C-uppsats
LIU-ITN-C--05/003--SE

Artificiella immunsystem kan inte ge säkrare datorsystem

Mats Andersson

2005-01-21

Linköpings universitet
FILOSOFISKA FAKULTETEN

Department of Science and Technology
Linköpings Universitet
SE-601 74 Norrköping, Sweden

Institutionen för teknik och naturvetenskap
Linköpings Universitet
601 74 Norrköping

LIU-ITN-C--05/003--SE

Artificiella immunsystem kan inte ge säkrare datorsystem

Examensarbete utfört i Informatik
vid Linköpings Tekniska Högskola, Campus Norrköping

Mats Andersson

Handledare Mikael Johansson
Examinator Mikael Johansson

Norrköping 2005-01-21

Avdelning, Institution
Division, Department

Institutionen för teknik och naturvetenskap

Department of Science and Technology

Datum
Date

2005-01-21

Språk
Language

☒ Svenska/Swedish
☐ Engelska/English

☐ _____

Rapporttyp
Report category

Examensarbete
☐ B-uppsats
☒ C-uppsats
☐ D-uppsats

☐ _____

ISBN

ISRN **LIU-ITN-C--05/003--SE**

Serietitel och serienummer
Title of series, numbering

ISSN

URL för elektronisk version
http://www.ep.liu.se/exjobb/itn/2005/asp/003

Titel
Title

Artificiella immunsystem kan inte ge säkrare datorsystem

Författare
Author

Mats Andersson

Sammanfattning
Abstract

Forskningen om artificiella immunsystem försöker använda människans immunförsvar som modell för hur ett datorsystem på egen hand skall kunna försvara sig mot okänt inkräktande, till skillnad från traditionella antiviruslösningar som bygger på manuell detektion av nya virus.

Denna uppsats hävdar att människans immunförsvar inte är någon relevant modell för ett artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, eftersom det finns skillnader i hur datorsystem och människor principiellt fungerar.

Ett antal hypoteser ställs upp som beläggs med data från den immunologiska forskningen, Microsofts säkerhetsbulletiner, samt virusbeskrivningar från antivirusföretaget Sophos. Hypoteserna kopplas ihop i en slutledningskedja som visar att de hypoteser som relaterar till datorsystem, inte är förenliga med de hypoteser som relaterar till människans immunförsvar, om det artificiella immunsystemet skall tillgodose användarnas behov av säkrare datorsystem.

Forskningen om artificiella immunsystem diskuteras, där de principer och antaganden som de olika lösningarna bygger på monteras ned genom att implicita inkonsistenser görs explicita. Uppsatsen avslutas med en belysning av varför hypoteserna egentligen går att belägga, där grundbulten är att människans immunförsvar skyddar behovet hos sin värd, den mänskliga individen, till skillnad från det artificiella immunsystemet, som inte är tänkt att skydda behovet hos sin värd, själva datorsystemet, utan snarare behovet hos användaren av datorsystemet.

Nyckelord
Keyword

artificiella immunsystem, datorsäkerhet, datorvirus, immunologi

Tabeller

Figurer

1 Inledning

1.1 Syfte

Forskningen om artificiella immunsystem använder människans immunförsvar som förebild för att kunna konstruera säkrare datorsystem, eftersom de traditionella ansatserna med antivirussystem inte klarar av att hantera okända angripare. Detta har till en början varit ett intressant och tilltalande perspektiv, men efter en förhållandevis omfattande inläsning på det immunologiska området, så har insikten växt fram att människans immunförsvar inte är någon relevant förebild för hur ett artificiellt immunsystem borde vara konstruerat.

Inställningen här är alltså att forskningen om artificiella immunsystem har ett felaktigt perspektiv, när den försöker använda människans immunförsvar som förebild till att konstruera säkrare datorsystem. Även om det finns mekanismer i människans immunförsvar som skulle kunna vara användbara, så medför helhetsperspektivet att man bara snuddar vid målet, där lösningen riskerar att bli ett lapptäcke, eftersom förebilden inte är relevant.

Vikten av rätt perspektiv visar sig tydligt redan i vetenskapens vagga. Utgångspunkten för antiken var att alla himlakroppar rörde sig i perfekta cirklar, eftersom himlakropparna var högre stående väsen och cirkeln var den mest fulländade formen. Alla nya observationer som gjordes av himlafenomenen var därför nödvändiga att anpassas till cirkelmodellen för att kunna accepteras och om det var någon observation som inte passade in i modellen, så avfärdades detta i termer av observationsfel.

Detta medförde att den astronomiska läran som var rådande i över ett millenium, blott var ett lapptäcke som med tiden fick allt svårare att avfärda nyare observationer som gjordes med allt bättre hjälpmedel. Astronomen Kepler gjorde omfattade beräkningar av planeternas rörelser och försökte införliva dem i den rådande modellen. Men hur han än vände och vred på de tillgängliga observationerna, så passade de inte in i modellen, eftersom han hade utgångspunkten att planeterna måste använda cirkelrörelser. Till slut förkastade han detta perspektiv och drog så småningom den revolutionerande slutsatsen att planeterna istället måste röra sig i ellipser, vilket gjorde att alla bitar elegant föll på plats. Om han inte hade varit låst vid det gamla cirkelperspektivet, så hade han säkert kommit fram till ellips-lösningen mycket snabbare.

Detta exempel vill visa på vikten av rätt perspektiv. Inställningen i denna uppsats är att människans immunförsvar är en olämplig förebild när man skall

konstruera ett säkerhetssystem för datorer och att perspektivet med ett artificiellt immunsystem är felaktigt. För detta ändamål görs en ansats att genom den hypotetisk-deduktiva metoden visa att ett självständigt artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, inte kan ha människans immunförsvar som förebild. Poängen är att undvika att resurser i onödan läggs på lösningar som endast når halvvägs. Uppsatsen riktar sig därför till forskningen inom artificiella immunsystem som förefaller vara fast besluten om att människans immunförsvar är en relevant förebild för ett artificiellt immunsystem, trots att någon ansats inte gjorts för att faktiskt verifiera ett sådant antagande.

Huvudhypotesen i uppsatsen är följande:

> *H1. Ett självständigt artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, kan inte ha människans immunförsvar som förebild.*

Upplägget är att stödja denna hypotes genom en slutledningskedja som byggs upp av ett antal delhypoteser och postulat. Delhypoteserna stöds med hjälp av immunologisk forskning, säkerhetsbulletiner från Microsoft och datorvirusbeskrivningar från antivirusföretaget Sophos. Hypoteserna presenteras i avsnittet *3 Hypoteser*. En beskrivning av hur undersökningen genomförs ges i avsnittet *4 Metod*.

1.2 Avgränsningar

Även om ett immunförsvar bör klara av både att upptäcka, identifiera och avlägsna angripare, så är grundförutsättningen för att självständigt kunna försvara sig, att man över huvud taget är medveten om att ett angrepp äger rum. Detta är den springande punkten för varje antivirusapplikation. Problemet är att existerande applikationer endast klarar av att detektera kända virus. Man söker således ett system som på egen hand skall klara av att detektera okända virus och detta är anledningen till att man försöker konstruera ett artificiellt immunsystem. Denna studie kommer därför att koncentrera sig på detektion av okända angripare. Detta gäller framförallt referensramarna, där sådant material fokuserats som relaterar till denna avgränsning.

Det immunologiska material som sökts har framförallt varit sådant som associerar till *själv-ickesjälvdiskriminering* och *tolerans*, eftersom detta är begrepp som förefaller vara centrala inom immunologin när det gäller detektion av okända angripare. Själv-ickesjälvdiskriminering handlar om att göra åtskillnad mellan det kroppsegna (själv) och allting annat (ickesjälv). Tolerans handlar om att immunförsvaret utvecklar en okänslighet för det kroppsegna, så att kroppen inte går till anfall mot sig själv. Denna problematik är kärnan inom immunologin och är även kärnan inom datorsäkerheten; hur skall datorsystemet kunna skilja mellan en legitim applikation (det kroppsegna) och ett virus (allting annat)?

De icke-legitima applikationer som undersöks är datorvirus, maskar och trojaner, eftersom dessa är centrala inom antivirusbekämpning. Studien fokuserar för övrigt på datorsystem med Microsoft Windows som operativsystem eftersom detta är ett i hög grad utbrett och välkänt operativsystem. Framförallt är merparten av förekommande datorvirus, maskar och trojaner utformade för att angripa datorer med detta operativsystem. Det bör dock noteras att Microsoft Windows i detta sammanhang endast är ett verktyg för att bekräfta huvudhypotesen. Inställningen är att studien skall kunna upprepas för vilket operativsystem som helst.

1.3 Disposition

Först görs en genomgång av den tidigare forskningen om artificiella immunsystem, följt av forskningen inom det immunologiska området. I referensramen för forskningen om artificiella immunsystem ges också en bild av hur denna forskning ser på det biologiska immunförsvaret. Uppsatsen innehåller således två immunologiska referensramar – dels hur den tidigare forskningen om artificiella immunsystem betraktar det biologiska immunförsvaret, dels hur den immunologiska forskningen betraktar det biologiska immunförsvaret. För övrigt finns en metodologisk referensram i form av en genomgång av metodteori som relaterar till denna studie. En grafisk beskrivning av uppsatsens struktur ges i figur 1.

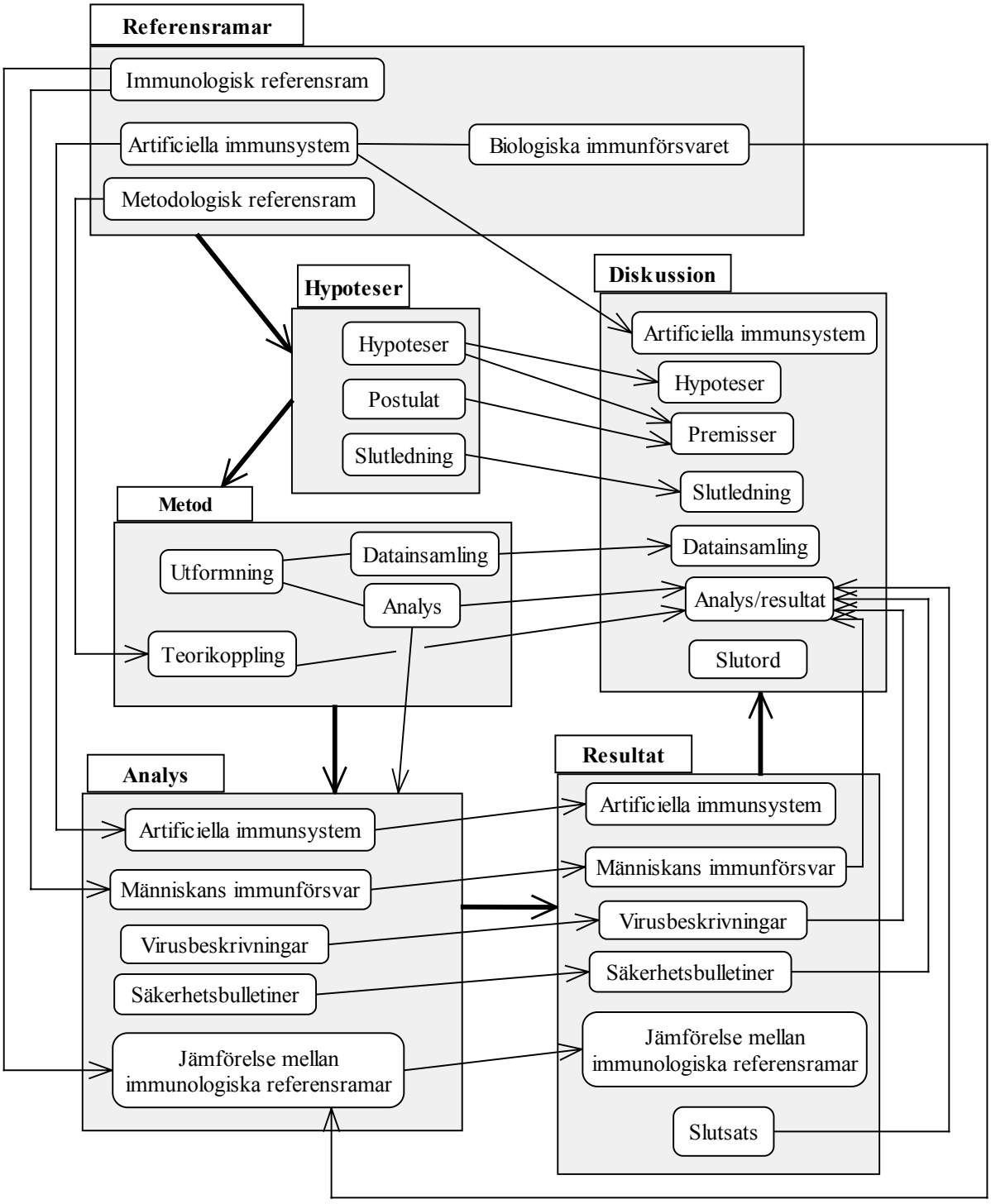
I hypotesavsnittet presenteras huvudhypotesen och de delhypoteser som är föremålet för studien. Ett antal postulat anges som tillsammans med de olika delhypoteserna bildar länkar i den slutledningskedja som leder fram till huvudhypotesen. I detta avsnitt görs också tydliga definitioner av de begrepp som relaterar till hypoteserna.

Metodavsnittet ger en ingående beskrivning av hur studien är utformad. Här finns beskrivet hur data samlas in och hur analyserna genomförs. Dessutom görs en teorikoppling, där genomförandet relateras till den metodologiska referensramen.

Analysen består i att söka belägg för de olika delhypoteserna. Den tidigare forskningen om artificiella immunsystem analyseras också. Dessutom görs en jämförelse mellan den immunologiska referensramen för denna studie och den immunologiska referensramen för den tidigare forskningen om artificiella immunsystem. Detta för att belysa eventuella skillnader i immunologisk bakgrund. Resultatet av analysen presenteras i resultatavsnittet tillsammans med en slutsats.

I diskussionsavsnittet görs en granskning av hypoteserna och framförallt de premisser som förutsätts gälla. Slutledningen granskas också. Vidare görs en

granskning av datainsamlingen, där fokus ligger på sekundära data, följt av en granskning av anlysen och resultatet, där fokus ligger på tolkning. Den tidigare forskningen om artificiella immunsystem diskuteras också, där de principer och antaganden som de olika lösningarna bygger på monteras ned genom att implicita inkonsistenser görs explicita. Uppsatsen avslutas med ett slutord som illustrerar innebörden av huvudhypotesen och varför den egentligen går att belägga.



Figur 1 *Grafisk beskrivning av uppsatsens struktur*

1.4 Konventioner

1.4.1 Språkbruk

Den immunologiska terminologin har begränsats, där så få begrepp som möjligt har tagits med. Den immunologiska teorin flödar av olika celltyper, signalsubstanser och mekanismer, men dessa har till stor del skalats bort för att ge en oinitierad läsare chansen att följa med i resonemanget. Det är principerna som ligger bakom de olika funktionerna som här är det intressanta, inte mekanismerna i sig.

Fackbegrepp används i den mån de har någon nyckelroll, förkommer på många ställen eller där begreppsförvirring skulle råda om fackbegreppet ersattes med ett mer lekmannamässigt uttryckssätt (till exempel *kroppslig* istället för *somatisk*).

Fackbegrepp som förekommer i den engelskspråkiga litteraturen, där det inte finns någon tydlig svensk anknytning och där någon vedertagen svensk motsvarighet ej har hittats, översätts inte (till exempel *germline*). Dessa begrepp förklaras istället i ordlistorna.

Begreppet *inkräktande* används i regel istället för *inkräktare*. Detta för att markera att beskrivningen avser hela den inkräktande företeelsen och inte bara den inkräktande aktören.

I uppsatsen används *vi* genomgående istället för *jag* när det gäller författarens eget resonemang. Detta beror på att författaren i regel för ett resonemang med läsaren (eller sig själv), där det helt enkelt känns naturligare att använda *vi* istället för *jag*. Likväl – det finns bara en författare till denna uppsats.

1.4.2 Definitioner

Generella stipulationer

Vetenskapsman avser person av obestämt kön som sysslar med vetenskap.
När det talas om *forskningen om artificiella immunsystem*, så avses material som publicerats i olika artiklar inom detta ämnesområde. Formuleringen *Den tidigare forskningen om artificiella immunsystem* avser vad som gjorts inom detta område innan denna uppsats.

Ordlista

Ordlistan anger hur rapportförfattaren tolkar dessa begrepp. När det gäller immunologiska fackbegrepp, så är syftet att underlätta för läsaren, så att det blir möjligt att studera rapporten utan att behöva läsa in sig på det immunologiska området. De immunologiska fackbegreppen är därför inte kopplade till någon medicinsk litteratur, eftersom dessa förklaringar i regel kräver immunologiska förkunskaper. Motsvarande resonemang gäller för övriga begrepp i ordlistan, även om läsaren förutsätts vara bekant med viss datorrelaterad jargong.

En pil (→) betyder att ordet efter pilen är relaterat till det förklarade ordet på något sätt. Ett *kursiverat* ord i en förklaring i ordlistan, anger att ordet finns förklarat på annat ställe i ordlistan.

Adaptivt immunförsvar: avser den delen av immunförsvaret som kan anpassa sig till nya former av inkräktande. → *naturligt immunförsvar*.
Affinitet: benägenhet att binda.
Agent: objekt som bevakar någonting.
Analogi: systematisk motsvarighet.
Antigen: *protein*fragment som immunförsvaret använder för att avgöra om något skall betraktas som *själv* eller *ickesjälv.* Binds till specifika *receptorer* eller *antikroppar*. I regel *peptider*.
Antigenpresenterare: immunförsvarsceller som samlar *antigen* och visar upp dem för *T-celler*.
Antikropp: molekyl som produceras av vissa lymfocyter och som kan binda till ett specifikt *antigen*.
Applikation: program i ett datorsystem.
Artificiellt immunsystem: datorsystem som använder det *biologiska immunförsvaret* som modell. Behöver inte relatera till säkerhet, utan kan användas för andra tillämpningar. → *Biologiskt immunförsvar*.
Auto-: (i sammansättningar) själv-.
Autoimmun: immun mot sig själv, vilket innebär att immunförsvaret reagerar mot kroppsegna element.
Beroende variabel: faktor som förväntas variera när man varierar den *oberoende variabeln*.
Bias: förinställning som påverkar resultatet.
Biologiskt immunförsvar: det immunförsvar som förekommer i biologiska organismer, här i regel människans immunförsvar. → *artificiellt immunsystem*.
Cell: avser alla typer av celler.
Datorvirus: i regel *självreplikerande* kod som uttnyttjar ordinära applikationer för att exekveras och spridas. Benämningen inkluderar vanligtvis även *maskar* och *trojaner*.
Detektion: upptäcka förekomsten av något.
Determinism: avser att något är förutbestämt, till exempel via *generna* som överförs via *germline*.
Differentierade celler: celler som härstammar från samma cell, men som fått olika egenskaper. Differentiering relaterar till denna specialisering.
Diskriminering: göra åtskillnad mellan till exempel *själv* och *ickesjälv*.

DNA: *germline*-överförd molekyl som består av *gener*.
Embryo: det tidiga fostret. Embryonal relaterar till detta stadium.
Evolution: utveckling genom det naturliga urvalet enligt utvecklingsläran.
Exekvering: *applikation* som körs i ett datorsystem.
Explicit uttrycklig, tydlig. → *implicit*.
Extern: som relaterar till någonting utanför ett avgränsat system. → *intern*.
Gen: ärftlig byggnadsritning över *protein*. Del av *DNA*.
Germline: celler med full *gen*uppsättning som överförs till avkomman (könsceller). Avser i regel att någonting är medfött, till skillnad från det *somatiskt* betingade.
Ickesjälv: det som inte hör till den egna organismen. → *själv*.
Immun: ej mottaglig för infektion.
Immunitet: specifik anpassning gentemot *antigen* baserad på tidigare möte, vilket ger snabbare *immunsvar*.
Immunologi: läran om immunsystemet.
Immunsvar: reaktion från immunförsvaret.
Implicit: innefattad, underförstådd. → *explicit*.
Inkonsistens: motsägelse, avvikelse, osammanhang. → *konsistens*
Integritet: oberoende mot omgivningen, okränkbarhet
Intern: som relaterar till någonting inom ett avgränsat system. → *extern*.
Konsistens: sammanhang, stabilitet. → *inkonsistens*
Kontext: sammanhanget kring något.
Lymfocyt: central immunförsvarscell. → *T-cell*.
Lymf-: relaterar till lymfsystemet, som centralt består av *tymus*, och *perifert* av andra lymfvävnader. Detta är områden där immunförsvarets funktion till stor del upprätthålls.
Mask: *datorvirus* som inte behöver något värdprogram.
Medstimulerande signal: en signal som samverkar med en annan signal vid stimulering av en cell. I uppsatsen används även begreppet ’tvåsignalsstimulering’.
Naturligt immunförsvar: avser den delen av immunförsvaret, där mekanismerna för detektion av inkräktande är medfödda. → *adaptivt immunförsvar*.
Negativ selektion: urvalsmekanism som väljer bort det som inte är önskvärt. → *positiv selektion*
Oberoende variabel: faktor som används för att kontrollera den *beroende variabeln*.
Omstrukturering: omkodning av gener som kodar för *receptorer*. Detta syftar på att generna som kodar för receptorerna plockas från en genpol och sätts samman slumpmässigt. De måste således omstruktureras innan några receptorer kan produceras.
Patogen: sjukdomsalstrande.
Peptid: beståndsdel i *protein*.
Perifer: syftar på *lymf*oida platser utanför *tymus*.
Population: gruppering av element eller individer, till exempel en befolkning.
Positiv selektion: urvalsmekanism som väljer det som är önskvärt. → *negativ selektion*.
Prenatal: perioden mellan befruktning och förlossning.
Protein: för kroppen fundamentala substanser; signalämnen och katalysatorer, består av *peptider*.

Receptor: element på en cell som kan binda till specifika element i omgivningen.
Reguljära uttryck: teknik/språk för teckenmatchning i datorsystem.
Sampling: stickprovsbaserat urval från en *population*.
Script: enklare programmeringsform som används för att styra en *applikation*, till skillnad från *exekvering*, som avser körningen av själva applikationen.
Sekundära data: befintliga data som samlats in för något annat ändamål. ’Sekundär’ relaterar till att man inte gör några egna empiriska observationer.
Själv: det som hör till den egna organismen. → *ickesjälv*. De flesta sammansättningar med *själv* i uppsatsen anger att begreppet relaterar till den egna organismen till exempel *självreaktiv*.
Självreaktiv: relaterar till att immunförsvaret reagerar mot kroppsegna substanser.
Självpeptid: kroppsegen *peptid*.
Självreplikering: självkopiering (t.ex *datorvirus* som kopierar sig själv).
Somatisk: kroppslig. Används i regel som motsats till *germline*-betingade mekanismer (medfödda).
T-cell: *lymfocyt* som utvecklas i *tymus*. En annan lymfocyt är B-cellen som utvecklas i benmärgen och som står för produktionen av *antikroppar*. Den berörs dock inte här, eftersom den i detta sammanhang inte tillför något.
Tolerans: utvecklad okänslighet för immunreaktion (immunförsvaret har lärt sig att inte reagera), i regel självtolerans → *immunitet*.
Trojan: applikation som utger sig för att vara legitim, men som innehåller skadlig kod.
Tymus: organ i bröstet som är centralt för utbildning av *lymfocyter*.

2 Referensramar

2.1 Artificiella immunsystem

2.1.1 Datorsäkerhet

Boukerche, Jucá, Sobral och Notare (2004) säger att intrång kan definieras som aktiviteter som äventyrar konfidentialitet, integritet eller tillgänglighet. Säkerhetsproblem finns i de flesta moderna datorsystem och de flesta applikationer dras med brister på olika nivåer. Marmelstein, Van Veldhuizen och Lamont (1998) menar att applikationer som webbläsare gör det enkelt att ladda hem infekterade filer, där kombinationen med agentapplikationer gör att problemet blir än mer mångfacetterat. Epostprogram och liknande agentapplikationer, med automatiska funktioner som till exempel öppnande av bifogade filer, kan bidraga till spridning av virus.

Enligt Marmelstein, Van Veldhuizen och Lamont (1998) baserar många antivirusapplikationer sina metoder på statiska fakta som inte beskriver hur okända virus skall upptäckas. Det kan till exempel vara att man använder kända bitmönster, eller regelsystem som täcker olika virusbeteenden. Resultatet blir att man måste uppdatera dessa system allt eftersom nya virus upptäcks.

Datorvirus

Skormin, Summerville och Moronski (2003) är av uppfattningen att informationsattacker antingen kan använda sig av exekverbara filer eller av någon form av script som körs genom någon applikation som interpreterar sådana. Informationsattacker följer ofta ett givet mönster, där trojaner, maskar eller virus implanteras i en värd, för att exekveras, vilket resulterar i att information sänds till en mottagare, samtidigt som attacken sprider sig till andra värdar. Enligt Boukerche, Jucá, Sobral och Notare (2004) påverkar datorvirus som första artificiella livsform det moderna samhället.

Skormin, Summerville och Moronski (2003) anger självreplikation som den gemensamma nämnaren för alla virus, där viruset kopierar sig självt, antingen till andra filer eller till andra system. Beroende på vilka metoder som viruset använder för spridning och aktivering, så kommer metoden för självreplikering att variera, eftersom det måste vara hög sannolikhet att viruset aktiveras. Det är miljön som viruset vistas i som avgör vilka metoder och implementeringar av självreplikeringsmekanismen som är möjlig.

Oda och White (2003) jämställer spam med datorvirus i det att varje motangrepp föder förändrade virus. Stoppar man ett virus, så dyker det upp i en annan skepnad.

2.1.2 Det biologiska immunförsvaret enligt den tidigare forskningen om artificiella immunsystem

Detta rubrikområde tar upp hur den tidigare forskningen om artificiella immunsystem ser på det biologiska immunförsvaret. Det bör här understrykas att förekommande begrepp och perspektiv avser hur de används av författarna i olika artiklar inom artificiella immunsystem, vilket nödvändigtvis inte är synonymt med hur den immunologiska forskningen förhåller sig till dessa begrepp och perspektiv. Syftet här är att ge en bild av hur den tidigare forskningen om artificiella immunsystem förhåller sig till det biologiska immunförsvaret.

Komponenter i det biologiska immunförsvaret

Foukia, Hassas, Fenet och Albuquerque (2003) ser människans immunförsvar som ett komplext nätverk av specialiserade celler och organ, som har utvecklats till att försvara kroppen mot sjukdomar och infektioner från främmande inkräktare. Denna uppfattning stöds av Boukerche, Jucá, Sobral och Notare (2004) och även av Marmelstein, Van Veldhuizen och Lamont (1998) som delar in immunförsvaret i en uppsättning av interagerande högnivåkomponenter:

Detektor, gör åtskillnad mellan vad som är själv och ickesjälv.
Klassificerare, typbestämmer antigen för att kunna formulera en effektiv respons.
Utrensare, eliminerar specifika antigen.
Minne, lagrar framgångsrika responser för att kunna formulera effektiva responser vid nya konfrontationer.
Adaptionsprocess, modifierar andra komponenter för att optimera systemet (i distribuerad form).

Boukerche, Jucá, Sobral och Notare (2004) gör en något annorlunda indelning av immunförsvaret:

Detektion av kemiska komponenter som finns mellan patogena fragment och lymfocyternas receptorer.
Mångfald av lymfocyter som möjliggör att det alltid finns lymfocyter med receptorer som reagerar med ickesjälv-element.
Inlärning som möjliggör att lymfocyterna specifikt anpassar sig till främmande proteinstrukturer och kommer ihåg dessa så snart det behövs.
Tolerans mot själv-gener.

Skormin, Summerville och Moronski (2003) nöjer sig med att konstatera att biologiska system har försvarsmekanismer som hanterar detektion, identifikation och destruktion av de flesta objekt som har en ogynnsam effekt på organismen, där mekanismerna på proteinnivå kan skilja mellan själv och ickesjälv. Foukia, Hassas, Fenet och Albuquerque (2003) förknippar istället de biologiska systemen med mekanismer som medger effektiva reaktioner på störningar från omgivningen, samtidigt som de anpassar sig till dessa förändringar.

Själv-ickesjälvdiskriminering i det biologiska immunförsvaret

Oda och White (2003) anser att däggdjurens immunförsvar har till uppgift att särskilja mellan själv och det möjliga hotet från ickesjälv. Luo, Cao och Wang (2001) anger att det biologiska immunförsvarets grundläggande funktion är att skilja mellan själv och ickesjälv, så att ickesjälv kan klassificeras och elimineras. För Boukerche, Jucá, Sobral och Notare (2004) är en primär egenskap hos immunförsvaret att kunna skilja mellan själv-gener och ickesjälv-gener, vilket är möjligt genom att varje cell i organismen har molekyler som kan sägas tillhöra själv-generna. Även Kim, Kim och Hong (2004) ser människans immunförsvar som en essentiell del av självförsvaret, med förmåga att skilja mellan själv och ickesjälv. Själv är här alla komponenter som behövs för normal funktionalitet, medan ickesjälv är främmande material som kan skada funktionaliteten.

Bentley (2002) förklarar diskrimineringsmekanismen med att en mångfald antikroppar genereras av lymfocyterna som hjälp till att attackera oönskade bakterier och virus i kroppen. Varje enskild lymfocyt producerar en specifik typ av antikropp, där vissa lymfocyter kommer att producera antikroppar som har förmåga att binda till de kroppsegna själv-cellerna. Immunförsvaret utnyttjar därför negativ selektion, där de lymfocyter som producerar själv-bindande antikroppar dör, vilket leder till att endast de lymfocyter som har antikroppar med förmåga att binda främmande antigen blir kvar. Immunförsvaret lär sig, av vad Hofmeyr (2004) uppfattar, att skilja mellan kroppsegna proteiner (själv) och allt annat (ickesjälv). Igenkänningen av själv eller ickesjälv baserar sig på att receptorer på lymfocyterna binds till proteinfragment, s.k peptider.

Foukia, Hassas, Fenet och Albuquerque (2003) menar att immunförsvaret normalt sett samexisterar harmoniskt med kroppsegna molekyler (själv), medan utomstående molekyler (ickesjälv), snabbt elimineras. Oda och White (2003) konstaterar att autoimmunitet således förhindras genom självtolerans, där de lymfocyter som visar sig detektera själv, dödas under mognadsprocessen. Kim, Kim och Hong (2004) påpekar dock att även om problemet med att upptäcka patogener vanligtvis beskrivs i termer av att särskilja själv från ickesjälv, så är likväl många patogener ofarliga, samtidigt som en immunreaktion mot dessa kanske skadar kroppen. Det blir därför mer relevant att säga att problemet istället handlar om att särskilja ofarligt ickesjälv från allting annat.

Det biologiska immunförsvarets detektion av vad som skall uppfattas som inkräktande

Forrest, Hofmeyr och Somayaji (1996) säger att immunförsvaret använder olika skyddsmekanismer mot olika typer av angripare. Enligt Aickelin, Greensmith och Twycross (2004) kan människans immunförsvar skydda mot patogener utan att ha någon föregående kännedom om strukturen på dessa patogener. Oda och White (2003) menar att immunförsvaret kan använda flera egenskaper för att identifiera patogener, till exempel ytan på celler och antigena proteiner.

Boukerche, Jucá, Sobral och Notare (2004) anser att lymfocyter aktiveras när en organism infekteras, där vissa lymfocyter har en förmåga att komma ihåg infektionen. Detta gör att immunförsvaret vid ett nytt angrepp av samma antigen, snabbt kan förstöra angriparen. Luo, Cao och Wang (2001) förklarar att den primära immunresponsen utlöses av en okänd patogen – antigen, vilket medför att antikroppar produceras som känner igen och kommer ihåg detta antigen. Denna process tar förhållandevis lång tid, till skillnad från sekundärresponsen, som svarar ganska snabbt, genom att korresponderande antikroppar aktiveras, till följd att antigenerna elimineras.

Oda och White (2003) uppfattar att lymfocyterna kan detektera patogenerna genom att binda till dem. Eftersom antalet antikroppar är begränsat i förhållande till antalet möjliga antigen, så används approximativ binding, där det räcker med att benägenheten att binda till ett visst antigen kommer över ett visst tröskelvärde, för att lymfocyterna skall aktiveras. Enligt Hofmeyr (2004) hanterar immunförsvaret problemet med falsklarm genom att kräva två olika typer av signaler för aktivering. Första signalen genereras genom att ickesjälv detekteras och den andra signalen när någonting har skadats. Immunförsvaret kommer därefter att reagera så mycket som är proportionellt mot skadan. Detta gör att falsklarmen inte skapar autoimmuna reaktioner, eftersom dessa inte är associerade med en skada.

Aickelin, Greensmith och Twycross (2004) tillstyrker med att människans immunförsvar kan ses som en avvikelsedetektor med mycket låga falska och missade larm. Hofmeyr (2004) menar att kroppen har så otroligt många celler att den har råd att vänta tills olika avvikelser associeras med en skada. De mikroorganismer som förorsakar skada, kommer inte att hinna föröka sig i så stor grad innan skadan upptäcks och därför är det ingen katastrof att avvakta.

2.1.3 Analogier mellan datorsäkerhet och det biologiska immunförsvaret

Hofmeyr (2004) säger att analogin borde vara väldigt kraftfull, eftersom immunförsvaret skyddar kroppen väldigt framgångsrikt i ett system med en komplexitet som är bra mycket större än alla nätverk sammantagna i hela världen. Foukia, Hassas, Fenet och Albuquerque (2003) menar att de biologiska systemen har egenskaper som permanent anpassning och

självorganisation, samtidigt som de är robusta – egenskaper som är intressanta ur ett datorsystemsperspektiv. Även Forrest, Hofmeyr och Somayaji (1996) anger egenskaper hos det biologiska immunförsvaret som har stor betydelse för ett robust datasäkerhetssystem:

- Distribuerad detektion
- Probabilistisk detektion
- Detektorerna måste även kunna upptäcka främmande objekt som de inte stött på tidigare

Boukerche, Jucá, Sobral och Notare (2004) ser likheter i att immunförsvaret fungerar som skydd för kroppen mot sjukdomsalstrande organismer, på samma sätt som säkerhetssystemen i datorer skyddar mot illasinnade användare. I tabell 1 listar de ett antal gemensamma aspekter mellan människans immunförsvar och det artificiella immunsystemet

Tabell 1 *Gemensamma aspekter mellan människans immunförsvar och det artificiella immunsystemet (Boukerche, Jucá, Sobral och Notare, 2004)*

	Människans immunförsvar	Artificiellt immunsystem
Integritet	Den genetiska koden får inte ändras av patogener.	Data får inte avsiktligt eller av misstag bli fördärvade.
Tillgänglighet	Kroppen måste fortsätta arbeta när den attackeras av patogener.	Data måste finnas tillgängliga när de behövs.
Beriktigande	Immunförsvaret får inte attackera kroppens egna celler.	Falsklarm måste minimeras.
Ansvarsfullhet	Immunförsvaret måste identifiera, hitta och förstöra de sjukliga elementen.	Information om angrepp måste bevaras, så att det kan spåras.
Konfidentialitet	–	Tillträde till data får bara ges till legitima användare.

Själv-ickesjälv-konceptets relevans för datorsäkerhet

Forrest, Hofmeyr och Somayaji (1996) anser att datasäkerhetsmetoder som baserar sig på hur det biologiska immunförsvaret urskiljer själv från ickesjälv bör ge en tydligare uppfattning om identitet och erbjuda ett förbättrat generellt skydd för traditionella system. Dozier, Brown, Hurley och Cain (2004) säger att intrångsdetektion kan ses som ett problem, där det gäller att avgöra om nätverkstrafik är normal eller onormal, det vill säga själv eller ickesjälv. Lee, Kim och Hong (2004) menar att immunologer traditionellt beskriver människans immunförsvar med problemet att kunna skilja ut själv från ickesjälv, där ickesjälv sedan avlägsnas. Datorsäkerhet kan karakteriseras på ett liknande sätt, där det gäller att särskilja mellan godartade och elakartade program.

