Kandidatarbete i Datavetenskap 10p C-nivå
Blekinge Tekniska Högskola IT99.
Institutionen för programvaruteknik och datavetenskap

Ronneby VT 2002

InformationsKrigföring

– Den *nya teknikens* hot -

Författare: **Dennis Jönsson**
Ted Stålhammar
Handledare: **Göran Gustafsson**

Abstract

The new information society has revolutionised almost the entire world. But the new technique does not only bring good. That which was before only available on paper may today only be available on a computer system. This makes it possible to send data electronically. In the wrong hands that information can become a threat against the security of an individual, a company or even a nation.

The possibility to protect oneself against attacks from the outside becomes increasingly difficult. There are a lot of factors involved but a major factor is the fast technical development we now see within this area. Our defence minister, Björn von Sydow, writes in an article that it is almost impossible to protect one self against the unexpected. Björn Andersson (SÄPO) says as well that there are no secure systems, only more or less easy penetrable systems for the attacker to attack.

The threat against Sweden is quite diffuse. The old threat of invasion is no longer which can make it difficult to identify a specific threat. The word of the governments today is terrorism.

The purpose of our paper, considering this background, is to take a look at the possible threats against swedish information systems and to see the seriousness of the threats these systems are facing. It mainly consists of systems for ensuring we are provided with power and water and that finance and communication works.

The questions that we ask ourselves are if information warfare indeed is a threat ? Who are the attackers and what drives them to perform the actions they perform ? Which are the targets they aim their attacks against ? Are the techniques behind information warfare realistic and is there really a threat, or is it all just blown out of proportions ?

To get answers to our questions we have gone through a lot of material. A lot of it was downloaded from the Internet and has been of varying character. We have also been given a lot of material from our government and we have read some literature about the area of interest. We have finally done some interviews with staff from Lunds Energi, Skanova Networks and Säkerhetspolisen.

Sammanfattning

Det nya informationssamhället har revolutionerat nästan hela världen. Men det är inte bara rosor den nya tekniken medför. Det som tidigare bara funnits på papper finns kanske idag i ett datoriserat system istället. Detta medför att datan kan skickas vidare elektroniskt. I fel händer kan informationen bli ett hot mot säkerheten mot en individ, ett företag eller till och med ett land.

Möjligheten att skydda sig mot attacker från utomstående angripare blir allt svårare. Det finns många faktorer inblandade men en stor bidragande faktor är den snabba tekniska utveckling vi nu ser inom detta område. Vår försvarsminister, Björn von Sydow, skriver i en artikel att det är nästintill omöjligt att skydda sig mot det oväntade. Samtidigt säger Björn Andersson (SÄPO) att det finns inga säkra system. Bara mer eller mindre svårare system för angriparen att angripa.

Hotet mot Sverige är ganska diffust. Det gamla invasionshotet finns inte längre kvar vilket gör att det kan vara svårt att identifiera ett specifikt hot. Det ord regeringar i industriländer talar om idag är terrorism.

Syftet med vår uppsats, med tanke på denna bakgrund, är att se på de eventuella hot som finns mot svenska informationssystem och se på graden av det hot som dessa system ställs inför. Det gäller i huvudsak system för drift av el-, vattenförsörjning, bank/finansväsendet samt kommunikation.

De frågor vi ställer oss är ifall informationskrigföringen är ett hot över huvud taget ? Vilka är utövarna av denna teknik och vad är det som driver dem till de handlingar de utför ? Vilka är de mål som de riktar sina attacker mot ? Är tekniken bakom informationskrigföring realistisk och finns det verkligen ett hot, eller är detta bara ett luftslott ?

För att få svar på våra frågor har vi gått igenom en hel del material. Mycket av detta material har hämtats från Internet och har varit av varierande relevans. Vi har också tagit del av en hel del material från Regeringskansliet och läst en del litteratur inom området. Vi har slutligen också genomfört intervjuer med personal från Lunds Energi, Skanova Networks samt Säkerhetspolisen.

Förord.

Vi har i arbetet med denna uppsats kommit i kontakt med en del personer som hjälpt oss med information, dels genom intervjuer dels genom rapporter som skickats till oss.
Vi vill tacka kriminalinspektör Björn Andersson på Säkerhetspolisen (SÄPO) för givande aktuell information.
Tack också till Lunds Energi och till Skanova Networks för svar på frågor.
Tack till Istvan Zsiga på Värnpliktsnytt för de aktuella reportagen från tidningen och visat intresse.
Tack till vår svenska försvarsmakt för alla broschyrer och rapporten.

Ett stort personligt tack till Johan Jönsson för all hjälp vi fått med vår uppsats.

Tack till er som visat intresse om arbetet vi jobbat med.

Dennis Jönsson &Ted Stålhammar

Innehållsförteckning

1. Inledning.

1.1 Bakgrund

Det moderna IT-samhället har skapat nya möjligheter, men samtidigt som systemen blir mer och mer komplexa ökar även deras sårbarhet. Den traditionella formen av frontkrigföringen minskar vid militär planering. Landsgränserna har ingen betydelse längre då fientliga IT-förband kan förstöra både militära och civila ledningssystem utan att ens vara i närheten. Fenomenet *terrorism,* som det idag talas mycket om, kan förknippas med den nya IT-tekniken. Terrorister har idag nya möjligheter att skapa kaos och utpressning. Små minoritetsgrupper kan utmana stormakter.

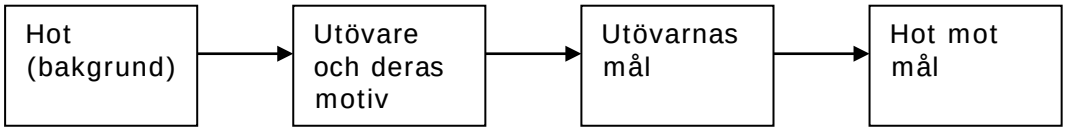
Informationskrigföring handlar både om att skydda de egna informationssystemen mot angrepp, och om att kunna angripa motståndarens system för att manipulera eller förstöra värdefull information. Nackdelen är att utvecklingen har gått i ett sådant rasande tempo att informationssäkerheten inte hunnit med eller till och med blivit helt bortglömd. Effektiv informationskrigföring skulle därför kunna vinna kriget innan det ens hunnit börja.[1]

Det digitala informationssamhället har blivit utsatt för en ny typ av terror från cyberrymden. Detta är ett hot som växt fram i den dataålder vi lever i. På bara några år har Internet blivit den gränsöverskridande kanalen. En kanal som används på både gott och ont.[2]

Vid en intervju med kriminalinspektör Björn Andersson (SÄPO) fick vi bekräftat att Informationskrigföring är ett ämne som borde behandlas mer. Samhällets hotbild ser idag inte längre ut som den har gjort.

1.2 Teori

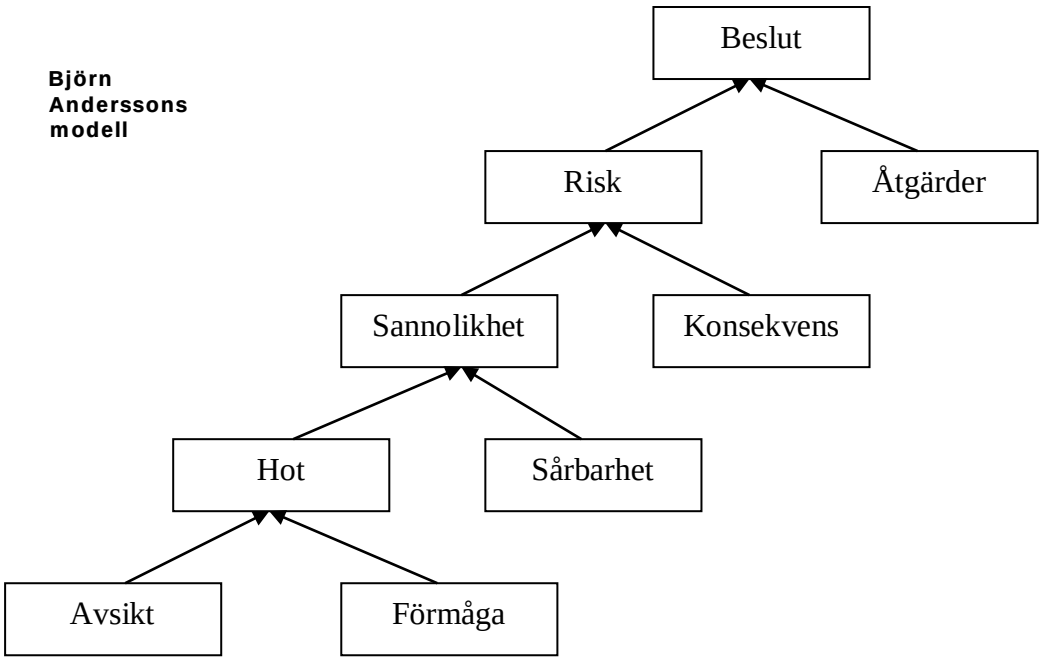
Vi kommer att arbeta utifrån nedanstående teori, eller modell, för att besvara vårt problem och uppfylla vårt syfte.



Observera att detta inte är någon vedertagen modell utan en modifierad modell vi kommer att använda oss av för att få en röd tråd i vår uppsats. Varje del av modellen har sitt innehåll ifrån både teori och empiri.

Den modell som ligger till grund för vår egen modifierade modell är den modell vi tagit del av under vår intervju med Björn Andersson från SÄPO. Här har vi lyft ur de delar som vi anser vara relevanta för att uppfylla syftet med vår uppsats. Vi kan då som vi nämnt erhålla en röd tråd för såväl läsaren som för oss själva under arbetets gång.

[1] Arbetsgruppen om informationskrigföring, 1997, s 8 f
[2] Hagen Fahlén, 1999, s 1



Med den bakgrund vi finner, d.v.s. i tekniken bakom informationskrigföring, kan vi gå vidare för att identifiera de utövare som finns inom detta område. Vet vi sedan vilka utövarna är bör vi också kunna utröna vilka motiv dessa har till sina handlingar. Detta ger oss förhoppningsvis en inblick i vilka tänkbara mål dessa då har. Vet vi vad som driver dem, exempelvis pengar, vet vi att bankerna är tänkbara mål. Det är först när vi kommit så långt som vi kan utröna ifall det finns tekniker som dessa utövare kan använda sig av för att hota ett system.

1.3 Problem

Idag är informationsflödet enormt högt via de nätverk som finns tillgängliga för såväl privatpersoner som för företag. Vad vi vill veta är hur allvarlig sårbarheten är på dessa nätverk, vad det finns för möjligheter inom informationskrigföringens ramar att angripa system som upprätthåller viktiga samhällsfunktioner såsom elförsörjning eller vattenförsörjning.

