FOI-R--1283--SE
Juni 2004
ISSN 1650-1942
Underlagsrapport

Martin Karresand, Mats Persson, David Lindahl

Scenarion och trender inom framtida informationskrigföring ur ett tekniskt perspektiv

Ledningssystem
581 11 Linköping

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Ledningssystem
Box 1165
581 11 Linköping

FOI-R--1283--SE

Juni 2004

ISSN 1650-1942

Underlagsrapport

Martin Karresand, Mats Persson, David Lindahl

Scenarion och trender inom framtida informationskrigföring ur ett tekniskt perspektiv

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--1283--SE	Underlagsrapport
Ledningssystem	**Forskningsområde**	
Box 1165	4. Ledning, informationsteknik och sensorer	
581 11 Linköping	**Månad, år**	**Projektnummer**
	Juni 2004	E7091
	Delområde	
	41 Ledning med samband och telekom och IT- system	
	Delområde 2	

Författare/redaktör	Projektledare
Martin Karresand	Mikael Wedlin
Mats Persson	**Godkänd av**
David Lindahl	Jonas Hallberg
	Uppdragsgivare/kundbeteckning
	FM
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Scenarion och trender i framtida informationskrigföring ur ett tekniskt perspektiv

Sammanfattning (högst 200 ord)

I tre tänkbara framtida militära scenarior studeras informationskrigföring ur ett mer tekniskt perspektiv. Det görs även ett antal prognoser om tekniken i den framtida IT-domänen och de militära ledningssystemen. Det visade sig att avståndet mellan de övergripande generella scenariona och den djupare tekniska nivån var större än förväntat.

Nyckelord

Övriga bibliografiska uppgifter	**Språk** Svenska
ISSN 1650-1942	**Antal sidor:** 21 s.
Distribution enligt missiv	**Pris: Enligt prislista**

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Command and Control Systems P.O. Box 1165 SE-581 11 Linköping	FOI-R--1283--SE	Base data report
	Programme Areas 4. C4ISTAR	
	Month year June 2004	**Project no.** E7091
	Subcategories 41. C4I	
	Subcategories 2	

Author/s (editor/s)	Project manager
Martin Karresand Mats Persson David Lindahl	Mikael Wedlin
	Approved by Jonas Hallberg
	Sponsoring agency FM
	Scientifically and technically responsible

Report title (In translation)

Scenarios and trends for future information warfare from a technical viewpoint

Abstract (not more than 200 words)

Information warfare is studied in three possible future military scenarios from a technical viewpoint. Some predictions are also made about technology in the future IT domain and the military command and control systems. The report shows that the distance between general scenarios and the more detailed technical level was larger than expected.

Keywords

Further bibliographic information	**Language** Swedish
ISSN 1650-1942	**Pages** 21 p.
	Price acc. to pricelist

1 Inledning

I det här kapitlet beskrivs bakgrunden till rapporten, dess syfte, problemformulering, metod för studien med mera.

1.1 Bakgrund

FoT-projektet *Strid i IT-domänen* initierades med målet att studera hur framtidens ledningssystem och andra IT-baserade system kan tänkas påverkas och skyddas ur ett strikt tekniskt perspektiv. Projektet sträcker sig över tre år och den här rapporten är en milstolpe i projektets första år. Projektet i sig är en fristående fortsättning på projektet *IT-vapen i en laborativ miljö* och syftar till att möjliggöra studier och utveckling av försvar och defensiva förmågor i framtida ledningssystem.

Till vår hjälp har vi haft två forskare (Göran Kindvall och Erik Nordstrand) från avdelningen för försvarsanalys. De har bidragit med kompetens kring scenarion och deras utveckling, samt generella trender inom försvar och framtida ledningssystem. Deras mest påtagliga bidrag till den här rapporten är de tre scenarion [ENH04, KN03] som använts för att underlätta arbetet. Med hjälp av dessa och erfarenhet från andra projekt med inriktning mot framtida ledningssystem har sedan denna förberedande studie gjorts.

1.2 Syfte

Rapporten syftar till att beskriva möjliga tekniska lösningar och hot mot framtida ledningssystem. Den kan sedan användas som ett komplement till de befintliga scenarion som finns. Följaktligen blir ytterligare ett syfte med rapporten att fungera som idégivare och inspirationskälla, både internt inom projektet och externt vid försvarsmaktens spel och övningar.

1.3 Problemformulering

De problem som rapporten syftar till att behandla är att:

- Visa på de tekniska möjligheter och hinder som en angripare ställs inför när målet är att påverka ett ledningssystem.
- Peka på troliga tekniska lösningar som kommer att användas i framtida ledningssystem.
- Fungera som idégivare och grund att bygga på vid laborativ utveckling av programvarubaserade verktyg för strid i IT-domänen.

1.4 Metod

Den metod som valts är att använda befintliga scenarion och dokumentation från bland annat en konferens inriktad på nätverksbaserat försvar (NBF) som bas och sedan fritt utifrån dessa dra slutsatser om hur ett ledningssystem skulle kunna vara uppbyggt om 10 till 15 år. Likaså har scenariona och dokumentationen fungerat som underlag för antagandena om hur dylika system kan angripas. Även utvecklingen inom programvarubaserade IT-vapen har studerats och sedan interpolerats för att ge en uppfattning av dessa vapens förmågor i framtiden.

1.5 Avgränsning

Rapporten behandlar endast de möjligheter, faktiska och tänkbara, som programvarubaserade IT-vapen ger. Alltså utelämnas all slags fysisk påverkan, som till exempel HPM och bomber. Även psykologiska operationer och annan påverkan av användarna och de människor som kan påverka systemet har uteslutits.

Rapporten riktar sig till personer som är allmänt orienterade om de tekniska aspekterna av informationssäkerhet och arbete därmed. Även läsare utan teknisk bakgrund kan ha nytta av rapporten, men de termer som används i rapporten anses vara kända av läsaren och förklaras bara närmare i de fall då projektgruppen haft delade meningar om deras uttolkning.

