FOI

Vilseledning av lägesbild

JOHAN SCHUBERT, JONAS CLAUSEN MORK, RONNIE JOHANSSON,
TEODOR SOMMESTAD, MARKUS SVENSSON, HAMPUS THORELL

FOI-D--0717--SE Mars 2016

Johan Schubert, Jonas Clausen Mork, Ronnie Johansson, Teodor Sommestad, Markus Svensson, Hampus Thorell

Vilseledning av lägesbild

Titel	Vilseledning av lägesbild
Title	Deception of Common Operational Picture
Rapportnr/Report no	FOI-D--0717--SE
Månad/Month	Mars/March
Utgivningsår/Year	2016
Sidor/Pages	28 p
Kund/Customer	FOI
Forskningsområde	12. Övrigt
FoT-område	
Projektnr/Project no	I35416
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Den som har inblick i och genom vilseledning kan påverka motståndarens lägesuppfattning ges övertaget i militära operationer: egna operationer gynnas, och skyddas mot liknande metoder från motståndaren. Vilseledning kan delas in i två kategorier, antingen för att framhäva en viss verksamhet eller för att dölja en annan. I vårt arbete har vi valt att fokusera på det tidigare, dvs. att uppvisa skenbar aktivitet för att därmed påverka motståndarens beslut i en för oss gynnsam riktning.

Detta dokument utgör slutrapporten för det avdelningsöverskridande kompetensutvecklingsprojektet *Vilseledning av lägesbild* som har pågått under åren 2014 och 2015. Projektet omfattar tre avdelningar (IAS, STS, FA) och fyra systemperspektiv: ett operativt perspektiv, ett informationsperspektiv, ett telekrigsperspektiv, och ett cyberperspektiv. Spännvidden i kompetenser ger möjlighet till överblick och tvärvetenskapliga angreppssätt som spänner över stora delar av vilseledningsinsatser.

Med hjälp av detta tvärvetenskapliga projekt har vi skapat ny kunskap inom FOI som lyfter forskningen om informationskrigföring till en högre nivå än tidigare genom att koppla ihop den med informationsfusion. Centralt i arbetet har varit integrationen av de olika perspektivens metoder.

De olika perspektiven har utvecklat en lösning för sin respektive domän samt ett sätt att integrera perspektiven till ett enhetligt system för vilseledning.

Ett marklägesscenario beskrivs och används för att demonstrera det föreslagna vilseledningssystemet.

Nyckelord: Vilseledning, telekrig.

Summary

The one who has access to the enemy's situation picture and the ability to manipulate it through deception enjoys an advantage in military operations. By deception, our own operations can be more successful, and deceptive activities from the enemy can be detected. Deception can be divided into two categories, either to promote the existence of a certain activity, or to conceal another. In our work, we focus on the former, i.e., to show some non-existent activity to beneficially affect the decisions of the enemy.

This document is the final report of the multi-department competence development project *Deception of Common Operational Picture*, which was performed during the years 2014 and 2015. The project involves three departments (IAS, STS, FA) and four system perspectives: an operative perspective, an information management perspective, an electronic warfare perspective, and cyber perspective. The spread of competencies provides an opportunity to get comprehensive overview and realize cross-disciplinary solutions that cover many parts of deception activities.

By this inter-disciplinary project, we have created new knowledge at FOI that widens our research on information superiority by connecting it to information fusion. The integration of the different perspectives have been of importance.

The different perspectives have developed a solution for their respective domains and a way to integrate to a homogeneous system for deception.

A ground warfare scenario is described and used to demonstrate the proposed deception system.

Keywords: Deception, electronic warfare.

Innehållsförteckning

1 Inledning

Detta dokument utgör slutrapporten för det avdelningsöverskridande kompetensutvecklingsprojektet *Vilseledning av lägesbild* som har pågått under åren 2014 och 2015. Projektet omfattar tre avdelningar (IAS, STS, FA) och fyra systemperspektiv: ett operativt perspektiv, ett informationsperspektiv, ett telekrigsperspektiv, och ett cyberperspektiv. Spännvidden i kompetenser ger möjlighet till överblick och tvärvetenskapliga angreppssätt som spänner över stora delar av vilseledningsinsatser.

Med hjälp av detta tvärvetenskapliga projekt har vi skapat ny kunskap inom FOI som lyfter forskningen om informationskrigföring till en högre nivå än tidigare genom att koppla ihop den med informationsfusion. Centralt i arbetet har varit integrationen av de olika perspektivens metoder.

1.1 Bakgrund

Ett sätt att uppnå och behålla ett informationsöverläge är genom vilseledning. Vilseledning definieras enligt Försvarsmaktens handbok för informationsoperationer [1] som:

> *”Medvetna åtgärder som syftar till att ge motståndaren ett felaktigt beslutsunderlag för att få aktören att disponera sina resurser på ett som gynnar våra syften.”*

Den som har inblick i och genom vilseledning kan påverka motståndarens lägesuppfattning ges övertaget i militära operationer: egna operationer gynnas, och skyddas mot liknande metoder från motståndaren. Vilseledning kan delas in i två kategorier, antingen för att framhäva en viss verksamhet eller för att dölja en annan [1]. I vårt arbete har vi valt att fokusera på det tidigare, dvs. att uppvisa skenbar aktivitet för att därmed påverka motståndarens beslut i en för oss gynnsam riktning.

Kunskap om sensorer och kommunikationslänkar samt hur de bekämpas med telekrig och cyberkrigföring, bearbetning av information till ökad förståelse, samt hur denna omsätts i taktiska och operativa beslut, finns vid FOI men är utspridd på olika avdelningar.

1.2 Problemnedbrytning och projektorganisation

Fyra olika perspektiv på vilseledning representeras i projektet: *informationsperspektivet* (INFO) underhåller den egna lägesbilden samt en uppfattning om en motståndares uppskattade lägesbild; det *operativa perspektivet* (OP) som värderar vilseledningsinsatser ur det operativa perspektivet; och slutligen *telekrigs- och cyberperspektiven* (TK respektive CYB) som avgör vilka faktiska vilseledningsinsatser som är möjliga och lämpliga vid ett visst tillfälle. Systemet syftar till att uppskatta och efterlikna motståndarens lägesbild för att därigenom kunna avgöra vilken vilseledning som bör utföras. Varje perspektiv, utom CYB, motsvaras av en egen mjukvarumodul i ett hypotetiskt vilseledningssystem. I fortsättningen kan vi hänvisa till den vilseledande (egna) parten som *Blå* och den vilseledda (motståndaren) som *Röd*.

Anledningen till att CYB-perspektivet har lyfts ut ur mjukvaran är att det visade sig under projektets gång vara svårt att på ett enkelt sätt förena hanteringen av TK- och CYB-insatser i samma program. De CYB-insatser som föreslås i projektet måste nämligen aktiveras under en längre tidsperiod och deras konsekvenser är mindre tydliga och förutsägbara än TK-insatser. För tydlighets skull har vi därför valt att fokusera på hur TK-insatser kan styras för att stödja OP-perspektivets behov av vilseledning.

Varje perspektiv omfattar en mjukvarumodul för ett hypotetiskt vilseledningssystem och scenario (scenariot beskrivs vidare i avsnitt 1.3). I mjukvaran, som är utvecklad i programspråket MATLAB, fungerar INFO-modulen som en medlare mellan OP-modulen

och hanteringen av vilseledningsresurserna i TK-modulen, och som skapare och underhållare av motståndarens uppskattade lägesbild.

Programkoden återges kortfattat nedan. Rad 1–7 är en slinga som upprepas ett visst antal gånger (i projektet har vi använt oss av tre tidssteg i simuleringen). I rad 2 uppdateras Röds lägesbild (`sp`) för det aktuella tidssteget (genom att samla in och fusionera sensorobservationer). Lägesbilden modelleras som en sannolikhetsfunktion över Blås handlingsalternativ (alternativen beskrivs vidare i avsnitt 1.3). I rad 3 anropas OP-modulen som beslutar vilken vilseledningsoperation som är mest önskvärd (`desired_sp`) och förmedlar detta till INFO-modulen. I rad 4 räknar INFO-modulen i sin tur ut hur motståndarens aktuella lägesbild bör förändras (`requested_update`) för att OP-modulens ideal skall nås. Önskad förändring skickas vidare till TK-modulen i rad 5. Det är inte säkert (snarare osannolikt) att TK-modulen lyckas uppfylla önskemålet fullständigt givet situation och tillgängliga resurser. Därför returneras TK-modulens bästa resultat (`achieved_update`), som i rad 6 fusioneras med Röds lägesbild för att uppdatera vår uppskattning av denna.

```
1: For t = 1 to #simulation_steps
2:    sp = update_situation( t )
3:    desired_sp = OP( sp )
4:    requested_update = INFO( desired_sp )
5:    achieved_update = TK( requested_update )
6:    sp = update_deception( achieved_update )
7: End
```

Centralt i vårt vilseledningssystem är representationen och hanteringen av Röds lägesbild. Eftersom det är osannolikt att Blå har säker och detaljerad kunskap om Röds ledningssystem så är det inte meningsfullt att försöka beskriva Röds lägesbild i för mycket detalj. Det blir ändå inte helt rätt. Istället kan man försöka efterlikna det som är rimligt på en mer allmän nivå vilket även ger en del friheter (exempelvis att man kan försöka anpassa hantering och representation till Blås syften).

Blås hantering av Röds lägesbild beskrivs övergripande i programkoden ovan, men en minst lika utmanade uppgift är att välja dess representation. I vårt arbete har vi valt en lägesbeskrivning som direkt berör just den vilseledningsoperation som Blå avser att utföra mot Röd. Oavsett Röds verkliga interna lägesbild så skär Blå ut den del av läget som berör vilseledning och i vårt fall blir det inte en fysisk situation utan intentionen hos Blå. Blå kan i det korta tidsperspektivet (ett par timmar) antas vilja göra ett av följande sju alternativ: 1) stanna i Arlanda; 2) förflytta till Knivsta¸ 3) förflytta till Rimbo; 4) förflytta till Almunge; 5) förflytta till Uppsala; 6) förflytta till Skoby; eller 7) förflytta till Knutby. För att introducera osäkerheter i Röds lägesbild så låter vi en sannolikhetsfunktion med föregående sju nämnda alternativ som domän vara Blås interna representation av Röds lägesbild. Denna representation är också den primära informationen för kommunikation mellan de olika programmodulerna. Exempelvis i rad 3 anropas OP-modulen med denna probabilistiska uppfattning av Röds lägesbild och som svar får man önskad lägesbild hos Röd uttryckt på samma sätt. I rad 4 är resultatet, `requested_update`, visserligen av annan typ (det handlar om hur lägesbilden bör förändras inte om lägesbilden själv), men representationen är densamma (dvs. en sannolikhetsfunktion över de sju handlingsalternativen).