Vi kommer också att titta på utövaren för att kunna se vilka motiv och mål denna kan ha. En utövare kan ju exempelvis vara ute efter pengar, men är det då så självklart att målet är en bank ? Vi måste alltså se vad det är som driver en utövare för att identifiera tänkbara mål, detta är inte alltid självklart.

Är dessa handlingar realistiskt genomförbara ? Vad vi vill se är om det finns ett hot mot informationssystem eller om hotbilden endast är ett luftslott.

1.4 Frågeställningar

För att besvara vårt problem har vi identifierat följande frågeställningar:

- Är informationskrigföringen ett hot och vilka är utövarna, deras motiv och mål ?
- Finns det en realistisk hotbild mot dessa mål ?

1.5 Syfte

Syftet är att uppmärksamma det/de eventuella hot som finns mot olika informationssystem i dagsläget. Vi vill utreda ifall det finns ett hot och i så fall hur allvarligt det är. Vi vill alltså se om det idag finns ett hot mot svensk säkerhet.

1.6 Målgrupp

Vi vänder oss till säkerhetsansvariga för att visa på hur hotet ser ut i dagsläget och om dessa hot kan ha konsekvenser. Med säkerhetsansvariga menar vi de som på företag och myndigheter runt om i landet ansvarar för att skydda informationssystem mot intrång och attacker. Rapporten vänder sig även till övriga personer som är intresserade om området.

1.7 Avgränsning

Vi avgränsar begreppet ”samhälle” till den del som endast berör Svenska Totalförsvaret och koncentrerar oss på hot och attacker mot svenska intressen. Exempel från andra länder än Sverige kommer dock att finnas med i arbetet. Oundvikligt är också att använda företag för att exemplifiera i olika situationer.

Vi begränsar hotbilden till el-, vattenförsörjning, finans/bankväsendet och kommunikation (telefoni, Internet). Detta för att dessa områden är de områden som av Björn Andersson på SÄPO anses vara de områden som ska prioriteras eller som är de som har mest omfattande konsekvenser. Vi begränsar oss också till att endast behandla de datasystem som används i syfte att driva dessa funktioner.

Vi begränsar också oss till de tekniker för angrepp som vi ansett oss hinna med, detta på grund av att det inte finns tillräckligt med tid för att diskutera alla de tekniker som finns idag. Dessutom finns det också angreppssätt idag som vi inte känner till varpå vi begränsar detta område.

1.8 Dispositon av uppsats

I kapitel ett redogör vi först och främst för uppsatsens bakgrund vilket leder fram till vår problemformulering. Vidare redovisar vi syfte och avgränsningar.

I kapitel två redovisar vi de metoder vi använt oss av och hur vi utnyttjat dessa.

I kapitel tre behandlar vi den teroretiska referensramen. Här förklarar vi de teoretiska bitarna i informationskrigföringen.

I kapitel fyra avser vi att studera verkligheten. Detta med hjälp av intervjuer utförda med SÄPO, Lunds Energi samt Skanova Networks.

Kapitel fem är en uppföljning av empirin i förhållande till teorin, det är här vi utför vår analys.

I kapitel sex redogör vi slutligen för våra slutsatser.

2. Metod

2.1 Övergripande arbetssätt

2.1.1 Undersökningsmetoder

Enligt Holme & Solvang[3] finns det två metoder som kan användas när man ska samla in data, nämligen en kvalitativ- och en kvantitativ metod. Metoderna kan användas var för sig eller en kombination av de båda.[4]

2.1.1.1 Kvantitativ metod

Den kvantitativa metoden är mer formaliserad och strukturerad. Den är till stor utsträckning präglad av kontroll från forskarens sida. Metoden avgör i större grad också vilka svar som är tänkbara, då forskaren ofta har standardiserade frågeformulär som respondenten svarar på. Uppläggning och planering kännetecknas av selektivitet och avstånd i förhållande till informationsskällan. Allt detta är nödvändigt för att kunna genomföra formaliserade analyser, göra jämförelser och pröva om de resultat som framkommit gäller de enheter forskaren önskar uttala sig om. Statistiska mätmetoder spelar en central roll i analysen av kvantitativ information.[5]

2.1.1.2 Kvalitativ metod

I en kvalitativ undersökning frågar forskarna ett fåtal kunniga respondenter. Målet är då inte att göra generaliseringar för en målpopulation, utan att försöka få ökad insikt i ett problem samt att beskriva detta. Forskarens mål är insikt snarare än statistisk analys. I motsats till kvantitativ metod görs inte urvalet med hjälp av någon statistisk metod och det är inte heller nödvändigt att urvalet är representativt för hela målpopulationen. Respondenterna har stor flexibilitet och uppmanas att uttrycka sig fritt.[6] Det centrala i denna metod är att forskaren genom olika sätt att samla in information, dels kan få en djupare förståelse av det problemkomplex som studeras, dels kan beskriva helheten av det sammanhang som detta inryms i. Metoden kännetecknas av närhet till den källa, från vilken forskaren får sin information.

I boken *Att utreda och rapportera* skriver Eriksson och Wiedersheim-Paul (1989, s 65) att när en undersökning görs med hjälp av en kvalitativ metod leder inte alltid resultatet till en ny teori eller ett nytt resultat, utan kan istället bekräfta en redan känd teori. Den typ av intervju forskaren bestämmer sig för att utföra kommer till viss del att vara beroende av det syfte och tema undersökningen har. För att få idéer om vilka områden som passar kan forskaren genomföra preliminära intervjuer och låta intervjun vara ostrukturerad, d.v.s. respondenten har stor frihet att tala runt omkring ett visst ämne. Behövs det sedan mer specifik information om något bör frågorna ha en viss struktur, för att forskaren rent konkret ska få svar på det han eller hon var ute efter.

[3] Holme. I M., Solvang. B K., 1991, s 84
[4] Aronsson. L., Eriksson. L, Wiedersheim-Paul. F., 1975, s 26
[5] Holme. I M., Solvang. B K., 1991, s 13 f
[6] Holme. I M., Solvang. B K., 1991, s 86

2.1.1.3 Fallstudier

Eriksson och Wiedersheim-Paul (1989, s 65) skriver om en typ av kvalitativ metod; fallstudier. En fallstudie är alltså en undersökning av en specifik företeelse, t ex ett program, en händelse, en person, ett skeende, en institution eller en social grupp. Fallstudien är också mer inriktad på förståelse och beskrivning av en process än på beteendemässiga följder. Författarna skriver vidare att en fallstudie även kan göras i en kvantitativ undersökning.

Gummesson (1985, s 53) skriver om två typer av fallstudier. Den första baseras på ett begränsat antal fallstudier och forskaren använder sedan dessa för att dra allmänna slutsatser. Det andra alternativet är att dra en särskild slutsats efter att ha studerat endast ett fall.

En fallstudie är en kvalitativ undersökningsmetod som sker på en mindre avgränsad grupp t ex en individ, en grupp individer eller en organisation. En fallstudie visar att en företeelse faktiskt finns och att en viss verksamhet fungerar.

För att samla in vetenskapligt material till en fallstudie kan all sorts information införskaffas, det går alltså lika bra med ett test som en intervju.[7] Insamlingsmetod väljs efter hur uppgiften ser ut.

Styrkan med fallstudien är att den gör det möjligt för forskaren att koncentrera sig på en speciell händelse eller företeelse och försöka få fram de faktorer som inverkar på företeelsen ifråga.[8]

Varje organisation har egenskaper som är gemensamma med andra organisationer, men kan också uppvisa drag som är unika. Den forskare som använder sig av fallstudiemetoden vill ha tag i dessa drag och egenskaper och visa hur de påverkar genomförandet av idéer i ett system eller hur de påverkar det sätt varpå en organisation fungerar.

Falltudie är en ypperlig arbetsteknik för att belysa nutida händelser och händelser som är verkliga. I fallstudien har vi använt oss av intervjuer.

2.2 Handgripligt angreppssätt

2.2.1 Arbetsgång

Valet av ämnet kom fram då vi läste en artikel i en månadstidskrift om cyberkrigföring. Artikeln handlade om hur ett tredje världskrig skulle kunna utspelas och hur den ”nya tekniken” skulle kunna användas. Denna artikel ledde till att vi började leta information om ämnet för att se om det fanns material nog till en uppsats.

Till en början ägnade vi mycket tid åt att leta information och att sålla denna information efter värde varpå vi kunde strukturera upp vårt arbete. Teorin hittade vi främst till att börja med på Internet. Det visade sig att det kommit ut en mängd rapporter inom området efter attentatet mot World Trade Center den 11 september 2001.

[7] Merriam. S B., 1994, s 74
[8] Bell. J., 1993, s 16

Vi valde också att införskaffa nyutgiven litteratur om såväl cyberkrigföring som informationskrigföring i allmänhet. Nästan all litteratur som fanns att tillgå var utländsk. Att hitta material skrivet på svenska var nästintill omöljigt och det vi fann var sällan relevant. Vi har även använt oss av annan litteratur som inte direkt ingår i arbetet utan som istället ska ses som instuderingsmaterial.

Den teoretiska informationsmängden var ändå så pass omfattande att vi i ett tidigt skede var tvungna att begränsa oss kraftigt. Syfte och avgränsning fick därför hög prioritet.

Efter att ha funnit ett klart avgränsat problem samt syfte började vi att författa vår teoridel, vilken många gånger har reviderats i syfte att få med väsentlig teori till vår uppsats.

Vi visste vad för slags information vi behövde och hade tillgång till och ville gärna knyta samman detta med verkligheten (empiri) och behövde alltså komplettera med uppgifter från såväl företag som statliga organ. Vi tog därför kontakt med en del företag och statliga organ såsom Lunds Energi och SÄPO.

De som valde att svara på våra frågor var Bo Bengtsson på Lunds Energi, Sten Svensson på Skanova Networks samt Björn Andersson från Säkerhetspolisen (SÄPO). Vi fick även ta del av en hel del material från Regeringskansliet, material som vi använt under vår teoretiska del.

Intervjuerna med Bo Bengtsson på Lunds Energi och Sten Svensson på Skanova Networks sköttes via mejl. Med Björn Andersson stämde vi ett möte och fick gott om empiriskt material genom honom.

2.2.2 Datainsamlingsmetoder

2.2.2.1 Sekundärdata

Sekundära källor innebär en tolkning av något som redan ägt rum och som baseras på en primärkälla, t.ex. en historisk händelse.[9] Här har vi fått bedöma sanningshalten och har gjort så med tanke på ursprung. För att minimera feltolkningar eller missuppfattingar har vi använt oss av ett flertal källor. Våra främsta källor är rapport nr.1 från Arbetsgruppen om informationskrigföring samt Hans Hagens och Jan Fahléns rapport ”*Informationskrigföring en definition*”.

