



Krigsvetenskap - metod och självständigt arbete (18 Hp)

<i>Författare:</i> Oskar Åkergren	<i>Program & kurs</i> OP 09-12, 1OP147
<i>Handledare:</i> Niklas Stenlås	
	<i>Antal ord:</i> 10 367
En nations åverkan av en cyberattack - En fallstudie på cyberattacken mot Estland	
Sammanfattning: I denna uppsats beskrivs en fallstudie på överbelastningsattacken mot Estland 2007, där attackens skeden redovisas samt visar på vilka åtgärder som vidtogs för att stoppa attacken, samt på vilket sätt attacken drabbade Estlands befolkning. Därefter analyseras attacken med hjälp av Richard Stiennons teori, om cyberkrigets fyra pelare. Avslutningsvis diskuteras de två frågorna som rör; vilka möjligheter en nation har när det kommer till försvar mot cyberattacker samt vad som kan tänkas räknas som militära problem. Syftet med uppsatsen är att visa på hur en nation drabbas, när den blir utsatt för en cyberattack och vilka handlingsåtgärder som är möjliga att vidta. Resultatet visar på att sättet Estland drabbades på, var att nationen var tvungen att isolera sig från det internationella internet, men att internet inom nationen kunde upprätthållas. Diskussionen mynnar ut i att en nation har mycket få handlingsmöjligheter till att försvara sig själv, när det kommer till cyberattacker från aktörer som inte är andra nationer. En viktig slutsats var att fallet Estland inte var ett militärt problem, utan kunde lösas helt civilt	



The harm on a nation from a cyber attack

- A case study on the cyber attack against Estonia

Abstract

This thesis describes a case study on the Distributed Denial of Service attacks against Estonia in 2007. The attack phases are presented, what counter measures were taken to stop the attack and of how the attack affected the Estonian population. The thesis then analyzes the attack with the help of Richard Stiennons theory, the four pillars of cyberwar. Finally, a discussion in the two topics; which options a nation have when it comes to defend itself against cyber attacks and what might count as military problems.

The purpose of this thesis is to show how a nation is affected when it becomes a victim of a cyber attack, and what courses of action are possible for the nation to take to be able to defend it self. The results shows that the way Estonia was affected, was that the nation had to isolate itself from the international internet, but the internet within the nation could be maintained. The discussion concludes that a nation has very few possibilities of actions to defend itself, when it comes to cyber attacks from actors, who are not other nations. An important conclusion was that the case of Estonia was not a military problem, it was solved completely civilian.



Innehåll

Innehåll.....	3
1 Inledning.....	4
1.1 Bakgrund	4
1.2 Syfte	5
1.3 Forskningsläge	5
1.4 Frågeställning	7
1.5 Avgränsningar	7
1.6 Metod	8
1.7 Källor och källkritik	8
1.7.1 Böcker	8
1.7.2 Artiklar	9
1.8 Teori	9
1.8.1 Underrättelse	10
1.8.2 Teknologi	10
1.8.3 Logistik.....	12
1.8.4 Ledning.....	12
1.8.5 Diskussion kring teorin	12
1.9 Definitioner av centrala begrepp	12
2 Redovisning.....	15
2.1 Fallstudie Estland	15
2.1.1 Bakgrund	15
2.1.2 Attacken	16
2.1.3 Motåtgärder	17
2.1.4 Följdverkan.....	18
2.1.5 Efterspel	18
2.1.6 Diskussion kring fallstudien.....	19
2.2 Applicering av teori.....	20
2.2.1 Underrättelse	20
2.2.2 Teknologi	20
2.2.3 Logistik.....	22
2.2.4 Ledning.....	22
2.2.5 Diskussion kring appliceringen	23
3 Diskussion och slutsatser	24
3.1 Vilka möjligheter till försvar mot en cyberattack har en nation?.....	24
3.2 Ett militärt problem?	26
Slutsatser	27
Förslag på vidare forskning.....	27
Källor och litteratur	28
Bilaga 1	29



1 Inledning

1.1 Bakgrund

I en allt mer datoriserad värld förlitar vi oss dagligen på tillgången till internet. Vi sköter allt fler sysslor över internet, allt ifrån bankärenden till resebeställningar och informationsinhämtning. I Finland har tillgängligheten till en bredbandsuppkoppling till internet, klassats som en mänsklig rättighet. Frågan som uppstår är då, hur skyddat är internet från attacker, som har till syfte att omöjliggöra åtkomsten till de tjänster som vi tar för givet?

Prefixet "cyber" är hämtat från ordet cybernetik som härstammar från det grekiska ordet cybernetikos. Cybernetiks första användning i modern tid, är för det akademiska området cybernetik som vi i Sverige benämner som styr- och regler teknik. Termen cybernetik definierades redan på slutet av 1940-talet, men det var författaren William Gibson som började använda termen cyberrymden i slutet av 1980 och gav ordet den innebörd som vi idag ser ordet som.

Cyber är idag ett prefix för att benämna den virtuella värld som byggs upp av datorer, servrar och deras kommunikation mellan varandra. Skillnaden mellan att använda sig av cyber och internet som prefix, är att läsaren riskerar att låsa sig till "World Wide Webb" när termen internet används och se attacken så som att det är själva sidorna som blir utsatta. Cyber som prefix är bredare än så. Cyber inkluderar WWW, men även den telekommunikations- och datateknik, som vi inte kan se, men som är nödvändiga för att upprätthålla kommunikationen, distributionen och administrationen av det vi kallar för internet.

Fenomenet med cyberattacker är, i militära sammanhang, relativt nytt men är inte helt okänt. Redan under Kosovokonflikten 1999 drabbades NATO av en cyberattack som resulterade i problem med deras e-posthantering och att deras webbplats låg nere i tio dagar.¹

Sedan 1999 har användandet och beroendet av internet ökat oerhört mycket. I och med att allt mer data lagras och hanteras på internet, så ökar både intresset och värdet av att komma över denna data. På grund av det ökade värdet av denna data ökar även säkerhetsbehovet. USA har tagit steget att införa U.S. Cyber Command i och med det möjliga hot som en cyberattack kan innebära. Med anledning av det uppfattade hotet har USA, utöver införandet av USCC, tillkännagivit cyberrymden som en ny arena för krigföring.

Fastslagna internationella definitioner saknas kring cyberattacker, vilket gör det oklart kring vilka befogenheter en nation har, för att försvara sig mot ett cyberangrepp. Oklarheten beror till mångt och mycket till att cyberattacker inte faller naturligt under definitionen väpnat angrepp som FNs resolutioner bygger på. Även om en cyberattack inte kan räknas som ett väpnat angrepp, kan en cyberattack komma att få sådana effekter att delar av en nation att stanna upp.

Jag vill i denna uppsats beskriva hur en cyberattack kan slå mot en nation, hur en cyberattack är uppbyggd och vilka åtgärder som går att vidta för att försvara sig mot en cyberattack.

¹ Riegert, 2002, s. 32-33



1.2 Syfte

Syftet med uppsatsen är att analysera en cyberattack riktad mot en nation, sett ur en militär synvinkel samt att visa på vilka följder attacken leder till för det civila samhället. Vidare syftar uppsatsen på att föra en kortare diskussion kring problematiken med cyberattacker och rådande internationella resolutioner.

1.3 Forskningsläge

Det har bedrivits forskning inom områden som berör cyberattacker och cyberkrigföring, dock främst med inriktning på det rent militära delarna. Forskningen är i mångt fokuserad på hur cyberattacker ska implementeras i den militära verksamheten eller hur försvaret ska skydda sig från militära cyberattacker. Mitt perspektiv på denna uppsats är hur en nation drabbas när nationen blir utsatt för en cyberattack. Den tidigare forskningen är inte helt är överensstämmande med mitt arbete, dock finns det intressanta delar som jag har tagit till mig.

Uppsatser och böcker

Den internationella forskning som har använts i denna uppsats består av tre böcker skrivna av: Richard Stiennon, säkerhetsexpert och grundare av det oberoende analysföretaget, IT-Harvest; Jeffrey Carr, cybersäkerhetsanalytiker och grundare av projektet Grey Goose som undersöker cyberkonflikter via öppna källor samt Kenneth Geers som skriver sin bok för NATO Cooperative Cyber Defence Center of Excellence.

Stiennon beskriver i sin bok *Surviving cyberwar*, ingående om olika metoder som kan komma att nyttjas i ett cyberkrig. Stiennon ger flertalet exempel på handlingar som skett och kan betecknas som cyberattacker. Stiennon redovisar en teori som enligt honom ska vara en guide för att tillskansa sig en total informationsdominans under ett cyberkrig.

Carr skriver i boken *Cyber warfare* i detalj om problemet med cyberattacker kontra den internationella lagstiftning som finns idag, rörande rätten att tolka cyberattacker som en krigshandling.

Geers skriver i boken *Strategic cyber security*, om två fallstudier av cyberattacker samt resultatet av en övning inom cyberförsvaret. Resultatet av undersökningen analyseras genom att nyttja Sun Tzus "Art of War" teori.

Det svenska forskningsläget, har jag byggt på tre uppsatser skrivna av officersstuderande på FHS samt en rapport utgiven av Krisberedskapsmyndigheten KBM.