1.3 Scenario

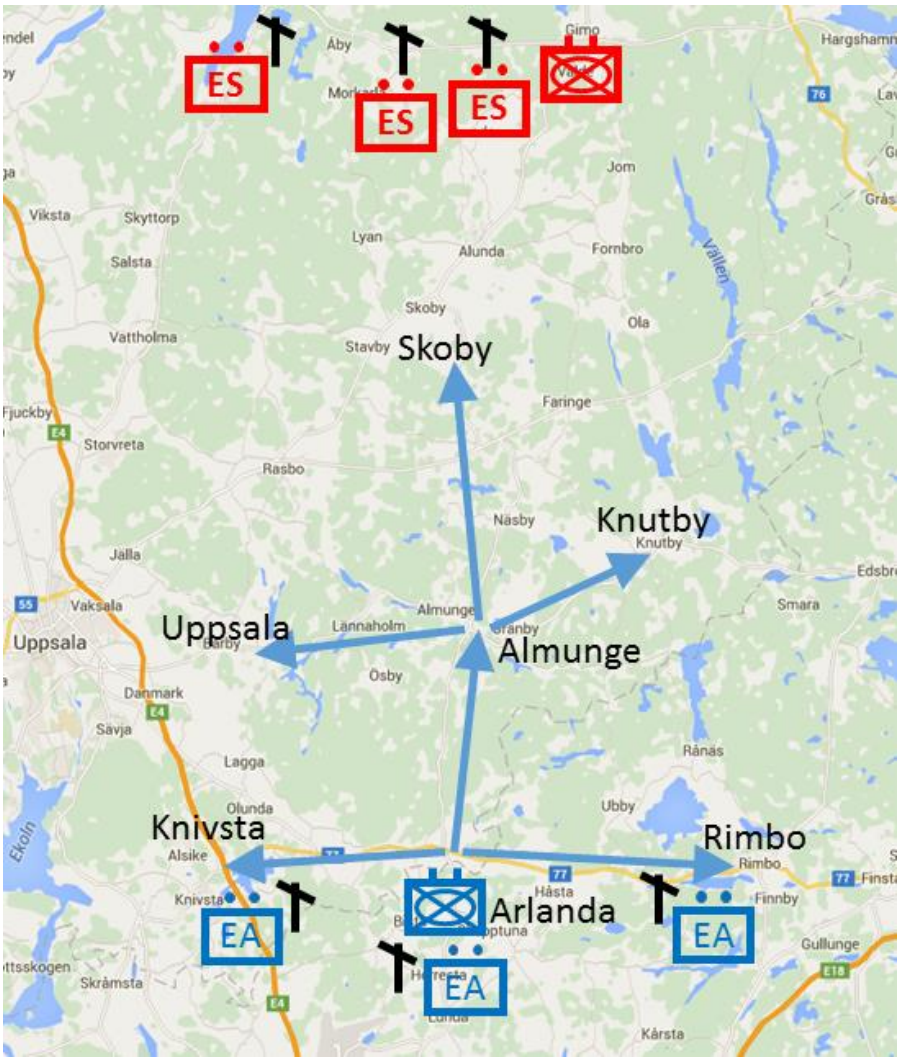
Det exempelscenario som vi använder i projektet omfattar två aktörer: en försvarande mekaniserad bataljon (Blå) vars startposition är i närheten av Arlanda och en angripande mekaniserad bataljon (Röd) som startar i Gimo-trakten (se Figur 1).

Scenariot simuleras i tre steg och uppskattningsvis förflyter 20–30 minuter i scenariot mellan varje tidssteg. Blå förflyttar sig under simuleringen först till Almunge och därefter

till Skoby. Blå avser att vilseleda om sin förflyttning och destination för att kunna möta och överraska Röd i Skoby.

Blå har till sitt förfogande tre störsändare (med beteckning EA[1] i figuren) som används för att via radiosignaler kunna vilseleda om Blås rörelser. På Röd sida finns mottagare som kan ta emot de vilseledande signalerna (med beteckning ES[2]).

I varje tidssteg uppdateras Blås uppfattning om Röds lägesbild baserat på Röds sensorer, men även Blås avsiktliga vilseledning (vilket framgår av rad 2 och 6 i programkoden i föregående avsnitt).



Figur 1. Vi tänker oss ett scenario med en Blå försvarande och en Röd angripande styrka. Den blå styrkan har för avsikt att vilseleda den Röd om sin framryckning för att kunna leda Röd till Skoby för en överraskningskonfrontation.

1.4 Översikt

I de följande fyra kapitlen behandlas de olika systemperspektiven på vilseledning, dvs. operativa (kapitel 2), information (kapitel 3), telekrig (kapitel 4), samt cyber (kapitel 5), var för sig. Därefter avslutas rapporten med ett kapitel som redogör för en exempelkörning av vårt föreslagna vilseledningssystem och projektets slutsatser.

[1] Elektronisk attack.
[2] Elektronisk stödverksamhet.

2 Operativa perspektivet

I det operativa perspektivet har fokus legat på att formulera ett konkret behov av vilseledningsåtgärder som kan förbättra möjligheterna att uppnå militära mål.

2.1 Problemdiskussion

Spelteori är ett verktyg för att formellt analysera interaktion mellan parter där varje parts utfall av interaktionen beror på de övriga parters agerande. Militär konflikt är just en sådan domän: konsekvenserna av en viss strategi beror på vilka strategier motparten eller motparterna har valt.

När två rationella motståndare ställs mot varandra kan de förväntas välja de strategier som ger dem själva det bästa möjliga utfallet, givet vad de bedömer att motståndaren kommer att göra. En kombination av strategier för båda spelare som är sådan att ingen spelare ser skäl till att ensidigt ändra strategi kallas för en (Nash-)*jämvikt*. Ett (finit) *spel*, en formell situationsbeskrivning, har alltid *minst en* sådan jämvikt, men kan ibland ha många. Det finns, i spelteorin, en rad olika jämviktsbegrepp som på olika sätt förfinar detta genom att ställa upp ytterligare krav, men för detta arbete har vi nöjt oss med att använda Nash-jämvikten som lösningskoncept.

Vilseledning, rätt genomförd, kan ändra den vilseledda partens uppfattning om vilket spel som spelas, och därmed påverka vilken strategi denne förväntas välja. Låt oss kalla detta *indirekt vilseledning*. I ett militärt sammanhang kan det handla om att förändra bilden av sådant som vilka enheter som finns tillgängliga, var de finns, hur man värderar terrängen och vilka framryckningsvägar som är brukbara. En svårighet med indirekt vilseledning är att den kan kräva många samordnade insatser att uppnå samt att den är beroende av en god förståelse av motståndaren och dennes beslutsfattande.

En annan form av vilseledning är att fokusera på att ändra motståndarens uppfattning om vilken strategi som man själv kommer att välja (eller redan har valt), utan att (nödvändigtvis) manipulera spelets synbara övriga struktur. Låt oss kalla detta *direkt vilseledning*. Här kan det handla om att få motståndaren att tro att man kommer att röra sig 10 km västerut, när man avser att röra sig 10 km österut. För direkt vilseledning är en utmaning att den specifika strategi som man försöker övertyga motståndaren om att man avser genomföra kan se orimlig ut, givet dennes helhetsbild av situationen, vilket i sin tur kan undergräva möjligheten att få motparten att tro på vilseledningen. Det kan också vara så att vilseledningen är irrelevant för motståndaren, på så sätt att den inte leder till ett strategibyte, även om motparten tror på den.

Syftet med vilseledning, oavsett om den är direkt eller indirekt, är att motståndaren ska välja en strategi som är bättre för den vilseledande parten än vad som hade varit fallet utan vilseledningen. Här är det viktigt att påpeka att det inte är garanterat att en lyckad vilseledning, som faktiskt genererar ett strategibyte hos motparten, leder till ett bättre utfall. Ett exempel är om den ena parten, Blå, är militärt överlägsen den andra parten, Röd, och Röd skulle ge sig utan strid om detta var känt. Om Blå vilseleder Röd om sin styrka så att Blå verkar svagare än vad som är fallet, så kan detta leda till att Röd väljer att ta strid. I den situationen tar Röd stora förluster och Blå vissa förluster, vilket är sämre för både Röd och Blå.

Slutsatsen av detta är att vilseledning som inte kan kopplas till ett gynnsamt militärt utfall riskerar att hindra, snarare än hjälpa.

2.2 Genomfört arbete

I detta arbete har vi konstruerat en enkel spelteoretisk modell som tillåter utvärdering av olika strategival. Utgångspunkten har varit markstrid där två parter strävar efter tre saker:

(1) att tillfoga motståndaren förluster, (2) att begränsa sina egna förluster och (3) att ta kontroll över geografiska områden.

Modellen tar följande parametrar som input:

- Enheter på Röd och Blå sida, inklusive deras typ[3] och status,[4]
- En uppsättning områden, samt Röds och Blås värderingar av områdena,
- Röd och Blå sidors relativa prioriteringar mellan kontroll över områden, begränsning av egna förluster och maximering av motståndarens förluster.

Trots att avsikten från början var att genomföra en simulering eller demonstration i flera tidssteg är detta något som inte har hunnit implementeras i mjukvara i det operativa perspektivet. Istället är modellen för närvarande ett icke-konstantsummespel på s.k. *strategisk form*, där båda spelare väljer sina strategier, en gång för alla, utan att känna till motståndarens val. En mer realistisk modellering vore att analysera spelet på s.k. *extensiv form*, där det finns en tidsordning mellan de delbeslut som bygger upp en strategi för hela spelförloppet, samt att modellera inverkan av att spelarna får nya uppgifter under spelets förlopp.

För att göra det enkelt att analysera olika variationer av spel behövdes automatisk generering av dels *strategier*, dels *utfallsvärden* (eller *payoffer*). Utöver detta behövdes också generering av *lösningar*, d.v.s. identifiering av *rimliga* eller *rationella* strategier i spelen. Dessa tre frågor behandlas i de följande avsnitten. Därefter diskuteras frågan om variation av spel och identifiering av möjliga vilseledningsåtgärder.

2.2.1 Generering av strategier

Spelmodellen utgår, som nämndes ovan, ifrån en uppsättning *strategiska områden* (geografiska platser) som (i) har värde för spelarna, (ii) kan kontrolleras av spelarna och (iii) där spelarna kan mötas för strid. Precis hur detta med strid, kontroll och värde fungerar beskrivs i avsnittet nedan om utfallsvärden. Det som är centralt för strategigenereringen i modellen är att varje strategi i spelet är en fördelning av *specifika enheter* till *specifika strategiska områden*.

Exempel: Om det finns två strategiska områden, A och B, och Blå sida har enheten *Blå 1* tillgänglig, då är ”Blå 1 till område A” och ”Blå 1 till område B” två olika strategier.

