FOI-R--1620--SE
Mars 2005
1650-1942

Underlagsrapport

CNA-scenarier ur ett tekniskt perspektiv

Mikael Wedlin

Ledningssystem
Box 1165
581 11 LINKÖPING

Totalförsvarets forskningsinstitut
Ledningssystem
Box 1165
581 11 LINKÖPING

FOI-R--1620--SE
Mars 2005
1650-1942

Underlagsrapport

CNA-scenarier ur ett tekniskt perspektiv

Mikael Wedlin

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets forskningsinstitut Ledningssystem Box 1165 581 11 LINKÖPING	FOI-R--1620--SE	Underlagsrapport
	Forskningsområde: Ledning, informationsteknik och sensorer	
	Månad, år: Mars 2005	Projektnummer: E7091
	Verksamhetsgren: Uppdragsfinansierad verksamhet	
	Delområde: Ledning med samband, telekom och IT-system	
Författare/redaktör: Mikael Wedlin	Projektledare: Mikael Wedlin	
	Godkänd av: Johan Allgurén	
	Uppdragsgivare/kundbeteckning: FM	
	Tekniskt och/eller vetenskapligt ansvarig	

Rapportens titel

CNA-scenarier ur ett tekniskt perspektiv

Sammanfattning

Syftet med denna rapport och försöket att formulera scenarier på en teknisk nivå, är att den skall utgöra underlag i det fortsatta arbetet med inriktning av projektet samt att användas i interna workshops och i referens/styrgruppsarbete. Det är också författarens förhoppning att vi med hjälp av denna ansats skall kunna koppla försvarsmaktens typscenarier och andra liknande arbeten till innehållet i forskningen på vår tekniska nivå. Här kan man dock konstatera att vi fortfarande har långt kvar. Man kan också i viss mån använda rapporten som underlag vid diskussioner om vad IT-krigföring är och om de mekanismer som beskrivs i denna rapport är rimliga antaganden om en trolig framtid.

Nyckelord

Övriga bibliografiska uppgifter	Språk
	Svenska
ISSN: 1650-1942	Antal sidor: 19
Distribution: Enligt missiv	Pris: Enligt prislista Sekretess: Öppen

Issuing organization	Report number, ISRN	Report type
Swedish Defence Research Agency Command and Control Systems Box 1165 SE-581 11 LINKÖPING Sweden	FOI-R--1620--SE	Base data report
	Programme Areas: C4ISTAR	
	Month year: March 2005	Project no.: E7091
	General Research Areas: Commissioned Research	
	Subcategories: C4I	
Author/s (editor/s): Mikael Wedlin	Project manager: Mikael Wedlin	
	Approved by: Johan Allgurén	
	Sponsoring agency: Swedish Armed Forces	
	Scientifically and technically responsible	

Report title

CNA-scenarios from a technical perspective

Abstract

The purpose of this report is to formulate scenarios that could be used as foundation for the planning of the rest of the project. It is also the author's hope that this way of formulating technical scenarios will make the connections to other scenarios a simpler task. We do, however, have a long road to walk before we reach that goal. Another usage of this report could be in discussions about what IT-warfare is and if these kind of scenarios are likely to happen.

Keywords

Further bibliographic information	Language
	Swedish
ISSN: 1650-1942	Pages: 19
Distribution: By sendlist	Price: Acc. to pricelist Security classification: Unclassified

Innehåll

1. Inledning

Inom försvarsmakten tillverkas det ett stort antal scenarier på olika sätt och med olika format. Att detta är ett såpass vanligt förekommande arbetsredskap beror sannolikt i hög utsträckning på att det är ett enkelt och effektivt sätt att fokusera tankar och idéer mellan och inom arbetsgrupper av olika storlek. Man kan med ett scenario relativt enkelt hålla fokus i en diskussion eller ett samarbete utan att för den skull behöva genomföra en verklig övning, vilket kanske inte är genomförbart över huvud taget.

