Nicklas Simu
1OP147

2015-05-26

Självständigt arbete (15 hp)

Författare		Program/Kurs
Nicklas Simu		OP SA 12-15
Handledare		**Antal ord: 10243**
Lars Wikman	**Beteckning**	**Kurskod**
Peter Haldén		1OP147

STRATEGISK BOMBNING I CYBERSPACE

ABSTRACT:
Why has some cyber-attacks been more successful than others? There has been in the near past examples of cyber-attacks used with different purposes. How do we understand these chosen targets and what result the attack accomplished?
Research has discussed similarities between aviation warfare and cyber warfare, and how the first could explain what is happening in cyber warfare now. There is also opposing opinions whether cyber warfare should be seen as a method to alone force a will on your opponent or if cyber warfare should mere be supporting other military means. The essay test Warden's theory "The Enemy as a System" capacity to explain why the effect of cyber-attacks can differ. It will also compare the effect in different cases based on standalone and supporting cyber-attacks.

The essay concludes that Warden's theory does not have any explanatory value but the difference in effective and ineffective cases is whether the cyber-attack was supporting other military means or a standalone attack.

Nyckelord:
Cyberattacker, Cyberkrigföring, Subversion, Warden, The Enemy as a System, militära medel.

Innehållsförteckning

1 Varför lyckas vissa cyberattacker?

Cyberkrigföring används i moderna mellanstatliga konflikter och det kommer inte att försvinna. Cyberattacker används till exempel för att fördröja framställning av kärnvapen, skapa instabilitet i ett land, slå ut ett lands internetuppkoppling som en form av maktdemonstration eller som förbekämpning inför en invasion.

Eftersom användandet av cyberattacker är ett relativt nytt fenomen som militärt medel så saknas färdigarbetade teorier och tillämpbara doktriner. Trots att området cyberkrigföring är nytt och forskningen är i ett tidigt stadie så används det för att påtvinga en motståndare en vilja eller hindra denne från att ändra sin vilja, men hur uppnås detta? Hur förstår vi vilka mål som angrips och vad det ger för resultat? Varför lyckas vissa cyberattacker?

Syftet med uppsatsen är att empiriskt testa, genom en fallstudie, hur det kommer sig att liknande cyberattackerna kan skilja sig i utfallet och varför effekten inte är densamma. Här kommer uppsatsen att reda ut hur effektiva cyberattacker har sett ut och om en cyberattack bör ses som ett självständigt vapen eller understödjande till andra militära medel.

Uppsatsen kommer utifrån Wardens teori om fienden i ett system att kategorisera angripna mål vid ett antal kända fall. Därefter kommer effekten bedömas och jämföras med målvalen samt om cyberattackerna skedde med eller utan andra militära medel. Effekten kommer att bedömas som ”Effekt” eller ”Ingen effekt”, dessa begrepp diskuteras mer ingående senare i uppsatsen. Effekten kommer att diskuteras utifrån ett hypotetiskt eller faktiskt syfte med en attack och vad attacken åstadkom för resultat.

Hur kan effekten av cyberattacker förklaras utifrån Wardens teorin om fienden i ett system?

Hur påverkas effekten om en cyberattack varit självständig eller understödjande till andra militära medel?

Uppsatsen ämnar reda ut hur effektiva cyberattacker har sett ut och om en cyberattack bör ses som ett självständigt vapen eller understödjande åt andra militära medel. Bidraget från den här uppsatsen är tvådelat inom den tidigare forskningen. Den kommer att pröva en sedan tidigare oprövad luftmaktsteori för att försöka förklara cyberkrigföring. Detta mer teoretiska bidrag är riktat mot den debatt som pågår kring den teoretiska utvecklingen kring cyberkrigföring som nyttjar tidigare luftmaktsteorier. Det andra mer empiriska bidraget kommer även att diskutera skillnader i fallen Estland, Georgien och Kyrgyzstan som påverkar utfallet av cyberattackerna. Denna utgår ifrån diskussionerna i den tidigare forskningen om cyberattacker skall ses som självständiga eller understödjande.
Bidraget är alltså i första hand prövandet av en ny teori i en fallstudie och i andra hand en förklaring av hur cyberattacker påverkas av att kombineras med andra militära medel.

1.1 Material

Materialet bygger i stort på andrahandskällor och tidningsartiklar.

Stor del av empirin är tagen från en rapport utgiven av Cyber Defence Centre of Exellence (CCD COE), en institution upprättad efter cyberattackerna mot Estland. Empirin har dock triangulerats med nyhetsartiklar samt andra rapporter och tidigare forskning om fallen.

1.2 Cyberattacker

Begreppet cyberattacker kan till en början upplevas som ett ganska simpelt begrepp. Det är alltså attacker som genomförs i cyberspace. Cyberspace kan förklaras utifrån Butler som simpelt definierar det som en ny arena i familjen om luft, sjö, mark och rymd.[1] Nationalencyklopedin definierar cyberspace som: ”C*yberrymd, en vision av ett universum av information och kultur, en gemensam, global, av datorer upprätthållen virtuell värld som existerar parallellt med den fysiska världen och i vilken människor kan interagera med varandra och med världen och dess innehåll.*”[2] För att underlätta förståelsen av begreppet cyberspace så kommer det att användas som Butler definierar det, en arena, alltså det utrymme inom vilket cyberattacker genomförs.

Detta förklarar alltså var cyberattacker genomförs, men vad är cyberattacker? Thomas Rid delar in cyberattacker i tre kategorier: sabotage, espionage och subversion som ger en tydlig uppdelning i de olika typerna av cyberattacker.

Sabotage förklaras som en cyberattack med skadliga program som har för avsikt att försvaga eller förstöra ett system.[3] Skadliga program är till exempel det som vanligare benämns som virus.

Espionage innebär att avlyssna eller hämta information från datornätverk eller system, där stor vikt ligger på anonymitet och att inte bli upptäckt.[4] Den här typen av verksamhet handlar sällan om att uppnå ett mål utan istället att inhämta information som kan användas för andra medels möjlighet att uppnå ett mål.[5]

Subversion handlar dels om att underminera en auktoritet, där Rid huvudsakligen utgår ifrån aktivist rörelser som använder sig utav denna typ av cyberattack.[6] I denna uppsats kommer kategorin subversion att innefatta underminerande och störande cyberattacker som defacement, DoS- och DDoS-attacker. Defacement kan vi se som propaganda medan DoS- och DDoS-attacker mer syftar till att störa en verksamhet genom överbelastning.[7]

1.3 Tidigare forskning

Butler ser cyberspace som en egen arena som bör förstås ytterligare för att utveckla specifika doktriner och teorier som är anpassade för just cyberspace och inte kopior

[1] Butler, Sean. Refocusing Cyber Warfare Thought. *Air & Space Power Journal* 27 no. 1 (January-February 2013): 44-57. http://130.252.58.169/docview/1318929576?accountid=8325 (Hämtad 2015-04-03). 46.
[2] Janlert , Lars-Erik. Cyberspace. Nationalencyklopedin. http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/cyberspace (Besökt 2015-05-07)
[3] Rid, Thomas. *Cyber War Will Not Take Place*. London: C. Hurst & Co. 2013. 56, 57.
[4] Ibid. 81.
[5] Ibid. 82.
[6] Ibid. 113, 114.
[7] Se bilaga för begrepp och förkortningar.

från en annan arena.[8] Han hävdar att vi inte kan se grundkoncept som utnötning och motkraft inom cyberkrigföring och att detta är en grund till att det kan vara farligt att använda teorier från andra arenor för att förklara cyberkrigföring. Detta utgår ifrån bristen av tidigare fall som kan användas för att förstå cyberkrigföring, det som talas om är fall av ”cyber war” eller cyberkrig.[9]
Utgångsläget för Butler förefaller vara att det handlar om ett cyberkrig, ett krig där huvuddelen, om inte alla strider, utkämpas i cyberspace. Om detta är troligt har diskuterats där Rid också ser brister i exempel på fall där ett cyberkrig har utkämpats. En av hans slutsatser är dock att cyberkrig kan vara något som i framtiden är oundvikligt.[10] Här diskuteras en viktig del för den här uppsatsen: cyberkrigföring utifrån möjligheten av ett cyberkrig, alltså att det sker upprepade attacker i cyberspace utan inblandning av andra militära medel. Med två parter som försöker påtvinga den andra en vilja enbart genom cyberattack.
Enligt ovan så bygger tankar om cyberkrig på spekulationer om det kommer att ske eller om det överhuvudtaget är möjligt. Alltså ett fristående cyberkrig, men detta saknas det tidigare exempel på.
Sharma har uppmärksammat cyberattacker som ett understödjande medel till större operationer. Detta anser Sharma inte är cyberattackers fulla potential. Cyberattacker har nyttjats som taktiska vapen i dessa operationer istället för att använda cyberattacker som ett huvudvapen för att uppnå ett strategiskt mål. Att cyberattacker som huvudvapen kan påtvinga motståndaren en vilja utan någon betydande fysisk militär styrka.[11] Här har Sheldon en annorlunda syn på hur det strategiska målet kan uppnås med cyberattacker: Att cyberattacker används för att påverka den strategiska miljön och att detta bör göras i kombination med andra militära medel för att uppnå den största effekten. Syftet med att använda cyberattacker mot motståndaren är att försvåra dennes beslutsfattande och vinna tid för att andra militära medel ska få större chans att lyckas.[12]
Det resonemang som Sharma för om ett nytt vapen eller en ny arena som näst intill självständig ska vara orsaken till att påtvinga motståndaren en vilja, hävdar Betz inte är något nytt. Det är ett resonemang som fördes mellan första och andra världskrigen i utvecklingen av luftmakt. Han tar upp J.F.C. Fuller som beskriver flyget som ett vapen som kan få ett land att ge upp utan egna förluster.[13] Forskningen är oense om cyberattacker utnyttjas bäst självständigt eller tillsammans med andra militära medel. Som Betz förklarar så är den diskussionen ett fall av det tidiga stadiet i utvecklingen av cyberkrigföring.