Tidsperspektivet för rapportinnehållet ligger omkring 10 till 15 år in i framtiden, det vill säga cirka år 2015-2020. Eftersom utvecklingen inom IT-området går mycket fort ska det som presenteras i rapporten naturligtvis enbart ses som kvalificerade gissningar.

1.6 Rapportens upplägg

I detta första kapitel ges läsaren den nödvändiga bakgrund som behövs för att läsa och förstå rapporten. Det andra kapitlet tar upp utvecklingsläget för två av delprojekten vid FOI inom den svenska NBF-utvecklingen. Som ytterligare bakgrund gör vi några prognoser om framtida trender i kapitel tre. I det fjärde kapitlet beskrivs kortfattat innehållet i de tre scenarion som legat till grund för rapporten. Det femte kapitlet innehåller en friare diskussion om scenariona och den pågående utvecklingen inom området med fokus på år 2015-2020. Detta kapitel tar också upp några tänkbara svagheter hos systemen och tänkbara sätt att angripa dem. Kapitel sex ger de slutsatser som projektgruppen dragit från arbetet med scenariona.

2 Utvecklingsläget

Som en bakgrund presenteras i det här kapitlet en översikt av läget inom ett par av de projekt vid FOI som syftar till att skapa ett nätverksbaserat ledningssystem.

2.1 Security Management

Security Management (SM) är det övergripande system som ska skydda Försvarsmaktens Ledningssystem 2010. Eftersom ledningssystemet är tänkt att fungera sömlöst och därför ha en dynamisk topologi, behövs det system för att hantera en ständigt föränderlig miljö. Systemet är också tänkt att ge en gemensam lägesbild åt alla användare utifrån deras egna önskemål. För att hålla ner utvecklingskostnaderna är det tänkt att systemet i möjligaste mån ska byggas av kommersiella produkter. Dock måste fortfarande behovet av sekretess, riktighet och tillgänglighet tillgodoses. Det gör att kraven som ställs på SM-funktionen är mycket höga.

Projektet har ännu inte hunnit till någon konkret implementation av en fungerande och heltäckande miljö som uppfyller alla de krav som ställs på det. För närvarande specificeras experiment som ska visa på möjliga utvecklingsvägar.

Tanken med systemet är att det ska fungera som ett slags meta-intrångsdetekteringssystem som utnyttjar även extern information för att få en heltäckande och aktuell lägesbild av det system som övervakas. Funktionen planeras innehålla såväl automatiska som manuella analysmetoder. Det kommer även att ha ett betydande inslag av specialutbildad personal som tillför ytterligare intelligens till analyskapaciteten.

De tekniska lösningarna för SM-funktionen är inte specificerade vid tidpunkten för den här rapportens framställning, vilket gör att det är svårt att uttala några mer exakta detaljer om detta. Vad som kan sägas är dock att det med stor sannolikhet kommer att ha inslag av agenter eller någon slags proxyfunktionalitet som fungerar som mellanhänder i systemet. De kan till exempel hantera delar av sammanställning och normalisering av insamlade data. Likaså kan de erbjuda ett enhetligt sätt att kommunicera mellan de olika ingående delarna. Ytterligare funktionalitet som kan tänkas finnas är autentisering och kryptering av SM-relaterad trafik mellan noder.

På en högre nivå kommer det att finnas funktionalitet för att korrelera larm. Det gör att systemet blir mer skalbart och att sannolikheten för att upptäcka distribuerade angrepp ökar. Korreleringen höjer också förmågan att detektera angrepp och att klassificera dem korrekt.

För att intrångsdetekteringssystemet ska kunna hantera och detektera intrång när nätverkstrafiken är krypterad behöver detektorerna ha möjlighet att kontrollera nätverkspaketen i klartext. Det enklaste och säkraste sättet är att använda nodbaserad intrångsdetektering, det vill säga placera detektorerna i noderna och låta dem kontrollera paketen efter det att noden dekrypterat dem.

Genom att placera detektorerna ute i noderna blir det också lättare att detektera avvikelser i användningsmönstret för noden. En sådan avvikelse kan till exempel tyda på att noden har fallit i fiendens händer, eller att användaren försöker överskrida sina får-privilegier eller felaktigt utnyttja sina kan-privilegier.

Tyvärr är risken för falsklarm relativt stor vid anomalidetektering (avvikelsedetektering). Därför är det tänkt att flera olika typer av detektorer kan samarbeta i varje nod och att deras resultat sedan korreleras för att ge ett sannolikhetsvärde för risken att det som detekterats är ett verkligt intrång.

Ett annat problem är hur olika grader av autonomitet ska hanteras. Det kan gälla både planerad och oplanerad autonomitet, det vill säga att en grupp soldater sänds ut på uppdrag där radiotystnad gäller, respektive att en grupp tappar kontakten med de egna trupperna av någon orsak. I båda fallen måste SM-funktionen erbjuda en lägsta nivå av säkerhet för de som ingår i den autonoma gruppen. Genom att använda nodbaserad intrångsdetektering borde inte SM-funktionen påverkas i någon nämnvärd omfattning, eftersom respektive nod kontrollerar sig själv och eventuellt bara kommunicerar med sina närmaste grannar.

Något som måste hanteras är dock hur återanslutning till nätverket ska gå till. Med stor sannolikhet har den autonoma gruppens klockor kommit ur fas med huvudsystemet. Det gör att eventuella intrångsförsök som gjorts under tiden inte går att korrelera med dylika försök som gjorts mot den autonoma gruppen. Därför måste tidssynkroniseringen lösas på ett tillfredsställande sätt. Likaså måste synkroniseringen av övriga systemändringar fungera. Det kan vara till exempel nya virusdefinitioner, ändrade inställningar för analysalgoritmerna, med mera.