Vi har under en längre tid samlat in sekundärdata och har gjort så från många olika källor. Största delen av våra sekundärkällor fann vi på Internet, detta då denna källa är så lättåtkomlig. Det gäller dock här att vara kritisk till källan, se begreppen validitet och reliabilitet 2.2.3.1 samt 2.2.3.2.

I övrigt har vi tagit fasta på de rapporter och material vi fått in från Regeringskansliet, en källa vi bedömmer vara trovärdig i allra högsta grad.

2.2.2.2 Primärdata

I Huvudsak har vi använt oss av den intervju vi gjorde med kriminalinspektör Björn Andersson från SÄPO. Detta för att knyta samman

[9] Bell. J., 1993, s 68

vår teoretiska del med verkligheten. Vi har med hjälp av Björn Andersson fått en förankring i empirin.

Övrig primärdata utgörs av kontakt via mail med Lund Energi och Skanova Networks samt faktiska händelser. Anledningen till att vi tog kontakt med dessa företag var att vi ansåg att informationen från Björn Andersson (SÄPO) behövde kompletteras.

2.2.2.2.1 Intervjuer

Vi valde att i första hand ta kontakt med företag och regeringsorgan via e-post för att inleda en kommunikation. På så sätt fick vi snabbt reda på vilka som var intresserade av att lämna ut information. Vi har därmed kunnat ställa följdfrågor till berörda parter när så behövts.

Vid kontakt med SÄPO visade Björn Andersson stort intresse och vi kom överens om att göra en besöksintervju. Fördelen med en besöksintervju är möjligheten att kunna ställa följdfrågor och att kunna klargöra missuppfattingar direkt. En negativ aspekt med besöksintervjuer kan vara att det blir svårt att ställa känsliga frågor, något som vi dock aldrig upplevde.

Intervjun med Björn Andersson från SÄPO utförde vi på Blekinge Tekniska Högskola. Vi inledde med att ställa ett par frågor till Björn Andersson som rörde de lite större områdena varpå vi hade möjlighet att ställa följdfrågor och mer precisera svaret. Följdfrågor kunde ställas direkt och missförstånd reddes upp direkt.

2.2.2.2.2 Mejlkorrespondens

De företag vi skötte kontakt med via mejlkorrespondens var Lunds Energi samt Skanova Networks.

Nackdelen med denna typ av ”intervju” är att det blir svårt att ställa följdfrågor vid oklara svar. Det är inte säkert att misstolkningar eller missuppfattningar kan elimineras.

Fördelen med denna metod är att det inte tar så lång tid och att respondenten kan svara när han/hon har tid. Respondenten har även gott om tid att tänka över sina svar.

När det gällde kontakten med både Lunds Energi och Skanova Networks sköttes denna korrespondens relativt smärtfritt. Att få svar från Skanova tog dock ganska lång tid då detta företag är betydligt större och har anställda som tyvärr har mindre tid över till att besvara frågor.

Lunds Energi besvarade dock frågor snabbt och var mycket intresserade av att kunna hjälpa till så gott de kunde.

2.2.3 Studiens trovärdighet

2.2.3.1 Validitet

Validitet är ett mått på om en viss fråga mäter eller beskriver vad man vill att den ska mäta eller beskriva. Om en undersökning inte är reliabel, har den inte heller någon validitet. Validiteten måste alltså bedömas via tolkningar av forskarens erfarenheter i stället för i termer av verkligheten.

Det är alltså inget som kan mätas, utan måste uppskattas. Oberoende forskningstyp är validitet och reliabilitet frågor som alltid går att åtgärda genom noggrann uppmärksamhet på grundläggande begrepp i undersökningen, hur datainsamlingen gått till, hur forskarna analyserat och tolkat informationen.[10]

2.2.3.2 Reliabilitet

Reliabilitet innebär att minimera felaktigheter och systematiska avvikelser. Reliabilitet är ett mått på i vilken utsträckning ett instrument eller tillvägagångssätt ger samma resultat vid olika tillfällen under lika omständigheter.[11]

I vår uppsats förbättras reliabiliteten genom en omfattande teoridel och en dokumentation av vårt tillvägagångssätt. Ytterligare en fördel är att vi är två personer som skriver uppsatsen vilket innebär att vi kan kontrollera varandra och använda varandra som ”bollplank”. Detta betyder att vi har funnit ett tillvägagångssätt för att minska risken för bearbetningsfel.

2.2.3.3 Brister i vår uppsats

Något tydligare exempel på hur en attack kan gå till och vad det är en angripare i huvudsak ger sig på vad gäller telecom-branchen kan inte ges då telecom-bolagen är mycket förtegna om detta. Det finns även en hel hel del av sådant material som är sekretessbelagt då detta bestämts av regeringen och telecombolagen i Sverige och respondenten kan därmed inte lämna ut denna information.

2.2.3.4 Källhänvisning

Vi använder oss löpande av fotnoter där fördjupningslitteratur har identifierats. I de fall vi använder oss av engelska uttryck har dessa ej översatts då det sällan finns något tydligt svenskt begrepp.

[10] Merriam. S B., 1994, s 175
[11] Bell. J., 1993, s 64

3. Teoretisk referensram

3.1 Definitioner av begrepp inom informationskrigsföringen

Begreppets formella definition är idag Information Warfare (IW). Det har förekommit viss kritik till benämningen på detta fenomen, främst på grund av att metoderna som används i informationskrigföring inte alltid kan kallas för krig. Gränsen mellan krig och icke-krig är i informationskrigföring mycket flytande.[12]

Informationskrigföring handlar om åtgärder för att komma åt, påverka eller utnyttja andra aktörers information och informationssystem, men samtidigt skydda sin egen information och sina informationssystem.[13]

Syftet med denna krigföring är att ge angriparen ett övertag mot sitt offer (försvararen). Föreberedelserna görs dolt och angriparen kan anfalla anonymt (om denna så vill). Offret kanske inte ens noterar att det rör sig om ett angrepp förrän efter en tid då det redan är för sent att handla. Skadan är redan skedd.

En övergripande definition av begreppet informationskrigföring nämns av *Dr John I Alger*. ”*Information warfare consists of those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary.*” [14]

Nicklas Hermansson på Värnpliktsnytt skriver att det inte är den starkaste som vinner, utan den smartaste. Angriparen kan vara vad eller vem som helst. Målet kan vara en enskild person, en organisation, ett företag, en religion, en myndighet eller en stat. Den som har informationsherraväldet överlever, dödar och vinner. Det gäller att hitta eller stjäla ny värdefull information och att skydda sin egen – som kan användas för att vilseleda motståndaren till att fatta ett felaktigt beslut.[15]

Med begreppet säkerhet menar vi att i så stor utsträckning som möjligt säkerställa drift av informationssystem. Detta innebär att intrång och attacker i största möjliga mån ska undvikas eller avstyras. Det innebär också att information ska skyddas från obehöriga.

3.2 Informationskrigföringens olika delar

Informationskrigföring delas oftast in i olika delar beroende på taktik och mål.

3.2.1 Ledningskrigföring

Denna del kallas oftast för C2W (Command and Control Warfare). Syftet med denna del är att påverka motståndarens förmåga att utöva ledning. Detta kan göras på två olika sätt. Den ena är att angripa motståndarens

[12] Hagen, Fahlén, 1999, s 1
[13] Arbetsgruppen om informationskrigföring, 1997, s 8 f
[14] Arbetsgruppen om informationskrigföring, 1997, s 10
[15] www.varnpliktsnytt.org/tidningar/2001/0114/reportage/reportage1.html, 2002-02-06

ledning och den andra är att angripa motståndarens ledningsförmåga att utbyta information med slagfältet.

Denna metod förknippas oftast med militär verksamhet. Men angriparen eller motståndaren behöver inte nödvändigtvis vara militär. [16]

3.2.2 Underrättelsetjänst

Informationsteknologin har inneburit stora förändringar och en revolution för underrättelsetjänsten. Informationsflödet har blivit större och öppnare. Med underrättelsetjänst gör man analyser av motståndaren och utifrån denna föreslå, eller till och med avgöra väpnade insatser. När statliga myndigheter i allt större utsträckning använder sig av civila kommunikationsnät ökar möjligheterna för underrättelsetjänsten, de kan numera få all sin sökta information i realtid. [17]

3.2.3 Telekrigföring

Denna del anses oftast som en bit av ledningskrigföringen. Telekrigföringen kallas även C3W (Command Control and Communications Warfare). Verksamheten telekrigföring innebär utnyttjande av elektromagnetisk energi för att påverka motståndaren eller som syftar till att minska effekterna av motståndarens utnyttjande av elektromagnetisk energi.[18]

Inom detta område används olika typer av störning av kommunikationsförbindelser, signalskydd för att förhindra eller försvåra för motståndaren att störa eller avlyssna densamma.

3.2.4 Psykologisk krigföring

Svenska Försvarsmaktens definition av detta begrepp är ”*Verksamhet som syftar till att påverka motståndarens militära chefer och förband på ett för våra avsikter gynnsamt sätt”*. Denna definition avser endast den militära verksamheten. Civila samhället kan också utsättas för denna krigföring, då använder angriparen informationskrigföring och media för att påverka befolkningens känslor för att få dem att göra eller inte göra vissa saker.

I denna metod används oftast media. Här säkerställer en part att media beskriver en bild som gynnar den egna sidans syfte, sant eller osant. Detta är ett sätt att ”skapa den sanning man vill”.[19]

3.2.5 Hackerkrigföring

Namnet hacker syftar till en ”IT-entusiast” som tar sig in till datorer som de inte förväntas få åtkomst till för att förstöra, komma åt, sprida eller ändra information.

Kategorin innefattar även användandet av tekniker, främst elakartad mjukvara för att förstöra, urarta, exponera informationssystem, både militära samt civila.[20]

[16] Hagen, Fahlén, 1999, kap3 s 1
[17] Arbetsgruppen om informationskrigföring, 1997, s 40
[18] Hagen, Fahlén, 1999, kap3 s 2
[19] Arbetsgruppen om informationskrigföring, 1997, s 40
[20] Hagen, Fahlén, 1999, kap3 s 3

3.2.6 Ekonomisk informationskrigföring

Detta är en mycket komplex typ av informationskrigföring och spänner över ett mycket vidsträckt spektrum av områden. Ekonomisk informationskrigföring skall inte förväxlas med ekonomisk krigföring, som innebär utnyttjande av tillgångar för att utöva makt mot annan part. Ekonomisk informationskrigföring går ut på att få tag på information i t.ex. databaser för att manipulera, stjäla eller på annat sätt utnyttja informationen för egen ekonomisk vinnings skull. Det är inte alltid lätt att avgöra om detta är en krigshandling eller om det bara är en brottslig handling.[21]

3.2.7 Cyberkrigföring

Uttrycket ”cyber” härstammar från ordet cyberspace, vilket kan definieras som datarymden. Det konstgjorda, datorskapade rummet eller elektroniska universum, som man befinner sig i när man kommunicerar via en dator. Internet är en del av denna rymd.