En möjlig strategi är också att inte sända ut några enheter, vilket vi kan kalla *nollstrategin*.

Mängden strategier ökar snabbt med mängden områden och enheter som analyseras och ges av:

$$1 + \sum_{i=1}^{k} \left\{ \binom{k}{i} \sum_{j=i}^{f_{max}} \binom{f_{max}}{j} i!\, S(j,i) \right\} \qquad (1)$$

Den initiala ettan svarar mot nollstrategin, att inte flytta någon enhet till något strategiskt område. Varje ytterligare strategi kan sägas bestå av ett antal delbeslut avseende parametrar i formeln:

- Hur många av de *k* strategiska områdena ska vi sända enheter till? Svaret ges av parametern *i*,

[3] T.ex. mekaniserad infanteribataljon eller stridsvagnsbataljon. Typen bestämmer vilket nominellt styrkevärde (*force value*) enheten har i modellen, och styrkevärden bestämmer i sin tur utfallet när två enheter möts i strid.

[4] En variabel som går från 0 till 1 och reflekterar stridsvärde. När en enhet tar förluster, tröttas ut eller gör av med resurser minskar statusvärdet. Tillsammans med enhetens nominella styrkevärde bestämmer statusen vilket faktiskt styrkevärde den har.

- För varje val av *i* stycken områden finns det $\binom{k}{i}$ kombinationer av punkter, och varje strategi är kopplad till en specifik sådan punktuppsättning,
- Hur många enheter ska vi sända till de *i* valda områdena i en given punktuppsättning? Svaret ges av parametern *j* och måste minst vara *i* (en enhet per område) och kan som mest vara f_{max}, vilket är antalet enheter som spelaren har tillgängligt,
- För varje val av *j* enheter finns det $\binom{f_{max}}{j}$ kombinationer av enheter, och varje strategi är kopplad till en specifik enhetsuppsättning,
- Slutligen kan varje specifik enhetsuppsättning av *j* enheter fördelas (partitioneras) över *i* områden på *S(j, i)* sätt, där *S* är det s.k. *Stirlingtalet av det andra slaget*, och det finns *i!* antal sätt på vilka partionerna med enheter kan fördelas till specifika områden inom den aktuella områdesuppsättningen.

Den MATLAB-kod som har skrivits inom projektet tar en uppsättning enheter och strategiska områden och genererar utifrån detta alla möjliga strategier. Koden tilldelar också utfallsvärden till strategi-kombinationer i två – en för Röd och en för Blå – *spelmatriser*, något som beskrivs i nästa avsnitt.

2.2.2 Generering av utfallsvärden

Varje kombination av en Röd och en Blå strategi innebär en fördelning av enheter över de strategiska områdena. När en strategikombination medför att enheter från de två sidorna befinner sig vid samma område antas de genomföra strid. Utfallet av denna strid skattas då med hjälp av en modell kallad *Force Ratio Calculator*, vilken ger procentuella förluster för de båda sidorna utifrån deras styrkeförhållanden. När de eventuella strider som förekommer har genomförts tilldelas kontroll över strategiska områden till den sida som är minst 3^5 ggr. starkare än motståndaren vid ett område. Enheter som befinner sig vid ett område utan närvarande motståndare tar automatiskt kontroll över området.

Efter dessa beräkningar tilldelas strategikombinationen ett poängvärde mellan 0 och 100 för de respektive spelarna. Poängvärdet räknas fram utifrån egna förluster, motståndarens förluster och kontroll av områden på följande sätt:

Egna förluster. Uteblivna egna förluster ger 100 poäng, alla egna enheter utplånade ger 0 poäng och däremellan är poängsumman omvänt proportionell mot de procentuella förlusterna (i styrkevärde). Sålunda ger 25%-iga egna förluster 75 poäng.

Motståndarens förluster. Motståndarens förluster ger en poäng per procentenhet förlorad, så alla motståndarens enheter utplånade ger 100 poäng och uteblivna förluster på motståndarsidan ger 0 poäng.

Kontroll av områden. För varje spelare fördelas 100 poäng över spelets strategiska områden, med möjlighet att ge vissa områden 0 poäng. För varje kontrollerat område tilldelas poängvärdet av den till den kontrollerande spelaren. Att vara helt utan kontrollerade områden innebär sålunda 0 poäng och kontroll över alla (värderade) områden ger 100 poäng.

Attitydviktning. Varje delsumma på 0–100 poäng enligt ovan tilldelas en vikt mellan 0 och 1, där vikterna summerar till 1. De tre viktade poängtalen summeras sedan till utfallsvärdet. Värdet är alltså en konvex kombination av de tre poängvärdena och varierar mellan 0 och 100. Viktningen kan t.ex. förstås som ett uttryck för mer offensiva eller defensiva förhållningssätt och kan fungera som en länk mellan den avgränsade stridssituationen och en större strategisk kontext.

[5] Detta är naturligtvis en i en rad omfattande förenklingar för att åstadkomma en modell att experimentera med.

2.2.3 Generering av lösningar

Med utfallsvärden på plats i spelmatriserna har Lemke-Howsons algoritm [2] använts för att ta fram en Nash-jämvikt[6]. Jämviktslösningen tilldelar sannolikheter till varje Röd och Blå strategi.

För demonstrationssyfte har vi ansett att det räcker med att ta fram *en* jämvikt per spel, men algoritmen kan hitta flera i den mån sådana finns. Den är dock inte garanterad att hitta *alla* jämvikter, utan då krävs alternativa algoritmer, såsom Support Enumeration eller Vertex Enumeration (se [3]). Såväl Support Enumeration och Vertex Enumeration, som bruk av Lemke-Howson [2] för att hitta flera jämvikter är beräkningsmässigt krävande.

2.2.4 Variation av spel och identifiering av vilseledningsåtgärder

Det spel som representerar Blå sidas bästa bedömning av läget, i frånvaro av vilseledningsåtgärder, kan vi kalla *utgångssituationen*. Vidare kan vi kalla de jämvikter som finns i utgångssituationen för *utgångsjämvikterna*. I den förenklade metod som vi har använt i detta projekt har endast en av dessa använts, och den kallar vi helt enkelt *utgångsjämvikten*. Det förväntade utfall som Blå har vid utgångsjämvikten kallar vi den *förväntade utgångsnyttan*.

Följande procedur har använts för att hitta vilseledningsåtgärder från nya spel där Röd spelar en mindre fördelaktig strategi än den i utgångsjämvikten:

1. Ta fram en mängd olika uppsättningar modellparametrar – kombinationer av sådant som Blå sidas tillgängliga enheter, Blå värdering av olika strategiska områden eller Blå sidas attitydviktning – och konstruera de spelmatriser som svarar mot dessa (osanna) parametrar. Låt oss kalla detta *variationsmängden*[7],
2. För varje spel i variationsmängden, ta fram deras jämviktslösningar,
3. För varje Röd jämviktsstrategi i variationsmängden, återför den till utgångssituationen och kontrollera vad skillnaden blir i förväntat värde för Blå. Kalla denna skillnad från den förväntade utgångsnyttan för den *förväntade variationsnyttan*. Blå förutsätts här fortsätta spela strategin från sin utgångsjämvikt, men det finns förstås andra tillvägagångssätt som kan vara aktuella. Exempelvis kan Blå vilja optimera sitt strategival utifrån Röds förväntade nya strategi, vilket dock kan visa sig problematiskt om vilseledningen misslyckas och Röd spelar i enlighet med utgångsjämvikten,
4. Ordna spelen i variationsmängden från högst till lägst förväntad variationsnytta, samt eliminera de spel som har negativ förväntad variationsnytta,
5. Vilseledningsåtgärder för varje spel blir de parametervärden som ger upphov till just det spelet (mål för indirekta vilseledningsåtgärder), samt de Blå jämviktsstrategier som hör till spelet (mål för direkta vilseledningsåtgärder). Den ordnade (i enlighet med punkt 4) listan med vilseledningsåtgärder sänds vidare med en order att genomföra det första möjliga paketet med vilseledningsåtgärder på den.

2.3 Slutsatser och frågor inför vidare arbete

I den utsträckning som den utvecklade modellen och dess lösningskoncept har tillämpbarhet i faktiska situationer så visar den hur indirekta vilseledningsåtgärder kan få en motståndare att välja en, för den vilseledande parten, mer fördelaktig strategi. Det är också uppenbart att

[6] En allmänt tillgänglig modul (skriven av Richard M. Katzwer, [Online] Available: http://www.princeton.edu/~rkatzwer (december 2015) till MATLAB har använts i beräkningarna.

[7] I den nuvarande implementationen har variationsmängden konstruerats manuellt, så att 100 variationer (med avseende på värdering av strategiska områden och attitydviktning för blå) av utgångsspelet har analyserats.

detta är möjligt med direkta vilseledningsåtgärder. I båda fallen kan dock vilseledningsåtgärderna försvåras om de förändringar från utgångsläget som de syftar till att projicera – antingen i synbara spelparametrar eller synbart vald strategi – förfaller alltför orimliga, och därmed också osannolika[8]. Att studera frågan om rimlighet, och hur *orimliga* åtgärder som kan lyckas förefaller vara ett viktigt område för vidareutveckling. Även om det genomförda, och något explorativa, arbetet är av förhållandevis blygsam omfattning har det varit mycket fruktbart just i termer av att identifiera möjlig vidareutveckling av systematisk framtagning av vilseledningsåtgärder.

Bland dessa möjligheter finner man följande:

- Modellering av spel på extensiv form i flera steg, med inkluderad modellering av observation av motståndarens handlingar och bedömd framgång för vilseledningen samt frågor om privat information i spelet (jmf. exempelvis attitydviktningen ovan),
- Explicit modellering av vilseledningsåtgärder som alternativ i spelmodellen, såväl sådana som kräver telekrigsresurser som andra utifrån ett *bibliotek* av åtgärder (egen falsksignalering, skenmål, förflyttningar, kamouflage, bekämpning av särskilda resurser o.s.v.),
- Utvärdering av huruvida regelstyrd beskärning av strategirymden, t.ex. där (på olika sätt) ekvivalenta strategier slås samman innan beräkning av lösningar, skapar beräkningsmässiga besparingar,
- Samarbete med militär expertis för att få ökad realism i utfallsvärdering, däri inkluderat frågor om väder, mörker och betydelsen av tid för förberedelser av anfall och försvar, samt överraskning,
- Inkluderande av geografiska data i generering av strategier, t.ex. konsekvenser av att ta en viss väg till en given punkt, att hålla olika hastighet o.s.v. samt beaktande av möjligheten att vilseleda om terrängens egenskaper,
- Utvärdering i krigsspel, där utfall av den i modellen föreslagna vilseledningen testas mot mänskliga motståndare,
- Komparativa studier där militär expertis får ta fram vilseledningsåtgärder med och utan datorstöd, och där sedan dessa testas i krigsspel,
- Modellering av vilseledning till sjöss och i luften,
- Modellering av vilseledning i situationer med andra syften än att ta terräng och tillfoga motståndaren förluster, t.ex. fördröjningsstrid,
- Utveckling av en strategi för generering och genomsökning av variationsmängden (de spelsituationer som avviker från den egna bästa bedömningen av situationen),
- Frågor om att ta hänsyn till möjligheten att motståndaren också vilseleder aktivt,
- Analys med andra lösningskoncept än enskilda Nash-jämvikter för att hitta de mest troliga spelutvecklingarna, t.ex. sökande efter paretooptimala jämvikter, delspelsperfekta jämvikter (subgame perfect) eller användning av empiriskt stödda tumregler för situationer där jämviktsspel är osannolikt av någon anledning.