Ytterligare ett förslag på funktionalitet i SM-funktionen är möjligheten att förändra de globala inställningarna stegvis. Inställningarna behöver inte nödvändigtvis vara direkt kopplade till SM-funktionen, utan kan omfatta även sådant som routing, bandbredd, rättighetstabeller och så vidare. En liknande funktion är de DEFCON-nivåer som den amerikanska försvarsmakten använder sig av. Några exempel på parametrar att förändra i SM-funktionen kan vara vilken typ av analysalgoritm som används, vilka data som ska samlas in för analys, sannolikhetsberäkningar och metoder för korrelering.

De externa data som är tänkta att kunna användas för att förbättra lägesinformationen som används av SM-funktionen för analys kan vara hämtade från många olika källor. Dessutom kommer källorna som används att variera beroende på vilket beredskapsläge som Sverige befinner sig i.

I fredstid spelar den personliga integriteten en större roll än i ofred. Därför används förmodligen ett mindre inslag av individpositionering och annan information som kan vara känslig. Dock är det tänkbart att till exempel uppgifter om personalens semesterperioder och förbandsplacering kan användas. På så sätt kommer det att finnas möjlighet att detektera om ett användarkonto blivit kompromett erat genom att det används på ett ologiskt sätt. Ett exempel kan vara att det inte går att använda en terminal i Luleå samtidigt som personen i fråga är förbandsplacerad i Karlskrona och inloggad på det interna nätet på något av marinens fartyg.

I ofredstider minskar förmodligen insiderhotet i förhållande till de externa hoten från fiendens trupper. Därför är det tänkt att SM-funktionens insamlingsfunktion kan förändras och ta emot data från bland annat NETINT, HUMINT och SIGINT. Dessutom kommer data från civila myndigheter att behövas i högre grad och bör därför vara möjliga att kräva in till SM-funktionen. Detta kommer dock att påverka den personliga integriteten och den exakta utformningen och nivån behöver utredas vidare.

2.2 System av system – web services

Detta projekt har haft följande målbild för det framtida försvaret och dess ledningssystem:

> Det framtida tekniska ledningssystemet måste byggas med en evolutionär utvecklingsmodell. Systemet måste vara designat så att det är möjligt med avknoppning och hopkoppling av delsystem, vilket innebär att systemet kommer att innehålla många delsystem. Dessa delsystem kommer att vara oberoende av varandra, självständiga, mobila och interoperabla med andra typer av system. Delsystemen ska vara lätta att byta ut eller modifiera. Målet med projektet är att maximera den defensiva förmågan hos våra egna system – att få starkast möjliga skydd mot obehöriga intrång.

Projektet ”System av system” startade 2003 och producerade det året två rapporter ”Identitetsverifiering över systemgränser” och ”Tilltro och policies för mobil kod i heterogena system och nät”. Dessa två rapporter var alltså fokuserade på säkerhetproblematiken inom system av system.

Inom detta projekt har det konstaterats att systemet måste kunna tillhandahålla ett antal tjänster i nätet. För att tekniskt kunna uppfylla detta är det sannolikt att man kommer att använda sig av Web Services. En webtjänst är enkelt uttryckt ett sätt att på ett standardiserat sätt beskriva en tjänst i nätet. Rent tekniskt är det en XML-interpretator som lyssnar på en särskilt port och tar emot och sänder meddelanden enligt client-server modellen, samt att denna XML-interpretator via ett gränssnitt skickar vidare data till applikationen på nästa nivå.

För närvarande studeras inom projektet en metod för att i webtjänst-meddelandet lägga in den passerade nodens namn och signera detta. Detta för att kunna spåra meddelandets väg genom nätet.

3 Framtida trender

3.1 Trender inom IT

IT kan delas upp i två delar, hårdvara och mjukvara. Trender inom hårdvarudelen är något enklare att förutsäga i och med att Moore's lag om processorernas klockfrekvens de senaste årtiondena har följt en väldigt förutsägbar kurva. De hårdvarutrender som brukar räknas som självklara är:

- Datorer kommer att bli snabbare. Inte bara på grund av snabbare CPU utan även av större interna minnen.
- Nätverken kommer att bli snabbare och ha högre överföringskapacitet.
- Storleken på externa lagringsutrymmen för data kommer att öka.
- Graden av datorisering och det totala antalet datorer per funktion kommer att öka.
- Mängden nät kommer att öka och trådlösa nät kommer att öka mest.

Den programvarumässiga, eller datalogiska delen av IT är svårare att förutspå. Hårdvarutrender kan ge stora effekter inom den datalogiska domänen. Om CPU och nät blir snabbare så kan man göra mer komplexa operationer på kortare tid. De generella trender som är troliga inom den datalogiska domänen är:

- Datorsystemen blir mer dynamiska och ständigt föränderliga. Både att programmens, datats eller tjänsternas positioner i nätet blir mer dynamiska, och att programvarans funktion kan förändras dynamisk från sekund till sekund.
- Användaren blir mindre och mindre involverad i administrationen av mjukvaran. Till exempel kommer operativsystemen själva uppgradera sig automatiskt.

Detta kan få negativa konsekvenser:

- Möjligheterna att införa elak programkod i näten ökar.
- Man blir mer beroende av nyckelpersoner som förstår IT.
- Den ökade komplexiteten medför ökade risker för fel.

3.2 Militära trender inom nätverkskrigföring

De senaste årens internationella utveckling inom olika länders försvarsmakter verkar i Europa, Nordamerika och delar av Asien vara inriktat mot att effektivisera och digitalisera utrustningen inom organisationerna [NCW04]. Efter att det kalla kriget har försvunnit har andelen gamla försvarssystem skurits ner och moderniseringar, tillsammans med nyinköp, sker efter de förväntningar länderna har på framtida konflikter. Försvinnandet av det kalla krigets världsbild har också lett till krav på nedskärningar i en del länder medan krigen i mellanöstern och det så kallade kriget mot terrorismen har lett till att upprustningar accepterats i andra länder, främst USA och Storbritannien.