Cyberkrigföring handlar om att utnyttja detta ”rum” till förande, och förberedelser att föra, militära operationer enligt informationsrelaterade principer. Här avses störande eller förstörande av informations- och kommunikationssystem i bred bemärkelse, som en motståndare är beroende av för att kunna verka. Här inkluderas inte bara tekniska system utan även organisationsstrukturer.

Det finns en strävan att få reda på allt om motståndaren, exempelvis vill angriparen veta vem motståndaren är, var denna befinner sig, mål, syften och hot denna kan möta.

Särprägeln cyberkrigföring ligger i när tekniken utnyttjas för att skapa eller utnyttja befintliga verkligheter. En möjlighet är att återge en faktisk händelse i realtid för på en annan plats än där den händer i verkligheten.

I cyberkrigföring väljer angriparen oftast om han ska vara anonym eller ge sig till känna och lämna spår efter sig. Det kan hända att den angripne inte inser och märker att intrång skett.[22]

3.3 Utövare och deras motiv

Inledningsvis ansågs det att utövarna kom från så kallade ”skurkstater”. Vi kan idag urskilja att angriparen kan finnas överallt. Den amerikanske debattören Winn Schwartau har gjort en gruppindelning på aktörerna i tre klasser.[23]

3.3.1 Klass 1 – personrelaterad.

Angriparen ligger på en individbas. Denna klass berör angrepp mot en personlig individ, dvs. intrång i den personliga integriteten. Här räknas t.ex. intrång i databaser/kundregister där information om den angripne finns. Syftet kan vara utpressning, undanröjning eller rent ”nöje”

[21] Hagen, Fahlén, 1999, kap3 s 3 f
[22] Hagen, Fahlén, 1999, kap3 s 4
[23] Arbetsgruppen om Informationskrigföring, 1997, s 8

Angriparen tar reda på information från t.ex. kontokortnummer, mediciniska journaler, brottsregister i syfte att utpressa, publicera eller på annat sätt utnyttja detta.

Om det finns falsk information om dig i ett register, vad är det som säger emot att detta skulle vara sant? Tusentals databaser innehåller tillsammans en digital profil av var och en av oss. Datorer byter information om oss konstant. Att rätta till felaktig information är nästintill omöjligt. Det är med andra ord ganska lätt att förstöra en persons identitet.

3.3.2 Klass 2 – marknadsrelaterad.

Angriparen handlar på företag/organisationsnivå. Denna typ av krigföring handlar om konkurrensförhållande mellan bolag. Angriparen måste inte tvunget vara den närmsta konkurrenten utan kan även vara en nation mot ett bolag.

I klass två handlar det för det mesta om industriella och ekonomiska spionage. Ett företags affärshemligheter kan vara ovärderliga för företaget. Skulle dessa komma i fel händer kan företaget gå under innan de insett vad som har hänt.

Det finns också en möjlighet att sprida falska rykten om företaget. Med dagens spridning av information, kan skadan redan vara skedd innan bolaget hunnit dementera de falska uppgifterna.

3.3.3 Klass 3 – globalt relaterad.

Angriparen består av stater eller statliga intressen, här räknas även terrorism med. Denna typ av krigföring riktas mot multinationella industrier, globala ekonomiska maktstrukturer eller mot länder eller andra geopolitiska strukturer.

Angriparen försöker i denna klass att underminera en nations styrka, ostabilisera dess ekonomi och hota landets demokrati

Vid denna typ av krigföring suddas de egentliga geografiska avstånden mellan fiende och offer ut. Detta innebär att en part på andra sidan jorden kan utföra en attack mot någon på den andra sidan.

3.3.4 Angriparens motiv.

Michael Wilson har målat upp några tänkbara syften som en angripare kan ha:

- Förstöra befolkningens tillit till samhällets sociala och politiska struktur och kapacitet.
- Skada funktionen hos socialförsäkringssystemet
- Förstöra samhällsekonomin
- Överbelasta brottsbekämpande myndigheter
- Försätta informationssystem ur funktion

Dessa åtgärder grundar sig på gemensamma motiv hos grupper som kan vara såväl ideologiska som ekonomiska. Vidare kan hämnd också vara ett motiv till angreppet. Sökande av spänning, erkänsla eller en gruppidentitet kan vara ytterligare motiv till angrepp.

Wilson utgår från att den tänkta fienden kommer att välja att angripa de delar av samhället där samhället traditionellt inte har något varningssystem mot angrepp. En av de största taktiska fördelarna med informationskrigföring är att det är en lågintensiv verksamhet som kräver låga insatser i termer av personer och material. Det säkraste sättet för angriparen att göra ett lyckat angrepp är att inte inrikta sig på de sektorer av samhället som normalt inte bevakas av olika underrättelseorgan, vilket leder till den privata sfären.

3.4 Huvudsakliga mål

Mikael Wilson radar upp ett antal tänkbara mål för informationskrigföring som huvudsakliga. Några av målen som Wilson[24] pekar på i sin genomgång är:

Kraftförsörjningen

Under en kris blir människors behov av information mycket större än vanligt. Ju längre ett problem varar, desto större blir kraven på informationen. Idag är det mesta av informationsflödet elberoende. Vid ett elavbrott så tystnar radio, TV och datorer - om du som mottagare inte har reservelverk eller batteridrivna apparater.[25]

För att ytterligare visa på hotet mot elförsörjningen hänvisar vi till det scenarion som kallas ”den Baltiska ringen” och som utspelas år 2050. Här beskrivs bland annat hur elnätet attackeras och tas ur drift i Mellansverige, Baltikum och St. Petersburg vilket får rejäla konsekvenser. Scenariot finns att läsa i sin helhet på RiskNets hemsida. [26]

Vattenförsörjningen

Vatten är vårt viktigaste livsmedel. Får du inte vatten under några dagar blir du helt utmattad och orkar inte göra någonting. Att kunna ordna vatten vid problem med vattenförsörjningen borde därför vara ett av de områden som kommunerna prioriterar. Tre dagar utan vatten medför att du blir mycket utmattad och blir liggande. En vecka utan vatten kan leda till total uttorkning och döden.[27]

Vi ser en grad av oro hos vår svenska regering och kan i proposition 2001/02:158 läsa ”*Försörjningen med vatten är också beroende av att det finns tillgång till el, tele och IT. Denna sårbarhet gör försörjningen med vatten känslig även för terrorsim och sabotage*”.[28] Detta om något är ett tydligt tecken på att det i dagsläget finns allvarliga brister som uppmärksammats. Ett uttalande som bekräftar detta står att finna på RiskNets hemsida och lyder ” *Det finns en tröghet i*

[24] Arbetsgruppen om Informationsteknologisk krigföring, 1997, s 16 f
[25] www.totalforsvaret.se 2002-04-03
[26] http://www.risknet.foa.se/it/fakta/Baltiskaringen.htm 2002-04-10
[27] www.totalforsvaret.se 2002-04-03
[28] Regeringens proposition 2001/02:158, *Samhällets säkerhet och beredskap*, sid 135

vattenförsörjningssystemen som gör det mycket svårt att göra snabba förändringar vid ett akut hot." [29].

Bränsleförsörjningen

Vi måste vara beredda på att lita mer på egna transporter. Det kan bli en ökad belastning på en kollektivtrafik som kanske ändå inte går för fullt. Tåg, spårvagnar och tunnelbanor är elberoende liksom att det krävs el till bensinpumparna i de stora bussgaragen.

Detsamma gäller också de vanliga bensinmackarna. Även om vi har egna bilar kanske vi inte kan tanka dem. Staten har via Överstyrelsen för Civil Beredskap köpt in och utplacerat ett antal bilbatteridrivna bensinpumpar som sänks ner i cisternerna. Men de är få till antalet och är främst till för räddningstjänsten, polisen och andra liknande viktiga funktioner.[30]

Bankväsendet/ finanssektorn

Terrorattacken mot World Trade Center kom att sända en chockvåg genom världens finansmarknader. Vad många i olika katastrofscenarier hade utmålat som en extrem katastrof blev plötsligt verklighet. New York-börsen öppnade aldrig tisdagen den 11 september. I stället förblev den stängd under resten av veckan. Världens övriga aktiemarknader med några undantag höll emellertid öppet och kurserna sjönk markant. Stockholmsbörsen sjönk med ca 5 procent från tisdag morgon till fredag kväll denna vecka.[31]

Som ytterligare exempel kan vi här nämna ett scenario, nämligen "The electronic doomsday scenario".[32] Här beskrivs hur två medlemmar ur Pearl Harbour 2 tar sig in i NASDAQ:s system i syfte att ta ner det, eller rättare sagt ta det ur drift. Ett scenario som anses fullt möjligt.

Lufttransporter

Lufttransportsystemet skall i militär fredlig tid fungera för bland annat sjöräddningsuppdrag, sjuktransporter, bekämpning av skogsbränder, transport av räddningspersonal vid större katastrofer[33]

3.5 Angriparens tekniker och metoder.

För att angriparen ska kunna utföra sitt dåd krävs det en hel del förberedelser. Till stor del består denna del av inhämtande av information om målet som ska attackeras. Besitter angriparen aktuell och rätt kunskap om målet har denna större chans att lyckas med sin informationskrigföring. De metoder som angriparen använder sig av innan själva angreppet är även det en del av informationskrigföringen. Dessa metoder kan vara inhämtning från öppna källor och system, intrång i datorer och nätverk samt övrig underrättelseinhämtning, som t.ex. spionage.[34]

[29] http://www.risknet.foa.se/va/ 2002-04-20
[30] www.totalforsvaret.se 2002-04-03
[31] http://www.fi.se/Publikationer/debatt/t20010928.pdf 2002-03-18
[32] Michael Erbschloe, 2001, s 86
[33] http://www.ambulansforum.se/PAM/forskning/ambhelisegstudie.shtml 2002-03-18
[34] Arbetsgruppen om Informationskrigföring, 1997 s 25 f

3.5.1 Syftet med metoderna.

I en rapport om ”åtgärder och skydd mot informationskrigföring”, från 1997, av *arbetsgruppen om informationskrigföring* skrivs det att informations-krigföringens metoder kan ha följande syften:

A. Avlyssning, underserrättelseinhämtning

B. Förvanskning, vilseledning

C. Blockering, t.ex. Denial of service

D. Påtvingande av information

E. Fysisk förstörelse

	Metod	Syfte
1	Infologiskt intrång, för avtappning eller kopiering av information	**A**
2	avtappning med specialenheter eller personal	**A**
3	signalspaning	**A**
4	elektromagnetisk störning	**C**
5	Infologiskt intrång för att förstöra, blockare eller förvanska	**B,C**
6	Infologisk störning	**C**
7	teknisk vilseledande signalering	**B,C**
8	Störning/vilseledning av navigationssystem	**B,C**
9	Obehörig access	**A,B,C,D**
10	Kryptologiskt genombrott	**A,B,C,D**
11	Vilseledande datakälla	**B,D**
12	Riktade telefonsamtal och e-post	**B,D**
13	Internet	**B,D**
14	Sabotageenheter	**E**
15	Laser och HPM, HERF-vapen mot info-system, satelliter och spaningssensorer	**E**
16	mikrober och nanomaskiner	**E**

3.5.2 Infologiskt intrång (för hämtning eller kopiering av information)

Metoden för infologiskt intrång som vanligtvis används idag är ”hacking”. Metoden går ut på att hitta ingångar till datorsystem. Angriparen kan även använda programvara som implementeras i systemet för att sända tillbaka intressant information till angriparen.

