NCW describes a system for warfare, where the functions are separated into different platforms and at the same time are working together, through a network that is realized by information technology. The working group NCW was formed in May 2001 and the task was to develop and apply methods to assess armed combat in net-centric environment. The issue when analysing NCW should be if NCW is possible and what limitations and advantages NCW can provide compared to Platform Centric Warfare. The purpose of the preliminary study report is to describe the way of working and show the results of the preliminary study. At the same time it will serve as a common base for the group and it's further work. Interesting scenarios for which we later want to investigate the possibility to use NCW are studied. Scenarios are described for a fixed target, tank, fighter aircraft, surface combatant and an underwater case. Trivial networks between Command and Control, Sensors and Shooters are introduced. A possible structure for a general network is shown, which can be used for studying characteristics and effects of a network consisting of a number of different components. Some well-known modelling methods are mentioned in the report. They can be of importance when finding a method for modelling the scenarios, which describe NCW.		
Keywords		
Further bibliographic information	Language Swedish	
ISSN 1650-1942	Pages 64 p.	
Price acc. to pricelist Security classification		

