Självständigt arbete (15 hp)

Författare		**Program/Kurs**
Kd.514 Björn Johansson		OP SA 15–18
		Antal ord: 10 616
Handledare	**Beteckning**	**Kurskod**
Jan Ångström		1OP415

HACKERGRUPPENS BETEENDE I INFORMATIONSKRIGFÖRING.

ABSTRACT:
With the ever-expanding speed of technological development and the dependence of social media outlets in everyday life. Information warfare can be used to strike targets with information operations from leaders down to the average person. Therefore, it is important to acknowledge the fact that attacks are being performed on our media corporations to influence are opinion. By influence opinion via deception the outcome of an attack even changes an election.

The aim of this paper intends to shed light on the behaviour of hacktivist groups. The Syrian Electronic Army will be the main character in this paper do to the groups plausible deniability connections to the Syrian regime. As this paper will show with the works of a case studies on this group with the theoretical framework of John Warden. Hacker groups with connections to a regime work towards influencing the public via the power of disinformation.

Nyckelord:
Information warfare, Syrian Electronic Army, John Warden, Strategic Theory

Innehållsförteckning

1 Inledning

1.1 Problemformulering

Kan man använda en krigsvetenskapligteori ur sitt vanliga element för att förklara situationer inom en annan del inom krigsvetenskapens stora område? Med ett nytt sätt att föra krig som uppstått i den nya generationens krigföring, eller hybridkrigföring som det även kallas, har det uppstått ett vakuum om vad som kan anses som fungerande teorier hämtade från reguljär och irreguljärkrigföring. Inom hybridkrigföring ingår informationskrigföring som har blivit en starkare del sedan 2010-talet. Denna typ av krigföring återfinns även inom reguljär samt irreguljär med aktioner med psykologiskkrigföring, propaganda samt även underrättelseinhämtning. Men med utvecklingen av internet samt den teknologiska utvecklingen av databaserade produkter gör det att informationskrigföring kan stå på egna ben som en typ av krigföring (Wither, 2016, ss. 75-76).

I och med att information kan ha en så pass stark påverkan mot en motståndare, till exempel det amerikanska presidentvalet 2016. Där påvisas det att det inom informationskrigföring är svårt att avgöra vem som gjort attacken (Inkster, 2016, s. 25). Konflikten som uppstod i Ukraina är också ett exempel på en konflikt där informationskrigföringen hade ett stort inflytande på hur konflikten skapades och fortgick (Boyd-Barrett, 2017). Ett ytterligare exempel på en aktör inom informationskrigföringen är Syrian Electronic Army. Denna grupp utförde attacker mot västerländska mål för att påverka västerländska nationer till följd av deras agerande inom den rasande syriska konflikten (Bertram, 2017, s. 5). Informationskrigföring är även en het potatis inför det kommande svenska riksdagsvalet 2018 (Sundberg, 2018).

Inom forskningen om informationskrigföring råder det delade meningar om tänkandet kring strategi och taktik i agerande (Robinson, Jones, & Janicke, 2015). Ur en teoretisk synpunkt blir det intressant att studera ett fall utifrån den systemteoretiska aspekten som John Warden presenterar. Den modell som Warden presenterar med att se en motståndare uppbyggd av olika system kan möjligen ge ett nytt synsätt på informationskrigföringens tillvägagångssätt.

Mellan 2011 och 2014 genomfördes operationer av en hackergrupp vid namn Syrian Electronic Army med kopplingar till den syrianska Assad regimen mot västerländska mål i cyberrymden. Redan 2008 hade likande operationer av denna typ genomförts av hackergrupper

med koppling till Ryssland mot Georgien för att påverka deras befolkning samt att öka stödet inom Ryssland för en aktion mot Georgien. Vidare sker samma fenomen med hackergrupper med kopplingar till Ryssland under krisen i Ukraina som resulterade i Krim-krisen. Ryssland kallar denna del av operationer för den nya generationens krigföring. Med hjälp av att använda informationskrigföring, som ett starkt hjälpmedel till att påverka en befolkning, samt att med detta handla i en gråzon där de kan använda sig av andra typer av krigföring för att nå strategiska mål (Blank, 2013, s. 44).

Forskningen visar, i avsnitt 1.2, att det är klassiska typer av strategiskt tänkande som styr utvecklingen av användandet av informationskrigföring. Olika traditioner samt kulturer kan vara en skillnad mellan hur informationskrigföring kan användas. För att förstå informationskrigföring mer skulle en ny teoretisk ståndpunkt möjligen förklara beteende och tillvägagångssätt mer genom att möjligen se saker som andra teorier inte fått fram. En teori som inte behandlats i djup i tidigare forskning är den luftstrategiska teorin fem-rings modellen framställd av John Warden, där Warden lutar sig mot en systemteoretisk anblick på en motståndare.

Med hjälp av en analys av Syrian Electronic Armys och deras attacker mot västerländska mål med John Wardens fem-rings modell kunna få en förklaring till vad en hackergrupp med kopplingar till en regim, eller stat, agerar inom informationskrigföringen. Samt att med en annan teori inom strategisk krigföring förstå hur attacker sker mot en motståndare med informationskrigföring utifrån ett ”system av system”-tänkande. Kan då en strategisk luftmaktsteori användas till att analysera informationskrigföring?

1.2 Forskningsöversikt

Under en jämförande fallstudie av Rysslands informationskrigföring i Georgien och Ukraina så drar författaren Iasiello slutsatser om att även mindre stater kan gå segrande i konflikter med informationskrigföring. Med hjälp av att analysera Georgien kriget och konflikten på Krim utifrån en teknisk och en psykologisk aspekt. Iasiello grundar sina slutsatser på en kvalitativ innehållsanalys. Författaren presenterar sina slutsatser att Georgien själva genomförde lyckade informationsoperationer för att ligga på framkant med den inhemska legitimiteten samt legitimitet mot västvärlden (Iasiello, 2017, s. 54). De brister som finns i Iasiellos arbete kan möjligen vara användandet av debattartiklar som källa. Dock är det så att det kan vara de-

battörens tankar och slutsatser som presenterat. Detta möjliggör att texten kan vara relevant beroende på hur Iasiello har analyserat sin empiri.

Ignas Kalpokas skriver i sin artikel *Information warfare on social media: A brandmanagement perspective* om informationskrigföring på och via sociala medier. Författaren ger ett förklarande perspektiv på debatten om hur socialmedier påverkar en stat. Detta genom en kvalitativ metod, metoden som författaren har används sig av är en kvalitativ innehållsanalys. Författaren påstår att en stat kan påverkas av händelser på sociala medier på grund av till exempel negativ opinionsbildning.

Kalpokas för sin argumentation utifrån att beskriva varumärken och effekter som påverkar dessa i sociala medier. Författaren definierar i detta en stat som ett varumärke då det kan påverkas på samma sätt via sociala medier. Ett pro-argument som tas upp är att med hjälp av sociala medier så kan strategisk information bli en seger trotts förlust i en operationell/taktisk kontext. Ett annat argument som författaren tar upp är hur påverkan lättare kan ske. Författare tar då upp att på grund av den ständiga uppkopplade individen så finns det tillgång till att influera fler till en lägre ekonomisk kostnad. Påverkan på individer blir också mycket lättare att genomföra på grund av det faktum av hög nivå av uppkoppling (Kalpokas, 2017). Slutsatserna som Kalpokas drar utifrån sin studie är att det är viktigt för en stat att framhålla en god bild av sig själv som stat. Risken för att påverkas ökar både inom landet som utom landet. Enstaka individer kan enkelt påverka en stats status med hjälp av sociala medier.

Alan Chong argumenterar i sin artikel *Information Warfare?: The Case for an Asian Perspective on Information Operations* om hur strategier om informationskrigföring i Asien inte kommer kopiera västerländska tänkare i deras strategier. Författaren har med en kvalitativ innehållsanalys gjort en komparativ analys av västerländsk syn på informationskrigföring mot tidiga asiatiska strategiska tänkare (Chong, 2014). Författaren ger en förklarande aspekt på hur de tidigare tänkarna påverkar och influerar.

Chong argumenterar för att den västerländska synen på teorier om strategier i informationskrigföring inte kommer influera asiatiska länder, framförallt Kina, lika starkt som de västerländska tänkarna tror. Chong grundar sina argument om att den österländska filosofin om

strategier har större påverkan än vad som tros. Artikeln jämför den västerländska teorin om informationskrigföring mot klassiska österländska strategiska tänkarna som Sun Tzu, Mao och Giap. Argument för den mer filosofiska inriktningen för asiatiska länder menar Chong ligger inom kulturen som länderna har gemensamt. Olika kulturella traditioner påverkar hur asiatiska länder agerar och tolkar situationer gentemot de västerländska teorierna (Chong, 2014, s. 618). Författarens stringens genom arbetet är tydlig. Chong presenterar den västerländska teorin och jämför sedan med de klassiska tänkarna.

Det som kan uppfattas som konstigt i arbete är att det baseras på gamla tänkare som inte hade den teknologiska tillgången som finns idag. Dock presenterar Chong ett bra påstående att den västerländska teorin till grunden bygger på värderingar och tankade från Clausewitz. Det blir på detta sättet tydligt att det inte innebär att arbetet inte enbart är en textanalys utan att det även finns en diskursanalys. Detta då tolkning av vad de österländska tänkarna samt kulturen säger om det som står och hur det kopplas till nutid.