Metoden som sådan kan oftast vara svår att upptäcka och spåra och kan därför lämna angriparen anonym. Angriparen kan även lämna spår som leder till en skenbar aktör för att vilseleda den angripne.

Hacking är idag ett vanligt förekommande medel som kan utföras av åtskilliga aktörer. Programvara för sniffning finns väl utdelat på Internet och underlättar för ”hackern”. En ”bra” hacker urskiljer sig på det sätt att han/hon oftast kan konsten att hålla sig anonym. [35]

Program som kan nämnas i sammanhanget är D-sniff. Med detta program kan trafik till och från en dator fångas upp utan att den angripne uppfattar

[35] Hagen, Fahlén, 1999

intrånget. Angriparen kan bland annat göra en så kallad ”man-in-the-middle-attack” där angriparen fångar upp all trafik mellan en sändande aktör och skickar sedan informationen vidare till tänkt mottagare, utan att de två märker att informationen som skickats har snappats upp av en tredje part.

Information kan skyddas genom kryptering och så kallad ”checksum”. Kryptering skyddar informationen genom att endast mottagaren med rätt krypteringsnyckel kan läsa den krypterade informationen. ”checksum” kontrollerar att informationen som sänts inte har ändrats eller på annat sätt rörts.[36]

3.5.3 Avtappning med hjälp av specialenheter eller personal.

Specialenheter används för att avtappa information på sådana system som befinner sig inom ett ”skyddat” område. Områden som t.ex. byggnader vars nätverk inte är uppkopplade via Internet. Dessa nätverk går oftast inte att nå utifrån på elektronisk väg. Alternativet till att göra en elektronisk avtappning är avtappning av en fiber optiskt eller att utnyttja ”RÖS” (röjande strålning) från datorskärmar. Beroende på hur utrustningen är konstruerad, fångas strålningen upp från denna. En vanlig datormonitor avger mer RÖS än en plasmamonitor. En ledning till en enhet kan fungera som antenn. Signalerna kan förstärkas om tillfälle ges att preparera utrustningen.

Ska angriparen spana med hjälp av RÖS krävs en närspaningsmetod. Det sker med hjälp av enkla antenner som på några hundratals meters avstånd kan uppfatta signalerna från datorskärmen, höljet eller ledningarna. Det ger de krypterade meddelandena i klarskrift. Samtidigt spelar specialenheten in signalerna för att analysera denna på annan plats. Risken för upptäckt ökar naturligtvis ju närmare objektet angriparen måste operera.[37]

3.5.4 Signalspaning.

Signalspaning används för att spana mot kommunikationsnät och för att fastställa tekniska systemparametrar. Metoden används också för att fånga upp information och på så sätt fastställa sändares position.

"Militära förband måste avge signaler på något sätt vare sig de angriper eller försvarar sig. Detta ger oss en möjlighet att få information", säger Leif Thyrfelt som ingår i krigsförbandsledningens telekrigssektion[38].

”I dag kan vi pejla in främmande flygplan och fartyg med hjälp av deras egen utrustning. Att kunna identifiera föremål på ett tidigt stadium är både en svår och viktig del i underrättelsetjänsten. Den tekniska utrustningen ligger långt framme jämfört med andra länder”, säger Bengt-Arne Johansson[39].

Den ökade användningen av mobiltelefonnät ger angriparen ytterligare ett område att utföra signalspaning på. Angriparen kan samtidigt som han avlyssnar samtal även lokalisera den angripne.

Motmedel till avlyssning är så kallad kryptering av meddelande. Med kryptering begränsas angriparens spaning till att endast se trafikflöde samt

[36] William Stallings, 1997, s 548
[37] Hagen, Fahlén, 1999
[38] http://www.mil.se/fmforum/698/reportage2.html - 2002-05-13
[39] http://www.mil.se/fmforum/698/reportage2.html - 2002-05-13

lokalisering av sändningsplatser. Informationen i sända meddelande görs svårtydda för angriparen.

3.5.5 Elektromagnetisk störning.

Med elektromagnetisk störning blockeras dataöverföring. Angriparen kan även sända ut felaktig information till tänkt mottagare av blockerad data. Störningen leder till att systemen blir opålitliga.

Tidigare och även idag så har elektronisk störning utnyttjats främst av militära förband för att förhindra och blockera fiendens kommunikationssystem. [40]

3.5.6 Infologiskt intrång (för att förstöra, blockera eller förvanska).

Det är inom denna teknik alla virus och hacking utgör basis. Syftet med metoden är att modifiera data, program eller dator. Nedan redogörs begreppen tillhörande metoden:[41]

Datavirus.

Virus är kanske den mest vanliga formen av krigföring mot datorbaserade informationskällor. Dock relaterar man oftast virus till spridning där den angripne är en enskild person. Det vi kopplar begreppet virus till är sabotage från unga personer med icke genomtänkt experimentlusta.

Ett virus är ett självproducerande programavsnitt, som placerar in sig själv som en del av ett större program. Spridningen kan ske via en diskett eller nätverk. Virus gömmer sig i filer. De kan ställa till skada genom att radera eller förvränga information. De flesta finns på PC-sidan.

Ett virus kan implanteras av en organisation i tänkt offers telefonsystems datorstyrda växel. Ett ”enkelt” virus gjort för enskild PC skulle därpå kunna slå ut hela telefonsystem.

Maskar.

En mask (worm) infiltrerar sig till motsats till virus inte andra program. Maskar förstör därför inte data. En mask reproducerar sig självt genom att konstant kopiera sig från en dator till en annan. Kopieringen fyller till slut systemet med ”maskar” och sänker hela systemet och dess resurser.[42]

Problemet för angriparen med denna metod kan vara att få en kontrollerad spridning och effekt.

Trojaner.

En trojansk häst (”trojan horse”) är, precis som i Iliaden, en fälla där den troskyldige användaren själv ovetande släpper in angriparen, dvs. ger behörighet åt denna. Trojanen är oftast ett program som utger sig för att vara spel, nyttoprogram eller annat.[43]

[40] Hagen, Fahlén, 1999
[41] Hagen, Fahlén, 1999
[42] http://www.microsoft.com/sverige/security/software_threat/default.asp?threat=1 – 2002-05-02
[43] http://www.microsoft.com/sverige/security/software_threat/default.asp?threat=3 – 2002-05-02

En trojan är alltså ett kodfragment som döljs inne i ett program i datorn och genomför där en förtäckt åtgärd.

Trojanska hästar kan i många fall förtäcka och gömma virus och maskar. En bra skapad trojan lämnar inga spår av sin närvaro och är därmed svår att upptäcka.

Logiska bomber.

En logisk bomb är en typ av trojansk häst, som skapas för att släppa loss ett virus, en mask eller någon annan attack mot ett datorsystem.

En logisk bomb är en enkel "if-sats" som sätts i verksamhet så fort som de ingående parametrarna införlivas. Detta kan vara en speciell tid eller så fort ett namn används eller utelämnas.[44]

Bakdörrar.

En bakdörr (”backdoor”) är en del av ett program som ger utvecklaren en lönndörr in till användaren som använder programmets dator.

Om t.ex. Microsoft skulle använda sig av ovan nämnd metod skulle de ha en access till i stort sett de flesta PC:s kopplade till Internet.

Chipping.

Att förse ett chip med särskilda funktioner som kan aktiveras av någon annan än ägaren av systemet. Chipping, läggs in i hårdvaran och är en metod att lägga in en bakdörr, en trojansk häst, virus mm. Därigenom kan angriparen när denne vill gå in i systemet, då risk för direkt upptäckt är som lägst, och operera.

Chipsen kan även konstrueras på så sätt att de t.ex. förstörs efter en viss tid.

3.5.7 Infologisk störning

I denna metod ingår t.ex. e-post bombning (mail-bombning) där angriparen med hjälp av program ”sänker” e-post-servrar med mängder av e-post.[45]

3.5.8 Teknisk vilseledande signalering

En delfunktion av denna metod är skensändning av krypto. I detta sammanhang så handlar det om att generera falsk kryptotrafik för att binda upp motståndarens resurser till kryptoanalys.[46]

3.5.9 Störning/vilseledning av navigationssystem

Navigationssystemet som angriparen idag attackerar är oftast GPS-systemet som oftast används av militära trupper. GPS (global positioning system) är ett satellitbaserat positionssystem, där användaren via en teknisk modul kan bestämma sin position.[47]

[44] http://www.protectdata.se/security/seclib_virus_school.jsp - 2002-05-02
[45] Hagen, Fahlén, 1999
[46] Hagen, Fahlén, 1999
[47] Hagen, Fahlén, 1999

3.5.10 Obehörig access

Denna metod går ut på att genom få tillgång till lösenord till datorsystem ta sig in på obehöriga informationsområden. Angriparen tar över en identitet som har rättigheter till ett datorsystem. Systemet kan då inte längre avgöra om användaren är en obehörig person som är ansluten.

Med olika snifferprogram kan angriparen fånga upp användarnamn samt lösenord till ett system, då angriparen osynligt fångar upp trafik mellan en användare och ett datorsystem.

Med hjälp av obehörig access kan sedan angriparen hämta, ändra eller förstöra data i informationssystemet.

Person som utövar denna metod utger sig oftast för att vara en ”cracker”.[48]

3.5.11 Kryptografiskt genombrott

Kryptografi går ut på att dölja text och meddelanden med olika bokstavs- eller teckenkombinationer. Den tänkta mottagaren använder en kryptonyckel för att få fram rätt tecken ur den krypterade massan.