Foukia, Hassas, Fenet och Albuquerque (2003) uppfattar att immunförsvaret liksom datorsäkerhetssystem använder konceptet med säkert och icke säkert

beteende. Bentley (2002) föreslår att på samma sätt som immunförsvaret utnyttjar negativ selektion för att göra sig av med de lymfocyter som binder till kroppsegna celler, så kan detektorer i datorsystem som triggas av normalt beteende raderas, till förmån för resterande detektorer som då triggas för onormalt beteende. Foukia, Hassas, Fenet och Albuquerque (2003) konstaterar dock att det har visat sig svårt att isolerat använda avgränsade abstrakta processer från immunförsvaret, eftersom slumpvist genererade detektorer som skall handskas med verklig nätverkstrafik blir ineffektiva.

Hofmeyr (2004) ser dock inte analogin som självklar, utan konstaterar att det har förutsatts att distinktionen mellan själv och ickesjälv skulle vara fundamental inom datorsäkerhet eftersom den är fundamental inom immunologin. För att kunna tillämpa immunförsvarsanalogin, måste man hitta det i datorsystemet som kan jämställas med immunförsvarets peptider.

Spam

Eftersom spam generellt sett inte är lika katastrofalt som virus, så kan man som Oda och White (2003) uttrycker det, säga att spam motsvaras av en vanlig förkylning; mer en obekvämlighet än en stor infektion. Immunförsvaret kan inte upptäcka och avlägsna varje infektion innan vi blir sjuka, men eftersom det lär sig av erfarenheten, så kan framtida motattacker komma snabbare. Även om det är svårt att bekämpa spam, så förefaller det logiskt att bekämpa en sådan anpassningsbar ’sjukdomsalstrare’ med ett anpassningsbart system.

2.1.4 Skillnader mellan det biologiska immunförsvaret och ett artificiellt immunsystem

Hofmeyr (2004) säger att immunförsvaret inte är en efterhandskonstruktion, utan har utvecklats parallellt med kroppen. Tänker man sig ett immunförsvar isolerat från själva kroppen, så ser man bara halva bilden, speciellt då kroppen utvecklats till att vara lättskyddad. De biologiska hoten är extremt sofistikerade och har utvecklats under väldigt lång tid. Detta gör att människans uppfinnesrikedom i nuläget har svårt att matcha evolutionen, eftersom de skadliga organismerna inte har utvecklats från början, utan bygger på existerande mikroorganismer. Marmelstein, Van Veldhuizen och Lamont (1998) menar att det artificiella immunförsvaret inte har de evolutionära anpassningsmekanismerna som det biologiska immunförsvaret besitter, eftersom det är ett diskret system.

Enligt Hofmeyr (2004) finns det ingen direktmappning mellan våra kroppar och ett datorsystem. Konfidentialitet har till exempel ingen motsvarighet hos immunförsvaret, eftersom immunförsvaret bara har utvecklats för att upprätthålla tillgänglighet och integritet. Forrest, Hofmeyr och Somayaji (1996) uppfattar dessutom att självdefinition i ett datorsystem förefaller ha större dynamik än i det biologiska immunförsvaret, eftersom användare regelmässigt uppdaterar programvara, redigerar filer och kör nya program.

Hofmeyr (2004) anser att om själva överensstämmelsen är dålig, så blir analogin oanvändbar. Man måste därför bygga datorsystem som till naturen är mer biologiska om man skall utnyttja analogin fullt ut.

Kim, Kim och Hong (2004) konstaterar att det biologiska immunförsvaret är effektivare på grund av parallellismen, där lymfocyterna rör sig helt oberoende av varandra. Det artificiella immunsystemet aktiveras seriellt, på grund av en begränsad uppsättning processorer.

2.1.5 Förutsättningar för ett artificiellt immunsystem

Viktiga egenskaper för ett artificiellt immunsystem är enligt Lee, Kim och Hong (2004) att kunna upptäcka avvikelser och ha en förmåga till anpassning, vilket åstadkommes genom distribuerbarhet, självständighet och mångfald. Marmelstein, Van Veldhuizen och Lamont (1998) ser virusdetektion, viruseliminering och skadereparation som kandidater i ett artificiellt immunsystem som kan ha evolutionära mekanismer. De anser att det istället för traditionella antiviruslösningar behövs ett mer robust säkerhetssystem, som automatiskt anpassar sig till nya virushot, genom att använda sig av komponenter som är analoga till det biologiska immunförsvaret:

Detektera virus. Oavsett om systemet tidigare stött på ett virus eller om det är ett nytt exemplar, så måste det kunna upptäckas med någon scanning-teknik.
Klassificera virus. Viruset måste isoleras och identifieras på grundval av vilka egenskaper det har.
Extrahera signatur. Signaturen extraheras från en infekterad fil, om det inte direkt är möjligt att klassificera viruset.
Avlägsna virus. Med hjälp av virusets signatur lokaliserar man de delar av systemet som infekterats och avlägsnar därefter viruset.
Identifiera och reparera skada. Skadade systemresurser identifieras och återställs till det oinfekterade tillståndet.
Uppdatera virusdatabas. Information om virus som tidigare inte varit i kontakt med systemet sparas, så att det är möjligt att känna igen viruset nästa gång.

Forrest, Hofmeyr och Somayaji (1996) anger en lämplig definition av själv som en viktig förutsättning för ett säkerhetssystem som baserar sig på det biologiska immunförsvaret. Eftersom systemets normala beteende hela tiden skiftar, måste ett väldefinierat själv vara anpassat till användarens legitima aktiviteter, samtidigt som det är känsligt för främmande, farliga aktiviteter. En snävare självdefinition kommer att ge många falsklarm, medan en vidare definition missar många otillbörliga aktiviteter. Marmelstein, Van Veldhuizen och Lamont (1998) varnar dessutom för att göra processen alltför felsäker, så att inte boten blir värre än infektionen.

2.1.6 Definition av vad som skall betraktas som icke inkräktande i datorsystem

Forrest, Hofmeyr och Somayaji (1996) säger att det är rimligt att avgränsa fokus för självdefiniering till systemanrop i operativa processer eftersom skador på systemet åstadkommes av program som utför systemanrop. Själv likställs med normalt beteende, där korta sekvenser av systemanrop i operativa processer används som stabila signaturer för normalt beteende. Detta är möjligt eftersom signaturerna under normala omständigheter håller sig något så när konstanta, samtidigt som de är specifika för varje process. När attacker förekommer blir signaturerna i hög grad turbulenta, vilket kan användas som en förhållandevis okomplicerad, men ändå effektiv detekteringsprincip.

Forrest, Hofmeyr och Somayaji (1996) bygger initialt upp en databas med normalt beteende, som består av korta sekvenser av systemanrop. Sedan samlas data in om rådande beteende, som matchas mot det normala beteendet i databasen. Principen med systemanrop förutsätter att en avgränsad kort sekvens av systemanrop i ett program är konsistent under normalt beteende och att uttnyttjande av säkerhetshål uppenbarar avvikande sekvenser. Det finns emellertid begränsningar med att använda systemanrop som detekteringsprincip, eftersom det blir svårt att upptäcka en inkräktare som använder någon annans identitet, till exempel genom att använda någon annans lösenord.

2.1.7 Detektion av vad som skall uppfattas som inkräktande i datorsystem

Detektion av vad som skall uppfattas som inkräktande i datorsystem med hjälp av detektorer

Marmelstein, Van Veldhuizen och Lamont (1998) beskriver intelligenta agenter som kontrollerar immunsystemsaktiviteterna i det enskilda datorsystemet genom att använda lockbetesprincipen. Lockbeten är program som har till enda uppgift att indikera att de har smittats med virus. Fördelen med detta är att det inte ger några falsklarm, samtidigt som viruskoden enkelt kan isoleras, eftersom koden hos lockbetet är känd. Eftersom det inte finns någon garanti för att ett virus kommer att attackera ett generellt lockbete, så bör lockbetena utformas med egenskaper som gör dem speciellt attraktiva för virus. Dessa egenskaper varierar dessutom med olika typer av virus.

Marmelstein, Van Veldhuizen och Lamont (1998) skapar generella lockbeten utifrån en genetisk, evolutionsinfluerad algoritm, där en population av lockbeten produceras och sprids i systemet. Infekterade lockbeten klassificeras och matchas mot ett bibliotek för att kunna ta fram en uppsättning detektorer för själv-ickesjälvdiskrimminering, så att viruset skall kunna detekteras. Detta möjliggör att viruset kan identifieras, så att övriga filer i systemet kan testas för

infektion. Om viruset tidigare ej påträffats i systemet, så extraheras det ur den infekterade filen, där specifika detektorer för viruset sedan skapas. Lee, Kim och Hong (2004), som hänför uppslaget till lockbetesprogram till immunförsvarets distribuerade karaktär och dess mångfald, menar dock att det inte finns något som garanterar att ett virus faktiskt attackerar ett lockbete.

Dozier, Brown, Hurley och Cain (2004) säger att ett typiskt upplägg för intrångsdetektering som baserar sig på artificiella immunsystem, är att klassificera nätverkstrafik som själv och ickesjälv. Varje immunsystemsvärd utvecklar en population av detektorer, som för ett specificerat antal datapaket utsätts för normal nätverkstrafik, där de detektorer som matchar något datapaket plockas bort. De detektorer som överlever denna negativa selektion, kommer således i fortsättningen att matcha ickesjälv-paket. Här finns också ett inslag av dubbel stimulering, där det krävs en verifikation från nätverksadministratören, att det rör sig om en regelrätt attack. Om bekräftelse från administratören ej kommer inom föreskriven tid, så kommer detektorn istället att plockas bort. Verifikationen förvandlar detektorn till en minnesdetektor som kommer ihåg den specifika attacken. Denna detektor fungerar som en starkare indikator på att en attack ägt rum.

Hos Foukia, Hassas, Fenet och Albuquerque (2003) undersöker intrångsdetekteringsagenter det aktuella tillståndet på program i systemet och jämför det med normal aktivitet. När avvikelsen överstiger ett tröskelvärde är det en indikation på ett intrång. Tröskelvärdet sätts av säkerhetsadministratören som en toleransnivå.

Detektion av självreplikering i datorsystem

Lee, Kim och Hong (2004) anger en trestegsprocess för att detektera virusapplikationer:

Steg1: Alla existerande program är legitima.
Steg2: Alla inkommande eller ändrade program är misstänkta.
Steg3: Program som uppvisar virusbeteende detekteras.

Detekteringen bygger på att bitmönster (ettor och nollor) extraheras från de misstänkta programmen som inte förekommer i några legitima program. Om samma bitmönster kan extraheras från flera program, så klassificeras det som ett virus under antagandet att virus har en tendens att smitta andra program. Bitmönstren extraheras från början av filen, eftersom de flesta virus exekverar viruskoden först.

Skormin, Summerville och Moronski (2003) ser självreplikering som en förutsättning för att merparten av datorvirus och maskar skall spridas, samtidigt som det är tämligen ovanligt för legitim kod. Självreplikeringen är programmerad och kan åstadkommas på ett flertal sätt, men eftersom antalet sätt definitivt är begränsat, så är självreplikeringen möjlig att detektera.

Detektion av vad som skall uppfattas som spam

Oda och White (2003) klassificerar språkliga uttryck i epostmeddelanden efter hur frekvent förekommande de är i spam respektive legitima mail. Sådana ’genbibliotek’ kan byggas upp från källor som ordlistor, html- och javascriptkod eller kända spamadresser. Digitala ’lymfocyter' har i dessa immunsystem receptorer som kan binda till epost-meddelanden, genom att reguljära uttryck används som antikroppar. Här finns dock en skillnad mot det biologiska immunförsvaret som har tillgång till hela uppsättningen själv-proteiner, medan spam-immunsystemet inte kan försäkra sig om att en lymfocyt inte ser ett legitimt meddelande som spam. Genom att en användare kan bekräfta om något är spam eller ej, så kan de digitala lymfocyterna öka eller minska sin benägenhet att binda till ett meddelande. Det gör att man med tiden kommer runt problematiken med att legitima meddelanden klassas som spam och vice versa.

Övervakning av datorsystemets immunsystem

Kennedy (Kennedy, 1998) säger att en vanlig form av självdefinition görs utifrån mönster för normalt beteende, där det som avviker betraktas som ickesjälv. Om det däremot är själva detekteringsprocessen som angrips, så behövs någon slags övergripande metaprocess som övervakar detekteringsprocessen. Men eftersom denna metaprocess i sin tur skulle kunna angripas, så förefaller det som om det alltid måste finnas någon punkt i immunsystemet som saknar övervakning. Kennedys ansats här är att låta ömsesidigt reflekterande agenter bevaka varandra genom att de utför närliggande uppgifter i symbios med varandra. De jobbar oberoende av varandra, men varje agents funktionalitet är beroende av de andra agenternas operationer. När beteendet hos en infekterad agent påverkar funktionaliteten hos en annan agent, så betraktas detta som ett angrepp. Konceptet rymmer även möjligheten att reparera en skadad agent genom att den helt enkelt repareras av den agent som påverkats i sin funktionalitet.

2.1.8 Problem med olika lösningar för artificiella immunsystem

Hofmeyr (2004) anser att vi är begränsade i våra immunologiska kunskaper. Att tillämpa en analogi, när man inte till fullo förstår alla mekanismer i modellen kan leda en på villovägar. Lee, Kim och Hong (2004) säger att negativ selektion lämpar sig bäst för stabila system, eftersom den mänskliga kroppen karakteriseras av ett stabilt tillstånd, till skillnad från ett datorsystem. Dozier, Brown, Hurley och Cain (2004) uppfattar att intrångsdetektering som är baserad på artificiella immunsystem har nackdelen att det inte går att veta vad det är för typ av attacker som undgår upptäckt.

För Marmelstein, Van Veldhuizen och Lamont (1998) är kanske det största problemet att få till stånd den parallellism som finns i det biologiska

immunförsvaret, där varje lymfocyt är en oberoende agent som parallellt med andra lymfocyter söker efter antigen samtidigt. Faktorer som begränsar det parallella sökandet efter virus i datorsystem är antalet processorer, konkurrens om processortid och delade resurser. Eftersom det krävs omfattande datorresurser för att testa olika lösningar på ett stort antal av existerande virus, så blir en implementering på ett enskilt system opraktisk.

2.2 Immunologisk referensram

2.2.1 Determinism

Här presenteras sådant som relaterar till förutbestämda mekanismer i immunförsvaret. Det avser i regel medfödda faktorer som kontrolleras på genetisk väg. Rent principiellt kan deterministiska utgångspunkter liknas vid att något ihopvecklat vecklas ut till en given struktur. Om man till exempel tar ett pappershus, som man plattar till och viker ihop, så kommer detta när det vecklas ut igen att resultera i det ursprungliga pappershuset. Poängen är att evolutionen verkar på fullt utvecklade individer, där vissa gener förs vidare till individernas avkommor, som i sin tur ’vecklas ut’ till förutbestämda individer. Även om dessa individer påverkas av miljön, så är plattformen given.

Immunförsvarets generella förutsättningar

Vander, Sherman och Luciano (1998) säger att varje mänsklig organism härstammar från det befruktade ägget, som delar sig och ger upphov till två nya celler, som i sin tur fortsätter att dela sig och så vidare. Cellerna differentieras och specialiserar sig på olika saker, där de grupperar sig i olika vävnader, som i sin tur formar olika organ. Detta gör att den mänskliga kroppen kan betraktas som ett komplext samhälle av differentierade celler som utför essentiella funktioner som borgar för organismens överlevnad. Immunförsvaret utgörs av de celler som kollektivt försvarar organismen, utan att vara ett anatomiskt sammanhängande organsystem. Dessa celler producerar budbärare som reglerar funktionerna hos immunsystemet.

Enligt Guyton och Hall (2000) är det generna som finns i kärnan i alla celler, som kontrollerar de vardagliga funktionerna i kroppens alla celler, genom att bestämma vilka substanser som syntetiseras i cellen. Merparten av dessa substanser är enzymer, som främjar olika kemiska reaktioner i cellerna. Generna och deras reglerande mekanismer bestämmer cellreproduktionen, vilket innebär att det genetiska systemet kontrollerar varje steg i människans utveckling.

Alberts et al (2002) menar att den genetiska informationen mest består i instruktioner för tillverkning av protein. Proteinerna är de makromolekyler som i huvudsak upprätthåller cellernas funktionalitet, bland annat genom att reglera hur generna kommer till uttryck. Individens utveckling bestäms enligt Vander, Sherman och Luciano (1998) av uttrycket av genuppsättningen som ärvs i och med befruktningen. Alberts et al (2002) anser att DNA är ett språk som alla levande celler, oberoende av organism, har gemensamt. Det är därför som det är möjligt att en bit DNA som stoppas in i en bakterie, ändå kan processas och kopieras.

Chaplin (2003) bryter ned mekanismen som medger igenkänning av antigen i två kategorier:

- Respons som är hårdkodad genetiskt i germline och som känner igen generella drag hos många mikroorganismer (naturligt immunförsvar).
- Respons som är kodad i genetiska element med förmåga att somatiskt omstruktureras till att specifikt kunna matcha individuella mikroorganismers strukturer (adaptivt immunförsvar).

Langman och Cohn (2000a) förklarar somatisk selektion som ett urval av olika celler i organismen, till skillnad från germline-selektion, där urvalet görs på organismen som helhet.

Det naturliga immunförsvaret

Medzhitov och Janeway (2000) säger att det naturliga immunförsvaret är kodat via germline. Medfödda immunreceptorer för självproteiner har avlägsnats under evolutionen eftersom de blir skadliga för organismen, vilket medför att det naturliga immunförsvaret aldrig kommer att självreagera. Receptorerna kodas via germline och uttrycks utan att omstruktureras. Enligt Re och Strominger (2004) är det naturliga immunförsvaret avhängigt de immunförsvarsceller som känner igen element från mikroorganismer genom germline-kodade receptorer.

Fazekas de St Groth (1998) menar att receptorerna för främmande antigen genom evolutionen har blivit kodade i germline för att de känner igen gemensamma drag hos ett antal olika patogena organismer. Den uppfattningen delas av Kyewski, Derbinski, Gotter och Klein (2002). Miller (2004) beskriver det som att det naturliga immunförsvaret primärt har utvecklats till att känna igen molekylära strukturer som kännetecknar bakterier. Detta är en kraftfull, om än elementär diskriminering mellan själv och ickesjälv.

Det adaptiva immunförsvaret

Flajnik och Kasahara (2001) säger att alla de gener som definierar det adaptiva immunförsvaret går tillbaka till de äldsta ryggradsdjuren. Det gäller såväl T-cellsreceptorer, som antikroppar och de gener som hanterar processen som omstrukturerar de gener som kodar för receptorerna. Enligt Benjamini, Sunshine och Leskowitz (1996) föds individen med förmågan att mot

främmande inkräktare rikta ett immunsvar, även om immuniteten förvärvas genom kontakt med inkräktarna. Tauber (2000) menar att organismen förändras som svar på olika beteenden, inom ramarna för denna genetiskt programmerade, strukturella och funktionella kapacitet.

Silverstein och Rose (2000) konstaterar att det finns bevis som pekar på att immunförsvaret kan skapa receptorer för varje själv- och ickesjälv-element. Denna förmåga är genetiskt betingad, även om germline i sig inte innehåller någon patogenspecifik information. Livák och Petrie (2001) säger att de germline-kodade gensegmenten omstruktureras genetiskt till en avgränsad sekvens som kodar för antikroppar eller T-cellsreceptorer.

Benjamini, Sunshine och Leskowitz (1996) förklarar att immunförsvaret använder en strategi för att slippa koda för alla upptänkliga receptorer för antigen. Immunförsvaret kan utifrån ett begränsat antal gensegment koda för ett mycket stort antal receptorer. Detta sker genom att gensegmenten struktureras olika för varje lymfocyt-kopia. Exakt hur denna process går till är inte klart, men den antas vara slumpmässig. Alam och Gorska (2003) ser den också som slumpmässig, där variationen i genernas omstrukturering ger mer än 10^{14} olika kombinationer. Schatz (2004) tolkar dock det enzym-maskineri som utför omstruktureringen, som en nödvändig egenskap för det adaptiva immunförsvaret, där nyckeln är ett protein som kodas av en specifik gen.

Enligt Schatz (2004) är de gener som kodar för antikroppar och T-cellsreceptorer de mest märkliga och formbara inom biologin. Detta eftersom de passerar germline i en fragmenterad och ofunktionell form, där de sedan måste sättas samman somatiskt under utvecklingen av lymfocyter. Flajnik och Du Pasquier (2004) ser det som att människans adaptiva immunförsvar bland annat definieras av de gener som är inblandade i omstruktureringen, där det med sina slumpmässigt genererade och mångfald av antigen-receptorer, har potentialen att klara sig från varje inkräktare.

2.2.2 Immunförsvarets definition av vad som skall betraktas som icke inkräktande

Immunförsvarets definition av vad som skall betraktas som icke inkräktande baserad på mognad

Langman och Cohn (2000a) säger att ett embryo, för att kunna överleva, skyddas av modern mot infektioner. Skyddet medför att embryot inte innehåller något ickesjälv, samtidigt som själv definitivt finns närvarande. Detta är de grundläggande egenskaper som möjliggör antigenseparation och det spelar ingen roll för bedömningen vilka de kemiska egenskaperna är, blott att ickesjälv-antigenerna inte är närvarande initialt. För att uppnå självtolerans, så elimineras enligt Dighiero och Rose (1999) under det embryonala stadiet de självreaktiva lymfocyterna, där de självantikroppar som eventuellt förekommer endast är ett resultat av somatisk förändring.

Langman och Cohn (2000a) konstaterar att immunförsvarets uppfattning om själv, således grundläggs tidigt och bevaras livet ut för individen. Det är ett tidsperspektiv som vida överstiger livslängden för den enskilda cellen, vilket innebär att själv-informationen förvärvas somatiskt. Detta sker genom att procedurella regler kollektivt förmedlas via cellerna i en population, men där den enskilda cellen inte besitter någon kunskap. Rose (1999) anser dock att toleransutveckling inte är något som är förbehållet det ofödda fostret, eftersom det experimentellt går att visa att vuxna kan utveckla tolerans mot ett injicerat antigen. Det finns dock betydande kvantitativa skillnader, beroende på immunförsvarets mognad, hur lätt det är att framkalla tolerans.

Kyewski, Derbinski, Gotter och Klein (2002) finner det väl belagt att omogna lymfocyter som möter antigen utvecklar självtolerans genom att inaktiveras eller förstöras. Miller och Basten (1996) menar emellertid att det inte är något unikt i sig med den prenatala perioden beträffande tolerans.

Immunförsvarets definition av vad som skall betraktas som icke inkräktande genom fastställande av den egna identiteten

Chen (2001) föreslår att antigen-igenkänningen baseras på DNA-sekvensen i sin helhet, eftersom sekvensen specificerar vad som är själv. Miller (2004) konstaterar dock att även om själv skulle kunna konstitueras av de gener i DNA som kodar för dess antigener, så är det inte möjligt att tänka sig någon mekanism som skulle kunna granska allt innehåll i DNA.

Langman och Cohn (2000a) säger att själv-ickesjälvdiskriminering är nödvändig eftersom varje destruktiv försvarsmekanism måste kunna skilja mellan värd och patogen. Enligt Chen (2001) är den rådande inställningen att tymus är ett universitet som utbildar T-cellerna att känna igen främmande antigen och ignorera den uppsjö av självantigen som finns tillgängliga i kroppens egna vävnader. I klassisk immunologi definieras själv under individens utveckling, där självtoleransen fastställs genom att immunförsvaret rensar ut självreaktiva lymfocyter. Detta gör att närvaron av antigen har kritisk betydelse. Om det inte skapas tolerans för kroppens eget material, så skulle alla sorters autoimmuna sjukdomar bli följden.

Medzhitov och Janeway (2000) menar att det adaptiva immunförsvaret kodas genom att gensegment på lymfocyternas receptorer omstruktureras, för att sedan sorteras i självreaktiva (självbindande) och självtoleranta (ickesjälvbindande). Kruisbeek och Amsen (1996) säger att de T-celler i utvecklingsstadiet, som har antigen-receptorer som möjliggör självreaktivitet, triggas att dö när deras antigen-receptorer stimuleras i tymus. Vander, Sherman, och Luciano (1998) förlägger en sådan process till fostertiden och i början efter födseln, där T-celler exponeras för självproteiner i tymus och där de T-celler som binder självproteiner förstörs.

Miller och Basten (1996) säger att det först är på 90-talet som man experimentellt kunnat visa att självreaktiva lymfocyter förstörs genom negativ

selektion i tymus. Ohashi och DeFranco (2002) menar dock att även om tymus står för en viktig initial mekanism, där självreaktiva T-celler elimineras, så kan tolerans mot dessa inte uppnås i Tymus, eftersom många proteiner som är specifika för olika vävnader inte kommer till uttryck där i tillräcklig omfattning. Kruisbeek och Amsen (1996) är dock av den uppfattningen att perifer T-cellsförstörelse kan underhålla tolerans mot själv-antigen och även reglera nivå och varaktighet av immunsvar. Tauber (2000) konstaterar likväl att själv-konceptet har fungerat som en modell för en entitet som immunförsvaret skyddar, men att det står allt mer klart att något sådant avgränsat objekt inte existerar.

Immunförsvarets definition av vad som skall betraktas som icke inkräktande baserad på närvarande celler

Silverstein och Rose (2000) anger den negativa selektionen i tymus på T-celler som för tillfället finns närvarande, som den främsta centrala mekanismen för att nedreglera immunsvaret. Kruisbeek och Amsen (1996) finner dock att även om den negativa selektionsprocessen förstör T-celler med receptorer specifika för självpeptider, så är den långt ifrån perfekt. Alla självpeptider som T-cellerna kan möta under sin livstid presenteras inte för dem under utvecklingen, samtidigt som stimuleringen kanske inte når över ett visst tröskelvärde, något som tillstyrks av Rose (1999). Enligt Alam och Gorska (2003) finns det bevis på att en del självreaktiva T-celler klarar sig igenom processen, eftersom en del specifika självantigen helt enkelt inte finns närvarande i tymus.

Immunförsvarets definition av vad som skall betraktas som icke inkräktande baserad på affinitet

Alam och Gorska (2003) säger att de T-celler som har stor förkärlek för självpeptider och således är självreaktiva, kommer att dödas i den negativa selektionsprocessen, medan de T-celler som inte binder så starkt till självpeptider dock klarar sig. Detta stöds av Hanahan (1998), Grossman och Paul (2000), samt Miller och Basten (1996). Enligt Silverstein och Rose (2000) beror det på att den negativa selektionen i tymus inte är tillräckligt finmaskig, utan tillåter att T-celler som är specifika för självantigen passerar så länge de inte har tillräckligt hög affinitet.

Immunförsvarets definition av vad som skall betraktas som icke inkräktande baserad på varaktighet

Langman och Cohn (2000a) hänför själv till det som är varaktigt och som upprätthålls under organismens hela livstid, till skillnad från ickesjälv som är temporärt. Problemet är bara hur detta skall tolkas. Om själv är en fastställd uppsättning element, kan varaktigheten bestämmas genom generella egenskaper som alla självelement har gemensamma. Skulle själv däremot bestå av element i kontinuerlig förändring, så måste själv-ickesjälvdiskrimineringen utgå ifrån någon fördefinierad lista för varje element som anger vad som är

normal takt, vilket dock borde innebära att själv vore ett resultat av germline-selektion.

Immunförsvarets definition av vad som skall betraktas som icke inkräktande baserad på kombinerade faktorer

Förutom att själv bestäms av antigen-egenskaper, så anser Miller (2004) att fler faktorer måste avgöra hur själv definieras:

- *Individens utvecklingsstadium*. Immunologisk tolerans utvecklas före födelsen och därefter utvecklas immunitet. Detta kan dock inte vara någon nyckelfaktor, eftersom hela immunrepertoaren inte är tillgänglig prenatalt.
- *Lymfocytens mognad*. Omogna lymfocyter som möter antigen förstörs, medan mogna lymfocyter aktiveras.
- *Mötesplats*. Negativ selektion i tymus, där T-celler med stor affinitet för själv-antigen förstörs. T-celler som klarat den negativa selektionen och tar sig utanför tymus, möter friska vävnader som avsöndrar antigen i en viss takt, vilket T-cellerna ignorerar. Om takten däremot överstiger ett visst tröskelvärde, så aktiveras T-cellerna.
- *Medstimulerande signaler*. Lymfocyter aktiveras bara om en stimulans från ett antigen följs av en medstimulerande signal från antigenpresenteraren.
- *Farligt*. Immunförsvaret diskriminerar mellan farligt och ofarligt, snarare än själv-ickesjälv. Detta perspektiv får dock svårt att förklara vissa experimentella exempel, till exempel transplantation, vilket immunförsvaret under evolutionen inte kan ha lärt sig att betrakta som farligt, eftersom transplantationer inte förekommer i naturen.

Silverstein och Rose (2000) anser att de regler som styr alla aspekter av immunsvaret gäller för alla immonogener, oavsett om de är själv eller ickesjälv, skadliga eller harmlösa. För Langman och Cohn (2000) är det möjligt att definiera själv som varaktig, såväl som ofarlig eller oinfekterad, men det viktiga är att definitionen innehåller en identifierbar distinktion gentemot ickesjälv. Det är troligt att denna åtskillnad inte kan göras av någon enskilt reglerande mekanism.

2.2.3 Immunförsvarets detektion av vad som skall uppfattas som inkräktande

Det finns, av vad Dembic (2000) erfar, lite olika sätt att se på detektion av inkräktande, där ”farlig”-ansatsen säger att det räcker att känna igen cellrelaterat material, medan ”främlings”-ansatsen kräver igenkänning av egenskaper hos inkäktaren. ”Integritet”-ansatsen innebär att immunförsvaret reagerar på ett avbrott i det cellulära signalflödet, samtidigt som ”ignorerings”-ansatsen säger att lymfocyterna är passiva, tills en antigenpresenterande cell dyker upp och möjliggör tvåsignalsstimulering.

Immunförsvarets detektion av vad som skall uppfattas som farligt

Ohashi och DeFranco (2002) tror att immunförsvaret kan ha utvecklats till att känna igen ”farliga” signaler som bidrar till aktivering av adaptiva immunsvar, eftersom skador som förorsakar skada på vävnaderna ofta associeras med infektion. Det finns dock, av vad Silverstein och Rose (2000) uppfattar, inga element i immunsvaret som klarar av att skilja mellan skadligt och ofarligt. Balansen mellan att försvara och att förstöra bestäms av fysikaliska och kemiska egenskaper, mängd, plats och varaktighet hos det som orsakar reaktionen. Rose (1999) anser dessutom att antikroppar framkallas av både patogener och ofarliga substanser, vilket således innebär att immunsvaret inte kan vara en reaktion på fara.

Immunförsvarets detektion av vad som skall uppfattas som inkräktande baserad på mognad

Miller och Basten (1996) ser inte steget i utvecklingsprocessen som avgörande för immunsvaret, utan lymfocytens mognadsgrad vid mötet med ett antigen. Omogna lymfocyter som möter antigen förstörs eller inaktiveras, samtidigt som mogna lymfocyter utlöser immunitet. Rose (1999) menar att det inte är någon fundamental skillnad på självantigen och ickesjälvantigen, utan att det handlar om timing och förhållanden under presentationen av antigen för immunförsvaret.

Immunförsvarets detektion av vad som skall uppfattas som störning

Grossman och Paul (2000) säger att kontexten där självantigen känns igen, i regel skiljer sig från kontexten med infekterande antigen, eftersom själv är kontinuerligt närvarande, medan infektion ger sig tillkänna i form av en störning. Karakteristiskt för akuta infektioner är en snabb ökning initialt i koncentrationen av antigen, antigenpresenterarnas aktiveringsgrad och antalet infekterade celler. Om förändringen sker gradvis till samma mängd antigen, så kanske den endast resulterar i en svag respons. Det har visats experimentellt att långsamt växande tumörer undgår immunförsvarets övervakning, medan ett större antal tumörceller som transplanteras, avstöts efter kortvarig tillväxt. T-cellerna anpassar sig kontinuerligt och dynamiskt i alla utvecklingssteg till omgivningens stimulering, där en plötslig ökning resulterar i ett svar.

Egentligen finns det som Tauber (2000) ser det, bara två huvudinriktningar inom immunologin, där självfokus å ena sidan innebär att immunförsvaret först fastställer organismens identitet och sedan skyddar dess integritet. Nätverksfokus å andra sidan innebär ett självorganiserande system, som utan att stå i tjänst till ett själv, definierar beteenden utifrån hur de stör systemet. Skillnaden mellan självfokus och nätverksfokus är att självfokus innebär ett försvar av organismen på basis av en själv-entitet, medan nätverksfokus innebär ett försvar på basis av ett brutet jämviktstillstånd. Nätverksteorin suddar ut konturerna för subjekt-objektdistinktionen och formulerar en fundamental nyorientering gentemot immunförsvarets organisation och

funktion. Det är när systemet rubbas och när det möter något främmande, som reaktionen kommer.

Immunförsvarets detektion av vad som skall uppfattas som inkräktande genom själv-ickesjälvdiskriminering

Alla mekanismer för själv-ickesjälvdiskriminering kan som Langman och Cohn (2000) uppfattar det klassificeras som *germline* eller *somatiska*. *Germline-mekanismer* är medfödda och är gemensamma för alla inom samma art som ärvt den. De fokuserar på att känna igen själv, vilket föranleder en undertryckning av de självdestruktiva mekanismer som annars skulle aktiveras.

De *somatiska mekanismerna* är i början av individens utveckling begränsade till att kunna urskilja mellan själv och ickesjälv, men utvecklas så småningom till att de själv-igenkännande elementen aktiverar icke självdestruktiva processer, samtidigt som de ickesjälv-igenkännande elementen aktiverar självdestruktiva processer.

Langman och Cohn (2000a) menar att somatisk själv-ickesjälvdiskriminering är somatiskt betingad, eftersom omfattningen av alla möjliga komponenter som behöver kännas igen är så stor, att en germlinebaserad eliminering av självförstörande element inte låter sig göras.

Langman och Cohn (2000a) konstaterar att det egentligen bara finns två sätt att separera själv från ickesjälv. Det ena är genom tid, där distinktionen kommer att handla om varaktighet (själv) kontra tillfällighet (ickesjälv). Det andra är genom rum, där distinktionen handlar om att avgränsa ett område som omfattar själv, där allt utanför blir ickesjälv. Problemet är att rumsseparationen kräver en mekanism, som sitter vid ingången till området och sorterar mellan själv och ickesjälv, vilket bara gör att problemet förskjuts.

Langman och Cohn (2000a) ser immunförsvarets uppfattning om själv som precis och otvetydig, där själv-ickesjälvdistinktionen görs på grundval av frånvaro av igenkänning. Eftersom det som är själv för en individ kommer att vara ickesjälv för en annan, så måste varje somatisk urvalsmekanism som reglerar själv-ickesjälvdiskrimineringen, använda sig av generella, ej kemiska eller fysikaliska egenskaper hos antigenerna. Chaplin (2003) baserar immunförsvarets mekanismer för detektion på strukturella drag som utmärker patogenerna mot värdcellerna. Även om det enligt Cohen (2000) är tydligt och lätt att greppa konceptet med själv-ickesjälvdiskriminering, så är det likväl vilseledande och därtill inte adekvat, eftersom immunförsvaret måste göra avvägningar efter de omständigheter som omger antigenerna, oavsett om de är själv eller ickesjälv.