En gemensam egenskap hos alla de scenarier författaren sett är dock att de beskriver ett händelseförlopp på en relativt hög nivå. Vi har tidigare försökt använda dessa som fokus för vår tekniska forskning, men det har visat sig att den övergripande nivån gör att vi haft svårt att på ett effektivt sätt kunnat föra in våra tekniska resonemang [1]. Vi har därför i denna rapport försökt oss på ett annat angreppssätt genom att tillverka egna scenarier som beskrivs på en nivå där vi känner oss mer bekväma. Förhoppningen är sedan att vi enklare skall kunna anpassa våra beskrivningar med scenarier från andra discipliner.

1.1 Syfte

Syftet med denna rapport och försöket att formulera scenarier på en teknisk nivå är att rapporten skall kunna fungera som underlag i det fortsatta arbetet med inriktning av projektet i interna workshops och i referens/styrgruppsarbete. Det är också författarens förhoppning att vi med hjälp av denna ansats skall komma lite längre i arbetet med att kunna koppla försvarsmaktens typscenarier och andra liknande arbeten till innehållet i forskningen på vår tekniska nivå. Man kan också i viss mån använda den som underlag vid diskussioner om vad IT-krigföring är och om de mekanismer som beskrivs i denna rapport är rimliga antaganden om en trolig framtid.

1.2 Avgränsningar

Eftersom syftet med rapporten har varit att ge några exempel och att experimentera med formerna så har fokus legat på beskrivningarnas nivå och typ av händelser. Innehållet i händelseförloppen har därför tillåtits växa fram ur relativt ostrukturerade diskussioner inom gruppen. Vi har inga ambitioner att i det här tidiga skedet kunna spänna upp hela utfallsrummet av möjliga händelseförlopp. De scenarier vi presenterar här får därför ses som just exempel.

Scenarierna är beskrivna ur den försvarande sidans perspektiv med fokus

på de tekniska systemkomponenter som är inblandade. Konsekvenserna på ett högre plan har inte beaktats mer än tämligen ytligt och då endast med avseende på tekniska konsekvenser.

Vi har också valt att studera situationer som beskriver en i grunden defensiv verksamhet där de offensiva inslagen i allt väsentligt är reaktioner på motsidans angrepp. Man kan i och för sig tänka sig rent offensiv CNO, men om detta är något som är lämpligt är mycket mer en politisk och folkrättslig fråga än en teknisk och vi har därför valt att inte beröra dessa aspekter i denna rapport.

Den miljö som är omgivning till scenarierna är ett NBF byggt på vad som skulle vara möjligt att skapa med dagens teknik, både vad gäller den försvarande som den anfallande sidan. Man kan förutse att styrkeförhållandet kommer att vara konstant i ett längre perspektiv även om de tekniska komponenterna kommer att se helt annorlunda ut. Skälet till detta val är naturligtvis att det är helt omöjligt att göra några förutsägelser om teknisk utrustning och dess styrkeförhållande på en så detaljerad nivå som det är fråga om här ens i det korta perspektivet.

Fredstida militära nätverk har inte studerats då hotbilden mot och skyddet av sådana inte skiljer sig nämvärt från vilka civila nätverk som helst. Det som är specifikt för militär verksamhet är operationer mot en tydlig och kompetent motståndare.

Att Sverige har valts som part skall inte tolkas som något annat än ett uttryck för författarens dåliga fantasi. Om Sveriges försvarsmakt kan eller bör operera på det sätt som beskrivs i rapportens olika scenarier är överväganden som görs på annat håll. Författaren har i denna rapport ingen tanke eller önskan att förespråka det ena eller det andra opererationsmönstret.

Hur skyddet av Sveriges IT-system är organiserat har inte heller beaktats. Rapporten använder istället de generiska beteckningarna CNO-förband, CNO-personal o.s.v. för att indikera att speciell personal används.