Linda Kits, officersprogrammet 07-10, skrev i sitt självständiga arbete 2010 om "De Grundläggande Förmågorna vs Cyberterrorism". Uppsatsen fokuserar på hur ett cyberangrepp mot Försvarmaktens ledningssystem, det tänkta nätverksbaserade försvaret (NBF), skulle påverka Försvarmakten, sett ur de sex grundläggande förmågorna.

Kits uppsats har ett annat perspektiv än den som jag avser skriva, då Kits skriver om en attack riktad direkt mot en försvarsmakt, medan min uppsats avser behandla en attack riktad mot en nation generellt.

Mattias Hansson skrev 2002 en uppsats med titeln "Försvaret mot cyberkrigföring" som handlar om, ett då framtida behov, av förmågan att motstå cyberattacker. Uppsatsen skrevs 2002 och



behandlar försvarets behov av en cyberförsvarsförmåga 2010. Hansson beskriver hur ett mer IT-baserat samhälle blir mer sårbart och att det blir svårare för Försvarsmakten att överblicka alla de olika privata aktörer som de svenska isp:erna utgör.

Uppsatsen är fokuserad på Försvarsmakten och dess förmåga att hantera en cyberattack och är inte direkt kopplad mot någon genomförd cyberattack. Att uppsatsen inte är direkt kopplad till en attack är förklarligt, med tanke på när den är skriven.

Harry Kantola skrev 2011 på HSU en uppsats med titeln ”Datanätverksattacker, trend eller nödvändighet?”. Kantolas uppsats är inriktad på vilken förmåga försvarsmakter runt om i världen besitter för att genomföra cyberattacker.

KBM, idag omstrukturerad till myndigheten för samhällsskydd och beredskap MSB, har skrivit en rapport om cyberattacker och dess inverkan. I den rapport jag tagit del av genomförde KBM en fallstudie på cyberattacken på Estland och ställer den mot hur en liknande attack skulle drabba Sverige.

Författarnas slutsatser, resonemang och teser

Kantola diskuterar om förmågan att genomföra informationsinhämtning, försvar mot cyberattacker och att genomföra cyberattacker idag är fördelad på flera olika funktioner i den svenska försvarsmakten och att denna fördelning bör ses över. Vidare skriver Kantola att vid en omstrukturering bör ”samhällets andra aktörer inkorporeras”. Kantolas förslag till omstrukturering stämmer väl överens med Hansons slutsatser om att CNA och CND är ”intimt sammankopplade och bör ligga inom samma organisation”

Carr, Stiennon och Kits argumenterar, oberoende av varandra, kring problematiken runt avsaknaden av internationella vedertagna definitioner och resolutioner rörande cyberattacker. Kits påstår att skillnaden mellan cyberkriminalitet och –terrorism ligger i syftet med attacken,² medan Carr hävdar att det inte borde finnas en skillnad mellan cyberbrottslighet och andra typer av cyberkonflikter. Carr pekar på många av de hackare som är med och genomför stora cyberattacker även är involverade i cyberbrottslighet, hackarna ser på cyberkriminaliteten som deras dagliga värv för att få en inkomst. Dessutom så genomförs kriminella cyberattacker, i stora drag, på samma sätt som cyberkrigshandlingar.³

Geers och Carr resonerar båda om att nyttja olika konventioner som berör kärnvapenspridning och –användning för att kunna stoppa spridning av viss skadlig kod och rättfärdiga att handlingar vidtas mot den som står bakom attacken. Den stora utmaningen här är att enskilda individer kan besitta tillräcklig kunskap för att skapa och nyttja dessa system, trots eventuella internationella konventioner.

Genom att individer har kapaciteten att slå mot kända system, med hjälp av mängder av metoder, så hävdar Geers att attackerare har ett övertag mot försvarande nationer, på grund av det stora antal tekniker och möjligheter som finns att utföra attacker på och hur olika mjukvaror utvecklas och är mottagliga för attacker. En nation har helt enkelt för många olika uppsättningar av system och mjukvaror för att uppnå en fulländad övervakning.

² Kits, 2010, s. 14

³ Carr, 2011, s. 5



Geers resonerar kring att det finns tre huvudtyper av cyberattacker, där de olika attackerna används för att uppnå olika mål.

Den första typen riktar sig mot tillförlitligheten hos den data som kommuniceras eller lagras, det vill säga att lyssna av eller inhämta känslig data och information.

Den andra typen av cyberattacker riktar sig mot integriteten hos datan, där målet oftast är att ändra eller förstöra data.

Det tredje typen riktar sig mot tillgängligheten, där syftet med attacken är att förhindra åtkomsten av den data som finns.

Carr beskriver att det måste till resolutioner som kan avkräva att nationer att lämna ut eller straffar individer som hjälper till i stora attacker. Utan sådana resolutioner kommer hackers kunna gömma sig i nationer som inte ser ner på deras aktiviteter.

1.4 Frågeställning

Frågeställningen som jag avser att besvara i denna uppsats, kommer att framför allt handla om cyberattacken mot Estland och hur Estland påverkades. Vidare kommer jag att ta upp det rättsliga dilemmat som kan uppstå vid just en cyberattack då fenomenet är relativt nytt, sett ur en militär synvinkel, och att vedertagna internationella definitioner saknas.

Hur var cyberattacken mot Estland uppbyggd och vilka konsekvenser fick attacken för det Estniska samhället?

- Hur genomfördes överbelastningsattacken mot Estland?
- Vilka möjligheter till försvar mot en cyberattack hade Estland?
- Var cyberattacken ett militärt problem?

1.5 Avgränsningar

Jag kommer att i denna uppsats fokusera på överbelastningsattacker, den tredje typen av cyberattacker enligt Geers, för att den attacktypen intressant ur ett rättsligt perspektiv. Denna typ av cyberattacker kan komma att slå mot civila i en nation och störa ut stora delar av IT-infrastrukturen, men utan att utgöra ett hot mot nationens säkerhet, vilket gör att användandet av militära enheter kan bli diskutabelt. En annan intressant aspekt av överbelastningsattacker är att överbelastningsattacker kan verka väldigt effektfulla, med tanke på den mängd trafik som nyttjas när hemsidor sänks, men vilken skada och verkan uppnås verkligen genom denna typ av attacker?

Jag fokuserat på en fallstudie av cyberattacken mot Estland då det var en av de första stora cyberattackerna som genomfördes och som skapade stora konsekvenser. Tidigare cyberattacker hade genomförts, till exempel Kosovokonflikten 1999, där NATO tappade viss effekt i och med att de fick problem med sin e-posthantering. Detta problem berörde dock endast NATOs egen e-posthantering och resulterade inte i ett tillräckligt stort problem för att attacken skulle påverka Kosovoinsatsen i stort.



1.6 Metod

Som metod för denna uppsats har jag valt att genomföra en fallstudie av cyberattacken mot Estland.

Anledningen till att jag väljer att göra en fallstudie, är att jag vill visa på ett faktiskt exempel av en nation som blir drabbad av en cyberattack. Jag kommer analysera attacken och visa på hur den genomfördes och redovisa på vilka effekter som attacken i självverket ledde till.

Motivet till fallet Estland är flera. Estland var vid tidpunkten för anfallet en långt utvecklad IT-nation med mycket god IT-infrastruktur. Attacken skedde under fredstid och var både omfattande och mycket väl organiserad.

Jag kommer att genomföra fallstudien genom att använda mig av flertalet tryckta källor som redovisar cyberattacken mot Estland, sedan lägga samman dem för att få en god bild över händelseförloppet.

1.7 Källor och källkritik

1.7.1 Böcker

Sveriges beredskap mot nätangrepp

Boken är skriven av den svenska krisberedskapsmyndigheten, nuvarande myndigheten för samhällsskydd och beredskap. Även om det inte anges direkta referenser i boken, står det i förordet att informationen har tagits fram med hjälp av ”estniska myndigheter och från personer med speciell insikt i hur hantering av nätincidenter fungerar”⁴. Enligt min bedömning ser jag inga konstigheter i trovärdigheten hos denna publikation.

Kampen om det kommunikativa rummet

Boken är skriven av Kristina Riegert för ”Styrelsen för psykologiskt försvar” och behandlar informationskrigföring under Kosovokonflikten, i syfte att se vilka lärdomar det svenska civila försvaret skulle kunna dra. Jag ser boken som saklig och ser inga konstigheter att använda den som källa.

Surviving Cyberwar

Stiennon tar upp fallet Estland i sin bok och redovisar kortfattat händelseförloppet.⁵

Jag har valt att inte inkludera Stiennon som källa i min fallstudie då jag upplever honom som tendensiös med citat som ”the technical community of Estonia found it self enlisted in an ad hoc team to counter the Russian cyber attacks” och med ett tonfall som riktar anklagelser mot Ryssland, trots att inga bevis finns för att Ryssland låg bakom attacken.

Däremot har han intressanta tankar och idéer kring cyberkrigföring och jag har valt att använda mig av hans teori av cyberkrigföring, då dessa uppgifter inte är beroende av Stienmons tendens.

