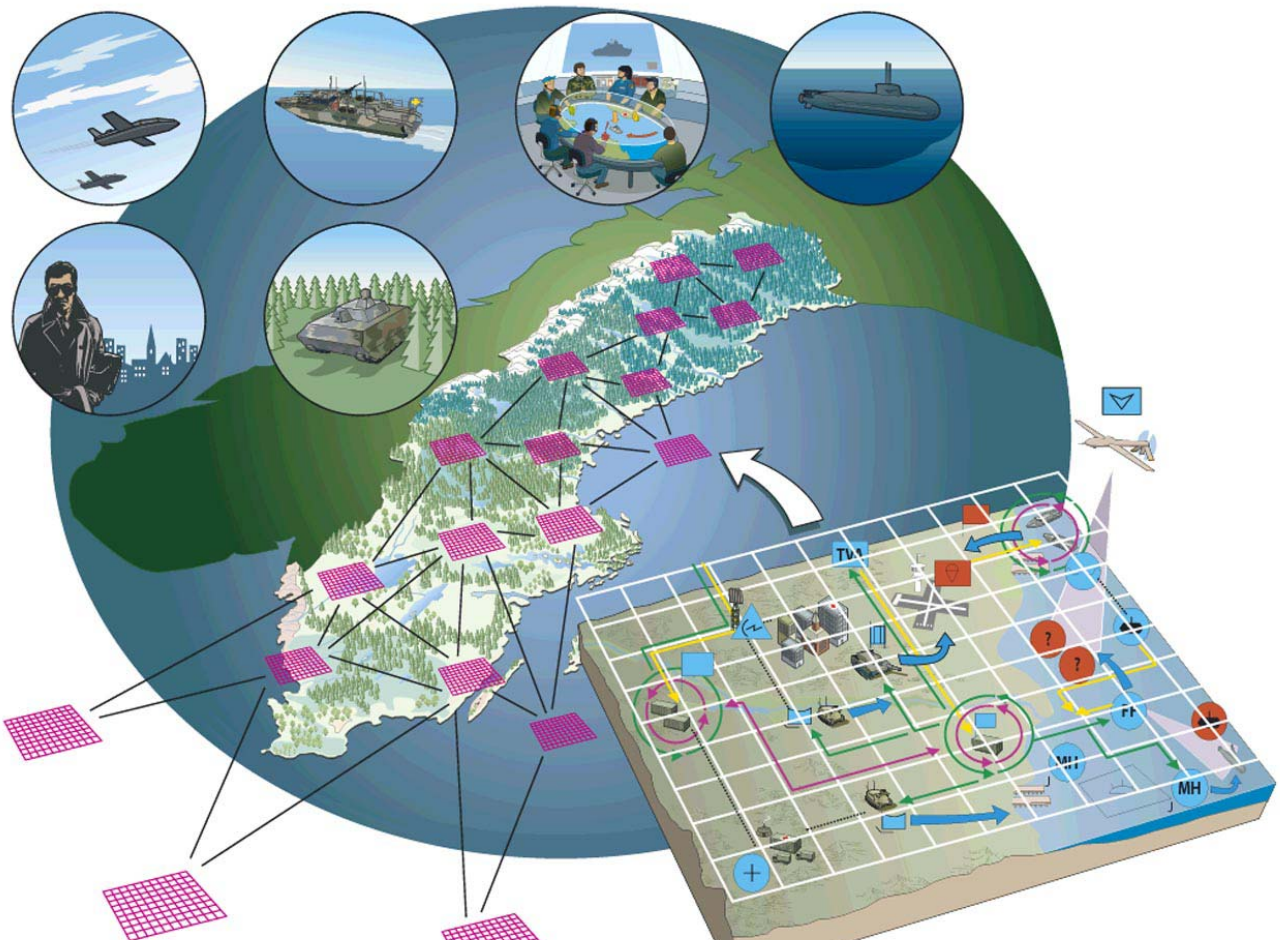
FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R--0671--SE
December 2002
ISSN 1650-1942
Metodrapport

Lars Höstbeck

Metoder för värdering av nätverksbaserad strid

Underlagsrapport i FoRMA



Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT
Försvarsanalys
172 90 Stockholm

FOI-R--0671--SE
December 2002
ISSN 1650-1942
Metodrapport

Lars Höstbeck

Metoder för värdering av nätverksbaserad strid

Underlagsrapport i FoRMA

SAMMANFATTNING

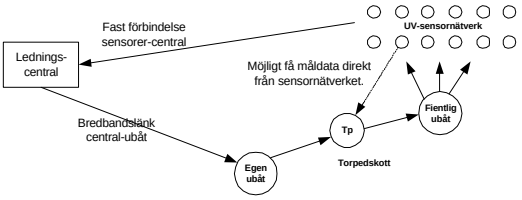
Denna rapport utgör dokumentation av det arbete som utfördes av arbetsgruppen Nätverksstrid under perioden september till december 2001. Arbetet fram till september 2001 finns dokumenterat i rapporten ”Värdering av nätverksorienterad krigföring – Förstudie, underlagsrapport till FoRMA” (FOI-R– 0338– SE).

Arbetsgruppen Nätverksstrid bildades i maj 2001 med deltagare från i första hand FOI Försvarsanalys och FOI Systemteknik. Från och med januari 2002 ombildades arbetsgruppen och fick en delvis annan inriktning. Arbetsgruppens uppgift under 2001 var att utveckla metoder för värdering av nätverksbaserad krigföring. De centrala frågeställningar som vi ville besvara var:

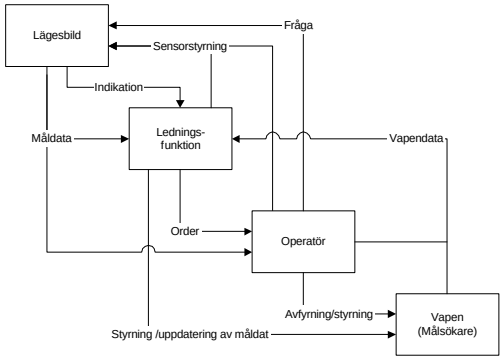
- I vilka fall är nätverksbaserad strid möjlig?
- Vad är gränssättande?
- Vilka mervärden tillför nätverksbaserad krigföring framför traditionell plattforms-baserad?

Tanken med arbetsupplägget var att koncentrera arbetet på att värdera ”sensor-to-shooter”-kedjor och att avgränsa arbetet till enbart väpnad strid. För att besvara frågorna konstruerade vi fem typfall kallade Fast mål, Stridsvagn, Stridsflyg, Ytstridsfartyg och Undervatten. Typfallen valdes så at de skulle ha olika karaktäristik avseende tidskonstanter, bakgrund, informations-överföringshastighet och målens rörelseförmåga.

För att värdera typfallen bestämdes att vi för varje typfall jämföra en nätverkslösning med en traditionell plattformsbaserad lösning. För att genomföra detta konstruerades nätverkslösningar för samtliga typfall. I första värderingen användes vad vi kallade ett trivialt nätverk, vilket vi definierade som ett nätverk bestående av minsta antal noder som krävdes för att realisera ”sensor-to-shooter”-kedjan. Dessa nätverksbilder (fig A1.) generaliserades till en schematisk beskrivning av kedjan (fig A2).



Figur A1. Schematisk beskrivning av en nätverkslösning för typfallet Undervatten



Figur A2. Sensor-to-shooter schema för ett nätverk av avancerade system.

Värderingen avsågs ske genom att vi för varje fall tog fram en systemeffekt, dvs ett mätetal på hur bra kedjan fungerade. Systemeffekterna för nätverksfallen skulle sedan jämföras med

systemeffekterna för plattformsfallen i avsikt att besvara frågorna ovan om när det är möjligt och vilka mervärden som tillförs genom övergång från plattformsorienterad till nätverksbaserad krigföring. Genom variationsresonemang och känslighetsanalys för de olika fallen avsågs att få indikationer på vilka parametrar som är gränssättande. Tidigt i resonemangen framstod det som tydligt att systemeffekten inte var ett entydigt begrepp. Samma effekt, t ex överlevnadssannolikhet kunde uppnås med olika stora resurser och beroende på hur mycket tid som fanns att agera på. Vi tror därför att avvägningen effekt-resurs-tid är viktigt för att få en helhetsbild av hur förmågan till väpnad strid på verkas av övergången till ett nätverksbaserat försvar.

Som en metod för att ta fram systemeffekterna och studera hur olika parametrar såsom tid och precision i läge påverkar systemeffekten utvecklade vi det vi kallade Funktionsscheman. Idén är hämtad från FMV och LVU99. Dessa scheman är en sekventiell beskrivning av hur en kedja gör mellan olika aktörer och utgör en grund för att beräkna vilka tidskonstanter som krävs respektive erbjuds av nätverket.

Intimt kopplat till tidskonstanterna är precision i lägesbestämningarna. Ett snabbt överfört målläge med stort fel är inte mer värt än ett långsamt överfört läge med god precision. Det är också på området lägesbestämning och överföring av lägesdata som man kan förvänta sig att informationsteknologin ger stora möjligheter till förbättringar. Det framstod därför för arbetsgruppen som viktigt att finna metoder för att värdera kvaliteten på lägebilden och hur den nyttjas. Vi introducerade därför begreppet abstrakt lägesbild som kan anses bestå av samtliga lägesdata som existerar i nätverket. För att presentera en rollbaserad lägesbild någonstans i ledningssystemet antas existensen av en funktion F som opererar på den abstrakta lägesbilden för att ta fram en konkret, rollbaserad lägebild. Denna funktion F utgör en ”ny” informationskomponent i den nätverksbaserade lösningen som inte funnits i samma utsträckning i de tidigare, plattformsorienterade lösningarna. Värderingen av denna informationskomponent blir därmed en viktig del av värderingen av det nätverksbaserade konceptet. I ett försök att värdera vissa av dessa olika funktioner utvecklas metoder för att beräkna mått på kvaliteten på mållägesbilden. Denna metodutveckling är påbörjad i och med det arbete som utfördes under hösten 2001, men den är inte avslutad.

Som en enkel form av ”benchmarking” har vi studerat tre olika metoder för värdering av nätverksbaserad strid som publicerats i öppen litteratur. De tre som studerats är den som beskrivs av Alberts et al i ”Network Centric Warfare” [Alberts 1999], NUWC metod för värdering av nätverksbaserad ubåtsjakt [Cleveland 1999, Christian 2001] och RANDs ”MOE for the Information Age Army” [Darilek 2001].

Ur detta publicerade material kan vi se en trend i att information behandlas som en storhet i beslutskedjan där informationen genomgår en process från att den samlas in till att den omsätts i en åtgärd. Denna process är relativt generell och stämmer ganska väl med vår arbetsgrupps syn på information, dock med det förbehållet att denna arbetsgrupp inte berört de högre nivåerna i beslutskedjan. Synen på hur man skall värdera nyttan av informationen i beslutskedjan skiljer sig dock åt mellan olika organisationerna. De två sätt man kan skilja ut är dels att försöka se hur informationskomponenten påverkar traditionella parametrar som räckvidd och reaktionstid, dels att försöka kvantifiera information som en storhet i sig och sedan lägga till en informationsfaktor i sina modeller. Medan vi i stort ansluter oss till den första synen, att se hur informationen påverkar traditionella parametrar, har RAND valt den andra, att skapa en ”kunskapsfaktor” som sedan läggs in i Lanchesterekvationerna.

FÖRORD

Arbetsgruppen Nätverksstrid har varit en grupp. Resultatet av arbetet är en följd av hela gruppens bidrag. När gruppen bildades var det klart uttalat att olika individer skulle bidra med olika kompetenser. Självklart har olika individer bidrag olika mycket på olika områden, men de flesta har kunna komma med fruktbara bidrag även på de områden som inte varit ”deras”. Deltagare i gruppen var, förutom undertecknad, även Lisa Alsér, Ulla Backlund, Leif Lundgren, Karina Waldemark. Martin Hagström, Maria Sjöblom och Sten-Åke Nilsson, samtliga vid FOI samt Lars Flemström, FMV.

Denna rapport behandlar i huvudsak värderingen ur ett teoretiskt perspektiv. Även om undertecknad har skrivit huvuddelen av innehållet och står som författare så är de flesta tankar och idéer följder av diskussioner i arbetsgruppen mellan framförallt, mig själv, Leif Lundgren, Karina Waldemark och Lars Flemström.

Stockholm i december 2002

Lars Höstbeck

INNEHÅLLSFÖRTECKNING

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 inom informationsteknologiområdet.

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 i termer av funktioner, förmågor och tjänster, sammanhållet av ett gemensamt nätverk.

Inom det svenska försvaret har de förestående förändringarna i tur och ordning betecknats med RMA (Revolution in Military Affairs), Ny krigföring och Nätverksbaserat förvar, NBF. Också andra begrepp såsom Nätverksorienterad krigföring och Nätverkscentrerat försvar före-kommer. Om inget annat anges kommer i denna rapport dessa begrepp, och varianter av dem, att användas synonymt med varandra.

1.1 Uppgift och arbetsgrupp

Vid FOI, och tidigare vid FOA, pågår studier kring NBF i projektet FoRMA (Forskning om RMA). Inom ramen för FoRMA arbetade under 2001 en delstudiegrupp med att studera väpnad strid i en nätverksorienterad miljö.

Delstudiegruppen bildades i maj 2001 med representanter från framför allt FOI Systemteknik och FOI Försvarsanalys. En av gruppens uppgifter under 2002 är att utveckla och tillämpa metoder för att värdera väpnad strid inom ramen för ett nätverksbaserat försvar. De centrala frågeställningarna vid analys av nätverksbaserad strid formulerades som:

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

Under arbetets gång har det blivit mer och mer tydligt att det finns väldigt lite material tillgängligt avseende värdering av nätverksbaserat försvar. Medan det finns åtskilligt publicerat kring värdering av plattformar och system finns det väldigt lite publicerat kring funktionsuppdelade lösningar och system av system. Arbetsgruppens första uppgift var därför att avgränsa och definiera problemet så att det fick en hanterlig form för att sedan utveckla metoder för att värdera lösningar inom denna form, med sikte på de tre frågeställningarna ovan.

När gruppens arbete startade våren 2001 avsågs arbetet att bedrivas i en förstudiefas som avslutades i september 2001 och en huvudstudiefas som skulle avslutas i april 2002. Från och med årsskiftet 2001/02 fick gruppen nya instruktioner från ledningen av FoRMA-projekt och då ändrades också arbetets upplägg, liksom gruppens sammansättning. Ursprungligen planerades en förstudierapport under hösten 2001[1], en lägesrapport vid årsskiftet (denna rapport) och en slutrapport under våren 2002. Då arbetsupplägget ändrats så har även tidpunkter och inriktning av rapporter ändrats jämfört med den ursprungliga planen.

1.2 Angreppssätt

Den övergripande metodik som arbetsgruppen avser att följa finns beskriven i förstudierapporten (Alsér m fl 2002). Angreppssättet kan sägas vara en ”bottom-up” metod för att försöka värdera väpnad strid i nätverksstrukturer. Vi begränsar oss till ”sensor-to-shooter”-kedjor där vi försöker värdera hur dessa kan fungera i ett nätverksorienterat system som disponerar mer information

och annorlunda ledningsförmåga än det traditionella plattformsbaserade systemet. Vi gör inte något försök att värdera informationen i sig eller hur information på ett övergripande sätt påverkar förutsättningarna för Försvarsmakten att lösa sina uppgifter. Vidare begränsar vi oss till just väpnad strid och försöker inte värdera nätverkslösningar i samband med PSO.

Det är dock uppenbart att den största skillnaden mellan det nätverksbaserade försvaret och det traditionella försvaret är just informationskomponenten. Hur denna informationskomponent påverkar förmågan på den ”sensor-to-shooter”-nivå vi rör oss är därför viktigt att förstå och hantera. En synnerligen begränsad studie av några få tillgängliga publikationer har därför gjorts i syfte att studera hur informationskomponenten kan vägas in i värdering av det nätverksbaserade försvaret.

1.3 Läsanvisning

Denna rapport utgör dokumentation av det metodutvecklingsarbete som skedde under hösten 2001 och ett urval av angreppssätt för värdering av nätverksorienterad strid som det gått att finna i publicerade artiklar och i litteratur. Avsnitt två ger en kort genomgång av den verksamhet som genomförts i projektet fram till december 2001.

Avsnitt tre innehåller beskrivningar av metoder som utvecklades av arbetsgruppen under hösten. Dessa syftar till värdering av begränsade ”sensor-to-shooter”-kedjor i ett antal väl definierade typfall. Dessa typfall finns beskrivna i förstudierapporten samt kortfattat i bilaga ett till denna rapport. Det som beskrivs avseende metoderna är så långt som arbetet kommit ungefär vid årsskiftet 2001/2002. Det innebär att mycket återstår. Specifikt så finns ett stort antal parametrar, framförallt sannolikheter, som används men som inte definierats. Vidare arbete kan bestå i att forma uttryck för dessa parametrar.

Begreppet funktionsscheman som arbetsgruppen ”ärvde” från LVU99 som ett verktyg för att ställa samman kunskap om olika delsystem och –processer till en sammanhängande kedja presenteras i avsnitt fyra. I detta sammanhang är det viktigt att påpeka att gruppen till årsskiftet aldrig hann löpa igenom en hel värderingsprocess och därmed prövades aldrig funktionsschemat som arbetsmetod.

Avsnitt fem visar på några vägar att värdera informationskomponenten i nätverksstrid som presenteras i icke sekretessbelagd litteratur. Detta skall ses som en introduktion till hur man på annat håll tänker sig att värdera nätverksbaserat försvar. Tid och resurser har inte medgivit att detta kunnat följas upp, varför det föreslås bli en uppgift på framtida projekt kring värdering av NBF.

Avsnittet sex innehåller slutsatser, rekommendationer och förslag till fortsatt arbete. Rapporten avslutas med en bibliografi med förslag till litteratur som är relevant för värderings-problematiken. För en utförligare litteraturlista avseende nätverksbaserat försvar hänvisas till bibliografin i förstudierapporten.

[1] Alsér, L m fl, ”Värdering av nätverksorienterad krigföring – förstudie”, FOI-R–0338–SE, januari 2002.

2 GENOMFÖRD VERKSAMHET

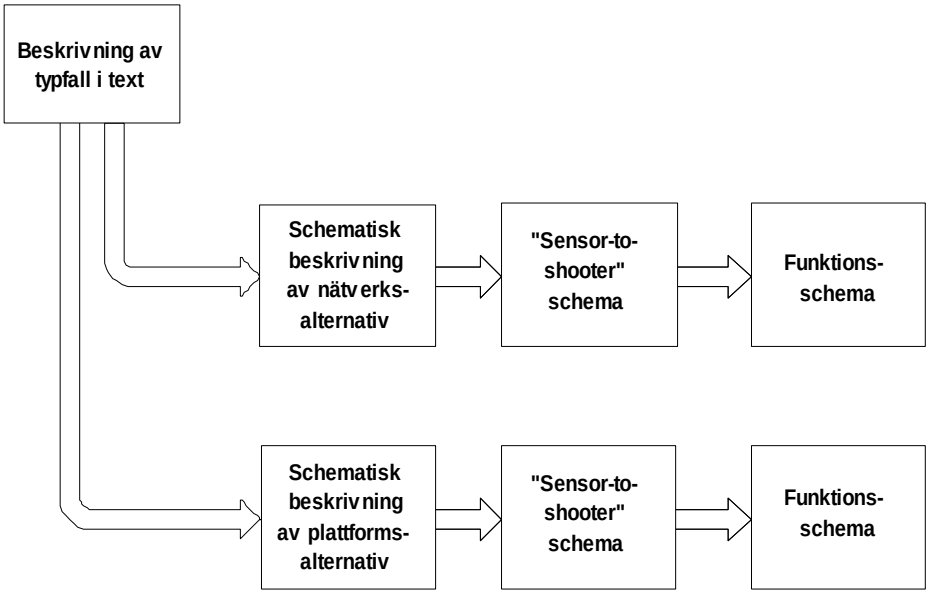
2.1 Arbetsgång i korthet

Under förstudiefasen, maj-september 2001, genomfördes det övergripande metodutvecklingsarbetet. Arbetet delades upp i fyra delmoment kallade Definition, Trivialt nätverk, Generellt nätverk och Modelleringsansats. De olika delmomenten beskrivs ingående i förstudierapporten. Under förstudien genomfördes huvuddelen av definitionsmomentet. Däri ingick bland annat att ta fram de olika typfall vi avsåg att arbeta vidare med.