Robinson et al. bidrag till forskningen med sin artikel är slutsatsen att ämnet gällande informationskrigföring är fortsatt odefinierat och på så sätt svårt att tolka. Detta ger forskningsluckor som författarna menar endast kan lösas av att genomföra specifika studier inom de olika ämnena som finns inom informationskrigföring (Robinson, Jones, & Janicke, 2015, s. 91). Slutsatsen byggs på en studie som genomförts med argumentationsanalys och kvalitativ innehållsanalys med en stor mängd insamlade data. Den data som har analyserats är tidigare forskning inom ämnet som rör cyber war eller cyber warfare.

Bishop och Goldman argumenterar för att förståelsen kring informationskrigföring måste analyseras utifrån en attackbaserad analys. I motsats till effektbaserad analys är en attackbaserad analys den mest passande då försvar mot informationskrigföring byggs på genomförda attacker och inte deras effekter. Förståelsen kring attacker menar författarna är viktigt för att skapa defensiv kunskap om attacker. (Bishop & Goldman, 2003, ss. 135-136). Med en kvalitativ studie försöker författarna att konkretisera vad för typ av strategiskt och taktiskt medel som krävs för att förstå informationskrigföring.

Utifrån dessa studier som genomförts så blir det mer tydligt att det finns en forskningslucka. Chong meddelar med sin artikel att det inte enbart är den västerländska filosofin kring krigföring som kommer inspirera inom informationskrigföring. Med gamla asiatiska tänkare som grund kommer artikeln med ny information kring hur dessa tänkare som är mer subjektiva kan vara mer gynnsamma inom informationskrigföringen. Utifrån ett varumärkesperspektiv visar Kalpokas på att det är tydligt att en stat inte gärna vill hålla på med informationskrigföring öppet. Samtidigt visar Kalpokas att stater behöver utföra någon form av informationskrigföring mot egna medborgare samt mot omvärlden. En aktör som har diffusa kopplingar till en stat kan påpeka sin autonomi samtidigt kan staten påpeka dess oskuld vid en eventuell aktion. Vidare presenterar Iasiello sin slutsats om hur små stater även kan åstadkomma påverkan inom informationskrigföring. Det som tas upp är vilken typ av strategi som de olika staterna använde. Iasiello presenterar mycket av den ryska visionen om informationskrigföring. Det som kallas för den nya generationens krigföring, där de bästa delarna från alla möjliga krigföringskonster plockats ihop i samma korg för att vinna kriget.

Robinson et al. menar på att även små stater kan hävda sig inom den stora informationsarenan. Samtidigt så påstår Bishop och Goldman att analyser inom informationskrigföring ska genomföras utifrån ett attackbaserat perspektiv. Detta då analysverktyget bäst förklarar den på vilket sätt som defensiva kunskapen kan öka. I och med att attacker är ständigt skiftande medans effekten som ska uppnås kan var den samma som tidigare strategier.

Med problemformuleringen i åtanke och denna forskningsöversikt blir det tydligare att en lucka finns. Luckan handlar utifrån det presenterade om attackbaserad teori kan förklara en liten aktör inom informationskrigföringen.

1.3 Syfte

Med en fallstudie av Syrian Electronic Army mellan år 2011 och 2014 som analyseras utifrån John Wardens fem-rings modell. Detta för att förklara beteendet hos aktörer som har en koppling till mindre stater, samtidigt som aktören ska ha en fasad av att verka autonomt. Samt vilka delar av modellen som kan användas inom informationskrigföring.

Det inomvetenskapliga syftet med detta arbete blir att studera en aktör med kopplingar till en stat som utför informationskrigföring. Medans det utomvetenskapliga syftet blir att visa hur informationskrigföring kan påverka människor till vardags.

1.4 Frågeställning

Hur kan attacker som genomförts av Syrian Electronic Army förklara deras beteende med hjälp av en analys med Wardens fem-rings modell?

1.5 Avgränsningar

Syftet med arbetet är att undersöka en grupp inom informationskrigföring. En avgränsning sker här genom att definiera begreppet informationskrigföring som ett begrepp med mycket bredd. Definitionen sker i nästkommande kapitel.

En avgränsning sker också i analysen av Syrian Electronic Army gällande tiden. Arbetet kommer att analysera gruppens incidenter mellan 2011–2014. Med syftet att analysera gruppens beteende och dra slutsatser utifrån Wardens teori så sker avgränsningen i tid. Avgränsningen sker för att precisera men även också för att få in mer data att analysera. Då incidenter med Syrian Electronic Army sker över en längre tid anses det viktigt att göra en avgränsning i att analysen görs över tid och inte genom en specifik händelse.

1.6 Disposition

I teorikapitel presenteras först centrala begrepp samt den valda teorin för arbetet, John Wardens fem-rings modell. Därefter presenteras en bakgrund till det valda fallet, en presentation om Syrian Electronic Army och dess historia samt deras tillhörighet. Efter denna bakgrund till det valda fallet presenteras operationaliseringen av den valda teorin. Slutligen presenteras en diskussion rörande kritik om den valda teorin.

I metodkapitlet presenteras den valda forskningsdesignen. Valet av teori, fall, operationalisering samt metod diskuteras och motiveras. En materialdiskussion sker sedermera i slutet av kapitlet för att diskutera principerna för källkritik i samband med valet av empiri och litteratur.

I analyskapitlet presenteras analysen av fallstudien utifrån den operationalisering som skett tidigare. I detta kapitel presenteras även resultaten av analysen.

I det avslutande kapitlet presenteras slutsatserna av resultatet samt svaret på problemformuleringen. Vidare återfinns det ett avsnitt om relevansen till krigsvetenskapen och officersprofessionen samt förslag på vidare forskning. Kapitlet avslutas med ett avsnitt med reflektioner om arbetet.

2 Teori

I detta kapitel presenteras valet av teori och fem-ringsmodellen av John Warden närmare. En introduktion till *Syrian Electronic Army* samt varför denna grupp valdes till att analyseras. Kapitlet avslutas med att presentera den kritik som finns mot denna teori samt argumentation för den valda teorin.

2.1 Centrala begrepp

Nedan kommer centrala begrepp för detta arbete att presenteras. De presenteras i syfte att ge begreppen en tydlig innebörd för kommande teoriavsnitt och analysdel.

Informationskrigföring.

Informationskrigföring definieras i detta arbete som den krigföring som sker med medel som innefattar information som presenteras eller sänds ut digitalt. Det vill säga allt från att en psykologiskoperation i form av en tidningsartikel till en elektroniskattack i form av en överbelastnings attack mot en digital värd. Cyberattacker, psykologiska operationer och attacker mot ledningsfunktioner för att störa ut en motståndare faller alla in under denna definition av informationskrigföring (Libicki, 1996, ss. 85-89).

Beteende

Beteende definieras i detta arbete som det mönster som en hackergrupp har i sitt agerande. Med teorier som fokuserar på effekt av påverkan blir beteende den del som kan sammanfatta detta i en diffus arena som informationskrigföring. Mönster som framkommer kommer således att kunna tolkas lättare i en analys.

2.2 Wardens fem-rings modell

Strategiskt tänkande enligt Warden är en deduktiv metod för att genomföra krig. Detta menar Warden är på grund av den tidigare erfarenheten. Den erfarenhet som insamlats hos befälhavare gör att de drar antaganden som är välgrundade utifrån kunskapen på taktisknivå. Warden gör jämförelsen mellan en arkitekt och en murare för att förklara att arkitekten inte kan se på ett uppdrag ur varenda tegelsten utan måste ha ett större perspektiv för att lösa en byggnation. Medans muraren, enligt Warden, inte kan bygga ett fungerande hus genom att bara stapla tegelstenar (Warden, 1995, s. 42).

John Warden beskrev sin teori om motståndaren som ett system av system i sin artikel *Enemy as a system* 1995. Med bakgrund i agerandet av den amerikansk ledda koalitionen under Gulfkriget 1990 presenterar Warden teorin med fem, för att vinna kriget, väsentliga delar för att en motståndare skall bekämpas snabbt och effektivt (Warden, 1995, s. 43). Dessa delar är underbyggda för hur man skall se på en motståndare. En motståndare består enligt Warden av system av system. Han presenterar även teorin med ett tankesätt om *center of gravity* där dessa fem delar rangordnas utefter dess effekt att möjliggöra att vinna kriget snabbt. Modellen består av *leadership, organic/system essentials, infrastructure, population* och *fielded military* (Warden, 1995, s. 44), modellen visualiseras i *bild 1*. Dessa ringar har en inbördes ordning. Ordningen baserar Warden på antalet individer eller antalet byggnader som finns i vardera ring. Detta gör Warden för att förklara att det är färre individer som ska påverkas i ledningsringen gentemot i populations-ringen. Detta på grunda av att det krävs mer effekt för att påverka en större massa än en mindre massa. Nedan kommer modellens ringar att presenteras mer ingående.

