Självständigt arbete (15 HP)

Författare		**Program/Kurs**
Tom Andersson		OP SA 13-16
Handledare		**Antal ord: 11980**
Sofia Ledberg	**Beteckning**	**Kurskod**
		1OP303

HAR RYSSLANDS NYTTJANDE AV INFORMATIONSKRIGFÖRING FÖRÄNDRATS MELLAN 1999-2014?

ABSTRACT:

The absence of previous research regarding Russia´s use of information warfare has not been able to show if there has been a new way of adapting information warfare alongside the development in the warfare in general. The previous research has established a development in warfare by the means of information technology. This is important to understand as it constitutes an equalizer between small states and great powers in the global arena. At the same time, it is even more important to understand that the development of Russian behavior has implications on warfare in a global perspective. The purpose of this thesis is to contribute to the conclusions of previous research which predicted a transformation in the warfare and give a new view of the transformation by inspecting Russia´s use of information warfare in modern warfare and probe if there has been a change. Additional purpose of this study is to understand Russia´s way of conduct in modern conflicts and have a better ability of control in forthcoming conflicts. The method used reflects the qualitative case and is constructed as a one-case study with variation in time, using three different conflicts. The analysis is conducted by the means of operational indicators extracted from Libickis theory. The result of the study shows that Russia have changed their way of using information warfare in between all of the three conflicts, and it is not that easy to say that the use of information warfare has changed. It might depend on the situation or the opposite side and how the individual conflict occur. There is no clear answer on that question, but this essay gives a deeper view in the use of information warfare by Russia in modern conflicts.

Nyckelord:

Informationskrigföring, hybridkrigföring, Ryssland, Libicki, Andra Tjetjenienkriget, Georgien, Krimkrisen

Innehållsförteckning

1. INLEDNING 5

1.1 INLEDNING 5
1.2 BAKGRUND 6
1.3 PROBLEMFORMULERING 7
1.4 SYFTE & FRÅGESTÄLLNING 7
1.5 MATERIAL 8
1.6 DISPOSITION 8
1.7 TIDIGARE FORSKNING 9

2. TEORI 12

2.1 INLEDNING 12
2.2 INFORMATIONSKRIGFÖRING 12
2.3 TEORI SOM VERKTYG FÖR ANALYSEN 15

3. METOD 16

3.1 INLEDNING 16
3.2 FALLSTUDIE 16
3.3 KVALITATIV TEXTANALYS 17
3.4 KÄLLKRITIK 18
3.5 OPERATIONALISERING 20
3.6 EMPIRI 22

4. ANALYS 22

4.1 ANDRA TJETJENIENKRIGET 1999-2001 23
4.1.1 C2W 23
4.1.2 Psycological warfare 24
4.1.3 Electronic warfare 25
4.1.4 Hacker warfare 25
4.1.5 Economic information warfare 25
4.1.6 Intelligence based warfare 25
4.2 GEORGIEN 2008 25
4.2.1 C2W 26
4.2.2 Psycological warfare 26
4.2.3 Electronic warfare 27
4.2.4 Hacker warfare 28
4.2.5 Economic information warfare 28
4.2.6 Intelligence based warfare 28
4.3 KRIMKRISEN 2014 29
4.3.1 C2W 29
4.3.2 Psycological warfare 29
4.3.3 Electronic warfare 31
4.3.4 Hacker warfare 31
4.3.5 Economic information warfare 31
4.3.6 Intelligence based warfare 31
4.4 JÄMFÖRELSE MELLAN FALLEN, NÅGON FÖRÄNDRING? 31
4.4.1 Command and control warfare 31
4.4.2 Psycological warfare 32
4.4.3 Electronic warfare 33
4.4.4 Hacker warfare 33

4.4.5 Economic based warfare *33*
4.4.6 Intelligence based warfare *33*
5. AVSLUTNING 34
5.1 SVAR PÅ FRÅGESTÄLLNING 34
5.2 RESULTAT OCH SLUTSATSER 34
5.3 DISKUSSION 36
5.3.1 Teori *36*
5.3.2 Metod och material *36*
5.3.3 Återkoppling till tidigare forskning *37*
5.3.4 Forskningens betydelse för yrkesutövningen *37*
5.4 FORTSATT FORSKNING 38
5.5 SLUTORD 38
6. LITTERATURFÖRTECKNING 39