I det vidare arbete kan det också vara användbart att göra bruk av mjukvarupaketet Gambit och dess Python-interface, då Gambit har fler spelteoretiska moduler implementerade än vad som finns allmänt tillgängligt till MATLAB.

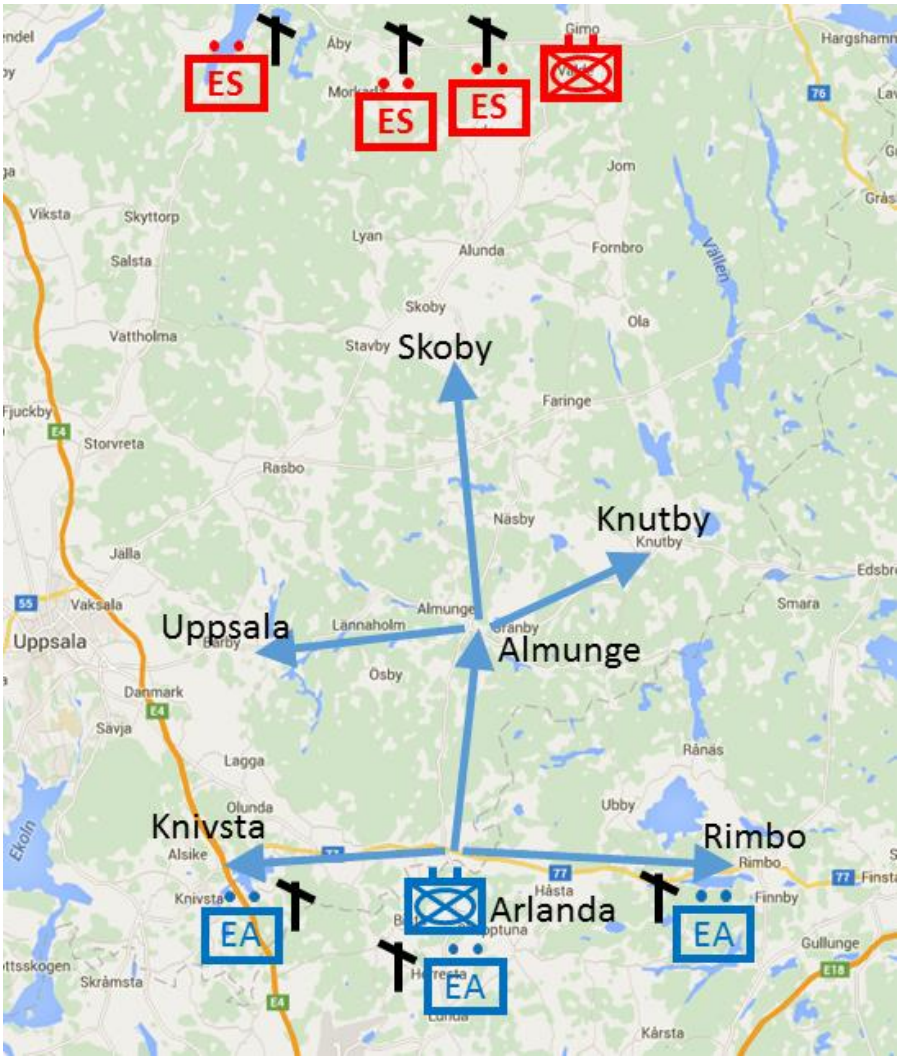
[8] För aktiva vilseledningsåtgärder kan en väg vara att, i första hand, projicera att man ska spela någon strategi som tillhör det s.k. *stödet* för någon jämviktsstrategi. Alla sådana har en initial rimlighet, och det kan göra skillnad precis vilken strategi inom sina respektive stöd som spelarna väljer.

3 Informationsperspektivet

Informationsperspektivet har framför allt behandlat bearbetningen av osäker information (Blås lägesbild och vilseledande information) och den konceptuella integrationen av de olika perspektiven och deras mjukvarumoduler (uppdelningen i perspektiv och mjukvarumoduler finns beskriven i avsnitt 1.2).

3.1 Grundläggande idé

Den grundläggande idén som, i en första ansats, förenar de olika perspektiven är den om Röds lägesbild. Som gemensamt språk för perspektiven har vi Blås handlingsalternativ i en viss given situation, $B = \{b_1, b_2, \ldots, b_n\}$ och Röds $R = \{r_1, r_2, \ldots, r_n\}$. Här beskriver B en mängd alternativa taktiska handlingsalternativ för en Blå bataljon och illustreras i Figur 2 (bilden är en identisk upprepning av Figur 1 i avsnitt 1.3).



Figur 2. Blås handlingsalternativ *B* består av de sju strategiska destinationerna Arlanda, Knivsta, Rimbo, Almunge, Uppsala, Skoby, och Knutby.

Vi inför även en symbol L_B, som representerar hela Blås lägesbild (dvs. inklusive positioner för Blås resurser och uppskattade positioner för Röds resurser, framför allt dennes sensorer).

Vi låter L_R, Röds lägesbild, endast bestå av det vi vill vilseleda om dvs. Blås alternativ *B*. Värt att nämnas kan vara att även om *B* är vår uppfattning/gissning om Röds representation av vad Blå kan tänkas ha för alternativ, så får det ändå antas vara ganska nära sanningen, givet Röds och Blås gemensamma kunskap om terräng och militära resurser. Eftersom det är osannolikt att Blå har säker och detaljerad kunskap om Röds ledningssystem så är det inte meningsfullt att försöka beskriva Röds lägesbild i alltför mycket detalj. Det blir ändå inte rätt. Istället kan man försöka efterlikna det som är rimligt på en mer allmän nivå vilket även ger en del friheter (exempelvis att man kan försöka anpassa hantering och representation till Blås syften).

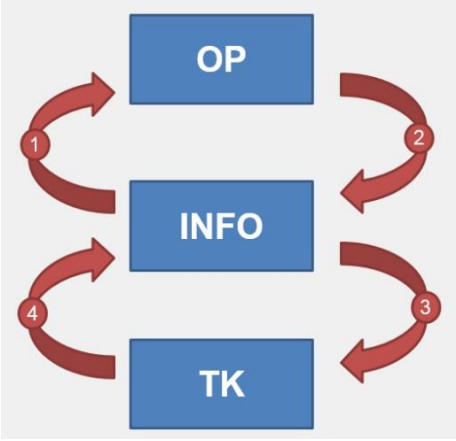
Vi tänker oss vidare att Röd har ett osäkerhetsmått över *B* som i praktiken rangordnar olika alternativ i *B* givet Röds uppskattade kunskap om läget; låt oss kalla den ursprungliga uppfattningen om L_R för m_1. Vi väljer att i INFO-perspektivet primärt behandla osäkerheten som en så kallad massfunktion inom Dempster-Shaferteori [4]. Massfunktionen är en generalisering av sannolikhetsfunktionen, ett släktskap som gör att man kan omvandla det ena till det andra och vice versa[9]. Det utnyttjar vi i kommunikationen mellan mjukvarumodulerna. Medan INFO-modulen hanterar L_R som en massfunktion, med de verktyg som därmed står till buds, så sker informationsutbytet med OP- och TK-modulerna med sannolikhetsfunktioner (vi betecknar motsvarigheten till *m* med symbolen *p*) då dessa är mer lätthanterliga för OP- och TK-perspektiven.

Genom vilseledningsinsatser hos TK och CYB manipuleras m_1 till m_1', $m_1 \oplus m_2 = m_1'$ ($\oplus$-operatorn här är den så kallade ”Dempsters regel”). Matematiskt representerar vi denna vilseledning som informationen m_2. Syftet med att introducera Dempster-Shaferteori inom INFO-modulen är för att kunna beräkna m_1', vilket inte låter sig göras inom sannolikhetsteori.

Interaktionen mellan arbetspaketen syftar nu till att 1) se till att m_1 förmedlas och uppdateras korrekt; 2) att m_1', den önskade lägesbilden hos Röd, uttrycks korrekt baserat på OP:s uppdragsprioriteringar; och slutligen 3) att de tillgängliga vilseledningsoperationerna påverkan på m_1 kan uttryckas i termer av samma osäkerhetsmått.

3.2 Process

Vår process för att samordna de olika perspektivens mjukvarumoduler illustreras i Figur 3.



Figur 3. Processförslag med fyra steg

Notera att cyberperspektivet inte ingår i den aktuella lösningen på grund av de skäl som angavs i avsnitt 1.2. De fyra stegen förklaras nedan:

[9] En massfunktion omvandlas till en sannolikhetsfunktion med hjälp av den så kallade ”pignistic” transformation [5], och å andra sidan kan en massfunktion skapas direkt som ett specialfall av en sannolikhetsfunktion.

1. INFO förser OP med aktuell uppskattad Röd lägesbild över Blå, dvs. p_1 (sannolikhetsversionen av m_1), samt Blås lägesbild L_B,
2. OP svarar INFO med behov uttryckt som p_1' och som INFO översätter till m_1'. Det här steget behandlas i kapitel 2,
3. INFO beräknar önskad effekt av lyckad vilseledningsoperation, dvs. m_2, och vidarebefordrar till TK efter omvandling till p_2. Rent tekniskt beräknas m_2 som en invers av Dempsters regel (vilket fångar) som vi kan beteckna med symbolen ”$\ominus$”, dvs. $m_2 = m_1 \ominus m_1'$.
4. TK undersöker vilken möjlig vilseledningsoperation som bäst kan möta önskemålet från OP, och implementerar det mest lämpliga, m_2' som även återsänds till INFO. Det här steget behandlas i kapitel 4. Observera att TK även behöver tillgång till L_B för att beräkna m_2' (exempelvis information om var Röds sensorer är placerade).

Observera att vi antar att TK alltid kan ge ett (någorlunda) tillfredsställande svar på förfrågan om m_2. Om TK inte har något bra svar på m_2 eller flera möjliga likvärdiga alternativ kan diskussion med övriga moduler krävas. Eventuell kan det också vara fördelaktigt att OP-perspektivet i förväg förser TK-perspektivet med information med avgränsningar av vilka typer av vilseledningsinsatser som kan vara av intresse.