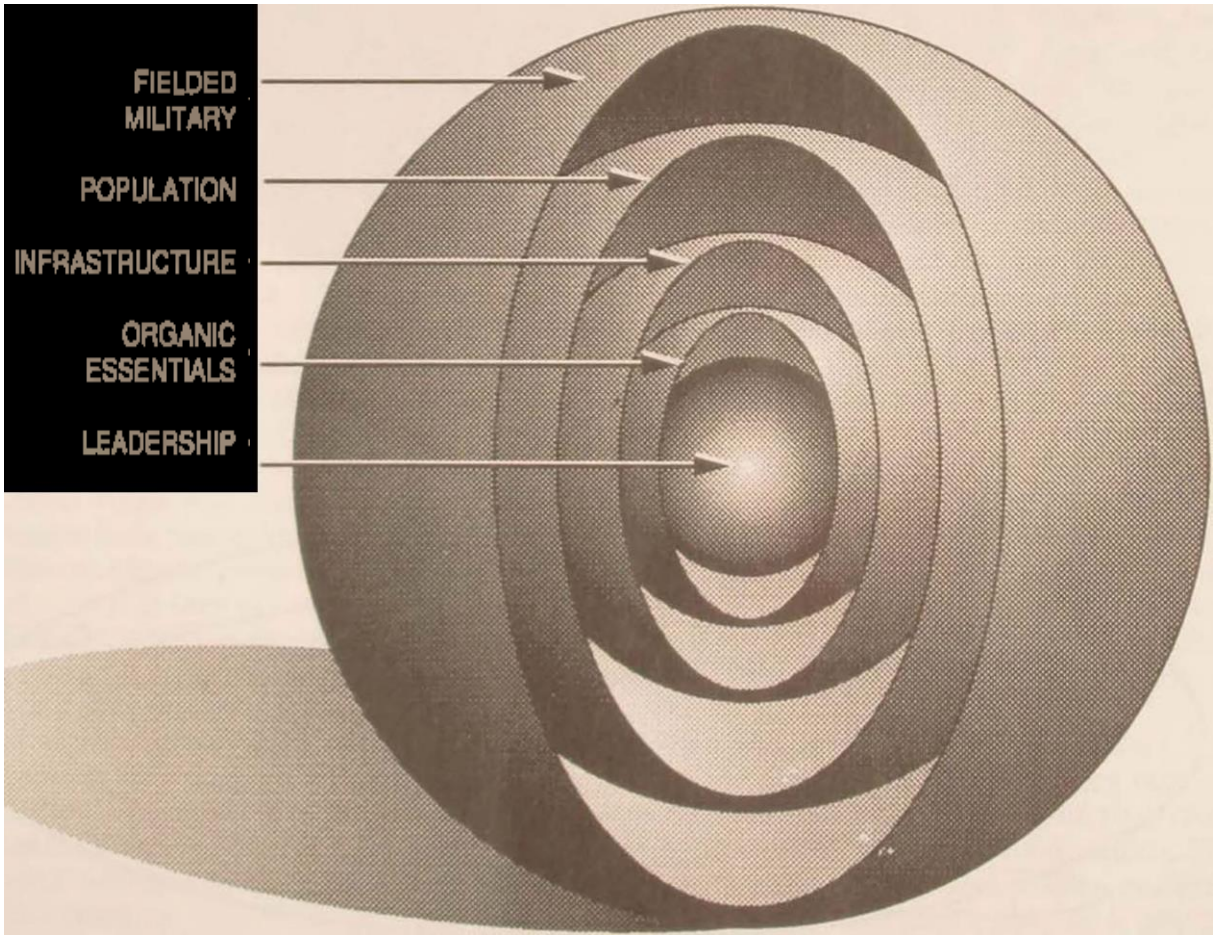

Bild.1. Fem-ringsmodellen visuellt presenterad (Warden, 1995, s. 47)

2.2.1 Center of gravity

För att förstå fem-rings modellen så måste Wardens tankar om *center of* gravity presenteras. Med *center of gravity* syftar Warden till den punkt som har kontrollen för att använda ett förenklat utryck. Kontrollen syftar till den del hos en motståndare som med minsta möjliga kraft kommer påverka den maximala bredden (Warden, 2000, s. 7). Ett exempel är ledningen. En militär chef som leder en verksamhet har information om vad som planeras ske, vad som skett och hur de styrkor som finns kommer att användas nära till hands. Med olika medel påverka denna punkt i en, för exemplets skull, militär operation kommer ge väldigt stor påverkan på det resultat som förväntas av den militära chefens ledning. *Center of gravity* är på så sätt den punkt som vid påverkan kommer att påverka andra funktioner likt ringarna på vattnet. Med denna tanke om systemets kärna menar Warden på att systemkollaps uppstår snabbare.

2.2.2 Leadership (ledning)

Denna ring i modellen är med tyngdpunkt på ledare eller ledning inom en stat eller organisation. Warden beskriver denna del likt hjärnan, ögonen och nervsystem i en människa. System som är vitala för att vi ska inhandla information, utvärdera och skicka vidare signaler (Warden, 1995, s. 45).

Denna ring är den klart viktigaste delen i modellen. På grund av att ledare och ledning är så fundamentalt för det basala sociala systemet. Organisatoriska system är en del av det mänskliga beteendet inom sociala konstruktioner, det finns allt som oftast någon typ av maktstruktur där organisationens beslut tas och senare sprids ut i organisationen (Warden, 1995, s. 52).

2.2.3 Organic/systems essentials (kritiska system)

Organic essentials eller system essentials är de system inom systemet som möjliggör andra funktioner. Ser vi till liknelsen till människokroppen menar Warden att detta steg är maten eller syret som människan sedermera omvandlar i sina organ till energi. En annan liknelse är i en stat till exempel energisystem (oljetillgångar, elnätet) samt även pengar (Warden, 1995, s. 45).

Det gäller att inte förväxla denna ring med infrastruktur. Den diffusa definitionen av ett elnät kan samtidigt också vara en form av infrastruktur. Skillnaden blir mer tydlig i om man tolkar

elnätet som ett kritiskt system som helhet för att till exempel infrastrukturen, med sjukhus etc., ska fungera klanderfritt.

2.2.4 Infrastructure (infrastruktur)

Infrastrukturen är enligt Warden de system som är transportsystemet som sammankopplar de olika system med varandra. Inom kroppen är det då ben, muskler och blodomloppet. Inom en stat är det till exempel vägar som sammankopplar ett oljeraffinaderi till hamnen. Vattenledningar som finns inom en stad och fram till dess vattenverk (Warden, 1995, s. 50). Som nämndes tidigare är det lätt att para ihop denna ring med organic systems. Definitionen av denna ring ligger mer mot den faktiska kopplingen mellan olika delar inom, till exempel, en stad.

2.2.5 Population (Population/Befolkning)

Populationen är det system i denna modell som inom krigsvetenskapen kan tolkas som väldigt lättolkad vad det är. Befolkningen i en stat eller inom en organisation (Warden, 1995, s. 50). Med indirekta medel menar Warden att befolkningen påverkas. Dock menar Warden att man inte kan räkna med effekt med tankar om indirekt verkan mot populationen (Warden, 1995, s. 51).

2.2.6 Fielded military (Försvar)

Denna del utgör de väpnade styrkor en stat har. Det markburna-element i en motståndares krigsorganisation. Denna del i teorin är den del som Warden hävdar ger minst effekt att slå ut för att vinna kriget snabbt. Warden menar att lägga effekt på att slå ut en motståndares styrkor är ohållbart. Detta menar Warden beror på att de väpnade styrkorna inte kan elimineras tillräckligt fort för att vinna kriget samt att de andra delarna i teorin spelar högre roll mot att nå ett strategiskt mål (Warden, 1995, s. 51).

2.2.7 Parallella attacker

En motståndares vitala funktioner inom modellens ringar är oftast få till antalet. Inom ledning-ringen är det uppenbart att det allt som oftast bara finns en officiell ledare av en stat. Inom ringarna organic/system essentialls och infrastruktur finns det oftast ett antal mål som vid påverkan har potential att få systemet att kollapsa. Dessa mål är oftast av den art att de till exempel är väldigt dyra eller svåra att reparera samt att det kan finnas få reservfunktioner. En attack mot ett sådant mål gör att dessa är optimala att slå ut då det krävs mycket resurser för

att åtgärda uppstående problem (Warden, 1995, s. 54). Ett exempel är ett kraftverk och dess elnät. Det finns allt som oftast enbart ett begränsat antal kraftverk inom en stat. Reparationer eller reservdrift kan göra det svårt att få ut önskad effekt.

Med parallella attacker skapas en mer gynnsam effekt för att vinna det strategiska kriget. Vid användandet av serieattacker så kan en motståndare sprida ut sina vitala funktioner för att motverka attackernas effekt. Parallella attacker syftar till att slå mot flera av modellens ringar samt funktioner inom ringarna samtidigt för att uppnå en större strategisk effekt av attackerna (Warden, 1995, s. 54).

2.2.8 Sammanfattning

Med modellen som Warden framställer visar han på att en motståndare är ett system av system. För att vinna ett krig på effektivaste sätt kategoriserar Warden motståndarens system (*ringarna i modellen*) för att påvisa vilken som det är mest tyngdpunkt i (*center of gravity*). Utifrån denna kategorisering kan sen planer byggas för att på enklaste sätt vinna kriget med hjälp av att uppnå en systemkollaps. Systemkollapsen uppstår när en eller flera av ringarna påverkas så pass mycket att dess funktion upphör. Detta menar Warden kan uppstå med hjälp av att genomföra parallella attacker mot motståndaren.