I det andra momentet kallat Trivialt nätverk avses att värdera en ”sensor-to-shooter”-kedja för vart och ett av de fem framtagna typfallen. Kedjan skall värdera dels ett traditionellt plattformsorienterat system, dels ett nätverksorienterat system. Dessa två alternativ skall sedan jämföras med varandra för att man skall kunna göra en utsaga om för- och nackdelar samt (eventuella) vinster med ett nätverksbaserat system. I detta andra moment avses nätverket bestå av det minsta antal noder som krävs för att realisera ”sensor-to-shooter”-kedjan. Detta blev också den definition vi använde på begreppet Trivialt nätverk.

I moment tre avses värderingen att göras om för samma typfall men nu i ett Generellt nätverk. Med ett Generellt nätverk avses ett nät som består av flera, redundanta noder och kommunikationskanaler, och kanske också med flera samtidiga verksamheter, som därmed konkurrerar om bandbredd etc. Ett sätt att göra detta som diskuterades i arbetsgruppen var att låta nätverket hantera samtliga fem typfall samtidigt.

Under förstudiefasen genomfördes en inventering av modelleringstekniker och verktyg som kan tänkas stödja värderingen i delmomenten två och tre. Delmoment fyra utgör modelleringen av de metoder som utvecklas. Under perioden oktober-december 2001 hann inte modelleringen påbörjas.

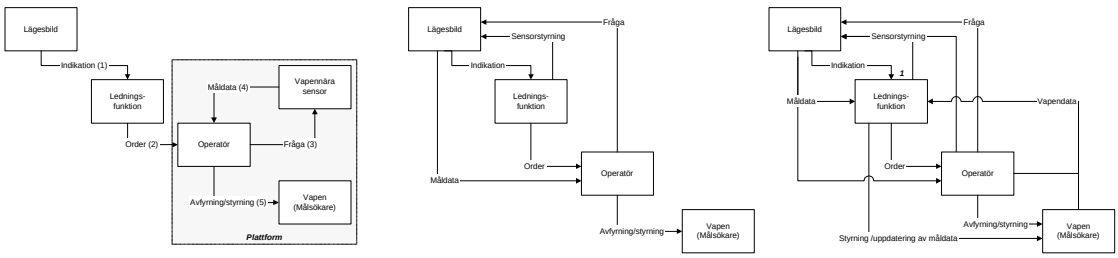


Figur 1. Arbetsgång för att översätta ett typfall i text till funktionsschema. Observera att för varje typfall tas två funktionsscheman fram, ett för nätverksalternativet och ett för plattformsalternativet.

2.2 Typfall och nätverk

Första steget i värderingen av typfallen är att översätta dessa till de funktionsscheman som vi valt att arbeta med. Denna process sker i tre steg där typfallet först struktureras i en schematisk beskrivning, denna beskrivning generaliseras till en ”sensor-to-shooter”-kedja och kedjan slutligen beskrivs i ett funktionsschema. Arbetsgången illustreras i fig 1.

De schematiska beskrivningarna av typfallen presenteras i förstudierapporten. De återfinns också i avsnitt fyra i denna rapport. Utgående från dessa schematiska beskrivningar togs motsvarande ”Sensor-to-shooter”-scheman fram (fig 2 nedan). Efter detta steg framstod det som att de typfall vi tagit fram kunde sorteras in i tre olika ”senors-to-shooter”-scheman. De tre olika kan sägas svara mot plattformsfallet (fig 2 vänster), ett fall med ungefär dags system sammanknutna i ett nätverk, kallat Nätverk av befintliga system (fig 2 mitten) och ett fall med nätverksanpassade system sammanknutna i ett för dessa system avpassat nätverk , kallat Nätverk av avancerade system. (fig 2 höger). De olika varianterna presenteras närmare i avsnitt tre.



Figur 2. De tre varianterna på ”Sensor-to-shooter”-scheman som identifierats ur de fem typfallen. Från vänster till höger kallade Plattform, Nätverk av befintliga system och Nätverk av avancerade system.

2.3 Systemeffekter

Vi har utgått från att varje typfall, såsom de beskrivs av scheman enligt fig 2 ovan kan beskrivas med en systemeffekt. Denna systemeffekt antas bero på vilka egenskaper system har, såväl tekniska som organisatoriska, och vilka resurser som finns tillgängliga. Vidare antas att tiden för att lösa uppgiften är en ”fri” parameter i den meningen att samma systemeffekt antas kunna uppnås med färre resurser om det finns mer tid tillgänglig. Ett typexempel på det kan vara förvar av fartyg mot sjömålsrobotar där man under vissa förutsättningar kan förvänta sig samma överlevnadssannolikhet (= systemeffekt) med färre lv-system om man har med tid på sig att bekämpa ett inkommande hot.

Första steget i värderingen blir att ta fram systemeffekterna i de olika typfallen. En ansats till hur man kan gå tillväga presenteras i avsnitt tre. Systemeffekterna enligt vårt arbetssätt har sin grund i tekniska och taktiska parametrar såsom överföringshastigheter, gångtider, precision i lägesuppgifter etc. Redan i detta skede kommer vi till en viss del att besvara frågorna ”När är nätverksbaserad strid möjlig?” och ”Vad är gränssättande?” genom att vissa stridsförlopp förväntas kräva sådan kvalitet på data i tid och rum att nätverket inte förväntas kunna leverera dem.

För att besvara frågan ”Vilka mervärden tillför nätverksbaserad krigföring framför traditionell plattformsbaserad?” avses göras jämförelser mellan de nätverksbaserade och de plattforms-baserade fallen. En försiktighet i slutsatserna av en sådan jämförelse är nog på sin plats då den metod vi avser använda oss av inte tar hänsyn till sådant som ”dual-use” av tekniska system eller systemens nytta vid andra aktiviteter än dem vi formulerat i typfallen.

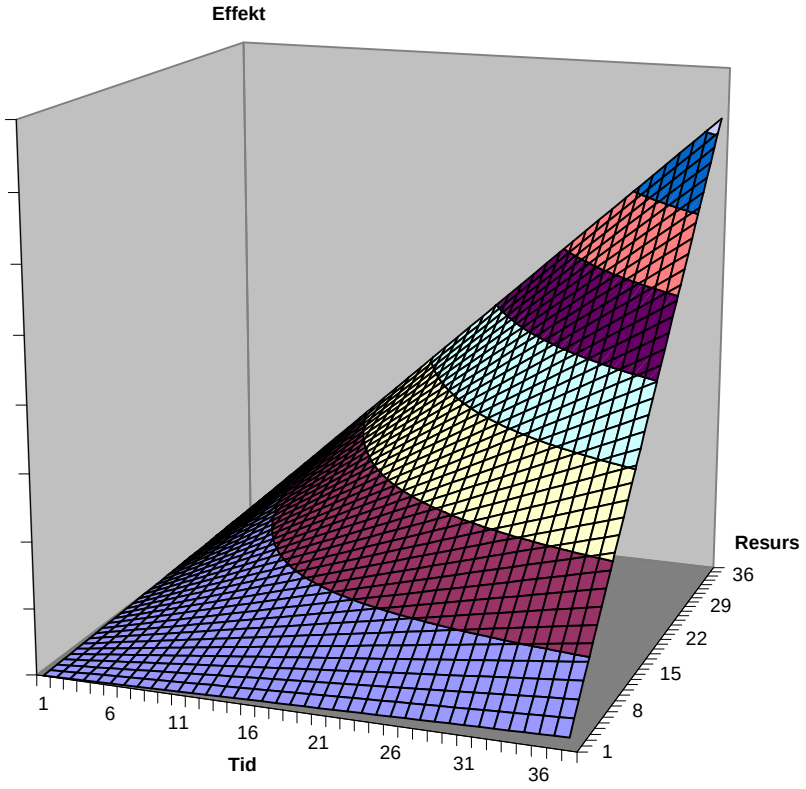
Som antyds ovan i exemplet med lv-system och sjömålsrobotar förväntar vi oss viss flexibilitet i systemet. Särskilt förväntar vi oss en korrelation mellan parametrarna systemeffekt, tid och resurs. Med större resurser förväntas högre systemeffekter och med längre tid till förfogande förväntas samma systemeffekt kunna uppnås med en mindre resurs. Ett hypotetisk samband mellan tid, resurs och effekt visas i figur 3.

Genom en känslighetsanalys av relationen effekt-tid-resurs som tas fram hoppas vi kunna undersöka två principiellt olika processer:

- Nätverkets uppbyggnad
- Nätverkets sönderfall

I frågan om uppbyggnad av nätverket kan man tänka sig att vi kravställer vilken som är den minsta systemeffekten som kan accepteras och sedan optimerar systemet med avseende på tid som står tillbuds och resurs som krävs. Vi kan också tänka oss att låsa någon av de andra parametrarna och sedan studera vilken systemeffekt som uppnås då tillgänglig tid respektive resurser förändras.

När det gäller nätverkets sönderfall så handlar det om att nyttja relationen effekt-tid-resurs till att studera hur ett systemeffekten av ett bestämt nät degraderas då resurser tas bort , dvs bekämpas eller allokeras för annat ändamål. Ett önskemål vore kunna hantera detta i en simuleringsmodell så att ett stort antal variationer på varje typfall kan köras för att ge ett statistiskt uttalande om hur ”värdefulla” de olika noderna och länkarna i nätverket är.



Figur 3. Exempel på ett enkelt, hypotetiskt samband mellan effekt, tid och resurs. Samma effekt kan nås med flera olika kombinationer av tid och resurs, medan samma resurs leder till olika effekt beroende på den tid som finns till förfogande. Genom att ta fram dessa ytor för de olika typfallen kan man studera hur förändringar i en parameter påverkar de andra.

3 VÄRDERINGSANSATS

För att skapa en förmåga att värdera nätverksstrid är det viktigt att veta hur nätverket är uppbyggt i den betydelsen att vi bör veta vilka flöden som förekommer i nätet. Under arbetsgruppen Nätverksstrids inledande arbetet med olika typfall framstår det som om det finns olika grader av ”nätverksanpassning” av systemen. De tre som finns representerade bland våra typfall har vi betecknat:

- Plattform
- Nätverk av befintliga system
- Nätverk av avancerade system

Att det är skillnad mellan det traditionella plattformsfallet och nätverksfallet är i princip en förutsättning för arbetet, även om det ännu inte är bevisat. Att det däremot kan vara skillnad mellan olika nätverkskoncept är inte lika tydligt, men synnerligen troligt.

3.1 Olika aktörer i kedjan

I nedanstående beskrivning av olika typer av sensor-to-shooter-kedjor används ett antal aktörer och begrepp som bör definieras.

Lägesbild: En gemensam datamängd avseende läget i ett område. Datamängden byggs upp av flera källor och finns tillgänglig på olika nivåer och plattformar. Bilden har någon grad av gemensamhet och någon kvalitet avseende överensstämmelse med verkligheten och relevans för det syfte lägesbilden skall fylla. I beskrivningen nedan ska lägesbild ses som en samlingsbeteckning på all lägesinformation som finns i systemet. Presentationen av lägesbilden kan konkret se olika ut på olika nivåer i systemet.

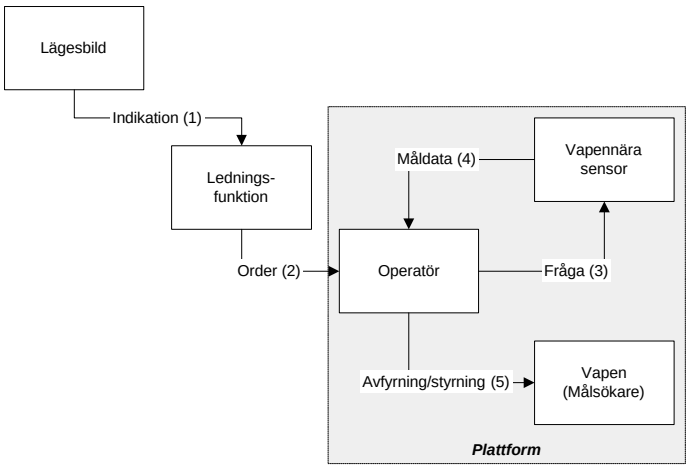
Ledningsfunktion: En funktion för ledning på en eller flera nivåer där beslut om insats kan fattas. Observera att ledningsfunktionen i sig kan bestå av en kedja av ledningsnivåer, till exempel taktiskt kommando, brigad, bataljon, kompani.

Operatör: Detta är den enhet som fyrar av vapnet och som är ansvarig för att vapnet prepareras och riktas rätt. Det kan till exempel vara en robotpluton vid amfibiebataljon eller en flygförare i JAS 39.

Vapennära sensor: Detta är den sensor som finns knuten till ett visst vapen eller en viss plattform, speciellt avsedd för vapeninsats. Det kan vara en eldledningsradar på ett fartyg eller ett TV/IR-riktmedel i en stridsvagn. Detta är den sensor som operatören normalt ”siktar” med.

Vapen: Den del av systemet som ger verkan i målet. Det kan vara ett ballistiskt vapen, t ex en kula, bomb eller granat. Det kan vara ett styrt vapen, t ex en laserstyrd bomb eller en kommandostyrd robot eller det kan vara ett målsökande vapen, t ex en långräckviddig jaktrobot eller en torped.

3.2 Plattform



Figur 4. Schema för en funktions-/ insatskedja i plattformsfallet

Plattformsfallet är det som används traditionellt. En schematisk bild visas i fig 4. Siffror i parentes hänvisar till motsvarande händelse i fig 4. En lägesbild ger en indikation (1) till ledningsfunktionen om att det krävs någon form av insats. Ledningsfunktionen ger sedan order (2) till en enhet/plattform att utföra insatsen. Operatören på den skjutande enheten siktar sedan på målet genom att ”fråga” (3) sin eldledningssensor var målet finns. När tillräckliga måldata (4) erhållits avfyras vapnet (5).

I det fall det handlar om ett ballistiskt vapen slutar kontrollmöjligheten efter avfyrning. Den vapennära sensorn kan ibland, men inte alltid, användas för bedömning av effekt av insatsen.

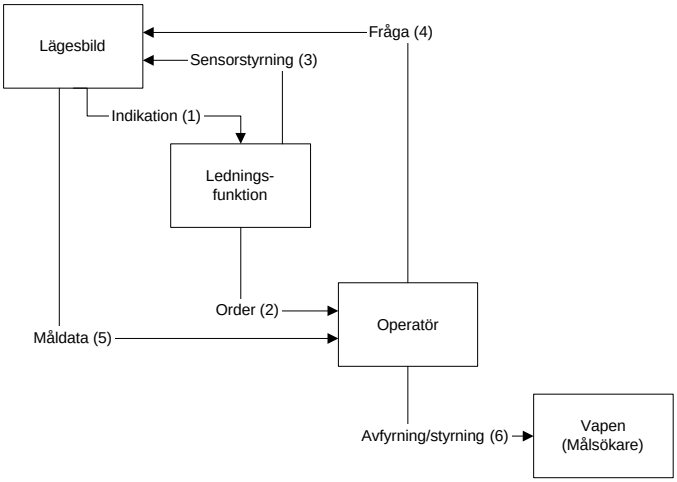
Om det är ett styrt vapen fortsätter operatören att kontrollera vapnet genom att upprepa kedjan fråga (3), måldata (4) och styrning (5) tills vapnet träffat i målet eller på annat sätt förbrukats.

Ett målsökande vapen har sannolikt operatören ingen kontroll över efter avfyrning och det kan därför ur värderingssynpunkt behandlas såsom ett ballistiskt vapen med hög träffsannolikhet.

3.3 Nätverk av befintliga system

Nätverket av befintliga system kan ses som en övergångslösning under en period då befintliga system nyttjas och kopplas ihop på sådana sätt att systemeffekten blir större än den traditionellt skulle ha varit. Några nya förmågor hos de enskilda systemen introduceras inte. Däremot skapas förhoppningsvis en ny systemförmåga hos nätverket som helhet, den att kunna nyttja data i den gemensamma lägesbilden för att invisa vapen.

En insats inleds på samma sätt i detta nätverk som i plattformsfallet. En schematisk bild visas i fig 5. Siffror i parentes hänvisar till motsvarande händelse i fig 5. Det inleds med en indikation (1) från en lägesbild. Skillnaden är att informationsteknologin nyttjas på ett sådant sätt att lägesbilden håller en bättre kvalitet än motsvarande bild i plattformsfallet. Av den anledningen är det viktigt att kunna fastställa kvaliteten på lägesbilden för att kunna avgöra skillnader mellan nätverksfallet och det klassiska plattformsfallet. Ledningsfunktionen beslutar om en insats och en order (2) går till en operatör. Här förutsätts en förändring mot plattformsfallet i det att operatören inte är beroende av en egen, vapennära sensor för insatsen utan kan använda de sensordata som finns i den gemensamma lägesbilden.



Figur 5. Schema för funktions-/insatskedja för ett nätverk av system som i huvudsak är anpassade för traditionell krigföring.

Styrning av vapen kräver sannolikt mer detaljerade lägesdata än vad som krävs för beslut om insats. För att nätverket skall kunna tillhandahålla data av tillräckligt kvalitet måste sannolikt högupplösande sensorer styras in mot målet. Detta kräver i sin tur någon form av sensorstyrning (3) som ser till att måldata av rätt kvalitet finns tillgängliga i systemet i rätt tid. Frågan (4) om måldata går inte till egen sensor utan till lägesbilden som sedan levererar måldata (5) till operatören. Operatören avfyrar (6) och styr sedan sitt vapen på samma sätt som i plattformsfallet ovan. Det krävs att uppdatering av måldata från det gemensamma sensornätet sker snabbt och med sådan kvalitet att det duger för styrning av vapnet. Om det inte är möjligt måste systemet kompletteras med en vapennära sensor.

För att lägesbilden skall kunna generera måldata av sådan kvalitet att de kan användas för en vapeninsats krävs att sensornätverket styrs genom någon form av sensorledning/styrning (3). Skillnaden mellan data som används för övervakning och måldata som kan användas för invisning av vapen antas vara olika krav på tids- och positionsnoggrannhet respektive klassificering/identifiering. Måldata kan sannolikt skapas i lägesbilden på två olika sätt.