I kapitel 6 presenterar vi en exempelkörning av vårt vilseledningsprogram på scenariot i Figur 2.

4 Telekrigperspektivet

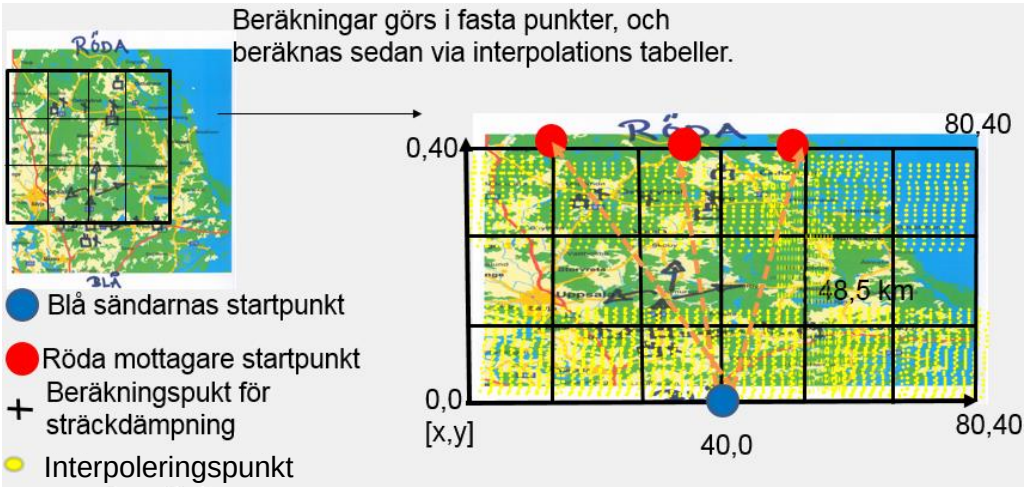
Vilseledning ur telekrigperspektivet (TK) är här definierad som: *Blå störsändarna flyttats till en position där deras sändområde hörs av en Röd mottagare.*

Handlingsalternativen för Blå sändare, vars intentioner är att *vilseleda*, är:

1. Stanna på befintlig position,
2. Flytta mot Knivsta,
3. Flytta mot Rimbo,
4. Flytta mot Almunge,
5. Flytta mot Uppsala,
6. Flytta mot Skoby,
7. Flytta mot Knutby.

4.1 Lägesbild

Scenariot har implementerats i MATLAB. TK hanterar en önskad lägesbild och har tillgång till tre störsändare för att uppnå önskad vilseledningsresultat. Dessa har en fast uteffekt på 50W och en antennhöjd på två meter. Baserat på sändarnas positioner skapas ett *effektnät*, med hjälp av beräkningar gjorda i Deterministisk vågutbredningsmodell (Detvag90), vilket sedan interpoleras och transformeras till en viktmatris. Vikten baseras på antalet mottagare som nås. Processen illustreras i Figur 4.



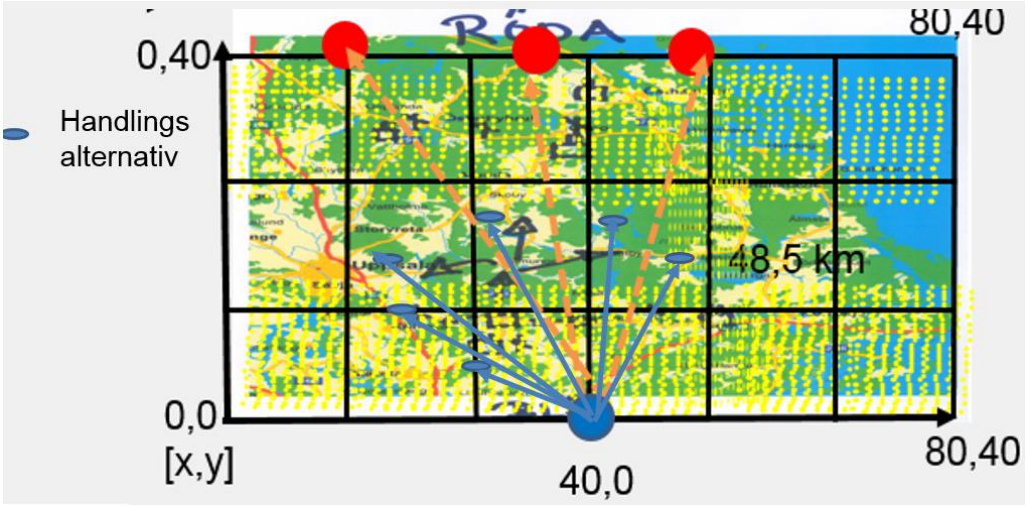
Figur 4. Bilden visar hur nätet med beräknade sträckdämpningar interpoleras och ger en viktmatris.

4.1.1 Detvag90

Detvag90 är baserad på *Geometrical Theory of Diffraction*, ett FOI-utvecklat program för avancerade vågutbredningsberäkningar som inkluderar terrängdata såsom; höjdinformation och information om marktyp (skog, sjö, åkermark, bebyggelse, etc.). Detta möjliggör beräkning av inkommande effekt hos en mottagare. Den inkommande effekten beräknas utifrån position av mottagare och sändare, antennhöjd samt uteffekt på sändaren. För ytterligare beskrivning av Detvag90 se [6].

4.1.2 Optimeringsalgoritm för m_2'

Nästa steg är att hitta de möjliga sändarpositionerna, detta görs genom att ta bäring mot det givna handlingsalternativet. Detta illustreras i Figur 5.



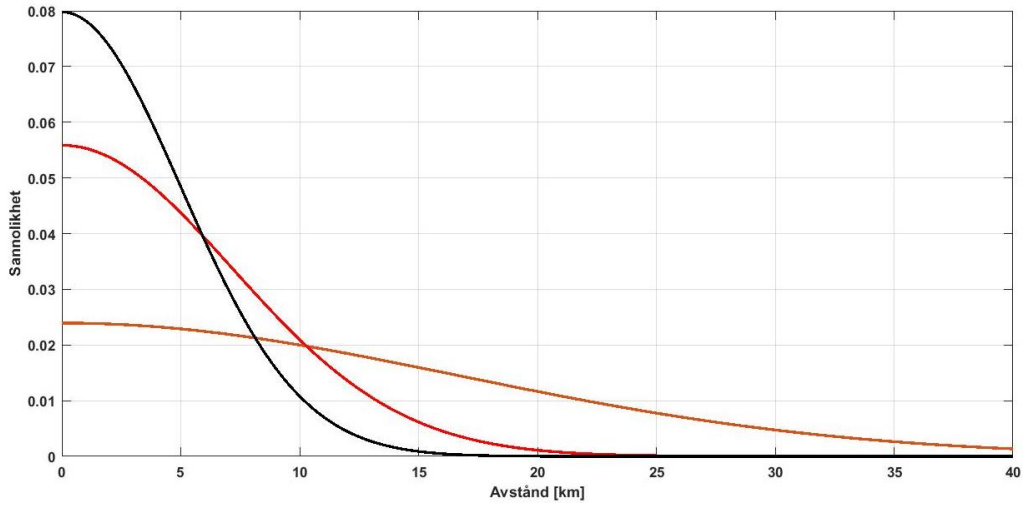
Figur 5. Bilden illustrerar hur det nya m_2' generas.

I optimeringsalgoritm beräknas alla möjliga m_2', den totala kombinationen: $m_2' = \{m_2^{1\prime}, m_2^{2\prime}, m_2^{3\prime}\}$ anges sedan som $m_2' = 1 - (1 - m_2^{1\prime})(1 - m_2^{2\prime})\,(1 - m_2^{3\prime})$, där $m_2^{1-3\prime}$ representerar den enskilda sändarens bidrag. En begränsning i sökningen för möjliga m_2' är satt till tre riktningar.

Här representeras m_2 och m_2' som sjudimensionella vektorer där α anger den euklidiska vinkeln mellan m_2 och m_2', α ger då ett mått på *likhet*. Minimering av α, dvs. skillnaden mellan m_2 och m_2', ger *bästa* $m^{2'}$, α anges i ekvation 1.

$$\alpha = arccos \frac{m_2 \cdot m_2'}{|m_2||m_2'|}. \qquad (1)$$

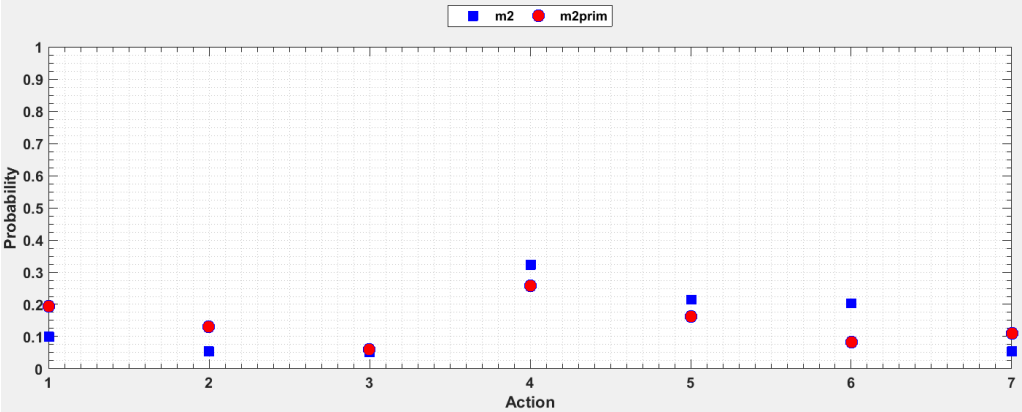
Figur 6 visar hur sannolikheten för en given position avtar beroende på antalet mottagare som nås.



Figur 6. Bilden visar hur sannolikheten för en position på avstånd 0–40 km avtar beroende på hur många mottagare som nås.

4.1.3 Resultat

Här visas ett resultat i Figur 7.



Figur 7. Bilden illustrerar resultat där det givna m_2 representeras av Blå fyrkanter och m_2' av Röda prickar.

$$m_2 = [0{,}0981\ 0{,}0541\ 0{,}0506\ 0{,}3233\ 0{,}2156\ 0{,}2045\ 0{,}0539]$$

$$m_2' = [0{,}1935\ 0{,}1308\ 0{,}0613\ 0{,}2582\ 0{,}1631\ 0{,}0837\ 0{,}1094].$$

All data som används är fiktiva eller hämtade från öppna källor. Syftet är att visa metodiken.