De förväntningar som finns på framtida konflikter verkar vara att de kommer att ske i tillfälliga koalitionssammansättningar, De kommer att vara tillfälliga och på olika ställen i världen. Världsläget har också blivit mycket mer svårförutsägbart. Detta sammantaget gör att förberedda positioner och fasta anläggningar inte verkar lika attraktiva som tidigare. Konflikterna väntas heller inte vara lika renodlade som tidigare. Skillnaderna mellan olika typer av konflikter, som fredsbevarande och fredsframtvingande väntas minska. I framtida konflikter finns troligen också mer än två parter inblandade, dessutom i olika hög grad. Modeord som används är ”joint”, ”Mobile”, ”Multi-role” bland andra.

En annan trend som trots att den inte är ny fortfarande verkar vara stark är att försöka minska mängden personal inblandad i strider och underhåll. Detta naturligtvis för att spara liv i en eventuell konflikt, men också för att minska kostnader. Dessa kan minskas genom automatisering av arbetsuppgifter, effektivisering, men också genom militär ”outsourcing” till privata företag, eller civila, men statliga, organisationer.

Bland de förändringar som militärmakterna har inlett finns ett par som verkar vara gemensamma åtminstone i intentionerna hos de högre beslutsfattarna.

- Man vill försöka få bort de spärrar som finns mellan förband och vapenslag så att de kan samarbeta i taktiska situationer.
- Detta förutsätter att de olika vapenslagen och förbanden kan kommunicera och att de har tillgång till en gemensam lägesbild.
- För att kunna utnyttja varandras resurser i en taktisk situation måste även de olika enskilda fordonsförarna och vapenoperatörerna dela samma lägesbild och kunna kommunicera med varandra.
- Alltså måste lägesinformation och sensorinformation göras tillgängliga mycket snabbt inom organisationerna och inte bli ”upplåsta” hos staberna.
- Dessutom måste varje delorganisation göra sensorinformation tillgänglig för andra än sensoroperatören och dennes överordnade. I synnerhet m a p olika vapenslag.
- Förutom de ovanstående punkterna vill man i hög grad möjliggöra informationsdelning över nationsgränserna vid koalitionskrigföring.

- De tekniska hjälpmedel som används i det moderna samhället för kommunikation, ledning och informationslagring vill man använda i de militära organisationerna för att åstadkomma en effektivare ledning i fredsträning och skarpa operationer.

De ovanstående punkterna innebär ur ett tekniskt perspektiv

- Kommunikation måste standardiseras så att sensordata, bilder och ljud kan överföras mellan i princip alla enheter oavsett organisationstillhörighet.

- Dataöverföringen måste kunna ske automatiserat mellan enheter som inte känner varandras existens. Det blir inte möjligt för varje spaningspilot att hålla reda på alla infanteriplutoner som finns i området han spanar över som vill ha reda på hans spaningsresultat.

- Dataöverföringen måste kunna ske i flera steg utan att sändaren eller mottagaren känner till det. Om ett förband tillfälligt befinner sig i radioskugga eller utom räckhåll för en sensor, men staben har kontakt med den måste information fortfarande kunna göras tillgänglig utan (signifikant) fördröjning.

- Användningen av radio blir ofrånkomlig för snabbt manövrerande enheter. Men mängden data kommer att leda till att bandbreddsfrågor blir mycket viktigare än förut. Eftersom en stor mängd data kommer att samlas in och fördelas, men bara små mängder data kommer att vara viktig för en enhet lågt ner i hierarkin är det rimligt att anta att användningen av trådkommunikation, eller höghastighetsradiolänkar blir nödvändiga för att överföra större mängder data.

- Det leder till en uppdelning av nätverket i minst tre kategorier. En snabb infrastrukturberoende kategori som använder tråd, fiber och radiolänksystem för att överföra data mellan fasta och semifasta enheter som radartorn, staber, och fartyg. En snabb, men radioberoende kategori som överför data mellan ledningsfordon och staber, och slutligen en kategori som används för lokal taktisk kommunikation mellan ledningsfordon och stridsfordon, eller fordon och avsuttna soldater. Troligen kommer de sista kategorierna att vara ”ad hoc-nätverk”.

- För att spara pengar och öka effektiviteten kommer troligen kommersiella civila system att användas i de system där det går att göra. Så kallade COTS-alternativ. I staber, och till viss del fast monterade i ledningsfordon kan vanliga kontorssystem fungera lika bra som specialbyggda alternativ. I en framskjuten taktisk miljö är det svårare att hålla COTS-alternativ fungerande på grund av de uppenbara kraven på temperatur- fukt- och stötokänslighet men dessa krav har i allt högre grad börjat tillgodoses redan i dag. Exempel är GPS, satellittelefoner och PDA:er för friluftsmänniskor, yrkesarbetande med speciella miljökrav som lantmätare, oljeborrare etc. Om denna trend fortsätter kommer mycket av utrustningen som behövs även för en taktisk användning att finnas tillgänglig som COTS.

- Kombinationen av COTS-beroende och en automatiserad reläad dataöverföring mellan olika typer av enheter leder till slutsatsen att i det korta tidsperspektivet (0-3 år) finns inget annat alternativ än att använda IP-baserade lösningar. Troligen kommer IPv6 att ersätta de nuvarande IP-protokollen i det medellånga perspektivet (3-5 år). Men inget tyder på att paketförmedlande nätverk av IP-typ kommer att ersättas av någon annan standard på minst 10-15 år.

- Dock bör utrustningarna som används kunna anpassas för olika typer av protokoll och standarder i de högre lagren av OSI-modellen. Det tyder på att mjukvarubaserade lösningar för kommunikation blir viktigare än tidigare.

För att illustrera de ovanstående exemplen hänvisar författarna till föredrag som hölls i samband med Network Centric Warfare-konferensen i Stockholm 1-2 juni 2004 [NCW04].

3.3 Exempel på osäkra analyser

Vid läsning av detta kapitel är det vitalt att inse att diskussioner om framtida teknisk utveckling i bästa fall är osäker, även om den förs av högt kompetenta tekniker. Läsaren uppmanas att vara synnerligen kritisk.