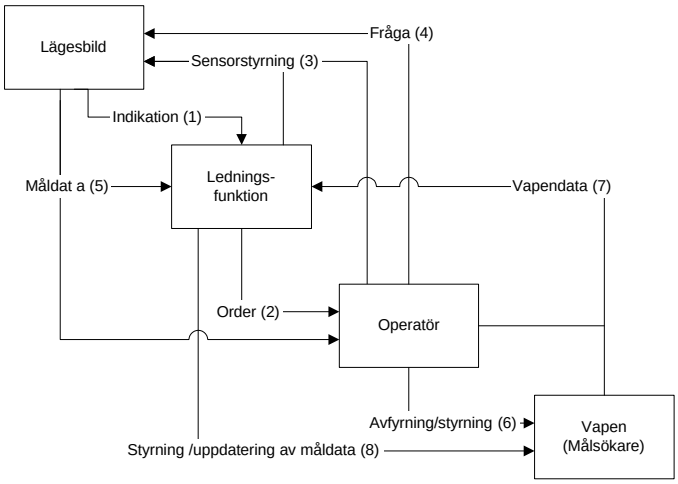
Det första sättet är reaktiv spaning där en eller flera sensorbärande plattformar sänds ut för att mäta in målet. Ett vanligt sätt att lösa detta i spel och studier för land- och sjömål är att nyttja UAV/UUV. Det andra sättet är att med befintliga sensorer i nätverket efterfråga mer detaljerad information. Detta kan vara möjligt om det i nätet redan finns data eller sensorer som inte nyttjas fullt ut eller som kan fusioneras med en högre grad av detaljnoggrannhet. Denna möjlighet blir beroende på hur sensornätet byggts upp och möjligheten kanske inte alltid står till buds.

Skillnaden mellan det traditionella plattformsbaserade fallet och fallet med befintliga system sammankopplade i ett nätverk förväntas vara att nätverket ger en bättre lägesbild med högre kvalitet på data. För att realisera detta krävs någon form av sensorledning. För att bedöma skillnaden mellan plattformsalternativet och nätverksalternativet krävs en värdering av kvaliteten på lägesbilden avseende hur den överensstämmer med verkligheten över tiden och hur relevat den är för de uppgifter som skall utföras.

3.4 Nätverk av avancerade system

Nästa steg i utvecklingen är ett nätverk uppbyggt av avancerade system direkt anpassade för att agera i nätverket. Först när sådana system är framtagna kan den fulla potentialen i ett nätverksbaserad försvar exploateras.

En schematisk bild visas i fig 6. Siffror i parentes hänvisar till motsvarande händelse i fig 6. Detta fall börjar precis som de andra med att ledningsfunktionen får en indikation (1) från lägesbilden på att en insats krävs. En order (2) om insats går till en operatör av ett vapensystem. Om systemen designas specifikt mot ett nätverksbaserat försvar bör även operatören av vapensystemet ha en viss sensorledningsförmåga och kan därför själv begära de sensorresurser som behövs (3). Operatören frågar sedan sensornätet om måldata (4) som sedan levereras av lägesbilden (5) varefter operatören avfyrar (6) sitt vapen.



Figur 6. Schema för funktions-/ insatskedja för avancerade system som är designade för nätverket.

Om vapnet har sådan kapacitet att det har egna sensorer, kommunikation och styrförmåga kan nu vapnet själv informera operatören och ledningsfunktionen om sin position och status (7). Ett exempel på det kan vara en fiberoptisk robot som skickar tillbaka en bild av vad den ser i sin målsökare.

För system där vapnet inte själv har denna förmåga att informera ledningsfunktionen om sitt läge och status kan det tänkas att informationen istället skickas till ledningsfunktionen (7) från operatören eller från någon annan som har förmåga att mäta in vapnet. Förutsatt att det någonstans i ledningsfunktionen finns tillgång till måldata kan nu vapnet överlämnas av operatören till någon annan som styr det (8). Detta kan nyttjas till exempel då man vill placera missiler i vänteläge och nyttja dem mot hastigt uppdykande mål som någon annan än operatören kan observera.

Skillnaderna mellan fallet Nätverk av befintliga system och Nätverk av avancerade system ligger i huvudsak i att systemen i det senare fallet är speciellt framtagna för att agera i nätverket. Ett antagande om de avancerade systemen är att de kommer att ställa större krav på nätverkets kapacitet för kommunikation än vad ett nätverk av befintliga system gör.

3.5 Systemeffekter

De centrala frågeställningarna för analys av nätverksbaserad krigföring som definierats i arbetsgruppen är:

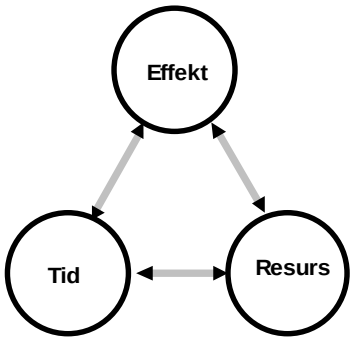
- När är nätverksbaserad väpnad strid möjlig?
- Vad är gränssättande?
- Vilka mervärden tillför nätverksbaserad krigföring framför traditionell plattformsbaserad?

De metoder som vi diskuterat och som beskrivs i denna rapport syftar till att besvara dessa tre frågor för fem olika typfall. Typfallen beskrivs översiktligt i bilaga ett och mer i detalj i förstudierapportn [Alsér 2002]. För att värdera typfallen föreslås att vi nyttjar vad vi kallat systemeffekter. Dessa systemeffekter kan definieras som mått på ”nätverkssystemets” respektive ”plattformssystemets” förmåga att lösa en väldefinierad uppgift. Med system menas här den sensor-beslutsfattare-vapen kedja som nyttjas i respektive typfall. För de fem typfallen föreslås uppgifter enligt tabell 1. Varje systemeffekt kan beskrivas med flera olika parametrar. De parametrar som inledningsvis har diskuterats är:

- ***Effekt*** - Med hur stor sannolikhet uppgiften löses.
- ***Tid*** - Hur snart efter upptäckt kan ett mål bekämpas eller hur lång tid har man på sig efter upptäckt att bekämpa ett mål, respektive vilka tidskonstanter är acceptabla.
- ***Resurs*** - De resurser som krävs i form av sensorer, vapen och plattformar i nätverks- respektive plattformscentrerade fallen.

Tabell 1. Förslag till definition av effekt och tänkbara parametrar för de olika typfallen. Värderingen antas ske i två steg. I första steget bedöms hur parametrarna varierar med val av tekniska system, organisation och struktur. I andra steget bedöms hur effekten varierar med förändringar i parametervärden.

Typfall	Effekt	Förslag på mått/parametrar
Fast mål	Kanon utslagen med sannolikhet P_k.	Tid från upptäckt till vapeninsats Antal avfyrade vapen
Stridsvagn	Stridsvagn utslagen med sannolikhet P_k.	Tid från upptäckt till vapeninsats Antal sensorer eller sensorbärare Kvalitet på lägesbild Tidskrav på måldataöverföring Antal avfyrade vapen
Stridsflyg	Sannolikhet $P_ö$ för att skyddat mål överlever flygattack med mindre än X% skador	Tid från upptäckt till vapeninsats Antal sensorer/sensorbärare Tidskrav på måldataöverföring Antal avfyrade vapen
Ytstridsfartyg	Sannolikhet P_{TU} för att främmande fregatt blir taktiskt utslagen.	Tid från insatsbeslut till avfyrning Kvalitet på lägesbild Tidskrav på måldataöverföring
Undervattensmål	Ubåt bekämpad med sannolikhet P_k	Tid från insatsbeslut till avfyrning Kvalitet på lägesbild



Figur 7. Tid-effekt-resurs. De tre parametrarna påverkar varandra varför jämförelser mellan nätverks-centrerat och plattformscentrede fallen bör göras så att en parameter hålls konstant, t ex effekt. Jämförelsen kan sedan ske genom att se hur stora resurser som krävs för att nå den önskade effekten.

Värderingsarbetet blir nu en fråga om att ta fram värden eller uttryck för de förslagna/valda effektmåtten i respektive typfall. Detta skall göras både för det nätverkscentrerade och det plattformscentrerade fallet. Eftersom de tre parametrarna effekt, resurs och tid sannolikt påverkar varandra bör jämförelsen ske genom att man låser en eller två parametrar och studerar hur den tredje varierar.

Fråga 1: När är nätverksbaserad väpnad strid möjlig?

Svaret på frågan är att nätverksbaserad strid är möjlig när nätverket erbjuder en tillräcklig systemeffekt inom tidsramar som är acceptabla och med en acceptabel nivå på resurserna. För vart och ett av typfallen måste det göras en bedömning av vad som kan anses vara en acceptabel systemeffekt och utifrån det får avgöras om priset för en nätverksorienterad lösning är värt att betala. Det kan komma att visa sig att det finns tekniska begränsningar, t ex att det inte är tekniskt möjligt att uppnå de nödvändiga tidskonstanterna i kommunikationssystemen[1] för att nätverksbaserad strid skall vara möjlig. De två typiska situationerna där detta kan uppstå är då situationen förändrar sig mycket snabbt, till exempel vid bekämpning av snabba luftmål (Mach 3-robotar) eller då informationsöverföringshastigheten i kommunikationslänken är mycket låg, t ex vid hydroakustisk undervattenskommunikation.

Förutom begränsningar i tekniska system bör man vara uppmärksam på skillnader i den operativa miljön som påverkar möjligheten till nätverksbaserad strid, till exempel huruvida det finns ett basnät för kommunikation med hög kapacitet eller ej.

Fråga 2: Vad är gränssättande?

Utifrån svaret på fråga 1 om när väpnad strid i nätverk är möjlig bör en känslighetsanalys genomföras i syfte att ta reda på hur tid, resurs och effekt varierar med förändringar i indata, t ex teknisk förmåga hos ingående system, målets signatur och väderleksförhållanden. Denna känslighetsanalys skall ge svar på frågan om vad som är gränssättande.

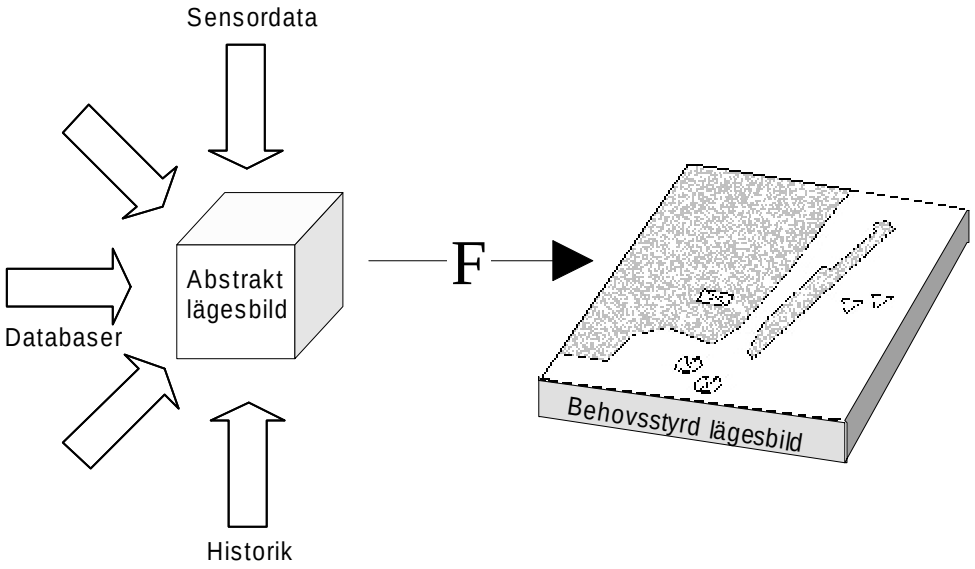
Fråga 3: Vilka mervärden tillför nätverksbaserad krigföring framför traditionell plattformsbaserad?

Svaret på fråga 3 kommer ur jämförelsen mellan det nätverkscentrerade och det plattformscentrerade fallet. Givet samma systemeffekt kan en jämförelse göras mellan fallen avseende vilka tider som står till förfogande för att lösa uppgiften respektive vilka resurser som krävs. Precis som för fråga 1 ovan bör man vara uppmärksam på andra värden än de rent tekniska, till exempel rörlighet.

3.6 Lägesbilden

3.6.1 Abstrakt och behovsstyrd lägesbild

Den lägesbild som är utgångspunkten för de modeller som presenterats i avsnitt 3.2-3.4 ovan skall ses som en abstrakt lägesbild som består av samtliga data som finns tillgängliga i systemet, dvs det urval som gjorts i de yttersta noderna, i kombination med de databehandlingsalgoritmer som finns implementerade. För olika behov görs olika projektioner av data från den abstrakta lägesbilden till olika behovsstyrda, eller rollbaserade, lägesbilder. Dessa behovsstyrda lägesbilder har olika egenskaper. Den behovsstyrda lägesbild som behövs centralt för att visa var samtliga svenska förband befinner sig har sannolikt lägre detaljnoggrannhet än en bild hos en skjutande enhet som med stor noggrannhet behöver veta vad som finns inom dess närmsta omgivning.



Figur 8. Abstrakt och behovsstyrd lägesbild. Den abstrakta lägesbilden utgör summan av tillgänglig lägesinformation. Den behovsstyrda lägesbilden är en av många tänkbara presentationer av den abstrakta bilden. Den information som finns i den abstrakta bilden omformas av en funktion F till en presentation.I ingår sådant som datafusion, filtrering av data och jämförelser med historiska data i databaser.

De sensorer som levererar data till den abstrakta lägesbilden är organiserade i ett sensornätverk. Det ställs dubbla krav på sensornätverket. Dels måste nätet snabbt kunna ge övergripande information om händelser, t ex enheters rörelser, över en stor yta, dels måste det kunna ge detaljerade data (t ex position, typ, individ, eller beteende) om ett begränsat område eller ett specifikt mål. Nätverket kommer därför att bestå av två fundamentalt olika typer av sensorer. Den första typen är ”permanenta” sensorer[2] som används för att bygga normallägesbilden och som har sådana egenskaper att de kan används som indikation på att något är på gång. Den andra typen av sensorer är sådana som associeras till reaktiv spaning, dvs sensorer som styrs mot ett visst mål i syfte att få mer detaljerad information om just detta mål.

Det faktum att vi har två typer av sensorer där nyttjandet av den ena sensortypen är en reaktion på händelser som observerats från den andra sensortypen innebär att det krävs någon form av sensorledning. Sensorledningens uppgift blir att fördela sensorresurser till det område eller den funktion som för närvarande bäst behöver dem. Följaktligen krävs också någon form av värdering av sensorledningen.

Utöver sensorer innehåller nätverket också databaser över till exempel sjöfarts- och flygrörelser samt historik över vad som skett tidigare. Med denna information skall det gå att identifiera ett klassificerat mål och jämföra det med historiska data för att kunna se t ex avbrott mot normala

mönster[3]. För att överföra informationen i den abstrakta lägesbilden till den behovsstyrda lägesbilden definieras en funktion F som en operator (egentligen ett flertal operatorer) som omformar data i den abstrakta lägesbilden till det som presenteras i den behovsstyrda lägesbilden (figur 4). Operatorerna kan bestå av t ex datafusion, modellbaserade räckvidds-bestämningar eller jämförelser mellan aktuellt målspår och historiskt registrerade målspår. Några exempel på hur olika funktioner F kan användas ges i tabell 2 nedan. Av vidare intresse i detta arbete är i huvudsak funktionerna Normalbild och Lägen för misstänkta mål.

Tabell 2. Exempel på överföringsfunktioner från den abstrakta lägesbilden till en presentation.

Funktion (F)	Parametrar	Presentation
Sensortäckning	Måltyp, sensorer och sensorernas positioner (X,Y,Z)	Visar vilka områden som täcks av en eller flera sensorer under aktuella förhållanden och mot angiven måltyp.
Prognos	Målnummer, tids-period	Prognos på hur ett visst mål förväntas uppträda baserat på hur andra mål av samma typ tidigare uppträtt.
Lägen för fientliga mål	Målnummer, måltyper etc	Visar information om angivna mål som om de vore föremål för vapeninsats. I presentationen igår kvalitetsindikation på lägesdata och osäkerhetsområden.
Normalbild	Målspårslängd	Visar nuläget i ett område med alla kända enheter i området inklusive målspår så långt tillbaka i tiden som önskas.

3.6.2 Värdering av lägesbilden

Behovet av lägesbildsvärdering

Som påtalats ovan så förväntas en av skillnaderna mellan plattformsbaserad och nätverksbaserad krigföring vara att såväl kraven, avseende t ex noggrannhet i position, som kvaliteten på den gemensamma lägesbilden är högre i det nätverksbaserade fallet (detta är själva grundstenen i DBA-tanken). Om data i den gemensamma (abstrakta) lägesbilden skall kunna användas för invisning av vapen kommer vissa grundkrav att ställas på denna lägesbild avseende noggrannhet i målposition och uppdateringshastighet.

Effektmått för indikation

Det finns givetvis många sätt att göra ett uttalade om en lägesbilds värde. Två skilda angreppssätt är att se till hur bilden är uppbyggd dvs vilka egenskaper som de system som levererat indata har, kontra att se vilka egenskaper bilden i sig har, oavsett hur den uppkommit.

Det första vi nyttjar lägesbilden till är att få en indikation på att ”något är på gång” (se till exempel 3.3 ovan, moment [1] i fig 5). Detta sker sannolikt genom att en varnarfunktion (eller en mänsklig operatör) noterar att något i lägesbilden skiljer sig från normalbilden. Ett kvalitets- eller effektmått (Measure of Effectiveness, MOE) på varnarfunktionen kan vara:

$$MOE = Q_{NLB} * P_{Upptäckt} * P_{varning} \quad (3.1)$$

Där MOE enbart är ett värde på hur ”bra” systemet är på att upptäcka uppdykande mål. Q_{NLB} är kvaliteten på normallägesbilden, dvs ett mått på hur ”bra” den bild som byggs upp av upptäckta mål är, och $P_{Upptäckt}$ är sannolikheten för att sensorerna upptäcker ett mål som verkligen finns och $P_{varning}$ är sannolikheten för att varnaren/operatören varnar för ett upptäckt mål. Bakgrunden till att ha både kvalitet, Q och sannolikhet, P i uttrycket är att P är en teoretisk faktor som beskriver funktionerna ”Upptäckt” respektive ”Varnare” medan Q är en kvalitetsfaktor som beskriver den datamängd som funktionen ”Varnare” opererar på. En bra varnarfunktion med usla indata är inget värd, liksom en bra bild utan varnare inte heller är till nytta.

För kvalitetsfaktorn Q_{NLB} kan till exempel ett uttryck som nyttjar den tid det tar för att skapa lägesbilden och osäkerheten i målets position nyttjas

$$Q_{NLB} = P_{ID} * \frac{A_{Mål}}{O_{Mål} * N_{Mål}} \tag{3.2}$$

P_{ID} anger sannolikheten för att målet klassificerats eller identifierats korrekt, $A_{Mål}$ är målets ”Area” (radarmålarean eller dess fysiska storlek), $O_{Mål}$ är osäkerhetsområdet, dvs det området kring den angivna positionen inom vilket målet finns och $N_{Mål}$ är antal mål i lägesbilden. Denna formulering av kvalitetsfaktorn innebär att stora mål som vi känner läget på med god precision ger en hög kvalitet på lägesbilden. Ju mindre målet blir desto högre måste precisionen i lägesdata vara för att ge samma kvalitetsfaktor. Det innebär också att ju fler mål vi har desto lägre blir kvaliteten på lägesbilden. Detta kan tolkas som att vi för en större del av det område vi bevakar inte vet huruvida det finns ett mål där eller ej, alltså är vår kunskap om läget lägre om $N_{mål}$ ökar, alltså gå $N_{mål}$ in i nämnaren på uttryck 3.2. Uttrycket 3.2 antar implicit att alla mål i området är likadana, vilket givetvis är en förenkling.

