Stuxnet-attacken mot Iran

Strukturell realism i informationsrevolutionens tidsålder

Erik Ryd

Institutionen för Säkerhet, Strategi och Ledarskap,
Försvarshögskolan Ht 13

Statsvetenskap, Påbyggnadskurs
Inriktning Säkerhetspolitik
Delkurs 3

Handledare: Simon Hollis
Examinator: professor Jan Hallenberg

Abstract

This study aims to explain the Stuxnet-attack against Iran in 2009-2010 by using the IR-theory of structural realism. By doing so the theory also faces the challenge of the impact of the information revolution on security and international relations. The structural realism that is at hand is that of Kenneth Waltz and his *Theory of International Politics* from 1979.

The study reaches the conclusion that Waltzs focus on the structure of the international system and the distribution of capabilities applies well to the case of Stuxnet as a cyber attack. The creators of the sophisticated Stuxnet, USA and Israel, also indicates that when it comes to this certain aspect of the information revolution and IR, states seem to still be the main actor.

Finally the character of one of the major features of the Stuxnet-attack; the internet, is shown to have an anarchic structure that fits well as an extension of the realist view of the international system.

Keywords: Stuxnet, Structural realism, Kenneth Waltz, Information revolution, Security, IR-theory

Innehållsförteckning

1. Inledning

1.1. Förändring, utveckling och IR-teorier

Vi skapar den, lever i den och påverkas av den. Förändring är ett konstant tillstånd för vilket människan och den värld hon omges av, befinner sig i. Historien bakom oss utgör en serie av bevis för detta. Jordbruksrevolutionen, med utgång i bördiga halvmånen, tog oss ifrån jägarsamhället och in i de första civilisationernas tid. Med en stark utveckling av agrarteknik möjliggjordes formandet av de första städerna och utvecklandet av de första samhällena. Den första, andra (och möjligen tredje[1]) industriella revolutionen gav en helt ny form av massproduktion, ökade transportmöjligheter och en snabbt tilltagande urbanisering. Teknisk utveckling har onekligen varit en stor faktor bakom framväxten av dagens värld. Och det är i dagens värld denna studie ämnar göra sitt avstamp, en värld som i hög grad har formats av den senaste revolutionen inom människans utvecklingshistoria; informationsrevolutionen[2]. Allt billigare och mer lättillgänglig informations- och kommunikationsteknik, även kallad ICT[3] har gjort att enheter som datorer och telefoner ökat drastiskt under de senaste åren (N. Choucri 2000, 248–252). Med dessa enheter väl uppkopplade mot, den kanske största symbolen för informationsrevolutionen; cyberrymden[4], eller internet, har de alla kapaciteten att

[1] Jeremy Rifkin pekar ut den tredje industriella revolutionen, i boken *The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World*, som en vision av vad "internet teknologin och förnybara energikällor" kommer att tillföra mänskligheten(Rifkin 2011).

[2] Omnämns också ibland som steget in i den ”Digitala Tidsåldern” (Eriksson and Giacomello 2006, 223)

[3] “information and communication technologies”

[4] Begreppet “cyberrymden” myntades av William Gibson (1984) och står, oftast i form utav Internet, som ikon för den digitala tidsåldern.

tillgå en historisk rekordmängd med information. Detta är förmodligen det i vardagen mest uppenbara som informationsrevolutionen gjort för oss. Via informationsteknisk[5] infrastruktur söks, distribueras och sparas idag en näst intill oöversiktlig mängd information Men i detta oupphörliga flöde av i grunden ettor och nollor finns också den information och kod som till exempel regalerar både vatten, gas och elektricitet. Även den data som möjliggör det komplexa finansiella system som hela samhällen idag bygger på tar sig fram via IT-infrastrukturen. Det har för oss möjliggjorts att omstrukturera våra samhällen till den grad att vi nu baserat stora delar av samhällsstrukturen på fiberkablar, servrar, uppkopplingsbara enheter och den virtuella värld som tagit form där emellan. Denna utveckling är förmodligen på gott och ont men den har lett oss till ett ofrånkomligt beroende. Innebörden av ett beroende är att någonting måste finnas eller vara möjligt att tillgå för att den egna tillvaron skall kunna fortgå. Informationsrevolutionens frukter, som vi nu håller på att bli mer och mer beroende av, medför att vi har fått ytterligare en sektor att skydda för att det egna samhället skall kunna fortgå (Geers 2011, 10; Adams 2001, 98). Det vi är beroende av blir oundvikligen en del av det vi vill skydda för att uppnå säkerhet.

Säkerhet är ett omtvistat begrepp inom studierna av de internationella relationsteorierna[6]. Diskursen har huvudsakligen gått kring vad som skall ingå i begreppet säkerhet. Skall de traditionella värdena som staters tillgångar och överlevnad var det enda eller borde begreppet säkerhet vidgas till att innefatta även

[5] Hädanefter ”IT”

[6] Hädanefter IR/IR-teori

företags säkerhet och individers trygghet?[7] Historiens gång och de tekniska utvecklingar den haft har med all sannolikhet påverkat de olika idéströmningar som lett fram till dagens IR-fält och dess syn på säkerhet. Allt ifrån den industriella revolutionens materiella bidrag till 1900-talets blodiga världskrig, till klyvandet av den första atomen och därmed utveckling som ledde till skapandet av kärnvapen och det Kalla Krigets struktur har visat detta. Men har informationsrevolutionen haft konsekvenser för säkerheten inom internationella relationer och hur har dessa tagit sig uttryck i så fall?

1.2. Stuxnet-attacken mot Iran

Den 17 juni 2010 fick en anställd på datasäkerhetsföretaget VirusBlockAda, i Minsk, in en rapport om en klients problem gällande en dator som fastnat i rebootläge(datorn startade om sig oupphörligt). Klienten i fråga befann sig i Iran. Detta kom att bli upptäckten av den kod som utgjorde viruset som först fick namnet ”Rootkit.TmpHider” (VirusBlockAda 2013) men som sedan skulle komma att kallas ”Stuxnet”. Virusets ändamål var från början okänt men i och med en grundlig analys av koden kunde ett team vid antivirusföretaget Symantec förstå dess slutmål:

En anläggning utanför staden Natanz i centrala Iran, syftet:

Att slå ut centrifuger för anrikningen av uran.

En främmande makt ville förhindra Irans planer på att skaffa sig möjligheten till tillverkandet av egna kärnvapen, metoden och medlen för att uppnå det:

Konstruerandet av en bit skadlig kod som efter sitt frisläppande tog sig fram via

[7] Detta är till stor del vad debatten inom IR-fältet gått ut på (Morgenthau, Thompson, and Clinton 2006; Keohane and Nye 1977; Buzan, Wæver, and Wilde 1998; Mearsheimer 2001)

olika former av IT-infrastruktur för att nå sitt mål där den orsakade direkt fysisk skada på maskineri avsett för anrikningen av uran.

Den 1 juni 2012 publicerade *The New York Times* en artikel där man avslöjade en amerikansk-israelisk operation med kodnamnet ”Olympic Games” (Sanger 2012). Operationen hade utgjorts av en serie cyberangrepp mot Irans misstänkta urananrikning avsett för skapandet av kärnvapen[8].

1.3. Problemformulering

1900-talet och början på 2000-talet utgör därmed en serie av exempel på hur både IR-teorierna och tekniken utvecklats. Denna utveckling kan verka göra formulerandet av teorier som försöker beskriva verkligheten omöjliga. Vissa aspekter av internationella relationer är kanske förändrade för alltid till följd av den tekniska utvecklingen. Men gäller detta för alla aspekter? Hur kan vi förstå Stuxnet-attacken mot Iran när så många till synes nya element är inblandade? Och hur mycket har egentligen nuvarande IR-skolor bemött den pågående informationsrevolutionen? Få försök har gjorts att applicera de olika skolornas teoretiska ramverk för en analys av konsekvenserna av denna tekniska utveckling, vilket Johan Eriksson och Giampiero Giacomello uppmärksammar i artikeln ”The Information Revolution, Security, and International Relations: (IR)relevant Theory?” (2006, 222). I denna artikel lyfts frågan om hur informationsrevolutionen påverkat ”säkerhet” samt vad existerande IR-teorier kan ha att säga om denna utmaning. Tre, generaliserade, IR-skolor granskas efter vad var och en kan ha att säga om säkerhet i denna digitala tidsålder. De utvalda skolorna är konstruktivismen, liberalismen och realismen. Eriksson och Giacomello sammanfattar

[8] Då Stuxnet-attacken utgör fallet och därmed empirin för denna studie återges hela händelseförloppet utförligt i stycket “Empiri: Stuxnet-attacken”.

vad de kommit fram till gällande IR-teorierna och säkerhet efter informationsrevolutionens intåg med:

”Liberalism and constructivism nominally seem to have more to say about our topic than is the case with realism.” (2006, 235–236). Kan då verkligen någon del av den realistiska skolan användas för att förstå en aspekt av informationsrevolutionens påverkan på internationella relationer som fallet Stuxnet?

2. Syfte

Den här studien syftar till att undersöka och förklara Stuxnet-attacken. Undersökandet av attacken bör påvisa vilka aktörer som har varit inblandade och vilka motiv dessa haft. Med rätt vald teori kan sedan aktörernas roll och motiv samt orsakerna till dessa förklaras. Stuxnet-attacken som fall är intressant i sig då den av många anses vara nydanande som cyberattack[9]. Teorin som valts för att förklara Stuxnet-attacken är Kenneth Waltzs strukturella realism.

Att Waltzs version av realismen kommer att användas för att förklara fallet gör studien än mer intressant att genomföra av tre anledningar. För det första formulerades den som IR-teori i en tid där informationsrevolutionen inte slagit igenom ännu[10]. För det andra härstammar teorin, och en del centrala teman inom den från den större realistiska skolan som kan spåra sina rötter långt bakåt i tiden. Studien ämnar sålunda förklara ett nydanande fall med en på många sätt traditionell och gammal teori. För det tredje tillmäts den realistiska skolan, och specifikt Waltzs strukturella realism som minst förklaringskraftig av IR-teorierna i informationsrevolutionens tidsålder av Eriksson och Giacomello (2006, 235).

Den här studien ämnar visa att det finns anledning att ifrågasätta denna brist på tilltro till Waltzs teori.

Här ligger också kopplingen till tidigare forskning. I och med syftet att undersöka och förklara Stuxnet-attacken mot Iran kan förhoppningsvis vissa styrkor hos Waltzs strukturella realism hittas. Som tidigare nämnt har applicerandet av existerande IR-

[9] Stuxnet-attacken som nydanande cyberattack (Zetter 2011; Clayton 2011; Maclean 2010)

[10] Den direkta revolutionerande effekten av informationsteknologierna kan möjligen ses som något förmildrande då TV och radio spred information väl före Waltzs tid. Men den den stora skillnaden ligger i den magnitud av information och möjliga uppkopplingspunkter till denna som blev möjliggjordes via bl.a. internet (Eriksson and Giacomello 2006, 224)

teorier på informationsrevolutionens konsekvenser inom IR och säkerhet varit få[11] och en av de tyngsta och möjligen första bidragen sätter ingen större tilltro till realismen och än mindre Waltzs gren av den.