Exempel på tidigare försök att analysera framtida trender:

Flygplan

"Airplanes can barely keep themselves in the air. How can they then carry any kind of load?" - *William Pickering, Astronomer (1908)*

"Airplanes suffers from so many technical faults that it is only a matter of time before any reasonable man realizes that they are useless!" - *Scientific American (1910)*

"No flying machine will ever fly from New York to Paris." - *Orville Wright*.

"Flygplan är intressanta leksaker men saknar militärt värde." - *Marshal Ferdinand Foch [Professor of Strategy, Ecole Superieure de Guerre] (circa 1911)*

"To throw bombs from an airplane will do as much damage as throwing bags of flour. It will be my pleasure to stand on the bridge of any ship while it is attacked by airplanes." - *Newton Baker, US minister of defense (1921)*

U-båtar

"Yes, it is possible!" -*William Bourne, engelsk uppfinnare. (1578)*

"The only thing that will happen is that the vessel will sink, and suffocate the crew" - *H. G. Wells, engelsk författare (1902) (U-båtar hade då använts sedan ca 1850)*

"Even if a submarine should work by a miracle, it will never be used. No country in this world would ever use such a vicious and petty form of warfare!" - *William Henderson, brittisk amiral (1914)*

Trådburen kommunikation

"Samuel Morse most have lost his mind if he believes in this idea himself!" - *Senator Oliver Hampton Smith, (1842) efter att ha sett en demonstration av telegrafen genomföras.*

"It is only righteous that Joshua Coppersmiths, who has tried to find investors to finance the development of a so-called telephone, is arrested for fraud!" - *En artikel in Boston Post (1865)*

Trådlös Kommunikation

"The radio has no future!" - *Lord Kelvin, British Mathematician(1897)*

"Use your time on something useful. All radios this country will ever need can easily fit on my desk!" - *W.W. Dean, direktör för American phone company "W.W. Dean"(1907), till Lee DeForrest (radiopionjär)*

"Radio is just a fashion contrivance that will soon die out. It is obvious that there never will be invented a proper receiver!" - *Thomas Edison*

"The wireless music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?" - *David Sarnoff's kolleger när han ville investera i musikradio under 1920-talet*

4 Scenarion

I det här kapitlet presenteras de tre scenarion som använts inom projektet. Scenariona har använts vid ett flertal tillfällen inom försvarsmakten för övning och utvärdering av ledningsfunktionen.

Det som presenteras här är valda delar av scenariona och det är främst de delar som kan härledas till IT-krigföring. Likaså nämns tekniska specifikationer i mån av tillgång och relevans.

För alla de tre utvalda scenariona gäller att de behandlar IT-krigföring (Information Warfare (IW), Computer Network Operations (CNO)) på en mycket generell nivå. Inte heller beskrivs ledningssystemen och deras arkitektur på detaljnivå utan endast mer övergripande. Till viss del kan det förklaras med att scenariona ska visa på möjliga situationer om 10 till 15 år. Det gör att scenarionas betydelse för arbetet med att studera trenderna för de tekniska delarna av IT-krigföring minskar. De finns dock med här för att i alla fall visa på de tankegångar som används vid ledningsövningar i dagsläget.

4.1 Roslagen

Scenariot utspelar sig någon gång kring 2015. Spänningen i Östersjöregionen har ökat under några år. För tillfället pågår en omfattande marinövning öster om Gotland med inslag av aggressivt uppträdande mot svenska fartyg.

En fientlig styrka landsätts i Kapellskär. Parallellt med detta inleds omfattande telekrigsinsatts mot Sverige. Avledande verksamhet försöker dra försvararnas uppmärksamhet mot Arlanda, bort från det begynnande brohuvudet i Kapellskär. Avledningen sker först och främst genom IW mot försvararnas ledningssystem. Kommunikationen på bataljonsnivå i det svenska försvaret sker i huvudsak med radionät av självupprättande karaktär.

Kindstrand och Nordvall [KN03, sidan 18] beskriver hur ett IT-försvarssystem i deras mening är uppbyggt av fyra delar:

1. *Flödeskontroll* för att styra informationsflödet och ge kännedom om normalläget.
2. *IT-ISTAR* (Intelligence, Surveillance, Target Acquisition, Reconnaissance) som främst ger möjlighet till spaning och övervakning, bland annat av FM IP-nät.
3. *IT-vapen* som ger offensiv förmåga i defensivt syfte. Det kan till exempel handla om vilseledning.
4. IO-ledning som fungerar tillsammans med andra ledningsfunktioner och inriktar sig på att leda försvaret i IT-dimensionen.

De beskriver vidare hur fiendens IW-insatser kan tänkas ta för form. Eftersom fiendens mål är att få de svenska trupperna att gå mot Arlanda vill fienden vilseleda svenskarna och göra det på ett raffinerat sätt för att öka trovärdigheten. Enligt Kindstrand och Nordvall [KN03, sidan 20] kan detta bara uppnås genom att antingen använda en insider hos svenskarna, eller genom att ha planterat in trojanska hästar och andra fjärrstyrda programvarubaserade IT-vapen som kan aktiveras via till exempel mail. Det senare alternativet håller de dock för mindre troligt eftersom de inte tror att systemen skulle vara så öppna att detta skulle vara möjligt.

Ett annat, mer trubbigt sätt för fienden att nå sitt mål är att utföra ett denial-of-service-angrepp mot det svenska nätet. På så sätt skulle om inte annat det svenska försvaret och dess truppförflyttningar fördröjas eftersom ledningen måste inhämta lägesinformation med manuella metoder. Dylika angrepp kräver dock att fienden känner till de IP-adresser som ska angripas, enligt Kindstrand och Nordvall [KN03, sidan 25]. De diskuterar även möjligheten att låta nätverksutrustningen bara acceptera paket från godkända avsändare, men förkastar tanken på grund av risken för att behörig trafik också kan stängas ute. Problemet i det fallet beror på svårigheten att hålla listorna med godkända avsändare uppdaterade.