Det skall dock betonas att ekvation 3.2 är *ett* sätt att skapa ett mått på lägesbilden, definitivt inte det enda sättet och sannolikt inte heller det bästa sättet. Dock bör det fylla sin funktion, nämligen att möjliggöra en jämförelse mellan i första hand nätverksalternativet och plattformsalternativet.

Osäkerhetsområdet kan ses som det område som ett mål ”måste” befinna sig inom mot bakgrund av den senast kända positionen. Den enklaste tänkbara approximationen av det området är att anta att det är en cirkel runt den senast kända positionen. Cirkelns radie blir då en funktion av hur gammal informationen är och hur snabbt målet rör sig samt precisionen hos sensorerna.

$$O_{Mål} = p * (v_{Mål} * \Delta t)^2 \tag{3.3}$$

Med $v_{Mål}$ som målets hastighet och Δt som den maximala åldern på den information som presenteras i systemet. För att göra formeln hanterbar kan Δt approximeras med

$$\Delta t = \frac{1}{f} + T_{Process} \tag{3.4}$$

Där f är den frekvens med vilken lägesinformationen uppdateras och den äldsta tänkbara informationen är (nästan) en period gammal. $T_{Process}$ är en tidskonstant som beskriver processeringstiden för informationen i systemet. $T_{Process}$ är i sin tur en summa av den tid det tar att bearbeta data och den tid det tar att kommunicera informationen genom nätverket.

Totalt sett fås nu ett uttryck för ett effektmått på lägesbilden enligt

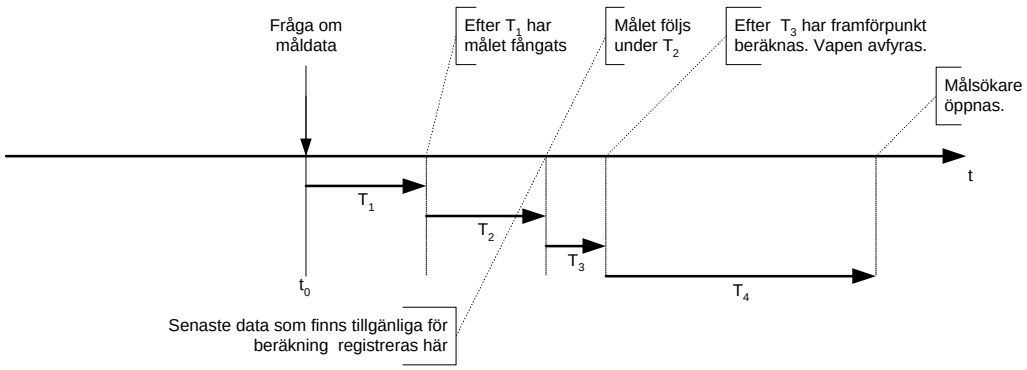
$$MOE = \frac{P_{ID} * P_{Upptäckt} * P_{varning}}{p\left(v_{Mål} * \left(\frac{1}{f} + T_{Process}\right)\right)^2} * \frac{A_{Mål}}{N_{Mål}} \tag{3.5}$$

Detta uttryck skall ses som ett förslag till effektmått på lägesbilden. För de enklaste tillämpningarna är det antagligen inte meningsfullt att ha med antalet mål (faktorn $N_{Mål}$) som inte skiljer plattformsbaserade från nätverksbaserad strid åt.

Nästa nytta vi har av lägesbilden är att den levererar måldata till operatören (se till exempel avsnitt 3.4, moment [5] i fig 6). Kraven på måldata kan inte anses vara säkert fastställda av arbetsgruppen, men en hypotes är att måldatat måste hålla en sådan kvalitet att osäkerhetsområdet för målet är mindre än det område som täcks av vapnets målsökare (om det är ett målsökande vapen). Vi får fyra olika fall svarande mot kombinationerna av vapennära sensor, respektive måldata ur nätverket och vapen med uppdatering av målläge under gång respektive ”fire-and-forget”, dvs vapen utan uppdatering av målläge under gång.

Vapennära sensor

För värdering av nyttjandet av en vapennära sensor, t ex en radar eller ett IR-riktmedel har arbetsgruppen tagit fram en modell för förloppet enligt fig 9 nedan. Från beslut om avfyrning till det att vapnet öppnar målsökaren genomgår en processen fyra steg: Låsa på målet (1) vilket tar tiden T_1, följa målet under en viss tid T_2 (2), beräkna en framförpunkt (3) vilket tar tiden T_3 och slutligen vapnets gångtid till målet T_4 (4).



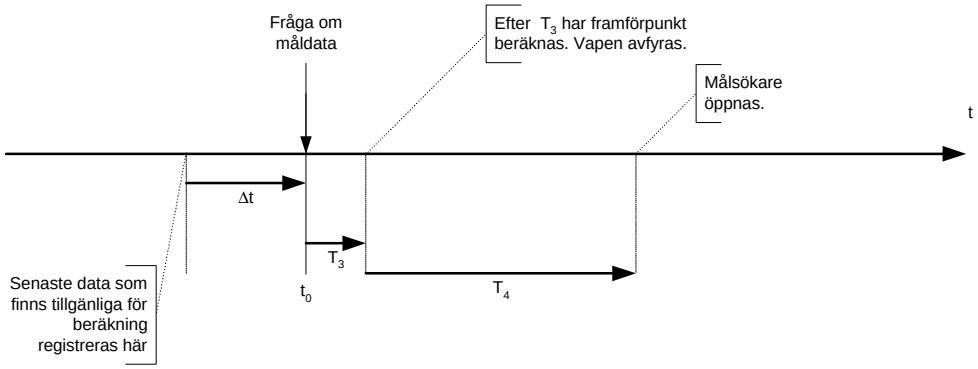
Figur 9. Tidslinjal för vapeninsats med måldata från vapennära sensor.

Det osäkerhetsområdet man måste hantera är beroende av hur gammalt det senaste målläget är. Med resonemanget om de fyra stegen kommer det färskaste måldatat att vara det som kommer ur steg (2), varför det är tiderna T_3+ T_4 som avgör osäkerhetsområdets storlek. Genom att ersätta Δt i ekvation 3.3 med T_3+ T_4+ τ fås ett osäkerhetsområde enligt 3.5 nedan. Att Δt enligt 3.4 inte kommer in i ekvation 3.5 beror på att $T_{process}$ avser tiden som nätverket behöver för att hantera data, en tid som inte är relevant då man nyttjar en vapennära sensor. För att kunna hantera tidsfördröjningar i det vapennära sensorsystemet läggs en tidskonstant τ in som en markering av att även detta system behöver en viss tid för att behandla inkommande data och presentera resultatet.

$$O_{Mål} = p * \left(v_{Mål} * \left(T_3 + T_4 + t\right)\right)^2 \qquad (3.5)$$

Måldata ur nätverket

Om man hämtar sina måldata ur nätverket kommer förloppet från beslut om avfyrning till det att vapnet öppnar målsökaren att se något annorlunda ut än ovan (fig. 10). Momenten (1) och (2), dvs fånga och följa målet kommer inte längre att behövas, samtidigt som de data man använder sig av istället kommer att vara äldre med en faktor Δt enligt ekvation 3.3 ovan.



Figur 10. Tidslinjal för vapeninsats med måldata från nätverket.

Ett uttryck för osäkerhetsområdet blir då

$$O_{Mål} = p * \left(v_{Mål} * \left(\Delta t + T_3 + T_4\right)\right)^2 \tag{3.6}$$

Osäkerhetsområdet enligt ekvation 3.6 ovan kommer nu att bli beroende av såväl Δt enligt ekvation 3.3 som $T_3 + T_4$ enligt ekvation 3.5. Detta kan förvisso tyckas vara en försämring jämfört med 3.5 men man måste hålla i tankarna att nätverket möjliggör betydligt tidigare upptäckt och avfyrning än vad enbart en vapennära sensor gör. Mot t ex sjömålsrobotar som kommer in mot ett fartyg innebär en tidigare upptäckt möjlighet att bekämpa fler robotar, och därmed större chans att överleva anfallet. Det kritiska är inte hur stort osäkerhetsområdet $O_{Mål}$ är utan huruvida det täcks av vapnets målsökare eller ej.

Vapen med uppdatering av målläge under gång

Om vapnet är styrt, dvs det finns en möjlighet att uppdatera målläget efter det att vapnet avfyras kommer tidslinjalen att se ytterligare annorlunda ut. De data man tillför vapnet kommer att ha en viss ålder då de når fram. I fallet med en vapennära sensor har de åldern $T_3 + T_{Kom}$, motsvarande att målet följts och en framförpunkt beräknats, T_3, samt den tid det tar för informationen att nå vapnet, T_{Kom}.

I de fall då måldata hämtas ur nätverket kommer de att ha ”åldern” $\Delta t + T_3 + T_{Kom}$, dvs Δt som är den ”allmänna” åldern för det bästa tillgängliga måldatat i nätverket, T_3 är tiden för att beräkna framförpunkten och T_{Kom} för den tid det tar att få fram dem till vapnet.

För vapen som styrs via optofiber eller direkt via radio-/radarlänk är sannolikt T_{Kom} försumbar. För vapen som styrs med hydroakustiska signaler eller signaler som går långa sträckor, till exempel om de studsar på en satellit, måste T_{Kom} sannolikt tas med i beräkningarna.

Slutligen är osäkerhetsområdet beroende av hur ofta vapnet uppdateras med ett nytt målläge. Ett antagande är att vid den tidpunkt då målsökaren öppnas så har det i snitt gått en halv period sedan senaste uppdateringen, dvs om uppdateringsfrekvensen är f_{Uppdat} så är

$$T_{Uppdat} = \frac{1}{2 f_{Uppdat}} \tag{3.7}$$

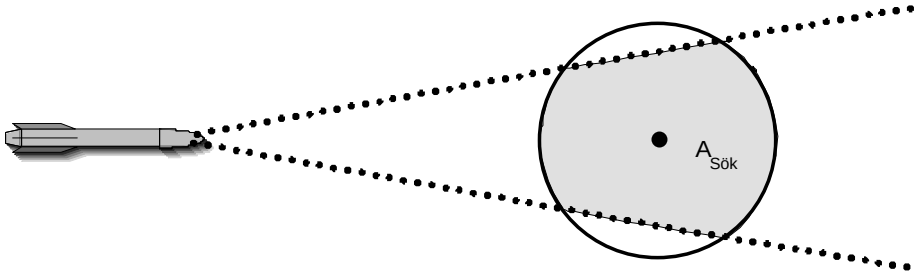
Osäkerhetsområdet blir nu för vapennära sensor (ekvation 3.8) respektive för måldata ur nätverket (ekvation 3.9)

$$O_{Mål} = p * \left(v_{Mål} * \left(T_3 + T_{Kom} + \frac{1}{2 f_{Uppdat}} \right) \right)^2 \tag{3.8}$$

$$O_{Mål} = p * \left(v_{Mål} * \left(\Delta t + T_3 + T_{Kom} + \frac{1}{2 f_{Uppdat}} \right) \right)^2 \quad (3.9)$$

Sannolikhet för att se målet

Ovanstående beräkningar av osäkerhetsområdena syftar till att ta fram ett uttryck för sannolikheten att ett vapen ”ser” målet i sin målsökare då den öppnas. Detta är i sin tur en av de egenskaper som arbetsgruppen förväntar vara gränssättande när det gäller om väpnad strid i nätverk är möjligt eller ej.



Figur 11. Osäkerhetsområdet och målsökarens synfält.

Ett tänkbart effektmått för plattformen respektive nätverkets förmåga att generera måldata av tillräcklig kvalitet är andelen av osäkerhetsområdet som ses av målsökaren. Låt detta område betecknas $A_{Sök}$ (fig. 11). Sannolikheten för att målet syns i målsökaren kan nu approximeras med

$$P_{Se-mål} = \frac{A_{Sök}}{O_{Mål}} \quad (3.10)$$

Där $O_{mål}$, beroende på situationen, är något av uttrycken 3.5, 3.6, 3.8 eller 3.9. Storleken på $A_{Sök}$ blir en funktion av målsökarens öppningsvinkel och avståndet från det att målsökaren öppnar till den förväntade målpunkten.

3.7 Ledningsfunktionen

Det som betecknats ledningsfunktion i figurerna 4-6 kan definitionsmässigt bestå av olika antal nivåer och funktioner. För närvarande finns det i arbetsgruppen ingen konkret kunskap om hur ledningsfunktionen i ett framtida nätverksbaserat försvar kommer att se ut. Amerikanska erfarenheter från Fleet Battle Experiment (FBE) Alpha och Bravo[4] visar på möjligheter (och möjliga vinster) i att nyttja informationsteknologi i förändrade ledningsstrukturer, t ex genom att sprida ordrar via e-post eller nyttja videokonferenser för genomgångar.

Det måste anses ligga utanför uppdraget för den här arbetsgruppen att ta fram olika förslag till ledningsstrukturer. För det vidare värderingsarbetet föreslås därför att ledningsfunktionens påverkan på systemet antas vara en tidsfördröjning från det att information kommer in tills det att ett beslut går ut. Storleken på denna tidsfördröjning bedöms för varje enskilt fall. Särskild hänsyn skall härvid tas till sensorledningen.

3.8 Egenskaper hos operatör och vapensystem

Det finns givetvis en uppsjö av tänkbara konfigurationer av vapensystem och tillhörande operatörer. Ur ett nätverksperspektiv kan man förslagsvis sortera in dem i två olika huvudalternativ:

- vapnet hanteras av en operatör på plats
- vapnet hanteras via nätverket

I båda alternativen antas det kunna existera vapen med och utan vapennära sensor.

Vapen med operatör

Detta är ett "traditionellt" system, t ex en sjömålsrobot eller en kanon med operatörskonsol som kontrolleras från den plattform där den sitter. Sannolikt står operatören under befäl av fartygschef, batterichef eller motsvarande. Den tid det tar från beslut om vapeninsats till dess att vapnet avfyras måste beräknas med hänsyn till att det kan finnas en eller flera ledningsnivåer mellan beslutsfattaren, t ex taktiskt kommando, och vapenoperatören.

Kontroll via nätet

Kontroll via nätet är tänkbart för avancerade system som kan tillåtas vara "semiautonoma", dvs system som kan tillåtas aktiveras och avfyras utan kontroll på plats. Ett exempel på ett sådant system är lv-system i containrar på handelsfartyg i konvoj som ingår i ett nätverk som skyddar konvojen.

Ur värderingsperspektiv måste vi förutom att värdera förmågan att fånga och träffa målet också ta hänsyn till nätverkets förmåga att kontrollera vapnet och få fram data tillräckligt snabbt. Vidare bör en rigorös värdering av ett system där vapnen kontrolleras vi nätverket ta hänsyn till nätverkets sårbarhet, möjlig motverkan mot nätet samt konkurrens om nätverksresurserna mellan olika tjänster, t ex förmedling av måldata avseende kända mål kontra övervakningsdata för att söka efter eventuella nya mål.

---

[1] Det kan t ex vara en situation där det krävs att data med en tidsmärkning som är noggrannare än en hundradelssekund måste förmedlas i systemet så att det når ”slutanvändaren” inom en sekund från att sensordatat skapades. Om slutanvändaren, t ex ett vapensystem, ställer sådana krav på data som nätverket inte kan leva upp till så blir nätverksstriden inte möjlig.

[2] Uttrycket permanent används som sammanfattning på fasta system, t ex radarstationer på marken och rörliga system som flygande spaningsradar som används för övervakning. Skälet till att inte direkt kalla dem ”övervakningssensorer” är att de mycket väl kan användas även till att ta fram mållägen. Beteckningen bör därför inte associeras till deras användning utan till deras tillgänglighet.

[3] Detta skall ses som exempel på vad som kan tillföras nätverket och tillämpningen, avbrott från normalbeteende, kan ses som en av många tänkbara tillämpningar. Eftersom syftet med denna text är att lägga grunden för värderingsarbetet och inte att utveckla nätverkets funktionalitet vidareutvecklas inte dessa tankar här.

[4] Dessa redovisas summariskt i t ex "What is Network Based Anti-Submarine Warfare", Raymond J. Christian, Naval Underwater Warfare Center.

4 FUNKTIONSSCHEMAN

Begreppet funktionsschema som metod för att värdera ett typfall är hämtat ur Luftvärnsutredningen, LVU-99[1]. Schemat skall ses som en mall eller ett mönster för att beskriva ett typfall på ett sådant sätt att de parametrar som tas fram enligt förslag i avsnittet tre (eller på annat sätt) kan sättas in i ett sammanhang. Att använda en gemensam mall fyller två viktiga syften, att göra värderingsmetoden för de olika typfallen så lika som möjligt samt att minimera risken för att viktiga pararmetrar missas och att det på det sättet finns brutna länkar i händelsekedjan, och därmed i värderingskedjan.

Schemat bygger på att det i horisontalled placeras olika aktörer eller funktioner. I schemat för bekämpning av fast mål med nätverksorienterade system (fig. 12) är aktörer/funktioner i tur och ordning externa spaningssensorer, lägesbild, bearbetning, beslut, insatsplanering, vapennära sensor, avfyrning, målsökare och verkansdel. Första halvan av denna process är densamma som processen för bearbetning av information som presenteras i avsnitt 5, Översikt över andra angreppssätt. Interaktion mellan olika aktörer/funktioner beskrivs som horisontella pilar (egentligen skall pilarna ha en vertikalkomponent, se nedan). Pilarna beskriver hur initiativet i processen övergår från en aktör/funktion till en annan. Data från externa sensorer går från funktionen extern sensor till funktionen lägesbild, informationen i lägesbilden går till en beslutsfattare som fattar ett beslut. Beslutet omvandlas till en vapeninsats som i slutskedet lämnar till målsökaren att upptäcka målet. För varje sådant överlämnande kan man ställa krav på vad systemet skall klara för att kunna lösa sin uppgift. I de flesta fall kan dessa krav omvandlas till mätbara storheter, t ex bandbredd för att överföra tillräcklig information eller öppningsvinkel på målsökaren för att den skall täcka ett tillräckligt stort område.

I vertikalledd i schemat finns tidsparametern. En händelse/pil som ligger ovanför en annan i schemat inträffar tidigare. Detta innebär en (implicit) vertikalkomponent för varje pil som motsvarar den tid händelsen tar. Vidare motsvarar väntetider i systemet sträckor i vertikalledd där ingenting händer. Genom att i schemat lägga in när en uppgift måste vara löst och sedan se om de händelser som måste ske för att uppgiften skall kunna lösas fås en visuell bild av när det är ett visst system av system fungerar respektive inte fungerar. Denna metod har vissa likheter med den beräkningsmetod som nyttjades i Marinledningens luftförsvarsstudie 1997[2]. De två olika tidsmått som omnämns i avsnitt 3.5 Systemeffekter, nödvändig tid respektive acceptabla tidskonstanter, kan nu visualiseras genom funktionsschemat där den tid systemet behöver för att bekämpa ett mål är funktionsschemats ”höjd” dvs hur lång tid som förflyter från den första pilens startpunkt till den sista pilens slutpunkt. Tidskonstanterna är de enskilda pilarnas vertikalkomponenter.