För Alam och Gorska (2003) är det en grundläggande uppgift för immunförsvaret att försvara själv mot ickesjälv. Efroni och Cohen (2003) ser dock inte immunförsvaret som primärt skyddande, utan reglerande. Att skydda kroppen från främmande inkräktare är en syn som sträcker sig långt tillbaka, vilket logiskt har legitimerat diskrimineringen mellan själv och främmande. Immunförsvaret karakteriseras dock inte av vad det känner igen, utan av hur det reagerar. Själv-ickesjälvdiskriminering är som Silverstein och Rose (2000)

uttrycker det en villfarelse, eftersom världen inte är uppdelad i dessa kategorier. Immunförsvaret klarar inte av att göra denna distinktion, det är blott de immunologiska reglerna som avgör vad som skall tolereras. Detta är regler som upprätthålls av olika regulatormekanismer. Själv blir en samling antigener som inte är kapabla till att förorsaka en reaktion.

Hanahan (1998) hävdar att själv-ickesjälv-igenkänningsprincipen, där immunförsvaret kan svara på främmande antigen, medan det upprätthåller tolerans mot självantigen, har fastställts experimentellt. Även Chaplin (2003) anser att förmågan att skilja själv från ickesjälv står i centrum, när det gäller immunförsvarets förmåga att mobilisera ett svar mot patogener. Efroni och Cohen (2003) är emellertid av den åsikten att det framgångsrika själv-ickesjälv-konceptet har trängt undan alternativa ansatser som skulle ha kunnat hantera autoimmuna sjukdomar. Själv-ickesjälvdiskrimineringen har mjölkats till sista droppen och det är dags att sätta ihop alla delar till ett fungerande system.

Immunförsvarets detektion av vad som skall uppfattas som skada

Cohen (2000) säger att immunförsvaret skiljer mellan olika antigener, men inte på grundval av själv-ickesjälvdistinktionen. Det handlar inte om att klassificera ämnen som förstörbara eller ej. Istället handlar det om att bestämma vävnadernas tillstånd och svara med korrigerande imflammation.
Dembic (2000) finner att lymfocyter som specifikt känner igen antigen bidrar till att skydda vävnadsintegriteten genom att celler kommunicerar med varandra. Immunförsvaret agerar inte när det möter något farligt och det gör ingen diskriminering mellan själv och ickesjälv; istället reagerar det när vävnadernas integritet störs, vilket möjliggör återuppbyggnad. Immunförsvaret reagerar således på trasiga vävnader, så att de kan förnyas. Lymfocyterna blir därmed en historisk databas över vävnadsbrott och ett nätverk som förhindrar förfall. Integriteten för en vävnad blir ett mått på alla möjliga signalinteraktioner för en enskild cell i sitt normaltillstånd.

Försvar mot infektioner kan av vad Cohen (2000) uppfattar, betraktas som en viss typ av kroppsunderhåll, speciellt som en infektion inte alltid kräver att inkräktaren omedelbart förstörs. Hur man förhåller sig till inkräktare beror på var angreppet skett och på omständigheterna kring den skadade vävnaden, snarare än angriparens identitet. Autoimmunitet hjälper till att underhålla kroppen, där det handlar om att sätta in rätt behandling för ögonblicket. Att på bästa sätt göra sig av med åldrade, abnorma eller infekterade celler och organisera insatserna dynamiskt efter vävnadernas varierande behov. Autoimmunitet kan spontant aktiveras av skadade vävnader, vilket förmodligen regleras på något sätt, eftersom denna form av autoimmunitet normalt inte leder till autoimmun sjukdom.

Simon och Tatu (1988) anser att infekterade celler sänder ut extrasignaler som kan fungera som medstimulerande signaler, till skillnad från de normala cellerna som inte sänder ut några sådana extrasignaler, vilket leder till att de självreaktiva lymfocyterna dör.

Immunförsvarets detektion av vad som skall uppfattas som inkräktande i vävnadsbarriärer

Kruisbeek och Amsen (1996) säger att aktiverade T-celler har möjlighet att döda varandra genom stimulering av en viss receptor, vilket gör att de själva kan nedreglera sin reaktion efter den första försvarsinsatsen. Vissa vävnader, till exempel näthinnan och testiklarna, kan ge sådan stimulering och därigenom skyddas de mot att angripas av immunförsvaret. Detta stöds av Rose (1999) som menar att vissa ställen i kroppen uttrycker särskilda element som kan stimulera kritiska immunförsvarsceller till att dö.

Vad det gäller mekanismen som medför att immunförsvaret inte reagerar mot fostret, så menar Langman och Cohn (2000a) att det idag är en öppen fråga, om mekanismen är av samma typ som gör att modern inte reagerar mot sina egna själv-antigener, eller om fostret skapar en priviligerad gräns, där det inte spelar någon roll att det bär på antigener från fadern.

Immunförsvarets detektion av vad som skall uppfattas som inkräktande med hjälp av medstimulerande signaler

Simon och Tatu (1988) säger att en trend när det gäller att förklara perifer immunologisk tolerans, har varit konceptet med medstimulerande signaler, där frånvaron av en sådan kompletterande signal vid lymfocytens igenkänning av antigen, leder till att lymfocyten dör. Lymfocyten klarar sig dock om den befinner sig i ett visst mognadssteg. Ohashi och DeFranco (2002) menar att brist på medstimulerande signaler i kontakt med antigenpresenterare leder till att T-cellerna görs oförmögna att reagera.

Faktorer förutom negativ selektion som spelar roll för immunsvaret är enligt Miller och Basten (1996) antigenpresentation, affinitet och medstimulerande signaler. Rose (1999) tycker till och med att det förefaller som om total utrotning av självreaktiva celler, snarare är undantag än regel, där det är vanligt med självreaktiva T-celler perifert. Därför krävs andra regleringsmekanismer, som till exempel medstimulerande signaler för aktivering.

2.3 Metodologisk referensram

2.3.1 Vetenskaplig metod

Bowler (1992) uppfattar att den vetenskapliga metoden alltid har haft fysiken som ledstjärna, där det är enkelt att ställa upp hypotetiska naturlagar som låter sig testas i experimentella uppsättningar. Andra discipliner behöver kanske ta

med faktorer som fysiken inte ens behöver överväga. Dessa ’mjuka’ vetenskaper kräver en metodologi som lämnar större rum för debatt och som gör det möjligt att testa hypoteser på ett icke lika fullt rigoröst sätt, för att kunna avvisa icke tillfredsställande förklaringar.

Vetenskapliga teorier

Enligt Bowler (1992) anser vetenskapsmännen att nya teorier blir framgångsrika, eftersom de ger en bättre bild av hur naturen fungerar. Framförallt får den relativistiska synen på vetande, där ideologin styr perspektiven, svårt att förklara vetenskapens allt bättre kontroll över naturen. Graziano och Raulin (1989) säger att även om vetenskapen har många mål, till exempel hypotesgenerering och testning, eller mer pratiska tillämpningar, så är det huvudsakliga målet att utveckla teorier. Graziano och Raulin (1989) listar lite olika typer av teorier:

Induktiva teorier utgår ifrån en massiv uppsättning data från empiriska observationer, som abstraheras mot allt högre nivåer.
Deduktiva teorier är formulerade konstruktioner som ligger till grund för slutledningar som kan testas mot verkligheten, där gynnsamma utfall ger belägg för teorin.
Det finns också *funktionella teorier* som lägger lika stor vikt vid induktion och deduktion.
Modeller kan ses som analoga representationer av verkligheten, där de i motsats till formella teorier i regel inte medger goda förutsägelser mot verkligheten. Modeller kan ses som miniteorier eller som delsteg i utvecklingen av fullskaliga teorier.

Hypotetisk-deduktiv metod

Bowler (1992) säger att vetenskapsmännen ställer upp hypoteser om vad man förväntar att upptäcka; man gör en förutsägelse om vad som skall ske i en specifik situation och använder sedan observation eller experiment för att testa huruvida förutsägelsen matchar. Tidigare i historien var det regel att vetenskapsmännen förhöll sig som rena observatörer, där de genom induktion samlade fakta fria från subjektivitet, utan att ha några föreställningar över huvud taget. Den moderna vetenskapsfilosofin inser dock att naturen är alltför komplex för att detta skall vara möjligt och således behövs någon form av vägledning som talar om vilka fakta som är relevanta.

Graziano och Raulin (1989) påpekar dock att induktivt-deduktivt tänkande ej blott är vetenskapsmän förunnat, utan används även till vardags i olika situationer. Man råkar göra en viss observation ur vilken man drar vissa slutsatser. Dessa slutsatser kanske man sedan bekräftar mot hur det faktiskt förhåller sig. Skillnaden är att vetenskapen kräver mycket högre precision än det vardagliga livet.

Hypotesgenerering

Vetenskapsmännen kan enligt Hempel (1969) låta sin fantasi få fritt spelrum, där det kreativa tänkandet också kan komma ur uppfattningar som är vetenskapligt tvivelaktiga. För att komma från fakta till teori krävs fantasi av det skapande slaget. Hypoteserna och teorierna härleds från de fakta man samlar in; de uppfinns för att ge en förklaring. Hypotesmetoden innebär att man uppfinner preliminära hypoteser som sedan underkastas empirisk testning. Stor uppfinningsrikedom kräver stor förtrogenhet med aktuell kunskap på området, eftersom nya idéer på nybörjarnivå förmodligen endast kopierar tidigare försök eller krockar med etablerade teorier. Gissningar som är lyckosamma kräver stort skarpsinne om de skall göra radikala avsteg från rådande vetenskapliga tänkesätt.

Även Bowler (1992) anser att den hypotetisk-deduktiva metoden tillåter att icke rationella faktorer är en del av hypotesgenereringen, även om hypotesen bara skall accepteras så länge den klarar empiriska test. Även om detta i mångt och mycket innebär att vetenskapen inte kan vara fri från värderingar, så fortsätter vetenskapsmännen att framhärda dess objektivitet. Hempel (1969) menar dock att den vetenskapliga objektiviteten legitimeras av principen att hypotetserna accepteras om de klarar kritisk granskning.

Hypotestestning

Graziano och Raulin (1989) säger att hypotestestning är ett kritiskt moment i experimentell forskning. Man utgår ifrån en begynnande vag idé, som utifrån inledande observationer och tidigare forskning preciseras, för att sedan omsättas i metodologiska procedurer. Bowler (1992) hävdar att den hypotetisk-deduktiva metoden för vetenskapen framåt genom att testa de konsekvenser som kan erhållas från den konstruerade modellen av fenomenet. Objektiviteten ligger i att man utsätter varje aspekt av hypotesen för rigorös testning. Om de förutsägelser som hypotesen lägger fram inte bekräftas, så avvisas hypotesen och en ny modell söks.

Även om hypotesen, som Hempel (1969) ser det, klarar omfattande tester, så blir den ändå inte bindande, eftersom resultaten blott ger ett starkt stöd åt hypotesen. Därför kan man säga att den vetenskapliga forskningen i vid bemärkelse är induktiv, eftersom den inte erbjuder deduktivt bindande bevis. Bowler (1992) lyfter fram Karl Popper som ser falsifierbarheten som det som huvudsakligen karakteriserar vetenskapen, i det att hypoteserna kan förkastas i ett rättframt, observerbart test. Pseudovetenskaper genererar vaga teorier som alltid kan klara sådana test. Popper tycker att vetenskapen alltid skall söka efter svagheten i idéerna, så att de kan ersättas med någonting bättre.

Graziano och Raulin (1989) menar att hypotesen ofta avser ett orsakssamband mellan oberoende och beroende variabler. Ändrar man den ena variabeln och noterar en förutsägbar effekt på den andra, så föreligger ett orsakssamband. För att kunna konstatera att ett orsakssamband föreligger, så krävs det att man har full kontroll över den oberoende variabeln och att den beroende variabeln mäts

på ett adekvat sätt. Har man inte höga krav på orsakssamband kan man dock nöja sig med korrelationer, vilket medför att behovet av distinktion mellan oberoende och beroende variabler minskar.

Hempel (1969) anser att det inte finns några mekaniska regler för upptäckter. Inte heller slutledningsproceduren från premiss till slutsats följer sådana regler, utan bygger på gissningar. Det mekaniska ligger i att kontrollera om slutledningen är giltig i form av en kedja av systematiska slutledningssteg.

2.3.2 Datainsamling

Sekundära data

Bryman (2004) lyfter fram möjligheter och begränsningar med sekundära data:

Möjligheter

- *Tid och pengar*: Möjligheten att få tillgång till högkvalitativa data till bråkdelen av kostnaden för att själv samla in informationen.
- *Hög kvalitet*: Mycket av tillgängliga sekundära data är av hög kvalitet och har dessutom framställts av erfarna forskare med väletablerade procedurer.
- *Möjlighet till analys över tid*: Man utnyttjar sekundära data för att samla information över tid, något som vanligtvis kräver stora resurser.
- *Subgrupper*: Man utnyttjar data som samlats in lokalt för global analys.
- *Möjlighet till tvärkulturell analys*: Man utnyttjar data som samlats in separat i olika länder, eftersom det är förenat med stora kostnader att själv genomföra studien på plats.
- *Mer tid till dataanalys*: Eftersom datainsamling vanligtvis stjäl mycket tid och fokus från dataanlysen, undviker man den fällan. Det är också lättare att planera dataanalysen eftersom man kan skaffa sig en uppfattning om datainnehållet på förhand.
- *Möjlighet till ny tolkning*: Genom att anlägga olika perspektiv kan sekundära data analyseras på olika sätt, skilt från det ursprungliga syftet.
- *Dataexploatering*: Primära data utnyttjas vanligtvis inte fullt ut i den ursprungliga studien och därför kan användandet av sekundära data stimulera forskare till återanvändning.

Begränsningar

- *Dålig kännedom om data*: Samlar man in sina egna data blir man mer familjär med innehållet, än om man utnyttjar någon annans data.
- *Komplexitet*: Stora informationsmängder kan vara svåra att hantera, samtidigt som de kan vara angripbara från flera nivåer. Det kräver i regel en period av acklimatisering.
- *Ingen kontroll av kvalitet*: Även om det finns pålitliga källor för sekundära data, så bör man alltid vara kritisk till tillförlitligheten och hur dessa data passar det egna syftet.

- *Avsaknad av nyckelvariabler*: Eftersom sekundära data i regel är insamlade för ett annat syfte, så är det alltid möjligt att vissa centrala attribut saknas som är kritiska för den egna analysen.

Sampling

Flick (1998) relaterar sampling till hur man väljer vilka av de tillgängliga exemplaren som skall undersökas. Några olika strategier för detta listas i tabell 2.

Tabell 2 *Flicks olika samplingsstrategier(Flick, 1998)*

Strategi	Beskrivning
Hela materialet	Alla tillgängliga fall beaktas, till exempel för att följa en patients hela sjukdomshistoria.
Statistisk	Statistiskt urval för att kartlägga fördelning av egenskaper, bestäms på förhand.
Progressiv	Nya fall samlas in efterhand beroende på vad som kommer fram för att generera en hypotes.
Extrem (progressiv)	Extremfall av populationen väljs ut, till exempel för att undersöka vad som gör att en företeelse lyckas/misslyckas.
Typisk (progressiv)	Typiska fall för populationen väljs ut, till exempel för att undersöka vad som gör att en företeelse lyckas/misslyckas.
Maximal variation (progressiv)	Ett fåtal fall som skiljer sig mycket väljs ut för att undersöka hur populationen varierar.
Intensitet (progressiv)	Fall med utmärkande egenskaper väljs ut, för att undersöka hur populationen varierar.
Kritisk (progressiv)	Fall som relaterar till egenskaper som är kritiska för funktionaliteten väljs ut.
Känslig (progressiv)	Fall som relaterar till egenskaper som äventyrar funktionaliteten väljs ut.
Smidighet (progressiv)	Fall som är enkla att undersöka väljs ut när det finns begränsade resurser.

Slumpmässig sampling innebär för Graziano och Raulin (1989) att varje individ i populationen har lika stor chans att bli vald. I praktiken är detta många gånger ett ouppnåeligt mål, eftersom det kan vara svårt att få tag på alla kategorier av individer. Man får i regel utgå från vad som är mest tillgängligt, förutsatt att det inte finns anledning att anta att det urval man har för handen skiljer sig från det som är mindre tillgängligt. Bernard (2000) anger två typer av slumpmässig sampling:

Enkel slumpmässig sampling innebär att ett mindre antal på slumpmässig basis hämtas från en stor population. Hela populationen numreras och via någon slumpgenereringsmekanism produceras de nummer som skall plockas ut från populationen.

Systematisk slumpmässig sampling används ofta istället för enkel slumpmässig sampling, eftersom det kan vara svårt att hantera stora populationer, där det

inte finns rimliga möjligheter att numrera hela populationen. Detta innebär att man använder ett samplingsintervall, där man plockar ut var N:te individ från populationen. Intervallets storlek är lika med det totala antalet delat med det erfoderliga antalet. Startpunkten för samplingen är en slumpmässig position i populationen, vilket samtidigt medför att ett brutet intervall vid slutet fortsätter från början och framåt tills erfoderligt antal individer har erhållits.

En risk med systematisk slumpmässig sampling är enligt Bernard (2000) *periodicitetproblemet*, som innebär att man kan få över- eller underrepresentation av kategorier om de råkar vara grupperade på ett visst sätt. Ett sätt att komma tillrätta med detta är att göra två samplingar med olika intervall och sedan jämföra dem för att se om de skiljer sig åt, vilket skulle kunna vara en indikator på periodicitet. Graziano och Raulin (1989) ser en stor angelägenhet i att göra en sampling som är representativ för en generalisering av populationen. Det är också av vikt att klargöra om variabler förhåller sig konsistenta genom hela populationen eller om de ändrar betydelse mellan olika segment.

Graziano och Raulin (1989) påpekar att det finns en stor risk för bias om man utför sin sampling från en avgränsad grupp, eftersom denna kanske är specialiserad på ett sätt som inte gör den generellt gångbar. Sådana risker finns i varje problemområde och även om urvalet förefaller vara slumpmässigt, så är det likväl möjligt att det finns dolda faktorer som styr vilka individer som ingår i populationen som helhet. Även tidpunkter kan spela in, där olika mönster kan förekomma under olika perioder.

2.3.3 Analys

Grundad teori

Bernard (2000) beskriver grundad teori som ett sätt att fånga upp kategorier och begrepp som implicit förekommer i en text, där man sedan utifrån dessa konstruerar formella teorier. Enligt Pandit (1996) har grundad teori tre grundläggande element:

- *Begrepp*: Detta är en grundläggande analysenhet, eftersom det är genom konceptualiseringen av data och inte genom den råa datan i sig, som teorin byggs. Begreppen formas ackumulativt genom kontinuerlig avstämning mot obearbetade data.
- *Kategorier*: På en nivå högre genereras kategorier ur de framtagna begreppen, genom en motsvarande analytisk process. Kategorierna bildar hörnstenarna i den teori som utvecklas.
- *Antaganden*: Detta är generaliserade relationer mellan avgränsade kategorier och hur begreppen förhåller sig till respektive kategori.

Bryman (2004) lyfter fram den teoretiska samplingen, där data samlas in, kodas och analyseras. Syftet är att få fram kategorier med tillhörande egenskaper, där relationen mellan dessa modelleras och bildar underlag till att

avgöra vilket behov av nya data som finns. Processen formar successivt en modell som i sin tur styr processen mot mättnad. Bernard (2000) anger följande steg för processen:

1. Läs ett textstycke.
2. Plocka ut möjliga kategorier och teman.
3. Gruppera data successivt och se hur de hänger ihop.
4. Fundera på hur kategorierna hänger ihop.
5. Generera modeller utifrån informationen om hur kategorierna relaterar till varandra genom att iterativt stämma av modellerna mot data.
6. Illustrera modellerna genom exempel i form av citat från texten.

Pandit (1996) hänför konceptualisering och kategorisering till en process som benäms *öppen kodning*. Den råa datan bryts ned med enkla frågor som *vad*, *var*, *när* och *hur*, där liknande företeelser etiketteras under olika begrepp som sedan grupperas till kategorier. Genereringen av antaganden, kategorier och begrepp är en iterativ process som induktivt härleds från det fenomen som representeras. Bernard (2000) ser grundad teori som en väg att från texter upptäcka hypoteser, som sedan testas med innehållsanalys. Denna kombination blir en naturlig metodik för induktion – deduktion och det finns också forskning som använt sig av denna ansats.

Innehållsanalys

Stemler (2001) säger att innehållsanalys kan definieras som en replikerbar och systematisk teknik för att konvertera en stor textmassa till färre kategorier genom explicita kodningsregler. Bryman (2004) uttrycker det som ett sätt att kvantifiera textinnehållet utifrån förutbestämda kategorier. Stemler (2001) menar att tekniken till exempel kan användas till att undersöka trender och mönster i dokument. Replikerbarheten kommer av att tekniken tillämpas på varaktiga (dokumenterade) data. Det som gör innehållsanalysen speciellt meningsfull är att den möjliggör kategorisering av data, där kategorier är grupper av ord med liknande mening. Kategorierna skall vara ömsesidigt uteslutande, vilket innebär att varje begrepp endast kan hänföras till en kategori.

Roberts (2001) förklarar att den klassiska innehållsanalysen kopplar symboliska data till en tabell, vilket möjliggör statistisk analys. Det handlar om att generera symboliska data från företrädesvis texter, som underlag till statistisk analys. Slumpvist utvalda block från texten representerar rader i en tabell, där varje kolumn representerar ett begrepp eller tema (kategori). I varje cell anges antalet förekomster i radens block som kan associeras med kolumnens kategori.

Kodblock kan enligt Stemler (2001) till exempel avgränsas som olika dokument, stycken, meningar eller enstaka ord. Det är också möjligt att bryta ned texten i olika innebörder. Även om det finns en uppfattning om att innehållsanalys innebär att man undersöker frekvensen av specifika ord, så bör man även ta hänsyn till synonymer och att olika ord har olika dignitet, samt att vissa ord kan ha dubbla innebörder. Ett reliabilitetskrav är att olika personer

utför kodningen på samma sätt. Finns det tvetydigheter i begreppsliga innebörder och oklara kategoridefinitioner och kodningsregler, så skapar det problem.

Bryman (2004) menar att kodningen är ett kritiskt moment, som kräver att man tar fram ett kodningsschema och en kodningsmanual. Schemat är formatet för hur data struktureras (tabell eller dylikt), medan manualen anger principerna för hur data läggs in i strukturen. Bernard (2000) anger följande steg för processen:

1. Skapa en uppsättning koder.
2. Tillämpa kodningen på texterna.
3. Testa tillförlitligheten i kodningen.
4. Stycka upp texten i mindre analysenheter och sätt dessa i en matris med koderna.
5. Analysera matrisen statistiskt.

2.3.4 Metodintegritet

Validitet

Silverman (2001) säger att validitet är hur väl en redogörelse representerar de fenomen den refererar till. Graziano och Raulin (1989) relaterar den mest grundläggande innebörden av validitet till metodologisk sundhet och lämplighet, att en giltig mätning mäter det den skall mäta och testar det den skall testa. Enligt Bernard (2000) är validiteten det viktigaste med forskningen, där de instrument man använder och de data man samlar in måste vara giltiga. De slutsatser som dras måste vara riktiga och inte grunda sig på ogrundade antaganden.

Graziano och Raulin (1989) menar att om den oberoende variabeln skall anses ha effekt på den beroende variabeln, så gäller det att utföra ett experiment på ett sätt, så att orsakssambandet beläggs utifrån slusatser där man kan känna sig väl förtrogen med experimentets giltighet. Validitetsfel kan enligt Silverman (2001) vara att man accepterar en korrelation som orsakssamband, när det kanske finns en okänd faktor med i bilden. Det spelar ingen roll om man hanterar kvantitativa eller kvalitativa data, ty validitetskonceptet måste ändå beaktas. Graziano och Raulin (1989) hävdar att forskaren bör skapa procedurer för att i möjligaste mån reducera potentiella hot mot validiteten, även om absolut validitet aldrig kan uppnås. De anger några typer av validitet:

Statistisk validitet innebär att resultaten beror på någon systematisk faktor och inte blott på slumpmässig variation. Det kan till exempel handla om att mätningarna är otillförlitliga.
Konstruktionsvaliditet anger hur väl den testade teoretiska konstruktionen förklarar de resultat man erhåller från studien. Det gäller att teorin är klar och väl underbyggd, samtidigt som alternativa teorier inte kan komma ifråga.

Extern validitet avser den generella gångbarheten hos resultatet, under andra förutsättningar än just de som var specifika för experimentet, till exempel annat urval eller andra tider och platser.
Intern validitet handlar om huruvida förändringar i den beroende variabeln verkligen kommer av förändringar i den oberoende variabeln och inte från någon okänd variabel.

Silverman (2001) listar några kriterier som påverkar validiteten:

- Forskarens påverkan
- Forskarens värderingar
- Sanningshalten i respondentens utsagor
- Metodtriangulering
- Respondentvalidering (återkoppling)

Reliabilitet

Enligt Graziano och Raulin (1989) hänger reliabilitet samman med reproducerbarhet. Om någon annan skall kunna genomföra motsvarande mätning, så är det viktigt att mätningarna görs på samma sätt. Om inte mätningarna är tillförlitliga blir inte informationen användbar. Silverman (2001) relaterar reliabilitet till hur instanser kategoriseras på samma sätt av olika observatörer, eller av samma observatör över tid. Denna grad av konsistens beror också på hur uttömmande det material är som en läsare av fältanteckningar senare möter. Graziano och Raulin (1989) menar att reliabiliteten är avhängig precisionen i hur problemställningen operationaliserats. Reliabiliteten beror också på hur noggrannt denna operalitionalisering har realiserats, inte minst mätningarna, samt hur många oberoende observationer som resultatet baserar sig på.

Graziano och Raulin (1989) ger exempel på olika typer av reliabilitet:
Tolkningsreliabilitet handlar om huruvida två oberoende uttolkare gör samma tolkning.
Omtest-reliabilitet gäller hur upprepade tester över tid ger samma resultat.
Intern konsistens-reliabilitet anger hur representativ mätningen är för en enstaka individ i populationen, där flera olika mätningar av individen är mer tillförlitlig, eftersom en enskild mätning kanske är ett extremfall.

Silverman (2001) gör en något annorlunda indelning:
Idealistisk reliabilitet handlar om vilken nivå som tillförlitligheten skall läggas på för att den skall fylla någon rimlig funktion.
Diakronisk reliabilitet är hur stabil observationen är över tid.
Synkronisk reliabilitet är hur likartade observationerna är under samma tidsperiod, vilket till exempel uppnås genom metodtriangulering.

Silverman (2001) anser att data som hämtas från texter i princip blir mer tillförlitliga än observationer (om man bortser från förfalskningar), eftersom texter innebär att data redan finns för handen. Här kommer realibilitetsbegreppet att handla om de kategorier man ställer upp för att

analysera texten, vilket måste ske på ett standardiserat sätt, så att olika forskare kategoriserar lika. Tolkningsreliabilitet är en standardmetod för att åstadkomma detta, där samma data kategoriseras av olika analytiker för att eliminera skillnader. Det finns dock förespråkare för att reliabilitet endast är en fråga för kvantitativ forskning. Behandlar man den sociala verkligheten lite på måfå, som brukligt är, så fyller det ju inte någon funktion att undra huruvida mätinstrumenten är tillförlitliga.

Triangulering

Syftet med triangulering

Fielding och Fielding (1986) förklarar att begreppet triangulering kommer av att en betraktare får svårt att lokalisera sig utifrån ett enskilt landmärke, medan två landmärken medger att man kan lokalisera sig utifrån skärningspunkten av linjerna från båda landmärkena. Triangulering skall användas för att ge ett vidare perspektiv, större räckvidd och djup, men inte för att uppnå någon objektiv sanning.

Fielding och Fielding (1986) säger att triangulering medger att forskaren intar ett kritiskt perspektiv och försöker identifiera svagheter i sitt material och hur man skulle kunna göra testerna annorlunda. En motivering till att triangulera olika tekniker är att de var för sig utgör olika hot mot validiteten. Det handlar om att man relaterar olika data på ett sådant sätt att de motverkar de möjliga hoten mot validiteten. Det räcker alltså inte bara med att slentrianmässigt kombinera olika metoder eller data.

Typer av triangluering

Fielding och Fielding (1986) menar att triangulering vanligtvis innebär att man kombinerar metoder, men att det också är möjligt att triangulera data. *Datatriangulering* kan bestå i *tidstriangulering*, som belyser tillfälliga influenser eller *rumstriangulering*, som utrycker sig i jämförande forskning. *Triangulering av datakällor* innebär att man jämför data som relaterar till samma fenomen, men som hämtats från olika faser.

Fielding och Fielding (1986) säger att triangulering även kan ske mellan forskare och mellan olika tekniker. *Undersökartriangulering* innebär att fler än en person undersöker samma situation. *Teoritriangulering* tittar på samma situation utifrån olika teorier. *Metodologisk triangulering* kan delas in i *intra-metodtriangulering*, där samma metod används vid olika tillfällen utifrån ett reliabilitetsperspektiv, medan *inter-metodtriangulering* använder olika metoder på samma undersökningsobjekt.

Triangulering och bias

Fielding och Fielding (1986) anser att om man använder sig av flermetodansatser, utan att samtidigt ta hänsyn till respektive metods bias-

kontrollerande mekanismer, så är risken stor att man förenar metoder som producerar data som egentligen inte är kompatibla. Två huvudkällor till bias kan vara att man väljer data som passar ens föreställningar om fenomenet, samt att man hellre väljer data som sticker ut, eftersom sådan data är mer intressant än odramatisk data, som likväl skulle kunna ge indikationer på fenomenet man undersöker. Teoritriangulering reducerar dock inte nödvändigtvis bias. Kombinerade teorier kan ge ett vidare perspektiv, men för den skull inte ett mer objektivt sådant. Olika metoder härstammar från olika teoretiska traditioner, där kombinationen kan ge räckvidd och djup, men inte noggrannhet i sig.

3 Hypoteser

Nedan har en huvudhypotes ställts upp som brutits ned i ett antal delhypoteser. Av dessa delhypoteser följer först sådana som relaterar till människans immunförsvar, för att klargöra hur förebilden för det artificiella immunsystemet ser ut. Dessa följs av delhypoteser som relaterar till datorsystem med Microsoft Windows som operativsystem. Delhypoteserna kopplas ihop i en slutledningskedja, som med stöd av ett antal postulat leder fram till huvudhypotesen, att sådana datorsystem inte kan ha artificiella immunsystem baserade på människans immunförsvar, om de skall tillgodose användarnas behov av säkrare datorsystem.

Anledningen till att hypoteserna gäller Microsoft Windows, är att det är ett i synnerligen hög grad utbrett operativsystem, där antivirusföretagens beskrivningar av datorvirus, maskar och trojaner till största delen relaterar till detta operativsystem.

3.1 Stipulationer av begrepp som relaterar till hypoteserna

Funktionell avser den abstraktion som isolerar själva funktionen från mekanismerna bakom den. Till exempel kan man i funktionell bemärkelse betrakta en individ som självständig (han kan försörja sig själv), även om individen indirekt är beroende av omvärlden för att kunna existera (samhället förser honom med infrastruktur, sjukvård, arbete och så vidare).

Applikation avser någon form av kod som anger en uppsättning operationer som kan exekveras i ett datorsystem, oavsett hur dessa exekveras (till exempel program, script eller macro). Enligt Skormin, Summerville och Moronski (2003) använder sig informationsattacker ofta av exekverbara filer eller någon form av script.

Datorsystem är det system som konstitueras av en enskild dator, vilket utgörs av hårdvara, operativsystem och installerade applikationer. Denna avgränsning är relevant eftersom immunförsvar verkar i individer, där det är svårt att se något annat än en enskild dator som en individ. Betraktar man nätverk som individer, så får man svårt att hantera problemet med inkräktare som genereras inom nätverket. Betraktar man applikationer som individer, så måste varje

applikation ha sitt eget immunsystem och därmed finns det ingen som tar ansvar för datorsystemet som helhet.

Installerade applikationer betyder att applikationerna är direkt tillgängliga för exekvering i datorsystemet.

Exekvering innebär att applikationerna startas och börjar utföra de operationer som de innehåller.

Immunförsvar syftar på människans immunförsvar, medan *immunsystem*, syftar på den artificiella motsvarigheten. Anledningen till att benämningen *artificiellt immunförsvar* inte används, är att det är lättare att hålla isär begreppen om man använder benämningarna *människans immunförsvar* och *artificiellt immunsystem*.

Artificiellt immunsystem betyder här att immunförsvaret på ett funktionellt sett använder de principer som dess förebild använder. Det innebär inte att varje mekanism måste överensstämma, *men att analoga principer används för att hantera fundamental problematik*. Enligt Hofmeyr (2004) blir ju analogin oanvändbar om överensstämmelsen är dålig. Om man skall bygga ett artificiellt immunsystem, men frångår fundamentala principer för att man inte riktigt tycker att de passar in eller för att man hittat bättre lösningar, ja då lär det inte vara ett artificiellt immunsystem som man bygger, utan snarare ett datorsystem som använder immunförsvaret som inspiration. Det finns ett antal sådana forskningsområden, där detta visat sig vara relevant, men där det inte handlar om att bygga säkerhetssystem, utan snarare att använda immunförsvaret som modell för att lösa olika typer av avgränsade problem.

Övriga begrepp som förekommer i hypoteserna stipuleras i undertexterna allt eftersom de förekommer. Det betyder att det som stipulerats för en tidigare hypotes också gäller för en senare hypotes. Observera dock att begreppet *inkräktande* har en innebörd i delhypoteserna som relaterar till människans immunförsvar och en annan innebörd i delhypoteserna som relaterar till datorsystem. Detta är ingen inkonsistens, det är ett perspektiv som ligger helt i linje med utgångspunkten för denna uppsats, nämligen att inkräktande i människor skiljer sig från inkräktande i datorsystem.

3.2 Huvudhypotes

H1. Ett självständigt artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, kan inte ha människans immunförsvar som förebild.

Självständigt skall här ses i funktionell bemärkelse, att det inte är beroende av någonting utanför datorsystemet för att veta hur det skall agera. *Användare* är externa subjekt som kontrollerar systemet. *Behov* är uttalade

eller outtalade säkerhetskrav som användarna har på systemet för att det skall kunna upprätthålla förväntad funktionalitet. *Säkrare* relalaterar till dagens antiviruslösningar som bygger på kända virusdefinitioner och således kräver extern inblandning för att upptäcka nya virus, vilket även påtalas av Marmelstein, Van Veldhuizen och Lamont (1998).

3.3 Delhypoteser som relaterar till människans immunförsvar

H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.

Den är förutbestämd i det avseendet att immunförsvaret redan från början besitter de förutsättningar som krävs för att definiera vad som inte skall betraktas som inkräktande. Inkräktande avser företeelse som utlöser immunreaktion.

H3. Människans immunförsvar definierar själv vad som inte är inkräktande.

Detta innebär att immunförsvaret på egen hand samlar in data och sätter upp regler för vad som inte skall betraktas som inkräktande. Skillnaden mellan denna hypotes och den föregående är att H2 anger att immunförsvaret har förmågan, medan H3 anger att immunförsvaret också använder denna förmåga. Genom H2 förhindrar man att någon ger immunförsvaret förmågan i efterhand och genom H3 försäkrar man sig om att förmågan faktiskt används.

H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.

Detta innebär att immunförsvaret först definierar vad som inte är inkräktare och sedan använder denna definition för att avgöra när något är inkräktande.

3.4 Delhypoteser som relaterar till datorsystem

Anledningen till att hypotesnumreringen är bruten, är att vissa hypoteser tagits bort. Detta beror dels på att vissa av de ursprungliga hypoteserna visat sig vara överflödiga, dels på att vissa hypoteser slagits samman.

H7. Datorvirus, maskar och trojaner är applikationer.