2. Bakgrund

Traditionellt militärt uppträdande bygger i hög grad på territoriellt tänkande på olika sätt med olika förflyttningar i denna teräng. Man talar t.ex. om att ha luftherravälde eller att kontrollera någon centralt placerad höjd för att förhindra framryckning i dalen nedanför.

IT-domänen som stridsrum är beskaffad på ett helt annat sätt. Noderna finns i den vanliga världen vilket kanske gör att man frestas att hantera även denna domän på samma sätt som de andra, men interaktionen mellan noderna i ett framtida nätverksförsvar (oavsett om vi kallar det för NBF, NCW eller något annat) gör att förflyttning och skalskydd får helt andra egenskaper än de vanliga.

Denna rapport försöker beskriva detta förhållande med några exempel på hur en framtida försvarsmakt skulle kunna utnyttja en CNO-förmåga.

2.1 Folkrättsliga aspekter

Författaren har ingen egen kunskap att bidra med på detta område mer än att man kan konstatera att IT-krigföring är ett outforskat och i högsta grad outrett område när det gäller denna aspekt. Man skulle nog snarast kunna kategorisera det som ett minfält som få stater har vågat sig ut i än. Speciellt nivå tre i de följande scenarierna har en omfattning av offensiv verksamhet som man nog i dagsläget svårligen skulle kunna tänka sig hos normala demokratier. Å andra sidan är det heller inte orimligt att tro att motståndet som en FN-gruppering framför allt kommer att möta inte har särskilt stora begränsningar i detta avseende utan tvärtom kommer att försöka dra full nytta av IT-krigföringens möjligheter. En djupare genomgång av folkrättsliga aspekter finns i [2]. I en nyligen genomförd internationell expertkonferens (International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17-19 Nov 2004 i Stockholm) var dock den allmäna meningen att åtminstone när en konflikt har övergått i direkta strider (Jus in Bello) så är CNA förenligt med folkrättsliga principer på samma sätt som andra krigshandlingar. I denna rapport kommer vi inte annat än undantagsvis att beröra dessa frågeställningar utan detta lämnas åt läsaren att själv ta ställning till.

3. Ram

Sverige deltar i en fredsbevarande internationell operation i Capzylien [3] på ett FN-mandat. Vi kan tänka oss att Capzylien den här gången ligger någonstans i centrala Afrika. Den förra regimen motsätter sig det nya styret (som valts i Capzyliens första fria val någonsin) och försöker med alla medel att återta kontrollen över landet.

Capzylska rebeller, som sympatiserar med den gamla regimen, finns framför allt grupperade i tre byar runt en större oljefyndighet i södra Capzylien. Man har även infiltrerat resten av samhället med agenter i stort sett överallt bland civilbefolkningen.

4. Scenario 1: Intrång och informationsstöld i egna system

Komponenenterna i detta första scenario är sådana som en systemadministratör från alla lite större organisationer skulle känna igen sig i och händelseförloppet är uppbyggt av element som författaren själv har upplevt i sin tidigare systemadministatörsgärning. Även de aktiva motåtgärderna är till stor del uppbyggt av metoder som redan används av nätverkstekniker. Skälet till denna likhet är naturligtvis att man i ett militärt nätverk i stor utsträckning använder systemkomponenter som bygger på samma standarder och principer som i ett civilt nät. Det som skiljer är framför allt två saker. Första skillnaden är att man finns i en miljö där vi vet att ständiga riktade störningar kommer att ske av kompetenta motståndare. I den normala, civila miljön kommer den stora mängden störningar att bestå av allmäna, oriktade angrepp som relativt enkelt detekteras och stoppas med brandväggar och andra tillgängliga skydd. När det gäller riktade och mer planerade angrepp är en starkt återhållande faktor att dessa i civil miljö är olagliga med medföljande risker för upptäckt. Den andra skillnaden mot civil verksamhet är att man i en militär operation på den försvarande sidan har en större palett av aktiva motåtgärder att ta till. Här börjar vi dock att närma oss ett område där svåra avvägningar måste göras. Av denna anledning är scenarierna i denna aspekt uppdelade i olika nivåer av aktiva motåtgärder. Författaren har som tidigare nämnts inga ambitioner att i denna rapport förespråka någon nivå som lämpligare än de andra.