⁴ KBM, 2008, s. 6

⁵ Stiennon, 2010, s.85-90



1.7.2 Artiklar

De två artiklar som jag använder som källor är: ”Estland under attack” återfinns i tidningen *TechWorld*, nr 2 2012 och “Hackers Take Down the Most Wired Country in Europe” *Wired Magazine*: Issue 15.09, 2007.

Tidningarna är inga vetenskaplig tidskrifter utan är tidskrifter inriktade på teknik och utveckling inom data och datorteknik . Det som artiklarna bidrar med, är intervjuer med högt uppsatta personer inom IT området i Estland, vid tiden för attacken. Personerna, vilkas intervjuer behandlas i den här uppsatsen är: Anto Veldre, Ago Väärssi och Alexey Salnikov.

Veldre jobbade vid tiden för attacken som informationssäkerhetschef för Danske Bank i Estland och med goda kontakter med CERT-EE och stöttade deras arbete under attacken. Intervjun ägde rum 2012 för tidningen TechWorlds räkning.

Väärssi var vid tiden för attacken IT-chef över tidningen Postimees, en av Estlands största tidningar. Intervjuades av tidningen *Wired* 2007.

Salnikov var vid tiden för intervjun vice direktör för ”Institute of Information Security Issues” vid universitetet Lomonosov i Moskva. Intervjun med Salinkov får visa på en bild kring hur Ryssland ser på cyberattacker. Även Salinkov intervjuades av *Wired* 2007.

Det är dessa intervjuer som jag använder som material och jag hävdar att dessa källor bör ses som tillförlitliga i form av den information personerna hade tillgång till. Det finns en risk att Veldre och Väärssi kan ses som partiska, men jag hävdar att intervjuerna är av den natur att detta inte ger någon större inverkan. Salinkovs intervju är till för att belysa problemet ur en rysk synvinkel och är därmed av naturen partisk.

1.8 Teori

Detta avsnitt (1.8) är min översättning av den teori som presenteras av Richard Stiennon och är i denna uppsats något förkortad då jag inte inkluderat samtliga exempel Stiennon tar upp i boken.⁶

Stiennon skriver i sin bok ”Surviving cyber war” om cyberkrigets fyra pelare och hävdar att dessa är de medel som behövs för att uppnå total informationsdominans. Pelarna ska fungera både en guide och en varning till nationer som förbereder sig för cyberkrig.⁷

Pelarna är intressanta för tre av fyra återfinns, åtminstone som namne, i de sex grundläggande förmågorna. Dessa grundläggande förmågor är det analysverktyg som försvarsmakten har för att analysera en motståndare av en traditionell karaktär, men även visat sig möjlig att applicera på både cyberterrorism och irreguljära förband. Pelarna i Stiennons teori är underrättelse, teknologi, logistik samt ledning.

⁶ Stiennon, 2010, s. 115-130

⁷ Ibid., s. 115



1.8.1 Underrättelse

Stiennon skriver att en effektiv underrättelseinsamling, kommer att ge nationer information som skapar fördelar i flera arenor. Han delar in pelaren i tre underrubriker; politisk underrättelseinsamling, vapenunderrättelse och militär underrättelse.

Politisk underrättelseinsamling

Genom att samla in underrättelser kring vad motståndaren tänker, planerar och genomför, kan en underrättelseoperation bidra med kritisk information vid viktiga tillfällen. För att förbereda sig inför diplomatiska möten, behövs en god uppfattning kring världsläget och en förmåga att kunna se ur varje parts perspektiv när det kommer till förhandlingar.

Vapenunderrättelse

Genom att komma åt underrättelser avseende vapenutveckling, kommer även svaga stater ha en förmåga att förbereda sig och utveckla motangrepp mot smartare vapensystem. Beroende på vilken sorts underrättelse som operationerna kommer åt, kan det vara möjligt att kopiera de vapensystem som är under utveckling, utan att själv ha behövt investera i utvecklingskostnaderna.

Militär underrättelse

Stiennon skriver att underrättelseområden som; motståndarens militära organisation, individerna i denna organisation, antalet soldater deployerade, fördelning av resurser och beredskapsgrad hör till militära underrättelser.

Traditionellt har denna underrättelse-inhämtning skett genom signalavlyssning och spionage, men genom internets utveckling, sänds väldigt mycket av denna information över internet.

Stiennon skriver vidare att en e-postserver är en av de främsta målen för en cyberspion. Genom att kontrollera en e-postserver, kan attackeraren kopiera samtliga e-post som servern står för, blockera inkommande e-post och till och med ändra utgående.

1.8.2 Teknologi

Teknologi är den pelare som skiljer sig från de grundläggande förmågorna. Stiennon beskriver under denna punkt, elva områden att ta i beaktande inför cyberattacker. Dessa områden är:

1. Upptäckt och utnyttjande av sårbarhet

Alla applikationer och program som antingen tar emot eller skickar data (input/output, I/O) över ett nätverk, kan vara känsliga för utnyttjande. Beroende på hur programmet är programmerat, kan en hacker utnyttja svagheter i dess utformning och i värsta fall få fullständig kontroll över den utsatta servern.

2. Automatiserade attacker

Genom att skapa ett enkelt skript som utnyttjar kända svagheter hos målet, kan hela attacken automatiseras. Skriptet tar sig in hos sitt mål, letar upp relevant data, för över datan till angriparen och städar sedan upp de spår skriptet lämnat.



3. Ledningen av cyberattacker befinner sig i ett förstadium

Stiennon hävdar att de flesta cyberattacker fortfarande sköts av en ensam individ. Genom att leda en samtidig cyberattack mot flera mål och använda sig av flera olika metoder, kommer attacken att leda till större framgångar.

4. Skadlig kod

Genom virus och maskar kan sårbara datorer anslutas till botnät, helt utan att användaren vet om detta. Genom att vara ansluten till detta botnät kan datorn, när signal ges från nätets ägare, vara med och bidra till till exempel en överbelastningsattack.

5. Rootkits

Rootkit är en särskild form av skadlig kod. Denna kod lägger sig i operativsystemets kärna (kernel) och kan därigenom inte upptäckas av antivirus program. Rootkits är svårare att sprida än virus och maskar då den kräver en installation. Spridningen sker då främst genom programvaror som installerar rootkitet dolt, samtidigt som det avsedda programmet installeras.

6. Bakdörrar

Bakdörrar är öppningar i programvaror som är medvetna av den som skrivit programmet. Bakdörrar kan då användas för att installera skadlig kod eller komma åt den hårdvara till klienten som programmet är installerat på. Ett fall där USA anklagas för att använda sig av bakdörrar är inför första gulf kriget. Enligt anklagelserna ska skrivare som sålts till Irak haft bakdörrar som gjort det möjligt för USA att få insyn i Iraks ledningssystem före invasionen.

Bakdörrar kan mycket väl vara ett effektivt sätt att föra cyberkrig på, men det är inte sannolikt att tillverkare lämnar bakdörrar öppna i sina produkter. Skulle det visa sig att en bakdörr lämnats öppen genom en produkt som ett företag tillverkat, skulle förtroendet rasa för detta företag.

7. Analys

I och med den stora mängd data som kan komma att samlas in vid en cyberattack, kommer det att krävas omfattande analysarbete av datan. Genom att utveckla automatiserade analysverktyg kommer arbetsbördan att minska samt effektiviteten öka.

8. Överbelastningsattacker

Dessa attacker kan ta flera former men har samma syfte, att binda upp en server så att denna inte kan utföra sitt egentliga syfte.

9. Manipulera BGP anvisningar

BGP är det protokoll som visar vilka IP adresser som hör till vilken hemsida. Genom att felaktigt ange vilka IP adresser en viss hemsida har, kommer den rätta hemsidan att vara oåtkomlig. Skulle den hemsidan vara väldigt trafiktung till exempel Google, Facebook eller YouTube, kommer den som faktiskt äger Ipadresserna bli överbelastad.

10. DNS-attacker

DNS står för "Domain Name System" och en DNS-server är den server som sköter kopplingen mellan den webbadress som förs in i adressraden på webbläsaren och det IP nummer som servern har. Detta IP nummer är det som angivits enligt BGP protokollet. Genom att sänka DNSServerar kommer inte det gå att komma åt webbplatserna via deras



webbadresser utan endast via deras IP nummer, vilket i praktiken innebär att webbplatserna är oåtkomliga för allmänheten.

11. SCADA-attacker

SCADA är ett protokoll som sänder instruktioner och tar emot data från pumpar och ventiler som styr elcentraler, olje- och gaspipelines. Genom att utveckla verktyg som slår direkt mot denna infrastruktur skulle vara en stor fördel i en cyberkonflikt.

1.8.3 Logistik

Logistik är den tredje av Stienmons fyra pelare. I cyberattacker har logistiken fått en något annorlunda innebörd, jämfört med fysiska världen. Cyberlogistiken riktar sig mot nätverk och förbindelser i huvudsak. Offensivt ägnar sig cyberlogistiken med att säkerställa att det finns resurser att fortsätta attacken i form av öppna vägar i nätverken och söka alternativa vägar för attacken att gå. Cyberlogistiken har även till uppgift att skydda de vägar som attackerna levereras genom.

Som skydd för det egna nätet, har cyberlogistiken till uppgift att kontrollera att servrar och routrar endast kommunicerar med säkra källor. Genom att kontrollera detta går det att undvika att routrar blir påverkade av en BGP manipulation som annars kan sänka hela nationers nät.