Resultatet från denna studie kan förhoppningsvis placera den strukturella realismen som möjlig teori för att förklara framtida, liknande, fall inom IR-fältet.

2.1. Frågeställning

Frågeställningen som skall besvaras med hjälp av Waltzs strukturella realism är:

Vilka mekanismer låg bakom Stuxnet-attacken mot Iran och hur kan dessa ses mot bakgrunden av informationsrevolutionen?

För att göra frågeställningen och vad som krävs för att besvara den mer begripligt följer här en kort förklaring.

För att mekanismerna bakom själva attacken skall kunna skönjas och förstås måste bakomliggande aktörer finnas. I sin tur skall dessa aktörers motiv klargöras. Slutligen skall drivkrafterna bakom dessa motiv kunna redogöras för. Med besvarandet av hur allt detta kan ses mot bakgrunden av informationsrevolutionen vävs aspekterna av den nya tidens teknik och dess inverkan på säkerhet och IR in.

2.2. Avgränsningar och dess motiveringar

Den största faktorn för de avgränsningar som gjorts i denna studie är det utrymme med tid och storlek som givits. Valet av att göra en fallstudie baseras bland annat på de naturliga avgränsningar som fås kring tid och rum och där med mängden

[11] Den tidigare forskningen på området redogörs mer utförligt i avsnittet Tidigare forskning.

underlagsmaterial.[12] Att endast ett fall; Stuxnet-attacken, tagits upp beror på två faktorer: den första hänger samman med det innan nämnda; den givna tiden och storleken för studien. Den andra faktorn har att göra med det begränsade material som finns att tillgå gällande olika aktörers agerande i framförallt cyberrymden[13] men också kring de fall där effekterna eller produkterna av informationsrevolutionen tydligt haft en roll. Eftersom att studiens mål är att undersöka och förklara Stuxnet-attacken med hjälp av den strukturella realismen vore det möjligen intressant att även analysera andra falla av cyberattacker. Detta då applicerandet av Waltzs teori på även dessa fall ytterligare skulle kunna påvisa dess tillämpbarhet eller brister. Men när det kommer till cyberattacker är Stuxnet i dagsläget det enda fallet som är tillgängligt för en heltäckande och djupare granskning. Stuxnet-attacken har till skillnad från andra uppmärksammade cyberattacker blivit så pass kartlagd, tack vare tekniskt detektivarbete och medierapportering, att en studie av den som fall nu är möjligt. Detta konstaterar bl.a. Jon Lindsay i artikeln ”Stuxnet and the Limits of Cyber Warfare” (2013, 368[14]). Vad detta innebär för studiens generalisering utvecklas i Metodavsnittet.

Att avgränsningen gjorts till att endast en IR-teori valts för denna studie ligger dels i den återkommande tids-och-storleks-faktorn. Valet att använda enbart Waltzs

[12] Ytterligare anledningar för valet av fallstudie som metod tas upp i Metod-stycket.

[13] Med cyberrymden åsyftas här den elektroniska värld som kopplar samman en mäng IT-enheter, vanligen likställt med Internet.

[14] - ”While in principle very different types of cyber attacks than Stuxnet are imaginable, this case has the distinction of being the only historical case available for scrutiny. A complete account of this episode must await disclosure of data from both sides of the attack, but it is now at least possible to begin testing the theoretical claims of the strategic consequence of cybersecurity.”

version av realismen togs dessutom med utgång i att det för det första blir allt för brett och på många ställen inre kollisioner[15] att använda ”realismen” som teoretisk grund till uppställandet av analysverktyg. För det andra så har Waltzs strukturella realism, inte oförtjänt, kommit att ses som ett steg mot ett mer vetenskapligt närmande av IR (Guzzini 1998, 127–128; Eriksson and Giacomello 2006, 228). Detta i relation till framför allt Morgenthaus filosofiska koppling mellan människans natur och uppställandet av en rad objektiva lagar för hur IR i grunden fungerade (Korab-Karpowicz 2013).

2.3. Tidigare forskning

Som tidigare nämnt så konstaterar Eriksson och Giacomello vid författandet av sin artikel ”The Information Revolution, Security, and International Relations: (IR)relevant Theory?" att det gjorts få försök att applicera existerande IR-teorier på informationsrevolutionen och dess konsekvenser på säkerhet (2006, 222[16]). Detta gör att ytterst lite tidigare forskning som är relevant för denna studie finns att tillgå. Mängden krymper dessutom när fokuset smalnar till användandet av den realistiska IR-skolan och mer specifikt Waltzs strukturella realism. Eriksson och Giacomello kommer dock fram till ett par konkreta och intressanta slutsatser gällande vad de tre IR-skolorna Konstruktivismens, Liberalismen och Realismen kan ha att säga om denna nya utmaning.

Konstruktivismens fokus på symboliska, retoriska och identitetsbaserade aspekter

[15] T.ex. avvikandet mellan Morgenthaus fokus på enheternas roll i ett system(2006, 4–5) jämfört med Waltz syn på systemets påverkan på enheterna(1979, 114–116)

[16] - "*In particular, very few attempts have been made to apply international relations (IR) theory in analyzing the information revolution, an exercise which seems warranted both for the understanding of the impact of the information revolution on security and for the development of IR theory.*"

verkar vara väl tillämpbara för analysen av den digitala tidsålderns säkerhet. Liberalismens syn på en bredare skara av aktörer där många har transnationell kapacitet lyfts fram tillsammans med ”sårbarheten av interdependens”, ekonomiska nätverk samt den konstanta perforeringen av före detta suveräna gränser.

Realismen bedöms tackla den digitala tidsåldern som den tacklat andra drag av globaliseringen – genom att ignorera den. Antigen kan informationssäkerhet tillmätas sfären politisk ekonomi eller möjligen den inhemska politiken. Ingen av dessa sfärer anses passa särskilt bra för vare sig neorealismen eller den klassiska realismen. Klassisk realism skulle möjligen kunna närma sig utmaningen genom att titta på de strategiska aspekterna där informationskrigföring är ett nyckelbegrepp. Enligt författarna blir alltså detta en teknologisk fortsättning på psykologisk krigföring och möjligen den nytillkomna elektroniska krigföringen.

Men utanför detta perspektiv går analysen inte bortom de rent militära aspekterna eller det statscentrerade fokuset. Kenneth Waltzs strukturella realism ses som den minst förklaringskraftiga då den ”enbart håller en hög logisk konsekvent men inte ses som relevant för studier av den verkliga världen” (Eriksson and Giacomello 2006, 228–229). Att det som görs i Eriksson och Giacomellos artikel är på en förenklad och generell nivå, t.ex. de olika IR-skolorna och konklusionen om deras respektive förklaringsförmågor, kan förslagsvis ha att göra med det givna omfånget ett arbete kan ha i artikelform. Dessutom är den generaliserande sammanställningen av realismens och de andra IR-teoriernas grunddrag täckande och tillräcklig i den meningen att den kan användas för deras syfte[17]. Med tanke på att de även i någon

[17] Syftet: “The purpose of this article is twofold: to analyze the impact of the information revolution on security and to clarify what existing inter- national relations theory can say about this challenge”(Eriksson and Giacomello 2006, 221)

form bröt ny mark så bör artikeln inte ses som bristfällig utan snarare som skapandet av en grund att bygga vidare på. Det som framkom om realismens möjligheter i Eriksson och Giacomellos artikel har nu redogjorts för i stycket ovan. Men vad har hänt efter denna nydanande artikel? Litteratur kring framförallt cyberrymden, säkerhet och internationella relationer har inte saknats[18], vare sig före eller efter artikeln, och utvärderingarna av informationsrevolutionens konsekvenser inom säkerhetsområdet är än mer utförliga[19]. Det är emellertid inte någon som direkt utvecklat det Eriksson och Giacomello påbörjade i och med försöket att applicera redan existerande IR-teorier. Att genomdriva studier om hur säkerhet och grunden för internationella relationer har påverkats av t.ex. cyberrymdens expansion och samhällets allt större beroende av IT-infrastruktur är dock inte på något sätt irrelevant. Genom studerandet av detta kan vi få en bättre kunskap och förståelse om vilka aktörer som blivit relevanta att studera, vilka nya medel som står till buds för att nå olika mål samt vad som uppfattas som reella hot kontra reella händelser. Allt detta kan bidra till att lägga en god grund för analysen av existerande IR-teoriers förklaringsmöjligheter men det är ingen analys i sig.

Detta är en lucka i tidigare forskning som behöver belysas och förhoppningsvis kan denna studie börja fylla i detta tomrum i och med applicerandet av Waltzs teori på Stuxnet-fallet.

---

[18] Se *Information technologies and global politics*(Rosenau and Singh 2002), *Power and security in the information age : investigating the role of the state in cyberspace*(Dunn Cavelty, Mauer, and Krishna-Hensel 2007), *Inside Cyber Warfare*(Carr 2012).

[19] Natos CCDCOE har bl.a. släppt ett antal rapporter, artiklar(CCDCOE 2013a) och böcker(CCDCOE 2013b) gällande detta.

Avsaknaden är dock inte total när det kommer till applicerandet av existerande IR-teorier efter The Information Revolution, Security, and International Relations: (IR)relevant, Theory (Eriksson and Giacomello 2006) men den är sparsam.

I boken *Cyberpolitics in international relations* (Nazli Choucri 2012) görs ett antal direkta konstateranden gällande realismen och dess förklaringsmöjligheter inom framför allt cyberrymdens påverkan på IR. Det första som pekas ut är dess brister gällande fokuset på ”major power politics” då cyberrymden är tillgänglig för ”alla” (Nazli Choucri 2012, 14). Detta byggs på med konstaterandet att i en värld där cyber-baserade interaktioner influerat mänskliga aktiviteter på alla nivåer. Tack vare detta finner sig den för traditionell teori (läs realismen) centrala staten i en allt mer komplex värld (Nazli Choucri 2012, 16). Utöver detta pekas militariserandet av cyberrymden ut som något som faller inom realismens ramar. Choucri menar att det militära bruket av cyberrymden är en ”naturlig förlängning av användandet av avancerade informationsteknologier, jämte behovet av att utveckla organisations och institutionella förmågor” (Nazli Choucri 2012, 148). Vidare pekas USAs roll som dominerande inom skapandet och kontrollerandet av IT-infrastrukturen som direkt relaterat till den maktbaserade politik som realismen håller centralt för IR (Nazli Choucri 2012, 231). Detta är möjligen en fortsättning på det av Eriksson och Giacomello påbörjade men det tillför inte särdeles mycket. Det första konstaterandet; att det snäva fokuset på stater, samt deras maktpolitik, inte är tillräckligt då cyberrymden möjliggör uppträdandet av en mycket bredare skara aktörer, pekas ut i styckena om realismen i Eriksson och Giacomello(2006, 229, 336). Så är även fallet med konstaterandena om den allt mer komplexa världen runt staterna som orsakats av informationsteknologierna och militariserandet samt den

naturliga förlängningen av användningen av avancerade informationsteknologier (Eriksson and Giacomello 2006, 228–229, 236). Hur USAs dominans på cyberarenan är relevant för realismens maktfokus är dock något som kan flaggas för som nytillkommet. Choucri applicerar fortfarande inte realismen på något specifikt fall och än mindre den strukturella realismen.