1. Inledning

1.1 Inledning

> Those who master the techniques of information warfare will therefore find themselves at an advantage over those who have not; indeed, information warfare will, in and of itself, relegate other, more traditional and conventional forms of warfare to the sidelines. [1]
>
> - Martin C. Libicki

Informationskrigföringen har blivit en allt mer viktig del att behärska inom senare konflikter, något som Ryssland identifierade efter Gulfkriget, 1991.[2] Informationskrig visade sig bidra med ytterligare en dimension till krigföringen, vilket utgjorde en utjämnare mellan små och stora aktörer. Genom att bäst behärska informationskrigföringen kunde nu små stater utmana stormakter, som till exempel Ryssland. Detta är något som har medfört att Ryssland har lagt kraft på att utveckla sin förmåga att bedriva krigföring mer än bara genom kinetisk verkan och tidigare forskning pekar åt att en förändring inom deras användande av informationskrigföring har skett. Dock saknas det fortfarande systematisk forskning inom ämnet som fastslagit om detta verkligen skett.

Arbetet utgör därför ett bidrag till det givna forskningsläget genom att systematiskt genomföra en undersökning på Rysslands nyttjande av informationskrigföring inom de 15 senaste årens konflikter för att beskriva och öka förståelsen kring Rysslands agerande. Då Ryssland utgör en kraftig aktör på den globala marknaden skulle en förändring i deras agerande möjligen leda till att krigföringen i sin helhet förändras.

Martin C. Libicki, forskare vid *Rand Corporation* menar att tidigare definitioner som försökt förklara informationskrigföring, tenderar att vara vida. Därav blir det komplicerat att upptäcka en gemensam begreppstråd annat än den uppenbara.[3] Libicki presenterar i sin teori sju former av informationskrigföring som är command and control warfare, intelligence based warfare,

[1] Libicki 1995. Sidan ix
[2] Ventre 2009. Sidan xvii
[3] Libicki 1995. Sidan 3-4

electronic warfare, psychological warfare, hacker warfare, economic information warfare och cyberwarfare, vilket han menar att denna typ av krigföring kan förstås utifrån.[4]

Betydelsen för denna undersökning ökar även genom den separation som uppstått mellan västvärlden och Ryssland, där flertalet länder kan tänkas hamna i konflikt med Ryssland och därav har ett behov av att förstå sig på deras agerande för att om möjligt skydda sig emot liknande attacker eller till och med lyckas undvika dessa situationer.

1.2 Bakgrund

Informationskrigföring är inget nytt begrepp. Dess historia sträcker sig långt bak i tiden, där ett exempel är från 1100-talet där mongolerna nyttjade detta, dock utan någon teknologisk utrustning.[5] Stora förändringar har givetvis skett fram till idag, vilket de teknologiska hjälpmedlen är ett tydligt exempel på. Libicki menar att informationssystem blir allt viktigare i dagens konflikter, dock utgör inte information ett eget medium av krigföringen, utan en ytterligare dimension.[6]

Överste Chekinov och generallöjtnant Bogdanov beskriver att framtida krig inte kommer att likna tidigare krig, eller krig som nyligen pågått.[7] Samtidigt beskriver Rod Thornton förändringen av den moderna krigföringen där hybridkrigföringen utgör en betydande roll.[8] Informationskrigföringen utgör en del inom hybridkrigföringen vilket därför kan antas ha förändrats i samband med en förändring inom hybridkrigföringen. Forskning tyder på en förändring inom krigföringen, dock saknas en forskning som beskriver om och i sådana fall hur informationskrigföringen har förändrats, vilket denna undersökning syftar ge en bredare förståelse för.

Även samhället gör sig allt mer beroende av informationssystem och tekniska hjälpmedel ökar sårbarheten av eventuella attacker. Om en förståelse för den tidigare utvecklingen av informationskrigföringens nyttjande finns, ökar sannolikheten att undvika eller skydda samhället mot dessa typer av attacker. [9]

[4] Se 2. Teori. Sidan 12
[5] Friman, et al 1996 Sidan 3
[6] Libicki, 1995. Sidan xi
[7] Chekinov och Bogdanov 2013. Sidan 12
[8] Thornton 2015. Sidan 40-48
[9] Ventre, 2009. Sidan xvii

1.3 Problemformulering

Forskning inom krigföringens utveckling har visat sig otillräcklig att beskriva om en förändring skett i nyttjandet av informationskrigföring.[10] För att undersöka om en förändring har skett inom nyttjandet av informationskrigföring riktas detta arbete till Rysslands agerande inom moderna konflikter. Varför Ryssland blir en intressant aktör att undersöka beror på landets flertaliga inblandning inom moderna konflikter, samt att deras krigföring blivit beskriven genom hybridkrigföringen och nya generationens krigföring.[11] Utöver detta har även en separation mellan Ryssland och västvärlden uppstått på grund av Rysslands aggressiva agerande.