1.8.4 Ledning

Stienmon hävdar att störa ut ledningsförmågor, är ett primärt mål för en cyberkrigföring som understödjer ett fullskaligt krig. Att utveckla förmågor att skydda ledningsstråken bör ligga i fokus för samtliga nationer eller organisationer som förväntar sig cyberattacker.

Att utveckla cyberattacker som slår mot motståndarens lednings infrastruktur, är en nyckelroll i cyberkrigföringens förmågor.

1.8.5 Diskussion kring teorin

Att Stienmon har ett militärt synsätt på cyberattacker är tydligt. De exempel på händelser som han tar upp, är ofta staters agerande mot antingen annan stat eller organisationer.

Teorin som Stienmon lägger fram liknar de sex grundläggande förmågorna, som jag tidigare nämnt. Jag anser att titeln "teknologi" skulle kunna jämföras med "verkan" då den pelaren beskriver olika tillvägagångssätt för att åsamka verkan hos en motståndare. De förmågor som då fattas är "skydd" samt "rörlighet" vilket jag ser som en fördel med denna teori. Eftersom en cyberattack inte tar form i den fysiska världen, skulle det bli väldigt långsökt att försöka analysera en cyberattack utifrån skydd och rörlighet

Jag tycker det är värt att notera att Stienmons fjärde pelare, ledning, riktar sig mot vikten av att slå mot motståndarens ledningsmöjligheter snarare än att beskriva sin egen förmåga till ledning. Den egna ledningen ingår i pelaren teknologi, område 3.

1.9 Definitioner av centrala begrepp

Krigföring

Krigföring är sättet att föra krig på. Krig i sin tur är något som stater för mot varandra, vilket gör att krigföring är en problematisk term när det kommer till cyberattacker. För att det ska



kunna klassas som cyberkrigföring måste det vara en stat som står bakom attackerna och dessa attacker ska i sin tur riktas mot en stat.

Attack

I den här uppsatsen använder jag termen attack som en aktiv handling, som avser att skada, störa eller spionera på en verksamhet.

Överbelastningsattacker

Överbelastningsattacker, även känt som Distributed Denial of Service (DDoS), syftar till att förhindra målet för attacken att blir nåbar. En överbelastningsattack genomförs genom att tvinga en server att skicka data, eller svara på anrop, till såpass många klienter att bandbredden tar slut. Genom att överbelasta servern på detta sätt, går det inte att använda servern till dess egentliga syfte, som till exempel att hålla uppe hemsidor.

Det finns många typer av DDoS attacker och de fungera olika bra, beroende på hur serverna de attackerar är uppbyggda.

Ett exempel på en vanlig DDoS-attack är att tvinga servern att svara på ping.⁸ Genom att pinga en server skickar du en signal och tvingar servern att svara, detta svar är inte särskilt stort, sett i data, men med en enkel kod kan en ensam användare tvinga en server att svara på 5000 förfrågningar med 1000 stycken paket i varje.⁹ Man kan enkel räkna ut att om många användare tvingar servern att svara på alla dessa ping kommer inte det finnas mycket bandbredd kvar att leverera tänkt data på.

Hacktevister

Ordet ”hacktevister” är en kombination av orden ”hacker” och ”aktivister”. En hacker är en individ som letar säkerhetshål i system och tränger sig sedan in i systemen för att kunna utföra en attack. Attackerna kan te sig olika beroende på syftet hos hackern.

En aktivist är en individ som aktivt deltar och är engagerad i en större rörelse.

Hacktevister är således individer som är engagerade i attacker mot system och samarbetar för att sänka systemet, eller på annat sätt åsamka skada. Det finns stora, mer eller mindre välorganiserade grupper av hacktevister som samordnar attacker. Exempel på sådana grupper som fått genomslag i internationellmedia är, Anonymous och Lulzsec.

Script kiddie

En script kiddie är en term för en hacktevist som deltar i attacker men utan att själv ha någon djupare kunskap eller förståelse för vad denne gör. En script kiddie bli ofta försedd med enklare skript att köra för att hjälpa till i en attack, men utvecklar inte egna skript eller söker säkerhetshål hos sin motståndare.

Skript

Ett skript är en enklare form av ett program och kan i sin enklaste form bestå av endast en handfull rader med kod.

⁸ Stiennon, 2010, s. 63

⁹ KBM, 2008, s.12



ISP

ISP är en förkortning som står för Internet Service Provider och är det företag som levererar och ansvarar för internetanslutningen till användare

Botnät

Botnät är en samling datorer, infekterade av en viss typ av maskar eller virus. Dessa typer av skadlig kod, gör att datorerna delvis kan fjärrstyras och därigenom tvingas delta i överbelastningsattacker. Personer eller grupper som utvecklar maskar som infekterar datorer att delta i botnät, tar sedan betalt av de organisationer som är intresserade av att nyttja tjänsten som en DDoS attack innebär.

CNA, CND

I Kantolas och Hanssons uppsatser används termerna CNA och CND vilka står för ”Computer Network Attack/Defence ” som beskriver cyberattacker och försvar av cyberattacker.

Port 80

Nätverkstrafik är indelad i olika portar där viss trafik är låst till en viss port. Port 80 är den port som trafiken för webbtrafiken går via.



2 Redovisning

2.1 Fallstudie Estland

2.1.1 Bakgrund

Befolkning

Estland är den nordligaste av baltstaterna och var en del av Sovjetunionen fram till 1991. I och med den sovjetiska historien, finns det idag en grupp om ca 400000 rysktalade personer i Estland. Dessa personer är av blandad ursprung, främst est-rysk, och de känner mer eller mindre tillhörighet till den Estniska nationen.

IT-utveckling

Tack vare frigörelsen från Sovjet, skapades nationen Estland helt fritt från gamla system. I och med frigörelsen i början på 1990-talet, låg vägen öppen för nationen att kunna skapa sig helt nya statliga och finansiella system, i den informationsålder som precis tagit fart.¹⁰

Estland har beskrivits som en nation som ligger i framkant av utvecklingen inom IT-infrastruktur och stora delar av dagliga ärenden sköts via internet. Framförallt inom bankväsendet har utvecklingen kommit långt, över 99% av alla banktransaktionerna görs via internet. Vidare sköter 92% av befolkningen sin deklaration över internet och det går även att rösta i parlamentsvalen genom internet.¹¹

2006 grundas organisationen The Computer Emergency Response Team of Estonia (CERT-EE). CERT-EE har till uppgift att sköta säkerheten inom topdomänen .ee och assistera estniska internet användare med implementeringen av förebyggande åtgärder för att minska eventuell skada från säkerhetsincidenter samt att hjälpa användarna på att möta säkerhetshot.¹²

Bronsstatyn

1941 reste Sovjetunionen en bronsstaty föreställande en rysk soldat och döpte monumentet till "Monumentet över Tallinns befriare". Statyn var centralt placerad och efter frigöringen från Sovjet börja den leda till delade känslor. Den ryska delen av befolkningen firade statyn varje år den 9 maj, för Sovjets seger i andra världskriget, men den estniska befolkningen såg monumentet som en symbol av det sovjetiska förtrycket. Dessa delade känslor ledde till bråk mellan de olika grupperna och 2006 fattades ett beslut att genomföra en flytt av statyn, till en krigskyrkogård belägen i en förort till Tallinn.¹³

Torsdagen den 26 april 2007 påbörjades förberedelserna inför flytten, av statyn, vilket ledde till omfattande kravaller i centrala Tallinn. Dessa kravaller ledde till bränder, plundring av butiker och ett dödsfall. Kravallerna fortsatte över helgen och på fredagskvällen den 27 april påbörjades cyberattacker.¹⁴

¹⁰ Städje, 2012, s.70

¹¹ Estonian Information System's Authority

¹² Ibid

¹³ KBM, 2008, s. 9-10

¹⁴ Ibid, s. 10-11



2.1.2 Attacken

De omfattande DDoS attackerna mot Estland skedde i tre vågor, där den första vågen slog till natten mot den 28 april, den andra vågen natten mot den 4 maj och den tredje natten mot den 9 maj. De välsynkroniserade höjningarna och sänkningarna av trafik som passerar, visar på att det var stora botnät som användes.

Första vågen

Natten mot den 28 april 2007 beskriver Anto Veldre, expert vid CERT-EE, hur det estniska nätet möttes av "en wall of sound".¹⁵ Han beskriver hur flera attacker sker simultant och är byggda på olika metoder. Han beskriver att normalt riktar sig en attack mot ett enskilt mål, medan denna attack var utformad för att lamslå hela samhället. Merparten av attacken bestod av så kallade script kiddie attacker och attacker baserade på botnät, vilket ledde till en väldigt stor åtgång av bandbredd.