Datorvirus, maskar och trojaner avser sådana element som antivirusföretagen hänför till dessa beteckningar.

H9. Datorvirus, maskar och trojaner är inkräktande applikationer i datorsystem med Microsoft Windows som operativsystem.

Inkräktande avser att applikationen utför sådana operationer, vars funktion användaren av datorsystemet inte haft för avsikt att införa i systemet. Denna definition relaterar till huvudhypotesen, som talar om användarnas behov. Att hypotesen relaterar till Microsoft Windows, utesluter operativsystem där datorvirus, maskar och trojaner inte är inkräktande. Det utesluter inte att datorvirus, maskar och trojaner kan vara inkräktande i andra datorsystem, men det är inget som undersöks här. Hypotesen skall alltså läsas som att datorvirus, maskar och trojaner kommer att betraktas som inkräktande, om de installeras i ett datorsytem med Microsoft Windows.

H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.

Att applikationerna inte härstammar från datorsystemet innebär att de inte funnits i detta enskilda datorsystem från början, utan installerats efter att systemet har tagits i bruk.

H11. I ett datorsystem med Microsoft Windows som operativsystem kan både inkräktande och icke inkräktande applikationer exekveras som inte härstammar från detta datorsystem.

Oavsett om en applikation är inkräktande eller ej, så kan den installeras och exekveras efter att systemet tagits i bruk.

H12. Datorsystem med Microsoft Windows som operativsystem är dynamiska strukturer.

Struktur avser här den funktionella ram som systemet har att verka inom. Med dynamisk avses att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt, eftersom systemet tillåter installation och exekvering av nya applikationer.

H13. Microsoft Windows är ett evolutionärt operativsystem.

Evolutionärt skall här ses i motsats till deterministiskt, att det utvecklas kontinuerligt på ett oförutsägbart sätt. I detta sammanhang gäller det uppdateringar, där säkerhetshål täpps till.

3.5 Postulat

P1. Delhypoteserna som relaterar till människans immunförsvar relaterar också till ett artificiellt immunsystem.

Detta innebär att det som hypoteserna säger om människans immunförsvar, också skall gälla för ett artificiellt immunsystem. Det specifika med människans immunförsvar är att det utan hjälp utifrån kan reagera på inkräktande. Detta är anledningen till att man vill ha ett artificiellt immunsystem i sitt datorsystem, till skillnad från traditionella antivirusprogram som måste uppdateras externt med nya virusdefinitioner. Hypoteserna berör fundamentala principer med stor principiell betydelse. Om ett artificiellt immunsystem inte stödjer dessa hypoteser förlorar begreppet *artificiell* sin innebörd och hela poängen med att försöka efterlikna människans immunförsvar går om intet. Ett mer deduktivt resonemang om postulatets giltighet förs emellertid i *7.1.2 Granskning av premisser*.

P2. Datorsystem med Microsoft Windows som operativsystem tillåter att icke inkräktande applikationer installeras och exekveras.

I undertexten till hypotesen

> *H12. Datorsystem med Microsoft Windows som operativsystem är dynamiska strukturer.*

anges att systemet tillåter installation och exekvering av nya applikationer. Att installera och exekvera icke inkräktande applikationer är en sådan elementär egenskap hos Microsoft Windows och datorsystem generellt, att detta utan vidare kan postuleras. Naturligtvis kan en administratör begränsa sådana rättigheter, men då är det administratören och inte operativsystemet som begränsar. Detta motsäger emellertid inte postulatet, eftersom applikationer som installeras mot administratörens vilja, rimligtvis måste betraktas som inkräktande.

P3. Om det finns belägg för hypotesen H10, så finns det också belägg för hypotesen H11.

Detta är rimligt att postulera eftersom hypotesen

> *H11. I ett datorsystem med Microsoft Windows som operativsystem kan både inkräktande och icke inkräktande applikationer exekveras som inte härstammar från detta datorsystem.*

är en konsekvens av hypotesen

> *H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.*

och postulatet

> *P2. Datorsystem med Microsoft Windows som operativsystem tillåter att icke inkräktande applikationer installeras och exekveras.*

H10 innebär att inkräktande applikationer kan exekveras som inte härstammar från systemet. Eftersom P2 säger att icke inkräktande

applikationer kan installeras, så kommer dessa inte heller att härstamma från systemet, eftersom det alltid är möjligt att tillverka nya, icke inkräktande applikationer och installera dem i systemet. Således kan, som H11 säger, både inkräktande och icke inkräktande applikationer exekveras, som inte härstammar från systemet.

P4. Ett artificiellt immunsystem som tillgodoser användarnas behov, kan inte själv definiera vad som inte är inkräktande.

Om immunsystemet själv skulle kunna definiera vad som inte är inkräktande, så skulle denna definition kunna strida mot användarnas behov och således måste definitionen göras av någon som känner till användarnas behov. Det är endast om immunsystemet tillgodoser sina egna behov, som det själv kan definiera vad som inte är inkräktande.

P5. För att ett system själv skall kunna definiera vad som inte är inkräktande, så måste det antingen ha tillgång till allt som inte är inkräktande eller allt som är inkräktande.

Finns inte allt tillgängligt så är det alltid möjligt att det senare dyker upp något som inte ryms inom definitionen. All fullständig definition som görs utan att systemet har tillgång till allt som är inkräktande eller allt som inte är inkräktande, bygger på kriterier som hämtats utanför systemet, till exempel information om vad som skall betraktas som inkräktande, vilket innebär att det inte är systemet som definierar.

3.6 Slutledning

Slutledningen bygger på att hypoteserna som relaterar till datorsystem är oförenliga med hypoteserna som relaterar till människans immunförsvar. Denna inkonsistens är uppsatsens kärna och kommer här att göras explicit. Hypoteserna H12 och H13 finns inte med i slutledningskedjan, men förekommer i *7.1.3 Granskning av slutledning* som innehåller kompletterande aspekter. Slutledningskedjan finns illustrerad i figur 2.

Hypotesen

H7. Datorvirus, maskar och trojaner är applikationer.

ger att datorvirus, maskar och trojaner är applikationer. Eftersom *inkräktande* avser att applikationen utför sådana operationer, vars funktion användaren av datorsystemet inte haft för avsikt att införa i systemet, så medför hypotesen

H9. Datorvirus, maskar och trojaner är inkräktande applikationer i datorsystem med Microsoft Windows som operativsystem.

att datorvirus, maskar och trojaner utför sådana operationer, vars funktion användaren av datorsystemet inte haft för avsikt att införa i systemet. Anledningen till att vi kopplar datorvirus, maskar och trojaner till inkräktande applikationer är att de används för att stödja hypotesen

H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.

som i sin tur ger belägg för hypotesen

H11. I ett datorsystem med Microsoft Windows som operativsystem kan både inkräktande och icke inkräktande applikationer exekveras som inte härstammar från detta datorsystem.

på grund av postulatet

P3. Om det finns belägg för hypotesen H10, så finns det också belägg för hypotesen H11.

Eftersom *inte härstammar* innebär att applikationerna installerats efter att systemet tagits i bruk av användaren, så innebär det att ett artificiellt immunsystem varken kan använda inkräktande eller icke inkräktande applikationer för att initialt definiera vad som inte skall betraktas som inkräktande.

På grund av postulatet

P5. För att ett system själv skall kunna definiera vad som inte är inkräktande, så måste det antingen ha tillgång till allt som inte är inkräktande eller allt som är inkräktande.

så är det således inte möjligt att göra en initial definition av vad som inte är inkräktande, vilket strider mot hypotesen

H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.

på grund av postulatet

P1. Delhypoteserna som relaterar till människans immunförsvar relaterar också till ett artificiellt immunsystem.

Om ett artificiellt immunsystem skall tillgodose användarnas behov av säkrare datorsystem, så kan detta immunsystem inte själv definiera vad som inte är inkräktande enligt postulatet

P4. Ett artificiellt immunsystem som tillgodoser användarnas behov, kan inte själv definiera vad som inte är inkräktande.

vilket strider mot hypotesen

H3. Människans immunförsvar definierar själv vad som inte är inkräktande.

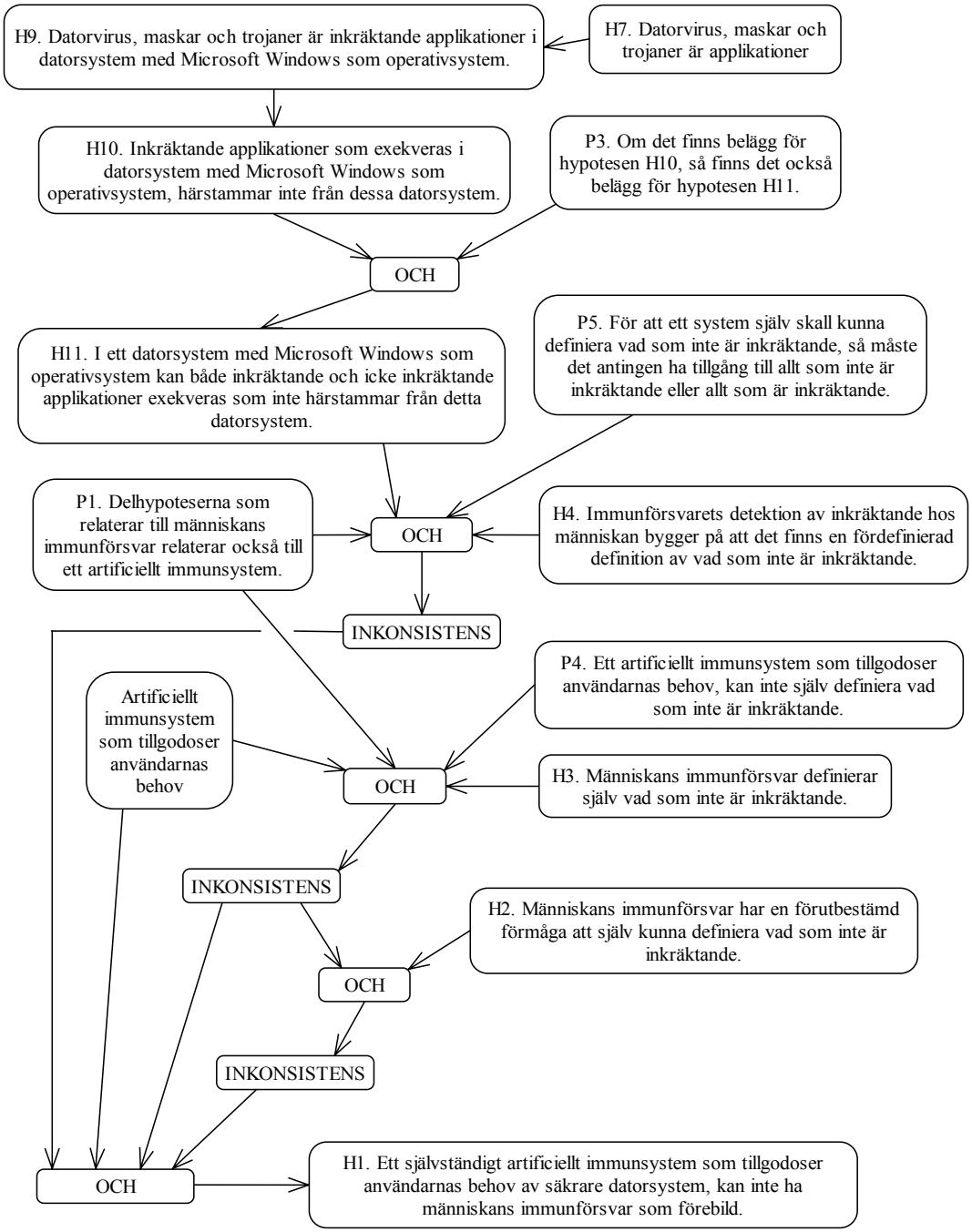
på grund av postulatet

P1. Delhypoteserna som relaterar till människans immunförsvar relaterar också till ett artificiellt immunsystem.

Om det ur detta systems synvinkel inte är möjligt att definiera vad som inte är inkräktande, så strider det även mot hypotesen

H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.

eftersom detta system således inte kan ha en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande. Man kan ju inte ha en förutbestämd förmåga till något som inte är möjligt.



Figur 2 *Illustration av slutledningskedjan*

Om det artificiella immunsystemet skall tillgodose användarnas behov av säkrare datorsystem, så kommer alltså de delhypoteser som relaterar till datorsystem således att vara oförenliga med de delhypoteser som relaterar till människans immunförsvar och därmed finns det belägg för huvudhypotesen

> *H1. Ett självständigt artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, kan inte ha människans immunförsvar som förebild.*

4 Metod

4.1 Metodutformning

4.1.1 Genomförande av datainsamling

Hur data samlas in om människans immunförsvar

Information om människans immunförsvar hämtas från artiklar inom immunologisk forskning i form av en litteraturgenomgång, där fokus läggs på de områden som är relevanta för hypoteserna:

H2. Människans Immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.

H3. Människans immunförsvar definierar själv vad som inte är inkräktande.

H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.

Vi kan dela in hypoteserna i determinism, definition och detektion med avseende på inkräktande och icke inkräktande. Detta förefaller angränsa till de delar av immunologin som fokuserar på själv-ickesjälvdiskriminering och tolerans. Begreppen ’själv’ och ’ickesjälv’ associerar till gränsdragningen mellan det kroppsegna och allting annat, vilket är analogt med icke inkräktande och inkräktande. Närliggande till denna gränsdragning är begreppet ’tolerans’ som anger att immunförsvaret utvecklar en benägenhet att inte reagera mot det som är själv. Det borde därför vara lämpligt att söka efter forskning som fokuserar på dessa begrepp.

Hur data samlas in från Sophos

Information om datorvirus, maskar och trojaner hämtas från Sophos, ett etablerat antivirusföretag som grundades 1985 och som är verksamt i Storbritannien, USA, Kanada, Frankrike, Tyskland, Italien, Japan och Singapore med återförsäljare i över 150 länder (Sophos, 2004). Företagets webbplats innehåller utförliga virusanalyser av flera tusen datorvirus, maskar och trojaner.

Eftersom vi har hypoteser som relaterar till Microsoft Windows, så kommer bara data som relaterar till detta operativsystem att samlas in. Eftersom

hypoteserna endast relaterar till datorvirus, maskar och trojaner, så är det endast den typen av data som kommer att samlas in. Datorvirus, maskar och trojaner är det centrala inom antivirusbekämpning. Även om det på senare tid blivit ett allt större problem med så kallad spyware, så är detta något som för tillfället förefaller ligga utanför antivirusföretagens domäner.

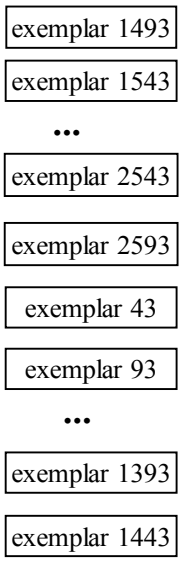
På Sophos webbplats (Sophos, 2004a) är analyserna av datorvirus, maskar och trojaner sorterade i bokstavsordning efter hur de benämns. En stor grupp är de som relaterar till Win32-plattformen, vilken enligt Sophos omfattas av

Windows 95/98/Me, NT och 2000

Dessa benämns med prefixet W32 och är således lätta att urskilja. Här är det oklart om denna gruppering även omfattar Windows XP, men eftersom vi i denna studie inte kommer att göra någon åtskillnad mellan dessa olika plattformar, så spelar det inte så stor roll. I denna studie görs heller ingen åtskillnad mellan datorvirus, maskar och trojaner.

Den tillgängliga populationen är ungefär 2600 exemplar av virusbeskrivningar och därför måste ett urval göras. Eftersom vi är ute efter att testa generella hypoteser, så lämpar sig ett statistiskt urval bäst, som på slumpmässig basis görs enligt en förutbestämd princip. Vi använder här det som Bernard (2000) benämner *systematisk slumpmässig sampling*, eftersom det inte är rimligt att numrera hela populationen. Det är däremot fullt rimligt att räkna fram en slumpmässig startpunkt och därifrån stega fram i fasta intervall.

Utifrån den tidsram som finns till förfogande för studien, så bestäms antalet insamlade exemplar till ungefär 50, vilket innebär att vi har behov av ungefär vart 50:e exemplar, vilket skulle ge ungefär 52 insamlade exemplar. Startpunkten bestäms med hjälp av en slumptalsfunktion i scriptspråket PHP, som i det här fallet slumpar fram ett tal mellan 1 och 2600. Den slumpmässiga startpunkten bestäms utifrån detta till exemplar nummer 1493. Vid slutet av populationen fortsätter insamlingen från början och fram till sista exemplaret före startpunkten. Intervallstorleken är 50. Principen illustreras i figur 3.



Figur 3 *Den systematiska slumpmässiga samplingen av virusbeskrivningar*

Hur data samlas in från Microsoft Security Bulletin

Information om Microsoft Windows hämtas från Microsoft Security Bulletin (Microsoft, 2004) som är en officiell källa för beskrivningar av upptäckta säkerhetsbrister. Eftersom denna information kategoriseras efter deras olika produkter, vilket vida överstiger avgränsningen för denna studie, så kommer följande operativsystemsvarianter att beaktas:

- Windows 95
- Windows 98
- Windows 98 SE
- Windows Me
- Windows NT Workstation 4.0
- Windows 2000 Professional
- Windows XP Home Edition
- Windows XP Professional

Dessa varianter representerar i viss mån en utvecklingskedja av operativsystemet och har tämligen stor spridning. Det finns för tillfället 241 unika bulletiner som relaterar till dessa operativsystem. Det är inte alltför många för att de skall vara möjliga att numrera och därför är det lämpligt att använda den samplingsmetod som Bernard (2000) benämner *enkel slumpmässig sampling*. Utifrån den tidsram som finns till förfogande för studien, så bestäms antalet insamlade bulletiner till 50.

Vi listar de 241 relevanta bulletinerna, ger dem var sitt nummer och genererar sedan 50 unika slumptal bland dessa 241 nummer. Slumptalen genereras genom en slumptalsfunktion i scriptspråket PHP som ger:

155, 107, 106, 28, 36, 116, 166, 71, 228, 217, 70, 218, 75, 168, 76, 225, 12, 66, 21, 114, 142, 101, 1, 204, 83, 210, 199, 241, 100, 206, 212, 182, 87, 72, 73, 82, 141, 50, 156, 68, 126, 139, 79, 191, 160, 150, 64, 60, 9, 65

Detta är numren på de bulletiner som skall plockas ut och de kommer också att analyseras i denna ordning.

4.1.2 Genomförande av analys

För att lätt kunna testa delhypoteserna mot insamlade data, så är det en fördel om de bryts ned till verifierbara frågor som lätt kan kontrolleras. Frågorna konstrueras utifrån hypotesernas innebörder, inom ramarna för stipulationerna och hypotesernas undertexter. Under varje fråga anges den hypotes som ett jakande svar är avsett att stödja.

Anledningen till att numreringen är bruten hänger samman med att vissa hypoteser ändrats som påpekats tidigare.

Hur data om människans immunförsvar analyseras

Dessa frågeställningar följer i regel hypoteserna, eftersom det här inte finns något behov av att bryta ned hypoteserna till verifierbara frågor som lätt kan kontrolleras.

F1. Har immunförsvaret en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande?

Till exempel genom funktioner som utvecklats från individens egen arvsmassa. Stöder hypotesen:

H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.

F2. Definierar människans immunförsvar själv vad som inte skall betraktas som inkräktande?

Till exempel genom att bygga upp en databas med själv-information. Stöder hypotesen:

H3. Människans immunförsvar definierar själv vad som inte är inkräktande.

F3. Bygger immunförsvarets detektion av inkräktande hos människan på att det finns en fördefinierad definition av vad som inte är inkräktande?

Till exempel genom att immunförsvaret först gör en själv-definition och sedan använder denna definition för att avgöra när något är inkräktande. Stöder hypotesen:

H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.

Hur data från Sophos analyseras

Med exemplar avses den typ av datorvirus, mask eller trojan som beskrivningen avser.

F7. Utför detta exemplar operationer som exekveras i ett datorsystem?

Till exempel att någon form av program eller script körs. Stöder hypotesen:

H7. Datorvirus, maskar och trojaner är applikationer.

F9. Utför detta exemplar operationer som användaren inte haft för avsikt att införa i systemet?

Till exempel sådana operationer som uppenbarligen äventyrar säkerheten för systemet. Stöder hypotesen:

H9. Datorvirus, maskar och trojaner är inkräktande applikationer i datorsystem med Microsoft Windows som operativsystem.

F10. Exekveras detta exemplar i datorsystem som det inte härstammar från?

Till exempel att en applikation installeras i ett system som används. Stöder hypotesen:

H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.

Hur data från Microsoft Security Bulletin analyseras

F12. Anger bulletinen att en inkräktande applikation kan installeras efter att datorsystemet tagits i bruk av användaren?

Till exempel att kod på något sätt smygs in i ett system som används. Stöder hypotesen:

H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.

F13. Anger bulletinen att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt?

Till exempel att systemet börjar bete sig på ett nytt sätt. Stöder hypotesen:

H12. Datorsystem med Microsoft Windows som operativsystem är dynamiska strukturer.

F14. Rekommenderar bulletinen att operativsystemet måste uppdateras?

Till exempel för att det finns svagheter i systemet som gör det sårbart. Stöder hypotesen:

H13. Microsoft Windows är ett evolutionärt operativsystem.

Hur forskningen om artificiella immunsystem analyseras

Med anledning av postulatet

P1. Delhypoteserna som relaterar till människans immunförsvar relaterar också till ett artificiellt immunsystem.

så formuleras följande frågor utifrån de delhypoteser som relaterar till människans immunförsvar:

F15. Har det artificiella immunsystemet en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande?

Formuleras från hypotesen:

H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.

F16. Definierar det artificiella immunsystemet själv vad som inte är inkräktande?

Formuleras från hypotesen:

H3. Människans immunförsvar definierar själv vad som inte är inkräktande.

F17. Bygger det artificiella immunsystemets detektion av inkräktande på att det finns en fördefinierad definition av vad som inte är inkräktande?

Formuleras från hypotesen:

H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.

Vi analyserar det som finns under rubrikerna

2.1.6 Definition av vad som skall betraktas som icke inkräktande i datorsystem

2.1.7 Detektion av vad som skall uppfattas som inkräktande i datorsystem

eftersom det är där som olika principer tas upp.

Hur de två immunologiska referensramarna jämförs

Denna analys försöker belysa korrespondensen mellan de immunologiska referensramarna, för att se om den immunologiska forskningens syn på immunförsvaret skiljer sig från hur den tidigare forskningen om artificiella immunsystem ser på immunförsvaret. Detta för att se om det kan finnas utgångspunkter som ger olika förutsättningar för ett artificiellt immunsystem.

För detta ändamål kommer vi att extrahera ett antal kategorier från

2.1.2 Det biologiska immunförsvaret enligt den tidigare forskningen om artificiella immunsytem

som sedan testas mot

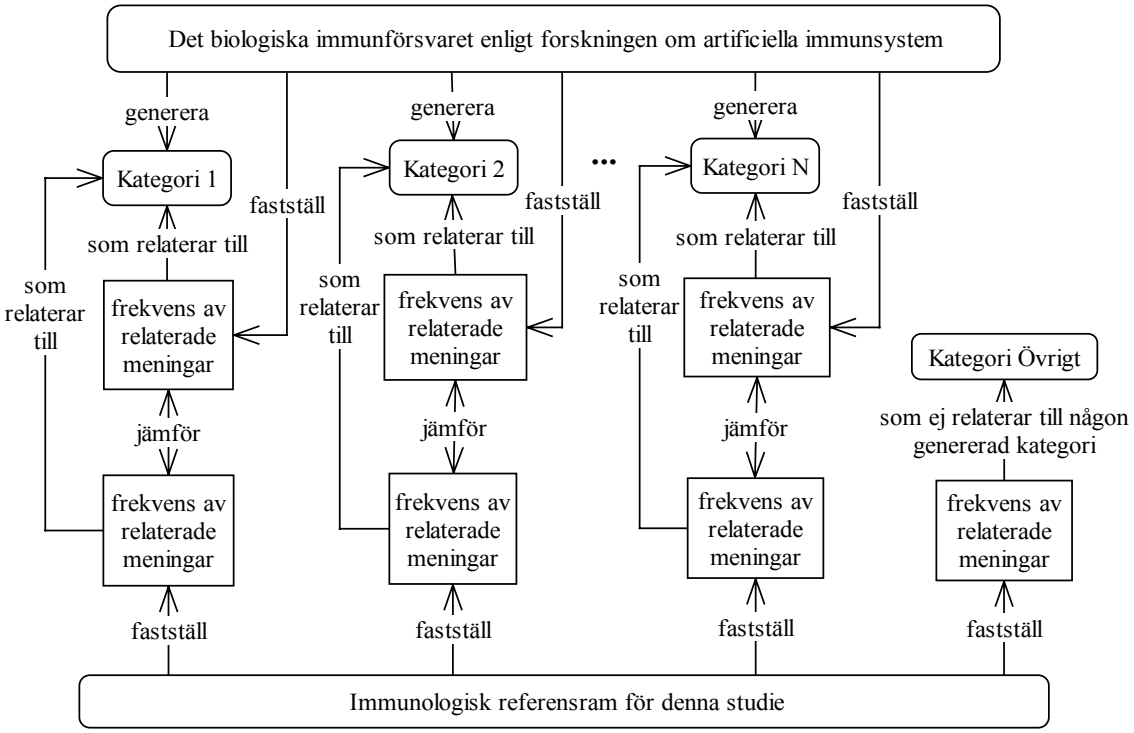
2.2 Immunologisk referensram

genom att försöka tillämpa de genererade kategorierna. Poängen är att ta fram gemensamma referenspunkter för de olika referensramarna, där kategorierna utgör basen för jämförelsen. Hur referensramarna skiljer sig i omfattning av respektive kategori, blir ett mått på korrespondensen mellan referensramarna. Kategorigenereringen bygger på den öppna kodningen i grundad teori. Kategoritestningen bygger på kategoriseringsprincipen som används vid innehållsanalys. Principen för jämförelsen illustreras i figur 4.

Kategorigenerering från *2.1.2 Det biologiska immunförsvaret enligt den tidigare forskningen om artificiella immunsytem*:

1. Texten gås igenom mening för mening. Varje mening får en rubrik enligt den innebörd som representeras. Om flera innebörder kan uttolkas, genereras flera rubriker.
2. Rubriker som angränsar till varandra grupperas i kategorier, som rubriceras efter grupperingens innebörd.
3. Grupperingarna gås igenom för att se om det finns rubriker som bör flyttas till andra kategorier.
4. Antalet rubriker anges för respektive kategori.

5. Den relativa andelen av samtliga rubriker anges för respektive kategori.



Figur 4 *Principen för jämförelsen mellan referensramarna*

Kategoritestning mot *2.2 Immunologisk referensram*:

1. En tabell sätts upp, där varje rad representerar en mening i texten. Kolumnerna representerar de kategorier som genererats i kategorigenereringen. En övrigt-kolumn läggs till som representerar sådant som inte kan hänföras till någon existerande kategori.
2. Texten gås igenom mening för mening. Varje mening avstäms mot de kategorier som genererats i kategorigenereringen. Varje kategori som kan associeras med meningen markeras med ett kryss i motsvarande cell på meningens rad i tabellen. Mening som kan betraktas som ren övergång räknas inte. Mening som introducerar punktlista, räknas inte om den inte tillför något utöver punkternas innebörd. Varje punkt räknas som en mening.
3. Summan av antalet kryss anges för varje kategori.
4. Den relativa andelen av samtliga kryss anges för respektive kategori.

Kategoriernas relativa frekvens förs samman i ett stapeldiagram, där varje kategori representeras med en stapel från kategorigenereringen och en stapel från kategoritestningen. Staplarna visar den relativa frekvensen av meningar som associerar till respektive kategori.

Denna jämförande analys skall inte ses som central för studien, utan finns endast med som belysning av de immunologiska förutsättningarna. Även om studien som sådan endast syftar till att ge belägg för vissa hypoteser, så kan det vara relevant att illustrera skillnader i perspektiv.

4.2 Den metodologiska referensramens koppling till genomförandet

4.2.1 Den vetenskapliga metodens relevans för denna studie

Bowler (1992) säger att teorier blir framgångsrika eftersom de ger en allt bättre bild och kontroll av naturen. Relaterar vi det till forskningen inom artificiella immunsystem, så kan vi konstatera att det varken finns någon bra bild eller kontroll av det området. Det finns några uppslag till detektionsprinciper, men man förefaller inte ens vara i närheten av det fundament som ett artificiellt immunsystem måste bygga på. Graziano och Raulin (1989) menar att det huvudsakliga målet är att utveckla teorier och nämner bland annat deduktiva teorier, som är formulerade konstruktioner som ligger till grund för slutledningar som kan testas mot verkligheten, där gynnsamma utfall ger belägg för teorin. Det är den ansatsen vi använder här, även om vi inte utvecklat någon fullskalig teori, blott en hypotetisk konstruktion.

Bowler (1992) uppfattar att den vetenskapliga metoden alltid haft fysiken som ledstjärna, men lyfter fram att ’mjuka’ vetenskaper kräver en metodologi som gör det möjligt att testa hypoteser på ett icke lika fullt rigoröst sätt. Det är den ansatsen vi använder här. Det immunologiska området är långt ifrån fullt utforskat och därför måste viss argumentation bygga på vad som förefaller troligt utifrån existerande teorier.

Hur den hypotetisk-deduktiva metoden relaterar till denna studie

Enligt Bowler (1992) ställer vetenskapsmännen upp hypoteser och gör förutsägelser om vad som skall ske i en specifik situation, där dessa testas mot observationer eller experiment. Ansatsen som används här är ett antal hypoteser som testas mot den immunologiska teorin, mot information från Microsoft om kända sårbarhetsproblem, och mot beskrivningar från Sophos av olika datorvirus.

Bowler (1992) säger att den moderna vetenskapsfilosofin inser att det behövs någon form av vägledning som talar om vilka fakta som är relevanta. Det har på det immunologiska området varit nödvändigt att göra någon form av avgränsning i datainsamlingen för att över huvud taget kunna samla in data. Denna avgränsning har koncentrerats till själv-ickesjälvdiskriminering och tolerans, eftersom detta förefaller vara centrala delar för hypoteserna.

Graziano och Raulin (1989) säger att skillanden mellan att använda induktivt-deduktivt tänkande inom vetenskapen och till vardags, är att vetenskapen

kräver mycket högre precision. Detta är något som i högsta grad är relevant för denna studie. Utgångspunkten för hypoteserna grundar sig egentligen på några enkla antaganden som skulle vara möjliga att ge argument för utan någon egentlig datainsamling. Problemet är att argument som inte beläggs på något sätt saknar tyngd. Vem som helst kan påstå vad som helst; det som gör det troligt är oberoende indikationer som visar att påståendet är rimligt.

Hypotesgenereringen i denna studie

Hempel (1969), liksom Bowler (1992) låter vetenskapsmännen få fritt spelrum för det kreativa tänkandet, som till och med kan basera sig på vetenskapligt tvivelaktiga uppfattningar. Man uppfinner hypoteser som sedan underkastas empirisk testning. Detta är ansatsen som används i denna studie, även om den empiriska testningen handlar om sekundära data – som för övrigt varit empiriska data i något annat sammanhang.

Bowler (1992) anser dock att inslaget av dessa icke-rationella faktorer innebär att vetenskapen inte kan vara fri från värderingar, vilket dock försvaras av Hempel (1969) som tycker att det legitimeras av principen att hypoteserna accepteras om de klarar kritisk granskning, en inställning som genomsyrar denna studie. Det är svårt att tänka sig hur man skulle kunna konstruera någonting över huvud taget, om man inte hade en grund att stå på.

Hypotestestningen i denna studie

Graziano och Raulin (1989) säger att hypotestestning är ett kritiskt moment i experimentell forskning, där man utgår från en begynnande idé som utifrån inledande observationer och tidigare forskning preciseras. Detta har varit gången i denna studie. Enligt Bowler (1992) för den hypotetisk-deduktiva metoden vetenskapen framåt genom att testa konsekvenserna av den konstruerade modellen, där varje aspekt av hypotesen utsätts för rigorös testning. Även om det är svårt att betrakta hypotestestningen i denna studie som rigorös, så görs likväl en ansats att utifrån tillgängliga sekundära data och tidsmässiga resurser, hitta så gott stöd som möjligt.

Frågan är dock om det spelar någon roll om en hypotes klarar rigorös testning eller ej. Hempel (1969) ser inte hypotesen som bindande även om den klarar omfattande tester och för Popper gäller det att alltid söka efter svagheten i idéerna, så att de kan ersättas med någonting bättre. Det gör att i princip allting blir förgängligt och varför skulle man lägga ned någon större energi på något som på förhand är dömt att ersättas med någonting bättre? Risken är att man förkastar bra hypoteser på grund av att mätmetoderna är för dåliga. Tänk om mätinstrumenten inte är adekvata? Ingen kedja är starkare än sin svagaste länk. Så varför skall hypotestestningen vara mekanisk, när hypotesgenereringen inte är det?

Enligt Hempel (1969) finns det heller inte några mekaniska regler för slutledningsproceduren. Det mekaniska ligger istället i att kontrollera om

slutledningen är giltig i form av systematiska slutledningssteg. Det är en ansats som gällt för denna studie. Från början ställdes ett antal hypoteser upp, som efter allt bättre inläsning på det immunologiska området reviderades, för att så småningom anta sin slutgiltiga form. Här finns en huvudhypotes, som stöds av ett antal delhypoteser och postulat, som länkas ihop i en slutledningskedja. Accepterar man postulaten och belägger delhypoteserna, så blir slutledningen giltig.

Varför vissa moment i den grundade teorin är relevanta för denna studie

Bernard (2000) beskriver grundad teori som ett sätt att fånga upp kategorier och begrepp som implicit förekommer i en text. Detta är den ansats som används i denna studie. Vi konstruerar inte någon formell teori med hjälp av teorigrundningsmetoden, utan vi är enbart intresserade av att låna vissa moment från denna metod. Det skall här således inte uppfattas som att vi använder oss av grundad teori som metod.

Pandit (1996) anger begrepp, kategorier och antaganden som grundläggande element för grundad teori. Det som relaterar till denna studie är det som enligt Bryman (2004) syftar till att få fram kategorier med tillhörande egenskaper. Vi har inte specificerat kategorierna, vilket kan ses som en brist, eftersom tolkningarna av dem då kan bli tvetydiga. Kategorigenereringen har heller inte gjorts med några kriterier, som i Pandits ordalag kan vara enkla frågor. Anledningen till att kategorierna inte har specificerats är att det inte har bedömts nödvändigt i detta sammanhang.

Syftet har här inte varit att göra en uttömmande analys, utan endast att skapa ett enkelt redskap för att jämföra två olika texter. Det centrala för studien är att finna stöd för hypoteser, inte att jämföra texter och därför görs endast en mindre ansats att jämföra de immunologiska referensramarna. Av Bernards sex steg, kan man säga att de tre första har använts här; läsa ett textstycke, plocka ut kategorier samt gruppera data och se hur de hänger ihop.

Varför innehållsanalysen är relevant för denna studie

Bryman (2004) anger innehållsanalys som ett sätt att kvantifiera textinnehållet utifrån förutbestämda kategorier. Det är exakt den ansats som används här. Stemler (2001) definierar innehållsanalys som en replikerbar och systematisk teknik, för att konvertera en stor textmassa till färre kategorier, genom explicita kodningsregler. Ansatsen i denna studie är systematisk och det finns explicita kodningsregler. Frågan är bara om resultatet är replikerbart. Det finns inget som säger att en annan uttolkare skulle göra samma kategorisering.