I bilaga 2 presenteras de funktionsscheman som togs fram för de fem olika typfallen för alternativet nätverksorienterat system respektive traditionellt plattformsbaserat. För varje typfall och alternativ presenteras dels funktionsschemat, dels en schematisk skiss av typfallet.

Metoden som användes för att ta fram dessa scheman var att utgående från de i text beskrivna typfallen rita typfallets insatskedja som ett flödesschema. Det stod tidigt klart att dessa insatskedjor representerade tre olika typer av insatser vilka betecknades Plattform, Nätverk av befintliga system och Nätverk av avancerade system, såsom beskrivs i avsnitt 3 ovan. I dessa flödesscheman motsvarar varje pil mellan två funktioner en händelse, dock saknas händelser inne i respektive funktion och dessutom saknas tidsaspekten.

Flödesschemat och funktionsschemat är två komplementära bilder av samma process. Skälet till att använda bägge två är att flödesschemat poängterar nätverksstrukturen medan funktionsschemat kan ligga till grund för ett värderingsarbete eftersom tidsaspekten finns med.

---

[1] Dokumentation av detta arbetet finns hos FMV.

[2] Höstbeck, Metoder för effektberäkningar av marint luftförsvar, FOA-R– 99-01003-201– SE, 1999.

5 ÖVERSIKT ÖVER ANDRA ANGREPPSSÄTT

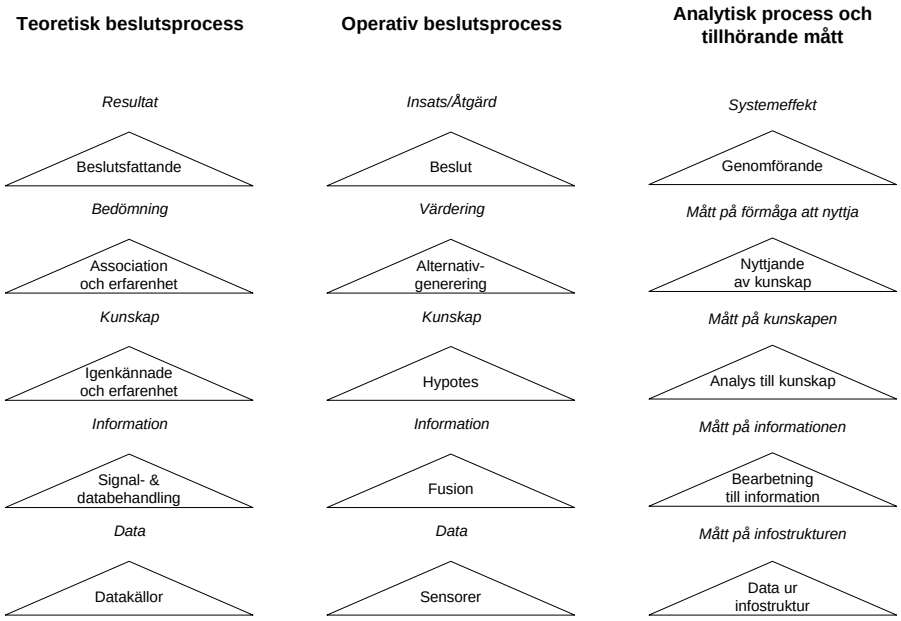
Det är i mångt och mycket den snabba utvecklingen av informationsteknologin (IT) och densammas påverkan på krigföringen som myntat begreppet ”Revolution in Military Affairs”. För att kunna göra övergripande värderingar av hur ”bra” ett IT-intensivt förvar är jämfört med ett traditionellt försvar är det kritiskt att kunna värdera vad informationskomponenten tillför försvarsförmågan. Detta är givetvis något som sysselsätter försvarsforskningsorganisationer världen över.

I detta avsnitt ges en kort introduktions till hur man kan se på information och hur den kan komma ledning och strid tillgodo. Därefter ges kortfattade exempel från olika håll på hur ett nätverksorienterat försvar skulle kunna värderas.

5.1 Vad är information?

Om hur information definieras finns åtskilligt skrivet, liksom hur den kan nyttjas. Detta avsnitt syftar enbart till att ge en kort introduktion till hur man kan se på informationskomponenten i det nätverksbaserade försvaret i syfte att värdera informationens effekter.

All information kommer någonstans ifrån. Det handlar ofta om sensorer som fångar upp vad som händer på stridsfältet. I framtiden handlar det också i större utsträckning än idag om att ta in information från databaser som innehåller registreringar av tidigare händelser, kända miljöparametrar som t ex bottentopografi eller operativa data såsom manifest för civila fartyg eller registrerade rutter för trafikflygplan.



Figur 12. Förslag till hur beskrivning av processen för omvandling av data till systemeffekt ur ett teoretisk, operativ och analytiskt perspektiv.

Från datakälla, sensor eller databas, till systemeffekt genomgår informationen en process där den bearbetas och förädlas på olika sätt. Figur 12 vänster illustrerar denna process. Detta är på intet sätt något nytt. Det som är nytt är att informationsteknologin utvecklats till att kunna stödja denna process i flera av dess steg, att IT har förmåga att bearbeta större data/informations-

mängder än tidigare och att bearbetningen sker snabbare än vad den gjorde i ett mindre IT-intensivt försvar. Ju mer datortekniken utvecklas desto större datamängd kan man förvänta sig att processen kan hantera och med det förväntas kvalitet på beslut, och därmed resultat av en insats eller en åtgärd, bli bättre. Figur 12 mitten illustrera denna operativa process som genomgås för ett insatsbeslut.

Värdet av denna informationskomponent kan antas öka om försvaret är organiserat i ett nätverk så att större mängder och fler olika typer av information finns tillgängligt inför ett beslut. Att värdera ett IT-intensivt försvar, även på ”sensor-to-shooter”-nivå såsom är syftet med detta arbete blir då inte bara en fråga om att jämföra två olika tekniska system, ett traditionellt med begränsad kunskap tillgänglig och ett modernt med ”bättre” kunskap tillgänglig. Värderingen måste ta hänsyn till hela processen och värdera nyttan av mer och bättre kunskaper och större bearbetningsförmåga hela vägen från datakällan till beslutet, figur 12 höger.

I den mycket begränsade internationella litteraturen som funnits tillgänglig kan man se två olika sätt att närma sig problemet med att värdera informationskomponentens ökade betydelse i processen. Det första är att på den tekniska nivån, värdering av informationsinfrastrukturen, eller infostrukturen, ta hänsyn till prestanda hos de tekniska systemen och därefter på successivt högre nivåer ta hänsyn till informationskomponenten i parametrar som sensorräckvidd, tid att producera order eller sannolikhet för att beslut fattas på korrekt grund. Detta är i princip den väg som denna arbetsgrupp valt. Denna vägen har den fördelen att den erkänner att kunskap alltid har funnits med i beslutsprocessen och att det IT-intensiva försvar vi står inför egentligen skall ses som en gradskillnad, realiserad av IT, men inte som en sakskillnad gentemot äldre system.

Den andra vägen att ta hänsyn till information är att försöka göra informationen till en storhet i sig som sedan vägs in i de modeller man utvecklar för att värdera sina scenarier. Detta är den vägen som RAND valt i refererat arbete nedan. Det har den fördelen att kunskapen blir tydligt synlig men nackdelen att man tvingas behandla moderna system annorlunda än äldre vilket är olämpligt om man vill jämföra de två.

För att hantera nätverksdelen av problemet, dvs att man inte bara har bättre lokal information utan tillgång till ett helt nät av kunskap kan man i det material som funnits tillgängligt läsa ut ett tänkbart angreppssätt. Varje nod i nätverket har någon av rollerna skapa, omforma, förädla eller förbruka information. Genom att studera vilken information som önskas förbrukas vid en viss tid, om den finns tillgänglig i nätverkets datakällor och om den kan förädlas och förmedlas i rätt tid kan en utsaga om nätverket förmåga göras. Det är i princip detta arbetsgruppen föreslår att man ska göra då vi föreslår funktionsdiagram (se avsnitt 4) för att besvara frågan om när näverksstrid är möjligt. Svaret är att nätverksstrid inte är möjligt då förbrukarens behov av kunskap är större än nätverket förmår att leverera.

Nedan refereras tre olika ansatser till värdering av informationskomponenten i en ”sensor-to-shooter” loop eller en motsvarande situation. Det finns många likheter mellan ansatserna, bland annat nivåresonemanget och tanken att informationskomponenten måste vägas in hela vägen från datakälla till beslut för att man skall kunna bedöma dess inverkan på systemeffekten. Det finns också stora skillnader. Den största är sannolikt medan CCRP och NUWC nöjer sig med att konstatera att informationskomponenten måste vägas in gör RAND ett försök att kvantifiera kunskap och föreslå hur den ska vägas in.

5.2 Bedöma potentialen hos nätverksbaserat försvar, CCRP 1999

Sammanställning av tankar kring värdering av NCW såsom de presenteras i boken “Network Centric Warfare – Deveolping and Leveraging Information Superiority”[1].

Trots att det existerar ett stort antal analysmodeller (och metoder) är det få som är lämpade för att värdera NCW. Många modeller är i grunden utvecklade för övnings- och träningsändamål och

behandlar dagens system och strukturer, ofta hårdkodade på ett sådant sätt att de saknar validitet för det nätverksbaserade fallet.

En orsak till svårigheten att värdera NCW är behovet och möjligheten att låta fler aspekter på uppgiften variera än vad i det traditionella fallet.[2] T ex behöver man inte i ett visst läge begränsa sig till de system som finns på en bestämd plattform. Nyckeln till en relevant analys och värdering är en uppsättning analytiska mått som kan representera systemeffekter på olika nivåer och som kan jämföras för olika alternativa system, eller system av system, som är föreslagna. För detta krävs inte bara mått för värdering av sensorer och vapen utan också mått för att värdera det nätverk och den ledningsfunktion som binder ihop sensor och vapen.

För att kunna värdera sammansättningen sensor-ledning-vapen räcker det inte med mått som beskriver förmågan i ledningssystemet, t ex kommunikationsförmåga mätt i sannolikhet att ett meddelande tas emot på ett korrekt sätt. Ett sätt att hantera detta är att gå från mått på förmåga till mått på förväntan. Frågor att ställa i ett sådant sammanhang kan t ex vara:

1. Vem i nätverket är bäst lämpad att fatta beslut om vapeninsats?
2. Stöder det operativa konceptet, doktrinen, organisationen och utbildningen detta?
3. Hur många beslut/ hur mycket ledning kommer att behövas, inom vilka tidsramar och är detta genomförbart i det valda systemet?
4. Vad är effekten av att inte delegera vissa beslut till olika nivåer?
5. Vilka beslut kan automatiseras och hur kan övriga beslut distribueras?
6. Vilken information är mest viktig för tidskritiska beslut och kan den göras tillgänglig för rätt person i rätt tid?
7. Vad är effekten av att ledning distribueras till olika grupper som kan agera utan samordning?

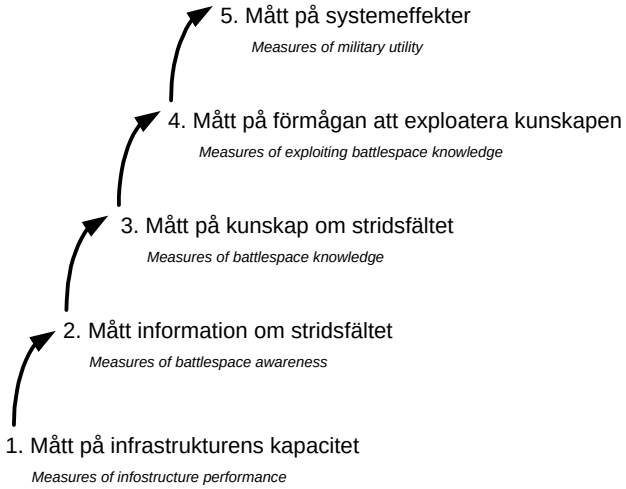
För att finna svaren på ovanstående och andra liknande frågor krävs empiriska data och effektmått som kan styra datainsamling och analys. Detta är ett skäl till att experiment och försöksverksamhet är en viktig del i att bygga det nätverksbaserade försvaret[3].

Att ett koncept leder till en större systemeffekt än ett annat är i allmänhet inte ett tillräckligt mått på ett systems förmåga. Det krävs också förståelse för varför effekten blir större. Det är t ex inte självklart att effekten blir större för att informationsmängden ökar eller att en ökad förmåga att koppla upp sig till omvärlden ger ett mervärde. Om vi jämför två nätverksorienterade system och finner att system A är bättre än system B är det först när vi förstår *varför* A är bättre än B som vi kan bedöma värdet av den nätverksorienterade konstruktionen. Detta är viktigt för att man inte bara skall kunna maximera utfallet utan också göra det kostnads- och resurseffektivt. Detta leder också till kunskap om när nätverksorienterade lösningar fungerar och när de inte fungerar.

Alberts et al föreslår fem olika hierarkiska nivåer av mått (fig 13) där den lägsta nivån, mått på infrastrukturens kapacitet inkluderar sådant som bandbredd och beräkningskraft. Det är inte självklart att en ökning av dessa automatiskt leder till ökad förmåga att lösa uppgiften.

I andra änden av skalan finns måtten som är relaterade till systemeffekt eller lösandet av uppgiften. Det kan vara sådant som tid för att lösa en uppgift, överlevnadssannolikhet eller förluster. Över dessa fem nivåer av mått skulle en sjätte kunna läggas, ”policy achievement”, dvs förmåga att uppnå de politiska mål som ställts upp för en viss operation eller uppgift.

Med de fem grundläggande nivåerna av mått kan det vara möjligt att analysera ett nätverksorienterat system för att bedöma vilken effekt nätverkslösningen har på de olika nivåerna, och därmed vilka tillskott eller delsystem som är de kritiska för att nå den högre systemeffekten.



Figur 13. Hierarki av analytiska mått enligt Alberts et al 1999.

5.3 Effektmått för nätverksbaserad ubåtsjakt, NUWC 1999, 2001

Sammanställning av tankar och idéer kring värdering av nätverksbaserad ubåtsjakt, publicerade i "Measuring Coordinated Battlespace Management – Network Centric Measures of Performance and Measures of Effectiveness"[4] och presenterade i "Concepts in Network-Centric ASW", SMi:s 4th annual conference on Submarines and ASW, 2001.

Ubåtsjakt är en typ av operation där unika förmågor hos olika plattformar samverkar för att uppnå ett gemensamt mål. Ubåtsjakt är därmed ett naturligt objekt för att studera hur nätverksorienterade lösningar skall byggas och för att utveckla analytiska mått associerade till nätverksorienterade system. Det existerar väldefinierade mått för att bedöma nätverkets förmåga att förmedla information. Dock innebär inte förbättrad kommunikation nödvändigtvis bättre förståelse eller bättre beslut.

För att bedöma effekterna av nätverksorientering av ubåtsjakt krävs också kvantitativa mått för sådant som samarbete och beslutsfattande. Effekterna av nätverket på kvalitet och kvantitet av information, ledning och beslutsfattande måste också bedömas. Följaktligen behövs nätverksorienterade effektmått i syfte att:

- Definiera och förstå systemeffekt i nätverksorienterade lösningar
- Utveckla operativa koncept, riktlinjer och taktik för det nätverksbaserade försvaret
- Utveckling av relevanta analysverktyg, inklusive modeller
- Genomföra kostnads - effektanalys vid systemanskaffning

Nätverksorienterad ubåtsjakt karaktäriseras av ett system av sensorer, beslutsfattare och vapen som gemensamt skall upptäcka, klassificera, lokalisera och bekämpa fientliga ubåtar. Ubåtsjakt utövas bäst i samverkan mellan olika typer av resurser[5].

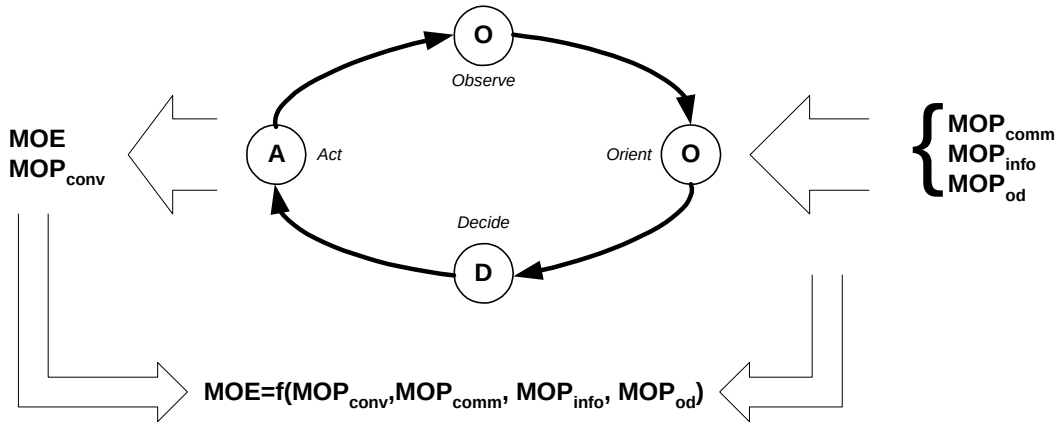
Den framtida ubåtsjaktmiljön förväntas bli kustnära med omväxlande miljöer som kräver in-situ mätning av miljöparametrar som sedan görs tillgängliga för hela styrkan i realtid. Den besvärliga

miljön leder till begränsade sensorräckvidder och kortare reaktionstider. Genom ett nätverksorienterat system kan man tänkas uppnå:

- Ökad förmåga att hantera multipla sensorer och sensortyper.
- Förbättrad upptäckt. Lokalisering och klassificering
- Högkvalitativ lägesbild i realtid
- Relevanta beslut i rätt tid

För att kunna bygga ett sådant system på operativ nivå[6] krävs analytiska mått på systemeffekter, beslutsfattande och kostnadseffektivitet.

Nätverkets påverkan på militära operation kan alltså beskrivas med högre informations-överföringshastighet, samlad hantering av olika typer av sensordata, förbättrad datafusion, bättre tillgång till information för användare, högre säkerhet och tillgänglighet till information m m. Dessa attribut kan i någon mening sägas vara sådant som nätverket tillför eller förändrar jämfört med det traditionella plattformsfallet. Därmed utgör dessa, och flera, attribut sådant som måste knytas till olika effektmått[7] för att man skall kunna värdera nätverksorienterade operationer. Sådana analytiska mått kan t ex definieras inom ramen för en OODA-loop (fig, 14)



Figur 14. Systemeffekt (MOE) inom ramen för en OODA-loop.

Tabell 3. Olika analytiska mått.

Mått	Beskriver
MOE	Operativ förmåga, systemeffekt
MOP_{conv}	Konventionell effekt av t ex vapensystem
MOP_{comm}	Kommunikationsmått, t ex bandbredd och tidsfördröjningar
MOP_{info}	Informationsmått, t ex tillgänglighet, kvalitet och mängd
MOP_{od}	”Orient-Decide”, mått på t ex alternativ och risktagning

Första steget för att genomföra en analys enligt ovanstående modell är att identifiera de övergripande målen och definiera dessa som systemeffekter. Dessa mål kan förväntas vara desamma för det nätverksorienterade fallet som för det traditionella plattformsfallet.