Det görs dock i *Cyberspace and International Relations* (Kremer and Müller 2014). I denna bok kommer ett flertal ytterst viktigt bidrag till applicerandet av IR-teori, däribland realismen, på informationsrevolutionens konsekvenser inom säkerhet och internationella relationer. I kapitlet ”In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare” av Hanna Samir Kassab görs ett flertal konkreta konstateranden kring framförallt Waltzs strukturella realism(Kassab 2014). Fokuset i kapitlet ligger på ”deterrence theory”[20] och hur denna teori åter kan bli relevant i cyberrymden. Författaren menar att om denna nya arena skulle få ett tillräckligt bra försvar och defensiva möjligheter skulle detta kunna leda till avskräckning för genomförandet av cyberattacker och därmed skulle ökad stabilitet nås (Kassab 2014, 75). För att kunna återkoppla till Kalla Krigets stabilitet mellan kärnvapenmakterna används Waltzs strukturella realism. Detta på grund av Waltzs teoris förklaringsförmåga och fokus kring maktbalansen under just denna period. Kassab frågar sig inledningsvis om strukturell realism kan ha något att säga om cyberkrigföring. Svaret blir ett direkt ja då Kassab menar att cyberkrig är kopplat till distributionen av förmågor och kapaciteter, relativ makt och

[20] Avskräckningsteori, främst kopplad till kärnvapenmakter och Kalla Krigets ”mutual assured destruction”: både USA och Sovjetunionen kunde uppskatta att kostanden för att avfyra sina kärnvapen var för stor; alltså infann sig en stabilitet mellan parterna.

därmed överlevnaden för staten i det internationella systemet (Kassab 2014, 63)[21]. Kassab använder sig dock av Morgenthaus definition av makt för att kunna tillgodogöra sig ett vidare begrepp för vad som skall kunna räknas som makt (Kassab 2014, 60, 63–64).

Här har vi sålunda ett undantag från tidigare forskning kring informationsrevolutionens produkter, säkerhet och realismen som IR-teori.

I och med främst Kassabs applicerande av traditionella IR-teorier på nya fenomen som cyberkrigföring har sålunda relevant tidigare forskning för denna studie tagit sig framåt sedan Eriksson och Giacomellos artikel 2006.

2.4. Begreppsutveckling: Cyberattacker

Centralt för studien är som tidigare nämnt fallet som skall analyseras. Vad Stuxnet-fallet är ett *fall av*[22] är cyberattacker vilket i sin tur är en aspekt av informationsrevolutionens konsekvenser på säkerhet inom internationella relationer. Men vad har begreppet cyberattack för egentlig innebörd? Av vad studien redan berört angående begreppet så är innehåller det för det första en aggressionsdimension och för det andra användandet av teknik (upp)kopplat till cyberrymden. För att mer precis kunna klargöra innebörden har studien lutat sig mot Kenneth Geers (2011, 137) definition av cyberattacker som i sin tur uppdelas i tre typer. Tabellen på nästa sida illustrerar dessa typer.

[21] Allt detta som är kopplat till Waltzs strukturella realism återkommer studien till under stycket ”Walts strukturella realism: Theory of International Politics” i teori-avsnittet.

[22] Diskussionen kring detta ligger under Metod-avsnittet

	Typ av attack	Exempel på attack
Konfidentialitet	Angriparen tar sig in i ett nätverk där denne sedan kan observera och tillgodogöra sig den befintliga informationen.	"GhostNet "- Ett cyberspinage-nätverk som tagit sig in i över 1000 datorer i 103 länder. Målen var diplomatisk, politisk, ekonomisk och militär information.
Integritet	Icke auktoriserat ändrande av befintlig information i t.ex. en databas. Kan fungera som sabaotage för kriminella, politiska eler militära mål.	Stater som censurerar Google-sökningar återger bara delar av sökmotorns förslag till slutanvändaren.
Tillgänglighet	Målet är att hinda auktoriserade användare från att tillgå vissa system eller data. Brukar kallas "denial-of-service (DoS).	2007 slogs Syriskt luftvärn ut av en cyberattack precis innan det Israeliska flygvapnet demolerade en Syrisk kärnkraftsreaktor.

Tabellen ovan är sammanställd för denna studie och är baserad på Kenneth Geers (2011, 137)

Som tabellen visar så finns det tre grundläggande typer av cyberattacker. Från dessa tre typer kan sedan alla attacker i cyberrymden härledas.

Efter att ha konsoliderat tabellen kan slutsatsen dras att Stuxnet-attacken hamnar inom *tillgänglighets*typen av cyberattacker. Angriparen har hindrat användare och dessutom maskineri från att kunna uppfylla sina uppgifter och funktioner genom en attack via cyberrymden. Presentationen av empirin senare i studien kommer visa att bl.a. förarbetet till attacken även innehöll element av de andra typerna av attacker. Sålunda är innebörden och de olika varianterna av cyberattacker redogjorda för.

3. Teori: Realismen

Teorin som skall ligga till grund för de analytiska verktyg studien ska bearbeta det empiriska materialet med är som redan nämnt en gren av den realistiska skolan. Mer specifikt har valet fallit på Waltzs strukturella realism med utgång i hans verk *Theory of International Politics* från 1979.

För att kunna ge en tillförlitlig och tillräckligt utförlig bild av studiens teori så kommer detta stycke inledas med en kortare redogörelse för realismens väg fram till Waltzs strukturella realism. Denna presentation görs med anledning av att Waltz teori, som de flesta teorier, inte fötts ur intet. I stället är den en utveckling och fortsättning på en lång och anrik skola inom IR-teorin.

Till hjälp för stycket nedanför har studien lutat sig på Magnus Christianssons *Säkerhetspolitisk Teori* (Christiansson 2004) som får tjäna som källa till realismens historia[23].

3.1. Realismens moderna historia

I någon mening har det funnits en realistisk idétradition sedan antiken. Den har utvecklats och omformats ett flertal gånger under historien fram tills 1900-talet.

De tänkare och tankar som kopplats ihop med dagens realistiska skola hade fram till det förra seklet alla delat ett par faktorer. Centralt är en pessimistisk syn på människan. Bibehållandet av, sökandet efter mer och rädslan för att förlora makt är något som kopplats samman med hur relationerna mellan såväl stater och individer

[23] Genomgången nedan (Morgenthau och realismen innan Waltz) är baserad på kap. 3 ”Realismen” (s. 21-30) ur Christianssons bok(2004).

är byggda. Etik, högre värderingar och universell moral kan inte stå ivägen för den politik som måste föras av de styrande. Att någon form utav högre ledning, oftast direkt likställt med en stat[24] , är enheten att fokusera på i det som vi nu benämner som IR återkommer också.

Nästa steg tar vi in i 1900-talets sekel. Där kom framförallt Hans J. Morgenthau att definiera realismen som en central teori för IR. Med hans *Politics Among Nations* (1948) kopplades människans natur, som är politisk, samman med hur utrikespolitik förs mellan stater. Individen söker alltid makt och förmågan att dominera sin omgivning. Detta sker på grund av viljan att trygga sin vidare existens. I utrikespolitiken speglas detta och resultatet blir att de internationella relationer som existerar mellan de olika staterna domineras av maktpolitik. Ovanför denna statsnivå kan därför ingen annan makt styra, drivkraften till att finna säkerhet hos varje stat är för stark. Därför var försöken, av bland andra Woodrow Wilson, att skapa ett överstatligt organ som Nationernas Förbund dömt att misslyckas enligt Morgenthau. Denna arena av maktpolitik, sökande efter egen säkerhet och därmed avsaknaden av någon övergripande ordning leder till den anarkiska världsbild som Morgenthaus syn präglas av.

Ovanstående är en kort sammanfattning av den både långa och anrika historia som dagens realism bär på. Morgenthaus syn på det anarkiska systemet blev tillsammans med fokuset på stater som den primära aktören genomgående för de tänkare som följde inom den realistiska skolan; en sådan tänkare var Kenneth N. Waltz.

[24]Det moderna statsbegreppet är självklart missledande när man skall prata om äldre riken och imperier. Innan den Westfaliska freden 1648 fanns det dock styrande institutioner som trots sin inte lika utvecklade byråkratiska struktur ändå utövad maktbaserad politik på både den egna befolkningen samt mot andra ”stater”. Det här noterar bl.a. Waltz(1979, 91).

3.2. Waltzs strukturella realism: Theory of International Politics

Med sitt klassiska verk *Theory of International Politics* (1979) kom han att dels bemöta den idealistiska strömning som kom med avtagandet av det Kalla Kriget[25] men också att bygga vidare på och utveckla den tidigare realismen, där framförallt Morgenthaus tankar varit dominerande. Waltzs började med att lösgöra sig ifrån kopplingen mellan den mänskliga naturen och hur den internationella arenan var konstruerad. Igenom att göra detta lämnade han också den filosofiska diskussionen om just människans inre. Waltz sätter istället sitt fokus på systemet som staterna befinner sig i. I och med detta kan Waltzs strukturella realism som IR-teori bara göra probabilistiska förutsägelser. Dessa förutsägelser blir dessutom allt som ofta generella i sin natur och kvantifieras inte. Detta har lett till att teorin inte alltid anses vara helt deduktivt[26] utvecklad (George and Bennett 2005, 202). Vilka implikationer och vad detta innebär för denna studie tas upp i Metodavsnittet.

Att skiftet i fokus går från människans natur till systemet som staterna befinner sig i motiveras efter samma linjer som den mikroekonomiska teorin är konstruerad. Enheterna, i detta fall stater, befinner sig i ett system där det saknas en övergripande och heltäckande auktoritet. Alltså är den mest relevanta nivån och strukturen att granska den internationella. Systemets ordning definierar strukturen som råder. Strukturen på denna nivå kommer inte av gemensamma beslut av de aktörer som tagit sig upp till den översta enhetsnivån: statsnivån. Denna struktur utgörs istället

[25] Se *Power and Interdependence : World Politics in Transition*(Keohane and Nye 1977)

[26] = Att från allmänna principer dra slutsatser om enskilda fall

av drivkraften bakom varje enhet. I den ekonomiska sfären skulle man nu titta på en (fri)marknad för att ha ett system att studera. Aktörerna, olika personer och firmor, agerar som separata enheter mot egna mål i detta system. De lägger inte ned kraft på att strukturera en övre ordning utan strukturen uppstår då likartade enheter samspelar och möts. Denna struktur kommer att påverka och begränsa alla enheter som finner sig i detta system (Waltz 1979, 88–90, 100). Jämförelsen här blir tydlig om personer och firmor byts ut mot stater och den fria marknaden ersätts av den internationella arenan. Strukturen blir, på grund av frånvaron av övre ordning och varje enhets individuella kamp för existens och säkrandet av denna, ett självhjälpssystem.