4.1 Bakgrund

En uppmärksam tekniker i ett artillerikompani hittar en process i sitt ordergivningssystem som han inte känner igen. När han skulle stänga av smartcardläsaren för uppdatering upptäckte han att processen inte försvann trots att läsaren var avstängd. Efter en stunds funderande inser han att processen han tror är smartcardläsaren heter scardsrr.exe istället för scardsvr.exe som den borde ha hetat. Ett telefonsamtal till IT-supporten på en högre stab får CNO-enheten att inleda trojanjakt.

Kommentar Att man av en händelse upptäcker intrånget på detta sätt förutsätter att intrånget skett i en vanlig dator och att den lokala operatören dels har en hög kompetens på sitt system, dels har rättigheter som lokal administratör. De utvecklingstendenser man ser idag gör att denna aspekt av systemadministration 'hands on' kommer att bli ovanligare. Speciellt gäller detta för inbyggda system där operatören inte har någon

aning om vad som händer på processnivån. Under alla omständigheter måste vi i alla fall förutsätta att vi på någon nivå kommer att ha övervakning av våra nät, både med personal och tekniska hjälpmedel i form av intrångsdetekteringssystem. Man kan tänka sig att den här typen av anomalier antagligen förr eller senare kommer att upptäckas av dessa.

4.2 Händelseförlopp 1

4.2.1 Rules of Engagements Enbart egna system hanteras. Inga offensiva IT-förmågor används.

4.2.2 Händelsekedja

1. Processen och programmet är inte känt sedan tidigare och finns inte med i referenssystemet hemma. Man drar slutsatsen att detta troligen är en trojan. En kopia plockas ut av CNO-personal för undersökning.

   Kommentar Att bara hämta ut en kopia av den exekverbara filen för undersökning skulle kunna göras på distans över nätverket, men man vet då inte om allt följer med eller om den har manipulerat resten av systemet för att dölja sina funktioner. Ett bättre sätt skulle vara att göra en kopia på hela hårddisken och att studera kopian med olika forensiska verktyg. Viktigt för att lyckas med denna utredning är tillgång till personal som både har en djup specialistkunskap om operativsystemet och har detaljerad kunskap om hur systemet är tänkt att fungera i sin normala miljö.

2. En sökning via IDS-monitorerna på systemen visar att denna process finns på en oroväckande stor del av de svenska systemen i Capzylien.

   Kommentar Här har vi förutsatt ett intrångsdetekteringssystem (IDS) som kan kontrollera olika aspekter på noderna på vår sida samt att dessa kommunicerar i ett kontrollnät. Det är inte orimligt att tro att ett sådant system i närtid kommer att finnas i någon enklare, signaturbaserad form byggd på befintlig teknik. Även om man har ett signaturbaserat system, som i det här fallet har ställts in att detektera just denna process, så kan man också också tänka sig att det var detta system som initialt upptäckte intrånget. Om angriparen råkat placera trojanen på ett system där den är tillräckligt avvikande för att detekteras av IDS-systemet, så skulle det kunna vara en alternativ inledning av scenariot.

3. IDS-monitorerna på några av de drabbade systemen ställs in att monitorera kommunikationen hos just dessa processer.

4. Man noterar att processerna med jämna mellanrum öppnar en förbindelse till informationsavdelningens webtjänst och hämtar nyhetsnotiser där. Misstankarna om att detta verkligen är en trojan stärks.