4.2 Kaukasus

Oljebolag från västvärlden har gjort investeringar i pipelines och petrokemisk utvinning i ett land i Kaukasus. Någon gång kring år 2015-2020 beslutar sig en samling utländska oligarker med intressen i oljeindustrin för att återta och utöka inkomsterna från olje- och gastransporterna i området. Deras plan är att göra det genom att sponsra olika grupper som vill ta över den politiska makten i området och på så sätt skapa instabilitet som höjer världsmarknadspriset på olja.

Landets ledning begär efter ett tag hjälp från EU, som inleder en fredsbevarande operation. Operationen försvåras av en hög massmedial närvaro, gisslansituationer, stora inslag av civilbefolkning och skiftande lojaliteter mellan olika konstellationer av kontrahenter.

Befolkningens utbildningsnivå anses relativt hög, likaså IT-mognaden. Många medier förmedlas via Internet och det finns optisk fiber dragen mellan några städer i landet. Regeringsmotståndarna och deras sympatisörer har global hjälp och avancerade kommunikationsresurser, både för att kunna förmedla information säkert och kunna avlyssna andras kommunikation. Till sin hjälp har de även hackerceller om fyra till sex hackers och konsulter, såväl som enskilda hackers.

Regeringsmotståndarnas mål är att få EU-styrkan att lämna landet. Deras plan för att uppnå detta är att angripa EU-styrkan och tillfoga den sådana skador att de drar sig ur uppdraget.

Kindstrand och Nordvall [KN03, sidorna 33-34] nämner inte specifikt vad för slags datornätverksoperationer (Computer Network Operations, CNO) som respektive part använder sig av, men det handlar i första hand om underrättelseverksamhet och spaning. Ett exempel är att via uppgifter ur affärs- och ekonomisystem få fram uppgifter om hur regeringsmotståndarna förflyttar sig. Kindstrand och Nordvall beskriver dock inte om detta görs med systemägarnas medgivande eller inte.

Vidare skriver de att det finns behov av att ”allokera relevanta IW-verktyg och anda resurser för att stödja egen och förstöra motståndarens verksamhet” [Kindstrand och Nordvall, KN03, sidan 34]. Dessa verktyg skiljer sig mellan olika nivåer beroende på om det handlar om till exempel strategiska, operativa eller taktiska verksamheter och likaså beroende på om den är nationell eller internationell.

Ett andra delscenario presenteras också i rapporten. Det har ett liknande upplägg som det som beskrivits ovan, med den skillnaden att det utbrutit inbördeskrig i landet och EU-kallas in för en fredsskapande operation. Då tillåts mer avancerade och kraftfulla medel. Några exempel på dylika medel kan vara att plantera in virus i datorsystem, göra DoS-angrepp och aktivera logiska bomber Kindstrand och Nordvall [KN03, sidan 41]. Återigen anges inte i vilka system eller på vilket sätt detta skulle kunna göras. Det som anges är att CNO ska användas.

4.3 Strid i urban miljö

Det här scenariot, som är ett ännu ej fastställt utkast skrivet av Evander, Nordstrand och Henningsson [ENH04] har inte någon exakt datering, utan är framtaget för att ge exempel på strid i urban miljö. Bakgrunden till scenariot är att B-land, som plågas av inre stridigheter, anfaller EU:s ordförandeland Sverige för att få EU att lämna landet i fred. EU har redan militära förband närvarande i B-land och ett alternativt delscenario är att den rörliga insatsledningen i Sverige smittas med maginfluensa som slår ut dem tillfälligt. Därför måste försvarsinsatserna ledas från B-land.

B-lands taktik bygger på att inta A-stad i Sverige och B-stad i Danmark samt med diverse relativt avancerade vapen idka gerillakrig mot Sverige. Det främsta hotet utgörs av en blockad av Öresund och hot om att spränga Öresundsbron. Blockaden iscensätts med hjälp av minor, självmordskommandon i gummibåtar och sjömålsrobotar. Det svenska försvaret och då främst dess ledningsförmåga angrips med hjälp av kryssningsrobotar och manburna luftvärnssystem, men det förekommer även IW-verksamhet.

Svenskarna vill först och främst återta A-stad och sätta stopp för blockaden av Öresund. Det hela kompliceras av en hög koncentration civila och ett intensiv mediabevakning. Likaså idkas det IW mot det svenska ledningssystemet.

Några av de frågor med bäring på IT-krig som tas upp i rapporten är hur det svenska försvaret ska kunna skapa ett lokalt nätverk i staden, hur detta nätverk kan kopplas samman med insatsledningen och även hur nätverket ska skyddas mot intrång. Det svenska försvaret sägs ha tillgång till CNO-kapacitet som används mot inkräktarna. Några mer detaljer om hur den används och med vilka medel anges inte i rapporten. Inte heller beskrivs något av de båda landens ledningssystem i mer detalj. Det som nämns är att det svenska ledningssystemet fungerar sömlöst [ENH04, sidan 16].

5 Diskussion

Detta kapitel innehåller en friare diskussion med olika kommentarer om de scenarion som beskrivits ovan, samt en lite allmännare diskussion om tekniken för informationskrigföring.