Detta självhjälpssystem är således anarkiskt ordnat. Detta kan direkt jämföras med hur staterna ser ut på individuell nivå där den rådande strukturen är hierarkisk. Hierarkin bygger på en kedja av olika ”mäktiga” aktörer som per definition blir varandra olika, de fyller t.ex. olika funktioner och har därmed olika förmågor. Den inomstatliga eller nationella nivån karaktäriseras sålunda av auktoritet, administration och lag (Waltz 1979, 113). I ett anarkiskt system, som den internationella arenan, fyller de olika enheterna, staterna, samma funktion och har därmed liknande förmågor. Strukturen i systemet ”bestraffar och belönar” enheterna som befinner sig i det. Mer exakt blir vissa handlingsmönster mer lyckade än andra och de är därmed också vanligare förekommande då enheterna som valt dessa naturligt består över tiden. Därmed ger det anarkiska systemet likhet hos sina enheter, tillskillnad från det hierarkiska (Waltz 1979, 92, 104). Som *lika* enheter är staterna dock inte *jämlika* enheter. Precis som att det i ett marknadssystem finns olika starka företag så återfinns olika starka stater i det internationella systemet. Waltz pekar ut avgörande faktorer för detta som storlek på populationen och

territorium, resursrikedom, ekonomiska förmågor, militär styrka samt kompetens. Staterna försöker hela tiden att bedöma och uppskatta dessa förmågor hos andra, särskilt förmågan att orsaka skada (Waltz 1979, 131). För att kunna mäta sig med andra stater och kontra exempelvis tillväxten hos en granne så används olika former av styrkor eller makt. Makt var det centrala ordet för klassiska realister som Machiavelli och Morgenthau. Där utgjorde makten både medlet och målet. På just denna punkt skiljer sig förmodligen Waltzs strukturella realism som mest från den klassiska synen på makt. I Waltzs internationella system formar strukturen enheterna till att använda sin makt till att finna säkerhet och inte till att för evigt söka mer makt, för maktens skull (Waltz 1979, chap. 126). Detta fostrar stater till att söka balansera makten (*balance-of-power*[27]) sinsemellan och inte att enbart försöka maximera makten som klassiska realism och offensiv neorealism hävdar[28].

Sammanfattningsvis står alltså det internationella systemets struktur i fokus för Waltz. Tre faktorer definierar denna struktur: den första är den rådande anarkin då det inte finns någon övergripande auktoritet över systemets stater. Den andra faktorn är de olika interagerande enheternas (staternas) funktioner och förmågor. Staterna söker säkerhet för att överleva och deras beteende kan inte ändras om inte själva systemet förändrar sig. Den tredje och sista faktorn som definierar systemet är distributionen av förmågor mellan staterna; olika militär stryka, resursrikedom, populationsstorlek etc.

Med den för studien använda teorin redogjord följer nedan ett stycke om de mer precisa analysverktyg som tagits ut för analysen av Stuxnet-attacken.

---

[27] Waltz använder sig av den redan etablerade teorin balance-of-power, se ”The Balance of Power: Prescription, Concept, or Propaganda?”(Haas 1953), som i huvudsak går ut på att beskriva bildandet av koalitioner och samarbeten mellan stater på den internationella arenan.

[28] För offensiv neorealism se *The Tragedy of Great Power Politics*(Mearsheimer 2001)

3.3. Analysverktyg från teorin

För att kunna analysera fallet Stuxnet och förklara mekanismerna bakom cyberattacken mot Iran krävs en uppsättning tydliga teoretiska verktyg. Kraven som togs upp i frågeställningsavsnittet; vilka aktörerna var, vilka motiv de hade och varför dessa motiv fanns, måste bemötas var och ett. Analysverktygen som skall användas för detta har kategoriserats i de tre grupper som följer nedan.

3.3.1. Enheter

Enheterna, eller aktörerna, som är centrala för Waltzs strukturella realism är stater. Anledningen till detta är att de utgör de primära enheterna på den internationella nivån. Det är därför relevant att undersöka vilken typ av aktör som attackerades av Stuxnet samt naturen hos den aktör som låg bakom angreppet.

3.3.2. Motiv

Enheterna, eller staterna, drivs hela tiden av sitt sökande efter säkerhet för den egna fortlevnaden. Det primära verktyget för att uppnå säkerhet är relativ makt över andra stater. Målet för staterna är inte att maximera sin makt utan att bibehålla den relativt till andra stater. Detta formar motiven bakom staters handlande på den internationella arenan.

3.3.3. System och Struktur

Orsaken till enheternas drivkraft, med andra ord staternas motiv, är det internationella systemets struktur. Det internationella systemets struktur karaktäriseras av anarki, funktionen och förmågan hos enheterna i systemet samt distributionen av förmågor och kapaciteter mellan dessa enheter.

4. Metod

4.1. Teorikonsumerande fallstudie

Denna studie är en *teorikonsumerande fallstudie*. För att ge någon klarhet i vad detta innebär redogörs nedan vad innebörden av dessa begrepp är.

Den första delen av hur studiens metodologi skall vara formad kommer genom valet att göra en *fallstudie*. Fallstudier inom statsvetenskap är något som fått ökat intresse och blivit allt mer sofistikerat under de senaste årtiondena. Detta inte minst tack vare bidraget från den filosofiska utvecklingen av vetenskap som lett till en mer robust grund för fallstudier (George and Bennett 2005, 8). En relevant fråga att börja med är: vad är ett fall? Alexander George och Andrew Bennet definierar ett fall som ”en del av en klass av händelser” (George and Bennett 2005, 17). Denna formulering behöver kanske en mer utvecklad förklaring. En klass av händelser skulle kunna vara demokratiska val, revolutioner eller inbördeskrig. En enskild del, eller händelse, kan vara riksdagsvalet i Sverige 2006, Ryska oktoberrevolutionen 1905 eller Etiopiska inbördeskriget 1974-1991.

I denna studie är fallet Stuxnet-attacken mot Iran. Stuxnet-attacken är ett händelseförlopp som utgör en del av fenomenet cyberattacker. På en högre abstraktionsnivå är i sin tur cyberattacker en del av informationsrevolutionens påverkan på säkerhet och IR.

Fallstudiers främsta kvalité är den höga *konceptuella validitet* de medför. Med andra ord är det lätt att identifiera och mäta de kriterier som motsvarar det teoretiska ramverk studien i fråga använder sig av (George and Bennett 2005,

19). I denna studies fall blir det teoretiska ramverket Waltzs strukturella realism och kriterierna som dras ifrån den är de analysverktyg som presenterades i slutet på teori-stycket. Att mäta värdena för kriterierna är något som ofta kan vara svårt inom statsvetenskapen. Ta exempelvis variabler som demokrati, makt och politisk kultur. Alla är ytterst svåra att uppmäta ett egentligt värde av, särskilt om man skulle utföra en studie baserad på statistik.

Här sätts kvalitativ metod mot kvantitativ metod. När en studie har variabler som kan uppskattas med relativt exakta värden är den kvantitativa metoden vägen att ta. När variabler som de ovan nämnda exemplen skall undersökas måste en kvalitativ analys och bedömning göras. Men den kvalitativa processen kantas av problem som författarens egna förkunskaper och dolda inre tankeprocess. Lösningen på detta är fallstudien tätt kopplad med. Genom att tydligt dokumentera de steg som tas genom studien och utforma dessa så tydligt som möjligt för utomstående kan reliabiliteten säkras. Kort sagt: En annan individ skall kunna genomföra denna fallstudie och nå samma resultat som denna studie presenterar (Yin 2009, 45).

I en fallstudie kan dessutom problemen som är kopplade till en kvalitativ metod ytterligare överbryggas. Detta tack vare fallstudiens starka invägande av kontextuella faktorer. I den här studien tas den strukturella realismens teoretiska ramverk till bruk för att förklara en *liten* del av informationsrevolutionens påverkan på säkerhet och IR. Denna lilla del, eller aspekt, är cyberattacker och i och med valet av det enskilda fallet ”Stuxnet-attacken” kan studien bidra med kunskap om den aktuella teorins förklaringsförmåga gällande detta nya fenomen.

En framförd kritik mot användandet av fallstudier är bristen på representativitet

(George and Bennett 2005, 30). Det är extra svårt att påstå att resultatet från denna studies användande av strukturell realism kan vara representativt för andra fall av cyberattacker då Stuxnet som tidigare nämnt verkar vara det enda fallet i nuläget tillgängligt att studera[29]. Dock hotar inte detta generaliserbarheten. Vad som kan göras för att säkra generaliserbarheten är att ge studien en tillräckligt god *reliabilitet*. Genom att tydligt dokumentera de steg som tas genom studien och utforma dessa så tydligt som möjligt för utomstående kan reliabiliteten säkras. Kort sagt: En annan individ skall kunna genomföra denna fallstudie och nå samma resultat som denna studie presenterar (Yin 2009, 45).

Den andra delen av metodologin är studiens status som *teorikonsumerande*. Denna kategorisering hänger på en mycket specifik faktor, vilket Peter Esaiasson och Mikael Gilljam pekar på i *Metodpraktikan* (2007, 42–43). Den första är att det enskilda fallet; Stuxnet-attacken, står i fokus. Med användandet av en existerande teori, Waltzs strukturella realism, skall fallet kunna förklaras. När det kommer till resultatet från studien närmar dock studien en omisskännligt teoriprövande karaktär. Detta kommer sig av att resultatet från studien har en påverkan på vår tilltro till den använda teorin. Om den strukturella realismen visar sig oförmögen att bidra till förståendet av Stuxnet-attacken mot Iran så minskar såklart tilltron i någon mån (Esaiasson 2007, 43).

4.2. Operationalisering

I denna studies analys operationaliseras analysverktygen *Enheter, Motiv* samt

[29] Se avsnittet ”Avgränsningar och dess motiveringar” tidigare i studien.

System och Struktur med syftet att fungera som teoretiska glasögon för att hjälpa till att finna svar på mekanismerna bakom Stuxnet-attacken.