IT-chefen för tidningen Postimees, Ago Väarsi, beskriver hur tidningens bandbredd konstant minskar och hur data som tar sig in till serverna får dessa att krascha och starta om sig själva. Han väljer att stänga av kommentatorsfunktionen hos tidningen och tjänar in bandbredd för en stund, men bandbreddsåtgången stannar inte upp utan fortsätter minska. Väarsi beskriver hur han ser attackerna ändra på sig och anpassa sig efter de filter som han själv sätter upp, vilket visar på en aktiv motståndare.¹⁶

Vid en analys av den inkommande trafiken till Postimees, visar det sig att det främsta landet som besöker tidningen är Egypten. De länder som följer är Vietnam och Peru. Väarsi, som vid det här laget börjar se att det här gäller en omfattande cyberattack, försöker öppna tidningens konkurrenters sidor, men även deras hemsidor ligger nere. Vid det här laget ser Väarsi ingen annan utväg än att blockera all utrikestrafik till och från tidningen. Genom denna blockad minskar bandbreddsåtgången betydligt och sidan går upp.¹⁷

Det genomfördes även attacker mot skolor och kommuner i den Estniska landsbygden, vilket kan tolkas som att den övergripande attacken var okordinerad och var ett verk av flertalet enskilda aktörer.¹⁸ Men beskrivningen av attacken mot Postimees talar mot denna tes samt de plötsliga ändringarna i bandbredd som brukas. Det visar snarare på att attacken var ett verk av hackteviser med god kännedom om hur attacker ska utföras och sedan spred enkla koder för så kallade script kiddies att använda för att hjälpa till i attacken.

Även om attacken alla tre vågor dominerades av överbelastningsattacker, genomfördes även några manipulationsattacker. Ett exempel på en sådan manipulationsattack är när hackare lyckades ta sig in på Reformparitets webbplats och placera en falsk officiell ursäkt för att statyn flyttades.¹⁹

I attacken deltog det även kompetenta hackers som försökte ta sig in i viktiga routrar hos isp:erna. Genom att komma in i isp:ernas routrar hade dessa hackers sedan kunnat komma åt det finansiella nätet, dock lyckades samtliga lågnivå attacker avvärjas enligt Veldre.²⁰

¹⁵ Städe, 2012, s. 72

¹⁶ Davis, 2007, s. 165

¹⁷ Ibid, s. 165

¹⁸ KBM, 2008, s. 13

¹⁹ Ibid, s. 11

²⁰ Ibid



Andra vågen

När nästa våg av överbelastningsattacker slår in mot Estland har myndigheterna hunnit organisera sig och är bättre rustade att stå emot attacken. Problemet är att även attackerarna har organiserat sig bättre.²¹

Denna attack riktar sig mot myndighetsservrarna och myndighetsnäten. Botnäten som används, har omplacerats till nationer utan incidenthanteringsorganisationen likt CERT, eller där incidenthanteringsförmågan är svag. Användandet av botnäten har i denna våg blivit bättre samspelt, vilket visar sig i förmågan att snabbt kunna rikta om näten mot enskilda mål.²²

Tredje vågen

Denna våg slår in natten mot den 9 maj och är större än de andra vågorna. En uppskattning av de datorer som deltar i denna attack uppgår till omkring en miljon²³ och är minst lika väl ledda som under den andra vågen. Attacken riktar sig mot en rad olika sidor, med en spännvidd från utrikesdepartementet till bankernas hemsidor och har kapaciteten att fylla ut hela Estlands bandbredd, vilket skulle plocka ner Estland från internet återigen.²⁴

Vid den här tidpunkten har dock CERT kommit i fas och kan avvärja effekterna av attacken redan innan den nått fram till Estland.

2.1.3 Motåtgärder

För att komma undan attacken valde CERT att den 29 april stänga av Estland från det övriga internet. På samma sätt som Postimees var tvungna att stänga av sig från trafik utifrån, var CERT tvungna att skära av hela Estlands internet. Detta handlingsätt var det enda som CERT hade att arbeta med för en snabb lösning för att kunna återinföra det estniska nätet.²⁵

Något dygn efter första vågen av attacken, organiserade estniska myndigheter en stab för att koordinera arbetet och skaffa en övergripande lägesbild. Det skickades ut information till internationella CERT organisationer för att skapa en möjlighet att filtrera datan redan innan den nått Estland.²⁶

CERT fick även hjälp av personer utifrån Estland som reste till Tallinn, personer godkända av de största ISP:erna med befogenheter att stänga av personer från internet.²⁷

Efter att Estland stängt port 80 och skurit av sig själva från internet, minskade den första vågen i omfattning, då den inte levererade någon effekt längre.

När den andra vågen slog till var myndigheterna väl organiserade och hade hög beredskap,²⁸ kapaciteten att koppla från internationella användare från internet infann sig dock inte förrän inför våg nummer tre.

²¹ KBM, 2008, s. 15

²² Ibid

²³ Davis, 2007, s. 169; KBM, 2008, s. 16

²⁴ Davis, 2007, s. 169

²⁵ Davis, 2007, s. 167; Städje, 2012, s. 73

²⁶ KBM, 2008, s. 14

²⁷ Davis, 2007, s. 167 - 168

²⁸ KBM, 2008, s. 15



Under den tredje och avslutande vågen kunde CERT kontrollera varifrån attackerna härstammade och med förmågan att koppla från användare från internet, var följderna av denna våg betydligt lägre.²⁹ Detta trots att attackens omfattning var större än de föregående vågorna.

2.1.4 Följdverkan

Hur påverkades då det estniska samhället av attacken?

Under den första vågen tog bandbredden slut för Estland, vilket innebär att hela deras internet låg nere, åtgärden som vidtogs då var att stänga av port 80. Eftersom Estland var tvungna att stänga av port 80 för omvärlden, kunde ingen trafik utanför Estland komma in, vilket betyder att det även var omöjligt att komma åt hemsidor utanför Estlands gränser.

Statoil fick problem med sitt betalnät och var tvungna att stänga ner detta nät under fyra dagar. Avstängningen av betalnätet resulterade i att inga köp gick att hantera med bank- eller kreditkort utan endast kontantbetalning kunde genomföras.³⁰

Mycket av den trafik som berör de finansiella systemen filtrerades via Finland vilket gjorde att bankärenden kunde skötas, om än långsamt, under större delen av attacken.³¹ Från utlandet var dock bankerna helt blockerade och trots filtreringen via Finland gick två banker ner helt periodvis under tidsperioden 10 – 15 maj.³²

Även e-postfunktionerna påverkades. Ett exempel är då Estlands parlament var tvungna att stänga sin e-postserver under 12 timmar, på grund av överbelastning, innan den kunde öppnas igen.³³

2.1.5 Efterspel

Som en följd av cyberattacken och dess verkan, reagerade NATO och frågor väcktes rörande om NATOs artikel 5 kunde vara applicerbar i dessa situationer. NATO valde att grunda en cyberförsvarscentra, Cooperative Cyber Defence Center of Excellence med uppgift att:

[CCD CoE:s] mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation.³⁴

Platsen för detta center blev just Tallinn, Estland.

CERT-EE utvecklades från att ha varit en mer informell klubb snarare än en myndighet, till att strukturera upp hierarkin och skapa noggranna listor kring nyckelpersoners kontaktuppgifter.³⁵

²⁹ Davis, 2007, s. 169

³⁰ Städje, 2012, s. 73

³¹ Ibid, s. 73

³² KBM, 2008, s. 16

³³ Ibid, s.13

³⁴ NATO Cooperative Cyber Defence Center of Excellence

³⁵ Städje, 2012, s. 71-73



2.1.6 Diskussion kring fallstudien

Inget självklart syfte

Att cyberattackerna skedde till en följd av flytten av bronsstatyn, är en slutsats dragna av de författare som refererats, dock har inte syftet med attacken kunnat presenterats. Det presenterades nämligen aldrig en klar kontext till, varför attackerna skedde, från attackerarna, annat än att visa sig patriotisk inför det ryska samhället.³⁶ Det skickades inga hotelsebrev så det var ingen utpressning,³⁷ utan hela attacken verkar vara en form av show of force.

Nätverkande

Cyberattacker är ett internationellt problem vilket fallet Estland visar och en av de största lärdomarna från Estlands cyberattack, är att ett internationellt samarbete är nyckeln för framgång.³⁸ Genom att skapa sig ett stort kontaktnät, samarbeta och visa sig tillförlitlig, kan en organisation knyta kontakter med organisationer så som ISP:ers och CERT i andra länder. Genom ett samarbete, skapas det en möjlighet att bygga det förtroende som krävs, för att kunna fatta snabba beslut, om till exempel att stänga av användare som är delaktiga i cyberattacker, från internet.

Om samarbetet inte funnits, kommer det att ta tid att visa på att nationen verkligen är utsatt för en cyberattack. Vidare kommer det att bli tidskrävande att visa på att din organisation verkligen är tillförlitlig och inte är ute efter att stänga av obekväma användare från internet.

Polisens huvudvärk

Absoluta merparten av attackerna kom utanför Estlands gränser, men det fanns vissa attacker som kom inifrån. Genom ett bra samarbete i den organisation som sattes upp för att hantera cyberattacken, lyckades adresserna tas fram till de attacker som härstammade från Estland och polisen lyckades gripa den misstänkte. Detta gripande avskräckte fler hacktevester att visa sitt missnöje på internet inifrån Estland och attackerna sjönk till en mycket låg nivå.³⁹

Det stora problemet som uppstod nu är att polisens befogenheter stannar vid den Estniska gränsen. Många av de hacktevester som identifierats var från Ryssland, men det vidtogs inga särskilda åtgärder från Rysslands sida att leta upp dessa hacktevester och ställa dem inför rätta.⁴⁰

Öppnande av gränserna och attacker övertiden

Jag har i texten beskrivit att Estland stängde av sig helt från omvärlden under den första attacken, men det beskrivs inte när de öppnade upp sig igen. Det finns inget som säger exakt när de öppnade upp sig igen för omvärlden, men de har gjort det i omgångar eftersom nya attacker har lyckats letat sig in.