När nätet tillförs är dock inte den traditionella systemeffekten (MOE) enbart beroende av de traditionella effektmåtten, (MOP_{conv}) utan även av mått som är associerade till nätverket (MOP_{comm}, MOP_{info} och MOP_{od}). För att få en så fullständig förståelse som möjligt för hur nätverket inverkar på ubåtsjaktsförmågan måste man studera och värdera hur nätverket påverkar samtliga delfunktioner och –system som ingår i en ubåtsjaktsoperation. Denna påverkan måste sedan kopplas till respektive MOP.

5.4 Effektmått för informationsarmén, RAND, 2001

Redogörelse för ett arbete utfört av RAND för US Army i syfte att identifiera effektmått som passar de operativa koncept som presenterades i Joint Vision 2010/2020. Arbetet presenteras i rapporten "MOE for the Information-Age Army, RAND, 2001.

Det är uppenbart att tillgång till information kommer att påverka våra system mer i framtiden än vad som tidigare varit fallet. Dock saknas förståelse för hur denna påverkan skall kunna mätas. Förståelsen för hur effekten av informationskomponenten skall kunna mätas är viktig då stora investeringar planeras i IT-system. Det krävs analytiska verktyg och metoder för att få fram bra beslutsunderlag. De viktigaste verktygen är bra effektmått (MOE) som kan relatera påverkan av information på den totala systemeffekten.

Rapporten utgår från de operativa koncept som beskrivs i Joint Vision 2010/2020. Det som idéerna baseras på är att kunskap skiljer sig från information (jmf fig 12) genom att kunskap tar hänsyn både till informationens värde och kvalitet. Därmed kan kunskap anses vara information som är relevant och användbar.

Arbetet utgår från en sannolikhetsmodell för kunskap där man försöker ta hänsyn till såväl kunskapens värde som kvalitet. Kunskapen kan sägas ha värde om den är till nytta för en beslutsfattare. Dess kvalitet kan bestämmas av sådana faktorer som huruvida den är korrekt, finns tillgänglig i rätt tid och är komplett.

Med detta som grund definieras en militär enhets kontrollområde [Control Area] som det område där enheten kan uppträda fritt efter eget godtycke. Enhetens kontrollradie, r_i, definieras som den minsta av storheterna vapenräckvidd, sensorräckvidd och radie på tilldelat operationsområde. Kunskap, K definieras nu som den grad av kännedom som en befälhavare har om motståndarens dispositioner i befälhavarens kontrollområde.

K definieras nu som en funktion

$$K = f(U, V, n, i)) \tag{5.1}$$

Där

U: Antal fientliga heter i området

V: Antal upptäckta fientliga enheter i området

n: Maximalt antal fientliga enheter

i: Antal sensorrapporter

Givet två aktörer, Blå och Röd med kunskaper $K_{Blå}$ respektive $K_{Röd}$ så sägs Blå ha informationsöverläge då $K_{Blå} > K_{Röd}$ och Röd ha informationsöverläge då $K_{Blå} < K_{Röd}$. Vidare definieras tröskelvärden $\delta_{Blå}$ och $\delta_{Röd}$ som innebär att endera sidan kan få informationsdominans då K är större än motståndarens K och högre än tröskelvärdet δ.

Det första steget är att nyttja dessa mått på kunskap i spelteoretiska beräkningar där fyra olika spelsituationer svarande mot 1) $K_{Blå} = K_{Röd}$, 2) $K_{Blå} > K_{Röd}$, 3) $K_{Blå} >> K_{Röd}$ och 4) $K_{Blå} > d_{Blå}$

$> K_{Röd}$ Resultatet av analysen är värden på hur mycket informationskomponenten bidrar till framgången för respektive spelare.

Nästa steg är att informationskomponenten läggs in i Lanchesterekvationerna. Här testas två olika sätt att modellera kunskap i såväl den linjära som den kvadratiska lagen. Det framstår inte som självklart, givet presentationen i rapporten, huruvida något av angreppssätten är att föredra framför de andra.

Rapporten fortsätter med en definition av olika systemeffekter knutna till de operativa koncept som presenteras i Joint Vision 2010/2020. man har valt att fokusera på de två koncepten Dominant Maneuver och Full Dimensional Protection. Systemeffekterna utgår från kunskapsparametern K men är i mångt och mycket bara förslag till hur informations-komponenten skall infogas i de traditionella effektmåtten.

För Dominant Maneuver föreslås följande effektmått:

> **Operativ förflyttning** (Deployment). Föreslaget mätetal är förflyttade enheter per tidsenhet. Effekten av mer kunskap förväntas vara kunskap om fiendens försök att blockera transportvägarna.
>
> **Taktisk räckvidd** (Operational Reach). Enhetens förmåga till taktisk förflyttning inom det tilldelade operationsområdet. Föreslaget mätetal är kilometer per tidsenhet. Informationskomponentens bidrag är kunskap om fiendens förväntade motstånd längs förflyttningsvägarna.
>
> **Kontroll av stridsfältet** (Battlespace Control). Beskrivs som förmågan att agera fritt i ett område samtidigt som man förhindrar fienden att agera i detsamma. Den förväntade effekten av information är att kontrollradien (se ovan) ökar.
>
> **Framryckningshastighet** (FLOT Movement, FLOT = Front Line of Troops). Detta är ett traditionellt mått (I US Army) som kan mätas i kilometer. Informations-komponenten förväntas bidra med bättre kunskaper om fiendens gruppering och förmåga, och därmed snabbare framryckning för de egna trupperna.

För Full Dimensional Protection föreslås följande effektmått

> **Skydd mot direkt och indirekt eld**. Detta mäts traditionellt med storheterna hårdhet, vilseledning och rörelse. Dessa föreslås ersättas med kunskapsbaserad (knowledge enhanced) hårdhet, vilseledning och röresle.
>
> **Förluster** (Casualties) förslås i framtiden liksom tidigare mätas i antal förluster (Number of Losses).

Slutligen förs en diskussion kring effektmätt för fredsstödjande operationer/stöd till samhället (MOOTW). Även här görs en koppling till de operativa koncepten i Joint Vision 2010/2020. Föreslagna effektmått listas i tabell 4.

Tabell 4. Förslag till mått på systemeffekt för de fyra operativa koncepten i Joint Vision 2010 inom ramen för fredsstödjande operationer och stöd till samhället.

Operativt koncept	Effektmått
Dominant Maneuver	Försåelse för lokal miljö Lokal infrastruktur Informationshantering Mellanstatliga relationer Civil ordning
Precision Engagement	Människor som påverkas Resursflöde
Full-dimensional protection	Förluster Skydd för egna styrkor mot fientligt inställda grupper Skydd för hjälporganisationer mot fientligt inställda grupper Skydd mot miljöförstöring
Focused Logistics	Underhåll i tid Lastkapacitet

[1] Alberts, Garstka , Stein, "Network Centric Warfare – Developing and Leveraging Information Superiority, 2nd ed, CCRP, 1999.

[2] Jämför hur man skall värdera förmågan för en viss kombination av fartyg och flygplan, var och en med sina fasta system, att lösa en uppgift med att låta ett system av system, funktionsuppdelat, lösa samma uppgift där man mer eller mindre fritt kan välja olika kombinationer av ingående system.

[3] Denna experimentverksamhet som summariskt nämns i Alberts et al 1999 är egentligen kärnan i den evolutionära utvecklingsprocessen. För svenskt vidkommande innebär det t ex att Demo 05/06 bör användas till att testa olika koncept mot i förväg uppställda analytiska mått. Analysen av dessa tester kan sedan ligga till grund för förändringar inför nästa generation av demonstratorer.

[4] Cleveland, Christian, Incze, "Measuring Coordinated Battlespace Management – Network Centric Measures of Performance and Measures of Effectiveness", NUWC 1999.

[5] Jämför t ex den svenska ubåtsjaktsstyrkan från 1980-talet som bestod av en kombination av olika typer av ytfartyg, helikoptrar och egna ubåtar.

[6] Originalartikeln [Cleveland 1999] använder begreppet "Theater level" vilket här översatts med "operativ nivå"

[7] Artikeln [Cleveland 1999] skiljer på systemeffekt, MOE, Measure of Effectiveness och mått på olika delsystems förmåga vilket kallas MOP, Measure Of Performance.

6 KOMMENTARER OCH FORTSATT ARBETE

Denna rapport redovisar inte ett slutfört arbete, enbart förslag till metoder och ett försök till utveckling av de metoder som krävs för att genomföra en värdering. Som de tre exemplen från CCRP, NUWC och RAND visar så är värdering av nätverksbaserad strid ett område som man arbetar på även i andra organisationer.

6.1 Olika sätt att hantera informationskomponenten

Det som gör nätverksbaserad strid väsenskild från den traditionella, plattformsbaserade, striden antas vara förmågan att dela funktioner mellan olika plattformar och samtidigt nyttja information från andra källor än de egna. Detta innebär att det är informationskomponenten, och de möjligheter som kan realisera med ett större nyttjande av informationsteknologi, som kommer att skilja den nätverksbaserade striden från den plattformsbaserade. Att värdera nätverksbaserad strid blir då i mångt och mycket att värdera insamling, bearbetning, förmedling och nyttjande av information.

Detta att informationen är den kritiska storheten och att värderingen bör göras som olika steg i en process (jmf fig 12) är något som går igen i såväl våra metoder som i de olika metoder utifrån som refereras i rapporten. Det skiljer dock mycket i hur vi går tillväga med att värdera nyttan av informationen.

De metoder vi försökt utveckla innebär att vi försöker ta hänsyn till informationskomponenten genom att studera hur den påverkar ”traditionella” parametrar som räckvidd och reaktionstid. Det innebär att vi börjar på den allra lägsta nivån i beslutsprocessen, datainsamling, och studerar hur informationsteknologin förändrar försvaret på denna nivå, t ex genom att försöka bedöma räckvidder för sensornätverk. Därefter tar vi ett steg upp genom att titta på hur informationen kan nyttjas i en lägesbild genom att försöka mäta kvaliteten på lägesbilden, med de tekniska parametrarna för våra insamlade data som grund.

Nästa steg i vår process innebär att vi genom användandet av funktionsschemana försöker bedöma hur lägesbilden med mera nyttjas för att uppnå en systemeffekt. Detta ansluter i mångt och mycket till hur NUWC resonerar, dock med den skillnaden att NUWC inte redovisar hur deras MOP respektive MOE tas fram, bara att de behöver tas fram.

Alternativet till detta är att försöka ta hänsyn till informationen som en storhet i sig och sedan ta in denna storhet i beräkningsmodellerna. Detta är i princip vad RAND försöker göra. RANDs angreppssätt leder till ett matematiskt mer komplext problem där de ingående komponenterna är mindre intuitiva. Ur behovet av att värdera nätverkets bidrag till förvarets förmåga framstår RANDs metodik vid första anblicken som attraktiv eftersom den direkt adresserar den informationskomponent som nätverket antas bidra med. Dock får man intrycket att RANDs metod är ett försök att utifrån mätbara storheter som antal enheter och antal sensorrapporter gå direkt på en slutlig systemeffekt, utan att ta hänsyn till hur informationen bearbetas, förmedlas eller nyttjas. Det verkar därför finnas stora risker för att RANDs metodik missar viktiga steg i beslutsprocessen. För värdering av ”sensor-to-shooter”-kedjor framstår inte denna metodik som tillämplig.

6.2 Utveckla hierarkin av parametrar

Denna rapport ger få definitiva svar men kastar ut desto fler frågor. Den viktigaste komponenten i ett fortsatt arbete utefter de linjer som dras upp här är att försöka bryta ned den hierarki av parametrar såsom sannolikheter, osäkerhetsområden och målsökares öppningsvinklar från effektmått till mätbara storheter. Detta kräver kunskaper om såväl de tekniska system som avses, som kunskaper om nätverkets struktur och funktion.

Ett sätt att hantera detta är att bygga enkla simuleringsmodeller där de olika typfallen modelleras enligt de funktionsscheman som vi tagit fram och med de parametrar som kan komma fram ur en nedbrytning enligt ovan. Sådana simuleringsmodeller är sannolikt en förutsättning för att kunna göra en tillräckligt rigorös känslighetsanalys avseende de mest kritiska parametrarna. Sådan modellutveckling ingick frånbörjan i den övergripande planen för arbetsgruppen under 2001.

6.3 Metoder för att värdera sensorledning

Vidare bör komponenten sensorledning studeras närmare. Detta är något som inte existerar idag men som får antas ha en viktig roll i det nätverksbaserade försvaret. Hur sensorledningen realiseras och vilka metoder som nyttjas kan bli avgörande för hur framgångsrikt det nätverksbaserade försvaret klara att lösa en uppgift.

I avsnitt 3.3 nämns i förbigående två olika sätt att få fram ”bättre” måldata. Det första är att sända ut ytterligare plattformar med sensorer, traditionellt illustrerat med en UAV. Det andra sättet är att nyttja befintliga sensorer i nätet men att försöka få ut mer information ur dem, t ex genom ytterligare sensorfusion eller mer avancerad signalbehandling. En framtida uppgift för värderingen måste vara att studera om bägge dessa metoder är möjliga och under vilka förutsättningar samt hur val av metod påverkar det nätverksorienterade alternativtes förmåga att lösa sina uppgifter.

6.4 Nya typfall?

I förstudierapporten definieras de fem typfallen som också beskrivs kortfattat i bilaga 1 till denna rapport. Sedan det arbetet gjordes har ett antal olika scenarier tagits fram inom ramen för arbetet med Demo05 och Demo06. Det bör övervägas om det är lämpligt att ersätta vissa av våra typfall med scenarier ur Demo05/06. Detta skulle ha den fördelen att man använder ”samma” typfall/scenarier i de olika projekten som berör utvecklingen av NBF. Dock skall noteras att scenarierna för Demo05/06 i vissa fall inte rör väpnad strid. Eftersom syftet med detta arbete är att värdera väpnad strid måste sannolikt några av de egna typfallen behållas.

BIBLIOGRAFI

Alberts, David S, Garstka, John J, Stein Frederik P, ”*Network Centric Warfare – Developing and Leveraging Information Superiority, 2nd ed*”. CCRP, 1999

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

Cleveland, Jerome, Christian, Raymond, Incze, Brian, ”Measuring Coordinated Battlespade Management – Network Centric Measures of Performance and Measures of Effectiveness”, NUWC 1999.

Christian, Raymond, “Concepts in Network-Centric ASW”, NUWC 2001, Presenterad vid SMi 4th Annual Submarines and ASW Conference, London 1-2, oktober 2001

Darilek, Richard, Perry Walter, Bracken, Jerome, Gordon, John Nichiporuk, Brian ”Measures of Effectiveness for the Information-Age Army, MR-1115-A, RAND, 2001.

O’Hanlon, Michael, ”*Technological Change and the Future of War*”, Brookings Institution Press, 2000.

BILAGA 1 – SAMMANFATTNING AV TYPFALL

Här beskrivs kortfattat de fem olika typfallen som ska studeras. En omfattande redogörelse för varje scenario finns i förtsudierapoporten Värdering av nätverksorienterad krigföring- Förstudie, bilaga 1-5, Alsér 2002.

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.

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.

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.

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.

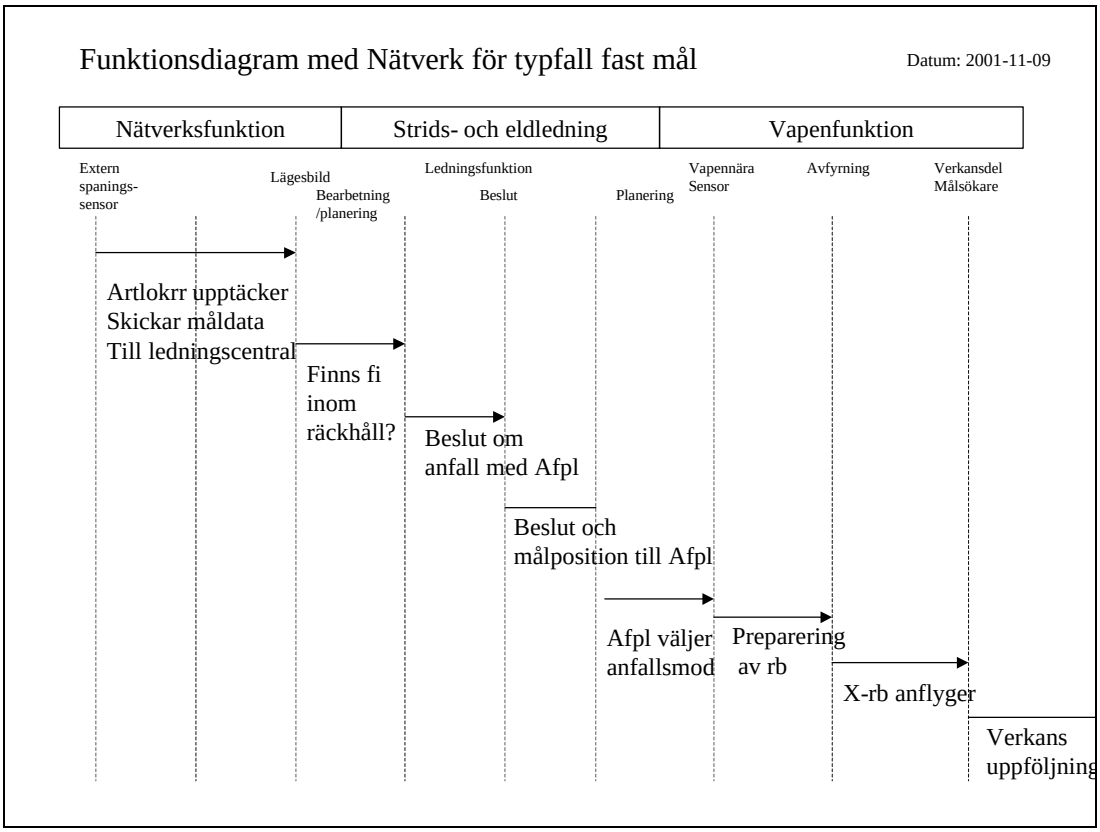
Undervatten

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.