4.1.4 Rekommendationer

Kvalitén på det givna m_2' kan förbättras genom:

- utveckla kartdatabasen till detvag90, genom att införa stöd för klimat,
  detta ger bättre skattningar av osäkerheter i temperatur, nederbörd, …, etc.
- förbättra beräkningsmodeller till detvag90.
- förbättra optimeringsalgoritmen för sökning av m_2'.
- parametersätt sändarnas uteffekt och sändningstid.

För utveckling av modellen rekommenderas även att stokastiska indata används som variabler till modellen, position och antennegenskaper exempelvis kan ges via en likformig fördelning, se följande exempel:

Låt X vara indata till objektets startvärde, $X_{start\ värde} \sim Lik(A, B)$, ges som: $X_{start\ värde} = A + (A - B) * \text{random}[0,\ 1]$.

5 Cyberperspektivet

Såväl Ryssland, USA och Kina ser vilseledning som en naturlig del av informationsoperationer, även i fredstid. I USA används termen *MILDEC*; i Ryssland används termen *maskirovka*. Cyberangrepp ses som en del av detta, och ökad användning av IT i militära sammanhang gör att cyberangrepp blir ett allt mer potent verktyg för att utföra vilseledning [7].

Den publikt tillgängliga forskningen inom cybersäkerhet fokusar främst på försvar av system och att försvåra för angripare. Det finns bland annat konkreta förslag på hur domänspecifika C2-system bör designas för att göra vilseledning genom manipulation av sensordata svårare. Ett exempel är [8], som fokuserar på tillståndsskattningar i drifteldningssystem för elkraft. Vilseledning används också ibland som ett försvar mot angripare. Det finns bland annat ett stort antal förslag på så kallat *moving target defence*, där egna IT-system förändras på oförutsägbara sätt så att angrepp mot dem [9]. Det finns även ett antal förslag som på hur fiktiva system (så kallade *honeypots*) och vilseledande systembeteende ska användas för att få angripare att avslöja sina intentioner, ödsla tid på irrelevanta aktiviteter, serveras felaktig information från system och så vidare [10–14].

Tekniker för cyberangrepp inte är något publika forskningen ägnas åt direkt. Trots detta finns gott om kunskap kopplat till detta – det är ju nämligen just detta som forskningen syftar till att försvåra. I detta kapitel ges först en översikt över vilka vilseledningsmöjligheter som cyberangrepp ger i scenariot som denna rapport använder. Därefter bedöms vilka förutsättningar som krävs för att lyckas med olika cyberoperationer. Sist ges ett exempel på en cyber-relaterad vilseledningsoperation som skulle kunna användas i scenariot som denna rapport fokuserar på.

5.1 Möjligheter och alternativ

Vad som är möjligt att åstadkomma med cyberoperationer avgörs av hur Röds cybermiljö är beskaffad. I USA:s doktrin delas cybermiljöer in i det fysiska (t.ex. fiberkablar och datorer), det logiska (t.ex. mjukvara och dess konfiguration) och de persona (t.ex. användarkonton) som verkar i cybermiljön [15]. Detaljer kopplat till dessa delar av cybermiljön kan vara helt avgörande för möjligheten att lyckas med en cyberoperation [16]. Att en nätverkssladd kopplats in fel kan till exempel innebära ett obevakat gränssnitt och möjligheter att flytta data mellan datornätverk; användning av en viss biblioteksfunktion i ett program kan innebära att en buffertöverskidningssårbarhet kan utnyttjas trots att operativsystemet har skydd mot det; en användares misstag eller goda vilja kan ge tillgång till användarkonton med resurser som förenklar angrepp betydligt. I denna rapport antas Röds cybermiljö vara konstruerad som den typiskt är i moderna försvarsmakter idag och hypotetiska resonemang förs kring detaljer som dessa och de potentiella cybersäkerhetsbrister som finns i Röds cybermiljö.

I moderna militära cybermiljöer är lägesinformation utspridd i ledningssystem på flera beslutsnivåer. Till exempel i form av taktiska displayer med nuvarande och framtida placering av styrkor, geografiska system för terrängvärdering, databaser med underrättelser, logistiska stödsystem, modeller för att prediktera utfall av sammandrabbningar och kommunikationslänkar som används inom eller mellan nivåer [17]. Det finns flera möjligheter att påverka Röds lägesbild med cyberangrepp mot sådana ledningssystem. Några alternativ är:

- Intrång i stabens ledningssystem via riktade nätfiskemeddelanden (*phishing*) till personal i staben. Till exempel genom att sprida dokument med inbäddad skadlig kod som personalen (förhoppningsvis) för in i ledningssystemen.
- Intrång i stabens ledningssystem via flyttbara lagringsmedium som förs in i systemen. Till exempel genom att smittade USB-stickor flyttas från

internetuppkopplade datorer som används för underrättelseinhämtning från öppna källor till datorer som används för att sammanställa underrättelser.

- Intrång i det stridsledningssystem som används av den taktiska staben för att överblicka egna styrkor. Till exempel genom använda ett bekämpat stridsfordons datorer och från det infiltrera motståndarens stridsledningssystem med hjälp av mjukvarusårbarheter.
- Plantering av vilseledande information i stabens logistiksystem genom att angripa och manipulera civila system som stabens logistiksystem inhämtar data ifrån. Till exempel förändra information om tillgängligt drivmedel i en leverantörs logistiksystem genom att utnyttja sårbarheter i leverantörens cybermiljö.
- Intrång militärfordons ledningsstödssystem via sårbarheter planterade i systemplattformen under utvecklingsprocessen. Till exempel för att kunna skicka falska radiomeddelanden till militärfordonen på ett sätt som ser autentiskt ut utan att känna till krypteringsnyckeln.
- Intrång i kommunikationssystem med dåligt skyddade förbindelser som används av staben. Till exempel genom att angripa taktiska satellitlänkar via underhållspersonalens datorer eller leverantörers driftövervakning.

Alla dessa intrång skulle kunna användas för att 1) *extrahera* information om Röds lägesinformation, 2) *manipulera* Röds lägesinformation eller 3) *försämra* Röds lägesinformation. Detta kan göras för att förändra lägesinformation kopplat till Röds styrkor eller lägesinformation kopplat till Blås styrkor. Det senare bedöms både enklare mer effektivt för att uppnå den vilseledningseffekt som eftersöks i scenariot.

Utöver angrepp mot som syftar till att påverka Röds ledningssystem kan angrepp utföras mot civila system som påverkar Röds agerande indirekt. Till exempel kan angrepp utföras mot Röds politiska ledare eller mot nyhetskällor Röd har tillit till, för att med hjälp av dessa sprida felaktig information som vilseleder Röds taktiska stab eller gör den taktiska staben mer avvaktande. I scenariot som används som utgångspunkt i denna rapport bedöms dock sådana indirekta vilseledningar som otillräckliga för att påverka Röd på det sätt som önskas.

5.2 Nödvändig tillgångar och förutsättningar

Som nämndes ovan är detaljer kopplat till Röds cybermiljö direkt avgörande för vilka cyberangrepp Blå har möjlighet att utföra. Underrättelser är därför helt nödvändiga för att lyckas med ett cyberangrepp. De underrättelser som krävs också på en detaljnivå som sällan behövs för andra typer av militära operationer [16]. Till exempel kan ett versionsnummer eller en konfigurationsparameter vara avgörande för om ett angrepp ger önskat resultat, eller inget resultat alls. Utöver sådana detaljerade underrättelser kräver en cyberoperation någon form av initial tillgång till den cybermiljö som ska angripas. Sådan tillgång kan till exempel vara möjlighet att kommunicera med en internetansluten server i cybermiljön eller att vissa användarkonton redan har komprometterats i cybermiljön. Den tillgång som är säkerställd innan cyberoperationen påverkar naturligtvis vilken effekt som kan åstadkommas inom givna tidsramar.

Både behovet av underrättelser och behovet av att på förhand bereda tillgång till system innebär att cyber-delen av vilseledningsmanöver behöver förberedas i god tid innan den verkställs. Kostnaden för sådan planering och beredning av tillgång kan ses som en funktion av det antal motståndare som planer behöver finnas färdiga för; kostanden är lägre om antalet tänkbara motståndare är få. Nedan förs några mer övergripande resonemang om de tillgångar och förutsättningar som krävs för att Blå ska lyckas med att *extrahera*, *manipulera* eller *försämra* Röds lägesinformation.

Att *extrahera* Röds lägesinformation kräver att data kan föras ut ur Röds IT-system. Detta är i regel är svårt i militära miljöer (där sekretess prioriteras högt), men tekniskt rättfram givet att ett sätt att föra ut data identifierats. Att *manipulera* Röds lägesinformation kräver inte att data kan föras ut ur systemet för att vara genomförbart, men blir betydligt enklare

om tvåvägskommunikation kan upprättas mot det kompromitterade systemet. Utan sådan tvåvägskommunikation behöver Blå på förhand är känna till hur insidan av Röds system är konstruerat på detaljnivå. Till exempel behöver Blå känna till hur fält i databaser är namngivna för att kunna justera deras värden till det önskade. Utan möjlighet till kommunikation med den skadliga koden krävs också att det innan intrånget bestäms hur och när manipulationen av motståndarens lägesbild ska göras. Det kan till exempel bestämmas att alla koordinater som ligger över blått territorium ska justeras i någon riktning när de skrivs ut eller att alla koordinater ska justeras åt någon riktning när ett visst kodord förs in i systemet (t.ex. ett ovanligt ord man tror att man lura motståndaren att föra in i systemet när så behövs). Det tredje alternativet, att *försämra* Röds lägesbild, blir också det enklare om tvåvägskommunikation kan ske och kräver likt manipulation att aktiveringstillfället bestäms på förhand. Men till skillnad från manipulation krävs ingen djup kunskap om hur insidan av Röds system är konstruerat för att lyckas. Till exempel är det förhållandevis enkelt att radera filer på en dator eller göra dem korrupta. Dessutom kan det vara fullt tillräckligt att elakartad kod förs in Röds system för att Röd skall misstro systemen i sådan utsträckning att Röds lägesinformation påverkas. Det vill säga, om Röd upptäcker att ny okänd kod exekverar i ledningssystemet kommer Röd rimligtvis misstro eller helt ignorera den lägesinformation som det innehåller, och därmed har Röds lägesinformation försämrats.

I en militär kontext är det rimligt att anta att Röds egna system är konstruerade så att det är väldigt svårt för Blå att föra ut information ur dem och så gott som omöjligt att upprätta tvåvägskommunikation mot dem som är användbar i ett skarpt läge. Framgång i komplexa cyberangrepp som de ovan förutsätter som nämnts ovan goda underrättelser om hur Röds system är konstruerat och noggranna förberedelser. Även under sådana förutsättningar kommer intrång behöva ske i blindo. Att inte kunna testa sig fram med angrepp innebär inte bara att det är svårt att lyckas med vilseledningsaktionen, utan också att det är svårt för Blå att veta ifall vilseledningsaktionen lyckades när den genomförs. Bedömningar av effekter från cyberoperationer är erkänt svårt [15, 18], bland annat för att effekten är beroende av detaljer i cybermiljön och för att planer omfattas av sekretess som gör forskning och utveckling i testmiljöer icke-trivialt [16]. Dessutom kan Röd, som nämndes i inledningen ovan, aktivt vilseleda Blå så att Blå felaktigt tror att operationen lyckats trots att angreppskoden upptäckts och oskadliggjorts.