5. Informationsavdelningen finns inhyst i ett hotell i Capztown och man har byggt om en skrubb till serverrum. CNO-personal hittar vid en fysisk inspektion av webservern i fråga en oauktoriserad kabel mellan printerportarna på denna dator och en dator man använder för personalens internetaccess. Datorn för internetaccess tas omedelbart ur drift och den stängs av. Den tas med av CNO-personalen för undersökning. En kopia av webserverns disk görs också för undersökning.

   Kommentar Här ser man tydligt effekerna av IT-domänens annorlunda beskaffenhet. En informationsenhet har inte alls samma fysiska hotbild som andra delar av nätet och man har av den anledningen använt civila lokaler och civilanställd personal. Motståndaren har valt att införa en fysisk förbindelse istället för att logiskt manipulera någon koppling mot omvärlden som vi själva infört. Man kan tänka sig att det finns dylika kopplingar mot t.ex. civila myndigheter, koalitionspartners eller helt enkelt en förbindelse till FMIP i Sverige. De medvetna kopplingarna är dock betydligt bättre skyddade och monitorerade så det var antagligen säkrare att skaffa sig en egen nu när man hade möjlighet. Intrången i webbservern och internetdatorn (den som användes för personalens internetaccess) underlättas också i hög grad av att man har tillgång till en insider. Att man efter upptäckt hanterar webbservern och internetdatorn olika beror på att den normala verksamheten är mer beroende av webbservern än av att personalen kan koppla upp sig mot vanliga internet.

6. Undersökningen av den ursprungliga trojanen visar att denna har kopierat alla order som passerat ordergivningssystemet och sparat dessa i oallokerade block på hårddisken. Med jämna mellanrum har den skickat dessa data dolda i webbkommunikationen. Man noterar också att klienterna har börjat skicka webbfrågor till ett speciellt persedelförråd istället.

   Kommentar Den här detaljnivån i undersökningen av trojanerna kräver dels specialister på en nivå som det inte finns speciellt många, dels en viss tid. Man måste nog räkna med att det tar åtminstone ett dygn innan ett användbart, första resultat kan vara klart.

7. Man fattar beslut att all ordergivning tills vidare skall ske via telefoni istället.

   Kommentar Detta är antagligen angriparens främsta syfte. Det är inte säkert att angriparen faktiskt lyckats få ut någon information från systemen, det är bara nödvändigt att skapa en misstro som gör att svenskarna övergår till långsammare och sämre övade kommunikationsmedel.

8. Genom att titta i loggarna för internetaccessen kan man se att informationsavdelningen, och nu även persedelförrådet, visar ett onormalt stort intresse för en gymnasieskola i Sydkorea. Det finns en amerikansk bas

i närheten och man ber via FN dessa ta kontakt med skolan morgonen efter. (Det är natt i Korea nu)

Kommentar Varför Amerikansk militär och inte Koreanska myndigheter? Sannolikt är det lättare att via sina koalitionspartners få kontakt med andra militärer än med en myndighet vars övergripande struktur man inte känner till.

Vi ser här ytterligare ett exempel på gränslösheten i internettekniken. Lite tillspetsat skulle man kunna säga att alla konflikter med ett inslag av datorkrigföring förvandlas till världskrig.

9. Undersökningen av trojanerna i svenska webbservrar och genomgång i nätet efter fler visar att man hittar tre till av samma typ i vilande läge. Om det finns andra versioner går inte att veta.

10. En snabb genomgång av webbloggarna visar att all ordergivning i systemet de senaste 15 dagarna måste anses som röjd.

11. Amerikanska experter lyckas tillsammans med gymnasieskolans tekniker (extraknäckande student) hitta en bakdörr i gymnasieskolans webbserver på förmiddagen den följande dagen. Inga indikationer på vem som använde denna bakdörr går dock att finna.