Betz talar dock även om en stor skillnad mellan luftmakten och cyberkrigföringen, anonymitet och låga anskaffningskostnader. Detta innebär att fler aktörer, som fattigare

[8] Butler. Refocusing Cyber Warfare Thought. 46.
[9] Ibid. 54.
[10] Rid, Thomas. Cyber War Will Not Take Place, *Journal of Strategic Studies* 35 no. 1 (2012): 5-32. DOI:10.1080/01402390.2011.608939. 29.
[11] Sharma, Amit. Cyber War: A Paradigm Shift from Means to Ends. I *The Virtual Battlefield: Perspectives on Cyber Warefare*, Czosseck, Christian och Geers, Kenneth. (Eds.) 3-17. Amsterdam: IOS Press BV, 2009. 15.
[12] Sheldon, John. Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly* 5 no. 2 (Summer 2011): 95-112. http://130.252.58.169/docview/871291547?accountid=8325 (Hämtad 2015-04-03). 103.
[13] Betz, David. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *The Journal of Strategic Studies* 35 no. 5 (October 2012): 689-711. DOI: 10.1080/01402390.2012.706970. 692, 693.

stater eller icke-statliga organisationer, kan ge sig in i cyberspace och kan även göra detta utan att riskera upptäckt.[14] Detta handlar då om en ingångsport till cyberspace, men om det istället handlar om att vara en stormakt i cyberspace så talar Butler om att det krävs en uppbyggd styrka som har välutbildat manskap och utrustning. Även storleken av denna styrka har avgörande betydelse. Han kopplar detta till United States Air Force som i sina doktriner om "counterair operations" menar att högsta prioritering är att kontrollera luftrummet. Här hävdar Butler att luftrum kan bytas ut mot ordet cyberspace för att nyttja ett gammalt tänkesätt på ett nytt område. Dock så menar han att denna kontroll uppnås genom en form av överlägsenhet och det syftar inte enbart till att slå motståndaren och försvara sig själv, utan just denna storlek på en styrka som har rätt utbildning för området.[15]
Trots de utmärkande faktorerna om anonymitet och låga anskaffningskostnader så håller Betz med om detta synsätt, där cyberspace används i en militär kontext. När det alltså handlar om användandet av cyberspace för militära mål så blir inte anskaffningskostnaderna längre låga. Här används exemplet om Stuxnet och cyberattacken mot det iranska kärnvapenprogrammet. Att tillverka Stuxnet krävde ett mellanstatligt samarbete samt underrättelser om målet.[16] Detta innebär att storskaliga cyberattacker ofta kräver kapacitet och ekonomiska medel som enskilda individer inte har, utan endast stater.
Även anonymitet beskrivs som en faktor som inte är intressant på en strategisk nivå då det inte går att påtvinga en motståndare vår vilja om motståndaren inte vet vem som angriper. Cyberattacker är alltså ett nytt tekniskt vapen som inte har stora risker för egna förluster, men anonymitet och låga anskaffningskostnader är irrelevanta då det talas om cyberattacker som militära medel. Därmed blir det stora likheter med luftmakt.[17] Detta påstående går att diskutera, speciellt med exempel om virusattacker som bevisligen kan påtvinga en vilja utan att den anfallande staten är erkänd. Detta resonemang kommer att fortsättas senare. Å andra sidan så kan detta påstående gå att försvara vid självständiga cyberkrig där det i förlängningen kanske inte går att vara anonym för att få sin vilja igenom.
Uppsatsen använder liknelser till luftmakten för att föra resonemangen om teorin fienden i ett system som togs fram för luftmakten men kan vara användbar även för att förklara delar ur cyberkrigföringen.

1.4 Avgränsning

Uppsatsen avser inte att försöka reda ut om ett cyberkrig, alltså ett fristående krig som utkämpas enbart i cyberspace, kommer att ske. Denna avgränsning är gjord kopplat till tidigare forskning där forskningsområdet är splittrat och fyllt med spekulationer som denna uppsats inte har tid eller utrymme för. Istället kommer uppsatsen att diskutera vilka effekter självständiga cyberattacker har fått i jämförelse med cyberattacker som kombinerats med andra militära medel. Det innebär inga stora brister i uppsatsen då den bygger på att förklara effekten av cyberattacker utifrån en teori, vilket är svårt att genomföra på cyberkrig som enligt tidigare forskning aldrig har inträffat.

[14] Betz. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. 694.
[15] Butler. Refocusing Cyber Warfare Thought. 53.
[16] Betz. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. 695.
[17] Ibid. 696.

Som tidigare förklarat så är begreppet cyberattacker brett och innefattar en mängd olika typer av attacker som kan användas för spridda syften. Den valda indelningen av cyberattacker med sabotage, espionage och subversion gör avgränsningen tydligare då kategorierna och dess innehållande cyberattacker medför viss problematik att analysera.
Kategorin sabotage är till en första anblick lätt att analysera utifrån resultat och syften. Till skillnad från övriga kategorier är syftena oftast väldigt tydliga och resultatet går att mäta. Det stora problemet med kategorin är att det finns näst intill inga fall av misslyckade cybersabotage. Det kan bero på olika saker. Det ena alternativet är att en stat inte erkänner att de blivit angripna av ett misslyckat cybersabotagförsök eftersom det kan tyda på eventuella brister i det egna systemet. Som vi kan se i viruset Stuxnet så byggdes det med underrättelser om målet.[18] Att då erkänna ett misslyckat angrepp visar på att det bör finnas brister. Det andra alternativet är att sabotageförsöket inte upptäcks av den angripna staten. Även här kan vi utgå ifrån Stuxnet som skulle uppträda dolt så länge som möjligt och påverka det angripna systemet så pass lite att det helst inte upptäcktes.[19] Om så är fallet men att viruset istället misslyckas med att påverka systemet, så kan det finnas stor risk att det aldrig upptäcks. Det misslyckade sabotageförsöktet kan då enbart erkännas av själva tillverkaren av viruset. I och med bristen på misslyckade fall kommer uppsatsen inte att behandla denna typ av cyberattack, då det skulle skapa obalans i analysen med en kategori som alltid har effekt trots att så inte är det verkliga fallet. Men motsatsen är som beskrivet svår att bevisa.
Kategorin espionage har till viss del samma problem som kategorin sabotage då espionage uppträder dolt. En väl genomförd cyberattack med espionage upptäcks aldrig, eller åtminstone döljer den vilken information som faktiskt stals. Det är problematiskt att bedöma ett syfte som sällan är uttalat. Bedömningen bygger då på de upptäckta källorna som har blivit utsatta för espionage. Som vi kan se i fallet av espionage mot USA, benämnt Moonlight Maze, så upptäcktes intrång på ett flertal websidor och databaser, men vilken information som faktiskt blev stulen eller om det var ytterligare källor som angreps är oklart.[20] Därav avgränsas även denna kategori från uppsatsen på grund av stora svårigheter att analysera eventuell effekt samt syften som bygger för mycket på spekulationer.

[18] Stuxnet: targeting Iran's nuclear programme. *Strategic Comments* 17 no. 2 (2011): 1-3. DOI: 10.1080/13567888.2011.575612.
[19] Stuxnet: targeting Iran's nuclear programme.
[20] Llongueras, Adrianna. *Moonlight Maze. The beginning of a new era*. Academia. http://www.academia.edu/6182336/MOONLIGHT_MAZE._The_beginning_of_a_new_era (Hämtad 2015-05-07).