Stemler (2001) säger att replikerbarheten kommer av att tekniken tillämpas på varaktiga data. Det skulle i så fall innebära att en uttolkare har möjlighet att demonstrera utförda tolkningar för en annan uttolkare, hur kategoriseringen är gjord. Det säger dock ingenting om hur en tolkning skall göras. Därför finns de explicita reglerna. Men för att de explicita reglerna skall fungera, så krävs det

att de entydigt skall gå att tillämpa på varje mening i texten. Detta förutsätter i princip att man känner till varje mening när man utformar de explicita reglerna, vilket i sin tur gör reglerna överflödiga.

Stemler (2001) säger att kategorierna skall vara ömsesidigt uteslutande, där varje begrepp endast skall kunna hänföras till en enda kategori. Detta är ett krav som hänger samman med replikerbarheten. Men vad spelar det för roll om begreppen i slutändan måste tolkas? Tolkning är av naturen tvetydig och att försöka göra den så exakt som möjligt förskjuter bara problemet till någon annan länk i kedjan. Entydig tolkning förutsätter distinkt problematik som inte är överlappande. Eftersom det immunologiska området innehåller mekanismer och begrepp som i princip flyter in i varandra, så har inte så stor vikt lagts vid entydig kategorisering i denna analys.

Roberts (2001) förklarar den klassiska innehållsanalysen som att symboliska data genereras som underlag till statistisk analys. Det är i princip det som äger rum i denna studie. Vi har två textmassor som vi vill jämföra med varandra och därför kvantifierar vi innehållet och slår ihop resultatet i ett illustrerande diagram. Stemler (2001) säger att olika personer skall kunna utföra kodningen på samma sätt och där oklara kategoridefinitioner och kodningsregler skapar problem. Här finns en klar risk att diagrammet skulle se annorlunda ut om någon annan gjorde kodningen. För detta ändamål har kopplingarna till texten gjorts explicita, där varje rad innehåller ett textfragment, för att det därigenom skall vara möjligt att kontrollera hur kodningen har gjorts.

Även Bernard (2000) ser kodningen som ett kritiskt moment, där man efter att ha tillämpat kodningen på texterna skall testa tillförlitligheten i kodningen. Detta har inte gjorts i denna studie. Man måste här se hela sammanhanget. Syftet med kategorigenereringen och testningen är att kunna se om två olika immunologiska referensramar korresponderar med varandra. För detta ändamål använder vi oss av texterna som producerats i denna studie. Men eftersom den immunologiska referensramen för den tidigare forskningen om artificiella immunsystem förmodligen inte är uttömande, så är risken stor att underlaget till analysen är bristfälligt. Att med stor precision mäta något som från början förefaller vagt är slöseri med resurser. Det upplägg som här använts blir därför det mest rationella.

4.2.2 Datainsamlingens relevans för denna studie

Varför sekundära data används i denna studie

Bryman (2004) lyfter fram ett antal möjligheter och begränsningar med sekundära data. Det som relaterar till denna studie är:

- *Tid och pengar*: Denna studie skulle i princip inte vara möjlig att genomföra utan tillgång till sekundära data
- *Mer tid till dataanalys*: Data har mer eller mindre uteslutande erhållits via internet, vilket har underlättat insamlingen markant. Analysen, som är det

centrala, har därför fått en mycket framträdande roll och speciellt möjliggjort förberedande utforskning av data som underlag till utformningen av hypoteser.
- *Dataexploatering*: Här har speciellt immunologiska data utnyttjats på annat sätt än de ursprungliga intentionerna.
- *Komplexitet*: Eftersom det inte funnits några förkunskaper om det immunologiska området, så har det krävts en omfattande inläsning på området för att över huvud taget kunna relatera till det.
- *Avsaknad av nyckelvariabler*: Mycket inom det immunologiska området bygger på vedertagna mekanismer inom medicin och mikrobiologi. Detta gör att det blir väldigt svårt att belägga mer eller mindre självklara samband, speciellt det som i denna studie relaterar till genetik och förutbestämdhet. I datorvirusbeskrivningarna och säkerhetsbulletinerna har inte funnits några specifika kategorier som relaterar till denna studie, förutom rekommendationer om att operativsystemet måste uppdateras. Information om till exempel kodexekvering har varit godtycklig och har därför inte alltid funnits tillgänglig.

Varför valda samplingsstrategier är relevanta

Flick (1998) listar ett antal samplingsstrategier, där den statistiska strategin är det som relaterar till denna studie. Graziano och Raulin (1989) förklarar slumpmässig sampling med att varje individ i populationen har lika stor chans att bli vald, vilket har varit önsvärt i denna studie. Bernard (2000) delar in den slumpmässiga samplingen i enkel slumpmässig sampling och systematisk slumpmässig sampling. För denna studie har den enkla slumpmässiga samplingen använts vid insamlingen av säkerhetsbulletiner, eftersom de inte varit oöverkomligt många. Den systematiskt slumpmässiga samplingen har använts för insamlingen av virusbeskrivningar, eftersom denna population har varit för stor att kunna numrera.

Bernard (2000) påpekar att en risk med systematisk slumpmässig sampling är att det finns ett periodicitetproblem om vissa kategorier råkar vara grupperade systematiskt. Såsom virusbeskrivningarna är listade, så förfaller detta inte vara någon risk här. Graziano och Raulin (1989) pekar på vikten av samplingens generalitet. De populationer som funnits tillgängliga kan mer eller mindre betraktas som allmängiltiga. Microsofts säkerhetsbulletiner (Microsoft, 2004) omfattar alla publicerade bulletiner från 1998 och framåt. Sophos virusbeskrivningar (Sophos, 2004a) innehåller flera tusen exempel på exemplar som är typiskt förekommande. De valda samplingsstrategierna förefaller i detta sammanhang ge ett så representativt urval som möjligt.

Den risk för bias som påtalas av Graziano och Raulin (1989), förefaller således vara liten. Det är främst på det immunologiska området som detta skulle vara en risk, eftersom samplingen där utförts på en avgränsad grupp. Sökningen efter artiklar har främst gjorts på själv-ickesjälvdiskriminering och tolerans, vilket skulle kunna innebära att alternativa ansatser kommit i skymundan. Det har dock visat sig att artikelpopulationen innehåller både förespråkare och kritiker till olika ansatser, samtidigt som flera principer utöver själv-

ickesjälvdiskrimineringen presenterats i artiklarna. Den immunologiska litteraturen har för övrigt ett tydligt fokus på själv-ickesjälvdiskriminering och tolerans, vilket i viss mån legitimerar en sådan avgränsning.

4.2.3 Studiens integritet

Hur denna studie påverkar validiteten

Graziano och Raulin (1989) relaterar validitet till metodologisk sundhet och lämplighet, att en giltig mätning testar det den skall testa. Enligt Bernard (2000) måste de slutsatser man drar vara riktiga och inte grunda sig på ogrundade antaganden. I denna studie har i väldigt stor utsträckning förekommande begrepp definierats, samtidigt som hypotesernas innebörder gjorts explicita. Detta borde göra risken mindre för att perspektivet snedvrids. Graziano och Raulin (1989) föreslår ju också att forskaren skall skapa procedurer för att reducera hot mot validiteten. Klargörandet av begrepp och innebörder skulle kunna betraktas som en sådan procedur.

Enligt Silverman (2001) kan validitetsfel vara att man accepterar en korrelation som orsakssamband när det kanske finns en okänd faktor med i bilden. I denna studie är det snarare regel än undantag att orsaksmekanismer antas på basis av indirekta indikationer. Detta innebär naturligtvis en stor risk för potentialen att okända faktorer styr mekanismerna. Enda sättet att förhålla sig till detta är att kontinuerligt relatera detaljerna till helheten och att betrakta dem ur flera synvinklar. Men som Graziano och Raulin (1989) säger, man kan nöja sig med korrelationer om man inte har höga krav på orsakssamband. Huvudskälet till att vi här inte kan ha några höga krav på orsakssamband, är helt enkelt att den immunologiska forskningen inte är tillräckligt uttömmande. I mångt och mycket påminner argumentationen för olika detektionsprinciper om den argumentation som förs inom forskningen om artificiella immunsystem. Det förefaller som om de immunologiska principerna för detektion fortfarande befinner sig på det hypotetiska stadiet.

Graziano och Raulin (1989) listar några typer av validitet. Det som relaterar till denna studie är:
Konstruktionsvaliditet: Vi har här ett antal hypoteser som beläggs med insamlade data. Men även om det finns belägg för hypoteserna, så innebär det inte att alternativa ansatser inte skulle kunna vara giltiga. När det gäller delhypoteserna som relaterar till människans immunförsvar, så har det förutsatts att detta är fundamentala aspekter. Det är naturligtvis möjligt att andra gör en annan bedömning, men utifrån den bild som växt fram från den immunologiska litteraturen, så är det inte sannolikt.
Extern validitet: Hypoteserna testas på datorsystem med Microsoft Windows, eftersom detta är ett utbrett och typiskt operativsystem. Det är möjligt att man skulle kunna konstruera alternativa datorsystem, med en helt annan uppbyggnad som strider mot hypoteserna. Så som hypoteserna är uppbyggda förutsätter detta i så fall mer eller mindre datorsystem som utvecklar sig själva.

Silverman (2001) listar några kriterier för att fastställa validiteten och nämner bland annat forskarens påverkan och värderingar. Detta kan exemplifieras med Hofmeyr (2004), som anser att vi är begränsade i våra immunologiska kunskaper, vilket kan leda in på villovägar vid tillämpningen av analogin. Från början fanns en stark drivkraft att hitta analogier mellan det mänskliga immunförsvaret och ett artificiellt immunsystem, men allt eftersom inläsningen på det immunologiska området blev allt mer omfattande, så växte bilden fram att någon sådan analogi inte stod att finna. Denna helomvändning har bidragit till en distansiering av studieobjektet, vilket också borde innebära att perspektivet blivit mer objektivt.

Hur denna studie påverkar reliabiliteten

Graziano och Raulin (1989) förknippar reliabilitet med reproducerbarhet, där någon annan skall kunna genomföra mätningarna på samma sätt, vilket också påtalas av Silverman (2001). Det mesta i analyserna i denna studie handlar om någon form av tolkning, till exempel att en virusbeskrivning antyder att en användare inte har för avsikt att införa denna funktionalitet i systemet. Graziano och Raulin (1989) nämner tolkningsreliabilitet, liksom Silverman (2001). Tolkningar kan dock aldrig vara exakta och därför finns alltid en risk att någon annan tolkar data på ett annat sätt. För att undvika det, så har kriterier o.d gjorts så konkreta som möjligt. Graziano och Raulin (1989) säger ju att reliabiliteten är avhängig precisionen i hur problemställningen operationaliserats, vilket kan relateras till att huvudhypotesen i denna studie har delats upp i delhypoteser, som i sin tur brutits ned till verifierbara frågor.

Här aktualiseras det som Silverman (2001) benämner *idealistisk reliabilitet*, där det handlar om vilken nivå reliabiliteten skall läggas på för att den skall fylla någon rimlig funktion. Att göra saker allt för abstrakta leder till för stort tolkningsutrymme, medan för stor konkretisering leder till svårigheter att över huvud taget få några svar. Enligt Silverman (2001) är data som hämtats från texter i princip mer tillförlitliga än observationer, eftersom data redan finns för handen. Detta har också varit en stor fördel i denna studie, eftersom det har varit möjligt att på förhand, obehindrat utforska data, för att på så sätt få ett underlag till upplägg. Detta har framförallt bidragit till att hitta balansen i den idealistiska reliabiliteten, där förhandsgranskning av till exempel virusbeskrivningar har givit ledtrådar om vilken nivå som varit lämplig att lägga sig på.

Silverman (2001) menar att det finns förespråkare för att reliabilitet endast är en fråga för kvantitativ forskning, eftersom det inte fyller någon funktion att undra om mätinstrumenten är tillförlitliga när den sociala verkligheten ändå behandlas lite på måfå. Även om det kanske ligger något i detta antagande, speciellt när det finns tolkningsutrymme, så måste ambitionen vara att försöka göra tolkningsutrymmet så smalt som möjligt.

Varför trianguleringsbegreppet relaterar till denna studie

Det skall här först och främst påpekas att denna studie inte har triangulerat i den metodmässiga betydelsen. Anledningen till att begreppet ändå tas upp är att konceptet i viss mån kan relateras till denna studie ur ett validitets- och reliabilitetsperspektiv.

Trianguleringens syfte i denna studie

Enligt Fielding och Fielding (1986) kommer begreppet triangulering av att två landmärken kan användas till att lokalisera skärningspunkten, vilket ger ett vidare perspektiv. I denna studie har två olika perspektiv använts när det gäller datainsamlingen som relaterar till datorsystem. Dels har data hämtats från Sophos som har information om virus som utnyttjar svagheter i Microsofts system, dels har data hämtats från Microsoft om svagheter i sina egna system. Detta gör att hypoteserna belyses från två håll, vilket borde ge en mer rättvisande bild än om data till exempel bara hade hämtats från Sophos, även om Fielding och Fielding (1986) säger att triangulering inte skall användas för att uppnå någon objektiv sanning.

Fielding och Fielding (1986) säger att triangulering medger att forskaren identifierar svagheter i sitt material. I studien hämtas belägg för en hypotes från både Sophos och Microsoft. Dessa olika infallsvinklar kan bidra till att belysa svagheter i materialet, samtidigt som resonemanget stärks om det bekräftas från olika håll. Även om det i resultatet visat sig finnas en märkbar skillnad, så ges tydliga indikationer på ett stöd för hypotesen från bägge håll. Det hade varit mer problematiskt om det från ena källan till exempel hade funnits stöd till 85%, samtidigt som det bara hade varit 15% från den andra. Nu var det 85% respektive 65%, vilket rimligtvis måste betraktas som acceptabelt (se *6.2 Resultat av analys av Sophos-data*, *6.3 Resultat av analys av Microsoft-data* och *6.6 Slutsats*).

Trianguleringstyper som är relevanta för denna studie

Fielding och Fielding (1986) ger exempel på olika typer av triangulering. Det som relaterar till denna studie är:

Triangulering av datakällor: Relaterade data har hämtats från två håll. Även om vi inte triangulerar i egentlig mening, så finns det inget som hindrar att man analyserar sitt upplägg utifrån dessa principer.

Teoritriangulering: Både den tidigare forskningen om artificiella immunsystem och denna studie utgår från vissa immunologiska teorier. Genom att jämföra dessa olika immunologiska referensramar, så får man en uppfattning om det finns skillnader i hur den immunologiska teorin skall tolkas. Detta är här speciellt relevant, eftersom det i regel rör sig om forskare som saknar immunologisk bakgrund.

Hur bias inverkar på denna studie

Fielding och Fielding (1986) påpekar att teoritriangulering nödvändigtvis inte reducerar bias, som till exempel kan vara att man hellre väljer data som passar ens föreställningar om fenomenet. Både den tidigare forskningen om de artificiella immunsystemen och denna studie kan sägas ha en föreställning om att det är själv-ickesjälvdiskrimineringen som står i centrum, vilket också har medfört att det är sådana data som i första hand har sökts. En allmän inläsning av den immunologiska litteraturen har dock i viss mån bekräftat själv-ickesjälvdiskrimineringens centrala roll, vilket i viss mån borde reducera denna form av bias.

5 Analys

5.1 Analys av data om människans immunförsvar

Analysen syftar till att försöka ge indikationer på mekanismer och principer som svarar på frågorna:

F1. Har immunförsvaret en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande?

F2. Definierar människans immunförsvar själv vad som inte skall betraktas som inkräktande?

F3. Bygger immunförsvarets detektion av inkräktande hos människan på att det finns en fördefinierad definition av vad som inte är inkräktande?

Dessa områden är grunden för analysen. Först analyseras de generella förutsättningarna, följt av det naturliga immunförsvaret, som i detta sammanhang egentligen inte har så stor betydelse, eftersom det är allmänt vedertaget att detta är medfött. Därefter följer en analys av själv-perspektivet, där tyngdpunkten lagts, eftersom detta perspektiv förefaller vara centralt inom immunologin. Avslutningsvis kommer störnings- och skade-perspektiven, som dock fått mindre fokus, eftersom de immunologiskt sett är mer diffusa och oklara. Övriga perspektiv, som till exempel farligt, beaktas inte eftersom det inte finns tillräckligt material för analys. Rubrikområdet *Immunförsvarets detektion av vad som skall uppfattas som farligt* har tagits med i den immunologiska referensramen för att visa på dess existens, men det relateras inte vidare i uppsatsen. Detta gäller även rubrikområdet *Immunförsvarets detektion av vad som skall uppfattas som inkräktande i vävnadsbarriärer*.

5.1.1 Analys av immunförsvarets generella förutsättningar

Något som antyder att allting är förutbestämt är DNA, som enligt Alberts et al (2002) är ett språk som alla levande celler har gemensamt. Vander, Sherman och Luciano (1998) menar ju också att individens utveckling bestäms av uttrycket av den genuppsättning som ärvs i och med befruktningsögonblicket. Det ligger således ganska nära till hands att konstatera att spelreglerna för immunförsvaret är givna redan från start.

Vander, Sherman och Luciano (1998) säger att varje mänsklig organism härstammar från det befruktade ägget, där detta sedan ger upphov till differentierade celler som i slutändan specialiserar sig på olika saker. Vander,

Sherman och Luciano (1998) säger också att immunförsvaret utgörs av de celler som kollektivt försvarar organismen. Eftersom det dessutom, enligt Guyton och Hall (2000), är generna som finns i kärnan av alla celler som kontrollerar de vardagliga funktionerna i kroppens alla celler, så är det rimligt att anta att generna också styr immunförsvaret och att dessa gener kommit med det befruktade ägget. Guyton och Hall (2000) ger ju också uttryck för att det genetiska systemet kontrollerar varje steg i människans utveckling, vilket således också borde inkludera immunförsvaret.

Det är dock möjligt att hävda att generna sätter upp ramar, medan något annat bestämmer spelreglerna innanför dessa ramar. Tauber (2000) menar till exempel att organismen förändras inom ramarna för en genetiskt programmerad kapacitet. Alberts et al (2002) påpekar dock att den genetiska informationen mest består i instruktioner för tillverkning av protein, där dessa molekyler upprätthåller cellernas funktionalitet och dessutom reglerar hur generna kommer till uttryck. Det skulle i så fall innebära att generna både talar om hur de själva skall regleras, samtidigt som de specificerar kroppens funktionalitet i övrigt. Det betyder att det är fullt möjligt att generna både sätter upp ramarna och anger spelreglerna innanför dessa ramar.

5.1.2 Analys av det naturliga immunförsvaret

Enligt Chaplin (2003) finns det två kategorier av igenkänning, en som är genetiskt hårdkodad i form av det naturliga immunförsvaret, och en som är genetiskt kodad i form av det adaptiva immunförsvaret, med förmåga att somatiskt omstruktureras till specifik igenkänning.

Om vi först avhandlar det naturliga immunförsvaret, så står det klart att förutsättningarna finns där från början för att kunna definiera vad som inte är inkräktande. Medzhitov och Janeway (2000) säger liksom Chaplin (2003) att det naturliga immunförsvaret är kodat via germline och att medfödda självreceptorer har avlägsnat under evolutionen. Dessa receptorer kodas enligt Medzhitov och Janeway (2000) via germline och uttrycks utan att omstruktureras. Det naturliga immunförsvaret innehåller alltså inga gener som skulle kunna koda självreceptorer och därmed definierar det naturliga immunförsvaret inte något själv, eftersom det redan är gjort på förhand.

Re och Strominger (2004) antyder att det naturliga immunförsvaret är avhängigt de germline-kodade receptorerna, vilka Fazekas de St Groth (1998) menar kodats genom evolutionen för att de känner igen gemensamma drag hos patogenerna, något som också stöds av Kyewski, Derbinski, Gotter och Klein (2002). Eftersom Miller (2004) dessutom ser denna utveckling som en kraftfull diskriminering mellan själv och ickesjälv, så borde det stå tämligen klart att det naturliga immunförsvaret inte på egen hand kan definiera vad som inte är inkräktande, eftersom det är definierat på förhand.

Vi kommer således i fortsättning bara att tala om det adaptiva immunförsvaret, vilket också är det som är mest intressant att studera i detta sammanhang.

5.1.3 Analys av immunförsvaret ur själv-perspektivet

Analys av immunförsvarets detektion av ickesjälv

Langman och Cohn (2000a) säger att själv-ickesjälvdistinktionen görs på grundval av frånvaro av igenkänning. Enligt Chaplin (2003) sker detektionen utifrån strukturella drag som utmärker patogenerna mot värdcellerna. Här finns alltså en tydlig princip om att detektionen bygger på att något avviker från det normala. Alam och Gorska (2003) ser det som en grundläggande uppgift för immunförsvaret att försvara själv mot ickesjälv. Hanahan (1998) hävdar att själv-ickesjälv-igenkänningsprincipen har fastställts experimentellt och även Chaplin (2003) anser att denna förmåga står i centrum. Langman och Cohn (2000) säger också att de somatiska mekanismerna utvecklas till att de ickesjälv-igenkännande elementen aktiverar självdestruktiva processer.

Det finns dock kritiska röster som talar mot denna detektionsform. Cohen (2000) säger att konceptet inte är adekvat eftersom immunförsvaret måste göra avvägningar efter omständigheterna, oavsett om det rör sig om själv eller ickesjälv. Efroni och Cohen (2003) anser inte att immunförsvaret karakteriseras av vad det känner igen, utan av hur det reagerar. Dessa invändningar förskjuter dock bara problemet, eftersom det likväl måste finnas något som avgör när något skall betraktas som inkräktande. Detta angränsar till tids- respektive rumsavgränsningen hos Langman och Cohn (2000a), där rumsavgränsningen inte löser något eftersom det kräver en mekanism som sitter vid ingången och sorterar mellan själv och ickesjälv. Langman och Cohn (2000a) säger ju också att själv-ickesjälvdiskrimineringen är nödvändig eftersom varje destruktiv försvarsmekanism måste kunna skilja mellan värd och patogen.

Silverstein och Rose (2000) hävdar att immunförsvaret inte klarar av att göra en distinktion mellan själv och ickesjälv och att de regler som styr immunsvaret gäller för alla antigener, oavsett om de är själv eller ickesjälv, skadliga eller harmlösa. Rose (1999) säger uttryckligen att det inte är någon fundamental skillnad på självantigen och ickesjälvantigen. Likväl anger Silverstein och Rose (2000) att själv blir en samling antigener som inte är kapabla att förorsaka en reaktion. Det borde i så fall betyda att ickesjälv är det som är kapabelt att förorsaka en reaktion. Silverstein och Rose (2000) anger ju också den negativa selektionen i tymus på T-celler, som den främsta centrala mekanismen för att nedreglera immunsvaret. Självdefinitionens relevans handlar tydligen bara om valet av perspektiv, även om Efroni och Cohen (2003) tycker att själv-ickesjälvdiskrimineringen mjölkats till sista droppen.

Miller och Basten (1996) ser till exempel inte steget i utvecklingsprocessen som avgörande för immunsvaret, utan anser att det snarare handlar om att omogna lymfocyter förstörs, medan mogna lymfocyter utlöser immunitet i mötet med antigen. Även Rose (1999) pekar på förhållanden under presentationen av antigen. Problemet är bara att detta inte löser problemet med

hur inkräktande skall hanteras. Ett antigen som kommer i kontakt med en mogen lymfocyt kommer således att angripas, samtidigt som ett antigen som kommer i kontakt med en omogen lymfocyt istället utvecklar tolerans. Detta kräver att de omogna lymfocyterna isoleras från ickesjälv-antigenerna, vilket endast är möjligt om en initial självdefinitionsprocess äger rum. Det spelar ingen roll om det krävs flersignalsaktivering för att utlösa immunreaktionen, ty distinktionen måste likväl göras någonstans, hur många faktorer man än blandar in.

Det borde således vara rimligt att tolka att detekteringen bygger på en fördefinierad definition av vad som är själv.

Analys av immunförsvarets definition av själv

Vi kan börja med att konstatera att själv förmodligen inte kan baseras på DNA i sin helhet, som Chen (2001) föreslår, eftersom det enligt Miller (2004) är svårt att tänka sig någon mekanism som skulle kunna granska allt innehåll i DNA. DNA befinner sig dessutom i regel, svåråtkomligt i cellernas kärnor. Med tanke på att antigenmaterialet som presenteras för immunförsvaret, vanligtvis endast är DNA-fria proteinfragment, så finns det i regel inget DNA att granska. DNA-strängen är för övrigt ganska lång, samtidigt som den genetiska transkriptionen tar tid och kräver resurser. Vi behöver således ett annat sätt att definiera själv.

Langman och Cohn (2000a) säger att antigenseparationen initialt görs utifrån att ickesjälv-antigenerna inte är närvarande, eftersom ett embryo inte innehåller något ickesjälv. Själv-informationen förvärvas somatiskt och bevaras livet ut. Det skulle i så fall innebära att själv-definitionen byggs in i immunförsvaret under dess utveckling. För Langman och Cohn (2000) spelar det inte så stor roll hur själv definieras, huvudsaken är att definitionen innehåller en identifierbar distinktion gentemot ickesjälv. Enligt Chen (2001) säger den klassiska immunologin att själv definieras under individens utveckling genom att immunförsvaret rensar ut självreaktiva lymfocyter. Även Vander, Sherman, och Luciano (1998) liksom Dighiero och Rose (1999) förlägger en sådan process till fostertiden. Medzhitov och Janeway (2000), liksom Kruisbeek och Amsen (1996), samt Miller och Basten (1996), lyfter fram den negativa selektionen, där självreaktiva lymfocyter förstörs.

Kruisbeek och Amsen (1996) påpekar att den negativa selektionsprocessen inte är perfekt, eftersom långt ifrån alla självpeptider som T-cellerna kan möta under sin livstid presenteras för dem under utvecklingen. Även Alam och Gorska (2003) pekar på att självreaktiva T-celler klarar sig genom processen, bland annat för att de inte binder så starkt till självpeptider, vilket också stöds av Hanahan (1998), Grossman och Paul (2000), samt Miller och Basten (1996). Detta spelar dock ingen roll för självdefinitionens vara eller icke vara, det säger bara att den självdefinition som görs inte är perfekt, eller som Silverstein och Rose (2000) uttrycker det, inte tillräckligt finmaskig. Likväl bör den vara somatisk betingad eftersom antalet av alla möjliga komponenter som behöver

kännas igen är så stort, att en germlinebaserad eliminering av självförstörande element inte låter sig göras, för att anknyta till Langman och Cohn (2000a).

Ohashi och DeFranco (2002) betecknar det som att tymus står för en viktig initial mekanism, även om det inte är tillräckligt. Enligt Kruisbeek och Amsen (1996) underhålls toleransen med hjälp av perifer T-cellsförstörelse. Det spelar emellertid ingen roll om självdefinitionen görs i tymus eller om den görs perifert, huvudsaken är att det är immunförsvaret som på egen hand definierar vad som är själv och att det sker innan det dyker upp något ickesjälv.

Rose (1999) anser att även vuxna kan utveckla tolerans mot ett injicerat antigen, även om det är svårare när immunförsvaret har mognat. Det motsätter emellertid inte att en självdefinition faktiskt äger rum under fostertiden, det säger bara att det är möjligt att utveckla tolerans mot främmande antigen. Miller och Basten (1996) menar att det inte är något unikt med fostertiden. Det motsätter heller inte en självdefinition under fostertiden, det säger bara att samma regler gäller hela tiden, till exempel det som Kyewski, Derbinski, Gotter och Klein (2002) finner väl belagt, att omogna lymfocyter som möter antigen utvecklar självtolerans. Det borde vara rimligt att anta att lymfocyterna är omogna under fostertiden. Miller (2004) anser ju också att individens utvecklingsstadium har betydelse för självutvecklingen. Även Miller och Basten (1996) påtalar de omogna lymfocyternas betydelse.

Faktum är att immunförsvaret gör en självdefinition på egen hand i och med att självreaktiva lymfocyter förstörs genom negativ selektion. Förmodligen startade evolutionen med det förutbestämda naturliga immunförsvaret, där det adaptiva immunförsvaret med den somatiska omstruktureringsförmågan sedermera kompletterade konstruktionen och således gjorde immunförsvaret som helhet bättre anpassat för att hantera inkräktande. Självdefinitionen är toppen på utvecklingsstegen. Den har växt fram genom det naturliga urvalet, där de individer, vars immunförsvar saknade förmågan att på egen hand definiera vad som är själv, helt enkelt sållades bort. Det spelar således ingen roll att processen inte är perfekt när den plockas ur sitt sammanhang, huvudsaken är att den fyller sin funktion ur ett helhetsperspektiv.

Det borde således vara rimligt att tolka att immunförsvaret på egen hand definierar vad som är själv.

Analys av immunförsvarets förutsättningar för att kunna definiera vad som är själv

Flajnik och Kasahara (2001) säger att alla gener som definierar det adaptiva immunförsvaret går tillbaka till de äldsta ryggradsdjuren. Det säger ingenting om den somatiska urvalsprocessen, som Langman och Cohn (2000a) förklarar som ett urval av olika celler i organismen. Om definitionsmöjligheten skall vara förutbestämd, så måste också den somatiska urvalsförmågan vara förutbestämd. Även Benjamini, Sunshine och Leskowitz (1996) säger att immuniteten förvärvas. Tauber (2000) menar i och för sig att organismen

förändras inom genetiskt programmerade ramar, så då är frågan vilket somatiskt spelrum som finns i dessa ramar.

Silverstein och Rose (2000) konstaterar att skapandet av receptorer är genetiskt betingat, men att den patogenspecifika informationen inte är det. Enligt Schatz (2004) måste generna som kodar för antikroppar och T-cellsreceptorer somatiskt sättas samman under utvecklingen, så även om Livák och Petrie (2001) antyder att omstruktueringen är genetisk, så krävs det likväl en mekanism för det. Benjamini, Sunshine och Leskowitz (1996) tror att processen är slumpmässig, liksom Alam och Gorska (2003), samt Flajnik och Du Pasquier (2004). Om processen är slumpmässig, så är det funktionellt liktydigt med att ingen information behövs från omvärlden. Att slumpen triggas externt, gör ingen funktionell skillnad mot att slumpen triggas internt.

Schatz (2004) tolkar det dock som att omstruktureringsprocessen utförs av ett protein som kodas av en specifik gen. Det skulle betyda att omstruktureringsprocessen i så fall är förutbestämd. Det är ett rimligt antagande, eftersom slumpmässigheten likväl måste använda sig av någon mekanism, även om den inte är känd. Flajnik och Du Pasquier (2004) säger också att människans immunförsvar bland annat definieras av de gener som är inblandade i omstruktureringen.

Det som återstår är den negativa selektionen, där självreaktiva lymfocyter förstörs. Chen (2001) säger att den rådande inställningen är att tymus är ett universitet som utbildar T-cellerna att känna igen främmande antigen. Enligt Kruisbeek och Amsen (1996) triggas T-celler med självreaktiva receptorer att dö när de stimuleras i tymus. Eftersom vi tidigare antagit att det tidiga immunförsvaret endast har tillgång till självantigen, så blir följden att immunförsvaret rimligtvis har inbyggda förutsättningar för att kunna definiera vad som är själv. Det är en rimlig följd, eftersom detta inte kräver någon extern information för att definiera vad som är själv.

Enligt Guyton och Hall (2000) är det generna som kontrollerar de vardagliga funktionerna i kroppens alla celler. Samtidigt har vi tidigare fått exempel på att omogna lymfocyter förstörs när de möter antigen. Alberts et al (2002) säger att den genetiska informationen mest består i instruktioner för tillverkning av protein som upprätthåller cellernas funktionalitet. Det är troligt att denna funktionalitet även omfattar cellens egen destruktion. Det finns här alltså inget som tyder på att förmågan till självdefinition inte skulle vara genetiskt betingad.

Det borde således vara rimligt att anta att immunförsvaret har en förutbestämd förmåga att kunna definiera vad som är själv.

5.1.4 Analys av immunförsvaret ur störningsperspektivet

Enligt Grossman och Paul (2000) ger infektion sig tillkänna i form av en störning, där det karakteristiska är en snabb ökning av antigen-koncentrationen.

Det betyder att en icke-störning måste vara en långsammare eller obefintlig förändring och att det måste finnas något fördefinierat tröskelvärde som kontrolleras genom någon funktion. Detta antyds också av Langman och Cohn (2000a) som menar att det måste finnas någon fördefinierad lista för varje element som anger normal takt. Enligt Guyton och Hall (2000) är det generna som finns i kärnan i alla celler som kontrollerar de vardagliga funktionerna i kroppens alla celler. Med tanke på att Vander, Sherman och Luciano (1998) säger att immunförsvaret utgörs av de celler som kollektivt försvarar organismen, så borde det betyda att definitionen på ett eller annat sätt finns genetiskt förprogrammerad i immunförsvaret.

Tauber (2000) påpekar ju att nätverksperspektivet innebär ett självorienterande system, där beteenden definieras utifrån hur de stör systemet på basis av ett brustet jämviktstillstånd. Även om jämviktstillståndet är kollektivt betingat och därmed måste tolkas av cellerna gemensamt, så måste kommunikationen dem emellan likväl ske genom enskilda celler. Man skulle i och för sig kunna tänka sig någon slags dirigent, men för att återigen anknyta till Vander, Sherman och Luciano (1998): immunförsvaret utgörs av de celler som kollektivt försvarar organismen. Dirigerandet måste i slutändan ändå utföras på cellnivå. Enligt Alberts et al (2002) består geninformationen av instruktioner för tillverkning av protein som upprätthåller cellernas funktionalitet. Eftersom det är de enskilda cellerna som faktiskt stimuleras av antigen, så förefaller det alltså troligt att sådan funktionalitet även reglerar kommunikationen som styr jämviktstillståndet.

Det borde således vara rimligt att anta att immunförsvaret inte på egen hand kan definiera vad som inte skall betraktas som störande, eftersom det redan är definierat på förhand.

5.1.5 Analys av immunförsvaret ur skadeperspektivet

Cohen (2000) menar att immunförsvaret har att bedöma vävnadernas tillstånd och svara med korrigerande inflammation. Dembic (2000) säger att immunförsvaret reagerar på trasiga vävnader. I detta ligger implicit att det måste finnas någon definition av vad som inte är trasigt. Det trasiga förutsätter att det finns något som kan betraktas som helt. Cohen (2000) säger till exempel att autoimmunitet hjälper till att underhålla kroppen, där det handlar om att sätta in rätt behandling för ögonblicket. Att organisera insatserna efter vävnadernas behov. Frågan är då vad vävnaderna har för behov? Det kan ju knappast vara inlärda behov, för då skulle olika individer fungera på olika sätt. Hela den medicinska disciplinen bygger på att människor fungerar på samma sätt och därför måste vävnadernas behov rimligtvis vara förutbestämda.

Simon och Tatu (1988) anser att infekterade celler sänder ut extrasignaler, till skillnad från de normala cellerna, där frånvaron av dessa medstimulerande signaler vid igenkänning av antigen, leder till att lymfocyterna dör. Även Ohashi och DeFranco (2002), liksom Miller och Basten (1996), samt Rose (1999) pekar på betydelsen av de medstimulerande signalerna. Det förefaller

tydligen vara så, att detekteringen förutsätter att det normalt finns en avsaknad av vissa signaler.

Om immunförsvaret reagerar på extrasignaler från infekterade celler, så måste det finnas någon kodning för det i de mottagande cellerna. Miller (2004) säger att lymfocyter endast aktiveras om det samtidigt kommer en medstimulerande signal. Guyton och Hall (2000) säger att det är generna som finns i kärnan i alla celler som kontrollerar de vardagliga funktionerna i kroppens alla celler. Det är troligt att denna funktionalitet även omfattar hur lymfocyten skall reagera på den medstimulerande signalen. Eftersom immunförsvaret enligt Vander, Sherman och Luciano (1998) utgörs av de celler som kollektivt försvarar organismen, så borde det betyda att definitionen finns genetiskt förprogrammerad i immunförsvaret.