    Kommentar Om skolan släpper in Amerikanerna i sina servrar är väl inte helt säkert, men författarens erfarenhet är att med hjälp av lite vänlighet och diplomati möts man i det flesta fall av hjälpsamhet i den här sortens situationer. Större organisationer kanske inte skulle släppa fram vem som helst till sina terminaler, men här kan man förutsätta att de skulle ha egen kompetens att sätta in och att man delar med sig av resultatet. Att man inte kommer längre i undersökningen här beror på att angriparna noterat att man blivit upptäckta och därför avlägsnat alla spår efter sig. Man har haft relativt gott om tid på sig.

4.3 Händelseförlopp 2

4.3.1 Rules of Engagement Offensiv CNA tillåten i begränsad utsträckning direkt mot opposition.

4.3.2 Förändringar mot tidigare händelsekedja

1. Trojaner i systemet tillåts vara aktiva, men med skillnaden att endast vilseledande order läggs in i systemet.

   Kommentar Om detta operationsmönster är en följd av ett mer offensivt inriktat RoE är nog tveksamt. Att göra på det här sättet är antagligen en rimlig idé under alla omständigheter, om det bara är möjligt.

2. De amerikanska experterna hittar tillsammans med gymnasieskolans tekniker en aktiv koppling från ett internetkafe i Capztown.

Kommentar Nu har vi lurat motståndarna att behålla kopplingarna bakåt så att vi fortfarande kan spåra dom. Möjligen skulle man som angripare hoppa mer än ett steg och dessutom ha som rutin att städa upp efter sig efter varje uppkoppling för att försvåra spårning.

3. CNO-förbanden avlyssnar kommunikationen vid detta internetkafe och kan se att det är en klient på kanal 13 i WLAN-nätet som är den man söker. Denna pejlas snabbt in av telekrigsenheten till en lägenhet i närheten.

   Kommentar Här har vi antagit att Internetkafét även driver en trådlös WLAN-hotspot (WLAN kommunicerar på ett antal kanaler).

4. Motståndnästet bekämpas med konventionella metoder.

4.4 Händelsesförlopp 3

4.4.1 Rules of Engagement Offensiv CNA tillåten utan begränsningar.

4.4.2 Förändringar mot tidigare händelsekedja

1. När gymnasieskolan i Sydkorea identifierats görs ett intrång i denna och den tas över.

   Kommentar Att genomföra ett intrång i en specifik server helt utan förberedelser måste nog betraktas som oerhört svårt. Predikterbarheten i resultatet är dessutom liten. Intrångsförsöken kan lika gärna resultera i att motståndarna inser att man är upptäckt och sopar igen spåren. Å andra sidan kanske servern finns placerad i något land där man inte kan förvänta sig någon samarbetsvilja och detta är då den enda möjligheten att komma vidare.

2. Man hittar kopplingen mot internetkafet.

3. Resten som i händelseförlopp 2.

5. Scenario 2: Kommunikationsstörning av koalitionspartner

Detta andra scenario är relativt likt det första scenariot, men innehåller mer interaktion med telekrigsförband. Vi får här ytterligare ett exempel på att skyddet har andra gränser än de normala. Detta gäller i extra stor utsträckning när vi använder olika trådlösa lösningar.

5.1 Inledning

Mitt under en gemensam aktion mot en av byarna vid oljefälten får man besked från belgiska enheter att man har stora problem i sitt datornätverk och att man har spårat ursprunget till svenska datorer. Man kommer tills vidare att koppla bort den direkta datorkommunikationen till de svenska styrkorna. All kommunikation måste tills vidare ske via alternativa kanaler.

Kommentar Det är idag ovanligt med direkt kommunikation mellan olika koalitionspartners på detta sätt i operativ verksamhet, men det är nog bara en tidsfråga innan vi får fler hopkopplade nät. Ett rimligt skydd här skulle kunna vara att man via brandväggar kopplar sig till ett litet gemensamt nät med något meddelande/kommunikationssystem. Vi kan då tro att problemen håller sig till detta gemensamma nät, men man kommer ändå att skylla på och spåra ursprunget till svenskarna.