2 Fienden i ett system

Warden talar om två faktorer som ger ett utfall, det fysiska och moralen. Han har skiftat vikten av dessa jämfört med tidigare luftmaktsteoretiker som förspråkade att angripa moralen och viljan att slåss istället för det fysiska. Denna skiftning hävdar han beror på bristande exempel där angrepp med moralen som mål inte har visat sig ge någon betydande effekt. Han hävdar att moralen eller viljan att slåss kan vara svår att förutse hos motståndaren då människor är olika och det som driver oss därför också är olika. Istället bör fokus ligga på att angripa det fysiska hos motståndaren. Detta innebär dock inte enbart dennes militära styrkor utan på ett strategiskt plan som kan innebära att förinta hela staten.[21]

Teorin om fienden i ett system förklaras utifrån en tabell av vad som finns i ett sådant system. Kategorier i systemet är ledarskap, organiska nödvändigheter, infrastruktur, befolkning och försvarsmekanismer. Dessa kategorier kan ses som en prioriteringsordning av vad ett system kräver för att fungera optimalt. Warden använder sig av flera exempel på olika system för att fylla i denna tabell och förklara dess kategorier, detta för att påvisa likheter i system och kategoriernas validitet.[22]

Denna modell kan även ses som en lök, där ledarskap är i mitten och följs med påbyggande lager av övriga kategorier.[23] Lagren kan ses som en stats svagheter i att fungera fullt ut. Desto längre in en stat angrips, desto svårare får denna att fungera. Det innersta lagret, ledarskap, är prioriteringsmålet.[24] Att angripa ledarkapet kanske inte alltid är möjligt men kan göras indirekt genom att angripa andra lager i löken och på så sätt tvinga motståndaren att ändra sin strategiska plan. Som tidigare så prioriteras lagren inifrån där Warden ger ett exempel på angrepp mot de organiska nödvändigheterna. Om ledarskapet hos en stat inte går att angripa direkt, så kan angrepp mot elektricitet eller drivmedel göras för att försvåra eller till och med omöjliggöra en stats funktioner. Dock så nämns det att ett angrepp mot yttre lager än ledarskapet kan kräva tid för att få verkan på ledarskapets beslutsfattande.[25] Warden ger fler exempel på övriga lager som kan leda till att ledarskapet måste ändra sina planer eller slutligen ge efter för angriparens krav. Ju längre ut i löken som angreppen sker, desto mer kräver det av angriparen.[26]

Det har vid ett flertal historiska tillfällen varit svårt att angripa motståndarens inre lager med flyg, oftast går det bara att nå de två yttre.[27] Här har vi något som kan vara en signifikant skillnad mellan luftmakt och cyberkrigföring och därmed också försvåra möjligheten att nyttja luftmaktsteorier för att förklara cyberkrigföringen. Tillskillnad från luftmakten så är inte cyberkrigföring bunden till de fysiska skillnaderna som angrepp med flyg mot de olika lagren innebär. Till exempel kan vi föreställa oss att ledarskapet befinner sig geografiskt placerad i mitten av en stat eller långt från

[21] Warden III, John. The Enemy As A System. *Airpower Journal* (Spring, 1995). http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (Hämtad 2015-04-03). 3, 4.
[22] Ibid. 5.
[23] Ibid. 8.
[24] Ibid. 10.
[25] Ibid. 11.
[26] Ibid. 12.
[27] Ibid. 13.

motståndaren. Ledarskapet har då övriga lager mellan sig och motståndaren, alltså kan modellen i detta fall även ses som en skyddslök där angrepp mot ledarskapet måste fysiskt med sina plan kunna passera övriga lager. Cyberkrigföring har inte dessa problem då angrepp inte är bundna till den geografiska eller fysiska platsen av respektive lager. Warden trycker, trots svårigheter att nå önskade lager, på vikten av ”parallella attacker” och att angripa flera delar inom ett lager eller flera lager för att rikta motståndarens uppmärksamhet mot olika delar och tvinga denna att fatta nya beslut om återuppbyggnad eller försvar på olika plan.[28]

2.1 Kritik mot Warden

Warden är som ovan en av de senare teoretikerna inom luftmakt men har blivit ifrågasatt. En av de stora bristerna i Wardens teori som diskuterats är om den verkligen bygger på representativ empiri eller om valda fall för att förklara teorin är sådana som passar in och bevisar teorin. Widén och Ångström skriver då att den bör ses mer som en hypotes än något som faktiskt avspeglar verkligheten.[29] Faber har också ifrågasatt de liknelser som Warden använder. Teorin ifrågasätts om liknelserna som används är representativa för verkligheten. Där används en liknelse som jämför det system den mänskliga kroppen är uppbyggd av och det system en stat är uppbyggd av. Ett exempel är att om huvudet huggs av en människa så slutar kroppen att fungera, men sker verkligen detsamma hos en stat? Faber hävdar att en stat inte nödvändigtvis slutar att fungera om huvudet eller ledningen huggs av från övriga systemet.[30]
Även Pape ifrågasätter syftet att slå ut ledarskapet och för diskussionen om hur påtvingandet av en vilja ska fungera på en motståndare utan ett ledarskap som kan ta emot meddelandet.[31] Att ifrågasätta det är relevant då vi ser till flygbombning. Bombning av ledarskapet kan medföra uppenbara svårigheter att framföra ett meddelande om en påtvingad vilja om mottagaren varken kan nås av angriparen eller har möjlighet att leda staten och förändra dess inriktning. När vi istället kopplar teorin till cyberattacker så försvinner denna problematik till stor del. Vi talar nu istället om att störa ledarskapet samt försvåra dennes kommunikationsmöjligheter. Papes kritik blir då inte relevant eftersom cyberattacker enskilt har svårt om inte omöjligt att stänga ner alla tänkbara kommunikationsmöjligheter för motståndaren.

2.2 Användning

Tidigare forskning visar på likheter mellan cyberkrigföring och utvecklingen av luftmakt under mellankrigsåren. Dessa jämförelser stannar ofta just vid mellankrigsåren och för fram de diskussioner som tidig luftmakt hade. Trots detta så är det väldigt få som gör faktiska jämförelser med luftmaktsteoretiker och om deras förståelse av luftmakt kan överföras till cyberspace. McCarthy är en av dessa som använder sig av luftmaktsteoretiker i sin avhandling som en del i att förklara hur makt tas i cyberspace. De teoretiker han har valt att använda är även dessa under den tidiga utvecklingen av luftmakt: Douhet, Mitchell och Seversky.[32]

---

[28] Warden III. The Enemy As A System. 17.
[29] Widén, Jerker. & Ångström, Jan. *Militärateorins Grunder.* Stockholm: Försvarsmakten, 2005. 267.
[30] Ibid. 267.
[31] Ibid. 267.
[32] McCarthy, Thomas David. *Traveling Domain Theory: A Comparative Approach for Cyberspace Theory Development.* Diss., The Fletcher School of Law and Diplomacy, 2012.
http://pqdtopen.proquest.com/doc/1029868522.html?FMT=AI (Hämtad 2015-04-03).

Warden fortsatte att utveckla luftmaktsteorier. Dessa belyser cyberkrigföringens utveckling, om dessa tidiga liknelser mellan luftmakt och cyberkrigföring fortsätter att finnas kvar. Warden talar likt många andra luftmaktsteoretiker om just hur luftmakt ska användas och vilka mål som ska angripas för att uppnå bästa effekt. Teorin om fienden i ett system kan möjligen, liksom utvecklingen av luftmakt, förklara utvecklingen av cyberkrigföring och vad angrepp mot olika mål ger för utfall.

3 Metod

Uppsatsen kommer att göras utefter en fallstudie. Fallstudien kommer att i huvudsak vara teoristyrd utifrån fienden i ett system och genom den förklara valda händelser och deras utfall. För att skapa djupare förståelse för enskilda händelser kommer fallstudien även att vara upptäcktsstyrd och jämföra flera händelser inom cyberkrigföringen.[33] Uppsatsen kommer alltså att ha en jämförande design, det beskrivs som en passande design när det råder brist på antal fall inom ett område.[34] Att det råder brist på fall om cyberattacker behöver inte vara ett faktum då det förekommer cyberattacker dagligen av varierande storlek. Det blir dock så i denna uppsats med de avgränsningar som är gjorda.
En av de största nackdelarna med en fallstudie är trovärdigheten i urvalen av fall och huruvida de kan ses som representativa för en större massa.[35] I denna uppsats finns det en svårighet att påvisa att fallen är representativa, då det inte finns en stor mängd fall att välja ifrån, men samtidigt underlättar det även trovärdigheten. Utifrån gjorda avgränsningar är fallen representativa och kan generaliseras. Dock är fallet Georgien det enda som har skett med liknande faktorer, vilket bör finnas i åtanke kopplat till de slutsatser som dras.

Uppsatsen kommer att använda sig av en kvalitativ analys av empirin, vilket medför och förstärker trovärdigheten. Förutom som redan diskuterats kring möjligheten att se slutsatser som generella vid fallstudier och kvalitativa analyser, så uppkommer ytterligare en nackdel, min inverkan och betydelse för analysen. Vad jag har för förutfattade meningar och min möjlighet att ha ett öppet sinne kan påverka och vinkla analysen och de slutsatser som dras.[36] Det finns även en risk att analysen letar efter en förklaring, att denna förklaring blir en förenkling av en komplicerad händelse.[37] Men detta kan krävas för att en generalisering ska kunna ske, att viktiga faktorer identifieras för att det överhuvudtaget ska gå att jämföra slutsatser dragna av valda fall med andra.[38]

3.1 Urval

Fallen är valda utifrån det som beskrivs som den teoriprövande undersökningsenheten. Att valda fall skall kunna pröva den valda teorin, att just dessa fall har de inslag som behövs för att kunna dra slutsatser från teorin.[39] Fallen har därför valts för att representera de olika kategorierna inom fienden i ett system. Valen har dock också präglats av uppmärksamheten kring olika incidenter. Fallen som har valts är alltså fall som har blivit uppmärksammade i såväl tidigare forskning som media.