Får angriparen tag på informationsnätverkets kryptonyckeldistribution kan han/hon inte bara läsa hemlig information utan har även en möjlighet att skicka falska meddelanden till nätverket för att vilseleda användarna. Användaren sitter då med en falsk säkerhetskänsla och uppfattar meddelandet som autentiskt.

Bland annat banker och försvaret använder idag sig av kryptering av informationsflödet. Angrepp mot dessa skulle kunna få mycket allvarliga konsekvenser för ett land.

Ett sätt att skydda sin kryptoanvändning är att byta nycklar ofta och att ha en säker distribution av nycklarna.[49]

3.5.12 Vilseledande datakälla

Metoden går ut på att göra en skenbar plats som lurar användaren att han/hon befinner sig på en särskild plats. Här handlar det mer om att vilseleda och sprida felaktiga uppgifter genom att tillhandahålla trovärdiga källor som ersätter de verkliga källorna.

Inom radio och TV kan angriparen manipulera bild och ljud för att påverka mottagaren att tro på uppgifterna. Inom Internet finns det en metod som kallas ”spoofing”. Genom att få läsaren att tro han/hon är inne på en sida som egentligen är tillverkad av en tredje part ta reda på andras lösenord och e-postadresser på Internet och sedan använda dessa.[50]

3.5.13 Riktade telefonsamtal och e-post

Genom sändning av riktade telefonsamtal eller e-post som påverkar mottagaren ges angriparen ett psykologiskt övertag.[51]

[48] Hagen, Fahlén, 1999
[49] Hagen, Fahlén, 1999
[50] Hagen, Fahlén, 1999
[51] Hagen, Fahlén, 1999

3.5.14 Internet

Genom att utge ett seriöst uttryck för besökaren kan tillverkaren påverka personer, grupper, statistik, beslut och börser med sin vilseledande information. Tillverkaren kan även få tillgång till information från besökare som ovetande lämnat personlig information till en oseriös individ/grupp.[52]

3.4.15 Sabotageenheter

Metoderna har traditionellt varit att förstöra olika objekt. Inom informationskrigföringen kan andra metoder vara mer relevanta. Det kan vara att skapa ingångar i näten genom att sammankoppla olika nät, koppla in radiolänkar, koppla upp sig mot vissa funktioner och manipulera data, styra och självdestruera olika system. Andra metoder kan vara att utlösa HERF-vapen (hög effekts radio frekvens) för att skada elektroniska system.[53]

3.5.16 Elektromagnetiska vapen

Den samlade definitionen på elektromagnetiska vapen är att de ger pulser med mycket stor energitäthet som kan slå ut IT-utrustning. Grunden till denna möjlighet ligger i att elektroniska kretsar är mycket sårbara. Några typer av elektromagnetsiska vapen som kan nämnas är:

- HPM-vapen (high power microwave)
- HERF-vapen (high energy radio frequency)
- HIRF-vapen (high intensity radiated fields)
- GTED (galvanic tracient electromagnetic device)[54]

Effekten av dessa vapen kan vara allt ifrån att systemen slås ifrån till att systemet helt enkelt slås ut. Den senare och allt mer allvarliga skadan innebär att hårdvarudelar i systemet blir fysiskt skadade, med systemkrascher som följd.

Ett HERF-vapen skjuter en högeffekts radiosignal mot målet. Angriparen skulle kunna slå ut mer än bara informationssystem, även larmsystem och övervakningskameror.

NSA (National Security Agency), Scotland Yard och FBI påtalar att hot som HPM och HIRF har verkställts mot banker och finansiella institutioner. Detta bekräftas även av en talesman från Bank of England.

Informationskrigföring med elektromagnetiska vapen är icke-letala (icke dödande) dvs. humana vapen och därmed är insatströskeln för en terrorist låg. [55]

3.5.17 Mikrober och Nanomaskiner

Det har konstaterats att det finns bakterier (mikrober) skapade i laboratorium, som favoriserar vissa plastmaterial eller andra ämnen som t.ex. silikon och kisel som ingår i integrerade kretsar.

[52] Hagen, Fahlén, 1999
[53] Hagen, Fahlén, 1999
[54] Hagen, Fahlén, 1999, s 4 f
[55] http://www.eme.se 2002-05-03

Nanomaskiner är fysiska enheter som kan användas för att sabotera informationsbehandlande enheter. Dessa maskiner är konstgjorda robotar i mycket liten storlek, mindre än nålsögon, vilka kan programmeras att anfalla speciella delar av en datainstallation.[56]

[56] Hagen, Fahlén, 1999

4. Empiri

4.1 Utövare och deras motiv

Björn Andersson talade här om att det var viktigt att kunna identifiera angriparen. Det är ofta svårt att skydda ett system från alla olika eventualiteter som finns särskilt som det inte alltid är så att det finns kunskap om vilka tekniker som kan användas. Nya tekniker och nya hot upptäcks varje dag och det är en omöjlig uppgift att hinna med och utveckla skydd för alla dessa sorters attacker. Därmed är det viktigt att identifiera angriparen. Vet vi vem som angriper kan vi förutspå vissa drag denna kan tänkas göra och därmed ligga ett steg före.

Vidare menar Björn Andersson att vet vi vem angriparen är så vet vi också på ett ungefär vilka typer av system som denna kan tänkas angripa. Exempelvis skulle en kriminell sällan ha något utbyte av att attackera ett mindre företags hemsida då detta inte skulle leda till någon större summa pengar, och med tanke på de konsekvenser denna handling kan få (d.v.s. fängelse eller liknande) för angriparen så ska det också leda till något mer givande.

Bilden av angriparen mot det svenska samhället kan bestå av fyra olika grupper. Björn Andersson på SÄPO nämner dessa nedanstående grupper som huvudsakliga angripare:

4.1.1 Hackers/Crackers

Dessa har oftast inget direkt syfte att såra samhället utan dennes mål är oftast att visa att de har de kunskaper som krävs för att utföra olika attacker. Det handlar här snarare för denna typ av angripare att få ett erkännande eller rykte inom olika hackerkretsar. Hackern/Crackern söker spänning vilket är delvis hans/hennes motiv till att utföra dessa handlingar. Denna angripares motiv är helt egoistiska, till och med narcisstiska och angreppen utförs endast för det egna egots vinning.

4.1.2 Kriminella

Handlingarna som den kriminella gruppen utövar är oftast ett led till en annan kriminell handling. Det handlar exempelvis om att ge sig på ett banksystem och se vilka svagheter som där finns i dess säkerhet för att därmed använda detta vid en eventuell utpressning. Målet för denna angripare är oftast att komma över pengar. Motiveringen till angreppet ska också överskrida riskerna som denna angripare utsätter sig för.

4.1.3 Extremister

Denna grupp utför oftast en sorts ideologisk handling. Grupper som här kan nämnas är högerextremister och djurrättsaktivister. Denna grupp utför sina attacker för att visa att de innehar en viss grad av makt över sin fiende och kan därmed hota denna till förändringar. I värsta fall kan extremisterna utföra sina handlingar.

4.1.4 Terrorister

Likt extremistens handlingsmotiv är terroristens motiv att visa sin makt gentemot sin ”fiende”. Exempel som kan nämnas är terroristgruppen ”Al Qaeda”. Terrorister är en farlig grupp som sällan tänker på de konsekvenser deras handlingar innebär för dem själva utan fokuserar istället på att skapa så stor förödelse som möjligt.

4.2 Huvudsakliga mål.

Björn Andersson på SÄPO nämner att det finns fyra övergripande områden som bör prioriteras högre än andra. Till dessa räknas el- och vattenförsörjning, kommunikation och finans/bankväsendet. Om några av dessa slås ut, eller lamslås, får Sveriges samhällen svårt att fungera på ett sätt som anses normalt.

Elförsörjningen anses vara viktigast att skydda eftersom om en angripare saboterar dessa system leder detta till att även andra system kraschar, det handlar om en slags dominoeffekt. För att exemplifiera kan vi nämna att om system för elförsörjning slås ut kommer även system för vatten, kommunikation och finans att stå stilla då dessa är beroende av kraftförsörjningen. En regel som är allmänt känd är den så kallade treregeln vilket innebär att du klarar dig tre minuter utan luft, tre dagar utan vatten och slutligen tre månader utan mat. Vad Björn Andersson då menar är att beroendet av el är högt då vattenförsörjningen i sin tur är beroende av el.

Samhällets beroende av kraftförsörjningen kan exemplifieras genom att nämna den händelse som inträffade i Ystad[57] i mars 2002 då en olycka inträffade vid en kraftledning som orsakade totalt strömavbrott i Ystad stad. Detta fick konsekvenser som att fabriker stannade upp, affärer fick stänga vilket bidragit till förlust av kapital i form av utebliven produktion eller försäljning. Sjukvården fungerade dock tack vare egna reservsystem, men prioriteringar fick göras då beslut måste tas om vilka avdelningar som krävde mer ström än andra.

Svenska Kraftnät sköter Sveriges elnät. Här medger Björn Andersson att det finns en del sårbara knytpunkter och att dessa är relativt lätta att identifiera. Bo Bengtsson på Lunds Energi medger även han att det finns möjligheter att slå ut kraftförsörjningen då deras leverantörer kopplar upp sig via modem. Under denna period då leverantörerna är uppkopplade finns det en lucka för eventuella attacker vilket givetvis gör systemet sårbart.

Det som är av störst intresse är både de servrar som finns ute hos leverentörerna såväl som den centrala server som finns hos Lunds Energi. Den sistnämna är den server som skulle bidra till störst skada vid en attack då det är denna server som står för centraliseringen av systemunderhållet. Slås denna ut står leverantörerna handfallna och kan alltså inte sköta sitt underhåll, något som kan få konsekvenser. Givetvis innebär det också att Lunds Energi för en tid blir handikappade och på längre sikt förlorar både anseende och pengar.

Björn Andersson nämnde också som hastigast att mobila nät är väldigt utsatta men att material som rör detta är sekretessbelagt. Vad som är intressant är dock att ett medgivande görs gällande detta och vi vet därmed att det finns ett befintligt hot.

[57] Ystads Allehanda, *Elavbrott lamslog Ystad*, 2002-03-07

Att attackera system som sköter bank- och finans är också ett primärt mål enligt Björn Andersson och är viktigt att säkerställa. Attacker som utförs här får allvarliga ekonomiska konsekvenser och drabbar såväl företag och organisationer som privatpersoner. Inte minst drabbas banker som liksom Lunds Energi förlorar anseede och på längre sikt pengar i form av förlorade kunder.

4.3 Angriparens tekniker och metoder

De tekniker och metoder som nämndes här av Björn Andersson gällde i första hand elektromagnetiska vapen såsom HPM. Detta är vapen som är väldigt effektiva och anonyma.