5.2 Händelseförlopp 1

5.2.1 Rules of Engagements Enbart egna system hanteras. Inga offensiva IT-förmågor tillåtna.

5.2.2 Händelsekedja

1. CNO-personal kan snabbt konstatera att de IP-nummer man fått från belgarna allihop kommer från en svensk underhållsbataljon grupperad i ett skogsparti 30 mil söder om oljefälten.

   Kommentar Här ser vi ännu ett exempel på att det är delen med lägsta säkerhetsnivån som sätter nivån för hela nätet. I allmänhet har man nog ambitionerna att hela nätet skall hålla samma höga nivå, men i stora nät finns det alltid någon enhet som slarvar.

2. Ingen av de utpekade datorerna uppvisar dock något onormalt beteende och IDS-monitorerna på de utpekade datorerna uppvisar heller inget

av trafiken man sett hos belgarna. Man misstänker att den skadliga trafiken injiceras någonstans på vägen.

3. Det interna nätet i bataljonen är radiobaserat och man pejlar snabbt in alla positioner av sändare. Det visar sig att ett 30-tal sändare finns i buskage och annan teräng omedelbart utanför grupperingen.

   Kommentar Att få externa noder att injicera trafik i ett nät utan att de ordinarie noderna blir förvirrade måste anses som relativt besvärligt, även om det inte är helt otänkbart att det går. Ett större problem för angriparen i det här fallet är nog att radionätet med största sannolikhet är krypterat. Man måste då ha antingen hittat en sårbarhet i just denna kryptolösning eller att genom någon form av infiltration lyckats stjäla svenskarnas kryptonycklar.

4. På de indikerade positionerna samlas ett antal lådor in.

5. De visar sig innehålla en GSM-telefonmodul, en radiomodul för det svenska trådlösa systemet och ytterligare en radiomodul, antagligen till för att sätta upp ett eget kommunikationsnät mellan sig.

   Kommentar Under förutsättning att vi använder någon form av COTS för vårt nät så skulle en sån här utrustning vara i det närmaste trivial att konstruera. Den enda svårigheten kommer från att lyckas bryta kryptot i det svenska nätet.

6. Tyvärr visar det sig att alla noderna var inställda att radera intern information när de flyttas så ursprunget går inte längre att utröna.

   Kommentar Ett naturligt beteende som man nog får förutsätta är implementerat. Man får också förutsätta att motståndarsidan initierar detta på avstånd för alla noderna så fort man får bekräftat att en nod är hittad.

5.3 Händelseförlopp 2

5.3.1 Rules of Engagement Offensiv CNA tillåten i begränsad utsträckning direkt mot opposition.

5.3.2 Förändringar mot tidigare händelsekedja

1. Vid pejlingen hittas även GSM-trafik.

   Kommentar Telekrigsresurser kommer antagligen att upptäcka detta relativt enkelt. Om man å andra sidan använder standardutrustning för att lokalisera sina egna noder, t.ex. har WLAN-nät standardutrustning för detta, så är det rimligt att man har kört denna utrustning kontinuerligt. Inkräktarnoderna skulle då ha upptäckts i ett mycket tidigare skede.

2. Med hjälp av lokal polis och div. operatörer spåras GSM-trafiken (GPRS) till internetkafét.

Kommentar Förutsätter naturligtvis att det finns en vänligt inställd lokal polis och en samarbetsvillig GSM-operatör. Detta är inte en helt självklar förutsättning.

3. Genom att ägaren till internetkafét talar om vilken klient det är som har det aktuella IP-numret så kan lägenheten från första scenariot pejlas och cellen oskadliggöras.

   Kommentar Se kommentaren på förra punkten.