2.2.9 Diskussion

Det råder en pågående debatt inom det luftstrategiska tänkande inom krigsvetenskapen. Robert Pape har motsatt sig Wardens teori och dess funktion med att vinna kriget endast med hjälp av luftmakt och strategiska medel.

Vidare kan det påpekas att Wardens teori är högt flygvapenorienterad för lösande av uppgiften att vinna kriget på egen hand. Detta gör att den förutsätter vissa saker och tar andra för givet. I inledningen till sin artikel där Warden presenterar sin teori påpekar han just vikten av att flygofficerare med längre tid i chefsbefattning har lättare till att tänka strategiskt. Till detta kan hävdas att det kan gälla samtliga vapengrenar, inte enbart flygvapnet. En chef som genomfört taktiska uppdrag en längre tid bör kunna ha högre förståelse för dessa taktiska uppgifter vid lösandet av strategiska mål senare i sin karriär oberoende av vapenslagstillhörighet. Teorin kan också syfta till att få en effektfull påverkan genom att tydliggöra att till exempel den amerikanska flygvapnet kan bomba ”skiten” rent strategiskt ur motståndaren.

2.3 Syrian Eletronic Army (SEA)

Den arabiska våren medförde revolutioner inom det politiska styret i länder som Egypten och Tunisien. Den syriska regimen med sin ledare Assad var en stat som kvävde den revolutionistiska gnistan hos befolkningen som kände sig orättvist behandlad (Abboud, 2016, ss. 59-60). *Syrian Electronic Army* hävdar att de är en grupp ungdomar som skapades för att skydda sitt Syrien mot cyberattacker. Gruppen berättar också att de inte tillhör någon officiell del av staten samt att de är politiskt obundna (Al-Rawi, 2014, s. 420). *Syrian Electronic Army* är en hackergrupp som utför informationsoperationer samt cyberattacker. Kopplingen mellan den syriska regimen och denna hackergrupp är en diffus gräns av att regimen hjälps och hjälper samtidigt som regimen kan stå fria från skuld med att hävda att gruppen är en autonom aktör (Al-Rawi, 2014, s. 423).

Relationen mellan hackergruppen och den syriska regimen ger att SEA är en tydlig pro-regimsk grupp. I och med att gruppen uppkom lämpligt i tid efter att informationsoperationer och attacker mot den syriska regimen. Detta gjorde att den syriska regimen stänge ner det öppna internet och sedermera hårdfiltrerade internets innehåll för sina medborgare. SEA ges dock fria tyglar på internet av regimen för att sprida propaganda och genomföra påverkanskampanjer (Grohe, 2015, s. 135; Bertram, 2017, s. 6). Den syriska regimen granskar sociala medier på rutin för att motverka oppositionella websidor och dylikt. Med en sådan strikt granskning så borde implicit den syriska regimen vara väl medveten om gruppen SEA och på så vis godkänna deras ageranden (Bertram, 2017, s. 6).

En annan stor koppling mellan Syrian Electronic Army och den syriska regimen återfinns i samröret mellan den syriska data styrelsen och regimens ledare Bashar al-Assad. Syrian Computer Society som är organet som bland annat äger domänen ***.sy*** grundades av Assad på 90-talet (Warren & Leitch, 2016, s. 204).

Med bakgrund till hur SEA har agerat som grupp så är en definition som autonom aktör svår att dra. För att gruppen ska vara autonom krävs det att den ska vara oberoende och självstyrande (Nationalencyklopedin, autonom, 2018). Oberoende kriteriet i definitionen av autonom uppfylls inte av SEA då de är har en pro-regim agenda. Definitionen om att det ska vara själv-

styre är den del som är svår att utröna. Kopplingar finns, som sagts tidigare, till Assad-regimen vilket gör grunden till denna definition skakig och opålitlig.

Utifrån forskarvärldens bild på Syrian Electronic Army är det en grupp som är svår att sätta en definition på. Det finns tydliga och uppenbara kopplingar mellan gruppen och den syriska regimen, men samtidigt finns det ingen bevisning som kan styrka detta påstående.

3 Metod

Metod kapitlet är till för att förklara hur författaren har gått tillväga med sin undersökning. I detta kapitlet kommer arbetets forskningsdesign att presenteras.

Inledningsvis kommer introduktion och förklaring till vald forskningsmetod. Därefter kommer det att följa avsnitt där materialet, *empirin*, diskuteras utifrån källkritiska riktlinjer inom forskningsetiken samt hur materialet valdes ut. Slutligen kommer en metoddiskussion om avslutat detta kapitel. I den avslutande diskussionen kommer reflektioner om metoden och arbetets gång presenteras för att möjliggöra en transparens för arbetets gång.

3.1 Forskningsdesign

Med hjälp av att genomföra en enfallsstudie samt kvalitativ textanalys kommer problemformuleringen att besvaras. En fallstudie för att analysera *Syrian Electronic Army*s genomförda attacker med Wardens fem-rings modell ger en

3.1.1 Motivering till vald teori

John Wardens teori valdes till detta arbete för att utifrån ett nytt perspektiv se på informationskrigföringen. Den systemteoretiska aspekten som Warden presenterar i sin teori förklarar tydligt hur man kan se på en motståndare. Detta då Wardens olika premisser inom teorin kan innefatta många aspekter inom en motståndares organisation som kan påverkas av en direkt kinetisk attack inom strategiskbombning. Warden bygger sin teori på att se motståndaren som ett system av system.

Alla system har ett *center of gravity*, den punkt där massan rör sig runt. De olika systemen inom modellen är i sin tur i en ordnad form av center of gravity. Den punkt som Warden menar är den som massan, de andra delarna inom modellen, roterar runt är *ledning*. Utifrån ringarna i modellen kan man således analysera en motståndare baserat på de premisser som Warden ställer i sin modell.

Teori visar med tyngdpunkten i ring modellen hur en motståndare kan tänkas vara uppbyggd av olika system. Det är inte säkert att alla systemen inom modellen existerar hos en motståndare men minst finns i alla fall ledningsringen enligt Warden.

Tillsammans med fem-rings modellen och Wardens tankar om parallella attacker på de olika ringarna, för att nå maximal effekt, så finns det god grund till att förklara en motståndares beteende utifrån denna Wardens tankar. De systemteoretiska aspekter om motståndaren som ställs fram i modellen är väldigt tätslutande kring att ta upp en större portion information om en motståndare än att vara specifik mot ett område.

I och med att informationskrigföring är ett brett ämne lämpar sig Wardens fem-rings modell med dess bredd om motståndaren till att utforska nya kunskaper i ämnet informationskrigföring.

3.1.2 Motivering till val av metod

Fallstudie

En fallstudie syftar till att undersöka ett eller flera fenomen inom en viss vetenskap. Fallstudier används för att samla data kring en händelse eller individ (Johannessen & Tufte, 2003, s. 56). I och med en teorikonsumerande ansats har utrönts så är en fallstudie den mest använda samt användbara metod att genomföra detta arbete (Esaiasson, Gilljam, Oscarsson, Town, & Wängnerud, 2017, s. 42). En undersökning om fallet Syrian Electronic Army med hjälp av Wardens fem-rings modell som analys verktyg kommer också att innebära att detta arbete även väger mot att vara en teoriutvecklande studie. Detta då en teoriutvecklandestudie ämnar ”resultera i ett förslag till nya förklaringar till det fenomen som studeras.” (Esaiasson, Gilljam, Oscarsson, Town, & Wängnerud, 2017, s. 43).

Med detta som bakgrund finner jag det mest lämpligt att genomföra en analys på fallet Syrian Electronic Army med John Wardens fem-ringsmodell som analysverktyg. Med en fallstudie kan problemet åskådliggöras lättare i en analys med hjälp av teorin.

Kvalitativ textanalys

I och med att fallstudie används för att se närmare på en händelse i informationsmiljön så måste det till att använda kvalitativ textanalys för att förstå vad som hänt. Kvalitativ textanalys grundar sig i att studera texter om till exempel en händelse, i detta fallet en fallstudie av SEA.

För att utröna vad som har hänt används den kvalitativa textanalysen för att förstå vad som skrivits utifrån ett objektivt sätt. Dock kan det vara en subjektiv text som undersöks för att

förklara ett fall, förförståelsen till det fallet är då väsentlig att förstå då det gör det lättare att tolka det som skrivits.

3.1.3 Motivering till valda fallet

Syrian Elecronic Army är ett fall av en nutida svår fråga: *vem är vem och vem gör vad på internet?* Denna fråga speglar svårigheten med att fastslå att gruppen tillhör en stat. Samtidigt visar flera forskare som studerat hacktivism, cyberkonflikter och informationskrigföring att det finns tydliga tecken på att gruppen är direkt länkad med den syriska regimen och regimens agenda (Al-Rawi, 2014; Grohe, 2015; Warren & Leitch, 2016). Dock är det svårigheterna i att bevisa just kopplingen mellan en stat och en cyberaktör som skapar dilemman i att forska inom området.