En stor fråga då fallen skiljer sig ganska mycket åt är om analysenheterna är homogena, om de är tillräckligt lika på områden som ej avses undersökas.[40]
En faktor som kan ha stor betydelse är landets ekonomiska situation och dess utveckling inom ICT. Hur beroende är en stat av internet? Det kan visas utifrån statistik på hur

[33] Denscombe, Martyn. *Forskningshandboken*. 2. uppl. Lund: Studentlitteratur AB, 2009. 63.
[34] Esaiasson, Peter. Gilljam, Mikael. Oscarsson, Henrik. och Wängnerud, Lena. *Metodpraktikan*. 3. uppl. Vällingby: Norstedts Juridik AB, 2010. 112, 113.
[35] Denscombe. *Forskningshandboken*. 71.
[36] Ibid. 384, 385.
[37] Ibid. 400.
[38] Ibid. 69.
[39] Ibid. 65.
[40] Esaiasson. Gilljam. Oscarsson. och Wängnerud. *Metodpraktikan*. 102, 103.

många per 100 invånare som använder internet. Utifrån valda fall och den stat som blev angripen så ser statistiken ut enligt följande:[41]

	Internetanvändare per 100 invånare
Estland (2007)	66,2
Georgien (2008)	10,0
Kyrgyzstan (2009)	17,0

Tabell 1: Internetberoende

Detta kan vara ett problem då vi kan se stora skillnader i hur utvecklat internet var i respektive land det år som cyberattacken skedde. En del i detta kan vara kopplingen mellan antalet invånare som använder internet och hur mycket ekonomiska medel som ett land lägger på försvar och säkra system mot inkommande cyberattacker. Å andra sidan så blir en stat med färre internetanvändare, färre e-tjänster hos banker och regeringen, drabbade lindrigare vid en attack. Alltså: ju lägre siffra i tabellen, desto troligtvis sämre försvar och åtgärdsmöjligheter mot en cyberattack, men samtidigt desto högre tolerans mot cyberattacker som inte påverkar lika stor del som ett land med högre siffra.

Det finns dock uppfattningar om vikten av dessa oberoende faktorer vid teoriprövande undersökningar. Vid just teoriprövande undersökningar så kan forskningen lägga mer fokus på de valda faktorerna, frågeställningar och det som prövas än faktorer som kan komma att påverka resultatet.[42] Undersökningens resultat och påverkan av oberoende faktorer kommer att tas upp ytterligare under Diskussionsavsnittet.

Urvalet och antagandet om att de är mellanstatliga, trots bristen på erkännande av den attackerande parten, bygger till en del på tidigare forskning och resonemang om att storskaliga cyberattacker kräver stor kapacitet och ekonomiska medel som i huvudsak finns hos stater och inte enskilda individer.

Som tidigare så har urvalet av fall försökt fylla de kategorier som ingår i teorin om fienden i ett system. Två kategorier har varit svåra att finna jämförbara fall till. Den första är infrastrukturen. I de valda fallen så har internetinfrastrukturen blivit angripen vilket kan tolkas in under den kategorin, dock så talar teorin i huvudsak om logistiska funktioner som infrastruktur. Att det är angrepp mot till exempel järnvägssystem och flygplatser som ingår i den kategorin.
Tolkningen av vad infrastruktur kan innefatta skiljer sig. Geers förklarar cyberattacker mot infrastrukturen som att angripa ISP[43] för att slå ut kommunikation och elektricitet.[44] Den tolkningen av infrastruktur faller i teorin om fienden i ett system in i både ledarskapet och befolkningen med angrepp mot ISP och kommunikation samt organiska nödvändigheter med angrepp mot elektricitet. Detta kan alltså bli problematiskt med val av fall för att passa in i fienden i ett system. Antingen kan teorin anpassas till hur man ser på infrastruktur inom cyberkrigföring eller så behålls den i sitt ursprungsskick. Den här uppsatsen kommer att behålla teorin i sitt ursprung då det är

[41] The World Bank. Internet users (per 100 people). http://data.worldbank.org/indicator/IT.NET.USER.P2 (Hämtad 2015-05-12).
[42] Esaiasson. Gilljam. Oscarsson. och Wängnerud. *Metodpraktikan.* 108, 109.
[43] Se bilaga för begrepp och förkortningar.
[44] Geers, Kenneth. *Strategic Cyber Security.* Tallinn: CCD COE Publication, 2011. 134, 135.

fullt möjligt för en cyberattack att angripa infrastruktur som Warden förklarar den, samt att om anpassning skulle ske så finns det risk att kärnan i teorin blir påverkad.
Den andra kategorin som saknar representativa fall är försvarsmekanismer. Detta är en brist i undersökning då det inte finns några uppmärksammade fall av angrepp mot försvarsmekanismer utifrån tidigare diskuterade avgränsningar. Dock så kan det finnas en anledning till att angrepp inte riktar sig mot den kategorin om utgångspunkten är i vald teori. Fienden i ett system förklarar som tidigare att angrepp mot motståndarens försvarsmekanismer skall undvikas om möjligt, då det är denna kategori som med största sannolikhet har högst tolerans mot attacker. Med det sagt så finns det attacker som ligger och väger på kanten mot kategorin infrastruktur men i den här undersökningen så kommer de ej att klassas som det, samt bristen på fall lämnar kategorin försvarsmekanismer tom men bidrar trots det till diskussion.

3.2 Operationalisering

3.2.1 Fienden i ett System

Warden förklarar begreppen enligt följande:[45]

Ledarskap – Den delen som är högst väsentlig för att övriga delar skall fungera. Utan denna del så kan övriga delar fortsätta att fungera begränsat men inte på ett strategiskt plan. Det är ledarskapet som är en beslutsfattande del som bestämmer hela systemets väg framåt.

Organiska Nödvändigheter – Den del som förser systemet med energi och/eller omvandlar något till energi. Alltså förbrukningsprodukter som system behöver för att fungera.

Infrastruktur – Den delen som innehåller systemets fysiska ramverk. De två först nämnda delarna beslutar om hur denna del jobbar och förser den med den energi som behövs. Kan klara av problem och skador medan system kan fortsätta fungera.

Befolkningen – Består av de levande inneboende i systemet och jobbar för att hålla systemet igång. Även denna del har hög tolerans mot skador och förluster innan system kollapsar.

Försvarsmekanismer – Denna del är egentligen inte ett krav för att systemet ska fungera men blir det om systemet är hotat utifrån. Då fungerar den som ett yttre skydd och mot angrepp inom systemet som kan hota dess funktioner.

Dessa begrepp har som tidigare beskrivits operationaliserats mot olika typer av system för att påvisa liknelser. Wardens operationalisering av begreppen kopplat mot en stat som system är enligt följande:[46]

Ledarskap – En regering eller militär beslutsfattare. Dess kommunikationsmöjligheter eller dess säkerhet.

[45] Warden III. The Enemy As A System. 5, 6.
[46] Ibid. 5, 10-13.

Organiska Nödvändigheter – Energi. Det kan innefatta t.ex. elektricitet, olja, mat och pengar.

Infrastruktur – Logistik. Det kan innefatta t.ex. vägar, tågrälser och flygplatser, även fabriker.

Befolkningen – Civilbefolkning. Människorna som bor och jobbar i staten.

Försvarsmekanismer – I huvudsak militära styrkor men kan även innefatta polis och brandförsvar.

3.2.2 Effekt

Nationalencyklopedin förklarar effekt med ord som ”verkan” och ”resultat”, begrepp som effektivitet förklaras som förhållandet mellan en insats och resultat.[47] Effekt i detta sammanhang blir en analys av vad en cyberattack (insats) tillsammans med ett syfte gav för resultat. Syftet är i vissa fall mer tydligt än andra. Vid fall där syftet inte är uttalat eller otydligt så kommer det att bedömas utifrån diskussioner som har lett till det mest troliga syftet. Förenklat så handlar det om vad en stat ville uppnå med en viss cyberattack. Påverkade denna cyberattack den angripna staten på det avsedda sättet, blev de tvingade att ändra sin vilja eller avstå från förändring?

Effekten kommer att delas in i två kategorier ”Effekt” och ”Ingen effekt”. Det finns självklart problematik med denna indelning av effekt. De två kategorierna är två motpoler, de tillåter egentligen ingen gråzon. Problematiken fortsätter då: som förklarat ovan så är syftet sällan tydligt, hur kan då kategoriseringen vara så svart/vit? Det finns stora utrymmen för diskussion kopplat till vad som ville uppnås. Detta vill jag istället se som en styrka med att ha tydliga indelningar. Om uppsatsen istället skulle ha flera kategorier som kan förklara effekten så finns det stor risk att det enbart skulle skapa mer otydlighet. Ett område med redan stora frågetecken kombinerat med ett flertal bedömda effekt kategorier kan skapa stor splitting bland fallen och skapa svårigheter att dra slutsatser. Istället bidrar dessa två kategorier med ordning och tydlighet som gör det möjligt att dra slutsatser utifrån vilka cyberattacker mot vilka mål som hade någon effekt.