Processen där analysverktygen från det teoretiska ramverket appliceras på empirin utgör själva operationaliseringen. Hur operationaliseringen genomförs har en stor påverkan på de resultat som studiens analys kommer att ge. De olika teoretiska definitioner som återges i teori-avsnittet måste stämma överens med de operationella indikatorer(analysverktyg) som används vid analysen av empirin. Om dessa inte skulle överstämma saknar studien *validitet*. Utan validitet är resultaten från studiens analys av Stuxnet-attacken inte trovärdiga och studien har därmed inte gett några användbara slutsatser om verkligheten (Esaiasson 2007, 59–61). Hur operationaliseringen av teorin till indikatorer ser ut redogörs det för i slutet på Teori-avsnittet.

4.3. Metodologisk kritik mot Walts realism som deduktiv teori

Att detta avsnitt hamnar här har att göra med dess koppling till studiens vetenskapliga genomförande rent metodologiskt. Waltzs strukturella realism anses som tidigare noterat inte vara en helt utvecklad deduktiv teori. Den kan endast göra probabilistiska förutsägelser där dessa i sin tur oftast är generella och dessa kvantifieras inte. Det här är slutsatser som görs av bl.a. Alexander George och Andrew Bennet drar (2005, 190–191, 202–203) men också Johan Eriksson och Giampiero Giacomello (2006, 228–229).

Vad detta innebär för användandet av teorin i verkligheten är att många möjliga utfall från ett händelseförlopp kan skönjas. Betänk konflikten mellan USA och Sovjetunionen efter andra världskriget. Waltzs teori kunde inte förutse om

konflikten skulle utvecklas till ett ömsesidigt influens-sfärs avtal, ett Kallt Krig eller ett tredje världskrig[30].

Andra variabler som den strukturella realismen inte tittade på behövdes tas med i ekvationen om man skulle kunna förutspå vilket utfall konflikten skulle få. Här kan ett annat problem kopplas in. Att fastslå om vissa oberoende variabler är nödvändiga som villkor för ett utfall är också problematiskt. För att göra detta skulle andra fall med samma utfall behöva hittas och om den oberoende variabeln saknades där kunde man bortse från den som ett absolut nödvändigt villkor (George and Bennett 2005, 189).

Om vi skall överföra denna problematik till denna studie finns dock en viss diskrepans. Fallet i denna studie, Stuxnet-attacken mot Iran, har redan blivit kartlagt gällande variabler som aktörer, motiv och resultat. Det här är ett historiskt fall som plockas isär, analyseras och förklaras i efterhand, till skillnad från Waltzs 1979 och konflikten mellan USA och Sovjetunionen. Sålunda behöver denna studie inte redogöra för ett framtida utfall.

Angående teorins höga generalitet så klargör Waltz i *Theory of interantional Politics* att hans teori förklarar internationell politik, inte staters utrikespolitik (Waltz 1979, 121). Med detta följer att teorin inte syftar till att förklara minsta utspel eller policy en enskild stat tar sig för. Den strukturella realismen beskriver i grunden de begräsningar som omger alla staters handlande. Dessa begränsningar leder i sin tur till formandet av alla staters strävan. Teorin gör sålunda främst antaganden om staters intressen och motiv (Waltz 1979, 122),

[30] Exemplet är hämtat från *Case studies and theory development in the social sciences*(George and Bennett 2005, 191)

vilket denna studies frågeställning kräver av sin teori.

Gällande bestämmandet av de oberoende variebalerna så klargör studiens analys och resultat om den strukturella realismens vilande på allmänna principer för att dra slutsatser om enskilda fall är bristande och otillräcklig. Om analysverktygen från teorin kan finnas vara applicerbara och leda till någon förklaring om mekanismerna bakom Stuxnet-attacken har teorin stärkts. Om inte är den försvagad. Här kan det som tidigare nämnt verka som om studiens metodologi närmar sig en mer teoriprövande orientering. Men skillnaden mellan teorikonsumerande och teoriprövande studier är också gradvis (Esaiasson 2007, 43).

De oberoende variablernas[31] nödvändighet som villkor för utfallet i Stuxnet-attacken är inte möjliga att jämför mot något annat fall av cyber-attacker, av tidigare angivna skäl. Säg att den strukturella realismen håller en stark förklaringsmöjlighet till Stuxnet-fallet som denna studie undersöker. För att Waltz teori skall kunna sägas stärkas måste andra fall av samma aspekt av informationsrevolutionens påverkan på IR och säkerhet undersökas (Yin 2009, 43–44).

Sist ska kritiken kring den externa och interna validiteten hos Waltzs strukturella realism tas upp, vilket i sig hänger samman med kritiken mot teorin som deduktivt lagd. Eriksson och Giacomello tar upp detta problem när de pekar på att den externa validiteten (huruvida teorin ger en ackurat förståelse för

[31] se *analysverktygen* i Teori-avsnittet

omvärlden) blir åsidosatt för den höga interna validiteten. Det här reflekterar främst två olika sätt att se på hur teorier skall byggas men kanske också två olika epoker inom den vetenskapliga filosofin och samhällsvetenskapen[32]. Denna skillnad ligger dock utanför det som skall tas upp för studiens syfte. Waltzs menade att hans teori hade en stark intern validitet då hans strukturella realism byggde på lagar. Då lagar i sig inte kan förklara det som händer behövs teorier för att förklara dem (Waltz 1979, 6). För att en teori skall kunna nå en ”stark förklaringskraft måste den röra sig bort från verkligheten”[33].

Här finner vi sålunda en diskrepans i synsätt på vad vetenskaplig teori är. Waltzs synsätt blir dock det enda som är relevant att ställa sig bakom i detta fall då studien är teorikonsumerande. Då fallet kommer i förstahand och en teori valts ut efter dess förväntade lämplighet som förklaringsmedel kan större delen av denna kritik således bortses ifrån.

[32] Denna studies syfte innefattar inte en vidare filosofisk utläggning om epistemologi, ontologi och (neo)positivism.

[33] - ”Explanatory power, however, is gained by moving away from ‘reality’, not by standing close by it” (Waltz 1979, 7)

5. Material

För att ge ett tillräckligt täckande underlag för studien syfte behövs material som innefattar såväl information om Stuxnet-attackens tekniska aspekter som bakomliggande aktör(er) och deras motiv. De tekniska aspekterna är säkerligen fascinerande i sig, den tillgängliga informationen om Stuxnet tyder på både stor innovation och uppfinningsrikedom kring ett komplext problem, men det är inte kodens geniala uppbyggnad eller det tekniska verkställandet utav den, som är mest centralt för denna studie. Dock är det fortfarande nödvändigt att återge hela händelseförloppet i fallet då informationsrevolutionens påverkan på framförallt tekniken framträder extra tydligt under ”jakten” på Stuxnets mål och skapare. Materialet som krävs behöver sålunda innehålla en tillräckligt detaljerad återgivelse av användandet av informationsrevolutionens ”produkter” för att uppfylla studiens syfte. Dessutom innehåller de tekniska aspekterna av fallet nyckeln till hur man kunde komma fram till vad som attackerats, vem som attackerade och därmed varför attacken skedde.

Det första materialet som läggs fram är den omfattande ”How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History” av Kim Zetter som publicerades på *Wired Threat Level Blog* (2011). Här återfinns en detaljerad och kronologisk återgivelse av Stuxnets upptäckt och hur man sedan gick till väga för att komma fram till dess syfte och mål. Detta material kompletteras med bl.a. rapporter från *International Atomic Energy Agency* (IAEA) och *Institute for Science and International Security* (ISIS). I sådana rapporter återfinns information om avvikande händelser och komplikationer som IAEA uppmärksammat vid Natanz vid tiden för den förmodade cyberattacken. Valet att låta Kim Zetters text stå som en central källa

och material för denna studie är gjort med tanke på textens täckande av den kronologiska händelseutvecklingen. Den återger allt från den första upptäckten av en bit skadlig kod till det följande detektivarbetet bakom virusets syfte och mål. Zetters text har dessutom redan används inom säkerhetsstudier (Lindsay 2013, 365–366), för vilket denna studie fullgott också kan bruka den som källa.

Materialet för studien som berör bakomliggande aktörer, motiv och (tänkta) effekter har naturligtvis en mindre teknisk natur. Den 1 juni 2012 publicerade *The New York Times* artikeln ”Obama Order Sped Up Wave of Cyberattacks Against Iran”, skriven av David E. Sanger (2012). I denna artikel pekades de ansvariga ut för Stuxnet, varför de släppt löst viruset samt vad det den tänkta effekten skulle bli.

Här finns egentligen allt det material som täcker fallet Stuxnet, så långt som denna studies syfte kräver. Men ett ytterligare material skall presenteras. I rapporten ” Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” från ISIS (Albright David, Brannan Paul 2010) utvärderas den totala skada som skett och därmed kan också den reella effekten av attacken redogöras för i denna studie. Den reella effekten här åsyftar den skadliga fysiska effekt Stuxnet hade på iranskt materiel och utrustning, i detta fall centrifuger för anrikning av uran. Valet att ta med detta sista material och tillhörande redogörelsen syftar till att ge läsaren en heltäckande bild av attacken, där Stuxnets verkliga effekt är relevant att ta upp.

6. Empiri: Stuxnet-attacken

Nedan kommer de olika utvalda materialen att gås igenom. Informationen från dem kommer att läggas samman för uppbyggnaden av en kronologisk återgivelse av attacken. Indelningarna som skall utgöra denna kronologiska genomgång är: ”Upptäckandet av koden och virusets mål”, ”Den tekniska attacken och dess effekt” samt ”Olympic Games: aktörer, motiv och resultat”. Som titlarna på styckesindelningen indikerar så är de två första styckena mer lutade på empiri gällande de rent tekniska sidorna av Stuxnet och Iran. Det sista stycket baseras istället på material som behandlar bakomliggande aktörer, konsekvenserna på internationella relationer och maktpolitik.

6.1. Upptäckandet av koden och virusets mål

Januari, 2010. En grupp med inspektörer från International Atomic Energy Agency (IAEA) har precis undersökt en urananrikningsanläggning utanför Natanz i centrala Iran. Något märkligt är på gång. En efter en bärs verkets centrifuger ut för att ersättas. Centrifugerna, som används till själva anrikningen av uran för kärnkraftverk men potentiellt också för kärnvapen, byts normalt ut med ett omfång på 10% av anläggningens 8700 stycken per år. I tempot som nu hölls åkte mellan 1000 och 2000 centrifuger ut under loppet av bara ett par månader (Zetter 2011, 1). Något hade orsakat skador på en stor del av iraniernas centrifuginnehav[34].