5.4 Händelsesförlopp 3

5.4.1 Rules of Engagement

Offensiv CNA tillåten utan begränsningar.

5.4.2 Förändringar mot tidigare händelsekedja

1. När GSM-kommunikationen upptäckts så avlyssnas länken mellan basstationen och operatören varvid internetkafét kan identifieras.

   Kommentar Anledningen till att man väljer att avlyssna denna trafik istället för den direkta trafiken mellan noden och basstationen är att mikrovågslänkarna i normalfallet inte är krypterade medan trafiken mellan telefonerna och basstationen oftast är det. Åtminstone säger vissa källor så. Andra källor påstår att även denna trafik naturligtvis är krypterad. Det troligaste är väl som vanligt att det beror på både länkleverantör och operatör hur tillgänglig trafiken i dessa länkstråk är.

2. Lägenheten pejlas in och istället för att göra ett direkt tillslag så gör man ett eget intrång i motsidans system och tömmer detta på användbar information innan tillslag sker.

   Kommentar Här ingår det också en avlyssning av trafiken vid internetkafét för att identifiera målet. Här kan även vår sida dra nytta av Internets gränslöshet. Vårt intrång kan lika gärna göras av specialister hemma i Sverige som från telekrigsbussen utanför internetkafét.

   En annan avvägning man får göra i detta skede är att ett intrång i enskilda system på detta sätt är både svårt och vanskligt. Det finns stora risker att man genom dessa försök röjer sig och att motsidan hinner städa bort alla spår av sin verksamhet. Ett alternativ är att göra det fysiska tillslaget på ett sätt som ger tillgång till motståndarnas utrustning.

6. Slutsatser

Även i arbetet med dessa scenarier ser vi att vårt tekniska angreppssätt är svårt att koppla till andra scenarier på ett naturligt sätt. Skillnaden i koncepts- och föreställningsvärld är inte triviala att överbrygga. Vi tror dock att vi med denna rapport är på rätt väg och att vi med dessa beskrivningar som utgångspunkt skall kunna hitta fler beröringspunkter mellan disciplinerna. Största skillnaden är fortfarande att våra scenarier är självständiga och relativt småskaliga utan speciellt många kopplingar utanför IT-domänen. Typscenarier å andra sidan förväntas innehålla en överblick som gör att man inte bottnar i några detaljer över huvud taget. Det huvudsakliga målet med detta arbete måste fortsätta att vara att hitta skärningsytorna mellan tekniska och övergripande scenarier, även om vi fortfarande misstänker att dessa skärningsytor är relativt små. Att de är små betyder dock inte att de är ointresanta utan bara att de är svårare att identifiera. En annan självkritisk fråga man måste ställa sig är om den här typen av scenariobeskrivningar fyller sitt syfte. Tekniska scenarier kanske bättre beskrivs av olika experiment med riktiga system. Kanske behöver vi hitta någon balans mellan att utföra experiment och sedan sätta in dessa i ett sammanhang med den här sortens beskrivningar? Detta är den sortens frågeställningar vi får fortsätta att arbeta med inom projektet.

Litteraturförteckning

[1] M. Karresand, M. Persson, and D. Lindahl, "Scenarion och trender inom framtida informationskrigföring ur ett tekniskt perspektiv," Institutionen för Systemutveckling och IT-säkerhet, Avdelningen för ledningssystem, Totalförsvarets forskningsinstitut, Box 1165, 581 11 Linköping, Tech. Rep. FOI-R–1283–SE, June 2004.

[2] C. Hellman, *IT-krigets lagar*. Försvarshögskolan, 2004.

[3] M. Wedlin and D. Lindahl, "It-vapen i laborativ miljö (dvd)," Institutionen för Systemutveckling och IT-säkerhet, Avdelningen för ledningssystem, Totalförsvarets forskningsinstitut, Box 1165, 581 11 Linköping, Tech. Rep. FOI-R–1056–SE, Dec. 2003.