För att begränsa problemen med att agera i blindo kan vilseledningsaktioner av enklare och mer förutsägbart slag därför vara att föredra. Vilseledning genom att försämra Röds lägesbild kan därför ses som ett lämpligt val för Blå, även om effekten i form av vilseledning är begränsad. Nedan ges ett tänkbart exempel på sådan vilseledning tillsammans med dess förmodade effekt i det aktuella scenariot.

5.3 Avbrott i kommunikation mellan ledningsnivåer

Den ledningsstab som Röd grupperat på blått territorium utbyter underrättelser och order den högre taktiska ledningsnivån som belägen på rött territorium. Mellan dessa staber kommuniceras lägesinformation, bland annat överförs bilder från Röds spaningssatelliter och övervakningssatelliter. Dessa används av ledningsstaben på blått territorium för att kartlägga och följa Blå styrkor.

Datautbytet sker via en satellitlänk som satts upp mot fast kommunikationsinfrastruktur på rött fastland. Kommunikationen till och från satelliten är väl skyddad med kryptering och därför inte möjlig för Blå att påverka med cyberangrepp. Blå har dock på förhand identifierat vilka anläggningar Röd använder för spaningssatelliter och övervakningssatelliter som täcker blått territorium. Blå har även identifierat ett gränssnitt för underhåll och driftövervakning mellan dessa anläggningar och en av satellitsystemets leverantörer. Hos en av dessa leverantörer har Blå sedan en längre tid skapat flera bakdörrar genom nätfiske mot utvald personal. En av dessa bakdörrar ger privilegier att utföra driftunderhåll på flera av Röds system.

Driftunderhållsprivilegierna gör det inte möjligt att läsa eller dekryptera den data som skickas via satellitlänken. De ger däremot rätt att uppdatera mjukvaror i plattformen som används i alla de radioanläggningar som används av de aktuella satelliterna. Sådana uppdateringar ska enligt avtal utföras först efter ordentliga tester av dem i ett referenssystem och avstämning med systemägaren, men kan rent tekniskt utföras på leverantörens eget bevåg. Denna möjlighet används av Blå för att tillfälligt slå ut satellitlänken genom att skicka ut en kompromitterad systemuppdatering av plattformsmjukvaran.

Det finns flera tänkbara sätt att göra detta på. Blå kan till exempel modifiera koden så att den innehåller buggar som resulterar i fatala minnesfel vid exekvering. Sådana fel skulle kunna leda till att plattformsmjukvaran kraschar varje gång den modifierade koden körs, även efter omstart av maskinen. Som ett resultat av skulle satellitlänken bli oanvändbar fram tills en fungerande mjukvara körs igen. Den beredskap Röd har för systemfel som detta bestämmer hur lång tid detta skulle ta. Att upptäcka att en korrumperad version körs och att återställa till en stabil version på egen hand eller med hjälp leverantören är förhållandevis enkelt. Att förhindra att proceduren med trasig uppdatering upprepar sig kräver dock att leverantören rättigheter identifieras som ett bestående problem och tas bort, vilket inte är en självklar slutsats att dra från en trasig mjukvaruuppdatering. I scenariot antas därför att möjligheten att kommunicera mellan ledningsstaberna försvinner under en timme, återkommer i tio minuter, för att sedan försvinna i ytterligare tjugo minuter innan Blå blivit av med sin möjlighet att påverkar kommunikationen via leverantören.

6 Experiment och slutsatser

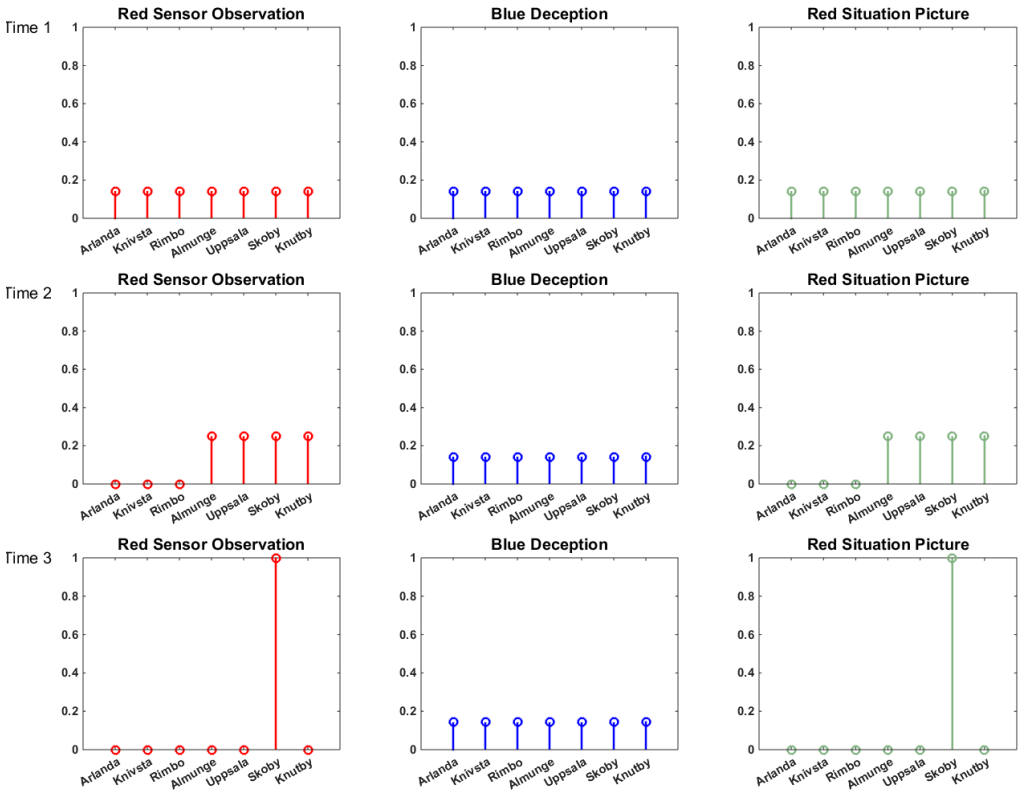
Projektet har uppvisat flera nyttiga resultat och slutsatser. För det första är vilseledning en utmanande aktivitet som berör flera delar av den militära organisationen. I projektet har vi sammanfört kompetenser inom både informationsbehandling, ledning, och hantering av konkreta resurser för vilseledning. Det har lett till både en överföring av ämneskunskap mellan de olika avdelningarna samt ett lösningsförslag för hur de olika delarna kan samverka (baserat på en gemensam osäkerhetsrepresentation för informationsdelning).

Både telekrig- och cyberresurser har förmåga att stödja vilseledning på olika sätt (vilket diskuteras i kapitel 4 respektive kapitel 5), men det visade sig vara utmanande att sammanföra de i samma programslinga bland annat för att de påverkar situationsbilden på olika sätt och en förändrad systemprocess är nödvändig.

Nedan redogör vi för en exempelkörning med scenariot i avsnitt 1.3 och systemprocessen i avsnitt 3.2. Exemplet upprepas tre gånger i tre olika varianter och syftet är att illustrera vilseledningens påverkan på Röds uppdaterade lägesbild.

I Figur 8 visar hur Röd lägesbild skulle se ut utan Blå vilseledning. I Figur 9 visar vi hur Röd lägesbild skulle se ut om Röd endast ser Blås vilseledning och inte verkligheten. Slutligen, i Figur 10 visar vi hur Röds lägesbild ser ut när Röd både uppfattar verkligheten och Blås vilseledning.

Resultatet av den första varianten redovisas i Figur 8. Kolumnerna visar (från vänster till höger) den osäkra informationen från Röds sensorer, Blås vilseledning (som den förväntas uppfattas av Röd), samt slutligen Röds resulterande lägesbild (L_R) baserad på kombinationen av Röds sensorobservation av verkligheten i kombination med Blås vilseledning. Varje rad rör ett tidssteg i simuleringen av scenariot som sträcker sig över tre tidssteg.

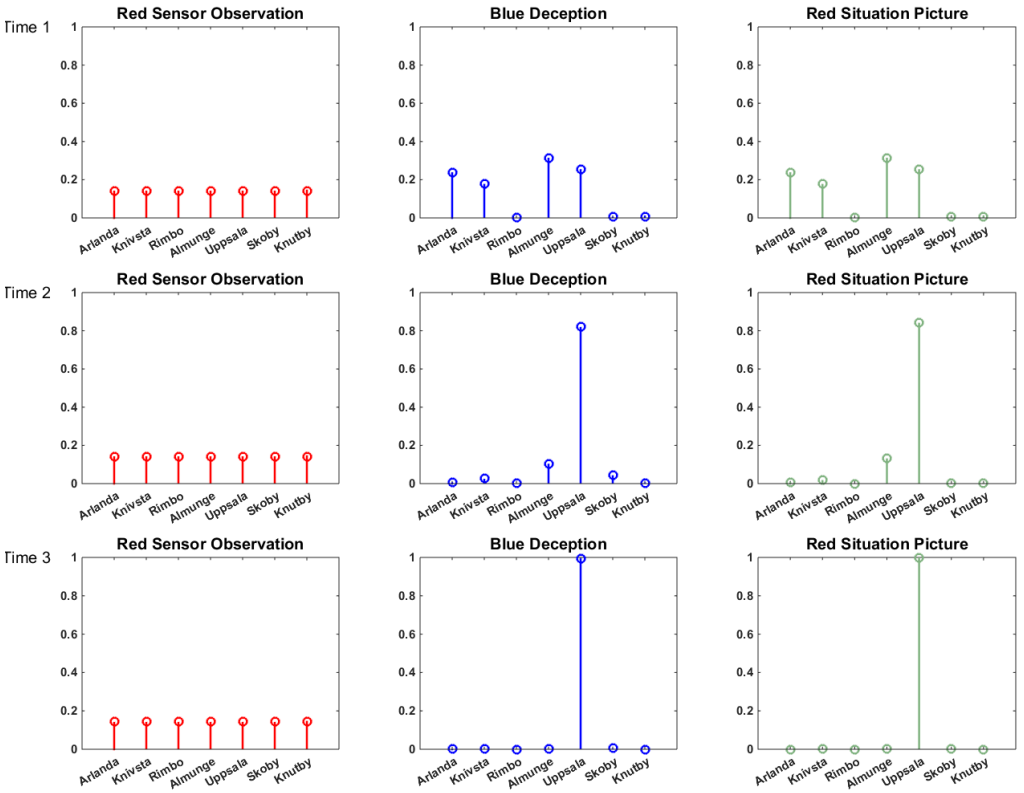


Figur 8. Graferna visar sensor observationer, påverkan från vilseledning samt resulterande lägesbild för Röd i de tre tidsstegen i scenariot. I det här fallet sker ingen vilseledning.