[34] Rapporten från International Atomic Energy Agency den 18 februari 2010(IAEA 2010, 2) stödjer bl.a. detta då det konstateras att 1804 IR-1 centrifuger kopplats ur på grund av komplikationer. Se även

Den 17 juni 2010 mottog Sergey Ulasen, anställd vid antivirusföretaget VirusBlockAda lokerat i Minsk, ett email från en kund i Iran. Det gällde en dator som fastnat i ett upprepat omstartningsläge. Så kom Rootkit.TmpHider(VirusBlockAda 2013), namnsatt av sina första upptäckare, att hittas. Viruset döptes senare under sommaren om av Microsoft till Stuxnet, baserat på filnamnen mrxcls.sys och mrxnet.sys som hittades i koden (Saade 2010). Efter närmare granskning kom Sergey Ulasen och hans team i Minsk fram till att viruset som satt sig i kundens dator använde sig av en ”zero-day”-exploatering[35] för att sprida sig. Bara att viruset utnyttjade en zero-day indikerade på att en ytterst potent kreatör låg bakom. Sättet viruset färdades på mellan olika anläggningar, där internetanslutning saknades, visade sig vara via USB-stickor. Mer exakt låg den utnyttjade svagheten i Windows Explorer. När USB-stickan sattes in i en dator scannade Explorer stickans innehåll. Koden vaknade och överförde i det dolda en stor bit kod till datorn. Med tiden skulle man upptäcka ytterligare tre zero-days i koden. Snart kom man fram till att virusets mål verkade vara Simatic WinCC Step7-mjukvara, utvecklad av Siemens. Denna mjukvara används inom industrin där den verkar som kontrollsystem till bland annat motorer, ventiler och switchar. Sådana hårdvaror används i sin tur inom alltifrån produktion av mat- och elektronikvaror till regleringsfunktioner inom infrastruktur för gas, elektricitet och vatten. Detta

---

Institute for Science and International Security’s rapport från den 22 december 2010(Albright David, Brannan Paul 2010).

[35] Zero-day är möjligen det mest potenta vapnet för hackers. Det bygger på finnandet av en tidigare okänd eller inte ännu rapporterad svaghet eller brist i en mjukvara. Då antingen mjukvarubolaget eller antivirusföretagen inte vidtagit några åtgärder mot denna ”lucka” blir den således en möjlighet att utnyttja för illasinnade programmerare(Zetter 2011, 2).

visade att virusets huvudmål var datorer som i någon form var kopplade till sådana industriella kontrollsystem. Åtgärder togs mot viruset och antivirusföretagen uppdaterade sina program emot det.

Här kunde undersökandet av Stuxnet slutat. Men anställda inom företaget Symantec fortsatte att granska Stuxnet-koden. Liam O Murchu och Eric Chien var två av dessa (Zetter 2011, 3). De började med att försöka se var viruset spridit sig. Inledningsvis fick de in information om 38000 infekterade datorer. Av dessa fanns 22000 i Iran. Efter ytterligare spårning av virusets framfart kom man fram till att fem olika organisationers datorer varit de första att bli attackerade. Alla fem organisationer var lokaliserade i Iran och borde varit tänkta som möjliga ”gateways”[36] till det verkliga målet. Viruset hade även dolt sig som en legitim programvara genom att använda två stulna certifikat från två riktiga företag, RealTek och JMicron Technology (Zetter 2011, 2). Vare sig de okända skaparna av Stuxnet brutits sig in hos de bägge företagen eller hackat sig in hos dem för att komma över certifikaten så stod det nu ännu tydligare klart: det var ytterst resursrika och potenta aktörer som skapat viruset.

När arbetet fortsatte med att granska Stuxnets funktion gick man in närmare i koden. Detta ledde således till upptäckten att datorer som använde Siemens Step7-mjukvara var nyckeln till målet med viruset. Mer exakt var det vanliga datorer som var uppkopplade mot PLCs(Programmable Logic Controller) där Step7 var mjukvaran som användes för att kommunicera de små PLC-datorerna. PLC-datorerna är i sig kopplade till den industriella utrustningen som skall

[36] ”Portar” eller ”dörrvägar” för viruset vidare spridning mot sin slutdestination.

styras. När Stuxnet stötte på en dator med Step7 fördes en DLL-fil[37] över. Filen var som ett bibliotek med olika skadliga kommandon. För att nå det riktiga målet behövde sålunda en vanlig dator, med Step7, infekteras. Nästa gång någon kopplade in datorn till en PLC började de nya skadliga kommandona att användas vilket skulle påverka det industriella maskineriet efter Stuxnet-skaparnas önskningar.

Virusets attackerande av PLCs kom att intressera Ralph Langner, arbetandes med säkerhet för industriella kontrollsystem. Han kom fram till att viruset inte bara var specifikt riktat mot Siemens kontrollsystem. Det var preciserat mot att sabotera en specifik anläggning (Zetter 2011, 6). I koden fanns en omfattande information om det tilltänkta målets strukturella och tekniska uppbyggnad. Alla offer för viruset som inte direkt matchade denna signatur lämnades oskadda och viruset jagade vidare. När detta lades ihop med virusets möjlighet att sprida sig via USB-stickor och det tydliga fokusområdet för spridningen kunde slutsatser börja dras. Irans anrikning av uran och läget på den geopolitiska arenan började kopplas samman med den tekniska utredningen av Stuxnet (Zetter 2011, 6, 7).

6.2. Den tekniska attacken och dess effekt

På Symantec hade man lyckats göra en bakåt-kompilering av koden i Stuxnet för att kunna se exakt vilken hårdvara den skulle reglera och sabotera. Det visade sig att Stuxnet skapats för att komma åt och reglera frekvenskonverterare. Dessa styrdes till att drastiskt sänka och öka frekvensen på enheterna de var kopplade till. Vad som än fanns i andra ändan var helt klart menat att ta skada av den

[37] Dynamic-link library: en fil som fungerar som ett bibliotek med olika programfunktioner. Filen används i sig av olika program som delar ett gemensamt behov av en viss funktion.

extrema frekvensregleringen (Zetter 2011, 7). Enheter skulle visa sig vara centrifugerna för urananrikningen i Natanz. Då anläggningen utanför Natanz inte hade anslutningar till internet kunde således skaparna av Stuxnet inte komma åt sina mål direkt. Men genom att infektera andra datorer i Iran kunde dessa fungera som gateways till det verkliga målet. När viruset till sist nådde en dator, med Step7-mjukvaran installerad, som kopplades upp mot en anläggning matchande den som viruset jagade "slog attacken till". Stuxnet tog via sin infekterade dator kontroll över PLCn som i sin tur reglerade frekvenskonverterarna till centrifugerna. Den fysiska attacken mot centrifugerna gick mer precist till på följande sätt:

Viruset låg och väntade i två veckor. Under denna tid det rekognoserade det systemet inför attacken. När attacken väl kom höjdes frekvensen under 15 minuter till 1410Hz för att sedan gå ned till normal frekvens igen på 1064Hz. Sedan var allt lugnt i 27 dagar. Nästa attack kom i form av en sänkning till 2Hz i 50 minuter. Sedan gick ytterligare 27 dagar innan sekvensen upprepades igen (Zetter 2011, 7). Denna extrema variation i frekvens orsakade till sist sådan skada på maskineriet att många centrifuger blev satta ur användbart skick. När attackerna kom styrde dessutom Stuxnet informationsflödet från PLCn tillbaks till datorn med Step7-mjukvaran där personalen sålunda inte kunde se några förändringar i verksamheten hos centrifugerna.

6.3. Olympic Games: aktörer, motiv och resultat

Med det geopolitiska läget i bakhuvudet kunde redan de som tekniskt undersökt Stuxnet ana varifrån attacken kommit. Men det skulle dröja till och med den 1 juni 2012 innan det verkliga avslöjandet kom. I och med artikeln "Obama Order

Sped Up Wave of Cyberattacks Against Iran" kunde Stuxnets skapare pekas ut: USA och Israel hade ingått i en gemensam operation för att hindra eller fördröja Irans misstänkta steg mot att skaffa kärnvapen (Sanger 2012). Två stater hade sålunda försökt hindra en tredje stats försök att öka sin militära kapacitet. Den amerikansk-israeliska operationen hade fått kodnamnet "Olympic Games". Operationen hade initierats av Bush-administrationen 2006 som en alternativ väg att ta för att hindra Iran från att skaffa sig kärnvapen. Då kriget i Irak grundats på anklagelser om Saddam Husseins försök att skaffa en egen kärnvapenarsenal krävde läget andra tillvägagångssätt. Sabotage riktade mot anläggningen hade redan försökts av CIA men med liten framgång (Sanger 2012). Den alternativa vägen in i anläggningen gick via IT-infrastrukturen. För att kunna använda sig av IT-teknik och cyberrymden krävdes dels att man skulle kunna skaffa sig kunskap om anläggningens struktur och innehåll men också ett sätt att överbrygga "luftspannet" mellan Natanz och internet. Uppdraget att skapa ett virus så sofistikerat att det kunde lösa bägge dessa uppgifter föll på amerikanska *National Security Agency* (NSA) och den Israeliska *Unit 8200*. Att inviga Israel i operationen hade två anledningar:

den första var deras djupa kunskap om Natanz som krävdes för att viruset skulle lyckas. Den andra anledningen var israelernas vilja att helt enkelt bomba anläggningen. Enligt flera källor kunde detta endast hindras om israelerna var djupt insatta i varje steg av programmeringen bakom den planerade attacken (Sanger 2012). När Barack Obama tillträdde presidentposten 2009 ökade trycket på Olympic Games lyckande i att hindra Irans försök att skaffa kärnvapen. När viruset under 2010 blev påkommet, och det verkade som om det var en tidsfråga innan man själva skulle pekas ut, informerades president Obama av de ansvariga

för operationen; försvarsminister Leon Panetta, vice försvarschef James E. Cartwright samt CIA:s vicedirektör Michael J. Morell. Anledningen till virusets spridning utanför Natanz påstods bero på ett fel i koden. Israelerna pekades även ut som skyldiga då de skulle modifierat viruset och "gått för långt" (Sanger 2012). Men rapporter kom snart in om hur ca 1000 centrifuger för anrikningen av uran slagits ut. Olympic Games fick fortsätta. Vad det verkliga resultatet av attacken verkligen blev är omdiskuterat. I bl.a. ISIS rapport "Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?" (2010) slås det fast att viruset slagit ut ett större antal centrifuger. Vad som är mer oklart är den totala effekten detta haft på Irans förmåga att närma sig ett eget innehav av kärnvapen. Rapporten från ISIS slår i slutändan fast att Stuxnet-attacken inte lyckades slå ut alla centrifuger och därmed stoppa anrikningsprocessen. Men om målet var att tillfälligt skapa ett bakslag för iranierna och deras framsteg inom urananrikningen så verkar det som om Stuxnet var en framgång (Albright David, Brannan Paul 2010).

7. Analys

I detta stycke kommer den ovan presenterade empirin att brytas ned och analyseras utifrån de i teoriavsnittet angivna analysverktygen. Upplägget nedan går efter den ordning som analysverktygen presenterades: *Enheterna, Motiv* samt *System och Struktur*.