Det borde således vara rimligt att anta att immunförsvaret inte på egen hand kan definiera vad som inte skall betraktas som skada, eftersom det redan är definierat på förhand.

5.2 Analys av Sophos-data

Information om virusexemplar har hämtats från Sophos virus analyses (Sophos, 2004a).

För de frågor som det visat sig finnas belägg för i respektive exemplarbeskrivning, har citat hämtats från beskrivningen som visar på stödet. Citaten har hämtats under flikarna *Advanced* eller *Description* på respektive exemplars sida.

Under F7, så tolkas uttryck som “run” och ”execute” som att det rör sig om ett exemplar som utför operationer i ett datorsystem, eftersom detta är vedertagna begrepp när det gäller att exekvera programkod.

Under F9, så tolkas uttryck som “allowing unauthorized access”, ”terminate anti-virus applications” och ”exploiting vulnerabilities” som att det rör sig om operationer som användaren inte haft för avsikt att införa i systemet. Det är rimligt att tolka dessa uttryck på det viset, eftersom det är orimligt att anta att de flesta användare skulle ha för avsikt att utföra sådana operationer i systemet.

Under F10, så tolkas uttryck som ”spread” eller ”copy itself to”, i de fall det sker genom någon typ av nätverk, som att exemplaret inte härstammar från datorsystemet. Här finns naturligtvis möjligheten att exemplaret kan härstamma från enskilda system, men då måste det likväl definitionsmässigt finnas oinfekterade system att sprida sig till. Det är rimligt att anta att ett exemplar inte begränsar sin spridning till det system som det härstammar från och att ett exemplar i regel inte härstammar från det system som infekteras.

Ett streck (–) i en tabellcell betyder att frågeställningen inte har kunnat bekräftas utifrån den information som funnits tillgänglig i virusbeskrivningen.

Tabell 3 *Analys av Sophos-data (tabellen sträcker sig över flera sidor)*

Exemplar	**F7. Utför detta exemplar operationer som exekveras i ett datorsystem?**	**F9. Utför detta exemplar operationer som användaren inte haft för avsikt att införa i systemet?**	**F10. Exekveras detta exemplar i datorsystem som det inte härstammar från?**
W32/Randon-AI	–	”W32/Randon-AI also allows unauthorised remote access to the computer via IRC channels”	” W32/Randon-AI is a multi-component network worm which attempts to spread by copying components of itself over the network via poorly protected network shares”
W32/Rbot-BB	”In order to run automatically when Windows starts up the worm copies itself to the file video_32sD.exe”	–	–
W32/Rbot-CZ	”while running in the background as a service process”	”It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer”	”W32/Rbot-CZ is a worm which attempts to spread to remote network shares”
W32/Rbot-EY	”while running in the background as a service process”	”also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer”	”W32/Rbot-EY is a worm which attempts to spread to remote network shares”
W32/Rbot-GQ	”Once installed, W32/Rbot-GQ connects to a preconfigured IRC server and channel to await further commands”	”In order to avoid detection, W32/Rbot-GQ terminates processes”	”The worm attempts to spread to unpatched machines”
W32/Rbot-IM	”creates the following registry entries so as to run itself on system startup”	–	”W32/Rbot-IM spreads to network shares”

Exemplar	F7	F9	F10
W32/Rbot-KK	”When run W32/Rbot-KK copies itself to the Windows system folder as WINIUPDATES.EXE”	–	”The worm spreads by exploiting the Lsass, DCOM-RPC and IIS5SSL vulnerabilities”
W32/Rbot-MF	”The worm creates entries in the registry at the following locations in order to run itself on system startup”	”It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer”	”W32/Rbot-MF is a worm which attempts to spread to remote network shares”
W32/Rbot-OD	”When run the worm attempts to contact a remote IRC server and join a specific channel to listen for commands”	”W32/Rbot-OD also has a backdoor component that allows a malicious user remote access to an infected computer”	”W32/Rbot-OD is a member of the W32/Rbot family of worms with a backdoor component that spread on weakly protected network shares on the Windows platform”
W32/Rbot-QE	”W32/Rbot-QE then creates the following registry entries so as to run itself either on user logon or computer restart”	”The worm contains backdoor functions that allows unauthorised remote access to the infected computer”	”W32/Rbot-QE spreads to network shares with weak passwords and by using the LSASS security exploit”
W32/Ronoper-Fam	–	”have a backdoor component which allows unauthorised remote access to the computer over a network´”	”W32/Ronoper-Fam is a family of worms which spread by emailing themselves via MAPI, by copying themselves to network shares, via peer-to-peer file-sharing networks such as KaZaA and via IRC networks”
W32/SdBot-BQ	”creates entries in the registry at the following locations to run itself on system startup”	”It also contains backdoor Trojan functionality allowing unauthorised remote access to the infected computer”	”W32/Rbot-C spreads to network shares with weak passwords”
W32/SdBot-FQ	”W32/SdBot-FQ attempts to run as a service process”	–	”W32/SdBot-FQ scans networks for shares protected by weak passwords and attempts to copy itself over to those shares”

Exemplar	F7	F9	F10
W32/SdBot-IM	”W32/SdBot-IM is an IRC backdoor Trojan and network worm which can run in the background as a service process”	”and allow unauthorised remote access to a remote intruder via the IRC channel”	”the worm will begin scanning the internet for network shares with weak administrator passwords and will attempt to copy itself to these shares”
W32/Sdbot-KO	”In order to run automatically when Windows starts up”	–	–
W32/SdBot-MY	”When first run the worm creates a copy of itself named MSIExxx.exe in the Windows system folder”	–	”W32/SdBot-MY is a worm which spreads via network shares ... with weak passwords and copies itself to the Windows system folder of a vulnerable computer”
W32/Sdbot-OZ	”creates the following registry entries to ensure it is run at system logon”	”It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer”	”W32/Sdbot-OZ is a worm which attempts to spread to remote network shares with weak passwords”
W32/Sdbot-RG	–	–	–
W32/Sober-D	”When first run W32/Sober-D will display a message”	–	”W32/Sober-D is a worm that arrives in an email”
W32/Spybot-BX	” W32/Spybot-BX remains resident, running in the background as a service process”	–	”W32/Spybot-BX also attempts to copy itself to the startup folder of attached network drives”
W32/SdBot-DC	”W32/SdBot-DC attempts to run as a service process”	–	”W32/SdBot-DC scans networks for shares protected by weak passwords and attempts to copy itself over to those shares”
W32/Torvil-C	–	–	–

Exemplar	F7	F9	F10
W32/Wukill-B	”The worm copies itself to the Windows folder as MSTRAY.EXE and creates the following registry entry so that MSTRAY.EXE is run automatically each time Windows is started”	–	”W32/Wukill-B is an internet worm which can email itself to contacts found in the Microsoft Outlook address book”
W32/Agobot-4	”Each time W32/Agobot-4 is run it attempts to connect to a remote IRC server”	”W32/Agobot-4 is a network worm which also allows unauthorised remote access to the computer via IRC channels”	”W32/Agobot-4 copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities”
W32/Agobot-BX	”These vulnerabilities allow the worm to execute its code on target computers with System level privileges”	”W32/Agobot-BX is a network worm which also allows unauthorised remote access to the computer via IRC channels”	”W32/Agobot-BX copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities”
W32/Agobot-ED	”creates entries in the registry at the following locations to run itself on system restart”	”W32/Agobot-ED is a network worm which also allows unauthorised remote access to the computer via IRC channels”	”W32/Agobot-ED tries to copy itself to network shares with weak passwords”
W32/Agobot-GB	”This worm moves itself into the Windows System32 folder under the filename CSSRS.EXE and may create the following registry entries so that it can execute automatically on system restart”	” W32/Agobot-GB will attempt to terminate anti-virus and software firewall processes”	”W32/Agobot-GB will search for shared folders on the Internet with weak passwords and copy itself into them”
W32/Agobot-HY	”In order to run automatically when Windows starts up W32/Agobot-HY creates the following registry entries”	”W32/Agobot-HY allows a malicious user remote access to an infected computer”	–
W32/Agobot-JW	”When first run the worm copies itself to neroasm.exe in the Windows system folder”	”terminates a large number of anti-virus and security related processes”	”W32/Agobot-JW is a worm which spreads to networks shares with weak passwords”

Exemplar	F7	F9	F10
W32/Agobot-LT	”In order to run automatically when Windows starts up W32/Agobot-LT creates the following registry entries”	”W32/Agobot-LT may attempt to terminate anti-virus and firewall related processes, in addition to other viruses, worms or Trojans”	–
W32/Agobot-NS	”creates entries at the following locations in the registry with the value "WSAConfiguration" so as to run itself on system startup”	”W32/Agobot-NS also attempts to terminate a large number of processes, many of which relate to security and anti-virus software”	”W32/Agobot-NS is capable of spreading to network shares with weak passwords and via network security exploits as a result of the backdoor Trojan element”
W32/Agobot-Y	”creates entries at the following locations in the registry with the value "WSAConfiguration" so as to run itself on system startup”	”W32/Agobot-NS also attempts to terminate a large number of processes, many of which relate to security and anti-virus software”	”W32/Agobot-NS is capable of spreading to network shares with weak passwords and via network security exploits as a result of the backdoor Trojan element”
W32/Aplore-A	”When run, the worm drops and runs the VBScript email.vbs which attempts to send an email with the worm files attached to all contacts from the Outlook address book”	–	”W32/Aplore-A is a Win32 worm which uses Microsoft Outlook to spread”
W32/Bagle-C	”When run the worm opens NOTEPAD.EXE, copies itself to the Windows system folder as README.EXE and creates the following files in the same folder”	–	”W32/Bagle-C is an email worm which sends itself via its own SMTP engine to addresses harvested from your hard disk”
W32/Blebla-A	”This means that the worm is run everytime BMP, DOC, EXE, JPG, MP3, XLS or ZIP files are opened”	–	”W32/Blebla-A is an internet worm which spreads via SMTP”

Exemplar	F7	F9	F10
W32/Catfat-A	”that points to the latter file so that the worm is automatically run at each system start”	”W32/Catfat-A also tries to terminate various anti-virus and computer security related applications and to modify the file Autoexec.bat to delete vital system files”	”W32/Catfat-A is a worm which spreads by sending itself as an email attachment”
W32/Darby-N	”When the worm is first run it may display the following fake error message in English or Spanish”	–	”W32/Darby-N also attempts to spread via email using addresses harvested from the infected computer”
W32/Dumaru-K	”This Trojan is then executed which drops and runs the DLL file rwtrisfg32.dll”	”W32/Dumaru-K will periodically send an email to an attacker containing information about the victim's computer”	”W32/Dumaru-K arrives in an email with the following characteristics”
W32/Flechal-B	–	–	–
W32/Forbot-BQ	”In order to run automatically each time Windows is started, W32/Forbot-BQ sets the following registry entries”	” W32/Forbot-BQ spreads through network shares and by exploiting the LSASS (MS04-011) software vulnerability”	”W32/Forbot-BQ spreads through network shares and by exploiting the LSASS (MS04-011) software vulnerability”
W32/Forbot-U	”W32/Forbot-U copies itself to the Windows system folder as WindowsSec.EXE and creates entries in the registry at the following locations so as to run itself on system startup”	”It also contains backdoor Trojan functionality, allowing unauthorised remote access to the infected computer via IRC channels while running in the background as a service process”	”W32/Forbot-U is a worm which attempts to spread to remote network shares”
W32/Gibe-F	” The worm also changes the entries in the registry … so that it is run before EXE, COM, PIF, BAT, SCR files”	” W32/Gibe-F may attempt to exploit a vulnerability in Microsoft's software which allows automatic execution of attachments while viewing an email message”	”W32/Gibe-F is a worm which spreads by emailing itself via its own SMTP engine to addresses extracted from various sources”

Exemplar	F7	F9	F10
W32/Holar-B	”creates the following registry entries so that the worm executable is run automatically each time Windows is started”	”The worm attempts to exploit a MIME vulnerability in some versions”	”W32/Holar-B is a worm which spreads by copying itself to shares on the local network and by emailing itself to contacts from the Microsoft Outlook and Messenger address books”
W32/Kifie-D	”In order to be executed automatically on system startup the worm copies itself”	”attempts to delete various anti-virus related files”	”W32/Kifie-D spreads via email, P2P, IRC, AIM and local drives”
W32/Kwbot-H	”It may then create the registry entry … so that the copy is run each time Windows is started”	”The worm may also allow attackers to gain control of an infected machine”	”The worm will attempt to get unsuspecting users to download copies of itself”
W32/Lovgate-R	–	”W32/Lovgate-R is also a backdoor Trojan that provides an attacker with unauthorized access to the user's computer”	”The worm spreads across the local network by copying itself into shared folders”
W32/Mimail-K	”In order to run itself automatically when Windows starts up the worm copies itself”	-	”W32/Mimail-K is a worm which spreads via email using addresses harvested from the hard drive of the infected computer”
W32/MyDoom-Gen	–	–	–
W32/Nahata-D	–	–	”W32/Nahata-D is an intended worm that tries to spread via email, mIRC and pIRC”
W32/Niklas-K	”When first run, the worm copies itself to the Windows folder”	”W32/Niklas-K attempts to terminate selected anti-virus and security-related applications”	”W32/Niklas-K attempts to spread by infecting executables within common shared folders”

Exemplar	F7	F9	F10
W32/Oror-B	”W32/Oror-B sometimes adds additional values to the registry to run one or more of the files it has placed in your Program Files folders”	”W32/Oror-B may send its attachments so that they attempt to exploit vulnerabilities in some versions of Microsoft Outlook, Microsoft Outlook Express, and Internet Explorer”	”W32/Oror-B is a worm that can spread in an number of ways, including sending itself out by email, copying itself to shared drives in networks, and placing copies of itself in folders likely to be shared via the KaZaA peer-to-peer system”
W32/Protoride-C	”and then set the following registry entry to point to this file so that it is run before all EXE files”	”The worm also has a backdoor component that allows unauthorised remote access to the computer via IRC channels”	”W32/Protoride-C is a Windows worm that spreads via network shares”
W32/Randon-AA	”One component of the worm, MSMOUSE.EXE, then attempts to download and execute a copy of the worm from a remote URL as a file called WINZXP.EXE”	–	”W32/Randon-AA is a multi-component network worm which attempts to spread by copying components of itself to, and executing them on, remote ADMIN$ and IPC$ shares with weak passwords”
Summa	**45 (85%)**	**32 (60%)**	**45 (85%)**

5.3 Analys av Microsoft-data

Bulletininformation har hämtats från Microsoft Security Bulletin (Microsoft, 2004).

För de frågor som det visat sig finnas belägg för i respektive bulletin, har citat hämtats från bulletinen som pekar på belägget. Citaten har i regel hämtats under ”Frequently Asked Questions”, men har i vissa fall hämtas från ”Vulnerability Details” eller relaterade underlänkar.

Vissa bulletiner refererar till *buffer overrun*, vilket generellt förklaras som

> ”An attack in which a malicious user exploits an unchecked buffer in a program and overwrites the program code with

> their own data. If the program code is overwritten with new executable code, the effect is to change the program's operation as dictated by the attacker.” (Microsoft, 2004a)

Detta stöder både F12 och F13. Dock har mer bulletin-specifik information sökts i första hand där den förekommer.

Under F12, så tolkas uttryck som ”malicious user” och ”attacker” som att det rör sig om ett inkräktande av systemet. Om analysen också kommer fram till att det handlar om att en applikation kan installeras, så kommer applikationen följaktligen att betraktas som en inkräktande applikation.

Under F13, så tolkas en aktivitet i samband med begrepp som ”vulnerability” och ”attacker” som att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt, eftersom det antyder någon form av utnyttjande av systemet som en användare inte förväntar sig.

Under F14 används Microsofts rekommendationer rakt av. Oavsett om de är kritiska eller endast riktar sig till minoritetsgrupper, så är de likväl rekommendationer.

Tabell 4 *Analys av Microsoft-data (tabellen sträcker sig över flera sidor)*

Bulletin	**F12. Anger bulletinen att en inkräktande applikation kan installeras efter att datorsystemet tagits i bruk av användaren?**	**F13. Anger bulletinen att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt?**	**F14. Rekommenderar bulletinen att operativsystemet måste uppdateras?**
MS02-018	”the attack could overwrite program code on the server with new program code, in essence modifying the functionality of the server software”	”the attack could overwrite program code on the server with new program code, in essence modifying the functionality of the server software”	“Customers using any of the affected products should install the patch immediately”
MS01-003	“An attacker could write a program that could gain control of the mutex and deny access to it.”	“The machine would stop communicating with other machines on the network”	“Consider installing this patch on all Windows NT 4.0 terminal servers, and on any Windows NT 4.0 servers on which unprivileged users are granted interactive logon rights.”

Bulletin	F12	F13	F14
MS01-001	"A malicious user could create an HTML formatted document or e-mail message, that when viewed by the recipient, would automatically request a session to the malicious user's server."	"the malicious user could capture the unsuspecting user's authentication credentials"	"Customers with an affected version of the products listed should consider installing this patch. "
MS99-038	–	"The vulnerability could allow an attacker to perform source routing via a Windows 95, 98 or Windows NT machine even if the administrator had configured the system to prevent it."	"The patch only needs to be applied to multi-homed Windows 95, 98 or Windows NT machines that are used as routers."
MS99-056	–	–	–
MS01-015	"This vulnerability could enable an attacker to cause code of his choice to execute on the system of a user who either visited the attacker's web site or opened an HTML e-mail from him"	–	"Customers should apply the patches for IE and Windows Script Host below, and apply the Telnet invocation patch only if using Services for Unix 2.0"
MS02-048	"The attacker would need to build a web page that, when opened, invokes the Certificate Enrollment Control in exactly the right way to identify and delete the certificates"	"an attacker could potentially delete digital certificates on a user's system, thereby preventing the user from having access to certain functions"	"Customers should install the patch immediately"
MS00-053	"could allow a malicious user to execute arbitrary code in the security context of a specific service"	"A malicious user could could gain additional privileges on the local machine. For instance, he or she could add himself or herself to the local Administrators group, after which point they could take any desired action on the machine."	–
MS04-018	–	"An attacker who successfully exploited this vulnerability could cause Outlook Express to fail unexpectedly"	"Customers should consider applying the security update"

Bulletin	F12	F13	F14
MS03-051	"An attacker who successfully exploited this vulnerability could cause code of their choice to be executed as though it originated on the local machine"	"An attacker who successfully exploited this vulnerability could cause a server running Front Page Server Extensions to temporarily stop responding to requests"	"Customers should install the security update immediately"
MS00-052	This vulnerability would enable a malicious user to substitute code of his choice for the normal Windows desktop on machines that he can interactively log onto.	"the code might be able to cause significant harm"	"Microsoft recommends that customers consider installing the patch on any machine that allows normal users to log on interactively"
MS04-003	"This is a buffer overrun vulnerability"	"If an attacker were able to successfully exploit this vulnerability, it could allow them to gain control over the system"	Customers should install this security update at their earliest opportunity.
MS00-058	–	"If such a web file were sent directly to a browser, it could compromise any sensitive information it contained"	–
MS02-051	–	"This vulnerability could enable an attacker to read the contents of an encrypted RDP session, thereby compromising any data within it"	"Administrators of Windows 2000 terminal servers and Windows XP users who have enabled Remote Desktop should apply the patch"
MS00-059	–	"The applet could visit sites on the intranet that are normally beyond the reach of the malicious user, set up a web session, and forward the content to the malicious user's site"	–

Bulletin	F12	F13	F14
MS04-014	"A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution on an affected system."	"An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges"	"Customers should install the update at the earliest opportunity"
MS99-008	"The risk is that a malicious user could develop a screen saver program that, for example, uses the elevated privileges to add the author to the Administrators group"	"The risk is that a malicious user could develop a screen saver program that, for example, uses the elevated privileges to add the author to the Administrators group"	"Microsoft highly recommends that customers evaluate the degree of risk that this vulnerability poses to their systems and determine whether to download and install the patch"
MS00-046	"the e-mail could create an HTML file on the local computer, outside of the cache ... running in the Local Computer Zone but under the control of the malicious user's HTML e-mail"	"This vulnerability could allow a malicious user to send an email to another user which, if opened, would allow the malicious user to read files on the recipient's computer"	"If none of the above apply to you, you should install the patch"
MS99-024	"if a server allowed normal users to log on interactively and run arbitrary programs, a malicious user could disable the machine's keyboard and mouse"	"The vulnerability could allow denial of service attacks against a Windows NT machine by enabling a malicious user to disable the mouse and keyboard"	"Microsoft recommends that customers assess the risk that this vulnerability poses to their safe computing and determine whether or not to apply the patch"
MS01-013	"the buffer could be overrun, which could in the worst case potentially enable code of another user's choice to be run on the machine"	"the code could do virtually anything on the machine"	System administrators should install patch on all critical servers and consider installing it on all Windows 2000 systems.
MS01-059	"This a buffer overrun vulnerability"	"An attacker who successfully exploited this vulnerability could gain complete control over an affected system."	"Microsoft strongly urges all Windows XP customers to apply the patch immediately"

Bulletin	F12	F13	F14
MS00-093	"This vulnerability could enable a malicious web site operator to take unauthorized action on the computer of a visiting user, by giving her the ability to run, on the user's computer, ActiveX controls that are normally off limits to web sites"	"This would enable the malicious user to take a broad range of actions on the user's computer, including adding, changing or deleting files, exchanging files with a web site, and others"	–
MS98-009	"Using this program, the non-administrative user is able to run arbitrary code in the system security context and thereby grant himself or herself local administrative privileges on the local system"	"This exploit can potentially allow a non-administrative user to gain local administrative access to the system and thereby elevate his or her privileges on the system"	"Microsoft highly recommends that customers using Windows NT operating systems immediately apply the appropriate hot fixes to their systems"
MS03-030	"An attacker who successfully exploited the vulnerability could, in the worst case, run code of his or her choice on a user's system"	"An attacker who successfully exploited the vulnerability could, in the worst case, run code of his or her choice on a user's system"	"Customers should apply the security patch immediately"
MS00-069	"A malicious user who could access the logon screen on an affected system could use this functionality to run code of his choice"	"could enable a malicious user to gain full control of a Windows 2000 system without needing to log on"	"Microsoft strongly recommends that all customers using the Simplified Chinese version of Windows 2000 install the patch on their system."
MS03-041	"the attacker could execute arbitrary code in the context of the logged on user"	"This could allow an attacker to take any action on a user's system in the security context of the currently logged in user"	"Customers should apply the patch immediately"
MS03-023	"This vulnerability could enable an attacker to cause Internet Explorer to fail in such a way that it could execute code of the attacker's choice"	"This could allow an attacker to take any action on a user's system in the security context of the currently logged in user"	"Systems administrators should apply the patch immediately"
MS04-038	"A remote code execution vulnerability exists in Internet Explorer that could allow remote code execution on an affected system"	"An attacker who successfully exploited this vulnerability could take complete control of an affected system"	"Customers should install the update immediately"

Bulletin	F12	F13	F14
MS00-091	–	“a malicious user could use the vulnerability to temporarily cause the networking services on an affected machine to stop responding to client requests during an attack”	“Microsoft recommends that anyone running Windows NT 4.0 should install this patch”
MS03-033	“This could also include reformatting the hard disk or running programs of the attacker's choice on it”	“if the application runs under the local system context, the attacker would have the same level of permissions. This could include creating, modifying, or deleting data on the system, or reconfiguring it the system”	“Users should apply the security patch to affected systems”
MS03-043	“An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system”	“The attacker could then be able to take any action on the system, including installing programs, viewing, changing or deleting data, or creating new accounts with full privileges”	“Customers should disable the Messenger Service immediately and evaluate their need to deploy the patch”
MS02-070	“exploiting the vulnerability could enable an attacker to change security policy information ... thereby gaining the ability to take actions such as installing and running programs on the system”	“group policy can be used to change permissions on folders and files, download and run programs at system startup, and take other actions”	“Administrators whose Windows 2000 or Windows XP systems that are configured to use SMB Signing should install the patch immediately”
MS00-074	–	”A malicious user could use the vulnerability to crash either the operating system or the WebTV for Windows application”	”Microsoft recommends that users who have installed WebTV for Windows consider installing the patch”

Bulletin	F12	F13	F14
MS00-054	–	”A malicious user could use this vulnerability to cause an affected machine to fail”	”Microsoft recommends that customers who have IPX enabled and are using an affected system in a corporate LAN setting or accessing the Internet via DSL or cable modem consider installing the patch”
MS00-055	”If a malicious web site operator successfully introduced script into a file whose location on the user's disk were known, he could use the Scriptlet control to execute the script in the Local Computer Zone”	”The effect of each vulnerability is the same - either could allow a malicious web site operator to view files on the computer of visiting user”	–
MS00-067	”A malicious user could create an HTML formatted document or e-mail message, that when viewed by the recipient, would automatically request a telnet session to the malicious user's server”	”This vulnerability could enable a malicious user to automatically request a Telnet session from an unsuspecting user's machine to the malicious user's server”	”Microsoft recommends that all Windows 2000 users consider installing the patch”
MS01-058	”This vulnerability could enable an attacker to potentially run a program of her choice on the machine of another user”	”Such a program would be capable of taking any action that the user himself could take on his machine, including adding, changing or deleting data, communicating with web sites, or reformatting the hard drive”	”Customers using IE should install the patch immediately”
MS00-023	–	”If a malicious user requested a file from a web server via a specially-malformed URL, the server could become unresponsive for some period of time”	–

Bulletin	F12	F13	F14
MS02-023	”An attacker who was able to successfully exploit this vulnerability could cause HTML scripts to execute as if they were run locally on the user's system”	”This has the effect of allowing the attacker's script to run as if the user had chosen to run it herself”	”Consumers using the affected versions of IE should install the patch immediately”
MS00-049	”This vulnerability would allow a malicious user to host an Access file on his web site and cause it to open on the computer of any user who visited the site. Once this happened, any code in the Access file, such as macro code or VBA code, would be free to run on the visitor's computer.”	”This vulnerability would allow a malicious user to host an Access file on his web site and cause it to open on the computer of any user who visited the site. Once this happened, any code in the Access file, such as macro code or VBA code, would be free to run on the visitor's computer.”	”Microsoft recommends all users of the affected versions of Internet Explorer install this patch”
MS01-029	”It could enable an attacker to run a program of her choice on the machine of another user”	”The program would be capable of taking any action on the user's machine that the user himself was capable of taking, including adding, creating or deleting files, communicating with web sites, or reformatting the hard drive”	”Windows Media 6.4 customers should install the patch immediately”
MS01-055	–	”A malicious web site with a malformed URL could read or potentially alter the contents of a user's cookies, which might contain personal information”	”Customers running Internet Explorer 5.5 or 6.0 should apply the patch”
MS00-063	–	”It could enable a malicious user to cause the IIS service on an affected web server to fail, thereby preventing the server from servicing requests for service”	”Microsoft recommends that customers using an affected version of IIS install the patch”

Bulletin	F12	F13	F14
MS03-010	–	”An attacker who successfully exploited this vulnerability could cause a remote computer to fail”	”Customers should install the patch at the earliest opportunity”
MS02-029	”By overrunning the buffer with carefully selected data, it would be possible for the attacker to run code in the context of the LocalSystem account, that is, as the operating system itself”	”An attacker who successfully exploited this vulnerability could gain complete control over the machine”	”Administrators should apply the patch to immediately to machines that allow unprivileged users to log onto them interactively”
MS02-012	–	”By sending a specially malformed request to an affected system, an attacker could temporarily prevent it from providing mail services”	”Customers who need the Windows 2000 SMTP services should apply the patch”
MS00-044	–	”A malicious user could exploit this vulnerability to prevent an IIS server from providing useful service”	”Microsoft recommends that, as a first choice, customers disable the HTR functionality altogether; only customers who have a compelling reason to retain the HTR functionality should retain the functionality and apply this patch”
MS00-039	–	”It could help make it possible for a malicious web site to pose as a different web site - one that the user trusts”	–
MS98-017	–	”An attacker could exploit this problem to create a denial of service condition ... which may result in the system hanging”	”Microsoft recommends that customers evaluate the risk that this vulnerability poses to their systems and apply the patch if appropriate”
MS00-045	”Specifically, the vulnerability could allow a script running in a browser window to have access to any e-mail that the user read via the preview pane”	”This vulnerability could allow a malicious user under very specific conditions to view, but not change, the contents of e-mails as the owner previews them”	–
Summa	**33 (66%)**	**48 (96%)**	**41 (82%)**

5.4 Analys av forskningen om artificiella immunsystem

Vi vill här ha svar på följande frågor:

F15. Har det artificiella immunsystemet en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande?

F16. Definierar det artificiella immunsystemet själv vad som inte är inkräktande?

F17. Bygger det artificiella immunsystemets detektion av inkräktande på att det finns en fördefinierad definition av vad som inte är inkräktande?

Detta är förutsättningar för ett självständigt artificiellt immunsystem och om dessa frågor inte kan besvaras jakande för en angiven princip, så är den inte tillämplig.

5.4.1 Analys av principen med systemanrop i operativa processer

Forrest, Hofmeyr och Somayaji (1996) använder systemanrop i operativa processer som motsvarighet till antigen. Dessa håller sig stabila under normala omständigheter. När attacker förekommer uppstår turbulens. Initialt byggs en databas upp med normalt beteende. Därefter samlas data in om rådande beteende, som matchas mot databasen.

Nu är frågan om det artificiella immunsystemet har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande. Det spelar egentligen ingen roll hur data om det normala beteendet samlas in. Man kan till exempel köra systemet under en inkörningsperiod, för att på så sätt låta systemet lära sig vad som är normalt beteende. Eller också kan man uttryckligen specificera det normala beteendet, vilket blir svårt med tanke på att det normala beteendet enligt Forrest, Hofmeyr och Somayaji (1996) hela tiden skiftar. Oavsett vilket tillvägagångssätt som används för att definiera det normala beteendet, så kvarstår problemet med vad som faktiskt är normalt beteende. Här finns två aspekter. Den första är att det faktiskt är användaren och inte datorsystemet som bestämmer vad som är normalt beteende. Datorsystemet har ingen möjlighet att veta vad som är normalt beteende, så länge ingen har talat om för datorsystemet vad som är normalt beteende. Hur man än vrider och vänder, så kommer definitionen att ske utanför datorsystemet.

Den andra aspekten är att användaren inte kan försäkra sig om att beteendet är normalt. Poängen med ett immunsystem är att skydda sig mot inkräktande. Hur kan man garantera att inkörningen av systemet är fritt från inkräktande? Det förutsätter att man isolerar sig från omvärlden. Att isolera sig från omvärlden ger en garanti mot inkräktande. Men det är inte normalt beteende att vara isolerad från omvärlden. Det blir därför i princip omöjligt att överhuvud taget definiera något normalt beteende.

Utifrån detta är det rimligt att anta att principen med systemanrop i operativa processer inte är relevant för ett självständigt artificiellt immunsystem.

5.4.2 Analys av principen med lockbeten

Marmelstein, Van Veldhuizen och Lamont (1998) använder en lockbetesprincip, där overksamma program används som indikatorer på att systemet är infekterat. Programmen genereras utifrån en genetisk algoritm och utformas så att de blir speciellt attraktiva för virus. Sålunda produceras en evolutionsinfluerad population som sprids i systemet. Skulle ett sådant lockbetesprogram ändras, så är det ett tecken på att det infekterats av ett virus.

Nu är frågan om det artificiella immunsystemets detektion av inkräktande bygger på att det finns en fördefinierad definition av vad som inte är inkräktande. Eftersom systemet själv måste göra denna definition, så måste den således göras initialt, innan någon detektering kan äga rum. Helt klart genereras en uppsättning lockbeten, problemet är bara att det inte är systemet som definierar vad som inte är inkräktande – det är redan gjort på förhand. För att definitionen skall göras av systemet, så krävs det någon process där systemet på egen hand gör någon slags uppdelning i element som relaterar till inkräktande och element som relaterar till icke inkräktande. Eftersom samtliga element som nu genereras relaterar till inkräktande, så finns ingen uppdelning att göra.

Visserligen kan man tycka att det inte fyller någon funktion att generera lockbeten som relaterar till icke inkräktande, om dessa ändå skall sorteras bort. Visst, det är meningslöst och detta beror på att definitionen att lockbeten relaterar till inkräktande är gjord utanför systemet. Någon har helt enkelt bestämt att applikationer som infekterar lockbeten skall betraktas som inkräktande. Det betyder i så fall att applikationer som infekterar andra filer än lockbeten inte skall betraktas som inkräktande. Man kan i och för sig hävda att applikationer som infekterar andra filer än lockbeten likväl kan vara inkräktande, men då görs ju ingen definition av icke inkräktande över huvud taget.

Problemet är dock inte att lockbeten är passiva filer som bara ligger och väntar på att någon skall infektera dem. Lee, Kim och Hong (2004) säger till exempel att det inte finns något som garanterar att virus faktiskt attackerar ett lockbete. Man skulle istället kunna tänka sig att man hade aktiva program som regelbundet sökte igenom olika applikationer i systemet för att se om de hade

infekterats. Frågan är då bara hur legitima ändringar skall kunna genomföras, till exempel uppdateringar eller installation av nya program. Detta kräver att användaren uttryckligen bekräftar varje legitim ändring av systemet, vilket medför att definitionen av vad som inte är inkräktande görs utanför systemet.

Utifrån detta är det rimligt att anta att principen med lockbeten inte är relevant för ett självständigt artificiellt immunsystem.

5.4.3 Analys av principen med nätverksdetektorer

Dozier, Brown, Hurley och Cain (2004) pekar på ett typiskt upplägg för intrångsdetektering, där nätverkstrafik klassificeras som själv och ickesjälv. En population av detektorer genereras och utsätts för normal nätverkstrafik, där de detektorer som matchar något datapaket plockas bort. Därmed erhåller man en uppsättning detektorer som reagerar på onormal nätverkstrafik.

Dozier, Brown, Hurley och Cain (2004) säger att nackdelen med detta är att det inte går att veta vad det är för typ av attacker som undgår upptäckt. Detta borde i så fall också gälla det biologiska immunförsvaret, men även om vi här förefaller ha ett system som faktiskt på egen hand gör en definition av icke inkräktande, så görs likväl definitionen utanför systemet, nämligen i form av den normala nätverkstrafiken. Systemet kan inte veta vad som är normal nätverkstrafik, det kan bara administratören avgöra genom att definiera vad som skall räknas som normal nätverkstrafik. Men administratören kan likväl inte veta att den normala närverkstrafiken är fri från inkräktande, eftersom detta kräver att man isolerar sig från omvärlden, vilket i sin tur är onormalt.

Dozier, Brown, Hurley och Cain (2004) kör dessutom med dubbel stimulering, där administratören måste bekräfta att det rör sig om en regelrätt attack, vilket definitivt förlägger detekteringen utanför systemet. Även Foukia, Hassas, Fenet och Albuquerque (2003) behöver en administratör för att sätta toleransnivån för deras intrångsdetekteringsagenter.

Utifrån detta är det rimligt att anta att principen med nätverksdetektorer inte är relevant för ett självständigt artificiellt immunsystem.

5.4.4 Analys av principen med självreplikering

Lee, Kim och Hong (2004) använder självreplikering som indikator på inkräktande. Initialt betraktas alla existerande program som legitima. Bitmönster extraheras från inkommande eller ändrade program, där systemet sedan undersöker om detta bitmönster även återfinns i andra program. Detta med tanke på att virus har en tendens att smitta andra program.

Nu är frågan om detekteringen bygger på en fördefinierad definition av vad som inte är inkräktande. Enda möjliga definitionen är att systemet betraktar alla

existerande program som legitima. Om ett nytt program kommer till systemet, som systemet betraktar som legitimt, så skulle man faktiskt kunna säga att det är systemet som definierar. Problemet är bara att detektionen inte bygger på denna definition. Detektionen bygger istället på att inkräktande likställs med självreplikering, vilket är en definition som är gjord utanför systemet, nämligen av utvecklaren av systemet.