Ett antagande om Syrian Electronic Armys koppling till den syriska regimen görs i detta fall då jag menar att agerandet som sker är det modus operandi som gäller för informationskrigföring. För att dra till med ett amerikanskt uttryck om situationen mellan stat och aktör är det *plausible deniability* som gäller. Det politiska styret i ett land ska kunna förneka all vetskap om vad det är som har genomförts när en grupp avslöjats.

3.2 Material/Empiri

I detta avsnitt kommer arbetets material och empiri att presenteras samt analyseras utifrån källkritikens olika principer.

Vid sökning för material och empiri till fallet på Anna Lindh bibliotekets sökmotor PRIMO så angavs sökorden *Syrian Electronic Army*. Resultaten sorterades sedan via avgränsning att det skulle vara från en vetenskaplig tidskrift samt att den skull vara expertgranskad, så kallad peer-reviewed.

Det empiriska material som finns att tillgå om Syrian Electronic Armys attacker i informations och cybermiljön är begränsad till studier som har genomförts om denna grupp. SEA aktioner mot mål inom informationssfären belyses av olika författare som gjort empiriska undersökningar om gruppen. Författarna till dessa texter använder också SEA som fall i fallstudier och det är tillsynes vittskilda saker som prövas med hjälp av deras insamlade empiri.

Artiklarna som har används till fallstudien är publicerade av vetenskapliga tidskrifter där de tillämpar god peer-reviewed sed, med detta menas att tidskrifterna har mer än en person som granskar alstren och det sker blint. Dock kan det anses finnas en konflikt gällande beroende-kriteriet inom dessa texter om SEA. Samtliga författare har granskat det som finns om attack-erna på internet. Detta gör att deras insamlade data är samma data på vissa punkter. Det kan tyckas att det är konstigt att ta empiri från artiklar som kan ha en källkritisk brist (Esaiasson, Gilljam, Oscarsson, Town, & Wängnerud, 2017, s. 293). Med detta sagt så är den data som är insamlad genom dessa författare den som fanns att tillgå på internet om SEA.

Med tanke på tiden som har gått från första attacken och nutid så är den data som är insamlad, för undertecknad, ett sätt att hävda att alla artiklar blir sekundära källor oberoende av varandra. Detta på grund av att internet är en så pass stor informationshubb där data kan upp-stå och försvinna på millisekunder.[1]

3.3 Operationalisering

Operationaliseringen av teorin genomförs för att kunna mäta teorin inom ett nytt område. Från luftstrategiskteori till teori om informationskrigföring är modellen tvungen att omvärderas för att kunna mäta den data som finns i cyberrymden.

Som teorin presenteras i kapitel 2 blir fem-ringsmodellen tvungen att bli operationaliserad för att kunna tolkas mot informationskrigföring. För att öka arbetets validitet måste Wardens teori operationaliseras till att innefatta mer relevans till det som ska studeras (Bergström & Boréus, 2005, s. 41). Informationskrigföring är inte samma sak som strategisk luftkrigföring. Med en operationalisering skapas i arbetet en ökad relevans till att undersöka det som ska undersökas. Alltså undersökningen av en grupp som genomför attacker inom informationsarenan genom linsen av en systemteoretisk luftstrategisk teori. Den initiala versionen av modellen är framta-gen för att vara hård strategisk och kinetisk krigföring i luftkriget. I och med att informations-arenan är en diffus, men binär arena, så är kinetiskkrigföring inte lika lätt att genomföra på det sätt som teorin i original menar att kriget skall vinnas på.

[1] Undertecknads egna reflektion om internets storhet. Ett exempel är Wikipedia där informat-ion lätt kan redigeras av användare utan att det märks av gemene användare.

En operationalisering görs för att få fram essensen i det som ska undersökas. I detta fall blir det att definiera de olika delarna i Wardens femringsmodell för informationskrigföring. Tanken med operationaliseringens slutprodukt är att forskning ska kunna göras på samma, i detta arbetet, definitioner. På så sätt ska arbetet kunna genomföras av en annan individ på samma sätt för att får samma resultat genom att använda samma operationalisering av Wardens teori. Detta för att ge en ökad reliabilitet till undersökningen (Esaiasson, Gilljam, Oscarsson, Town, & Wängnerud, 2017).

Forskningsfrågan som är ställd innefattar hur *beteendet* ska analyseras. I denna operationalisering ligger *påverkan* av en aktion tillgrund för indikatorer inom analysverktyget. Anledningen till att *påverkan* blir indikator i ringarna är att det är vad grupper som SEA fortfarande opererar för att uppnå. Beteendet i *hur* en grupp som SEA använder sig av attackerna definieras utifrån fem-rings modellen samt center of gravity och parallella attacker. Att operationalisera center of gravity och parallella attacker behövs ej då de samspelar med fem-rings modellen utifrån dess premisser av givna indikatorer. Center of gravity och parallella attacker kan inte anses som typiskt för informationskrigföring utan kan anses mer generella (Johannessen & Tufte, 2003, s. 45).

Nedan kommer operationaliseringen av de fem delarna i modellen för informationskrigföring att presenteras.

3.3.1 Leadership

Denna del i Wardens modell kommer inte att förändras. Ledning kommer fortfarande finnas för att påverkas inom informationskrigföring. Detta gör att definitionen enligt tidigare är den samma. Wardens syfte med sin strategiska teori är att ledning betyder person av ledande ställning, politiskt eller militärt, samt även grupp av människor som sitter på ledande positioner politiskt och militärt. Påverkan med lyckat utfall på dessa kommer betyda att ett strategiskt syfte uppfylls vilket gör att kriget går snabbare att vinna. (Warden, 1995)

Ett exempel på ett sådant här agerande kan vara hacker-pseudonymen Oliver Tucket som genomförde en attack riktad mot den syriska regimen. Denna attack var riktad mot regimens servrar där Oliver Tucket fick tillgång till och kunde läsa e-posttrafik, dokument. Hackaren

omdirigerade även länkar på webbplatser i syfte att skapa misstro mot den syriska staten (Grohe, 2015, s. 138).

3.3.2 Organic essentials/System essentials

Inom informationskrigföring är påverkan viktigt. För att definiera det system inom en motståndare som är mest väsentligt för att information ska nå fram definierats *system essentials* som mediahus/medier. Detta på grund av att medier är den källa till information som kan påverkan på en befolkning eller en population. Definitionen gäller inte medier i det som kan betecknas som sociala medier utan som etablerade nyhetstidningar och nyhetsföretag/nyhetskoncerner. Detta då den journalistiska idén är att presentera nyheter med opartiskhet och objektivitet (American Press Institute, 2018).

Även storföretag med kundkrets stor som hela världen till exempel Google, Microsoft, Facebook och Instagram faller in under denna ring. Dessa företag är så pass stora med så pass stor källa till information om människor samt deras aktiviteter och mönster inom internet. Detta gör att de också räknas in i organic-/ system essentials på grund av att de är kritiska för användningen inom internet och det som kan påverka en individ med behov av att surfa nyheter eller streama film. Dessa företag är som elkraftverket i ett elnät. Påverkas något av dessa företag av blir det svårare för till exempel ledningen att leda inom informationsmiljön. Likaledes blir det svårare att kommunicera då infrastrukturen inte kan föra fram lasten med information.

3.3.3 Infrastructure

Infrastruktur i denna operationalisering av Wardens modell för informationskrigföring definieras i detta arbete som nätverksstrukturen. Det inom informationsflödet som inte är visualiserat utanför ett serverrum. Med nätverksstruktur menas den del inom ett informationsbärande nätverk som är av digital art och fysiska dataprodukter.

Påverkan mot en nätverksstruktur kan skada mer än bara en organisation eller företag utan även privatpersoner. Denna operationalisering syftar till att begränsa detta till att endast mäta påverkan mot nätverksstrukturer.

Exempel på en attack för detta är en DDoS-attack som avser överbelasta serverar så att de stängs ner. Med detta exempel blir infrastrukturen överbelastad vilket i sin tur gör att information inte kan lämna eller ankomma servrarna som blivit nedstängda.

3.3.4 Population

Befolkningen påverkas av olika intryck. Sociala medier får en större tyngdpunkt i informationskrigföring gentemot populationen i en stat. Enligt ovan nämnda Kalpokas så har sociala medier en stor påverkan på befolkningen när det gäller att se ett land som ett varumärke. I och med att sociala medier har en så pass stor påverkan att influera människor så blir operationaliseringen av denna ring att sociala medier är en del av ringen population/befolkningen.

Anledningen till att det inte faller in under någon annan ring är på grund av att befolkningen rör sig mest inom sociala medier. På detta vis blir det mätbara värdet av sociala medier dess användare. Visserligen finns statliga aktörer och organisationer också inom sociala medier men den stora massan av användare är civila personer.

En stat kan påverka en större massa av sin befolkning genom att ha personer som skriver propaganda eller ger ut falska nyheter via pseudonym eller flera pseudonymer. Ryssland har genom enskilda individer, som haft över 100st fiktiva online-personer, påverkat befolkningen med pro-rysk vinkling av information (Iasiello, 2017, s. 56).

3.3.5 Fielded military

Denna del i modellen blir mer subjektiv än vad Warden tidigare menar. För att få ett mätbart värde inom informationskrigföring måste denna handla mer om moral och social påverkan mer än kinetisk energi mot ett markbundet förband under framryckning.