Att identifiera vilka aktörer som varit relevanta att studera i fallet Stuxnet-attacken mot Iran kan verka meningslöst och till och med absurt: att en stat var central i fallet var ett krav för att kunna använda Waltzs statsfokuserade teori. Men det finns ett stort delat värde i att analysera vilken natur de aktörer hade som riktade Stuxnet mot Iran. För det första är förståelsen av naturen hos skaparna av Stuxnet första steget mot att finna och därmed förstå mekanismerna bakom attacken mot Iran. För det andra skall detta finnande ställas mot bakgrunden av informationsrevolutionen. Med anledning av den sofistikerade och ytterst potenta insats som låg bakom skapandet av den kod som kom att användas i attacken mot Irans urananrikning är det relevant att undersöka detta mer noggrant.

Att informationsrevolutionen och främst cyberrymden öppnat upp för ett bredare spektra av aktörer inom säkerhet och IR är något som pekats på tidigare (Eriksson and Giacomello 2006, 230; Nazli Choucri 2012, 14). Att denna studie överhuvudtaget är möjlig att genomföra baseras på hur icke-statliga aktörer samlat och analyserat information som lett fram till avslöjandet av USA och Israel som skaparna till Stuxnet. Privata företag och individer har sålunda onekligen haft en roll i händelseförloppet som är fallet Stuxnet. Men det var stater som ”korsade

Rubicon”[38] när Stuxnet släpptes löst. Som Jon Lindsay noterar i ”Stuxnet and the Limits of Cyber Warfare” har skapandet av Stuxnet krävt en långsiktig planering i tid, insamlande av underrättelser och en ytterst utvecklad institutionell struktur hos skaparna (Lindsay 2013, 387). Denna grad av kvalifikationer finns sällan, om någonsin, utanför stater med tillhörande militär administration och styrkor. Detta konstaterade bland annat både antivirusföretaget Kaspersky labs och Symantecs vd Kevin Hogan efter att Stuxnet hittats[39].

Stuxnets slutliga effekt på Irans framsteg inom urananrikningen må vara omdiskuterade (Albright David, Brannan Paul 2010). Men virusets status som ”the most menacing malware in history” (Zetter 2011) är desto klarare. Att USA och Israel lyckats använda en rad av informationsrevolutionens produkter för att tillfoga fysisk skada hos en annan stats infrastruktur är uttalat nydanande eller till och med revolutionerande (Zetter 2011; Lindsay 2013, 366; Clayton 2011).

Waltzs strukturella realism sätter stater i fokus som de relevanta enheter att studera. Inte för att stater är de enda aktörerna i det internationella systemet. Men för att det internationella systemets struktur definieras av de ”tyngsta” aktörerna (Waltz 1979,

---

[38] Just uttrycket ”korsade Rubikon” användes av den före detta CIA-chefen Michael V. Hayden för att beskriva vad som hänt i och med användandet av Stuxnet: ”This is the first attack of a major nature in which a cyberattack was used to effect physical destruction,’rather than just slow another computer, or hack into it to steal data. ’Somebody crossed the Rubicon,’ he said.”(Sanger 2012)

[39] - … “Kaspersky Labs said the attack could only be conducted ‘with nation-state support’”,

- “We cannot rule out the possibility (of a state being behind it]. Largely based on the resources, organisation and in-depth knowledge across several fields - including specific knowledge of installations in Iran - it would have to be a state or a non-state actor with access to those kinds of (state] systems” (Maclean 2010)

93) Av alla aktörer som använder och är uppkopplade till cyberrymden är upptäckandet av USA och Israel som skaparna av det nydanande Stuxnet därför inte förvånande när den strukturella realismen nu används för att förklara Stuxnet-attacken. Nästa steg i analysen blir applicerandet av Waltzs *Motiv.*

I David Sangers artikel förklarades Stuxnet-attacken vara en del av operationen Olympic Games. Denna operation gick ut på att två stater har gått samman med motivet att hindra en tredje stat från det potentiella skapandet av egna kärnvapen. När vi applicerar Waltzs syn på staters motiv för att förklara detta framträder ett tydligt svar. USA och Israel har inte försökt att utöka den egna makten. De har inte medvetet utövat handlingar som leder till att de förlorat makt. Handlingen att stoppa en tredje stat från att införskaffa sig en kärnvapenarsenal är en direkt avbild av det Waltzs pekar ut som grunden för behållandet av relativ makt. Sökandet efter att få behålla sin relativa makt är i sin tur drivet av viljan att säkra sin egen överlevnad. Men för förstå hur en stat gör detta måste man se makt som det främsta verktyget. För Waltzs måste makt bli ”… defined in terms of the distribution of capabilities” (Waltz 1979, 192). Kärnvapen är i alla högsta grad är en kapacitet att ta med i beräkningen för en stats relativa makt. När vi utgår från läget innan Stuxnet-attacken var distributionen av denna kapacitet endast förlagd hos de två allierade staterna USA och Israel. Om Iran skulle lyckas skapa egna kärnvapen via den egna urananrikningen hade distributionen av den sökta kapaciteten varit fördelad hos bägge sidor. Detta hade minskat övertaget för USA och Israel och därmed deras relativa makt på den internationella arenan. För Iran hade skapandet av egna kärnvapen minskat den andra sidans övertag och därmed hade den relativa makten

ökat.

Sålunda finns det ett steg kvar i förklarandet av mekanismerna bakom Stuxnet-attacken: vad är det som har orsakat USAs och Israels motiv? För att förklara detta sätts nu det sista analysverktyget i ordningen in: *System och Struktur*.

Att motivet att attackera Iran överhuvudtaget fanns kan förklaras med systemet som de tre inblandade staterna befinner sig i. Detta system har en struktur som karaktäriseras av anarki, funktionen och förmågan hos enheterna i systemet samt distributionen av förmågor och kapaciteter mellan dessa enheter. I och med detta finns det en förklaring till varför ingen högre instans eller enhet ovanför de tre staterna ingrep istället för att attacken genomfördes[40]. Istället tog de två angriparna saken i egna händer och konstruerade det virus som behövdes för att uppfylla det gemensamma motivets mål.

Att motivet uppkommit från första början kan förklaras med att systemet även karaktäriseras av olikheter i förmågor och kapaciteter stater emellan. Dessa olikheter, som i det här fallet var innehavet av kärnvapen, driver de olika sidorna mot kolliderande mål. Iran vill stärka sin makt för att uppnå en högre säkerhet gentemot de andra staterna i systemet som innehar kärnvapen, alltså strävar Iran mot att införskaffa en egen arsenal. USA och Israel vill inte se en tredje stat öka sin relativa makt gentemot dem själva. Därför blir deras mål att stoppa eller försöka hindra Iran från att öka sina kapaciteter vilket sätter de bägge sidorna på motsatta kurser.

[40] Den uttryckta bristen på andra möjligheter att stoppa Iran från President Obama styrker detta (Sanger 2012).

Hur kan då *motiven* samt *systemet och strukturen* förklaras mot bakgrunden av informationsrevolutionen?

USA och Israel har använt sig av en rad av informationsrevolutionens produkter, där cyberrymden i form utav internet varit en central komponent, för att hindra Iran från att öka sin relativa ”förmåga”. Waltzs tar upp faktorer som ekonomi, population, storlek på territorium och militär styrka som exempel på förmågor att ta med i beräkningen för att förstå en stats makt relativt till andra stater. Det amerikanska NSA och Israeliska *Unit 8200* skapade och sände ett virus med funktionen att sabotera en annan stats infrastruktur. Förmågorna och kapaciteterna som dessa stater satt inne på, via bland annat dessa organisationer, ledde till förhindrandet av att distributionen av andra förmågor och kapaciteter ökade hos en tredje stat. Stuxnet-attacken påvisar således att förmågorna och kapaciteterna inom IT, ICTs och dessas koppling till cyberrymden påverkar distributionen av förmågor stater emellan.
Sålunda kan användandet av informationsteknologier ses som en del av staters förmågor som kan stå sig relativt starkt till andra stater och därmed utgöra en del av den strukturella realismens definition av makt.

Det finns ytterligare en dimension av den strukturella realismens syn på system och struktur som är applicerbart på informationsrevolutionens påverkan på säkerhet och IR i förklarandet av Stuxnet-fallet. Som tidigare nämnt har informationsteknologierna skapat en virtuell värld mellan sig; cyberrymden. Cyberrymden är benämningen på den mängd olika nätverk som sammankopplar

flera olika enheter med varandra så som ICTs men även industriellt maskineri etcetera. Det enskilt största nätverk som sammankopplar större delen av världens uppkopplingsbara enheter är Internet, vilket brukar få stå som symbol för cyberrymden. Karaktäriserande för Stuxnet-attacken, så väl som för andra attacker i cyberrymden är det stora mått av opererande i det fördolda och den från början okända identiteterna hos angriparen (Adams 2001; Lindsay 2013; Geers 2011, chap. 2). Detta faktum har som tidigare nämnts starkt bidragit till de svårigheter som finns kring studerandet av attacker i den virtuella världen.

Då Stuxnet-attacken unikt nog är så pass kartlagt gällande genomförande, mål och bakomliggande aktörer kan den här analysen genomföras.

Under Stuxnet-attacken kom cyberrymden och internet att utgöra en betydande komponent för virusets spridningsförmåga och framfart mot sitt slutliga mål i Natanz.

Cyberrymden saknar inte lagar: den styrs och struktureras i högsta grad av såväl fysiska begränsningar som den kod med vilken den är uppbyggd (Clunan 2010, 256). Notera här likheterna med de lagar som Waltzs anser finnas i det internationella systemets struktur.

Det saknas också en inbyggd auktoritet som kontrollerar de inkopplade enheterna. Avsaknaden av en hierarkisk struktur och övergripande auktoritet i den virtuella världen, som internet utgör en stor del av, möjliggjorde många av de steg som togs mot att infiltrera och sabotera centrifugerna i Natanz[41]. Om vi ser på den virtuella

[41] Betänk det breda spektra av de mål angriparna riktade in sig på innan attacken för att möjliggöra skapandet av den nödvändiga koden. I sin förlängning orsakade detta att analyserandet av Stuxnet hamnade hos en rad olika aktörer som både privatpersoner och företag (säkerligen mindre redovisat hos stater också). Det var således ingen högre instans eller enhet som behövde attackeras eller undvikas för att göra angreppet och därmed ingen sådan som ensidigt ”upptäckte” Stuxnet i efterhand.

världen, av informationsrevolutionen kommen, som ytterligare en arena där stater projicerar sina intressen som i sin tur möts och kolliderar blir cyberrymden onekligen en förlängning av det system som Waltzs realism studerar[42].

Stuxnet-attacken blir därför ett utmärkt exempel på hur cyberrymden kan uppfattas som ett system utan hierarki. Därför är denna arena anarkisk vilket gör den till en naturlig förlängning av det redan anarkiska internationella system som staterna befann sig i innan informationsrevolutionen[43].