Denna operationalisering av begreppet effekt kan innebära en tydlig brist i uppsatsen. Indikatorerna kan vara valida utifrån det teoretiska begreppet, men hur det tas fram från empirin är värt att diskutera vidare. Ett resonemang som förs fram i Metodpraktikan är kopplat till begreppet makt, där sättet frågor ställs på påverkar om det är en upplevd eller faktisk makt som mäts.[48] På samma sätt kan detta resonemang föras kopplat till begreppet effekt. Mäter jag genom de valda källorna den faktiska effekten som cyberattackerna uppnådde eller är det enbart en återberättad upplevd effekt. Om vi istället utgår ifrån ett hypotetiskt syfte, att störa delar ur regeringen, banker och befolkningen, är då den faktiska effekten även den upplevda effekten? Det handlar om att störa människor i deras vardag genom att försvåra kommunikation och andra e-tjänster. Att då bedöma effekten handlar om vad dessa människor har upplevt

[47] Nordling, Carl. Effekt. Nationalencyklopedin. http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/effekt (Hämtad 2015-05-07).
[48] Esaiasson. Gilljam. Oscarsson. och Wängnerud. *Metodpraktikan.* 64.

som störande.
Å andra sidan kan detta även innebära ett mörkertal som påverkar bedömningen av den tydliga skillnaden mellan ”Effekt” och ”Ingen effekt”. Kan vi utesluta att en cyberattack som avser att störa och skapa instabilitet uppnår effekt bara utifrån människors uttalade upplevelser? Oavsett om cyberattackens resultat begränsas så kan vi inte utesluta att viss störning och viss instabilitet skapades, att en rädsla uppkom. Som diskuterat tidigare så har operationaliseringen av begreppet effekt ett syfte med att vara antingen svart eller vitt, antingen Effekt eller Ingen effekt. De valda indikatorerna kan därför ses som att ”Effekt” syftar till att den fulla effekten som attackens bedömda avsikt uppfylldes, medan ”Ingen effekt” syftar till att det inte skede. Med det sagt så utesluter inte indikatorn ”Ingen effekt” att den angripna staten blev helt opåverkad av cyberattacker, utan enbart att den fulla effekten inte uppnådes.

3.3 Validitet

Gällande den interna validiteten så återkopplas resonemanget till det som diskuterats i början av avsnittet Metod. Den interna validiteten bygger till stor del på om det går att dra generella slutsatser med valen av fall. Uppsatsen har alltså en god intern validitet men det beror då som sagt på att det inte finns ett stort urval av fall.

Begreppsvaliditet kopplat till teorin om fienden i ett system kan förklaras utifrån den strategi som benämns resonemangsvaliditet, att kopiera en operationalisering av tidigare forskare.[49] Jag har alltså valt att använda de indikatorer som Warden har operationaliserat fram till de kategorier som finns i teorin. Som tidigare diskuterat så finns det andra sätt att mäta begrepp som infrastruktur. Dessa kan vara bättre lämpade som indikatorer vid diskussioner om cyberkrigföring. Valet att behålla är som sagt för att behålla teorin i sitt ursprung för att inte riskera att ändra kategorier som teorin bygger på.

Mer komplicerat blir det gällande operationaliseringen av begreppet effekt. De operationella indikatorerna som har tagits fram bygger till stor del på hur begreppet effekt definieras utifrån nationalencyklopedin men hur dessa indikatorer tas fram ifrån empirin bygger till stor del på bedömningar och ”mest troliga”-scenarion. Att ta med sig till slutsatserna är då alltså validiteten kopplat till den bedömda effekten, mäter verkligen indikatorerna rätt sak.

En teori ska vara grundad i empirisk forskning och att den därifrån bildar en allmän teori.[50] Detta medför vissa tvivel om begreppsvaliditet håller fullt ut, speciellt med Wardens operationalisering av begreppen. Detta eftersom under teoriavsnittet i denna uppsats anklagas Wardens teori för att ha bristande empirisk grund, att teorin är uppbyggd från empiri som är utvald för att passa in.

För att skapa extern validitet så har större delen av empirin blivit datatriangulerad.[51] Data från de olika fallen beskrivs oftast både inifrån och utifrån, där nyhetsbyråer och regeringen som har blivit angripen beskriver vad som har hänt, samt att i huvudsak nyhetsbyråer men även forskningsinstitut utifrån beskriver vad som har observerats.

[49] Esaiasson. Gilljam. Oscarsson. och Wängnerud. *Metodpraktikan*. 66.
[50] Denscombe. *Forskningshandboken*. 6.
[51] Ibid. 186.

Att inhämta data både inifrån och utifrån en händelse behöver dock inte säkra den externa validiteten. I de fall som används i denna undersökning så är större delen av data inhämtat från stater, forskningsinstitut och nyhetsbyråer där den objektiva synen på vad som inträffat kan ifrågasättas. Oavsett om informationen kommer från den angripna staten eller från en observatör utifrån så kan dessa två parter ses som att stå på samma sida i konflikten, eller åtminstone se den anklagade angriparen som en gemensam fiende och hot. I andra fall är data bekräftat från olika rapporter och artiklar som skiljer sig i utgivare och datum/årtal.

4 Mellanstatliga cyberattacker

4.1 Estland (2007)

Cyberattackerna mot estniska websidor, både privata och offentliga började den 27e april och fortsatte med varierande intensitet under 3 veckor. Detta var en följd av upplopp dagarna innan kopplat till en förflyttning av ett andravärldskrigsminne av Sovjetunionens seger mot Nazi-Tyskland.[52]

Attackerna var uppdelade i två faser. Den första fasen mellan 27e och 29e april riktade sig främst mot regerings- och nyhetssidor.
Under denna fas var inte attackerna speciellt planerade, detta troligtvis som en snabb påföljd av uppploppen. Attackerna utfördes av enskilda individer som samordnades via hackerforum och chattar mot specifika websidor med DoS-attacker[53] som medel.[54]

Den andra fasen av attacker varade mellan 30e april och 18e maj. Här kunde högre grad av samordning ses och attackerna gjordes med mer avancerade system som botnets.[55]
Spår till politiskt viktiga händelser kunde ses då attackerna ökade. Attackerna under denna period har delats upp i fyra vågor där olika mål attackerades vid specifika datum som var politiskt viktiga. Även intensiteten i attackerna ökade och minskade mellan och under dessa vågor.
Första vågen (4e maj): DDoS-attacker mot DNS[56] och websidor genom botnet-attacker med hög precision.
Andra vågen (9e-11e maj): Den 9e maj, Rysslands Victory Day, ökade attackerna 150 % och stängde ner 58 sidor samtidigt. Målen var regeringssidor och deras officiella kommunikationskanaler. Även banker angreps under denna våg.
Tredje vågen (15 maj): DDoS-attacker mot regeringsinstitutioner samt vissa banker. Dock så hade Estland lyckats vidta motåtgärder, som att öka nätkapaciteten, vilket minskade verkan av attackerna.
Fjärde vågen (18e maj): DDoS-attacker mot regeringssidor.[57]

Huvudmål
Informationskanaler för regeringen angreps men även för den privata sektorn. Inom affärsvärlden var det bankerna som drabbades hårdast. Estlands internetinfrastruktur drabbades samt möjligheten att nå fram till 112.
De politiska målen innefattade bland annat websidor för regeringen, presidenten, premiärministern, övriga ministerier, statliga myndigheter som polisen och det ledande oppositionspartiet.De privata målen innefattade Estlands två största banker, Hansapank och SEB Eesti Ühispank, med sporadiska begränsningar i sina E-tjänster samt Estlands sex största nyhetsbyråer.
Internetinfrastrukturen som drabbades innefattade Estlands huvud-DNS samt tre stora

[52] Tikk, E. Kaska, K. och Vihul, L. *International Cyber Incidents: Legal Considerations*. Tallinn: CCD COE, 2010. 15, 16.
[53] Se bilaga för begrepp och förkortningar.
[54] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 18.
[55] Se bilaga för begrepp och förkortningar.
[56] Se bilaga för begrepp och förkortningar.
[57] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 18-20.

ISP[58], Elion Ettevõtted, Elisa Andmesideteenused och Starman samt andra internetleverantörer för statens informationskanaler.[59]

4.2 Georgien (2008)

Cyberattackerna mot Georgien började redan småskaligt den 19e juli och pågick under hela augusti med en variation av propaganda och överbelastningsattacker[60].