I den första varianten finns endast information från Röds sensorer, ingen vilseledningsinformation. Notera att L_R representerar Röds uppfattning om Blås destination. I det första tidssteget kan Blå fortfarande nå samtliga destinationer och därför låter vi ”Red sensor observation” för det första tidssteget vara helt uniform (icke-informativ), dvs. sensorerna kan inte avslöja något om sluttillståndet. Eftersom ingen vilseledande information tillförs så blir även sluttillståndet för L_R, i tidssteg ett, uniform. I tidssteg två har den Röda styrkan rört sig till Almunge och baserat på en observation av detta av Röd så antas Blås destination troligtvis vara en av Almunge, Uppsala, Skoby, eller Knutby. Eftersom ingen vilseledning tillförs så speglar L_R sensorobservationen. I tidssteg tre har Röd styrka nått Skoby vilket också är destinationen. Detta observeras av Röds sensorer och Röds lägesbild L_R signalerar att Skoby är Blås destination (längs ner till höger i figuren p_{Skoby} = 1).

I det andra exemplet är situationen det omvända, dvs. Röd erhåller inga korrekta sensorobservationer utan enbart den vilseledande informationen. Resultatet visas i Figur 9. I varje tidssteg är ”Red sensor observation” en uniform fördelning (vilket återigen representerar saknad information). Vad som inte syns i figuren är OP:s önskemål om vilseledning och vilseledningsbeställningen till TK, dvs. p_2. I exempelkörningen råkar OP:s önskemål vara att vilseleda om att Blå har Uppsala som slutdestination. Efter INFO:s beräkningar blir även beställningen till TK, dvs. p_2, en sannolikhetsfunktion som lägger har all sannolikhet på alternativet Uppsala.

I den första raden kan vi se TK:s bästa resultat (och därmed implementerade vilseledning) för tidssteg ett. Resultatet har visserligen Uppsala som en stark kandidat, men flera andra är starka och en, Almunge, är till och med starkare. Anledningen till detta resultat är att TK:s sändares aktuella positioner som påverkar resultatet. Sändarna kan dock flyttas runt, vilket också sker mellan tidsstegen.



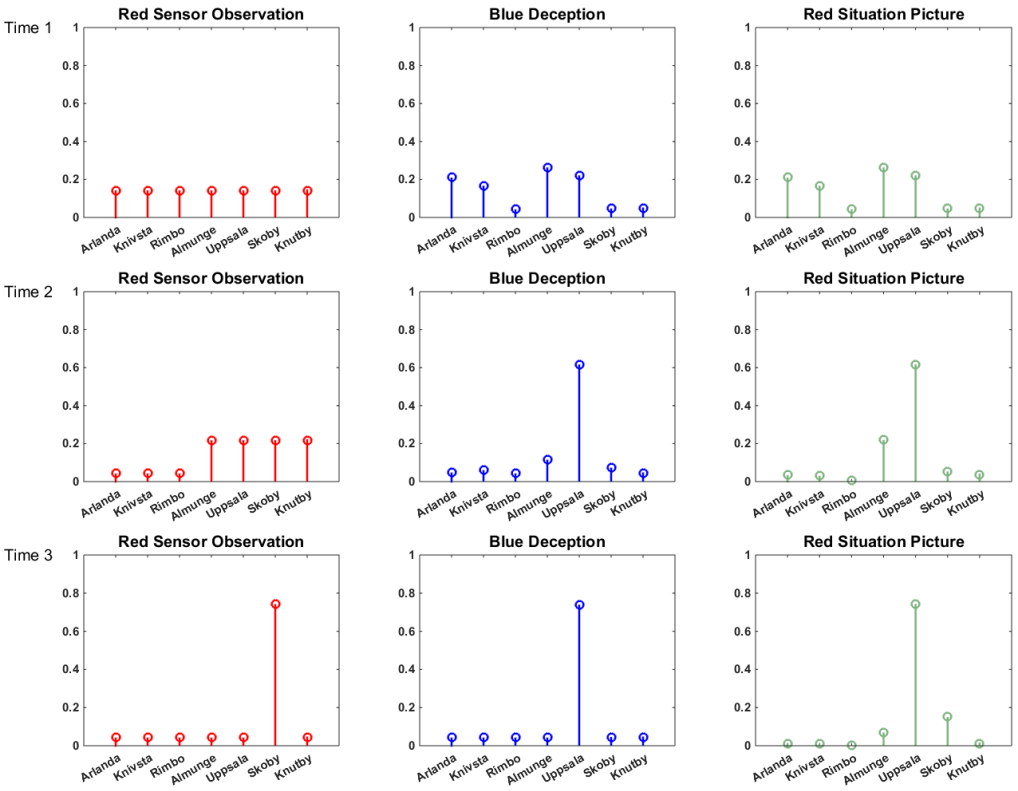
Figur 9. I det här fallet erhålls inga korrekta sensorobservationer utan Röds lägesbild uppdateras endast med Blås utsända vilseledande signaler.

I tidssteg två, då TK återigen får en beställning om att vilseleda om Uppsala, har sändarna hunnit hittat bättre positioner och lyckas betydligt bättre med sin vilseledning. Det avspeglar

sig också tydligt i Röds uppdaterade lägesbild där Almunge visserligen fortfarande är ett tänkbart alternativ men där Uppsala nu är starkast. I det tredje och sista steget har sändarna nått så lämpliga positioner är de entydigt kan ge sken av att Blå försöker nå Uppsala.

I den tredje varianten (Figur 10) har vi både korrekta sensorobservationer (vilka ju enskilt leder till att Blås slutdestination Skoby röjs) och vilseledande information. Även i detta fall väljer OP konsekvent att vilseleda om rörelse mot Uppsala. I det första tidssteget bidrar inte sensorinformation till lägesbilden utan endast vilseledningen påverkar (precis som i den andra varianten). I det andra tidssteget bidrar både sensorobservationer och vilseledning. Vilseledningen är dock starkare i sin utsaga och får större inverkan på L_R. I det sista tidssteget är sensorobservationen tydlig, men det är även vilseledningen och tillsammans med tidigare L_R så blir resultatet att den vilseledda destinationen troligast.

Detta exempel är det mest realistiska med både sensorobservationer och vilseledning. Vilseledningen är här framgångsrik genom att den dels pågår under en viss tid och genom att den vilseledande informationen är (avsiktligt) mer tydlig än den övriga sensorinformationen som Röd har tillgång till.



Figur 10. I det här fallet förekommer både korrekta sensorobservationer och vilseledning.

Exemplet visar att väl avvägd vilseledning som upprepas över tiden kan framgångsrikt manipulera Röds lägesbild.

7 Referenser

1. Försvarsmaktens handbok för informationsoperationer, M7739-352014, 2008.
2. Lemke, C. E., Howson, J. T. (1964). Equilibrium points of bimatrix games. *Journal of the Society for Industrial and Applied Mathematics* **12**(2):413–423.
3. von Stengel, B. (2007). Equilibrium computation for two-player games in strategic and extensive form, in N. Nisan, T. Roughgarden, E. Tardos, V. V. Vazirani (Eds.), *Algorithmic Game Theory*. Cambridge University Press, Cambridge UK, 2007, pp. 53–78.
4. Shafer, G., *A Mathematical Theory of Evidence*, Princeton University Press, 1976.
5. Smets, P., Kennes, R. (1994). The Transferable Belief Model. *Artificial Intelligence* **66**(2):191–243.
6. Holm, P. D. (2015). Detvag-90 – Propagation models 2015, Dnr FOI-2015-1562. Totalförsvarets forskningsinstitut, 2015.
7. Heickerö, R. (2010). *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations*. FOI-R--2970--SE, Totalförsvarets forskningsinstitut, 2010.
8. Teixeira, A., György, D., Sandberg, H., Johansson, K. H. (2011). A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator, in: *Proceedings of the 18th IFAC World Congress* (IFAC 2011), Milano, Italy, 28 August – 2 September 2011. International Federation of Automatic Control, Laxenburg, Austria, 2011, pp. 11271–11277.
9. Holm, H., Bengtsson, J., Löfvenberg, J., Persson, M., Sommestad, T. (2014). Moving target defense – En kartläggning av forskningsbidrag. FOI-R--3942--SE, Totalförsvarets forskningsinstitut, Sweden, 2014.
10. Neagoe, V., Bishop, M. (2006). Inconsistency in deception for defense in: *Proceedings of the 2006 workshop on new security paradigms* (NSPW 2006), Wadern, Germany, 19–22 September 2006. ACM, New York, NY, 2006, pp. 31–38.
11. Rowe, N. C. (2004). A model of deception during cyber-attacks on information systems, in: *Proceedings of the 2004 IEEE First Symposium on Multi-Agent Security and Survivability* (MASS 2004), 30–31 August 2004. IEEE, Piscataway, NJ, 2004, pp. 21–30.
12. Provos, N. (2004). A virtual honeypot framework, in: *Proceedings of the Twelfth USENIX Security Symposium* (Security '04), San Diego, CA, 9–13August, 2004. USENIX Association (Vol. 173), Berkeley, CA, pp. 1–13.
13. Cohen, F. (2006). The use of deception techniques: Honeypots and decoys. *Handbook of Information Security* **3**:646–655.
14. McQueen, M. A., Boyer, W. F. (2009). Deception used for cyber defense of control systems. In: *Proceedings of the Second conference on Human System Interactions* (HIS 2009), Catania, Italy, 21–23 May 2009. Interaction Design Foundation (Vol. 9), Aarhus, Denmark 2009.
15. Cyberspace Operations. Joint Publication 3-12 (R). Joint Chief of Staffs, 2013. [Online] Available: http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf (december 2015).
16. Harwell, S. D., Gore, C. M. (2013). Cyber joint munitions effectiveness manual (JMEM), *M&S Journal* (Summer 2013):5–14.
17. Schneider, B., Anglin, D., Baumgarten, E., Dinh, J., Hall, M. (2008). Raytheon Reference Architecture (RA): Enabling Timely & Affordable Customer Solutions, in: *Proceedings of the 13th International Command and Control Research and Technology Symposium* (ICCRTS), Seattle, WA, 17–19 June 2008. US Department of Defense CCRP, Washington, DC, 2008, Paper 40, pp. 1–22.
18. Musman, S., Temin, A., Tanner, M., Fox, R., Pridemore, B., Evaluating the impact of cyber attacks on missions, *M&S Journal* (Summer 2013):25–35.