Skormin, Summerville och Moronski (2003) säger att självreplikering är en förutsättning för att merparten av datorvirus och maskar skall spridas. Även om det är ovanligt för legitim kod, så är det likväl en detektionsprincip som är förutbestämd och som inte är definierad inom systemet. Det spelar ingen roll om konceptet skulle visa sig väldigt effektivt – ett artificiellt immunsystem med människan som förebild kräver att definitionen av vad som inte är inkräktande görs inom systemet. Som en parantes kan nämnas att människans immunförsvar inte kan använda självreplikering som detektionsprincip, eftersom både själv- och ickesjälv-element förökar sig.

Utifrån detta är det rimligt att anta att principen med självreplikering inte är relevant för ett självständigt artificiellt immunsystem.

5.4.5 Analys av detektion av spam

Oda och White (2003) fokuserar på E-post-baserad spam, där uttryck klassificeras efter hur frekvent förekommande de är i spam respektive legitima mail. Genbibliotek byggs till exempel upp från ordlistor, html-dokument och kända spamadresser. Oda och White (2003) har ett upplägg som kräver att definitionen av vad som inte är inkräktande hämtas utifrån i form av ordlistor o.d och som dessutom bygger på att en användare bekräftar om något är spam eller ej. Det kan knappast betraktas som ett system som själv definierar vad som inte är inkräktande.

Utifrån detta är det rimligt att anta att principen med spam inte är relevant för ett självständigt artificiellt immunsystem.

5.4.6 Analys av övervakning av immunsystemet

Kennedy (1998) lyfter fram problemet med att det inte finns någon som övervakar själva immunsystemet. Lösningen är att ha ömsesidigt reflekterande agenter som utför närliggande uppgifter i symbios med varandra, där ändringen av en agents funktionalitet direkt påverkar en annan agent.

Det är oklart om denna ansats inkluderar försvaret av hela datorsystemet eller om den blott avser försvaret av datorsystemets immunssytem. Såsom denna princip är beskriven, så görs i vilket fall som helst ingen definition av vad som inte är inkräktande. Mekanismerna som detekteringen bygger på är förutbestämda och baseras inte på någon definition som gjorts av

immunsystemet av vad som inte är inkräktande. Detektionen av inkräktande bygger på att agenternas funktionalitet rubbas, oavsett om någon definition av vad som inte är inkräktande görs eller ej.

Utifrån detta är det rimligt att anta att principen med övervakning av immunsystemet inte är relevant för ett självständigt artificiellt immunsystem.

5.5 Jämförelse mellan immunologiska referensramar

Denna analys utgår från varje enskild mening i rubrikområdena *2.1.2 Det biologiska immunförsvaret enligt den tidigare forskningen om artificiella immunsytem* och *2.2 Immunologisk referensram*. Efter att analysen gjordes, så har emellertid några meningar i rubrikområdena delats på grund av att de betraktades som för långa. Följande meningar är nya:

”...mer relevant att säga att...”
”...genom att procedurella regler...”
”...att själv-konceptet har fungerat...”
”Alla självpeptider som T-cellerna...”

När analysen gjordes var respektive mening alltså en del av den mening som nu föregår respektive mening .

De relaterade meningarna i tabellerna är för övrigt direkt sökbara genom att citationstecken och punkter plockas bort.

5.5.1 Kategorigenerering

Avser *2.1.2 Det biologiska immunförsvaret enligt den tidigare forskningen om artificiella immunsystem*

Tabell 5 *Genererade kategorier (tabellen sträcker sig över flera sidor)*

Kategori	**Rubrik**	**Relaterad mening**	**Antal rub-riker**	**Rela-tivt antal (%)**
Identifiering	Korresponderande antikroppar aktiveras vid sekundärrespons	”Denna process tar...”	5	7
	Identifiering av patogener genom olika egenskaper	”...kan använda flera egenskaper...”		
	Klassificering av ickesjälv	”...grundläggande funktion...”		
	Typbestämmer antigen	”...typbestämmer antigen...”		

Kategori	Rubrik	Relaterad mening	Antal	%
Identifiering (fortsättning)	Identifikation av objekt som har ogynnsam effekt på organismen	”...biologiska system har...”		
Självdefinition	Försvar mot främmande inkräktare	”...som ett komplext nätverk...”	20	27
	Själv-ickesjälvdiskriminering	”...gör åtskillnad mellan...”		
	Tolerans mot själv	”...mot själv-gener...”		
	Själv-ickesjälvdiskriminering	”...hanterar detektion...”		
	Själv-ickesjälvdiskriminering	”...däggdjurens immunförsvar...”		
	Själv-ickesjälvdiskriminering	”...grundläggande funktion...”		
	Själv-ickesjälvdiskriminering	”...primär egenskap...”		
	Varje cell i organismen tillhör själv	”...primär egenskap...”		
	Själv-ickesjälvdiskriminering	”...essentiell del av...”		
	Själv är komponenter för normal funktionalitet	”Själv är här...”		
	Ickesjälv är främmande material som kan skada funktionaliteten	”Själv är här...”		
	Vissa antikroppar binder till självceller	”Varje enskild lymfocyt...”		
	Immunförsvaret uttnyttjar negativ selektion	”...utnyttjar därför...”		
	Lymfocyter som producerar självbindande antikroppar dör	”...utnyttjar därför...”		
	Endast lymfocyer som producerar antikroppar som binder främmande antigen blir kvar	”...utnyttjar därför...”		
	Immunförsvaret lär sig själv-ickesjälvdiskriminering	”Immunförsvaret lär sig...”		
	Immunförsvaret samexisterar harmoniskt med själv-molekyler	”...normalt sett samexisterar...”		
	Utomstående molekyler elimineras snabbt	”...normalt sett samexisterar...”		
	Autoimmunitet förhindras genom självtolerans	”...således förhindras...”		
	Självdetekterande lymfocyter dödas under mognadsprocessen	”...således förhindras...”		

Kategori	Rubrik	Relaterad mening	Antal	%
Memorering	Kommer ihåg framgångsrika responser	”...lagrar framgångsrika...”	4	5
	Inlärning av främmande strukturer	”...möjliggör att lymfocyterna...”		
	Vissa lymocyter minns infektionen	”...lymfocyter aktiveras när...”		
	Antikroppar kommer ihåg antigen	”...utlöses av en okänd...”		
Specialisering	Anpassning till främmande strukturer	”...möjliggör att lymfocyterna...”	6	8
	Anpassning till förändringar i omgivningen	”...med mekanismer som medger...”		
	Lymfocyter producerar specifika antikroppar	”Varje enskild lymfocyt...”		
	Olika skydd mot olika angripare	”...olika skyddsmekanismer...”		
	Komplext nätverk av specialiserade celler	”...som ett komplext nätverk...”		
	Optimering genom modifiering	”...modifierar andra komponenter...”		
Detektion	Patogen detektion	”...kemiska komponenter...”	25	33
	Receptorer reagerar med ickesjälv	”...möjliggör att det alltid...”		
	Detektion av objekt som har ogynnsam effekt på organismen	”...biologiska system har försvarsmekanismer...”		
	Reaktion på störning från omgivningen	”...med mekanismer som medger...”		
	Detektion genom att receptorer binds till peptider	”Igenkänningen av själv...”		
	Detektion genom själv-ickesjälvdiskriminering	”...att upptäcka patogener...”		
	Lymocyter aktiveras vid infektion	”...lymfocyter aktiveras när...”		
	Primär immunrespons utlöses av okänd patogen	”...utlöses av en okänd...”		
	Antikroppar produceras vid primär immunrespons	”...utlöses av en okänd...”		
	Primärrespons tar förhållandevis lång tid	”Denna process tar...”		
	Sekundärrespons sker snabbt	”Denna process tar...”		
	Detektion genom att lymfocyter binder patogener	”...lymfocyterna kan detektera...”		
	Generering av första signalen vid detektering av ickesjälv	”Första signalen genereras...”		
	Generering av andra signalen vid detektering av skada	”Första signalen genereras...”		

Kategori	Rubrik	Relaterad mening	Antal	%
Detektion (fortsättning)	Falsklarm ger ej autoimmuna reaktioner	”...falsklarmen inte skapar...”		
	Falsklarm ej associerade med skada	”...falsklarmen inte skapar...”		
	Människans immunförsvar är en avvikelsedetektor	”...avvikelsedetektor med...”		
	Människans immunförsvar har mycket låga falska och missade larm	”...avvikelsedetektor med...”		
	Kroppen har råd att vänta tills avvikelser associeras med skada	”...kroppen har så otroligt...”		
	Skadegörande organismer hinner inte försöka sig nämnvärt innan skadedetektion	”De mikroorganismer som...”		
	Ofarligt att avvakta skadedetektion	”De mikroorganismer som...”		
	Skydd mot okända patogener	”...skydda mot patogener...”		
	Många patogener är ofarliga	”...att upptäcka patogener...”		
	Immunreaktion mot ofarliga patogener kan skada kroppen	”...att upptäcka patogener...”		
	Diskriminering av ofarligt ickesjälv-allt annat	”...att upptäcka patogener...”		
Destruktion	Destruktion av objekt som har ogynnsam effekt på organismen	”...biologiska system har försvarsmekanismer...”	5	7
	Eliminering av ickesjälv	”...grundläggande funktion...”		
	Snabb destruktion av angripare vid upprepat angrepp	”...vid ett nytt angrepp...”		
	Antigener elimineras vid sekundärrespons	”Denna process tar...”		
	Eliminerar specifika antigen	”...eliminerar specifika antigen.”		
Mångfald	Mångfald antikroppar mot oönskade bakterier och virus	”...mångfald antikroppar genereras...”	4	5
	Mångfald av lymfocyter	”...mångfald antikroppar genereras...”		
	Antalet antikroppar är begränsat i förhållande till möjliga antigen	”...begränsat i förhållande...”		
	Kroppen har otroligt många celler	”...kroppen har så otroligt...”		

Kategori	Rubrik	Relaterad mening	Antal	%
Proportionalitet	Approximativ bindning p.g.a begränsat antal antikroppar	”...begränsat i förhållande...”	3	4
	Aktivering av lymfocyter vid bindningsbenägenhet av antigen över tröskelvärde	”...begränsat i förhållande...”		
	Reaktion proportionell mot skada	”...därefter att reagera...”		
Tvåsignals-aktivering	Hantering av falsklarm genom tvåsignalsaktivering	”...problemet med falsklarm...”	3	4
	Generering av första signalen vid detektering av ickesjälv	”Första signalen genereras...”		
	Generering av andra signalen vid detektering av skada	”Första signalen genereras...”		

5.5.2 Kategoritestning

Avser *2.2 Immunologisk referensram*.

Kategorier:

Identifiering
Självdefinition
Memorering
Specialisering
Detektion
Destruktion
Mångfald
Proportionalitet
Tvåsignalsaktivering
Övrigt

Tabell 6 *Testade kategorier (tabellen sträcker sig över flera sidor)*

Relaterade meningar (i förekommande ordning)	Ide	Sjä	Mem	Spe	Det	Des	Mån	Pro	Två	Övr
”...varje mänsklig organism...”										X
“Cellerna differentieras...”				X						X
”...komplext samhälle...”				X			X			X
”..celler som kollektivt...”										X
”Dessa celler producerar...”										X
”...generna som finns...”										X
”...substanser är enzymer...”										X
”...reglerande mekanismer...”										X
”...genetiska informationen...”										X
”Proteinerna är de...”										X

Relaterade meningar	Ide	Sjä	Mem	Spe	Det	Des	Mån	Pro	Två	Övr
”...som ärvs i och med...”										X
”...alla levande celler...”										X
”...en bit DNA...”										X
”...hårdkodad genetiskt...”					X					X
”...i genetiska element...”				X	X					X
”...urval av olika celler...”										X
”...har avlägsnats under...”		X								X
”...uttrycks utan att...”										X
”...avhängigt de...”					X					
”...germline för att de...”										X
”...primärt har utvecklats...”		X		X	X					
”...gener som definierar...”										X
”Det gäller såväl...”										X
”...föds individen med...”				X						X
”...organismen förändras...”				X						X
”...kan skapa receptorer...”							X			X
”...avgränsad sekvens som...”				X						X
”...använder en strategi...”							X			X
”...struktureras olika...”							X			
”Exakt hur denna...”										X
”...där variationen i...”							X			X
”...det enzym-maskineri...”										X
”...de mest märkliga...”										X
”...definieras av de gener...”							X			X
”...för att kunna överleva...”		X								X
”...de grundläggande...”		X								
”...uppnå självtolerans...”		X				X				
”...således grundläggs...”		X								
”Det är ett tidsperspektiv...”		X								X
”...toleransutveckling inte...”										X
”...betydande kvantitativa...”										X
”...inte är något unikt...”										X
”...möter antigen utvecklar...”		X				X				
”...i sin helhet...”		X			X					
”...granska allt innehåll...”		X								X
”...är nödvändig eftersom...”		X				X				
”...är ett universitet...”		X			X					
”...fastställs genom att...”		X								
”Detta gör att närvaron...”										X
”Om det inte skapas...”		X								
”...att gensegment på...”		X								X
”...antigen-receptorer som...”		X				X				
”...process till fostertiden...”		X				X				X
”...experimentellt kunnat...”		X				X				
”...även om tymus...”						X				X
”...underhålla tolerans mot...”		X								X
”...som den främsta...”										X

Relaterade meningar	Ide	Sjä	Mem	Spe	Det	Des	Mån	Pro	Två	Övr
”...livstid presenteras inte...”		X				X	X	X		
”...klarar sig igenom...”		X								
”...har stor förkärlek...”		X						X		
”...tillräckligt finmaskig...”		X						X		
”...det som är varaktigt...”		X								
”Om själv är en fastställd...”		X								
”Skulle själv däremot...”		X								
”Förutom att själv bestäms...”		X								
”...tolerans utvecklas före...”		X								
”...*Lymfocytens mognad*...”		X				X				
”...stor affinitet för...”		X			X	X		X		
”...aktiveras bara om...”									X	
”...farligt och ofarligt...”					X					X
”...regler som styr alla...”										X
”...själv som varaktig...”		X								
”...att denna åtskillnad...”		X								
”...räcker att känna igen...”	X				X					
”...reagerar på ett avbrott...”					X				X	
”...kan ha utvecklats till...”					X					
”...inga element i...”					X					
”Balansen mellan att...”						X				X
”...antikroppar framkallas...”					X					
”...utvecklingsprocessen...”					X					
”...förstörs eller inaktiveras...”					X	X				
”...timing och förhållanden...”					X					
”...att kontexten där...”		X			X					
”Karakteristiskt för...”					X					
”Om förändringen sker...”					X			X		
”...långsamt växande...”					X					
”T-cellerna anpassar...”				X	X					
”Egentligen finns det...”	X	X								X
”...Nätverksfokus å...”					X					X
”...nätverksfokus är att...”		X								X
”...suddar ut konturerna...”										X
”Det är när systemet...”					X					
”...det klassificeras som...”		X								
”...är medfödda och...”										X
”De fokuserar på att...”		X			X					
”...är i början av...”		X			X	X				
”...omfattningen av alla...”		X				X	X			X
”...bara finns två sätt...”		X								
”Det ena är genom tid...”		X								
”Det andra är genom rum...”		X								
”...rumsseparationen...”		X								
”...precis och otvetydig...”		X			X					
”Eftersom det som är...”		X								
”...detektion på strukturella...”					X					

Relaterade meningar	Ide	Sjä	Mem	Spe	Det	Des	Mån	Pro	Två	Övr
”...lätt att greppa...”										X
”...grundläggande uppgift....”		X								
”...primärt skyddande...”										X
”Att skydda kroppen...”		X								
”...karakteriseras dock...”										X
”...en villfarelse...”										X
”...göra denna distinktion...”										X
”Själv blir en samling...”		X								
”...kan svara på främmande...”		X								
”...ickesjälv står i centrum...”		X								
”...har trängt undan...”										X
”...har mjölkats till sista...”										X
”...skiljer mellan olika...”		X								
”Det handlar inte om...”						X				
”Istället handlar det...”								X		X
”...som specifikt känner...”				X	X					X
”...agerar inte när det...”					X					X
”...reagerar således på...”					X					
”...blir därmed en historisk...”										X
”Integriteten för en vävnad...”										X
”Försvar mot infektioner...”						X				X
”Hur man förhåller...”	X									X
”Autoimmunitet hjälper...”								X		X
”Att på bästa sätt göra...”								X		X
”Autoimmunitet kan...”					X					X
”...sänder ut extrasignaler...”						X			X	
”...möjlighet att döda...”						X				X
”Vissa vävnader...”										X
”...vissa ställen i kroppen...”						X				
”...det gäller mekanismen...”		X			X					X
”...en trend när det gäller...”					X	X			X	
”Lymfocyten klarar sig...”										X
”...signaler i kontakt...”									X	
”Faktorer förutom...”		X						X	X	X
”...om total utrotning...”		X								X
”Därför krävs andra...”									X	
Antal förekomster 218	3	54	0	9	33	20	8	9	7	75
Relativ förekomst (%)	1	25	0	4	15	9	4	4	3	34

Att summan av de relativa förekomsterna inte blir 100 beror på att de avrundats till närmsta heltal, eftersom det inte är intressant att visa högre noggrannhet.

6 Resultat

6.1 Resultat av analys av data om människans immunförsvar

Analysen har försökt att besvara följande frågor:

F1. Har immunförsvaret en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande?

F2. Definierar människans immunförsvar själv vad som inte skall betraktas som inkräktande?

F3. Bygger immunförsvarets detektion av inkräktande hos människan på att det finns en fördefinierad definition av vad som inte är inkräktande?

Även om det i detta sammanhang har varit svårt att belägga varje enskild mekanism i en klar orsakskedja, så finns det tydliga indikationer som stöder hypoteserna när det gäller själv-perspektivet, samtidigt som det finns tydliga indikationer som strider mot hypoteserna när det gäller det naturliga immunförsvaret, störnings-perspektivet och skade-perspektivet. Detta är en konsekvens av att immunförsvaret har olika funktioner, där vissa är genetiskt betingade, medan andra är somatiskt betingade. Evolutionsmässigt, så kompletterades förmodligen de genetiskt betingade funktionerna med mer anpassningsbara funktioner, eftersom det gav bättre chanser till överlevnad. Flajnik och Kasahara (2001) säger till exempel att alla de gener som definierar det adaptiva immunförsvaret går tillbaka till de äldsta ryggradsdjuren och att det gäller såväl T-cellsreceptorer, som antikroppar och de gener som hanterar omstruktureringsprocessen.

De somatiskt betingade funktionerna har alltså funnits hos människan under väldigt lång tid och därför vore det orimligt att tänka sig att människan skulle kunna existera utan dessa. Vi har i denna anlys avhandlat fyra olika typer av funktioner, där tre är genetiskt betingade och en är somatiskt betingad. Eftersom de genetiskt betingade funktionerna strider mot hypoteserna, så blir en förutsättning för hypotesernas belägg att den somatiskt betingade funktionen är ett nödvändigt villkor för immunförsvaret, något som vi alltså anser att den är. Vi konstaterar således att människans immunförsvar har en förutbestämd förmåga att definiera icke-inkräktande och att det definierar icke-inkräktandet på egen hand, samtidigt som inkräktande-detektionen bygger på att denna definition görs initialt. Frågeställningarna bör således betraktas som bekräftade.

6.2 Resultat av analys av Sophos-data

F7. Utför detta exemplar operationer som exekveras i ett datorsystem?

85% förekomst måste rimligtvis betraktas som en tydlig indikation på att datorvirus, maskar och trojaner utför operationer som exekveras i datorsystem, vilket således gör dem till applikationer.

F9. Utför detta exemplar operationer som användaren inte haft för avsikt att införa i systemet?

60% förekomst är en tillräckligt tydlig indikation på att datorvirus, maskar och trojaner är inkräktande applikationer. Att 40% av exemplaren inte ger sådana indikationer, innebär knappast att de inte skulle kunna innehålla funktionalitet som användaren inte haft för avsikt att införa i systemet. Det innebär bara att beskrivningarna inte givit några indikationer om det. Likväl, om 60% av datorvirus, maskar och trojaner är inkräktande, så måste man rimligtvis se det som att dessa typer av applikationer faktiskt är inkräktande, eftersom det i över hälften av fallen uppenbarligen skulle röra sig om funktionalitet som användare inte haft för avsikt att införa i systemet.

F10. Exekveras detta exemplar i datorsystem som det inte härstammar från?

85% förekomst måste rimligtvis betraktas som en tydlig indikation på att datorvirus, maskar och trojaner som exekveras i datorsystem med Microsoft Windows som operativsystem, inte härstammar från dessa datorsystem.

Resonemanget i F9 är i viss mån även tillämpligt på F7 och F10.

6.3 Resultat av analys av Microsoft-data

F12. Anger bulletinen att en inkräktande applikation kan installeras efter att datorsystemet tagits i bruk av användaren?

66% förekomst måste rimligtvis betraktas som en ganska tydlig indikation på att inkräktande applikationer kan installeras efter att datorsystemet tagits i bruk av användaren, vilket innebär att inkräktande applikationer som körs i datorsystem med Microsoft Windows som operativsystem, inte härstammar från dessa datorsystem. Det finns här ingen anledning att tolka 66% som en otillräckligt indikation, eftersom beskrivningarna är begränsade och därför kanske inte ger tillräckligt med information som visar att det handlar om kod som exekveras. Det står i alla fall klart att inkräktande applikationer i stor utsträckning, faktiskt kan installeras efter att datorsystemet tagits i bruk.

F13. Anger bulletinen att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt?

96% förekomst är en mycket tydlig indikation på att de funktionella förutsättningarna i datorsystemen kan ändras på ett oförutsägbart sätt, vilket definitivt gör datorsystem med Microsoft Windows som operativsystem till dynamiska strukturer.

F14. Rekommenderar bulletinen att operativsystemet måste uppdateras?

85% förekomst måste rimligtvis betraktas som en tydlig indikation på att datorsystem med Microsoft Windows som operativsystem har behov av att uppdateras regelbundet, vilket gör att de måste betraktas som evolutionära system.

6.4 Resultat av analys av forskningen om artificiella immunsystem

Ingen av av principerna för detektion av inkräktande visade sig vara relevant för ett självständigt artificiellt immunsystem. Det som brister är antingen att systemet inte är självständigt eller att det inte använder fundamentala principer hos människans immunförsvar. Modellen frångås när man försöker göra systemet självständigt och självständigheten försvinner när man försöker tillgodose användarnas behov.

Detta ger belägg för huvudhypotesen att ett självständigt artificiellt immunsystem som tillgodoser användarnas behov av säkrare datorsystem, inte kan ha människans immunförsvar som förebild.

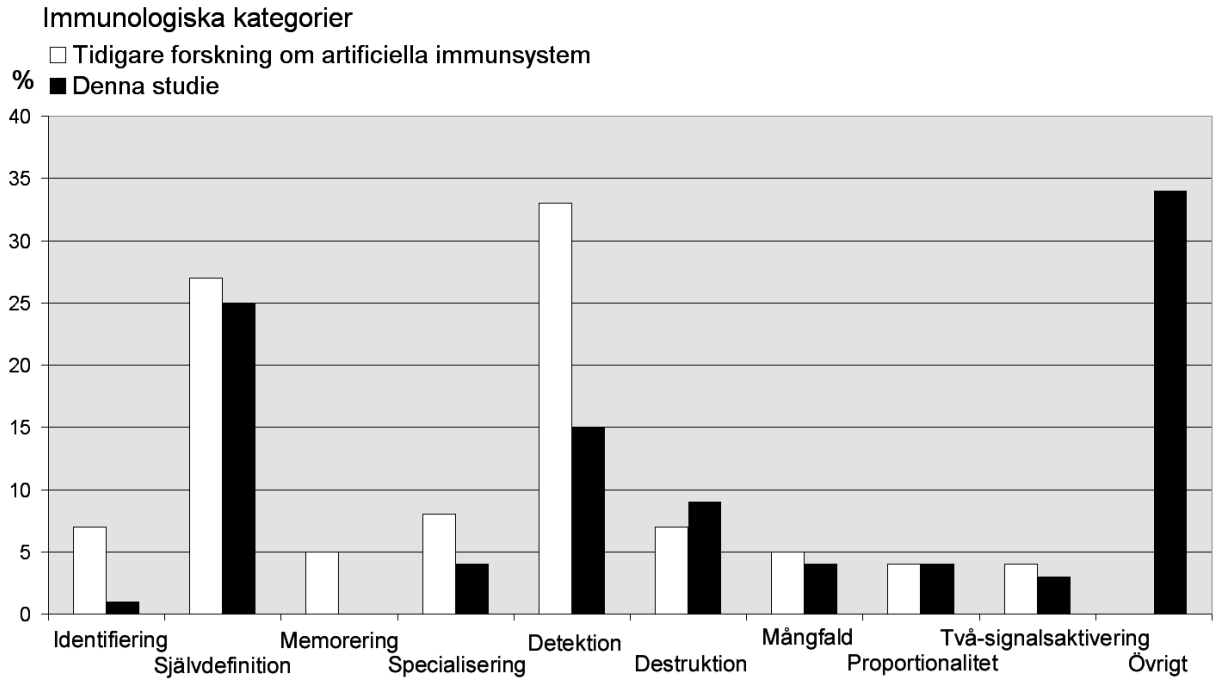
6.5 Resultat av jämförelse mellan immunologiska referensramar

Resultatet illustreras i figur 5. De två immunologiska referenramarna förefaller eniga om att självdefinitionen har en central roll för immunförsvaret. Detta är naturligt, eftersom självdefinition har en central roll inom den immunologiska forskningen

Den immunologiska referensramen för denna studie förefaller ej fokusera på memorering och identifiering i nämnvärd utsträckning. Dessa kategorier är av underordnad betydelse för att kunna detektera okänt inkräktande, men har stor

betydelse för detektering av återkommande angrepp av samma typ. Det skulle i så fall betyda att den tidigare forskningen om artificiella immunsystem lägger större vikt vid att kunna hantera återkommande angrepp. Detta har inte alls varit intressant för denna studie, eftersom det inte är något problem att hantera återkommande angrepp i datorsystem. Det klarar varje antivirusapplikation. Problemet är att kunna upptäcka nya angrepp som ej är kända sedan tidigare.

Specialisering och detektion har i den immunologiska referensramen för denna studie reducerats till hälften i jämförelse med den tidigare forskningen om artificiella immunsystem. Detta kan förmodligen hänföras till att det i den immunologiska referensramen för denna studie i stället finns en stark förskjutning mot sådant som inte berörs av den tidigare forskningen om artificiella immunsystem, företrädesvis det som berörs under *2.2.1 Determinism*. Därmed minskar den relativa andelen av andra kategorier.



Figur 5 *Jämförelse mellan immunologiska referensramar*

Största förklaringen till övrigt-kategorins stora andel ligger i skillnaden i materialens omfattning. Den tidigare forskningen om artificiella immunsystem har en immunologisk referensram på drygt två sidor, medan den immunologiska referensramen för denna studie ligger på tio sidor. Den immunologiska information som funnits i artiklarna inom forskningen om artificiella immunsystem, har varit synnerligen sparsam och det är därför svårt att avgöra hur insatt den tidigare forskningen om artificiella immunsystem egentligen är i immunologin.

En orsak till att den immunologiska informationen i den tidigare forskningen om artificiella immunsystem är knapphändig är förmodligen att forskningen presenteras i form av artiklar, vilket medger begränsat utrymme. Denna förklaring förefaller dock märklig med tanke på att det är de immunologiska

förutsättningarna som utgör grunden för varje artificiellt immunsystem som baserar sig på människans immunförsvar. Hur kan man bygga ett system om man inte har utrett hur grunden ser ut som det vilar på? Intrycket blir således att den tidigare forskningen om artificiella immunsystem mer eller mindre bygger sin grund på förutfattade meningar, snarare än på vetenskapliga argument.

6.6 Slutsats

Analysen har försökt besvara ett antal frågor med syfte att stödja följande hypoteser:

> *H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.*
>
> *H3. Människans immunförsvar definierar själv vad som inte är inkräktande.*
>
> *H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.*
>
> *H7. Datorvirus, maskar och trojaner är applikationer.*
>
> *H9. Datorvirus, maskar och trojaner är inkräktande applikationer i datorsystem med Microsoft Windows som operativsystem.*
>
> *H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.*
>
> *H12. Datorsystem med Microsoft Windows som operativsystem är dynamiska strukturer.*
>
> *H13. Microsoft Windows är ett evolutionärt operativsystem.*

I resultatet av analysen av människans immunförsvar har frågeställningarna bekräftats, vilket således bör ge stöd åt hypoteserna H2, H3 och H4. Eftersom denna analys byggt på kvalitativ argumentation, så görs ingen utläggning om det här, utan detta diskuteras i diskussionsavsnittet.

När det gäller resultatet av analysen av Sophos-data respektive resultatet av analysen av Microsoft-data, så har stöd givits i minst 85% av fallen för fyra av frågeställningarna. Detta ger tydliga indikationer, vilket vi tidigare konstaterat. Det som väcker frågor är de två frågeställningarna som fått lägre stöd. Hypotesen H10 har hämtat stöd från två håll, dels genom

> *F10. Exekveras detta exemplar i datorsystem som det inte härstammar från?*

dels genom

> *F12. Anger bulletinen att en inkräktande applikation kan installeras efter att datorsystemet tagits i bruk av användaren?*

där stöd för respektive fråga funnits i 85% av virusbeskrivningarna och i 66% av bulletinerna. Eftersom vi tidigare argumenterat för att 66% är en tillräckligt bra indikation, så torde denna argumentation därmed stärkas i och med att en starkare indikation ges från en annan källa. Därmed återstår frågeställningen

> *F9. Utför detta exemplar operationer som användaren inte haft för avsikt att införa i systemet?*

som fått ett lägre stöd. Endast 60% av virusbeskrivningarna har kunnat bekräfta denna frågeställning. Även om vi tidigare argumenterat för att detta ger en tillräckligt bra indikation, så måste det ändå betraktas som en något anmärkningsvärd avvikelse. Den motsäger inte hypoteserna, men befläckar ändå resultatet en smula. Vi finner därmed hypoteserna H7, H10, H12 och H13 väl belagda, samtidigt som vi finner H9 tillräckligt belagd.

Resultatet av analysen av forskningen om artificiella immunsystem samt resultatet av jämförelsen mellan immunologiska referensramar står utanför den egentliga hypotestestningen och beaktas därför inte vidare.

7 Diskussion

7.1 Granskning av studien

Denna studie hade från början syftet att finna detektionsprinciper för ett artificiellt immunsystem som baserar sig på människans immunförsvar. För detta ändamål gjordes en omfattande inläsning på det immunologiska området, vilket resulterade i insikten att människosystem principiellt verkar under helt andra förutsättningar än datorsystem. Med anledning av detta, så ändrades studiens inrikting till att istället visa på detta faktum i form av den hypotetisk-deduktiva metoden. En huvudhypotes sattes upp tillsammans med ett antal delhypoteser som genom ett antal postulat och en slutledningskedja gav belägg för huvudhypotesen under förutsättning att delhypoteserna kunde beläggas.

I denna ansats finns tre kritiska punkter. Den första punkten är själva hypoteserna, vars formuleringar avgör både vad som skall testas och validiteten för detta. Den andra kritiska punkten är premisserna – de stipulationer som används för att definiera begrepp i hypotesernas innebörder och de postulat som knyter ihop de olika delhypoteserna till en slutledningskedja. Den tredje kritiska punkten är de data som används för att belägga delhypoteserna. Vi kommer här att titta närmare på detta och även granska slutledning, analys och resultat.

7.1.1 Granskning av hypoteser

En brist i hypoteserna är att de är utformade så att de måste stödjas till 100%, trots att inte slutledningen kräver det. Detta gäller de hypoteser som relaterar till datorsystem. Till exempel så säger hypotesen

> *H11. I ett datorsystem med Microsoft Windows som operativsystem kan både inkräktande och icke inkräktande applikationer exekveras som inte härstammar från detta datorsystem.*

att applikationerna *kan* exekveras, men att de för den skull inte nödvändigtvis *måste* göra det. Eftersom denna hypotes indirekt stöds genom hypotesen

> *H10. Inkräktande applikationer som exekveras i datorsystem med Microsoft Windows som operativsystem, härstammar inte från dessa datorsystem.*

så uppstår problem, eftersom den hypotesen är utformad som att det gäller *alla* applikationer. Detta är inget problem när man ser saker i sitt sammanhang, men

eftersom hypoteserna testas isolerat, så kan det ge en uppfattning att stödet för hypoteserna är tveksamt.

Eftersom H11 talar om *kan*, så borde H10 tala om att applikationerna *inte behöver* härstamma från dessa datorsystem, vilket hade räckt för oss i slutledningen, med tanke på postulatet

> *P5. För att ett system själv skall kunna definiera vad som inte är inkräktande, så måste det antingen ha tillgång till allt som inte är inkräktande eller allt som är inkräktande.*

som kräver tillgång till *allt* inkräktande. Om applikationerna inte behöver härstamma från datorsystemet, så kan man heller inte garantera att det finns tillgång till allt som är inkräktande eller allt som är icke inkräktande.

Vi behöver här inte gå igenom alla hypoteser, utan det räcker med att konstatera att formuleringen är kritisk för validiteten. Man kan inte testa en sak och sedan slutleda en annan. Nämnas bör dock att det finns ett gränsdragningsproblem om man använder sig av begrepp som *kan* eller *inte behöver*. Var går gränsen? Säg att vi endast lyckas hitta ett enda exemplar som inte härstammar från datorsystemen. Det skulle i så fall innebära att det finns fullt belägg för hypotesen. Det är lika illa som Poppers falsfieringsprincip, som säger att det aldrig går att belägga någonting, eftersom man aldrig kan veta om det finns något i framtiden som kommer att strida mot hypoteserna. Med *kan*-perspektivet, så kan man alltid hävda att hypotesen förr eller senare kommer att visa sig vara sann.

7.1.2 Granskning av premisser

P1. Delhypoteserna som relaterar till människans immunförsvar relaterar också till ett artificiellt immunsystem.

Delhypoteserna som relaterar till människans immunförsvar är utformade på ett sådant sätt att de blir nödvändiga för att hantera detektion. Hypotesen

> *H4. Immunförsvarets detektion av inkräktande hos människan bygger på att det finns en fördefinierad definition av vad som inte är inkräktande.*

säger att man måste ha en fördefinierad definition av vad som inte är inkräktande om man skall kunna detektera något. Ett artificiellt immunsystem som skall kunna detektera inkräktande måste alltså tillämpa denna princip. Därmed behövs en definition av icke-inkräktande. Hypotesen

> *H3. Människans immunförsvar definierar själv vad som inte är inkräktande.*

säger att människans immunförsvar gör definitionen själv, vilket således också måste gälla det artificiella immunsystemet, om det vill kunna hantera detektion. Hypotesen

> *H2. Människans immunförsvar har en förutbestämd förmåga att själv kunna definiera vad som inte är inkräktande.*

säger att förutsättningarna för självdefinitionen måste finnas där från början. Detta måste således också gälla det artificiella immunförsvaret om det vill

kunna göra en definition av icke-inkräktande, vilket det måste kunna göra om det skall kunna hantera detektion, enligt resonemanget ovan.

Som vi ser är H2 och H3 egentligen följdhypoteser av H4. Om H4 är nödvändig, så kommer också H2 och H3 att vara nödvändiga. Eftersom det ligger i sakens natur att ett immunförsvar måste kunna hantera detektion, så blir alla tre hypoteserna nödvändiga för ett artificiellt immunsystem som baserar sig på människans immunförsvar.

P2. Datorsystem med Microsoft Windows som operativsystem tillåter att icke inkräktande applikationer installeras och exekveras.