Den 19e juli attackerades Georgiens presidents websida och blev oanvändbar under 24 timmar. Detta var en enskild incident som fortsatte den 8e augusti där cyberattacker genomfördes mot ett flertal regeringssidor och nyhetsbyråer, både georgiska och Georgienvänliga.
Den 9e augusti attackerades Georgiens största bank, TBC. Georgien förlitar sig på att förmedla information utåt genom sina websidor och letade nu efter alternativa sätt. Ett flertal sidor flyttades till andra servers, bland annat till företaget Tulip Systems Inc., Estniska servrar, Googles bloggtjänst samt dedikerade Polens president en del på sin websida för att sprida information från den georgiska regeringen.
Den 10e augusti fortsatte attackerna mot regeringssidor men även andra websidor.
Den 11e augusti släpptes attackerna mot presidentens websida men visade nu istället ett bildspel där presidenten likställdes med Hitler. Därefter fortsatte attacker som försvårade åtkomst av presidentens websida.
Den 27e augusti genomfördes den sista större attacken mot Georgien, även nu riktat mot regeringen.[61]

Huvudmål
De politiska målen var regeringens websidor med bland annat presidentens, olika ministeriers och parlamentets websidor.
De privata målen innefattade Georgiens största bank TBC samt ett flertal nyhetsbyråer och forum.[62]

4.3 Kyrgyzstan (2009)

Den 18e januari attackerades Kyrgyzstan med DDoS-attacker. Cyberattackerna riktade sig mot landets två största ISP som ansvarade för ca 80 % av landets internetuppkoppling. Attackerna varade till slutet av januari och höll större delen av Kyrgyzstan offline vilket även innebar att i princip all e-mailkommunikation omöjliggjordes.[63]

Huvudmål
Attackerna var inte riktade mot specifika websidor utan mot ISP, alltså internetleverantörer. De två leverantörerna var ns.kg och domain.kg.[64]

---

[58] Se bilaga för begrepp och förkortningar.
[59] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 21, 22.
[60] Se bilaga för begrepp och förkortningar.
[61] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 69-71.
[62] Ibid. 71, 72.
[63] Rhoads, Christopher. *Kyrgyzstan Knocked Offline*. The Wall Street Journal. 2009-01-28. http://www.wsj.com/articles/SB123310906904622741 (Hämtad 2015-05-04).
[64] Hodge, Nathan. *Russian 'cyber militia' takes Kyrgyzstan offline?*. Wired. 2009-01-28 http://www.wired.com/2009/01/cyber-militia-t/ (Hämtad 2015-05-12).

4.4 Sammanfattande tabell av mål

	Estland	Georgien	Kyrgyzstan
Ledarskap	X	X	X
Organiska Nödvändigheter	X	X	
Infrastruktur			
Befolkningen			X
Försvars-mekanismer			

Tabell 2: Angripna mål

5 Diskussion

5.1 Estland

5.1.1 Syftet

Syftet bakom attackerna måste förstås utifrån de två faserna som beskrivits tidigare. Under den första fasen var attackerna inte speciellt sofistikerade, och det var överlag enbart enskilda individer som låg bakom dem. Här har syftet troligtvis varit av emotionell karaktär som går att koppla till omplaceringen av en bronsstaty som symboliserade Sovjetisk vinst över Nazi-Tyskland. På grund av de enskilda individerna och attackerna som mer liknar cyberbrottslighet så är det den andra fasen som är mer intressant. Med mer sofistikerade cyberattacker så krävs det mer ekonomiska medel som har diskuterats under tidigare forskning. Den samordning och precision som attackerna skedde med tyder på att det inte kan vara civila som legat bakom dem.[65] Syftet kan ha varit i den redan påbörjade instabiliteten som uppstått att fortsätta skapa oro i landet. Eftersom NATO inte klassificerar cyberattacker som ett militärt angrepp så träder artikel 5 inte in vid en sådan incident, vilket innebär att en cyberattack kan ses som ett sätt att angripa ett NATO-land utan att starta ett fullskaligt krig.[66] Om vi utgår ifrån att Ryssland var angriparen som påstås vara skyldig trots att inget hittills har gått att bevisa, så kan den andra vågen ses som en möjlighet att fortsätta skapa instabilitet.

5.1.2 Resultatet

Den inhemska ekonomin drabbades på grund av attacker som hindrade vissa internettjänster och e-mailfunktioner för både regeringen och privata delar som banker. Detta drabbade inte regeringen enbart internt utan även deras möjlighet att kommunicera med befolkningen där e-mail var huvudkanalen för kommunikation. Dock så har detta inte bedömts som en stor splittring mellan regeringen och befolkningen då attackerna enbart begränsade e-mailfunktioner under tillfälliga perioder. Internettjänsterna som utsattes för attacker gav stor påverkan hos befolkningen som till exempel inte kunde sköta sin skattebetalning eller behandla eventuella statliga bidrag, men även dessa attacker varade endast under tillfälliga perioder. Cyberattackerna skapade även svårigheter för Estland att kommunicera med omvärlden genom internet. Information som vanligtvis skickas via internet från regeringen och nyhetsbyråer om vad som sker i landet gick inte fram. Detta resulterade i att alternativa sätt att kommunicera fick tas fram.[67] Vissa sidor i Estland valde även att koppla ner sig helt från det internationella nätverket för att försvåra cyberattack mot landet och upprätthålla ett stabilt nationellt nätverk.[68]

5.1.3 Effekten

Detta innebär att effekten inte uppnådde tänkta syften från angriparen, utan enbart skapade mindre problem och irritation hos delar av befolkningen. De utanför Estland som nyttjade dessa tjänster drabbades hårdast. Att information periodvis inte gick att skicka ut ur landet verkar inte heller ha påverkad avsevärt, dels på grund av sporadisk

[65] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 23.
[66] Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. 2007-05-17. http://www.theguardian.com/world/2007/may/17/topstories3.russia (Hämtad 2015-05-08).
[67] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations.* 24, 25.
[68] Davis, Joshua. *Hackers take down the most wired country in Europe*. Wired Magazine. 2007-08-21. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (Hämtad 2015-05-14).

störning samt att delar av Estland till slut beslutade sig för att koppla bort sig från omvärlden.

5.2 Georgien

5.2.1 Syftet

Syftet med cyberattackerna mot Georgien kan ha varit varierande. Cyberattackerna verkar inte ha haft något tydligt ursprung som i Estland med uppror som sedan övergick till cyberattacker. I Georgien fanns inte samma spår av emotionella, icke samordnade attacker utan redan från början fanns likheter med Estlands andra fas. Attackerna var redan från början sofistikerade och koordinerade. Även här är det Ryssland som, på grund av bristande bevis, inofficiellt utpekas som angriparen. Dessa cyberattacker startade även i direkt anslutning till Rysslands markinvasion av Georgien. Med den precisa timingen av cyberattacker och markinvasionen samt attackernas krävande samordning och ekonomiska tillgångar stärker påståendena om vem angriparen kan ha varit.
Med denna tydliga koppling mellan en markinvasion och cyberattacker så kan ett tänkt syfte fortsätta att utvecklas. Utifrån de genomförda cyberattackerna kan vi se dem som understödjande till markinvasionen. Två tydliga sätt att se på cyberattackerna som understödjande är att de hade som syfte att antingen skapa instabilitet i landet eller störa ledarskapet i beslutsfattande. Instabiliteten kan vi se från Estland där på samma sätt som i Georgien angreps organiska nödvändigheter, banker och deras e-tjänster. Ledarskapet blev störd i sin externa kommunikation mot omvärlden men främst den interna inom landet, mot befolkningen.

5.2.2 Resultatet

Attacker mot United Telecom of Georgia gjorde servrar oanvändbara i flera dagar. Caucasus Network Tbilisi blev attackerade men flyttade sin nätverkstrafik vilket gjorde att enbart ett fåtal ”internet providers” blev påverkade. Deras fysiska infrastruktur fanns även till en del i områden där kriget pågick, vilket resulterade i att det inte enbart var cyberattacker som påverkade Caucasus Networks verksamhet.[69]
Vid de tidiga cyberattackerna påverkades regeringens kommunikation mot omvärlden och den egna befolkningen kraftigt. I huvudsak påverkades moralen hos befolkningen samt deras tro på regeringen.[70]
Det huvudsakliga resultatet som uppnåddes med attackerna är, enligt ovan, försvårad kommunikation från regeringen till omvärld och befolkning. Men även attackerna mot banker i Georgien uppnådde effekt då beslut togs att stoppa alla internettjänster som erbjöds, som därefter hölls offline under 10 dagar.[71]

5.2.3 Effekten

Som resultatet visar så uppnåddes effekt med cyberattackerna. I huvudsak var det ledarskapet och organiska nödvändigheter som blev påverkat men indirekt även befolkningen som började tappa tron på ledarskapet. Vi kan alltså se detta som en liten bricka i understödjande operationer till markinvasionen med effekt utifrån ett troligt syfte.

[69] Tikk. Kaska. och Vihul. *International Cyber Incidents: Legal Considerations*. 77.
[70] Ibid. 77, 78.
[71] Ibid. 78.