Den subjektiva bedömningen kommer att avhandla om det sker en påverkan i moral, stridsvilja, eller vilseledning inom denna del av en krigsmakt. Moralen bland trupper kan påverkas av information som presenteras från främmande makt. Ett exempel på detta är propaganda som är riktad mot soldater eller mot en motståndares militära styrkor där meddelandet i dessa innehåller snedvridna citat från deras ledningen inom landet. Eller att det innehåller bilder på egna styrkor som ger upp eller skickar budskap om att ge upp.

3.3.6 Analysverktyg

För att möjliggöra en analys av empirin krävs det att ett analysverktyg används. Analysverktyget som kommer att användas i analysen består av att dela upp attackerna i hård respektive mjuk informationskrigföring. Detta analysverktyg tas fram för att skilja på två typer av genomförande av attacker inom informationskrigföringen. Detta för att visa att det finns skillnader inom informationskrigföringen samt att även få en tydligare förklaring för beteendet i hur en grupp som SEA agerar. De indikatorer som definieras för att få fram de som kan anses typiskt för denna undersökningen är hård- respektive mjuk informationskrigföring (Johannessen & Tufte, 2003, s. 45). Analysverktyget kommer under analysen underlätta att urskilja samt att sedermera förklara resultaten som inhämtats från empirin. Analysverktyget tas fram för att göra skillnad på subjektiv påverkan och dataintrång där system samt hårdvara påverkas.

Likt Iasiello (2017) som delar upp sin undersökning i *informational-technical* och *informational-psychological* ger detta att analysverktyget ger undersökningen mer validitet. Detta då Warden i sin teori vill uppnå systemkollaps genom kinetiskpåverkan på ringarna. Med denna uppdelning blir tolkningen av vad som kan uppbringa systemkollaps mer tydlig. Indikatorerna definieras enligt följande:

Hård informationskrigföring

Hård informationskrigföring definieras i detta analysverktyg som en attack där hårdvara och mjukvara påverkas i ett informationsbaserat system. Med påverkan menas att system utsätts för en kraftig överbelastning och på så vis inte kan lösa programmerad uppgift.

Mjuk informationskrigföring

Mjuk informationskrigföring definieras i analysverktyget som attacker riktade mot att skapa opinion, vilseledning samt annan typ av påverkan av individer i en stat.

4 Analys/Resultat

I nedanstående analys kommer begreppen som operationaliserats fram i kapitel 2 att utgöra ordningen i detta kapitel. Under vardera rubriken kommer empiri, analys och resultat att presenteras utifrån John Wardens fem-rings modell.

Detta kapitel kommer att avslutas med en diskussion om det som har presenterats. Detta för att på ett enkelt sätt presentera en valid bild av resultatet samt att öka reliabiliteten i arbetet innan slutsatserna presenteras i nästkommande kapitel.

4.1 Analys

Antalet incidenter som Syrian Electronic Army genomfört inom arbetets definition av informationskrigföring under perioden 2012–2014 är mer 30st (Valeriano & Maness, 2015, ss. 174-175). Utifrån dessa attacker kommer analysen att ske med hjälp av den operationaliseringen som genomförts av modellen. Gruppen sätter allt som oftast och en stämpel på attacken med sitt eget namn, eller för Syrien.

Ledning

Med en påverkansoperation år 2013 mot USA:s president Barack Obama twitterkonto ger SEA en tydlig indikation att påverka inom denna ring. Påverkansoperationen genomfördes så att en artikel om klimatet i själva verket omdirigerade läsaren till en video med pro-Assad budskap (Valeriano & Maness, 2015, s. 175).

Barack Obama som vid tillfället var USA:s president är i detta fallet en mycket ledande person utifrån lednings-ringen. En attack mot ledaren av den fria världens Twitterkonto kan ses som en aktion som kan komma att påverka en stor skara människor men även ekonomier och relationer mellan stater. Vidare finns det inte mer direkta ingångsvärden för att SEA har påverkat ledningsringen med en attack.

Denna attack mot ledningsringen definieras som mjuk informationskrigföring. Detta för att attacken innefattade budskap eller propaganda ämnad att stärka den syriska staten. Samtidigt som trovärdigheten hos den utsatte ledaren blir lägre.

Organic/system essentials

Vid flera tillfällen har SEA genomfört attacker mot mediekoncerner eller mediahus (Valeriano & Maness, 2015, ss. 174-175; Warren & Leitch, 2016, s. 209). Vid majoriteten av gångerna har SEA genomfört attacker med syfte att samla inloggningsuppgifter för att sedermera logga in och publicera falsk information eller meddelanden (Warren & Leitch, 2016, ss. 208-209).

9 september 2012 kapar SEA Al-Jazeeras Twitter konto. SEA publicerar en artikel om att Qatars premiärminister ska ha utsatts för mordförsök (Al-Rawi, 2014, s. 423; Valeriano & Maness, 2015, s. 175).

23 april 2013 genomförde SEA en attack mot mediahuset *Assosiated Press* (AP) och deras Twitter konto. Denna attack genomförs med att dela falska nyheter på AP:s om bombdåd och att den amerikanske presidenten har blivit skadad. (Valeriano & Maness, 2015, s. 176; Al-Rawi, 2014, s. 423).

27 augusti 2013 kapade SEA *New York Times* webbplats domän. Under kapningen av denna tidnings domän så blev besökare till sidan utsatta för propaganda. Både propaganda som var pro-Assad regimen samtidigt som anti-propaganda mot västvärlden. SEA lämnar även kvitto på att det är de som genomfört attacken (Valeriano & Maness, 2015, s. 177).

Även stora företag har drabbats av attacker från SEA. Microsoft utsattes för fyra stycken attacker under loppet av 20 dagar i januari 2014. Dessa attacker var då riktade mot att samla in information i form av bland annat inloggningsuppgifter. Perioden inleds med att både Microsoft och Skype attackeras för att skicka ut mail till användare om att sluta använda Microsoftprodukter. Senare går attackerna över till att inhämta information från anställda på Microsoft och från Microsofts interna system (Valeriano & Maness, 2015, s. 175).

Medier och sociala medier kan skapa en stor påverkan. SEA:s attacker på mediekoncerner samt deras tillhörande sociala medier visar på ett beteende av att skicka ut propaganda eller vilseledande information som skadar ledare eller högt uppsatta inom motståndaren värld.

SEA gav sig i stor utsträckning på just mediekoncerner, storföretag och sociala mediekoncerner (Valeriano & Maness, 2015, ss. 174-175; Warren & Leitch, 2016, s. 209).

Inom denna ring blir det mer diffust att se om attackerna är enbart hård eller mjuk informationskrigföring. Ett mönster som kan antydas är de attacker mot sociala medier också innefattar både hård och mjuk informationskrigföring. Först gör gruppen intrång i datasystemen hos sociala medieföretag för att sedan kapa konton hos mediekoncerner för publikation av desinformation och propaganda. Samtidigt blir mediaföretagen utsatta för mer mjuka attacker medans de företagen inom sociala medier och programutveckling blir utsatta för attacker med hård karaktär. Det är dock inte uteslutande hård informationskrigföring som sker mot dessa företag. Attacker av mjuk definition sker också. Vid attacker där desinformation och vilseledning sänds ut som nyheter så visar inte dessa inlägg på att de är en påverkan på kontot som skett. Till skillnad från när sociala mediakonton tas över eller deras hemsidor stängs ned då visar SEA att de varit på plats och orsakat skadan.

Infrastructure

Med Wardens tankar om att infrastrukturen är en känslig del av en motståndares system. Arbetar SEA med att genomföra attacker med syfte att även stänga ner internetsidorna för dessa företag och media mediahus som omnämndes tidigare i organic-/system essentialls. Den typiska funktionen som SEA då använder är DDoS attacker (Grohe, 2015, s. 135).[2] På detta sätt påverkar SEA infrastrukturen inom internet och även inom de fysiska servrarna.

Inom denna ring är det enbart hård informationskrigföring som sker. I och med att hård informationskrigföring definieras som påverkan mot hårdvara och mjukvara som skapar överbelastning. Samtidigt så blir ringen infrastructure väldigt snäv då den i sitt syfte utgör tolkningen av hård informationskrigföring. SEA visar även via sina sociala medier att de genomfört attacker på ett sådant här sätt. På så vis hävdar de att de har en förmåga att stänga ner webbplatser etc.

[2] Distributed Denial of Service (DDoS) attacker genomförs med hjälp av flera datorer samtidigt för att skapa en överbelastning på den server som önskad webbplats eller system finns.

Population

Mot populationen, eller befolkningen, är det en mer subjektiv analys. Den indirekta påverkan som kan ske genom att publicera falska nyheter, vilseledning med att länkar omdirigeras och propaganda är svårt att greppa. Det blir dock uppenbart att SEA med sina operationer försöker påverka en befolkning då de tydligt genomför attacker mot media för att skapa opinion eller desinformation. Ett exempel på detta med desinformation är de två nyheter som SEA publicerade dels om attacken på Vita Huset och Barack Obama samt nyheten mordförsöket mot Qatars premiärminister (Al-Rawi, 2014, s. 423). Ett exempel på propaganda är när SEA övertar hemsidor för medier eller omdirigering av länkar (Valeriano & Maness, 2015, s. 177). Med sina operationer och attacker i media försöker SEA att göra två saker samtidigt. Dels påverka motståndarens befolkning eller den inhemska befolkningen samtidigt som berörd media blir påverkad.