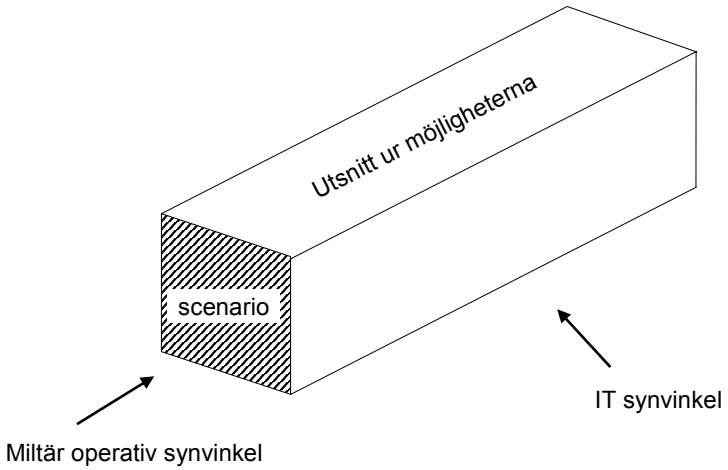
5.1 Allmänt

Det är mycket svårt att sluta sig till vilka möjligheter till angrepp och intrång som bjuds i framtidens ledningssystem. Utifrån vad som presenterats i de föregående kapitlen förs här en diskussion om hur det eventuellt skulle kunna se ut. Eftersom de scenarion som presenterades i kapitel 4 endast uppehöll sig på en övergripande nivå och egentligen inte visade på hur ledningssystemen skulle kunna fungera i framtiden, har flera antaganden fått göras om teknik och arkitektur.

En gemensam sak har dock gått att uttyda ur scenariona och den övriga information som studerats, ledningssystemen kommer att vara distribuerade och ha en dynamisk topologi där noder och domäner rör sig. Dynamiken återfinns såväl på en logisk som på en fysisk nivå och medför att de nödvändiga säkerhetslösningarna kompliceras.

5.2 Scenariona ur teknisk synvinkel

Scenariona tjänar väl sitt syfte att identifiera hot och möjligheter med informationskrigföring på en mer militär och operativ nivå. På denna nivå är scenariona ett utsnitt av möjliga militära operationer. Men ur en teknisk synvinkel är utsnittet alldeles för stort och spänner över för många möjligheter. En del teknik har dock funnits med i scenariobeskrivningarna, där scenario ”Roslagen” innehöll mest tekniska detaljer. De olika synvinklarna visas i nedanstående skiss:



Bilden visar att även om det militära utsnittet av möjliga scenarier är ganska litet, så är snittet ur IT-synvinkel mycket större och därmed täcker ett större område med möjligheter. Bilder försöker alltså visa att snittet av IT-domänen (cyberrymden) blir så stor att vi har haft svårt att utläsa något ur detta.

Vad är då egentligen IT-domänen, eller cyberrymden? Det kan vara bedrägligt att göra jämförelser med den reella världen. Till exempel att en väg skulle motsvara en kommunikationskabel, en vägkorsning en router eller en brandvägg skulle vara en vägspärr. Om man drar sådana paralleller kan man hamna i farliga fallgropar, inte minst när man hamnar i datalogin som ur vissa aspekter saknar motsvarigheter i den verkliga världen. Ett tydligt exempel är att det är synnerligen enkelt att tillverka en kopia av ett datorprogram. Att kopiera något fysiskt kan kräva betydligt mer resurser. Att kopiera ett papper är ganska enkelt men att kopiera en stridsvagn är tidsödande och kräver mycket arbete och stål.

En nackdel med de nya moderna grafiska gränssnitten som moderna datorer har, är att de döljer det komplexa och svårförståeliga. De är numera så enkla att använda att man lätt kan tro att man förstår dem. Det kan bli ännu värre om man fått djupare förståelse för en liten detalj och sedan tror att man kan använda denna kunskap till att förstå resten. En illustrerande parallell är om man har förstått hur flygplanspropellrar fungerar, för att sedan tro att man kan flyga baklänges om man vänder propellern på andra hållet.

Som nämnts tidigare har vi haft svårt att göra en djupare teknisk IW-analys av scenariona. IT-attacker är ganska situationsberoende, kanske mer än fysiska attacker. Dessutom kommer militära ledningssystem till stor del vara byggda av COTS, vilket gör att de inte kommer att utgöra någon särställning vad det gäller känslighet för IT-angrepp.

Scenarionas uppbyggnad är också ganska frikopplad från IT-delen av ledningssystemet, och eventuella uppbyggnad. På samma sätt som en spion-organisation är ganska frikopplad från militären. En IT-attack är ett scenario i sig, och går knappast att generera ur ett fysiskt militärt scenario.

5.3 Militär IW-kapacitet

Förutom ovanstående kritik mot scenariona så har vi ytterligare en invändning mot dem. Något som vi uppfattar som en brist i scenariona är att grundantaganden har gjorts utan att man poängterat deras betydelse. Exempelvis anges att de militära datorsystemen är så säkra att man måste ha insiders för att kunna göra intrång. Men inget sägs om den mängd personal som krävs för att hålla systemen i drift eller den utbildning som krävs för att hålla personalen i trim för sin uppgift. Detta trots att den organisation som FM har idag inte alls innehåller den mängd tekniker per stridande soldat som troligen kommer att behövas, eller har allokerat den budget som kommer att krävas för att hålla högt tränade IT-experter i organisationen så att de inte avviker till privata arbetsgivare. Inte heller har underhållssituationen tagits upp i scenariona. Om Sverige skickar en bataljon fredsbevarande soldater och upptäcker att ett helt kompani måste utgöras av tekniker för att kunna hålla IW-kapaciteten uppe, kommer man då att skicka den delen av truppen om man inte väntar sig IW-krig? Ska man använda civila företags konsulter för de tekniska tjänsterna, och kommer de i så fall att bli kombattanter, eller rent av betraktas som legosoldater? När Sverige deltar som en del av en EU-styrka, har man gemensamma IT-system, har man standardiserade system, har man samma kapacitet för skydd, underhåll och support av IT-systemen inom EU? Alla dessa frågor påverkar bedömningen av vilken teknisk nivå som systemen kan tänkas ha.

Som en något vidare kommentar när det gäller det som skrevs ovan om cyberkrig respektive fysiskt krig. CNO är ett ganska underligt djur, för att citera en kollega från S1. Till skillnad från alla andra typer av strid kräver det att den angripne besitter kapacitet för att kunna angripas. Om den ena sidan har stridsvagnar kan de angripa den andra sidan även om dessa saknar stridsvagnar. Men om den ena sidan har datorer, datornät och en datoriserad infrastruktur men den andra sidan saknar det, så kan den tekniskt överlägsna sidan inte göra någon form av CNO mot den tekniskt underlägsna. Det omvända är dock inte helt sant eftersom den mindre tekniskt kapabla aktören kan utnyttja legosoldater, eller bygga upp en liten teknisk bas för att kunna angripa den stora infrastrukturen i motståndarens land. Samtidigt som den egna infrastrukturen är osårbar.