4.3.1 HPM

Med ett HPM-vapen skickas en elektromagnetisk puls ut som förstör samtliga elektroniska komponenter inom en viss radie. Vapnet är tyst, syns inte och åsamkar endast skador på elektriska komponenter. HPM skadar alltså inte fysiska ting såsom djur och människor. Det finns heller inget skydd mot detta vapen då det tar sig genom exempelvis väggar. Detta är inget vapen som vem som helst kommer över eller kan använda varpå detta inte idag inte är ett stort hot.

4.3.2 Intrång på VLAN

En annan teknik som Björn Andersson nämnde handlade om intrång via VLAN (virtual local area network). Denna teknik innebär att en hacker tränger in i det trådlösa nätverket och fångar upp MAC-adress och IP-nummer som denna sedan använder i egna syften. Denna teknik är mer vedertagen inom de kretsar som utför angrepp och bör tas i beaktning. Användaren bör förstå riskerna med detta kommunikationssätt (VLAN). Björn Andersson exemplifierar risken med detta kommunikationssätt med att tala om att det är lika säkert som att sätta ut ett nätverksuttag på företagets parkeringsplats.

4.4 Åtgärder och skydd

Björn Andersson (SÄPO) säger att skyddet mot attacker försenas på grund av politiska faktorer. Politiker måste övertyga sina väljare till varför man ska tillsätta ekonomiska medel för att skydda sig mot tänkta angrepp inom olika områden. Dessa investeringar i framtida skyddsåtgärder är svåra att motivera dels för att det just handlar om framtida hot och dels för att det är åtgärder som inte direkt märks av av allmänheten.

En positiv effekt av den tragiska händelsen i USA den 11 september 2001, är att allmänheten fått en klarare bild av samhällets sårbarhet. Länder börjar allt mer omvärdera vad som är känslig information och vad som är ett hot mot samhället. Enligt Björn Andersson har vi i Sverige bland annat fått upp ögonen för att information som kartor över el-nätverket i Sverige oftast finns till allmän beskådning på bland annat Internet. Denna information börjar nu allt mer försvinna från Internet. I USA tas denna information på Internet bort helt därför att denna information egentligen inte behövs till allmän beskådning, det finns egentligen inget allmänintresse för denna sorts information.

Den så kallade lösning som Bo Bengtsson på Lunds Energi talar om vad gäller det problem med säkerheten som handlar om såväl el som

vattenförsörjning är att leverantören ber Lunds Energi koppla upp sig för systemunderhåll. Då minimeras risken, men den finns fortfarande. Ännu finns det ingen direkt åtgärd för att säkerställa informationstransaktioner, men det finns ett medventande om de säkerhetsluckor som finns.

Björn Andersson (SÄPO) nämner också ”Bin Laden-effekten”. Med det menas att företag och organisationer hade samlat all sin tankekapacitet centralt på en lokal punkt. En kraftfull centralisering av viktig information ger också en större risk att denna information ska försvinna. Att samla all information, företagsledning och tankekraft på ett ställe ökar givetvis kraftfullheten och samordningsförmågan, men sårbarheten ökar också dramatiskt. Som exempel kan vi nämna när WTC störtade samman den 11 september 2001. Då störtade också hela företag samman. All information om företagen som fanns i byggnaderna utplånades, som om dom aldrig hade funnits. Företagsledning, affärsplaner, information och affärer är borta. All den samlade kraft som företagen hade samlat försvann i ett ögonblick och har för många haft förödande konsekvenser. Många av dessa företag har fått börja om från noll.

För att visa på ett svenskt perspektiv nämnde Björn Andersson en tänkbar bild av att svenska flottan inte hade några stora slagkraftiga kryssare. Detta fartyg skulle kunna utgöra stor slagkraft i och med att så mycket kraft och resurser samlas på ett och samma ställe, men skulle någon lyckas slå ut denna enhet skulle skadan vara enorm mot svenska försvaret.

Vad Björn Andersson här menar är att en enkel åtgärd för att skydda sig är att sprida ut sin tankekraft istället för att centralisera. På så sätt kan detta hot elimineras.

Vi vet också att det idag finns ett visst skydd mot attacker vad gäller kommunikation. Sten Svensson på Skanova Networks (som driver det telenät där bland annat Telia ingår) skriver att det tagits en del säkerhetsåtgärder. Dessa består bland annat av dubbla framföringsvägar, d.v.s. dubbla teleledningar från vissa centrala och viktiga knytpunkter. Dubletter av viktiga funktioner är en annan åtgärd som tagits. En tredje åtgärd som Sten Svensson nämner är de elförsörjningssystem som finns på viktiga punkter.

Det krafttag som märks av allra tydligast är den nya myndighet som Björn Andersson talar om. Denna nya myndighet heter Krisberedskaps-myndigheten och har till uppgift att samordna arbetet kring säkerhetsfrågor och ska vara det organ som i framtiden ska sörja för att säkerhetsnivån är tillräckligt hög.

5. Analys

5.1 Utövare och deras motiv

De utövare som definieras i vår teori och empiri styrs till stor del av vilka mål och syften dessa har. Vi kan se att den enskilde individen som Björn Andersson (SÄPO) nämner, även kallad Hacker/Cracker, utgör oftast inget hot mot samhällets strukturer. Deras mål är oftast inte att rasera funktioner i samhället utan att visa sina kunskaper att göra intrång i datorsystem. Dock kan nämnas attt om denna individ opererar på en annan nivå än enskild basis som i exempelvis en terroistgrupp kan denna person utgöra ett mer allvarligt hot.

För alla utövare medför utvecklingen vad gäller nya angreppssätt och metoder att det finns ständig tillgång till nya tekniker vilket bidrar till att de system som utvecklas idag och anses vara säkra imorgon kanske inte är säkra längre då dessa nya tekniker kan användas av nämnda utövare. Utvecklingen vad gäller uppbyggnad av säkra system går inte lika fort och därmed har angriparen ett övertag.

Möjligheten att en individ på ena sidan av världen kommer i kontakt med en likasinnad individ i en annan del av världen ökas betydligt. Att fysiskt träffas och komma överens om angrepp och att planera en attack är inte längre nödvändigt då denna kontakt kan ske rent virtuellt via exempelvis Internet. Detta skapar en samhörighet bland utövare och kan bidra till att ett kontaktnät skapas mellan dessa. En angripare kan sitta på en sida av jorden och attackera ett mål på andra sidan. Detta i sig kan för angriparen utgöra en motivering, eller snarare förstärka motiveringen, till att utföra en attack då det ofta är svårt att spåra en duktig utövare.

Risken för att straffas eller bli påkommen minimeras på grund av denna globalisering. En duktig utövare vet i de flesta fall också hur spår ska sopas igen och risken för att bli påkommen minskar ytterligare.

De kriminella organisationerna som Björn Andersson nämner som opererar med informationskrigföring får med dagens utveckling nya mål och metoder att verka med. Tittar vi på avsnitt 3.3 ser vi vid en jämförelse en annorlunda indelning av utövarna och kan se att denna utövares angreppsområden sällan är globala utan snarare marknadsrelaterade.

De extremistgrupper som Björn Andersson talar om använder allt mer den ”nya tekniken” som ett verktyg att angripa sina mål med. Deras motiv kan vara marknadsrelaterade men även globala, det ser vi vid en jämförelse mellan det Björn påstår och den indelning som Winn Schwartau gör.[58] De mål som avses angripas kan med de allt mer utsuddade geografiska gränserna finnas på andra sidan jordklotet. Deras angrepp beror oftast på att försöka lämna sina budskap till omvärlden.

Terrorister kan med relativt enkla medel sabotera politiska strukturer. Minoritetsgrupper kan utöva sina, oftast politiska, attentat mot globala stormakter.

[58] Arbetsgruppen om Informationskrigföring, 1997, s 8

Som vi ser talar Björn Andersson mer tydligt om specifika utövare som t.ex. hackern, extrimisten eller den kriminella. Winn Schwartau talar dock om angriparen på ett annat sätt och väljer att istället dela in dessa i olika klasser beroende på utövningsområden. Men vi kan väva in de utövare som Björn Andersson talar om i Winn Schwartaus teorier då vi ser att det finns ett mönster vad gäller motivering och den nivå denna utövare opererar på.

Ovanstående faktorer som vi nämnt, såsom globalisering och tillgång till nya tekniker och metoder, bidrar till att dessa grupper ytterligare sporras att utföra sina handlingar.

5.2 Huvudsakliga mål

De mål som identifierats är många, men de som av Björn Andersson anses vara primära mål för angrepp är de system som sköter el- och vattenförsörjning, kommunikation samt bank/finans.

Att dessa utgör de huvudsakliga målen verkar det inte råda något tvivel om och inte heller råder något tvivel om att dessa system är av stor vikt för samhällets funktion. Vi ser att de mål som Mikael Wilson talar om under avsnitt 3.4 stämmer bra överens med de mål som Björn Andersson talar om.

Vi kan se att elförsörjningen som mål är det som kan orsaka mest skada för ett samhälle. Både i teori under avsnitt 3.4 och empirin har detta konstaterats. Björn Andersson talar om att elförsörjningen oftast är en grundsten till övriga mål, utan el kan inget bränsle pumpas upp från bensinstationer, färskvattnet kan inte pumpas ut i ledningar, informationsystem till bank och finansväsendet kan inte användas. Alla informationssystem är beroende av att ha tillgång till el. Det finns dock de system som för en kortare period kan förses med el via egna reservsystem, men skulle det uppstå ett uppehåll av tillförsel av el som är långvarigt så uppstår driftstopp även för dessa system.

Att angripa elförsörjningens fjärrmanövreringssystem är möjligt även om det krävs att veta exakt när, var och hur angreppet ska ske enligt Bo Bengtsson på Lunds Energi. Skulle ett sådant angrepp inträffa skulle till stor del även de andra nämnda målen som framhävts under avsnitt 3.4 också påverkas. Samhället är till stor del helt beroende av elförsörjningen och därför är samhället oerhört sårbart om detta mål skulle penetreras av en angripare.

Skulle det vara så att angrepp utförs på övriga mål vi tagit upp under avsnitt 3.4 så skulle även detta ha konsekvenser för samhället i sig då ett samhälle även är beroende av dessa funktioner enligt Björn Andersson. Ett angrepp mot Stockholmsbörsen skulle ha förödande konsekvenser runt om i landet även om systemet som sköter detta så bara var nere för en timme. Alla de transaktioner som skulle kunna ske under denna timme går förlorade och kan innebära stora ekonomiska förluster.

Att avslöja sina svagheter är inget företag gärna gör. Denna tendens är bland annat tydligt inom telecombranchen där mycket av matrialet är sekretessbelagt enligt såväl Björn Andersson som Sten Svensson på Skanova Networks. Vad detta beror på kan det på vår nivå endast spekuleras kring.