Påverkan på denna ring sker genom mjuk informationskrigföring. Med desinformation och regimvänlig propaganda försöker SEA uppnå påverkan på motståndarens population. Det är den psykologiska påverkan som ligger i tyngd i denna. Dock finns ju antydan till att hård påverkan sker. Detta genom att social mediers hemsidor och funktioner stängs ned. Men om nedstängning av sociala medier påverkar en befolkning i att det ger systemkollaps är väldigt svårbedömt. I dessa attacker framgår det inte heller att det är SEA som är källan. Detta är troligen för att informationen ska få mer genomslagskraft.

Fielded Military

Den 2 september 2013 genomförde SEA en attack riktad mot den amerikanska marinkåren, US Marine Corp (Valeriano & Maness, 2015, s. 175). Attacken skedde mot marinkårens rekryteringsida och visade demoraliserande budskap för den som gick in på sidan. Meddelandet var riktat mot soldater eller de som ville bli soldater. Meddelandet syftar till att man amerikansk soldat skickas in i döden i ett annat land och politikerna vet om att soldaterna kommer dö och är undertecknat med SEA emblem (Robertson, 2013).

Med detta moralsänkande meddelande blir denna attack mjuk informationskrigföring. I och med att de inte finns tecken på att systemet har skadats utan att sidan enbart blivit övertagen

för att skicka demoraliserande propaganda till den amerikanska marinkårens soldater och eventuella nya rekryter.

Parallella attacker

De attacker som kan räknas som parallella attacker som genomförts av SEA är de attacker som genomförts den 23 augusti 2013. New York Times utsätts för en DDoS-attack som gör att deras hemsida ligger nere i flera timmar. Samma dag genomförs en attack mot Twitter där SEA kommer in på DNS-servern vilket gör att de har möjligheten att lägga upp meddelande på olika högprofilerade konton (Valeriano & Maness, 2015, s. 174).

Parallella attacker innehåller både mjuk och hård informationskrigföring. Dock finns det endast ett exempel på en samtidig attack baserat på datum. Exemplet ovan genom för SEA attack för att stänga ner hemsidan för NY Times. Parallellt med denna attack sker en attack mot twitter och NY Times twitter-konto. Attacken kan då tolkas som att gruppen vill strypa en stor informationspipeline för att göra sin propaganda mer effektiv genom att styra populationen till att läsa nyheter som gruppen släpper via sociala medier i vilseledningssyfte.

4.2 Sammanfattning

Tabellen nedan visar en kortfattad sammanfattning av analysresultaten. Detta görs för att anknyta till analysen lättare vid genomgång av analysdiskussionen i kommande punkt 4.3.

Ring	*Hård informationskrigföring*	*Mjuk informationskrigföring*
Ledning		Propaganda som sänds ut via en manipulerad länk på Barack Obamas Twitter-konto.
Organic/system essentialls	Intrång och överbelastningsattacker mot mediekoncerners hemsidor.	Desinformation som skickar ut via mediers sociala mediakonton.
Infrastructure	Överbelastningsattacker mot sociala medier företag.	
Population		Desinformation, vilseledning och propaganda riktad mot befolkningen.
Fielded military		Demoraliserande budskap och desinformation riktad mot motståndarens väpnade styrkor.
Parallella attacker	DDoS attack för överbelastning och nedstängning	Övertagning av konton på social medier för att kunna skicka desinfomation eller propaganda via andras konton.

Tabell 2. Sammanfattning av analysen

4.3 Diskussion

Det utmärkande i analysen utifrån analysverktyget med hård respektive mjuk informationskrigföring blir att användningen av mjuk informationskrigföring är mer frekvent än hård. Huvuddelen av Syrian Electronic Armys attacker utförs för att skapa någon typ av opinion eller spridning av propaganda för Syriens fördel. Användningen av nyhetsföretags sociala medier för att skicka ut desinformation om ledande figurer är ett tecken. Till exempel nyheter om attacken mot vita huset. Samtidigt är det den pro-Assad och anti-västerländska propagandan som delas ut inom sociala medier.

Sambandet mellan de olika ringarna är inte speciellt starkt. Det finns ingen tydlig relevans eller koppling i analysens resultat att säga att samtliga ringar förklarar SEAs beteende av attacker. Attackerna är primärt riktade mot västerländsk media för att skapa pro-syrisk opinion. Det ringar som förklarar gruppen beteende mest är *organic/system essentialls* samt *infrastructure* ringarna. En eventuell förklaring till detta kan vara den tekniska sammankopplingen. Med attacker mot mediekoncerner eller nyhetsföretag konton på sociala medier så blir även de stora företagen drabbade. För att få åtkomst till en specifik tidnings twitter-konto kan en sådan här grupp lika gärna göra skada mot företaget Twitter samtidigt som de för ut sitt budskap genom kapning av ett nyhetskonto.

Utifrån Wardens teori så vill han med center of gravity och parallella attacker mot motståndarens system orsaka systemkollaps för att vinna kriget. Med detta beteende som SEA uppvisar med att mestadels genomföra attacker med mjuk informationskrigföring så blir det svårt att uppnå någon form av systemkollaps. SEA har inte attackerat statliga mål utan riktar in sig på den mjuka informationskrigföringen. Med detta i åtanke blir det mer tydligt att Wardens teori lämpligen kan förklara hur mjuk informationskrigföring kan motverkas.

Kopplat till analysen i helhet och analysverktyget så blir det tydligare att *center of gravity* inom informationskrigföring hamnar mer i ringen organic/system essentials. En stor del av attackerna riktar sig specifikt mot mediekoncerner och nyhetsbolag. Kontroll av media blir viktigaste tyngdpunkten i en modell inom informationskrigföring. Likaledes är det inget i SEA beteende som visar på att de genomför parallella attacker. Det har skett en gång enligt den

empiri som undersökts. Detta kan samtidigt ställa frågan varför de inte genomför parallella attacker? Är det på grund av brist på resurser eller på grund av strategiska val?

5 Avslutning

I detta kapitel kommer svaret på forskningsfrågan att presenteras. Det kommer även presenteras slutsatser utifrån resultaten. Därefter presenteras förslag på vidare forskning. Efter presentationen av slutsatserna kring resultatet och vidare forskning presenteras en diskussion om undersökningens, och dess resultat, relevans till krigsvetenskapen och officersprofessionen. Här kommer även en diskussion kring etik om detta ämne kopplat till officersprofessionen. Detta för att etiken inom officersprofessionens är viktig att förhålla sig till då professionsetiska val kan påverka så många människor. Slutligen i detta kapitel kommer reflektioner kring arbetets genomförande att presenteras.

5.1 Slutsats

En enfallsstudie av Syrian Electronic Army har i detta arbete presenterats utifrån en analys med John Wardens fem-rings modell för att analysera gruppens beteende inom informationskrigföringen. Gruppen SEA är en grupp som går att länka till en regim men hävdar själva att de är autonoma. Detta för att besvara frågeställningen.

Hur kan attacker som genomförts av Syrian Electronic Army förklara deras beteende med hjälp av en analys med Wardens fem-rings modell?

Det beteende som gruppen SEA framställer genom sina attacker är att, utifrån Wardens fem-rings modell, främst fokusera på utförandet av propagandaattacker mot etablerade västerländska mediaföretag och nyhetsbyråer. På grund av resultaten i analysen så finns det tecken på att SEA lägger fokus på att göra propagandakampanjer för att stärka Assad-regimens status inom och utom landet. Ringen Organic/system essentials är den ring som blir tyngdpunkten i SEAs attacker. Attacker sker mestadels mot mediekoncerner och nyhetsbolag. Attackerna är ämnade för att skapa opinion fördelaktig för Syrien.

Med grupper som hävdar autonomi men med hög sannolikhet inte kan motsäga sig att den styrs från en stat, i detta fall SEA, så finns det tecken på att just media ligger i fokus. Hur detta kommer säg är svårt att sia om. I och med att det inte finns konkreta bevis om direkta kopplingar mellan SEA och Syrien. Men det kan hävdas att det finns relevans i denna undersökning.

5.2 Diskussion

Nedan kommer en diskussion kring koppling mellan resultatet och teoretiskramverk samt studiens valda metod att genomföras. Detta för att tydliga och sammanfatta stringensen i arbetet.

5.2.1 Teori

Wardens ursprungliga teori avser vinna kriget snabbt och effektivt med kinetisk påverkan och effekt. För att förklara informationskrigföring bättre måste teorin tänkas om. Utifrån analysen i detta arbete går det att se tendenser inom mjuk informationskrigföring att center of gravity ligger mot ringen som är kopplat till vitala funktioner. Organic/system essentials är i detta arbete den ring som det flest attacker emot.