Min egen tanke kring detta är att Estland stängde av sig från omvärlden när de stora vågorna rullade in och öppnade upp sig igen när de största attackerna i vågen var över, för att stänga igen när nästa våg kom. Det framkom också att det pågick mindre attacker övertiden,⁴¹ men

³⁶ Davis, 2007, s. 168

³⁷ Stådje, 2012, s. 72

³⁸ Ibid, s. 73-74

³⁹ KBM, 2008, s. 15

⁴⁰ Davis, 2007, s. 182

⁴¹ KBM, 2008, s. 17-18



dessa attacker är inte alls av den magnitud som de tre vågorna och därav kan de hanteras på ett annat sätt.

Ett troligt scenario är att de mindre attackerna valde att attackera massmedia, eftersom media upplevde ett väldigt tryck på sina servrar i de stora vågorna, samtidigt som de började få slut på material att jobba med,⁴² medan de tre stora vågorna hade som mål att sänka Estland som helhet.

2.2 Applicering av teori

Jag kommer i det här avsnittet (2.2) applicera Stienmons teori på fallstudien av Estland och genom detta analysera hur attacken var uppbyggd. Jag kommer att behandla de fyra pelarna var för sig, i den turordning som de presenterades i teorin och avsluta avsnittet med en diskussion kring resultatet av analysen.

2.2.1 Underrättelse

Det Stienmon beskriver i sin pelare underrättelse, är väldigt fokuserat kring traditionell militär underrättelseinhämtning. Ingenting i cyberattacken mot Estland tyder på att någon sådan traditionell underrättelseinhämtning skedde, vilket jag ser som naturligt eftersom attacken inte var del i en större krigshandling eller förberedde en sådan. Med det sagt så anser jag att det ändå skedde en form av underrättelsearbete under attacken, eller framförallt innan attacken slog till. Veldre beskriver hur attacken riktar sig mot flera punkter som oftast inte angrips i en vanlig överbelastningsattack utan att attackerarna visste vad de höll på med. Attackerarna visade kännedom om hur ett samhälle var uppbyggt och fungerade, något som inte var brukligt för hackteviser vid tiden för attacken.⁴³

2.2.2 Teknologi

1. Upptäckt och utnyttjande av sårbarhet

Cyberattacken utmärkte sig genom att vara en överbelastningsattack, men det har även bekräftats att det skedde avancerade, långsamma och långtgående lågnivå attacker som försökte tränga in i ISP:ernas servrar. Dessa attacker är exempel på när en svaghet i ett system hittats och nyttjas. Hade attacken gått tillräckligt långt fanns det en risk att hela, eller del av, det finansiella nätverket hade blivit exponerat och hamnat under kontroll av attackerarna.

Ett annat exempel på ett utnyttjande av sårbarhet är när hackers lyckades komma in och manipulera information som publicerats på Reformparitets hemsida.

2. Automatiserade attacker

Det tillvägagångssätt som Stienmon beskriver för detta område är något som inte användes under attacken mot Estland. Stienmon har här ett synsätt som att en angripare är intresserad av att inhämta data från en motståndare, något som inte var fallet under denna cyberattack.

Sett till titeln på området ”automatiserade attacker”, så stämmer delar av attacken in på denna beskrivning. De skript som skrevs,⁴⁴ möjliggjorde för skript kiddies att enkelt utföra automatiserade angrepp som del i den stora överbelastningsattacken.

⁴² Städje, 2012, s. 73

⁴³ Ibid, s. 72

⁴⁴ KBM, 2008, s.12



3. Ledningen av cyberattacker befinner sig i ett förstadium

Hur attacken leddes är inte helt klarlagt. Den information som finns, beskriver hur delatagare lägger upp information på forum runt om på internet. Information om vilka mål som attacken kan rikta sig mot och hur man ska gå tillväga för att delta. Denna metod visar på att cyberattacken inte var ett enmansuppdrag, utan att flera individer var med i attacken, vilket fyller upp Stiennons definition av detta område.

Mycket tyder på att ledningen av attacken var mer komplex än enbart informationsspridning via internetforum. De stora botnäten som användes under attacken, nyttjades samspelt och synkroniserat. Angreppsmålen kunde skiftas med enbart sekunders mellanrum och attackmetoderna lika så.⁴⁵ För att lyckas med denna samordning behövs en bra ledningsförmåga och kommunikationsmöjligheter.

4. Skadlig kod

Attackerarna spred ingen skadligkod själva, i form av maskar eller virus, däremot nyttjade hacktevisterna datorer redan smittade med skadlig kod. Dessa smittade datorer blev ihopkopplade till botnät som deltog i överbelastningsattacken.

5. Rootkits

Det finns inget som visar på att rootkits användes under denna attack och med tanke på attackens natur, fyller rootkits inget egentligt syfte. Attacken skedde helt på distans, vilket gör att det är väldigt svårt att implementera ett rootkit hos en klient.

6. Bakdörrar

Det finns inga rapporter om att det ska ha funnits bakdörrar lämnade öppna för exploatering i de system som var mål för attacken. Jag finner det osannolikt att det finns några bakdörrar i systemen med tanke på den kritiska infrastruktur som systemen uppehåller och vilken prestigeförlust det skulle innebära för de företag som producerat produkterna.

7. Analys

Detta område riktar sig främst mot cyberattacker som har föravsikt att inhämta data och information. Detta var inte naturen av denna cyberattack utan det underrättelsearbete som skedde kring denna attack skedde främst innan attacken inleddes, vilket diskuterats ovan i 2.2.1 Underrättelse.

8. Överbelastningsattacker

Överbelastningsattacker var själva kärnan i cyberattacken mot Estland. Det genomfördes massiva attacker med kapacitet att mätta hela Estlands bandbredd och genomfördes med flera olika tillvägagångssätt.

Det cirkulerade skript som utförde enkla ping-attacker mot serverar vilket gjorde det enkelt för script kiddies att hjälpa till i attacken, men det har också dokumenterats attacker baserade på SYN vilket är betydligt svårare att skydda sig emot.⁴⁶

9. Manipulera BGP anvisningar

För att ha möjlighet att manipulera BGP anvisningar måste ändringen komma från antingen

⁴⁵ KBM, 2008, s. 15

⁴⁶ Ibid, s. 18



en ISP eller från det företag som har fått IP numren tilldelade. Denna typ av attack var inte del i attacken som träffade Estland.

10. DNS-attacker

Inga attacker som kopplas till cyberattacken Estland riktades mot DNS-servrar, enligt den litteratur som jag tagit del av.

Att attackera en DNS-server kan vara ett trubbigt instrument, då en server kan vara ansvarig för upprätthållandet av väldigt många webbplatser. Skulle en DNS-server bli sänkt, kan den dra med sig många platser som inte var mål för attacken och därmed rikta oönskad uppmärksamhet från omvärlden mot attackerarna.

En DNS-server är även dimensionerad för att klara av att hantera stora mängder anrop, eftersom serverns uppgift innebär att den anropas varje gång någon matar in en webbadress som den ansvarar för. Kapaciteten att klara av stora mängder anrop leder till att en DNS-server är svårare att sänka, än en webbplats som inte förväntar sig stora mängder anrop.

11. SCADA-attacker

Inte heller några SCADA-attacker genomfördes under denna cyberattack. För att komma åt SCADA-protokoll behövs avancerade lågnivåattacker och med tanke på denna cyberattacks natur var dessa lågnivåattacker inte aktuella. De former av lågnivåattacker som nämnts tidigare, riktade sig mot ISP:erna och inte mot de företag och myndigheter som sköter el, vatten motsvarande.

2.2.3 Logistik

Det finns tydliga tecken på att de individer som ledde cyberattacken mot Estland var medvetna om vikten av effektiv cyberlogistik och hur logistiken skulle nyttjas.

Exemplet med tidningen Postimees visar på att attackerarna känner av vilka av deras attacker som når fram till målet och när dessa blockeras byter attackerarna väg genom nätverket.

Veldre beskriver att det tog en timme för CERT att skriva och implementera en svartlista för att blockera IP-adresser vid tiden för attacken. Attackerarna analyserade motåtgärderna och började således byta IP-adresser på just timbasis för att nätet inte skulle bli blockerat för dem.⁴⁷

Vidare exempel på att säkerställa att attackerna når fram, är att botnäten byter plats efter första attacken. Botnäten omplaceras från nationer som har en organisation motsvarande CERT, till nationer som saknar en motsvarighet eller där organisationen är svag.

2.2.4 Ledning

Motståndarens ledningsförmåga, i detta fall Estniska statens ledningsförmåga, påverkades till viss del. Som nation blev Estland oförmögen att kunna rapportera till omvärlden via internetbaserad massmedia vad som skedde, eftersom de var tvungna att isolera sig för att undgå attacken.