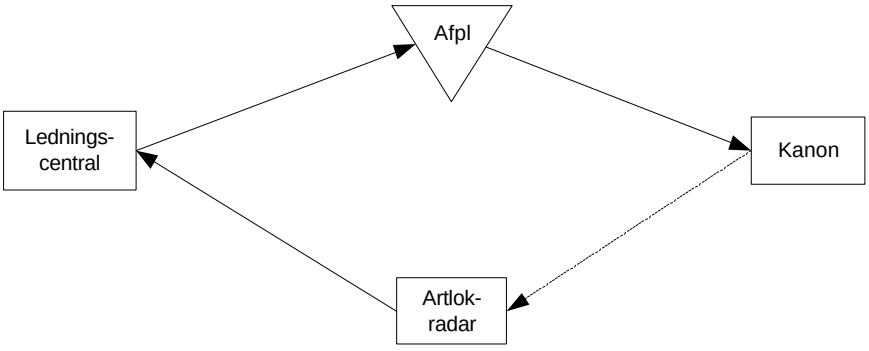
BILAGA 2 - FUNKTIONSSCHEMAN

Fast mål

Nätverk

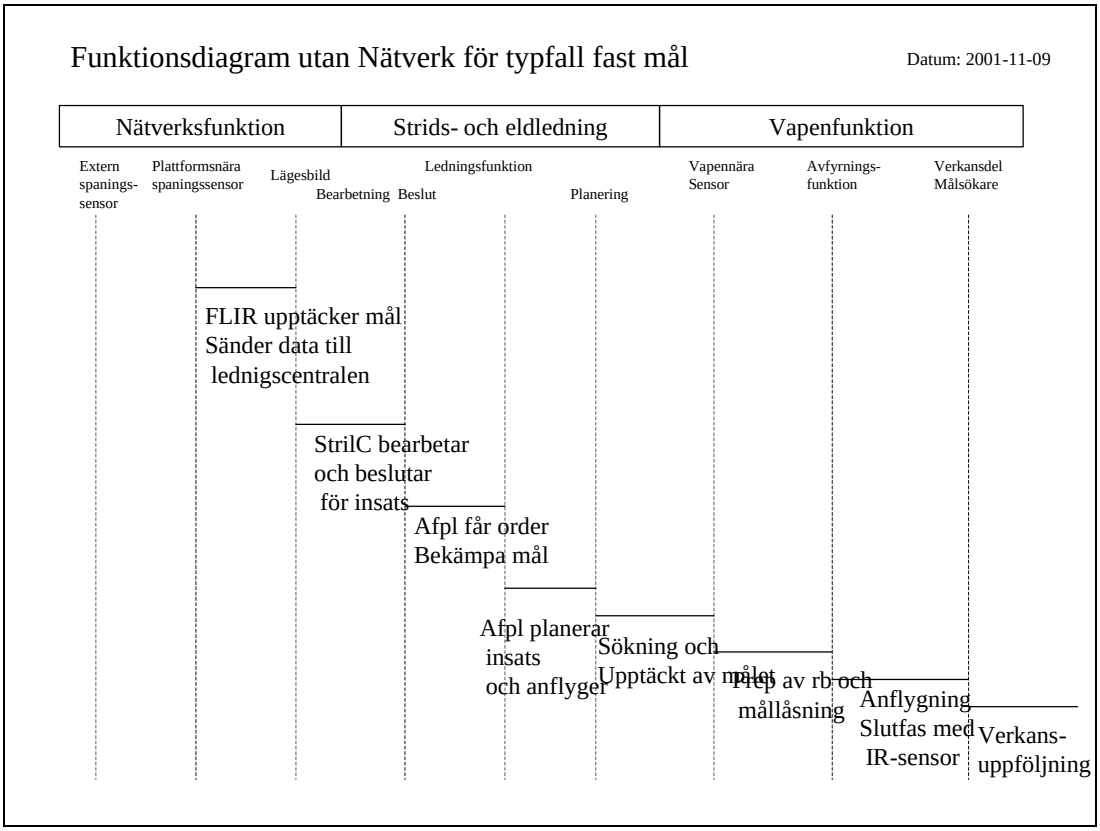


Figur 15. Funktionsschema för nätverk i typfallet Fast mål.

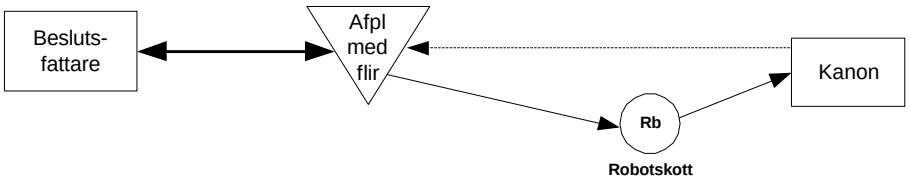


Figur 16. Schematisk beskrivning av en nätverksorienterad lösning för typfallet Fast mål. Motsvarande flödesschema följer strukturen i figur 5.

Plattform



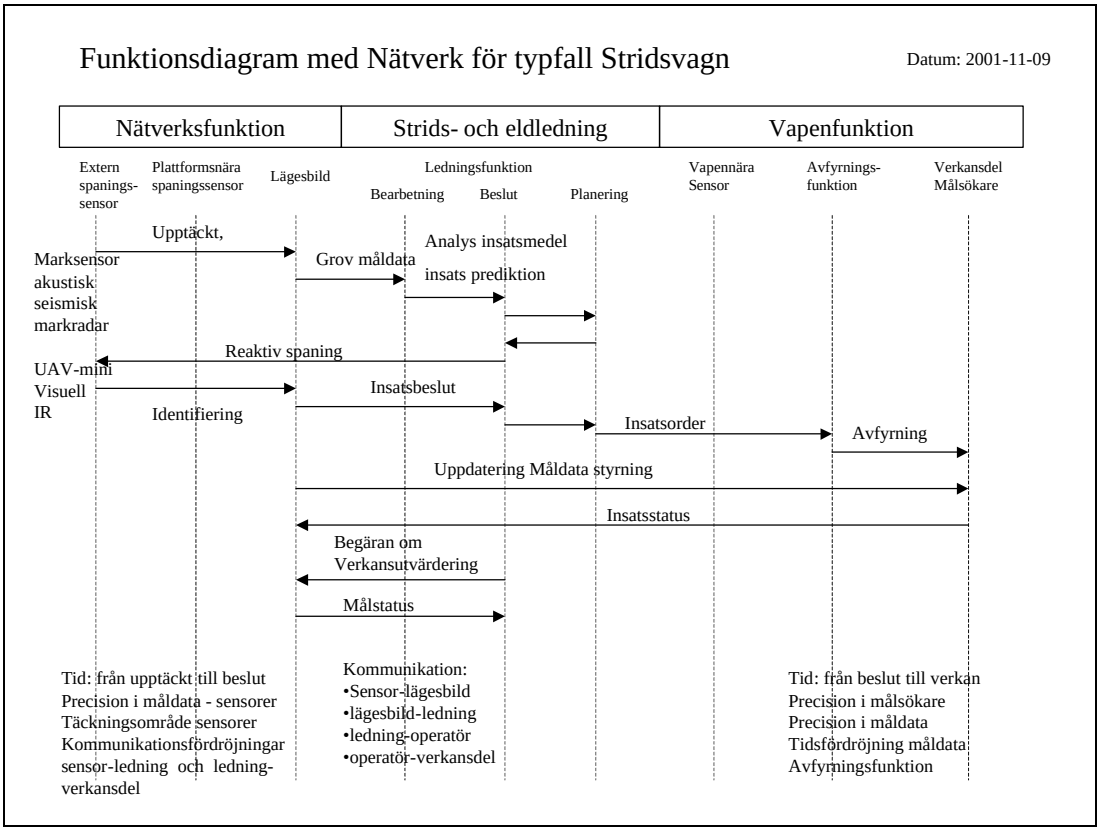
Figur 17. Funktionsschema för plattform i typfallet Fast mål.



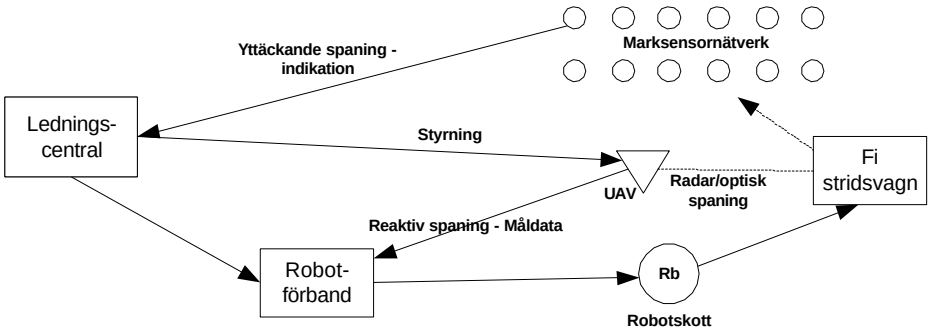
Figur 18. Schematisk beskrivning av en plattformsorienterad lösning för typfallet Fast mål. Motsvarande flödesschema följer strukturen i figur 4.

Stridsvagn

Nätverk

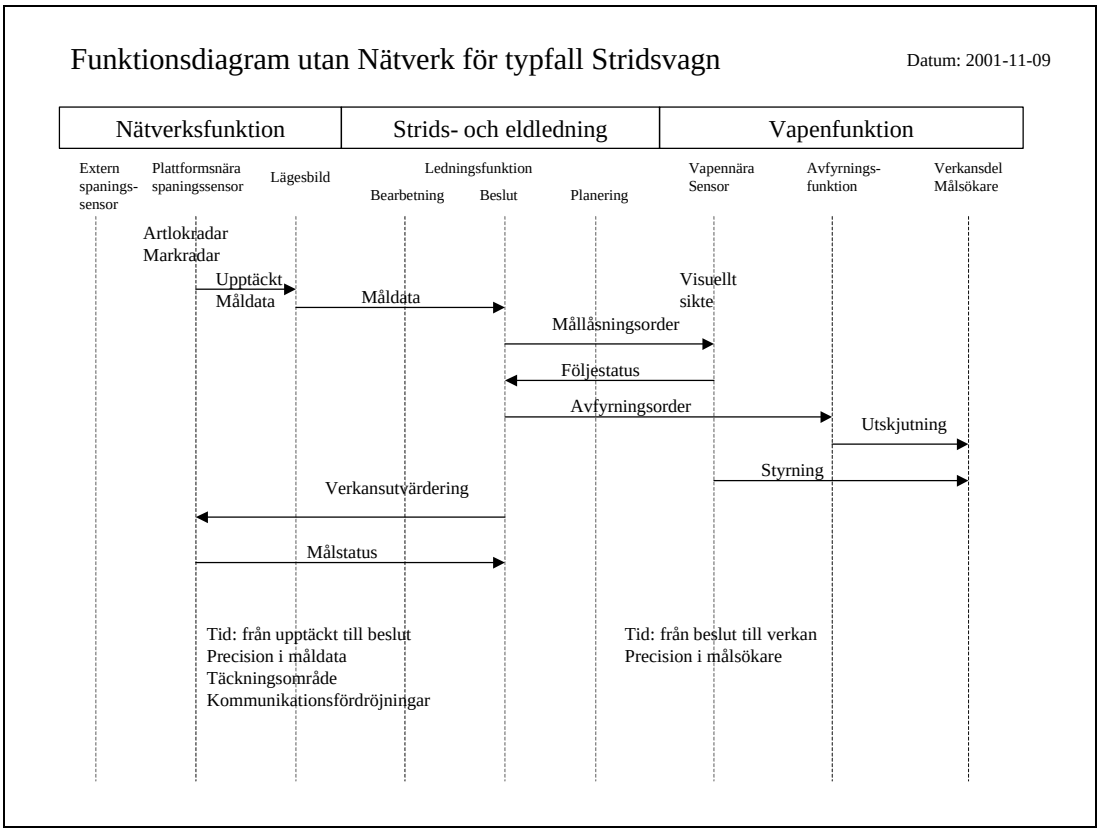


Figur 19. Funktionsschema för nätverk i typfallet Stridsvagn.

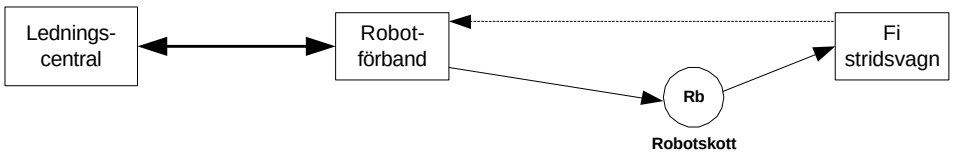


Figur 20. Schematisk beskrivning av en nätverksorienterad lösning för typfallet stridsvagn. Motsvarande flödesschema följer strukturen i figur 6.

Plattform



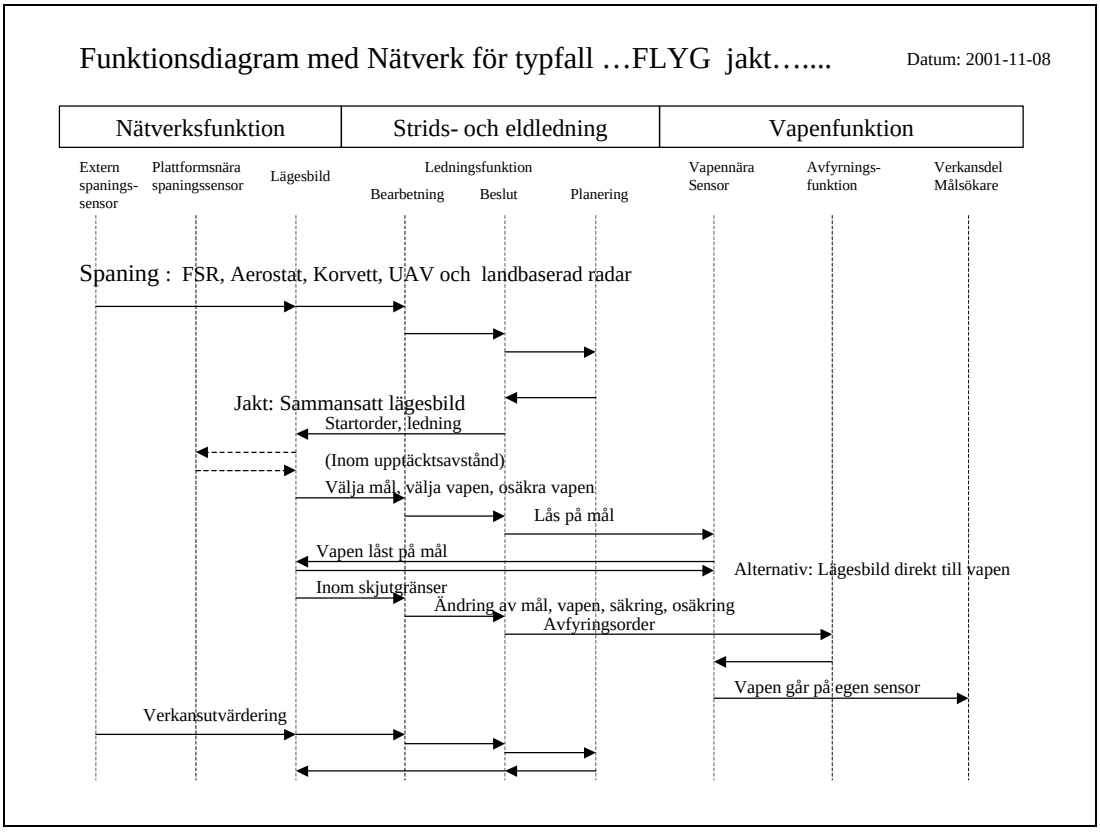
Figur 21. Funktionsschema för plattform i typfallet Stridsvagn.



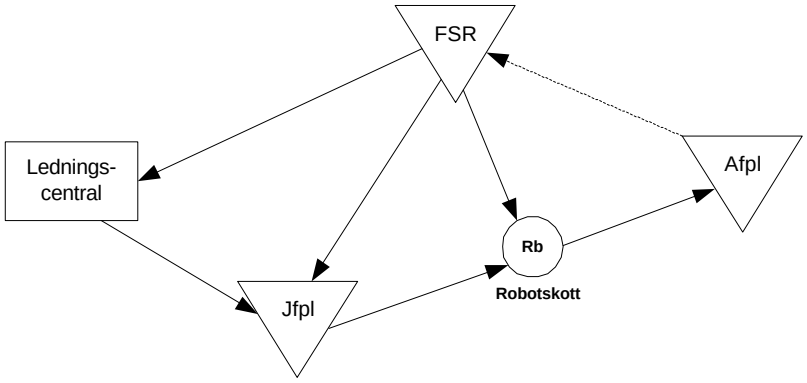
Figur 22. Schematisk beskrivning av en plattformsorienterad lösning för typfallet stridsvagn. Motsvarande flödesschema följer strukturen i figur 4.

Stridsflyg

Nätverk

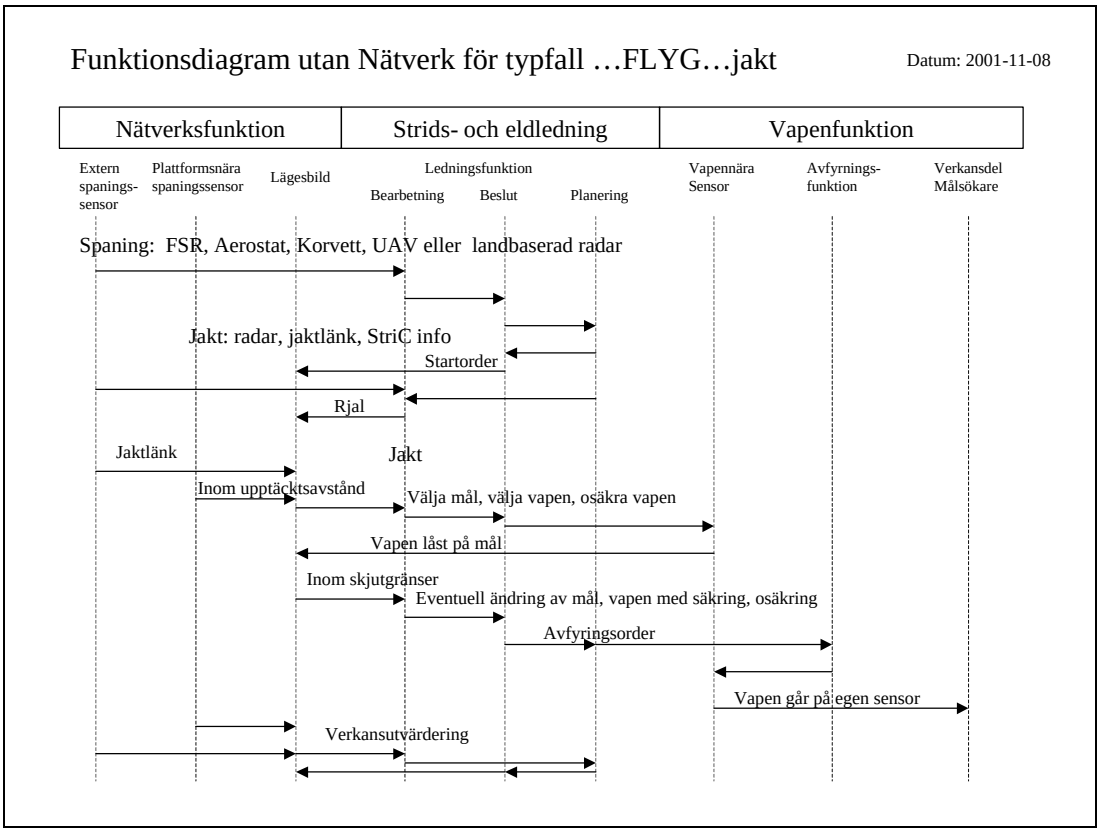


Figur 23. Funktionsschema för nätverk i typfallet Stridsflyg.