Med den tidigare forskningen i åtanke med attackbaserade analyser som kunskapslyftande för den defensiva förmågan, (Bishop & Goldman, 2003), kan följande påstås. Mediekoncerner samt företag inom sociala medier är de uppenbara målen vid genomförande at mjuk informationskrigföring. Samtidigt som mjuk informationskrigföring är huvudsyftet med en operation kan ett ytterligare syfte vara att göra skada med hård inriktning. Detta för att på så vis skada både mediekoncernens och sociala medieföretagets anseende utåt. Genom att använda Wardens teori i detta arbete kan en förståelse till vad som krävs för att upprätta ett lämpligt försvar ligga till grund.

5.2.2 Metod

Med en fallstudie på hackergrupper inom informationskrigföring har varit gynnsamt i fallet SEA. Det svåra med att genomföra fallstudier i liknande fall kan vara den brist på aktiv självidentifiering från grupper som genomfört attacker. SEA har ett mönster av att lämna tydligt att det som har skett kommer från SEA. Användning av en kvalitativ studie i form av textanalys är samtidigt bra att föredra för en sådan här studie. Med det material som finns tillgängligt med tanke på internets storhet och svårigheter så är det viktigt med textens mening än mot att använda en mer kvantitativ ansats.

5.3 Relevans till officersprofessionen

En försvarsmakt måste ha ständig fokus på att utveckla sina egna försvar mot informationsattacker. Med den breda definitionen av informationskrigföring som grund så är det en stor massa av mindre egenskaper en försvarsmakt måste ha stor kompetens inom. Genom att pre-

sentera denna studie så blir bilden av hur mindre nationer arbetar inom informationskrigföringen.

Med resultatet i hand om att SEA fokuserar sina attacker mot medier för att sprida propaganda är det viktigt att ha ett arbete mot att utbilda en befolkning till att vara källkritisk. Detta för att individer inte ska fastna vid att saker som står på internet omedelbart är sanning. Det svåra i detta är att en nation inte bör, eller ska, genomföra informationskrigföring mot sin egna befolkning för att minska risken för hot. I och med att internet, till stor del, är en öppen yta så är det mer meningsfullt att utbilda än att aktivt skydda genom att stänga ner och låsa ute människor från internets värld. I och med att beteendet hos en grupp som SEA är riktad mot medier så kan det bli ett etiskt felsteg att tillintetgöra tillgången till medier.

> *Kort sagt är de flesta underrättelser osanna och människans rädsla blir till ny kraft för lögner och osanningar. I regel är de flesta benägna att hellre förlita sig till det negativa än till det positiva. Var och en är böjd att förstora det ogynnsamma. De faror som rapporteras minskar ofta snart likt vågorna i havet, men i likhet med dessa kommer de alltid igen utan påtagligt skäl. Befälhavaren måste då förlita sig på sitt omdöme och stå fast som en klippa mot vilken vågorna bryts. Men det är ingen lätt uppgift. (von Clausewitz, 1991, s. 77)*

5.4 Vidare forskning

För att förstå grupper som SEA djupare måste det ske andra typer av studier där deras beteende studeras. Lösa kopplingar mellan stater och autonoma aktörer inom informationsarenan kan på så sätt vidare förklaras. Strategier inom informationskrigföring behöver inte vara grundande i klassiska teori. Förklaringar till detta kan i sin tur leda till en snabbare utveckling av ett försvar mot attacker inom informationskrigföring som genomförs av liknande grupper samt strategiska utvecklingar. Frågor som efter detta arbete uppstått är: Var dras gränsen för autonom kontra statlig hacktivsmgrupp? På vilket sätt kan Wardens teori utveckla informationskrigföringsstrategi?

Samtidigt tidigt vore det önskvärt att flera fall inom informationskrigföring undersöks och analyseras utifrån Wardens teori. Detta då Wardens teori definierar motståndarens som sy-

stem av system. I och med detta gör det att teori får en stor bredd i vad som kan innefatta dess olika delar.

5.5 Reflektion

Under arbetet har det blivit svårt att genomföra en mer utförlig analys av informationskrigföringen som SEA genomförde under perioden 2011–2014. Detta då källor som författare till artiklar har använd inte längre existerar på grund av olika policyöverträdelser som uppstått i sociala medier. Detta kan härledas till att dessa sociala medier är västerländska företag med olika intressen som gör att innehåll snabbt försvinner som inte håller måttet enligt västerländsk standard. Ett exempel på detta är det videoklipp som tas upp i analysen om Barack Obamas twitterkonto under Ledningsringen. Vid kontroll av denna länk för att se vad denna propagandavideo innehöll för budskap meddelar Youtube att innehållet tagits bort på grund av att videon strider mot deras policy om våld och våldsamt innehåll.[3]

Svårigheterna med att forska inom ett ämne som informationskrigföring är just att saker som är ämnade att skapa, av omvärlden, felaktig opinion allt som oftast tas bort. Detta kan göra att grupper som SEA möjligen fortsatt kan sända budskap men att de tas bort. Men bara för att de tas bort betyder inte det att skada inte har uppstått.

[3] Propagandavideons youtube-länk : https://www.youtube.com/watch?v=kN2kHth_tFw&feature=youtu.be (hämtad 2018-05-05)

6 Litteraturförteckning

Abboud, S. N. (2016). *Syria.* Cambridge, UK ; Malden, MA: Polity Press.

Al-Rawi, A. K. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review, Vol. 40*(3), 420-428.

American Press Institute. (den 16 April 2018). *What is the purpose of journalism?* Hämtat från American Press Institute: https://www.americanpressinstitute.org/journalism-essentials/what-is-journalism/purpose-journalism/

Bergström, G., & Boréus, K. (2005). *Textens mening och makt* (Andra upplagan uppl.). Lund: Studentlitteratur.

Bertram, S. K. (2017). 'Close Enough - The link between the Syrian Electronic Army and the Bashar al-Assad regime, and implications for the future development of nation-state cyber counter-insurgency strategies'. *Journal of Terrorism Research, Vol. 8*(1), 2-17.

Bishop, M., & Goldman, E. (2003). The Strategy and Tactics of Information Warfare. *Contemporary Security Policy, 24*(1), 113-139.

Blank, S. (2013). Russian Information Warfare as Domestic Counterinsurgency. *American Foreign Policy Interests, 35*, 31-44.

Boyd-Barrett, O. (2017). Ukraine, Mainstream Media and Conflict. *Journalism Studies,, 18*(8), 1016-1034.

Chong, A. (2014). Information Warfare? The Case for an Asian Perspective on Information Operations. *Armed Forces & Society, Vol. 40*(4), 599-624.

Esaiasson, P., Gilljam, M., Oscarsson, H., Town, A., & Wängnerud, L. (2017). *Metodpraktikan* (5 uppl.). Stockholm: Wolters Kluwer.

George, A. L., & Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences.* Cambridge, MA: MIT Press.

Grohe, E. (2015). The Cyber Dimensions of the Syrian Civil War: Implications for Future Conflict. *Comparative Strategy, Vol. 34*(2), 133-148.

Iasiello, E. J. (2017). Russia's Improved Information Operations: From Georgia to Crimea. *Parameters, 47*(2), 51-63.

Inkster, N. (2016). Information Warfare and the US Presidential Election. *Survival, 58*(5), 23-32.

Johannessen, A., & Tufte, P. (2003). *Introduktion till samhällsvetensskaplig metod.* Malmö: Liber AB.

Kalpokas, I. (2017). Information Warfare on Social Media: A Brand Management Perspective. *Baltic Journal of Law & Politics, Vol. 10*(1), 35-62.

Libicki, M. C. (1996). *What Is Information Warfare* (3 uppl.). Washington: National Defense University.

Nationalencyklopedin. (2018). *autonom*. Hämtat från Nationalencyklopedin: http://www.ne.se/uppslagsverk/encyklopedi/lång/autonom den 16 April 2018

Nationalencyklopedin. (2018). *Källkritik*. Hämtat från Nationalencyklopedin: http://www.ne.se/uppslagsverk/encyklopedi/lång/källkritik den 16 April 2018

Robertson, A. (den 2 September 2013). Syrian Electronic Army hacks recruiting site, tells Marines to refuse orders from 'traitor' Obama. *The Verge*. Hämtat från https://www.theverge.com/2013/9/2/4686848/syrian-electronic-army-hacks-marines-recruiting-site den 25 April 2018

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security, 49*, 70-94.

Sundberg, M. (den 28 Februari 2018). *Säpo varnar för utländsk påverkan i riksdagsvalet.* Hämtat från SVT Nyheter: https://www.svt.se/nyheter/inrikes/sapo-varnar-for-utlandsk-paverkan-i-riksdagsvalet den 19 April 2018

Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities: Cyber Conflict in the International System.* New York: Oxford Scholarship Online.

Warden, J. A. (1995). The Enemy as a System. *Airpower Journal, Vol. 9*(1), 40-55.

Warden, J. A. (2000). *The Air Campaign.* Lincoln, NE: toExcel Press.

Warren, M., & Leitch, S. (2016). The Syrian Electronic Army - a hacktivist group. *Journal of Information, Communication and Ethics in Society, Vol.14*(2), 200-212.

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections: The Quarterly Journal, 15*(2), 73-87.

von Clausewitz, C. (1991). *Om kriget* (3 uppl.). (H. Mårtensson, K.-R. Böhme, & A. W. Johansson, Övers.) Stockholm: Bonnier Fakta Bokförlag AB.