⁴⁷ Stådje, 2012, s. 73



Parlamentets e-posthantering var tvungen att stängas under en viss tidsperiod, vilket försvårade ledningsförmåga för parlamentet. Dock får inverkan på ledningsförmågan ses som begränsad då tidsperioden som e-posthanteringen låg nere var relativt kort, 12 timmar.

Möjligheten att leda organiseringen och etableringen för den stab som hade till uppgift att slå tillbaka attacken försvårades inte, inte heller riktades det några direkta attacker mot CERT.

Överlag påstår jag att attacken påverkade ledningsförmågan till en viss grad, främst i förmågan att informera samhället kring vad som pågick. Däremot påverkades inte förmågan att leda motåtgärderna kring attacken i någon större utsträckning.

2.2.5 Diskussion kring appliceringen

Var attacken en fulländad cyberattack?

Genom den analys som redovisats ovan, kan jag konstatera att cyberattacken mot Estland inte var en fulländad cyberattack. Attacken berör innehållen i respektive pelare och är en väl genomförd attack. Dock så saknar attacken delar ur Stienmons teori och framförallt saknas ett direkt syfte.

Attacken innehåller några områden inom pelaren teknologi, men inte många, utan är helt inriktad på DDoS. Det spreds ingen egen skadlig kod till estländskmyndigheter och inte heller angreps några e-postservrar annat än syfte att överbelasta dem.

Ledningen

Att attacken leddes på ett bra sätt råder det inga tvivel om när effekten av attacken nu redovisats. Det som är säkert kring attacken är att information delades ut via internetforum, men på detta vis lyckas man aldrig uppnå de simultana attackerna som botnäten utförde.

Min analys av denna aspekt är att internetforumen användes som en rekryteringsbas för script kiddies och för att skylta med sitt missnöje för Estlands agerande. De mer insatta och ledarna för hacktevisterna bör att kommunicerat på ett mer effektivt sätt, antingen via privata chattrum, någon form av telekommunikation eller ansikte mot ansikte.

Lågnivåattacker

Min analys av avsaknaden av lågnivåattacker, så som BGP manipulationer i den övergripande cyberattacken mot Estland, är att samma verkan uppnåddes med hjälp av botnät. Dessa botnät var antagligen både lättare att komma i kontakt med och att nyttja, då det inte krävs några avancerade hackingföretag för att uppnå verkan. För att ta BGP som exempel så krävs antingen ett godkännande från en ISP för att ändra BGP anvisningarna, eller att en ISP blivit hackad så att hackern kommit åt denna data. Det sistnämnda känns relativt osannolikt då BGP anvisningarna bör vara något som är högt prioriterat på säkerhetsläget hos respektive ISP, med tanke på följdverkan.



3 Diskussion och slutsatser

3.1 Vilka möjligheter till försvar mot en cyberattack har en nation?

Cyberrymden har inte samma självklara uppdelning i nationer och gränser som den fysiska värld vi lever i. Denna avsaknad av gränser kan leda till stora bekymmer eftersom de nuvarande regelverken för internationella relationer är uppstyrda efter just nationers uppträdande mot varandra. På grund av den gränslöshet som råder, kan data skickas och tas emot över hela världen utan några begränsningar, men det leder också till att cyberattacker kan genomföras från alla världens hörn. En ytterligare komplexitet med cyberrymden är att enskilda individer kan genomföra operationer som kan leda till stor skada, utan att nationen som blir utsatt har möjlighet att handla eftersom individen befinner sig i en annan nation.

Nationer, individer och grupper

För att kunna besvara frågeställningen kring vilka möjligheter till försvar, måste det först redas ut, vilka aktörer som kan tänkas utföra attacker.

Trots att cyberrymden inte är uppdelad och begränsad av nationsgränser, finns det nationella intressen att skydda från cyberattacker. Flera nationer har inrättat myndigheter eller organisationer som har sina huvudtjänster i cyberrymden och/eller informationskrigföring. USA har sitt US Cyber Command, Ryssland har flertalet militära- och civila organisationer med kapacitet för informationsövervakning och cyberattacker, Kina har inrättat en del av sin armé kallad "Blue Army" med inriktning på att kunna slå mot en motståndares kommunikativa nätverk,⁴⁸ för att nämna ett fåtal.

Stiennon hävdar i sin teori, att ledningen av cyberattacker fortfarande ligger i sin linda och att attackerna ofta sköts av en enskild individ. I cyberrymden kan en enskild individ utföra handlingar som kan leda till stora problem för företag och nationer. En ensam hackare kan lyckas ta sig in i en e-postserver och komma åt all den e-post trafik som genomförts, vilket kan leda till stora bekymmer för organisationen som äger servern och som är utmärkt data för kartläggning av en organisation.

Det finns flera organisationer där hackare som nämnts ovan ansluter sig i klusterliknande sammanslutningar. Exempel på sådana organisationer är Anonymous och Lulzsec, där organisationerna i sig är löst sammanslutna och utför attacker utifrån vad de anser vara rätt och fel. Med tanke på vilken kapacitet en enskild hackare har, kan ett samling av dessa leda till mycket svåra konsekvenser, inte minst med tanke på Estland. Ingen organisation gick ut och tog på sig ansvaret kring attacken mot Estland, men det finns organisationer som genomfört liknande attacker i sitt namn.

Dessa tre aktörer är de som jag identifierat som troligast att genomföra cyberattacker. Enligt Geers så har både stora och små aktörer sina för- och nackdelar. Enskilda hackare har möjligheten att agera snabbt och lämna mycket små avtryck som visar på var denne befinner sig. Nationer å andra sidan är ett väldigt stort mål, med många anfallsvinklar. Nationer har dock möjlighet till att skapa stora resurser, både i rå beräkningskapacitet och i mängden personal att sköta hanteringen och analys av cyberangreppen.

⁴⁸Carr, 2011, s. 257



Avsaknad av internationella regler

Det internationella regelverk som styr brukandet av våld, är baserat på staters handlingar mot varandra. Vidare använder sig dessa regelverk av termer kring väpnat våld, vilket gör att regelverken inte automatiskt kan appliceras på nätangrepp.

Detta är ett problem, sett ur ett säkerhetsperspektiv, då cyberrymden inte är begränsad av nationsgränser, utan informationen och datan kan flöda fritt. Detta fria flöde av data innebär att personer placerade långt bort ifrån den fysiska platsen där datan lagras, kan ha full tillgänglighet till den. Detta innebär även att enstaka individer kan ha möjlighet att åsamka skada och komma åt känslig information på ett sätt som inte har varit möjligt i den fysiska världen.

För att ta fallet Estland som utgångspunkt, så blev hela nationen utsatt för ett cyberangrepp, dock inte från en annan nation, vilket gjorde att de internationella regelverk som styr nationernas hantering av konflikter, inte gick att applicera. Estlands position blir nu knepig, för trots att de kan visa på varifrån stora delar av attacken härstammar samt visa på var ifrån informationsspridningen och ledningen sker, så har Estland som nation ingen möjlighet att gå in med attacker och stänga av dessa platser, då denna handling kan vara ett brott mot krigets lagar.⁴⁹

För att komma med ett konkret svar på frågan, om vilken möjlighet en nation har att försvara sig, är svaret att nationen endast kan skydda sig själv inifrån. Genom avsaknaden av internationella regler kring cyberattacker, finns det ingen möjlighet för en nation att genomföra offensiva handlingar i syfte att stänga ner en angripare som befinner sig utanför nationens gränser, utan nationen är helt låst till att nyttja defensiva metoder.

Att nationen är låst till defensiva metoder är problematiskt. Geers slår fast att i cyberattacker så är det attackeraren som har övertaget, vilket då skulle innebära att det bästa försvaret mot cyberattacker just är egna attacker. Nationer besitter också, som tidigare nämnt, kapaciteten att skapa stora resurser och därmed kunna slå tillbaka en svagare angripare, så som en sammanslutning hackteviser, men saknar idag de juridiska möjligheterna att kunna använda sådana resurser.

Lösningen på detta problem idag, är goda internationella samarbeten. Den nation som blir drabbad är helt utelämnad till att nationen som hackteviserna befinner sig i, agerar mot dessa. Problemet med denna lösning är att den endast fungerar ifall nationerna verkligen agerar mot inhemska hackare, vilket vissa länder inte gör.

Carr beskriver hur länder så som Kina och Ryssland snarare ser på sina inhemska hackare som tillgångar än problem, då fallen med att ställa hackare som varit inblandade i internationella attacker inför rätta är så få, att dessa är statistiskt betydelselösa.⁵⁰ Rysslands ignorering av fallet Estland,⁵¹ visar på ett synsätt att Ryssland inte har någonting emot att hackteviser från deras nation utför handlingar som har kapacitet att sänka en nation, så länge de inte riktar attacken mot Ryssland.

⁴⁹ Carr, 2011, s. 47

⁵⁰ Ibid, s. 29

⁵¹ Davis, 2007, s. 182



3.2 Ett militärt problem?

Fallet Estland löstes ut utan att någon form av militär verksamhet deltog. Det som genomfördes var att en stab upprättades av civila myndigheter, som sedan ledde arbetet med att samordna stoppandet av de pågående attackerna. Den civila myndigheten CERT tog kontakter med individer, erkända av de störst internationella ISP:erna och som därmed sitter med befogenhet att koppla ner användare från internet.