[42] En liknande slutsats dras av James Adams i artikeln ”Virtual Defense”: ”… cyberspace has become a new international battlefield” (Adams 2001, 98)

[43] Detta har även Constantine Petallides kommit fram till med resonemanget: “With no governing body or police force, the Internet perfectly fits the realist security model. In this setup, every state stands alone or with its allies, whom it can never fully trust, and desperately tries to build up its cyber strength and defenses while fearing that every breakthrough made by another state poses a direct threat to their security” (Petallides 2012)

8. Slutdiskussion

Med utgång i frågeställningen ”vilka mekanismer låg bakom Stuxnet-attacken mot Iran och hur kan dessa ses mot bakgrunden av informationsrevolutionen?” har analysen kunnat ge oss följande förklarning: mekanismerna bakom attacken grundade sig i att två stater, USA och Israel, gått samman för att skapa ett virus så potent att det kunde tillfälligt slå ut urananrikningen i anläggningen utanför Natanz. Motivet bakom attacken var att förhindra Iran att potentiellt komma ett steg närmare anskaffningen av kärnvapen. Det handlade sålunda om försöket att behålla relativ makt för två stater gentemot en tredje stat.

Att kunna förstå drivkraften bakom detta motiv gör att man måste se till systemet som de inblandade staterna befinner sig i. Systemet är anarkiskt i sin struktur och därmed tvingas de invävda staterna att söka sin egen säkerhet. Detta tog sig till uttryck som direkt handlande på eget initiativ från de två allierade. I sökandet efter säkerhet är makt det främsta verktyget. Makt definieras av styrkorna inom vissa förmågor och kapaciteter, som t.ex. innehavet av militära medel som kärnvapen, sett relativt till andra. Hur allt detta sedan kunde ses mot bakgrunden av informationsrevolutionen förklarades på följande sätt: Medlet för att behålla den relativa makten i Stuxnet-fallet kom i form av en cyberattack vilket påvisar att kontroll över och användande av informationsrevolutionens produkter är ytterligare en påverkningsfaktor av distribuerandet av förmågor och kapaciteter.
Därmed påverkas också den relativa makten och i slutändan säkrandet av överlevnaden för stater i det internationella systemet.
Utöver detta stärker upptäckandet av USA och Israel som skaparna av det ytterst potenta Stuxnet de traditionella staternas status som primära enheter i det internationella

systemet.

Slutligen påvisades också att strukturen hos det system som cyberrymden i form av internet utgör har en anarkisk karaktär vilket skulle kunna ses som en fortsättning, eller möjligen en förstärkning, på den mellanstatliga anarkin. Fallet Stuxnet och mekanismerna bakom det har därmed getts en möjlig förklaring i och med denna studies applicerande av Waltz strukturella realism. För vidare forskning vore det intressant att både granska utvecklingen av fenomen som cyberattacker men kanske främst undersöka och utvärdera hur IR-teorier som den strukturella realismen kan möta och förklara dessa *nya* företeelser.

Utifrån Eriksson och Giacomellos antaganden om svagheterna hos realismen och främst Waltzs strukturella realism så har denna studie av Stuxnet-attacken påvisat att teorin håller ett förklaringsvärde i informationsrevolutionens tidsålder gällande säkerhet och internationella relationer. Waltzs teori förtjänar möjligen ett tilltroende närmare den nivå som Hanna Kassab ger den när det kommer till cyberattack-aspekten av informationsrevolutionen (Kassab 2014, 63). Då informationsrevolutionens produkter visats sig påverka distributionen av förmågor mellan stater är en av Waltzs teoris mest centrala teman påtagligt relevant. Waltzs visade upp en rad exempel på faktorer där stater kunde vara olika framgångsrika och starka vilket i sin tur formade den rådande internationella arenan. I denna skara av faktorer kan nu rimligtvis även behärskande av informationstekniker och cyberrymden ingå.

Waltzs strukturella realism kan möjligen inte ge alla eller de mest ingående teoretiska verktygen för att förstå alla aspekter av informationsrevolutionen, något som till stor del hänger samman med den nivå teorin ligger på. Men tack vare teorins höga generella

nivå kan den mycket väl fungera som ett hjälpmedel för att förstå hur informationsrevolutionens konsekvenser på säkerhet och internationella relationer i slutändan blir ännu en arena där staters intressen möts, interagerar eller kolliderar med varandra.

Vidare studier och forskning krävs för att se vad den strukturella realismen, och hela den realistiska skolan, kan säga om ytterligare cyberattacker, när nya sådana skulle ske eller då mer fullständig information om redan skedda fall blir tillgängligt. Också andra aspekter av informationsrevolutionens påverkan på säkerhet och internationella relationer skulle kunna sättas under luppen för att antingen pröva olika tankar från realismen som IR-teori, eller till och med i slutändan utveckla den.

Källförteckning

Adams, James. 2001. “Virtual Defense.” *Foreign Affairs* 80 (3): 98–112. http://www.jstor.org/discover/10.2307/20050154?uid=16801480&uid=3738984&uid=2&uid=3&uid=18149320&uid=67&uid=62&sid=21103310333703.

Albright David, Brannan Paul, Walrond Christina. 2010. “Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?” http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/.

Buzan, Barry, Ole Wæver, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers. http://www.google.se/books?hl=sv&lr=&id=j4BGr-Elsp8C&pgis=1.

Carr, Jeffrey. 2012. *Inside Cyber Warfare*. 2nd ed. Beijing: O’Reilly.

CCDCOE. 2013a. “CCD COE - Reports & Articles.” Accessed December 2. http://www.ccdcoe.org/205.html.

———. 2013b. “CCD COE - Books.” Accessed December 2. http://www.ccdcoe.org/228.html.

Choucri, N. 2000. “Introduction: CyberPolitics in International Relations.” *International Political Science Review* 21 (3) (July 1): 243–263. doi:10.1177/0192512100213001. http://ips.sagepub.com/cgi/doi/10.1177/0192512100213001.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations*. Cambridge, Massachusetts: The MIT Press.

Christiansson, Magnus. 2004. *Säkerhetspolitisk Teori*. 1st ed. Stockholm: Militärhögskolan Karlberg.

Clayton, Mark. 2011. “The New Cyber Arms Race.” *Christian Science Monitor*: 26–71. http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race.

Clunan, Anne Harold A. Trinkunas. 2010. *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty*. Vol. 9. Stanford University Press.

Dunn Cavelty, Myriam., Victor. Mauer, and Sai Felicia. Krishna-Hensel. 2007. *Power and Security in the Information Age : Investigating the Role of the State in Cyberspace*. Aldershot, Hants, England: Ashgate.

Eriksson, Johan, and Giampiero Giacomello. 2006. “The Information Revolution, Security, and International Relations: (IR)relevant Theory?” *International Political Science Review* 27 (3) (July 1): 221–244. doi:10.1177/0192512106064462. http://ips.sagepub.com.proxy.annalindhbiblioteket.se/content/27/3/221.abstract.

Esaiasson, Peter. 2007. *Metodpraktikan : Konsten Att Studera Samhälle, Individ Och Marknad*. 3rd ed. Stockholm: Norstedts juridik.

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

George, Alexander L, and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, Mass.: MIT.

Gibson, William. 1984. *Neuromancer*. New York: Ace.

Guzzini, Stefano. 1998. *Realism in International Relations and International Political Economy : the Continuing Story of a Death Foretold*. London: Routledge.

Haas, Ernst B. 1953. "The Balance of Power: Prescription, Concept, or Propaganda?" *World Politics* 5 (04) (July 18): 442–477. http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=7650220.

IAEA. 2010. "IAEA Board Report, 18 February 2010." http://www.iaea.org/Publications/Documents/Board/2010/gov2010-10.pdf.

Kassab, Hanna Samir. 2014. "In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare." In *Cyberspace and International Relations*, edited by Jan-Frederik Kremer and Benedikt Müller, 59–76. Berlin, Heidelberg: Springer Berlin Heidelberg.

Keohane, Robert O, and Joseph S Jr. Nye. 1977. *Power and Interdependence : World Politics in Transition*. Boston: Little, Brown.

Korab-Karpowicz, W Julian. 2013. "Political Realism in International Relations." In *The Stanford Encyclopedia of Philosophy*, edited by Edward N Zalta, Summer 201. <http://plato.stanford.edu/archives/sum2013/entries/realism-intl-relations/.

Kremer, Jan-Frederik, and Benedikt Müller. 2014. *Cyberspace and International Relations*. Edited by Jan-Frederik Kremer and Benedikt Müller. *Cyberspace and International Relations*. Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/978-3-642-37481-4. http://link.springer.com/10.1007/978-3-642-37481-4.

Lindsay, J. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404. doi:10.1080/09636412.2013.816122. http://www.tandfonline.com/doi/abs/10.1080/09636412.2013.816122.

Maclean, William. 2010. "Iran 'First Victim of Cyberwar' -." *The Scotsman*, September 25. http://www.scotsman.com/news/iran-first-victim-of-cyberwar-1-811906.

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York: Norton.

Morgenthau, Hans J. 1948. *Politics Among Nations : the Struggle for Power and Peace*. 1st ed. New York: Knopf.

Morgenthau, Hans J, Kenneth W Thompson, and W David Clinton. 2006. *Politics Among Nations : the Struggle for Power and Peace*. 7th ed. Boston: McGraw-Hill Higher Education.

Petallides, Constantine J. 2012. "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Student Pulse* 4 (03). http://www.studentpulse.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat.

Rifkin, Jeremy. 2011. *The Third Industrial Revolution: How Lateral Power Is Transforming Energy, the Economy, and the World*. New York: Palgrave Macmillan. http://www.amazon.com/The-Third-Industrial-Revolution-Transforming/dp/0230115217.

Rosenau, James N, and J P Singh. 2002. *Information Technologies and Global Politics [Elektronisk Resurs] the Changing Scope of Power and Governance*. Albany, NY: State University of New York Press.

Saade, Tareq. 2010. "The Stuxnet Sting." *Microsoft Malware Protection Center*. http://blogs.technet.com/b/mmpc/archive/2010/07/16/the-stuxnet-sting.aspx.

Sanger, David E. 2012. "Obama Order Sped Up Wave of Cyberattacks Against Iran." *New York Times*, June 1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=4&hp&&pagewanted=all.

Shuster, Mike. 2009. "Iran Admits New Nuclear Facility." *NPR*, September 25. http://www.npr.org/templates/story/story.php?storyId=113217386.

Waltz, Kenneth Neal. 1979. *Theory of International Politics*. New York: McGraw-Hill, Inc. http://books.google.se/books/about/Theory_of_international_politics.html?id=Z17uAAAAMAAJ&pgis=1.

VirusBlockAda. 2013. "News VirusBlokAda - Rootkit.TmpHider." Accessed December 10. http://www.anti-virus.by/en/tempo.shtml.

Yin, Robert K. 2009. *Case Study Research : Design and Methods*. 4th ed. Sage Publications.

Zetter, Kim. 2011. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired Threat Level Blog*. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet.

Bilaga 1

Bild 1:*karta över Iran och Natanz* (Shuster 2009)

Bild 2:*satellitbild av anrikningsanläggningen i Natanz* (Zetter 2011)