5.3 Kyrgyzstan

5.3.1 Syfte

Cyberattackerna riktades mot Kyrgyzstan som helhet då man försökte slå ut all internettrafik, istället för att rikta attackerna mot specifika mål som enskilda websidor eller DNS. Detta kan tolkas som att det är befolkningen som angrips för att uppnå ett större syfte genom påtryckning eller att ledarskapet ska tvingas att agera. Alltså antingen genom att försvåra befolkningens vardagliga liv och få dem att vända sig mot ledarskapet eller att genom en maktdemonstration visa kontroll över landets internetåtkomst.
Det finns två spekulerade syften som grund för cyberattackerna. Det första är att genom påtryckning försöka tvinga regeringen i Kyrgyzstan att kasta ut amerikanska flygvapnet som nyttjar en flygbas i landet som utgångspunkt för operationer i Afghanistan. Det andra är att förtrycka och tysta ner en motståndsrörelse som använt sig av internet för att sprida sina åsikter. [72] Då nästan hela landets internetåtkomst stängdes ner istället för att slå ut just motståndsrörelsens websidor så är det första syftet mer troligt än det andra.

5.3.2 Resultat

Den amerikanska flygbasen stod kvar efter attackerna och stängdes inte förrän i mitten av 2014 i samband med att deras trupper dras tillbaka från Afghanistan. Cyberattackerna under 2009 verkar dock inte ha lämnat regeringen i Kyrgyzstan helt opåverkade. Presidenten i landet presenterade planer på att stänga ner basen under just 2009 men dessa planer gick inte igenom utan basens beteckning byttes enbart till att vara en mellanlandningsbas.[73]

5.3.3 Effekten

Genom detta kan vi se att påtryckningarna hade en verkan på regeringen, och ett agerande framtvingades. Dock blev det ingen förändring i det då rådande läget med extern militär på Kyrgyzstans mark. Dessa cyberattacker bedöms därför inte ha haft någon effekt utifrån det troliga syftet.

5.4 Liknande mål, liknande attack men olika effekter

Enligt följande sammanfattning av vilka mål utifrån fienden i ett system och om cyberattackerna hade någon effekt så kan vi se att samma typ av attack mot liknande mål inte uppnår samma effekt. Hur kan vi förklara att överbelastningar genom DoS- och DDoS-attacker mot ledarskapet inom en stat kan upplevas så olika utifrån effekt? Där i Estland och Kyrgyzstan uppmärksammades attackerna men påverkade inte tillräckligt för en förändring i ett agerande. Medan när Georgien utsattes för liknande attacker så påverkades ledarskapet mer av svårigheter att kommunicera och förmedla information. Vidare ser vi stor skillnad i agerande mellan Estland och Georgien vid attacker mot organiska nödvändigheter, i det här faller banker. Där Estland väntade ut attackerna och lät sina e-tjänster vara kvar med begränsad möjlighet till användning under angreppsskedena, medan Georgien tog det drastiska beslutet att ta e-tjänsterna offline. Vi kan se skillnaderna mellan Georgien och Kyrgyzstan i hur befolkningen blir påverkade. Där i Kyrgyzstan var attackerna till en del riktade mot befolkningen utan att

[72] Rhoads. *Kyrgyzstan Knocked Offline.*
[73] RT. *Key US air base supplying Afghanistan closes*. 2014-06-03. http://rt.com/usa/163276-us-leave-manas-airbase/ (Hämtad 2015-05-04).

uppnå stort missnöje och tvivel på regeringen, medan det i Georgien var ett kommunikationsmedel mellan ledarskapet och befolkningen som slogs ut och bidrog till en förlorad tro på regeringen.

	Estland	Georgien	Kyrgyzstan
Ledarskap	X	X	X
Organiska Nödvändigheter	X	X	
Infrastruktur			
Befolkningen			X
Försvars-mekanismer			
Effekt		X	
Ingen Effekt	X		X

Tabell 3: Angripna mål och bedömd effekt

En del i detta kan vara det som diskuterades tidigare angående hur beroende ett land är av internet och internetbaserade tjänster. Där diskuterades samband mellan att ett land med litet beroende har högre tolerans att genomlida cyberattacker. Detta verkar till viss del stämma om vi ser på Kyrgyzstan med den låga siffran 17,0, men Georgien med en ännu lägre siffra på 10,0 påverkades kraftigt. Även Estland med höga 66,2 påverkades inte avsevärt, dock så valde de att koppla ner sig internationellt för att kunna upprätthålla det nationella internetnätverket. Detta verkar inte ha så stor betydelse i kopplingen mellan en cyberattack och den effekt som attacken får.

Om inte de mål som cyberattackerna riktades mot kan förklara effekten, vad kan då vara en tydlig faktor som skiljer fallen åt?
Den mest uppenbara faktorn är att vid cyberattackerna mot Estland och Kyrgyzstan så hade cyberattackerna självständigt ett syfte utan involvering av andra militära medel, medan cyberattackerna mot Georgien syftade till att understödja en markinvasion.

Om vi då ser på fallen utifrån följande matris så blir skillnaderna tydligare och kan vara anledningen till att uppnå effekt eller inte.

	Effekt	Ingen Effekt
Understödjande attack	Georgien	
Självständig attack		Estland, Kyrgyzstan

Tabell 4: Självständiga eller understödjande till andra militära medel

Under avsnittet tidigare forskning så är detta något Sheldon skriver om. Han talar om att genom cyberattacker påverka den strategiska miljön som försvårar motståndarens beslutsfattning och vinner i sin tur tid för övriga militära medel. Det är vad vi kan se skedde i Georgien men saknades i Estland och Kyrgyzstan.

5.5 Slutsatser

Hur kan effekten av cyberattacker förklaras utifrån Wardens teorin om fienden i ett system?
Som hittills har diskuterats så finns det problem med att förklara cyberattackers effekt utifrån Wardens teorin om fienden i ett system. Vi kan se att de mål som angrips är den typen av mål som teorin förespråkar för att uppnå störst effekt. Även teorins förespråkande av ”parallell attacks” används med flera olika typer av mål inom samma

lager, till exempel olika typer av websidor inom ledarskapet. Samt att flera lager angrips som i Estland och Georgien med ledarskapet och organiska nödvändigheter eller Kyrgyzstan med ledarskapet och befolkningen. Men trots det så förklarar inte teorin varför två fall inte uppnår effekt medan ett fall uppnår effekt.

En anledning till varför just målvalen inte kan förklara effekten av en cyberattack kan vara den begränsade tiden som till exempel överbelastningsattacker sker. Enligt rapporterna från främst Estland så påverkade cyberattackerna landets kommunikation internt och externt inom regeringen och bankernas e-tjänster, men dessa överbelastningsattacker gick enbart att upprätthålla i kortare intervaller. Det medförde möjligtvis frustration men inget större avbrott i det vardagliga livet.

Förklaringen verkar istället ligga i den andra frågan, om cyberattackerna skedde som självständiga eller understödjande attacker. Denna del visar åtminstone på en tydlig skillnad mellan de cyberattacker som uppfattades ha effekt och de som inte hade effekt.

Hur påverkas effekten om en cyberattack varit självständig eller understödjande till andra militära medel?

Som tabell 4 visar så är det denna fråga som visar på en skillnad i fallen och dess effekt. Vi ser alltså cyberattacker som uppnådde ett bedömt syfte då de kombinerades med andra militära medel. Anledningen till detta kan ligga i fortsättningen på exemplet diskuterat i den första frågan, kopplat till tid. I Georgien samordnades dessa intervaller av cyberattacker med en markinvasion. Vi ser då att det inte fanns tid att vänta ut cyberattacken för att kunna upprätta kommunikationen igen, utan agerande för att upprätta kommunikationen behövdes omgående. En cyberattack bör alltså kombineras med ett annat medel om en politisk vilja skall påtvingas för att inte ge möjligheten att enbart vänta ut attacken.

6 Avslutning

6.1 Reflektion

Först vill jag fortsätta vissa diskussioner kopplat till Metodavsnittet. Under avsnittet lyftes resonemang fram om representativa fall. Med de gjorda avgränsningarna så kan urvalet ses som representativt, vilket möjliggör generaliseringar. Med de dragna slutsatserna så är det värt att diskutera kring det som anses vara ett lyckat fall, en cyberattack som uppnådde effekt. Georgien som är detta fallet sticker ut med den slutsatsen om kombinerade militära medel. Eftersom Georgien är ensamt med denna typ av kombination med cyberattack inom kategorin subversion och en markinvasion. Kan vi då dra den generella slutsatsen att detta är nyckeln till att lyckas med cyberattacker? Självklart skapar detta problematik när vi inte kan jämföra den slutsatsen med andra liknande fall för att antingen bevisa eller motbevisa vikten av att kombinera dessa militära medel. Trots det så är den slutsatsen den tydligaste faktorn i denna undersökning som skiljer valda fall åt i att uppnå effekt med cyberattacker.
Fortsatt så kan den slutsatsen ses som en förenkling och stor avskalning av tre komplexa fall. Det är en förenkling som är gjord för att möjliggöra en generalisering, att påvisa en faktor som skiljer sig och som kan vara en av orsakerna till effekt. Den slutsatsen får dock inte ses som huvudingrediensen till lyckade cyberattacker då det troligtvis finns en mängd andra faktorer som undersökningen med dess avgränsningar och vald teori har missat. Men återigen så är detta en del i ett större pussel.