5.3 Angriparens tekniker och metoder

Det finns idag en uppsjö av olika tekniker och metoder för att angripa informationssystem av olika slag. Detta kan handla om allt från så avancerade vapen som HPM till mindre avancerade tekniker såsom virus, det ser vi under avsnitt 3.5. Gemensamt för samtliga tekniker är att de på ett eller annat sätt åsamkar skada på system.

De tekniker som vi nämner i vår uppsats är endast ett fåtal och nya tekniker utformas ständigt. Vad som anses vara högteknologiskt idag kan imorgon vara pasé och gammalt. Utvecklingen inom detta område går snabbt och det kan mycket väl idag finnas tekniker och metoder som inte är kända enligt Björn Andersson. Detta i sig utgör ett hot då det är en omöjlig uppgift att hänga med denna utveckling och skapa system som klarar av att avvisa alla dessa hot.

HPM är ett högeffektivt och högteknologist vapen som inte används av gemene man. Vapnet skickar ut en elektromagnetisk puls som slår ut alla elektroniska komponenter och är högeffektivt i den mening att det just slår ut alla elektriska komponenter, något vi kan läsa om under avsnitt 3.5.

HPM-vapen är ett realistiskt hot enligt Björn Andersson och det finns tillgång till detta slags vapen idag. Det som gör detta vapen så farligt är att det nästan inte finns något skydd mot det som det ser ut idag.

Den teknik som ligger till grund för det trådlösa nätverk som kallas VLAN utgör en säkerhetsrisk och är relativt lätt att penetrera med rätt medel säger Björn Andersson. För detta krävs inga högteknologiska agreppssätt vilket bidrar till att det är lättare att attackera just denna form av kommunikationssätt.

I teorin nämns det ett flertal tekniker för att kunna utföra informationskrigföring med. Samtliga av dessa tekniker är faktiska och utgör därmed ett hot. Vi kan alltså urskilja från såväl avsnitt 3.5 som från intervjun med Björn Andersson att det finns tekniker och metoder som gör det möjligt för en angripare att ta sig in i system, mer eller mindre obemärkt.

6. Slutsats

Globaliseringen medför att en angripare kan finnas var som helst i världen. Detta beror till stor del på Internet som innebär att vem som helst kan bli mål för ett angrepp. Virus är ett angreppssätt som idag är vardagligt och som många utsätts för. Angriparen kan också vara vem som helst. Möjligheten att likasinnade individer kommer i kontakt med varandra har ökat dramatiskt, även detta på grund av Internet. Det är idag enkelt att samordna och planera via Internet.

Vi ser också att den tekniska utvecklingen ligger till grund till att attacker kan utföras. När någon kommer på ett skydd är detta redan överbryggat av någon ny teknisk möjlighet som gör det möjligt att förbigå detta säkerhetsystem. Vi kan kallt konstatera att det är omöjligt för utvecklare av säkerhetssystem att hålla jämn takt med de som utvecklar de nya tekniker som tar sig genom de säkerhetsluckor som finns.

Att elförsörjningen ligger till grund för drift av system som uppehåller viktiga funktioner såsom vattenförsörjning eller bank- och finanssystem ser vi tydligt. En slutsats vi kan dra är att alla informationssystem är beroende av eltillförsel och kan inte fungera utan den. Därför anser vi att detta är ett primärt mål och att det är detta mål som i första hand ska beskyddas. Stänger vi denna säkerhetslucka ser vi också till att eliminiera många av de risker som detta mål utgör.

Att ett faktiskt hot finns är något vi inte tvekar om i det här skedet. Med tanke på alla de tekniker och möjligheter till angrepp som vi funnit så är det nästintill omöjligt att inte se det hot som föreligger. Att teknikerna överhuvudtaget finns till, utgör ett hot. Vi får bekräftat i såväl empiriska data som i teoretiska data att exempelvis HPM är ett faktiskt hot. I och med detta anser vi att det finns ett hot om även så det bara finns en möjlighet till att slå ut ett informationsystem.

Syftet med uppsatsen var att påvisa ifall det fanns ett faktiskt hot mot olika informationssystem i dagsläget. Som vi redan konstaterat finns det alltså ett faktiskt hot i och med exempelvis HPM och möjligheten att penetrera ett VLAN.

Vi ser också att det finns utövare som använder sig av olika tekniker och att det finns utövare innebär i sig också att det finns ett hot. Finns det inga utövare, eller angripare, finns det ju heller inget hot. Och finns det inga medel eller metoder för att angripa borde det tillika inte finnas några utövare. Likaså kan vi också påstå att finns det inga mål att angripa finns det heller inga angripare.

Vi vågar därmed påstå att ett hot faktiskt finns. Var nästa attack sker är det oftast bara angriparen som vet.

Tittar vi sedan på de frågeställningar vi ställde upp, d.v.s. *”Är informationskrigföringen ett hot och vilka är utövarna, deras motiv och mål ?”* samt *”Finns det en realistisk hotbild mot dessa mål ?”* så anser vi att vi funnit svar.

I och med att vi kunnat påvisa ett faktiskt hot så anser vi att hotbilden är realistisk. Vad vi närmare menar är att vi bevisat att det finns medel för att

utföra attacker, därmed är också hotet verkligt och informationskrigföringen ska anses vara ett hot.

Vi har under arbetets gång också lyckats identifiera ett antal utövare, eller angipare. Att dessa existerar har påvisats från många olika källor och vi kan som exempel nämna hackern. Vad vi sedan alltid hävdat, d.v.s. att finner vi utövaren finner vi också motiv och mål, stämmer överens med den teori vi målat upp. Exempelvis har en kriminell oftast pengar som drivkraft.

Något som är svårt dock är att härleda specifika mål till olika utövare. Vi kan snarare identifiera målområden än specifika mål. Men detta hjälper oss trots allt då vi allt mer kan ringa in utövaren och dess mål.

En slutsats vi drar är att ju mer vi vet om utövaren ju mer troligt är det att vi kan ringa in det område han/hon anser attackera. Det blir alltså viktigare att identifiera angriparen än målen.

Lärdomar vi fått genom arbetet är det att det inte finns några säkra system. Att veta var, när och hur ett angrepp ska inträffa skulle vara densamma som att spå framtiden, med andra ord nästintill omöjligt. Det är nästan omöjligt att skydda sig mot det oförutsägbara.

7. Källförteckning

7.1 Litteratur

Aronsson, L., Eriksson, L., Wiedersheim-Paul, F., 1975, *Att skriva rapporter och uppsatser i företagsekonomi*, Lund

Bell, J., 1993, *Introduktion till forskningsmtetodik*, Lund

Erbschloe, M., 2001, *Information warfare, how to survive cyber attacks*, Berkeley

Holme, I M., Solvang, B K., 1991, *Forskningsmetodik – om kvalitativa och kvantitativa metoder*, Lund

Merriam, S B., 1994, *Fallstudien som forskningsmetodik*, Lund

Stallings, W., 1997, *Operating systems – internals and design principles,* New Jersey

7.2 Internetkällor

http://www.risknet.foa.se/it/fakta/Baltiskaringen.htm 2002-04-10

www.varnpliktsnytt.org/tidningar/2001/0114/reportage/reportage1.html 2002-02-06

http://www.protectdata.se/security/seclib_virus_school.jsp 2002-05-02

http://www.mil.se/fmforum/698/reportage2.html 2002-05-13

http://www.ambulansforum.se/PAM/forskning/ambheliseqstudie.shtml 2002-03-18

http://www.fi.se/Publikationer/debatt/t20010928.pdf 2002-03-18

www.totalforsvaret.se 2002-04-03

Hagen, H., Fahlén, J., *Informationskrigföring en definition*, 1999
http://www.algonet.se/~hhagen/infokrig.htm

Rapport om signalspaning
http://www.mil.se/fmforum/698/reportage2.html 2002-05-13

http://www.microsoft.com/sverige/security/software_threat/default.asp?threat=3 2002-05-02

Elektromagnetiska vapen – dödsstöten mot IT-säkerheten
http://www.eme.se 2002-05-02

7.3 Artiklar/rapporter

...arbetsgruppen om informationskrigföring, ”*åtgärder och skydd mot informationskrigföring*” rapport nr 1. 1997

Ystads Allehanda, *Elavbrott lamslog Ystad*, 2002-03-07

7.4 Personliga intervjuer

Björn Andersson, Säkerhetspolisen

Bo Bengtsson, Lund Energi

Sten Svensson, Skanova Networks

7.5 Övriga källor

Stallings, W., 1999, *Network security essentials*, New Jersey

regeringens proposition 2001/02:158 Sårbarhets- och säkerhetsutredningen, *SOU 2 001:41 ”Säkerhet i en ny tid”.*

8. Bilagor

8.1 Ordlista

Avtappning	
Backdoor	En hemlig ingång till ett datorsystem via nätverket
C2W	Command and Control Warfare
Checksum	Kontrollerar genom en algoritm om något har ändrats eller lästs i ett skickat meddelande
Cyberspace	Virtuellt datarum
DoS	Denial of service, åtgärd i syfte att förhindra leverans av information
EMP	Elektromagnetisk puls
GPS	Global Positioning System, ett redskap för navigation med hjälp av satellit
Hacker	Datakunnig person som ”tränger” sig in i datrosystem han/hon inte har access till
HERF	Högeffekt radiofrekvensvapen
HPM	High Power Microwave
IW	Information Warfare
Kryptering	Döljande av text med logiska krypteringsmetoder
Kryptonyckel	”Nyckel” som behövs för att kryptera upp ett krypterat meddelande
Man in the middle	En ”osynlig” vituell position mellan två datoranvändare som kommunicerar med varandra
RÖS	Röjande strålning som är oönskade signaler som avges av informationsbehandlande utrustning. Dessa oönskade signaler innehåller spår av den information som behandlas i utrustningen
Sniffning	
Trojan	Program/kod som släppts in av en användare i ett system som efter en stund exekveras

8.2 Intervjufrågor

Här finner ni bifogat de basfrågor vi utgick ifrån under den intervju vi genomförde på Blekinge Tekniska Högskola med Björn Andersson från SÄPO. Utifrån dessa ställdes en hel del följdfrågor, något vi inte kan eller anser nödvändigt att redovisa.

1. Vem kan tänkas angripa, vem är angriparen ?
2. Varför angripa, var ligger motivationen ?
3. Vilka mål (primära) har dessa angripare ?
4. Hur är det möjligt att genomföra ett angrepp ?
5. Vilka tekniker ligger bakom angreppen ?
6. Vad görs för att förhindra angrepp ?
7. Vilka konsekvenser kan dessa angrepp få ?
8. I händelse av krig, vem ansvarar för vatten, el etc. ?