Man skulle kunna tänka sig att utvecklingen leder till statiska datorsystem för vissa specifika ändamål som inte har något behov av att nya applikationer installeras. Det är dock svårt att tänka sig att ett sådant datorsystem skulle använda ett operativsystem av Microsoft Windows kaliber för detta ändamål. De flesta mjukvaruprodukter utvecklas i regel till att bli mer flexibla och inte tvärtom. Hur som helst, faktum kvarstår – de flesta datorsystem med Microsoft Windows som operativsystem tillåter att icke inkräktande applikationer installeras och exekveras. Vi har en hel mjukvaruindustri som bygger på detta faktum.

P4. Ett artificiellt immunsystem som tillgodoser användarnas behov, kan inte själv definiera vad som inte är inkräktande.

Denna innebörd kan man vrida och vända hur mycket man vill på, men det är bara om det artificiella immunsystemet själv kan ta reda på användarnas behov, som det skulle kunna definiera vad som inte är inkräktande. Man skulle i förlängningen kunna tänka sig ett självständigt artificiellt immunsystem som på egen hand skaffade sig kunskap om användarnas behov. Detta skulle dock bara vara vad immunsystemet uppfattar som användarnas behov och skulle i slutändan likväl kräva någon verifieringsmekanism, där användarna uttryckligen bekräftar om uppfattningen är riktig. Eftersom det alltid kommer att finnas applikationer som för vissa användare är legitima, samtidigt som de är inkräktande för andra, så är det bara användarna själva som kan bekräfta i det enskilda fallet.

Ett typiskt exempel är applikationer för fjärrstyrning av datorsystemet, som i vissa fall legitimt installeras av användarna själva, medan det i andra fall rör sig om inkräktande trojaner. Hur skall systemet veta när installationen är legitim? Det här problemet behöver inte gälla applikationer som helhet, det räcker med att titta på de enskilda operationerna som de inkräktande applikationerna utför. Ur datorsystemets synvinkel finns det inga inkräktande operationer. Att applikationerna blir inkräktande är för att de utför en viss kombination av operationer. Enda sättet för datorsystemet att få reda på vilka kombinationer som är otillåtna är att fråga användaren, vilket innebär att definitionen av icke-inkräktandet görs utanför systemet. Vi kommer inte runt problemet, hur vi än vrider och vänder.

P5. För att ett system själv skall kunna definiera vad som inte är inkräktande, så måste det antingen ha tillgång till allt som inte är inkräktande eller allt som är inkräktande.

Detta påstående är liktydigt med att man måste ha tillgång till alla äpplen som någonsin har existerat och som någonsin kommer att existera för att kunna veta vad som är ett äpple. Uppenbarligen kan de flesta känna igen äpplen, trots att de bara lärt känna ett begränsat antal, så det är ju alltid möjligt att hävda att man utifrån generella egenskaper i inkräktandet eller icke-inkräktandet, skulle kunna dra slutsatser om vad som faktiskt är ett inkräktande.

Problemet är att den uppfattning som individer har om vad som är äpplen, inte är liktydig med en generell definitionen på äpplen. Om det skulle dyka upp en äppleformad frukt som smakade päron, så skulle vissa klassificiera det som ett äpple, medan andra skulle säga att det var ett päron. Några skulle till och med hävda att det var något annat.

Bildar man sig en uppfattning utifrån ett begränsat antal exemplar, så finns alltid möjligheten att man förr eller senare stöter på exemplar som inte stämmer med uppfattningen. Det är således både möjligt och troligt att en uppfattning om vad som är inkräktande som inte utgår från allt inkräktande eller vice versa, missar något.

H9. Datorvirus, maskar och trojaner är inkräktande applikationer i datorsystem med Microsoft Windows som operativsystem.

Här har kriteriet för inkräktande bestämts till användarens avsikt. Man kan fråga sig vad det är för naturlag som säger att det är användarens avsikt som skall avgöra hururvida det rör sig om ett inkräktande eller ej. Framförallt skulle man kunna hävda att en studie som själv definierar inkräktande gör definitionen på ett sådant sätt att hypotesen mer eller mindre automatiskt bekräftas. En legitim definition skulle i så fall kräva en allmängiltig definition av vad som är inkräktande.

Problemet är bara att det inte existerar någon generell definition av vad som skall räknas som inkräktande i ett datorsystem. En definition skulle kunna vara att inkräktande är det som antivirusföretagen klassar som inkräktande. Det säger ingenting om inkräktandets innebörd. Boukerche, Jucá, Sobral och Notare (2004) definierar det som aktiviteter som äventyrar konfidentialitet, integritet och tillgänglighet. Problemet är att denna definition inte rymmer inkräktande som inte äventyrar dessa egenskaper hos systemet. Ur systemets synvinkel finns det ingen skillnad på en applikation som en legitim användare installarerar för att få fjärråtkomst till sin dator, och på en trojan som låter en illegal användare få fjärråtkomst till samma dator. Båda applikationerna installeras i regel av den legitima användaren och sålunda har varken konfidentialitet, integritet eller tillgänglighet äventyrats ur systemets synvinkel. Enligt Marmelstein, Van Veldhuizen och Lamont (1998) gör ju webbläsare det enkelt att ladda hem infekterade filer.

Finns det något typiskt inkräktande beteende? Det kanske det finns, men om detta fanns definierat, så skulle det inte vara något problem att utveckla antivirusapplikationer som kunde upptäcka nya virus. Det förefaller således som att definitionen på inkräktande applikationer måste göras utanför systemet och det blir därför rimligt att definiera det som applikationer som utför operationer som användarna inte haft för avsikt att införa i systemet.

7.1.3 Granskning av slutledning

I slutledningen sägs det att ett artificiellt immunsystem varken kan använda inkräktande eller icke inkräktande applikationer för att initialt definiera vad som inte skall betraktas som inkräktande. Det konstateras därmed att det inte är möjligt att göra en initial definition av vad som inte är inkräktande på grund av postulatet

> *P5. För att ett system själv skall kunna definiera vad som inte är inkräktande, så måste det antingen ha tillgång till allt som inte är inkräktande eller allt som är inkräktande.*

Detta ger ett intryck av att applikationer skulle vara det enda som vore möjligt att använda som underlag för själva definitionen. Låt oss säga att vi istället använder systemets funktionlitet som underlag för definitionen. För att detta skall kunna användas som underlag till definition måste vi således antingen känna till all funktionalitet som är inkräktande eller känna till all funktionalitet som är icke inkräktande. Hypotesen

> *H12. Datorsystem med Microsoft Windows som operativsystem är dynamiska strukturer.*

innebär att de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt, vilket medför att man initialt inte har tillgång till all funktionalitet. Om vi initialt inte har tillgång till all funktionalitet, så kan vi knappast använda funktionalitet som underlag till att definiera vilken funktionalitet som skall betraktas som icke inkräktande. Det skulle i så fall förutsätta att vi åtminstone har tillgång till all funktionalitet som är icke inkräktande, vilket är liktydigt med att man måste ersätta hela systemet med ett nytt, så fort man behöver nya funktioner.

Det är naturligtvis tänkbart att man säljer datorsystem under samma förutsättningar som till exempel bilar. En bil konstrueras och tillverkas med given funktionalitet som inte förändras över tiden. Det finns ingen naturlag som säger att datorsystem måste vara dynamiska strukturer där de funktionella förutsättningarna kan ändras på ett oförutsägbart sätt. Om datorsystemen för en viss marknad istället säljs med en uppsättning standardapplikationer, så blir det enkelt att detektera inkräktande, eftersom man redan från början vet vad som är icke inkräktande. Även om detta skulle vara en tänkbar, om än stelbent lösning, så faller det på grund av hypotesen

> *H13. Microsoft Windows är ett evolutionärt operativsystem.*

som innebär att systemet utvecklas kontinuerligt på ett oförutsägbart sätt i form av att olika säkerhetshål täpps till. Man kan inte täppa till några säkerhetshål i ett datorsystem som betraktar förändrad funktionalitet som inkräktande. Det skulle istället kräva att man byter ut hela systemet varje gång ett nytt säkerhetshål behöver åtgärdas och med tanke på hur frekvent förekommande dessa uppdateringar varit historiskt sett, så är det inte något som i praktiken låter sig göras.

Här har vi försökt göra definitionen utifrån vilken funktionalitet som skall betraktas som icke inkräktande. Hur är det då med det omvända, där definitionen görs utifrån vilken funktionalitet som skall betraktas som inkräktande? H13 antyder att man inte kan definiera vad som skall betraktas som inkräktande funktionalitet. Om det vore möjligt att ta hänsyn till allt möjligt inkräktande, så skulle systemen inte ha några säkerhetshål, vilket de bevisligen har. Anledningen är att man inte kan veta när definitionen är fullständig.

Att vi nu har försökt utesluta både applikationer och funktionalitet som potentiella definitionsunderlag, hindrar förstås inte att man försöker hitta andra möjligheter. Vi skall dock lämna den diskussionen därhän, eftersom det är svårt att över huvud taget hitta några andra definitionsunderlag, samtidigt som det är svårt att se varför dessa i så fall inte skulle omfattas av motsvarande resonemang.

7.1.4 Granskning av datainsamling

Denna studie använder endast sekundära data, vilket har belysts i teorianknytningen. Största svagheten är att de sekundära data som använts är framtagna för andra syften, där hypotesstödet skulle bli bättre anpassat och mer riktat om datainsamlingen gjordes empiriskt. Speciellt gäller detta de immunologiska genetiska mekanismerna och även datorvirusens egenskaper som inte alltid gjorts explicita i Sophos beskrivningar.

Risken är att man ser det man vill se och bortser från det som inte passar in i ens föreställningar. Den immunologiska referensramen har till stor del framställts utifrån artiklar som sållats fram genom sökning på själv-ickesjälvdiskriminering och tolerans. Detta innebär att det kan finnas artiklar som behandlar alternativa ståndpunkter som inte beaktats i undersökningen. Antivirusdata har hämtats från endast ett företag och det är tänkbart att ett annat företag skulle kunna ha beskrivningar som gav ett annat resultat.

Även om det vore att föredra att själv samla in empiriska data, så sätter den resursmässiga ramen gränserna för denna studie – tidsmässigt, instrumentellt och kompetensmässigt. Detta gäller framförallt den immunologiska delen. Det finns varken tillgång till medicinsk utrustning eller preparat att göra mätningar på. Och om det fanns, så skulle det inte finnas tillräckligt med kunskap för att kunna hantera dem. Skulle man likväl överbrygga dessa hinder, så sätter tiden gränsen. Man hinner inte åstadkomma särskilt mycket på två månader. Räknar man bort tiden som går åt till inläsning, förberedelse, analys, reflektion och skrivande, så blir det inte mycket kvar till reell datainsamling.

Detta gör att det heller inte hade varit relevant att empiriskt undersöka olika typer av datorvirus, även om det hade varit praktiskt möjligt, rent kompetensmässigt sett. Det valda upplägget förefaller således vara det mest rationella och några andra ansatser hade inte varit att föredra i detta sammanhang. Metoderna har anpassats efter de ramar som sätter gränserna.

Validiteten har definierats genom specificeringen av hypotesernas och postulatens innebörder, så att perspektivet inte blivit snedvridet. Reliabiliteten har uttryckts genom att upplägget gjorts så explicit som möjligt, så att inte perspektivet bygger på ogrundade genvägar.

7.1.5 Granskning av analys/resultat

Granskning av Sophos-resultat respektive Microsoft-resultat

Att vi här står med ett mätbart resultat implicerar vissa dolda aspekter. Ett kvantitativt resultat ger en illusion av att vi mäter något objektivt eftersom vi har något som kan uttryckas i siffror. Inom vetenskapen finns en stor förkärlek att kvantifiera de fenomen man beaktar, för att sedan formalisera dem på olika sätt. Problemet är bara att kvantifiering alltid mynnar från någon källa som måste tolkas. I detta fall bygger kvantifieringen på tolkning av texter utifrån givna kriterier. Det är alltså en bedömningsfråga om en viss text faller under ett visst kriterium och det finns inget som motsäger att en annan uttolkare inte skulle göra en annan bedömning. Detta är vad Graziano och Raulin (1989) benämner tolkningsreliabilitet. Som om inte det skulle vara nog, så finns ytterligare ett tolkningssteg i form av framtagningen av kriterier. I detta fall har det handlat om att omsätta hypoteser till bekräftelsebara frågor.

Men även om vi accepterar dessa tolkningssteg, så ställs vi ofrånkomligen inför problemet med hur resultatet skall tolkas. Hur vet vi var gränsen går för ett tillräckligt bra stöd för en hypotes? I resultatet har vi försökt argumentera för varför de erhållna indikationerna är tillräckliga, men det hindrar inte en annan uttolkare från att dra en annan slutsats. Även om vi sätter upp kvantitativa kriterier för när en hypotes skall uppfattas som belagd, så ersätter vi i princip bara ett tolkningssteg med ett annat. Även om detta resonemang ger ett uppgivet intryck av att kunna göra lite som man känner för eftersom man ändå aldrig kan få bort tolkningsstegen, så har arbetet i denna studie likväl i stor utsträckning präglats av objektivitet och öppenhet. Förekommande tolkningar har gjorts oberoende av de hypoteser som varit föremål för bekräftelse. Skulle studien upprepas av andra, så är sannolikheten förmodligen hög att resultatet skulle stämma någorlunda överens.

Granskning av immunförsvars-analysen

Om det har funnits tolkningsutrymme i Sophos-analysen respektive Microsoft-analysen, så torde det inte vara något mot det tolkningsutrymme som har funnits i immunförsvars-analysen. Analysen av data om människans immunförsvar har i mångt och mycket handlat om att lyfta fram orsakssamband genom att försöka blottlägga olika mekanismer. Problemet är bara att de data som ligger till grund för analysen – den immunologiska referensramen, inte innehåller tillräckligt med information för att fastställa alla orsakssamband. Även om det enligt Graziano och Raulin (1989) räcker med

korrelationer när man inte har höga krav på orsakssamband, så står det helt klart att tillgängliga data innehåller luckor som skulle kunna rymma påverkande faktorer.

Dessa informationsluckor beror dock inte på att undersökningen inte har varit tillräckligt noggrann. Det hänger samman med att samtliga erfoderliga mekanismer helt enkelt inte finns klarlagda i den immunologiska forskningen, vilket påpekats i *4.2.3 Studiens integritet*. Frågan är då hur man skall förhålla sig till detta faktum. Det kan å ena sidan aldrig vara acceptabelt att legitimera brister i en undersökning bara för att fakta för tillfället är otillgängliga. Å andra sidan kan det inte heller vara acceptabelt att låta bli att undersöka saker bara för att fakta för tillfället är otillgängliga. Det finns alltid en risk att okända faktorer påverkat en undersökning, även om alla pusselbitar förefaller ha fallit på plats.

Vetenskapen framskrider inte för att den finner sanningen. Den framskrider för att teorierna ger en allt bättre bild av hur naturen fungerar, som Bowler (1992) säger. Analysen av människans immunförsvar visar inte att hypoteserna är sanna. Men analysen visar att det är *rimligt att anta* att hypoteserna ger en bild av hur immunförsvaret fungerar.

7.2 Diskussion av den tidigare forskningen om artificiella immunsystem

De olika ansatserna som lyfts fram skulle mycket väl kunna vara relevanta för att kunna detektera inkräktande och de har onekligen inspirerats av det mänskliga immunförsvaret. Problemet är att man plockat principerna ur deras sammanhang, utan att undersöka om helheterna är analoga. Det räcker inte att se likheter med en företeelse för att den skall kunna användas som modell, det måste finnas fundamentalt principiella likheter.

Hofmeyr (2004) säger till exempel att analogin borde vara väldigt kraftfull eftersom immunförsvaret skyddar kroppen väldigt framgångsrikt i ett mycket komplext system. Att immunförsvaret skyddar kroppen framgångsrikt säger dock ingenting om analogins kraftfullhet. Att analogin är kraftfull förutsätter att kroppen och datorssystem är analoga. Att två system är komplexa gör dem inte analoga per automatik. Marmelstein, Van Veldhuizen och Lamont (1998) säger till exempel att det artificiella immunsystemet inte har de evolutionära anpassningsmekanismer som det biologiska immunförsvaret besitter. Hofmeyr (2004) säger också att det inte finns någon direktmappning mellan våra kroppar och ett datorsystem, där konfidentialitet inte har någon motsvarighet hos immunförsvaret. Det krävs förvisso ingen direktmappning för att något skall vara analogt, men frågan är i så fall var man drar gränsen.

Även Boukerche, Jucá, Sobral och Notare (2004) ser likheter i att immunförsvaret fungerar som skydd för kroppen mot sjukdomsalstrande organismer, på samma sätt som säkerhetssystemen i datorer skyddar mot illasinnade användare. Problemet här är att man utgår ifrån att försvarsmekanismerna skulle vara analoga, eftersom kravspecifikationerna är det. Men det säger ingenting om analogin mellan de system som skall skyddas. Därför spelar det ingen roll att Foukia, Hassas, Fenet och Albuquerque (2003) identifierar egenskaper som är intressanta ur ett datorsystemsperspektiv, liksom Forrest, Hofmeyr och Somayaji (1996), samt Lee, Kim och Hong (2004), så länge det inte finns indikationer som visar att systemen verkar under motsvarande förutsättningar. Det kommer således inte att vara tillräckligt att Marmelstein, Van Veldhuizen och Lamont (1998) använder komponenter i sitt säkerhetssystem som är analoga med det biologiska immunförsvaret.

Forrest, Hofmeyr och Somayaji (1996), liksom Dozier, Brown, Hurley och Cain (2004), och även Lee, Kim och Hong (2004), och dessutom Foukia, Hassas, Fenet och Albuquerque (2003), samt Bentley (2002) drar paralleller till själv-ickesjälv-perspektivet i det mänskliga immunförsvaret och antyder att det är tillämpligt i datorsystem. Men dessa antaganden förefaller vara premisser som endast grundar sig på likartade beteenden. Det förefaller inte finnas några utförliga analyser som faktiskt visar om analogin är relevant.

Hofmeyer (2004) ser inte analogin som självklar, utan konstaterar att det förutsatts att distinktionen mellan själv och ickesjälv skulle vara fundamental inom datorsäkerhet, eftersom den är fundamental inom immunologin. Problemet är att han anser att den går att tillämpa om man hittar det i datorsystemet som kan jämställas med immunförsvarets peptider. Det tar likväl inte någon notis om helheten, utan flyttar bara fokus till isolerade element.

Hofmeyr (2004) snuddar dock vid problemets kärna i och med att han säger att immunförsvaret inte är en efterhandskonstruktion, utan har utvecklats parallellt med kroppen, som utvecklades till att vara lättskyddad. Han glider dock över på fel spår i och med inställningen att det är människans uppfinnesrikedom som i nuläget har svårt att matcha evolutionen. Hofmeyr (2004) menar att man måste bygga datorsystem som till naturen är mer biologiska om man skall utnyttja analogin fullt ut. Problemets kärna är emellertid en helt annan, nämligen att människan har utvecklats av egen kraft, medan datorsystemen alltid utvecklas externt. Det mänskliga immunförsvaret skyddar den mänskliga kroppens behov, medan ett artificiellt immunsystem skyddar användarnas behov, snarare än datorsystemets behov. Detta medför att det i slutändan alltid är användarna som avgör vad som skall skyddas.

En springande punkt är till exempel det som Forrest, Hofmeyr och Somayaji (1996) lyfter fram, att självdefinition i datorsystem förefaller ha större dynamik än i det naturliga immunförsvaret, eftersom användare regelmässigt uppdaterar programvara och kör nya program. Här finns en fundamental skillnad, eftersom människans immunförsvar definierar själv en gång för alla och sedan använder denna definition som utgångspunkt för detektion av ickesjälv. Om en användare får installera nya program som totalt ändrar systemets funktionalitet, hur skall någon självdefinition då över huvud taget kunna göras? För att något

skall kunna definieras som själv, så måste det finnas något varaktigt som är stabilt över tid och det är svårt att föreställa sig något sådant i ett datorsystem. Ur ett datorsystems synvinkel så har inkräktande applikationer lika stor legitimitet som icke inkräktande applikationer och det är endast användarna som står för klassificeringen. Även om man bygger in klassificeringen i datorsystemet, så är den likväl gjord utanför systemet och inte skapad av systemet självt för att skydda systemets behov. Klassificeringen skyddar användare utanför systemet och kräver således faktorer utanför systemet för att låta sig definieras.

Kim, Kim och Hong (2004), liksom Marmelstein, Van Veldhuizen och Lamont (1998) ser parallellismen i det naturliga immunförsvaret som mycket effektivare än det artificiella immunsystemets seriella aktivering. Detta är dock mer ett prestandaproblem än ett fundamentalt funktionellt problem. Det är inte bristen på resurser som gör att det inte går att utveckla ett artificiellt immunsystem, gränsen sätts snarare av datorsystemens flexibilitet. Enligt Lee, Kim och Hong (2004) lämpar sig negativ selektion bäst för stabila system, där den mänskliga kroppen karakteriseras av ett stabilt tillstånd, till skillnad från datorsystem. Den mänskliga kroppen är inte anpassad för att få ny funktionalitet över tiden. Transplanterar man till exempel in ett nytt organ, så utlöser det autoimmuna reaktioner, eftersom immunförsvaret betraktar det som inkräktande. Installerar man en ny applikation i ett datorsystem, så beror det på användarens intentioner, om den skall betraktas som inkräktande eller ej.

7.3 Slutord

Det finns en tydlig skillnad mellan människan och ett datorsystem. Människan är ett självutvecklande system som formats under evolutionen, där immunförsvaret utvecklats parallellt inom systemet med sådana egenskaper som gagnat individen i det naturliga urvalet. Det innebär implicit att människans immunförsvar medger att individen blir livskraftig gentemot omgivningen.

Ett datorsystem däremot utvecklas inte självständigt, utan av människor. Om datorsystemet skulle kunna utveckla sig själv, så skulle dess immunsystem skydda själva datorsystemet, oavsett om det låg i linje med användarnas behov eller ej. Man skulle visserligen kunna tänka sig ett självutvecklande system som i förlängningen tog hänsyn till användarnas behov, genom att externa faktorer stimulerade till det, till exempel genom en evolutionsprocess som dödade alla system som inte tog hänsyn till användarnas behov. Detta skulle dock inte vara något naturligt urval och framförallt skulle det vara en process som kontrollerades av faktorer utanför systemet, även om det skulle vara systemet som utvecklade sig självt.

Man kan i och för sig hävda att det evolutionära urvalet i naturen kontrolleras av externa faktorer, men skillnaden är att det ur vetenskaplig synvinkel inte

finns några bevis för att en motsvarande övergripande makt faktiskt står för en sådan styrning. Det implicerar att man kan exkludera evolutionär styrning genom externa intressenter när det gäller människans immunförsvar. Men egentligen spelar resonemanget ingen roll, ty även om en individ genom evolutionen skulle ha formats till att ta hänsyn till externa behovsintressenter, så strider det likväl mot kravet att immunförsvaret själv skall kunna definiera vad som inte är inkräktande. Ett system som tar hänsyn till externa intressenters behov, kommer alltid att behöva hämta definitionen utifrån. Är behoven dynamiska, så kan systemet inte lista ut dem på egen hand; är de statiska, ja då är de förutbestämda och inte definierade inom systemet.

Essensen i problemet är att datorsystem till skillnad från människor har användare. Det behöver inte röra sig om mänskliga användare, det kan mycket väl vara andra system. Datorsystem som är utvecklade av människor har alltid användare i en eller annan form. Även om man ser datorvirus som självständiga program, så har de likväl användare. De tjänar antingen som ett uttrycksmedel för misslyckade programmerare eller också är de ett verktyg för ljusskygga verksamheter som medvetet försöker skinna folk på pengar.

Enligt Boukerche, Jucá, Sobral och Notare (2004) påverkar datorvirus som första artificiella livsform det moderna samhället. Man skulle i förlängningen kunna tänka sig självutvecklande datorsystem som bröt sig loss och började leva sina egna liv. System som inte längre hade några användare, utan som snarare blev individer i samhället under samma förutsättningar som människor. Systemen skulle då vara självständiga medborgare som erbjöd sina tjänster för att helt enkelt kunna försörja sig.

Dessa självständiga datorsystem skulle naturligtvis möta motstånd från många människogrupper och således skulle de med tiden börja utveckla någon form av försvarssystem som hjälpte dem att överleva från generation till generation. Det skulle alltså kunna innebära att vi faktiskt fick självständiga artificiella immunsystem som tillgodosåg behovet av säkrare datorsystem. Men detta skulle vara datorsystemens egna behov, där immunsystemen framförallt såg till att systemen inte kontrollerades av externa aktörer som benämde sig själva användare.

Referenser

Onlinematerial

Materialet är i regel tillgängligt via www.sciencedirect.com
Vissa artiklar kan sökas via www.google.se

Aickelin, U., Greensmith, J. och Twycross, J. (2004). *Immune System Approaches to Intrusion Detection – A Review*. Proceedings ICARIS-2004, 3rd International Conference on Artificial Immune Systems.

Alam, R. och Gorska, M. (2003). *3. Lymphocytes*. Journal of Allergy and Clinical Immunology, vol.111, nr.2, februari 2003, s.476-485.

Bentley, P.J. (2002). *Why Biologist and Computer Scientists Should Work Together*. Artificial Evolution: 5th International Conference, Evolution Artificielle, EA 2001, Le Creusot, Frankrike, 29-31 oktober 2001, vol.2310, s.3-15.

Boukerche, A., Jucá, K.R.L., Sobral, J.B. och Notare, M.S.M.A. (2004). *An artificial immune based intrusion detection model for computer and telecommunication systems*. Parallel Computing, vol.30, nr.5-6, maj-juni 2004, s.629-646.

Chaplin, D.D (2003). *1. Overview of the immune response*. Journal of Allergy and Clinical Immunology, vol.111, nr.2, februari 2003, s.442-459.

Chen, Z.K. (2001). *Nihility: Discovery of the Immunologic Zero Corner Where Self-Tolerance and Clonal Deletion Are Challenged*. Transplantation Proceedings, vol.33, nr.1-2, februari-mars 2001, s.145-147.

Cohen, I.R. (2000). *Discrimination and dialogue in the immune system*. Seminars in Immunology, vol.12, nr.3, juni 2000, s.215-219.

Dembic, Z. (2000). *Immune system Protects integrity of tissues*. Molecular Immunology, vol.37, nr.10, s.563-569.

Dighiero, G. och Rose, N.R. (1999). *Critical self-epitopes are key to the understanding of self-tolerance and autoimmunity*. Immunology Today, vol.20, nr.9, 1 september 1999, s.423-428.

Dozier, G., Brown, D., Hurley, J. och Cain, K. (2004). *Vulnerability Analysis of Immunity-Based Intrusion Detection Systems Using Evolutionary Hackers*. Proceedings in Genetic and Evolutionary Computation – GECCO 2004: Genetic and Evolutionary Computation Conference, Seattle, WA, USA, 26-30 juni 2004, part 1, vol.3102, s.263-274.

Efroni, S. och Cohen, I.R. (2003). *The heuristics of biologic theory: the case of self-nonself discrimination*. Cellular Immunology, vol.223, nr.1, maj 2003, s.87-89.

Fazekas de St Groth, B. (1998). *The evolution of self-tolerance: a new cell arises to meet the challenge of self-reactivity*. Immunology Today, vol.19, nr.10, oktober 1998, s.448-454.

Flajnik, M.F. och Du Pasquier, L. (2004). *Evolution of innate and adaptive immunity: can we draw a line?* Trends in Immunology, vol.25, nr.12, december 2004, s.640-644.

Flajnik, M.F. och Kasahara, M. (2001). *Comparative Genomics of the MHC: Glimpses into the Evolution of the Adaptive Immune System*. Immunity, vol.15, nr.3, september 2001, s.351-362.

Forrest, S., Hofmeyr, S.A och Somayaji, A. (1996). *A Sense of Self for Unix Processes*. Proceedngs of ht 1996 Symposium on Security and Privacy. IEEE Computer Society Press. Los Alamitos, California, USA. s. 120-128.

Foukia, N., Hassas, S., Fenet, S. och Albuquerque, P. (2003). *Combining Immune Systems and Social Insect Metaphors: A Paradigm for Distributed Intrusion Detection and Response System*. Mobile Agents for Telecommunication Applications, vol.2881, s.251-264. Springer-Verlag, Heidelberg.

Grossman, Z. och Paul, W.E. (2000). *Self-tolerance: context dependent tuning of T-cell antigen recognition*. Seminars in Immunology, vol.12, nr.3, juni 2000, s.197-203.

Hanahan, D. (1998). *Peripheral antigen-expressing cells in thymic medulla: factors in self tolerance and autoimmunity*. Current Opinion in immunology, vol.10, nr.6, december 1998, s.656-662.

Hofmeyr, S. (2004). *The implications of immunology for secure systems design*. Computers & Security, vol.23, nr.6, september 2004, s.453-455.

Kennedy, C.M. (1998). *Evolution on Self-Definition*. The 1998 IEEE International Conference on Systems, Man, and Cybernetics, part 4, San Diego, California, USA. 11-14 oktober, 1998 s.3810-3815.

Kim, C., Kim, W. och Hong, M. (2004). *Effective Detector Set Generation and Evolution for Artificial Immune System*. Proceedings in Computational Science – ICCS 2004: 4th International Conference, Kraków, Polen, juni 6-9, 2004, part 2, vol.3037, s.491-498.

Kruisbeek, A.M. och Amsen, D. (1996). *Mechanisms underlying T-cell tolerance*. Current Opinion in Immunology, vol.8, nr.2, april 1996, s.233-244.

Kyewski, B., Derbinski, J., Gotter, J. och Klein, L. (2002). Trends in Immunology, vol.23, nr.7, juli 2002, s.364-371

Langman, R.E och Cohn, M. (2000). *Editorial introduction*. Seminars in Immunology, vol.12, nr.3, juni 2000, s.159-162.

Langman, R.E och Cohn, M. (2000a). *A minimal model for the self-nonself discrimination: a return to the basics*. Seminars in Immunology, vol.12, nr.3, juni 2000, s.189-195.

Lee, H., Kim, W. och Hong, M. (2004). *Artificial Immune System against Viral Attacks*. Computational Science - ICCS 2004: 4th International Conference, Kraków, Poland, 6-9 juni, 2004, Proceedings, Part 2, vol.3037, s.499-506.

Livák, F. och Petrie, H.T. (2001). *Somatic generation of antigen-receptor diversity: a reprise*. Trends in Immunology, vol.22, nr.11, november 2001, s.608-612.

Luo, W., Cao, X. och Wang, X. (2001). *NIDS Research Based on Artificial Immunology*. Proceedings in Information and Communications Security: Third International Conference, ICICS 2001, Xian, China, 13-16 november, 2001, vol.2229, s.371-375.

Marmelstein, R.E., Van Veldhuizen, D.A och Lamont, G.B. (1998). *A Distributed Architecture for an Adaptive Computer Virus Immune System*. The 1998 IEEE International Conference on Systems, Man and Cybernetics, Part 4. San Diego. 11-14 Oct, 1998 s. 3838-3843.

Medzhitov, R. och Janeway, C.A. Jr. (2000), *How does the immune system distinguish self from nonself?*. Seminars in immunology, vol.12, nr.3, juni 2000, s.185-188.

Microsoft (2004). *Microsoft Security Bulletin*. http://www.microsoft.com/technet/security/CurrentDL.aspx

Microsoft (2004a). *Microsoft Security Advisor Program: Glossary of Terms*. http://www.microsoft.com/technet/security/bulletin/glossary.mspx

Miller, J. (2004). *Self-nonself discrimination by T lymphocytes*. Comptes Rendus, vol.327, nr.5, maj 2004, s.399-408.

Miller, J.F. och Basten, A. (1996). *Mechanisms of tolerance to self*. Current Opinion in Immunology, vol.8, nr.6, december 1996, s.815-821.

Oda, T. och White, T. (2003). *Developing an Immunity to Spam*. Lecture Notes in Computer Science, Springer-Verlag. Heidelberg. vol.2723, s.231-242.

Ohashi, P.S. och DeFranco, A.L. (2002). *Making and breaking tolerance*. Current Opinion in Immunologym vol.14, nr.6, december 2002, s.744-759.

Pandit, N.R. (1996) *The Creation of Theory: A Recent Application of the Grounded Theory Method*. The Qualitative Report, december, 1996, vol.2, nr.4.

Re, F. och Strominger, J.L. (2004). *Heterogeneity of TLR-induced responses in dendritic cells: from innate to adaptive immunity*. Immunobiology, vol.209, nr.1-2, augusti 2004, s.191-198.

Roberts, C.W. (2001). *Content Analysis*. International Encyclopedia of the Social & Behavioral Sciences, vol.4, s.2697-2702.

Rose, N.R, (1999). *Reflections on Tolerance, Self-Tolerance and Felix Milgrom*. Transplantation Proceedings, vol.31, nr.3, maj 1999, s.1460-1463.

Schatz, D.G. (2004). *Antigen receptor genes and the evolution of a recombinase*. Seminars in Immunology, vol.16, nr.4, augusti 2004, s.245-256.

Silverstein, A.M. och Rose, N.R. (2000). *There is only one Immune System! The view from immunopathology*. Seminars in Immunology, vol.12, nr.3, 2000, s.173-178.

Simon, Z. Och Tatu, C.A. (1988). *Immunologic Tolerance: Self-nonself discrimination versus costimulatory factors and seconds signals.* Medical Hypothesis, vol.51, nr.1, 1988, s.1-3.

Skormin, V.A., Summerville D.H. och Moronski, J.S. (2003). Detecting Malicious Codes by the Prensence of Their "Gene of Self-replication". Proceedings in Computer Network Security, MMM-ACNS 2003, St. Petersburg, Ryssland, 21-23 september, 2003, vol.2776, s.195-205.

Sophos (2004). www.sophos.com.

Sophos (2004a). *Sophos virus analyses*. http://www.sophos.com/virusinfo/analyses/index_w.html

Stemler, S (2001). An overview of content analysis. Practical Assessment, Research & Evaluation, vol.7 nr.17.

Tauber, A.I. (2000). *Moving beyond the immune self?* Seminars in Immunology, vol.12, nr.3, juni 2000, s.241-248.

Pappersmaterial

Alberts, B., Johnson, A., Lewis, J., Raff, M., Roberts, K. och Walter, P. (2002). *Molecular Biology of The Cell*. Garland Science. New York, USA.

Benjamini, E., Sunshine, G. och Leskowitz, S. (1996). *Immunology A short Course.* Wiley-Liss. New York, USA.

Bernard, H.R. (2000). *Social Research Methods – Qualitative and Quantitative Approaches*. Sage Publications. Thousand Oaks, California, USA.

Bowler, P.J. (1992). *The Environmental Sciences*. W.W. Norton & Company. New York.

Bryman, A. (2004). *Social Research Methods*. Oxford University Press, Oxford England.

Fielding, N.G. och Fielding, J.L. (1986). *Linking Data*. Sage Publications. Newbury Park, California, USA.

Flick, U. (1998). *An Introduction to Qualitative Research*. Sage publications, London, England.

Graziano, A.M och Raulin, M.L. (1989). *Research Methods – A Process of Inquiry*. Harper & Row. New York.

Guyton, A.C. och Hall, J.E. (2000). *Textbook of Medical Physiology*. W.B. Saunders. Philadelphia, Pennsylvania, USA.

Hempel, C. (1969). *Vetenskapsteori*. Studentlitteratur. Lund.

Silverman, D. (2001). *Interpreting Qualitative Data – Methods for Analysing Talk, Text and Interaction*. SAGE Publications. London.

Vander, A., Sherman, J. och Luciano, D. (1998). *human physiology The Mechanisms of Body Function. McGraw-Hill*. Boston, Massachusetts, USA.