I inledningen nämndes det att mycket material kommer från CCD COE. Detta är att ses som en västerländsk källa som har en grund i NATO. I flertalet artiklar läggs Ryssland fram som den troligt ansvarige för de cyberattacker som tas upp i uppsatsen. Dock så anklagas Ryssland aldrig då det inte går att bevisa fullt ut vem som varit ansvarig, men artiklarna gör det oftast svårt att tro något annat. Om detta har betydelse för uppsatsen kan ses utifrån två synsätt där undersökningen inte handlar om att ta reda på vem som är ansvarig för cyberattackerna. Men vid diskussioner om det bedömda syftet så finns det anledning att vara kritisk till vem som påstås vara ansvarig för attackerna. Syftet diskuteras utifrån Ryssland som ansvarig för att göra det möjligt att förstå varför cyberattackerna kan ha genomförts. Om den ansvarige skulle vara en annan stat så kan syftet vara något helt annat och påverka undersökningen.
Under validitetsavsnittet togs detta till viss del upp där försök att undvika påstående och felaktig information gjordes genom datatriangulering, men även den höll sig på en västerländsk sida. Detta kan då innebära stora brister i undersökningen och bör tas hänsyn till om en annan stat än Ryssland påvisas ansvarig för valda fall.

6.2 Resultatens betydelse för yrkesutövningen

Resultatens betydelse ligger på en operativ nivå men kan ha betydelse även på en taktisk nivå. Det handlar om att skapa en förståelse för cyberkrigföring och nyttjande av cyberattacker som en del i informationskrigföringen. På den taktiska nivån får resultaten betydelse genom att se cyberspace enbart som ett ytterligare område att upprätta kommunikationskanal. Att det taktiskt kan vara värt att blockera dessa kanaler på samma sätt som radiostörning sker.
Om vi istället ser det på en operativ eller till och med strategisk nivå så handlar det om att nyttja cyberattacker för att uppnå det stora syftet med hela operationen. Här behöver det inte enbart vara genom att störa kommunikationskanaler, utan det kan även ses som

störning av nätverk som hanterar e-tjänster som inte direkt är kopplade till motståndarens militära frontförband.

6.3 Fortsatt forskning

Den fortsatta forskningen kan ta två vägar utifrån denna uppsats. Den första vägen att genom andra teorier försöka förklara andra faktorer än cyberattacken som understödjande till andra militära medel som anledningen till att uppnå effekt. En teori, till skillnad från fienden i ett system, som inte fokuserar på vilken typ av mål som angrips.
Den andra vägen är att utbreda undersökningen av andra typer av cyberattacker som denna uppsats har avgränsat sig från. Att göra det med teorier som fienden i ett system eller andra teorier som utgår ifrån vilka mål som angrips.

7 Litteratur och referensförteckning

7.1 Litteratur

Czosseck, Christian. och Geers, Kenneth. *The Virtual Battlefield: Perspectives on Cyber Warefare.* Amsterdam: IOS Press BV, 2009.

Denscombe, Martyn. *Forskningshandboken*. 2. uppl. Lund: Studentlitteratur AB, 2009.

Esaiasson, Peter. Gilljam, Mikael. Oscarsson, Henrik. och Wängnerud, Lena. *Metodpraktikan*. 3. uppl. Vällingby: Norstedts Juridik AB, 2010.

Geers, Kenneth. *Strategic Cyber Security.* Tallinn: CCD COE Publication, 2011.

Rid, Thomas. *Cyber War Will Not Take Place*. London: C. Hurst & Co. 2013.

Tikk, E. Kaska, K. och Vihul, L. *International Cyber Incidents: Legal Considerations*. Tallinn: CCD COE, 2010.

Widén, Jerker. & Ångström, Jan. *Militärateorins Grunder.* Stockholm: Försvarsmakten, 2005.

7.2 Elektroniska källor

Betz, David. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed. *The Journal of Strategic Studies* 35 no. 5 (October 2012): 689-711. DOI: 10.1080/01402390.2012.706970.

Butler, Sean. Refocusing Cyber Warfare Thought. *Air & Space Power Journal* 27 no. 1 (January-February 2013): 44-57. http://130.252.58.169/docview/1318929576?accountid=8325 (Hämtad 2015-04-03).

Davis, Joshua. *Hackers take down the most wired country in Europe*. Wired Magazine. 2007-08-21. http://archive.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (Hämtad 2015-05-14).

Hodge, Nathan. *Russian 'cyber militia' takes Kyrgyzstan offline?*. Wired. 2009-01-28 http://www.wired.com/2009/01/cyber-militia-t/ (Hämtad 2015-05-12).

Janlert , Lars-Erik. Cyberspace. Nationalencyklopedin. http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/cyberspace (Hämtad 2015-05-07).

Kello, Lucas. The Meaning of the Cyber Revolution: Persils to Theory and Statecraft. *International Security* 38 no. 2 (Fall 2013): 7-40. DOI: 10.1162/ISEC_a_00138.

Llongueras, Adrianna. *Moonlight Maze. The beginning of a new era*. Academia. http://www.academia.edu/6182336/MOONLIGHT_MAZE._The_beginning_of_a_new_era (Hämtad 2015-05-07).

McCarthy, Thomas David. *Traveling Domain Theory: A Comparative Approach for Cyber-space Theory Development.* Diss., The Fletcher School of Law and Diplomacy, 2012. http://pqdtopen.proquest.com/doc/1029868522.html?FMT=AI (Hämtad 2015-04-03).

Nordling, Carl. Effekt. Nationalencyklopedin. http://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/effekt (Hämtad 2015-05-07).

Poirier, William. och Lotspeich, James. Air Force Cyber Warfare: Now and the Future. *Air & Space Power Journal* 27 no. 5 (September-October 2013): 73-97. http://130.252.58.169/docview/1475073629?accountid=8325 (Hämtad 2015-04-03).

Rhoads, Christopher. *Kyrgyzstan Knocked Offline*. The Wall Street Journal. 2009-01-28. http://www.wsj.com/articles/SB123310906904622741 (Hämtad 2015-05-04).

Rid, Thomas. Cyber War Will Not Take Place, *Journal of Strategic Studies* 35 no. 1 (2012): 5-32. DOI: 10.1080/01402390.2011.608939.

RT. *Key US air base supplying Afghanistan closes*. 2014-06-03. http://rt.com/usa/163276-us-leave-manas-airbase/ (Hämtad 2015-05-04).

Sheldon, John. Deciphering Cyberpower: Strategic Purpose in Peace and War. *Strategic Studies Quarterly* 5 no. 2 (Summer 2011): 95-112. http://130.252.58.169/docview/871291547?accountid=8325 (Hämtad 2015-04-03).

Stuxnet: targeting Iran's nuclear programme. *Strategic Comments* 17 no. 2 (2011): 1-3. DOI: 10.1080/13567888.2011.575612.

The World Bank. Internet users (per 100 people). http://data.worldbank.org/indicator/IT.NET.USER.P2 (Hämtad 2015-05-12).

Traynor, Ian. *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian. 2007-05-17. http://www.theguardian.com/world/2007/may/17/topstories3.russia (Hämtad 2015-05-08).

Warden III, John. The Enemy As A System. *Airpower Journal* (Spring, 1995). http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm (Hämtad 2015-04-03).

Bilaga: Begrepp och förkortningar

Bandbredd: Ett mått på den mängd data som kan hanteras. Alla internetfunktioner och websidor har en maxgräns på bandbredden och den data som kan hanteras per sekund.

Botnet: Datorer infekterade med virus som möjliggör en hackare fjärrkontroll av dessa datorer. Det handlar oftast om tusentals datorer som kontrolleras samtidigt, och möjliggör uppgifter som en enskild dator inte skulle klara av.

Defacement: Inom cyberattacker syftar detta begrepp till att deformera en websida, som till exempel kan syfta till att förlöjliga innehavaren av websidan eller för att sprida propaganda som ska se ut att komma från innehavaren.

Denial of Service (DoS) & Distributed Denial of Service (DDoS): Överbelastningsattacker som kan användas mot websidor för att överbelasta bandbredden, vilket stoppar åtkomsten till websidan. Det kan även innefatta massutskick av skräppost till e-mailadresser som även här överbelastar funktionen och nekar åtkomst och användning. Dessa typer av attacker sker ofta genom användning av botnets.

Domain Name System (DNS): Ett system som kopplar samman internetadresser, som till exempel www.namn.se, med en IP-adress.

Internet Protocol Address (IP-adress): En siffer kombination som varje dator har om den är ansluten till internet. Det är genom denna adress som datorn identifierar sig och kommunicerar på internet.

Internet Service Provider (ISP): Internetleverantörer som erbjuder tjänsten att koppla upp sig mot internet.