Jag skulle påstå att fallet Estland aldrig var ett militärt problem, problemet var helt civilt. Attacken skapade oreda och strypte tillgången till information, men attacken var aldrig ett hot mot nationens säkerhet.

Kits hävdar i sin uppsats att skillnaden mellan cyberbrottslighet och -terrorism ligger i syftet med attacken. Problemet som uppstår med den definitionen, är när en attack verkar sakna syfte, så som attacken mot Estland. Det angavs aldrig något syfte till varför attacken skedde, hur ska en sådan attack då behandlas utifrån Kits teorier?

Jag håller istället med Carr, som hävdar att det inte borde finnas en skillnad mellan hanteringen av cyberattacker, oavsett om avsikten med attacken är kriminalitet eller som en del i krigföring. Genom att ha en organisation som hela tiden är aktiv i att avvärja hot, som inträngningsförsök eller överbelastningsattacker oavsett syfte, kommer organisationen att optimera sig själv och lägga fram rutiner för att möta hotet. Vidare har organisationen möjlighet att knyta de kontakter, som visade sig nödvändiga i fallet Estland, för att snabbt få ett internationellt samarbete att stoppa attacken.

Kantola beskriver hur ”samhällets övriga aktörer” behöver tas i beaktande vid en omorganisation av förmågan till CND och CNA samtidigt som både Kantola och Hansson anser att båda dessa förmågorna bör ligga inom samma organisation för att effektivt kunna utveckla varandra. Här uppstår det ett problem, eftersom det just nu inte finns några möjligheter för en nation att genomföra cyberattacker, rent juridiskt, annat än mot en annan nation i händelse av krig. Ska en organisation utveckla CNA bör denna förmåga alltså ligga hos försvaret, dock så borde alltså CND ligga i samma organisation enligt rådande forskning. Läger man ihop Carrs slutsatser med Hansson och Kantola skulle det innebära att en militär organisation skulle behöva behandla samtliga cyberattacker, oavsett i vilket syfte som attacken genomförs. Enligt denna tolkning skulle samtliga incidenter rörande cyberattacker vara militära problem, vilket skulle ses som väldigt konstigt eftersom enskilda attacker inte är hot mot nationens säkerhet och därför inte bör ligga på en militär organisation.

Ett lämpligare alternativ, är att organisera två enheter där den ena jobbar inom försvaret med att utveckla CNA samt CND begränsat till försvarets nätverk, medan den andra enheten är civil och sköter alla cyberattacker oavsett om det gäller cyberkriminalitet eller -krigföring. Då skulle cyberattacker bli ett militärt problem först när attackerna är direkt riktade till att slå mot försvarets ledningsförmågor, medan alla andra attacker skulle vara ett civilt problem. Den civila enheten har inte möjlighet att nyttja CNA förmågor, enligt rådande regelverk, och behöver därför inte utveckla någon sådan. För att en nation ska kunna utföra regelrätta cyberattacker mot en annan nation måste nationerna vara i krig och därmed kan denna förmåga ligga på enheten inom försvaret.



Slutsatser

Det som jag har kommit fram till i denna uppsats är att cyberattacken mot Estland var en väl genomförd attack i form av ledning, dock saknade attacken ett uttalat syfte och målsättning, vilket gör att attackens verkan var begränsad. Effekten av attacken blev att Estlands befolkning inte kunde koppla upp sig mot omvärlden, men det inhemska internet var åtkomligt vilket möjliggjorde för dagligärenden, som till exempel bankärenden.

En annan intressant slutsats är att en omfattande cyberattack mot en nation inte behöver vara ett militärt problem. Cyberattacken mot Estland klarades ut, utan några inblandningar av militära enheter. En militär organisation är dessutom bakbunden med dagens internationella regelverk, eftersom det inte finns någon möjlighet att utföra motangrepp mot en cyberattack, som härstammar från en aktör som inte är en annan stat.

Förslag på vidare forskning

- Applicering av Stienbons teori på andra fall för att jämföra resultat och slutsatser.
- Genomföra fördjupad undersökning kring de internationella regelverk som styr brukandet av väpnat våld mellan nationer, med ett perspektiv ur cyberattacker.



Källor och litteratur

Carr Jeffrey, 2011, *Inside Cyber Warfare*, (2nd edition), O'Reilly Media, Sebastopol.

Davis Joshua, 2007, "Hackers Take Down the Most Wired Country in Europe" *Wired Magazine*: Issue 15.09, San Francisco

Estonian Information System's Authority:
Not 11: www.ria.ee/27525 (besökt 120429)
Not 12: www.ria.ee/cert-estonia/ (besökt 120509)

Europeiska kommissionen:
http://ec.europa.eu/information_society/policy/nis/docs/largescaleattacksdocs/s5_gadi_evron.pdf
(besökt 120520)

Geers Kenneth ,2011, *Strategic cyber security*, CCD COE, Tallin.

Hanson Mattias, 2002, "Försvaret mot Cyberkrigföring", FHS

Kantola Harry, 2011, "Datanätverksattacker, trend eller nödvändighet?", FHS

Kits Linda, 2010, "De Grundläggande Förmågorna vs Cyberterrorism", FHS

Krisberedskapsmyndigheten, 2008, *Sveriges beredskap mot nätangrepp*.

NATO Cooperative Cyberdefence Center of Excellence:
<http://www.ccdcoe.org/11.html> (besökt 120509)

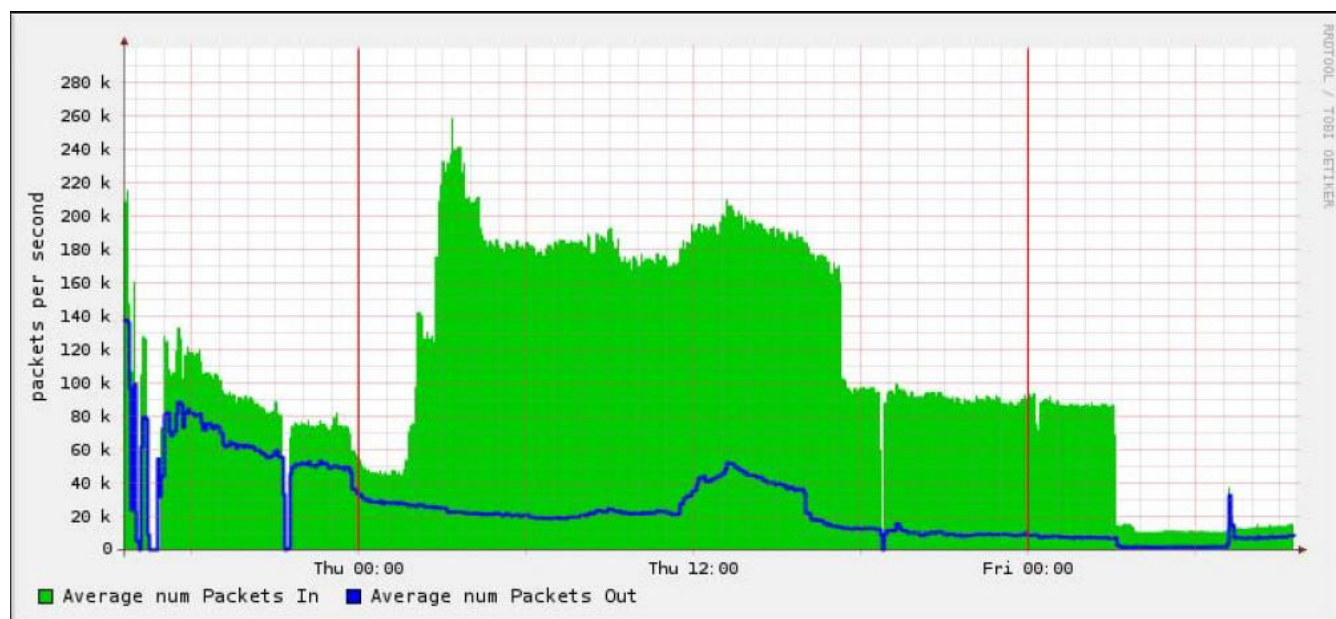
Riegert Kristina, 2002, *Kampen om det kommunikativa rummet : informationskrigföring under Kosovokonflikten 1999*, Styrelsen för psykologiskt försvar, Stockholm.

Stiennon Richard, 2010, *Surviving cyberwar*, Government Institutes, Lanham.

Städje Jörgen, 2012, "Estland under attack" *TechWorld*, nr 2, IDG AB, Stockholm



Bilaga 1



Graf över trafiken hos en server i Estland för tiden; 8-9 Maj 2007. Notera de tvära höjningarna och sänkningarna i trafikmängd.

Grafen är hämtad från powerpointbildspelet "Estonia: Information Warfare and Lessons Learnd" skriven av Gadi Evron och Hillar Aarelaid, chef för CERT-EE. Bildspelet är publicerat på Europeiska kommissionens hemsida.⁵²

⁵² Europeiska kommissionen, s.8