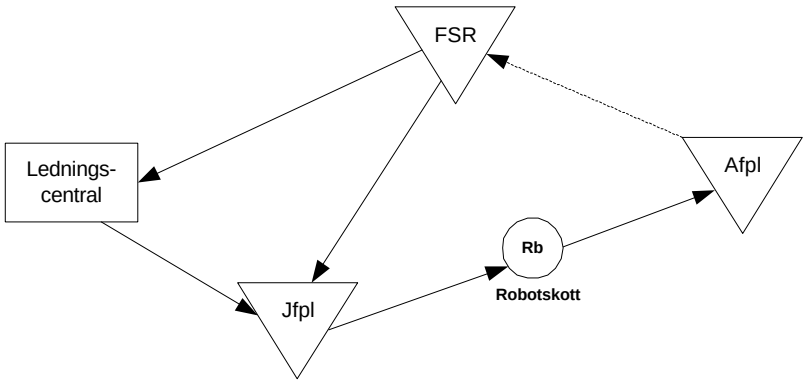


Figur 24. Schematisk beskrivning av en nätverksorienterad lösning för typfallet Stridsflyg. Motsvarande flödesschema följer strukturen i figur 5.

Plattform



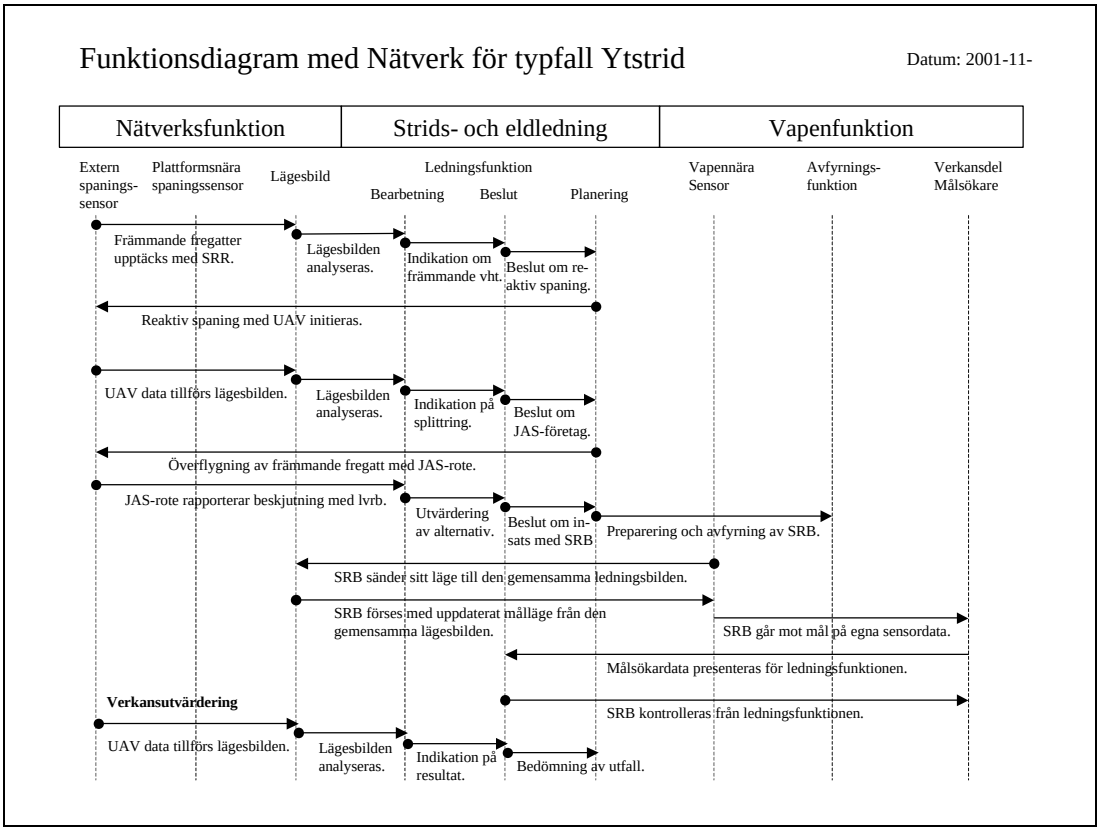
Figur 25. Funktionsschema för plattform i typfallet Stridsflyg.



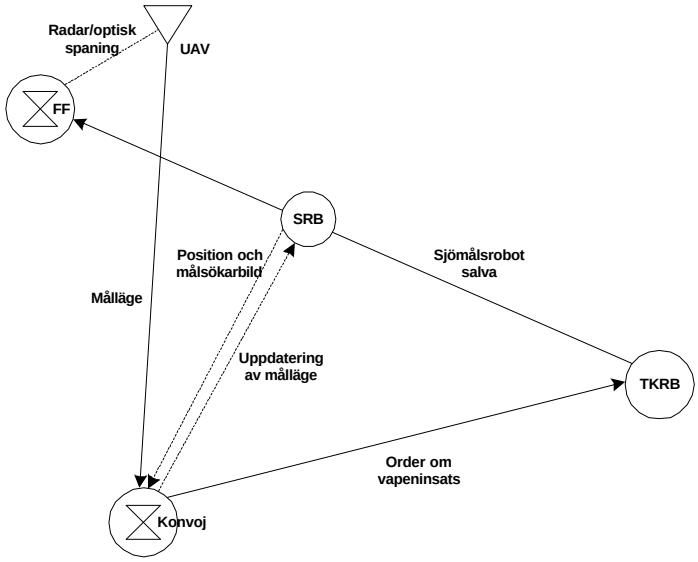
Figur 26. Schematisk beskrivning av en plattformsorienterad lösning för typfallet stridsflyg. Motsvarande flödesschema följer strukturen i figur 4. Skillnaden mellan plattforms- och nätverkslösningen är att FSR i plattformsfallet inte förutsätts kunna leda jaktrobotar mot sina mål.

Ytstridsfartyg

Nätverk

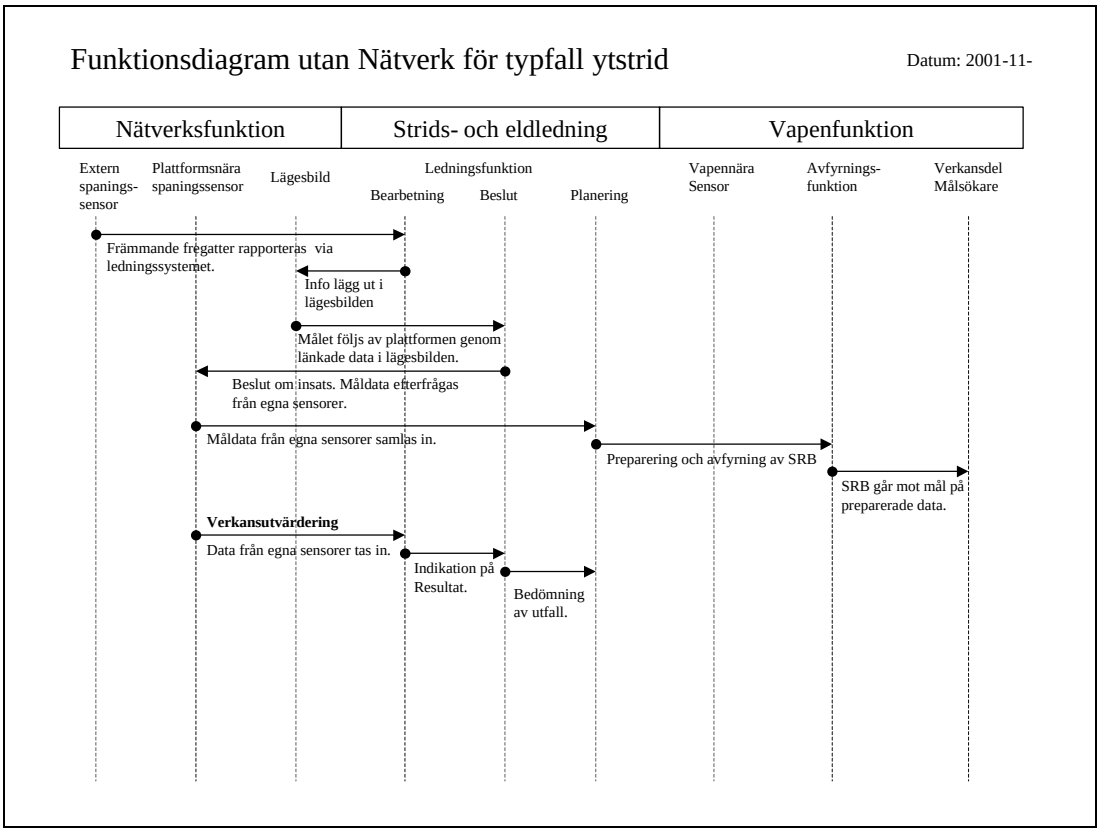


Figur 27. Funktionsschema för nätverk i typfallet Ytstridsfartyg.

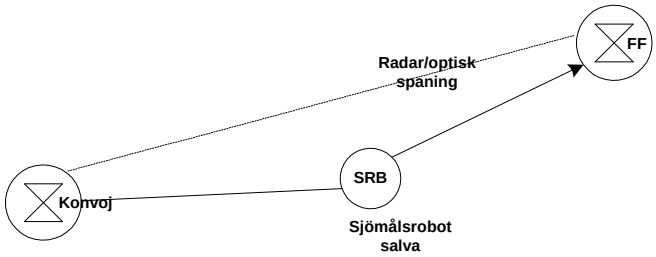


Figur 28. Schematisk beskrivning av en nätverksorienterad lösning för typfallet ytstridsfartyg. Motsvarande flödesschema följer strukturen i figur 6.

Plattform



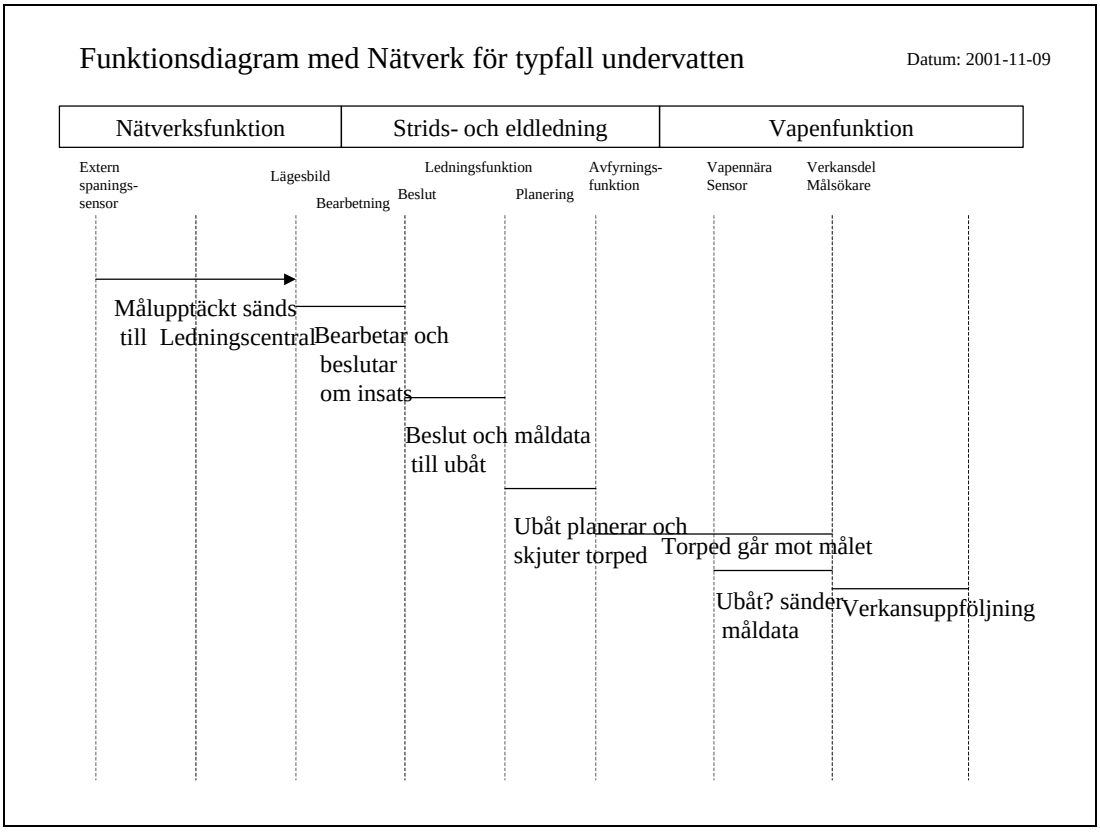
Figur 29. Funktionsschema för plattform i typfallet Ytstridsfartyg.



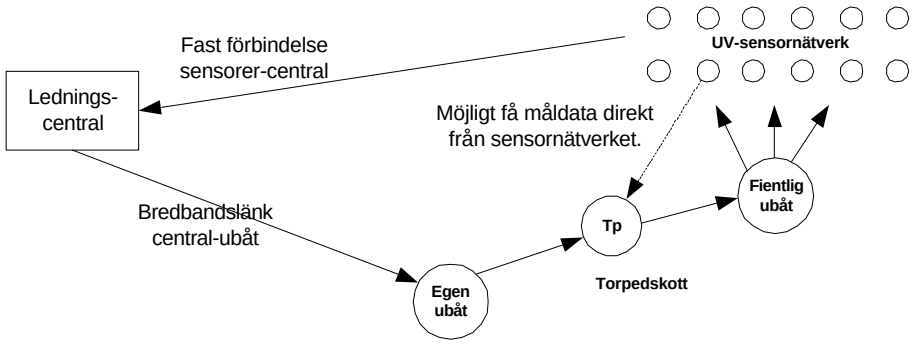
Figur 30. Schematisk beskrivning av en plattformsorienterad lösning för typfallet ytstridsfartyg. Motsvarande flödesschema följer strukturen i figur 4.

Undervatten

Nätverk

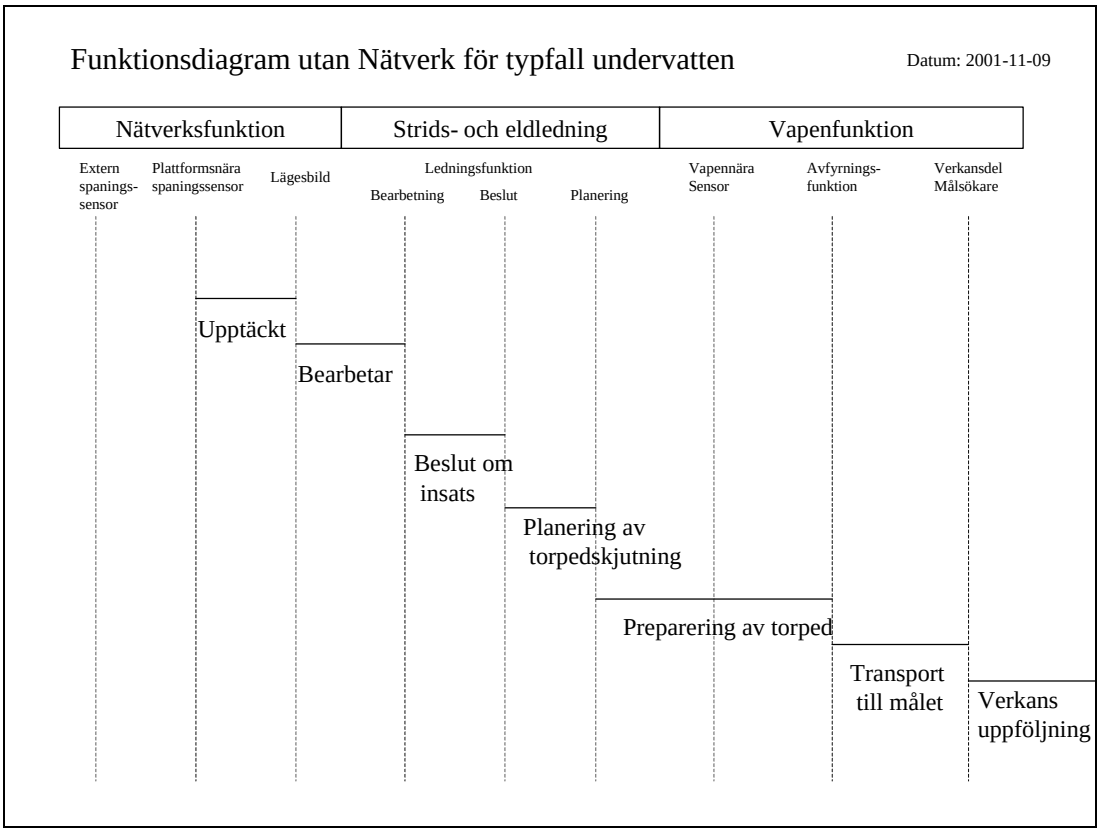


Figur 31. Funktionsschema för nätverk i typfallet Undervatten.

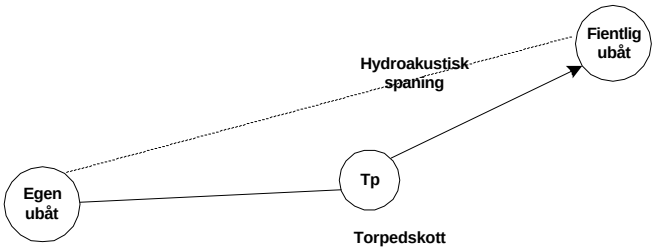


Figur 32. Schematisk beskrivning av en nätverksorienterad lösning för typfallet undervatten. Motsvarande flödesschema följer strukturen i figur 5.

Plattform



Figur 33. Funktionsschema för plattform i typfallet Undervatten.



Figur 34. Schematisk beskrivning av en plattformsorienterad lösning för typfallet undervatten. Motsvarande flödesschema följer strukturen i figur 4.

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI Försvarsanalys 172 90 Stockholm	FOI-R--0671--SE	Metodrapport
	Forskningsområde 2. Operationsanalys, modellering och simulering	
	Månad, år December 2002	**Projektnummer** E1805
	Verksamhetsgren 5. Uppdragsfinansierad verksamhet	
	Delområde 22 Metod och utredningsstöd	

Författare/redaktör	Projektledare
Lars Höstbeck	Olof Söderqvist
	Godkänd av Jan Foghelin
	Uppdragsgivare/kundbeteckning Försvarsmakten
	Tekniskt och/eller vetenskapligt ansvarig Karin Mossberg

Rapportens titel

Metoder för värdering av nätverksbaserad strid – underlagsrapport i FoRMA

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.

Denna rapport redogör för arbetsgruppens resultat under hösten 2001. I rapporten beskrivs den metod med olika analytiska mått och funktionsscheman som utvecklas för att värdera de ”sensor-to-shooter”-kedjor vi arbetar med. Vidare görs en jämförelse med tre olika metoder som publicerats i öppen litteratur.

Nyckelord

Nätverksbaserat försvar, NBF, värdering, effektmått, lägesbild

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 52 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm Sweden	FOI-R--0671--SE	Methodology report
	Research area code 2. Operational Research, Modelling and Simulation	
	Month year December 2002	**Project no.** E1805
	Customers code 5. Commissioned Research	
	Sub area code 22 Operational Analysis and Support	
Author/s (editor/s) Lars Höstbeck	**Project manager** Olof Söderqvist	
	Approved by Jan Foghelin	
	Sponsoring agency Swedish Armed Forces	
	Scientifically and technically responsible Karin Mossberg	

Report title (In translation)

Methods for assessment of Network-Centric Warfare – base data report to FoRMA

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.

This report describes the work done by the working group during the autumn of 2001. The report describes the method with various Measures of Effectivness (MOE) and charts that has been developed in order to assess the sensor-to-shooter loops the group has decided to work with. The report also compares the method developed to three different methods reported in the literature.

Keywords

Network Centric Warfare, NCW, Assessment, Evaluation, Measures of Effectiveness

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 52 p.
	Price acc. to pricelist