Det är alltså en form av krigföring som alltid gynnar den sida som i stort är mindre tekniskt utvecklad, men i små enheter har kapacitet att anfalla en högt ”teknologiserad” fiende.

Men detta förutsätter att man är beredd att anfalla den civila infrastrukturen. Militären har ju förmågan att kortare tider frigöra sig från den civila infrastrukturen och agera oberoende av datorerna. En bataljon som får sin kommunikation avskuren har de senaste ordrarna i minnet och kan agera utifrån vad de tror är den vettigaste planen och till viss del kompensera med ordonnanser för de viktigaste orderpunkterna.

Men jag som individ kan inte ordna fram pengar om transfereringssystemen har gått ner. Inte heller kan en ICA-butik rekvirera varor från ett centrallager när telenätet är borta.

För de militära aktörerna blir CNO:s betydelse för operationerna något som används likt telekrigföring och underrättelseaktivitet. En förmåga som minskar fiendens kapacitet för ledning och kommunikation samtidigt som den förbättrar ens egen. Men en förmåga för strid som enbart är uppbyggd kring telekrig och underrättelser kan inte vinna strider eftersom den saknar förmåga till förstörelse. Det är en aktivitet som är ett komplement till den väpnade striden.

Däremot kan CNO användas separat i den rent tekniska sfären för att slå ut datorsystem, påverka opinion, infrastruktur, ekonomi, politik i ett land. Frågan är hur ett försvar mot sådana aktiviteter ska kunna upprätthållas. Militären kan skydda sina egna system, men hur gör FM-log om grossisterna tappar bort alla beställningar och sjukvårdarna om sjukhusen inte kan ta emot de skadade för att medicintransporterna gått till andra adresser?

5.4 Fortsatt arbete

I vårt fortsatta arbete i detta projekt kommer vi att försöka konstruera tänkbara tekniska system som kan passa de tidigare beskrivna scenariona. Scenariona kan tjäna som utgångspunkt för att avgöra vilka tjänster som kan finnas i systemet. Ur de spel som utförs och den kapacitet som förutsägs i scenariona kan vi dra slutsatser om de tjänster som måste finna i lednings- och kommunikations-systemen. Vi kan för scenarion som ligger nära i tiden sätta upp rimliga tekniska lösningar som arkitekturer och protokoll som kan tänkas användas. I scenarion som ligger långt fram i tiden är detta svårare.

Scenarion kan även användas till att avgöra vilka mål och operationer som är viktiga i vilka skeden. Vid ett tillfälle i ett scenario kan till exempel kommunikationen vara beroende av en mindre säker länk än i andra skeden, eller ännu mer tidskritisk. Ett angrepp som slår ut de specifika länkarna i det specifika skedet skulle alltså få större konsekvenser än om angreppet utfördes vid ett annat tillfälle. Känner man till detta kanske man hellre väljer alternativa mål vid de andra tillfällena.

Det är även möjligt att låta de konstruerade tekniska systemen ha generella ingångsparametrar, som till exempel ”hög”, ”medel” och ”låg” säkerhetsnivå. Den höga nivån kan till exempel innefatta antivirus som uppdateras varje timme, operativsystem som alltid har de senaste säkerhetspatcharna, kommunikation har stark autenticering och kryptering.

Utifrån de tänkta tekniska systemen kan vi sedan beskriva svagheter och tänkbara angreppsmetoder på systemet. Scenariona i sin nuvarande form avgränsar händelseförloppet, men en teknisk avgränsning saknas nästan helt. En definition av den tekniska omgivningen kan ge nya förutsättningar och påverka händelseutvecklingen i scenariona.

6 Slutsatser

Det ursprungliga syftet med denna rapport var att genom ett antal tidigare publicerade scenarion visa på framtida trender för informationskrigföring mot militära ledningssystem. Detta visade sig vara något svårare än förväntat. Generella slutsatser är att:

- Digitalisering och nätverksanvändning ökar markant i länder som moderniserar sitt försvar.
- Framtida angrepp kommer att ske på dynamiska och distribuerade system med stor komplexitet. På motsvarande sätt måste man försvara ett snabbt föränderligt system. Målen blir rörligare.
- Det handlar inte bara om att se datorer som verktyg i militära ledningssystem och som hjälpmedel vid fysiska attacker. Cyberrymden kommer att bestå av stora datornätverk, som även kan vara trådlösa, innehållande ett stort antal datorer med en mängd tjänster. Denna rymd har sina egna regler för angrepp och försvar.
- Avståndet mellan scenariona och tekniken var större än förväntat. Detta tomrum kan betyda en av tre saker: antingen har scenariona ingen grund i tekniken, eller så kommer den framtida tekniken att se helt annorlunda ut, eller så saknas det metoder eller teorier för koppling mellan övergripande scenarier och den djupare tekniken. I vårt fortsatta arbete kommer vi att utgå från det sista alternativet.

7 Referenser

[ENH04] S Evander, E Nordstrand och J Henningsson, 2004, *Scenariobeskrivning Nationell strid i urban miljö – Version 1.02* (ej fastställd eller publicerad version), Försvarsanalys, Totalförsvarets Forskningsinstitut – FOI

[KN03] Göran Kindvall och Erik Nordstrand, 2003, *Informationskrigföring inom FoRMA – Dokumentation från spel 2001,* FOI-R--0810—SE, underlagsrapport, Försvarsanalys, Totalförsvarets Forskningsinstitut – FOI

[NCW04] Conference proceedings: Network Centric Warfare Europe 2004, 1st & 2nd June 2004, Stockholm, Sweden