Då Ryssland är en stor global aktör kan deras agerande förändra krigföringen generellt och därav uppenbarar sig ett behov att förstå om och hur deras agerande förändrats. Då tidigare forskning ej genomfört systematiska undersökningar på detta nya sätt att föra krig, informationskrigföring, finns ett behov att öka förståelsen för en eventuell förändring inom krigföringen. Det finns anledning att förutsätta en förändring inom krigföringen då utvecklingen och anpassning till informationssamhället ökat i dagsläget.

1.4 Syfte & Frågeställning

Syftet med detta arbete är att undersöka om en förändring i Rysslands nyttjande av informationskrigföring skett mellan åren 1999 till 2014. Arbetet skall genom denna undersökning bidra med en djupare förståelse kring Rysslands agerande i moderna konflikter och därmed bidra till en ökad förståelse för utvecklingen av krigföringen. Detta är en viktig del att förstå då tidigare forskning inom ämnet menar att det nya kriget förändrar krigföringen i stort var Ryssland utgör en vital aktör. För att besvara nedanstående frågeställning har tre stycken nedslag i tid gjorts vid; Andra Tjetjenienkriget, Georgienkriget och Krimkrisen.

Det är idag oklart hur dagens konflikter skiljer sig från gårdagens konflikter, däribland hur informationskrigföring användes. För att lyckas bringa klarhet i detta har författaren valt att utgå från ett teoretiskt ramverk och genom att studera Ryssland, där ett nedslag i tid har gjorts vid de tre största konflikterna de senaste 15 åren.
För att bidra med ett svar till denna fråga har författare valt att svara på hur tidigare informationskrigföring skiljer sig från senare genom att använda Libickis definition av informations-

[10] Se 1.7 Tidigare forskning. Sidan 9
[11] Ibid

krigföring vilken består av sju former.[12] Arbetets teoretiska ramverk utgörs av Martin Libickis sju former av informationskrigföring, då teorin är framtagen i syfte att definiera ett tidigare svårdefinierat område, informationskrigföring.[13]

Följande frågeställningar kommer utgöra grund för arbetet:

- Har Rysslands nyttjande av informationskrigföring förändrats, och i sådana fall hur har den förändrats?

1.5 Material

Inriktningen för undersökningen är att materialet främst skall utgöras av förstahandskällor dock kommer andrahandskällor att användas för att komplettera eftersom förstahandskällor inte räcker till, då dessa i vissa hänseende endast finns i en limiterad utsträckning. På grund av författarens språkkunskaper är det använda materialet endast skrivet på svenska och engelska.

1.6 Disposition

I kapitel ett redogörs det aktuella problemet som undersökningen kommer att behandla, varpå en lucka i det aktuella forskningsläget beskrivs och motiverar detta arbete dels utifrån tidigare forskning och dels utifrån de frågeställningar som framställs i kapitlet. I kapitel två beskrivs den teori som används som det teoretiska ramverk vilket undersökningen använder för att genomföra den senare analysen utifrån. I kapitel tre beskrivs den använda metoden i arbetet med motivering varför just denna metod lämpar sig väl för arbetet och vilka eventuella risker detta kan medföra i undersökningen. En redogörelse för operationaliseringen beskrivs, vilken syftar att tydliggöra på vilket sätt författaren genomför analysen. I kapitel fyra följer analysen av analysenheterna utefter tidigare beskriven metod och teori. Detta syftar till att leda fram till svar på undersökningens forskningsfråga. I kapitel fem summeras undersökningen genom svar på forskningsfrågorna, en slutdiskussion om varför det blivna resultatet blev som det blev och orsaker som kan ha en betydande roll. Ytterligare ger författaren en reflektion kring arbetet och förslag på vidare forskning, för att till sist ge avslutande ord för undersökningen. I kapitel sex återfinns all litteratur som använts i undersökningen.

[12] Se 2. Teori. sidan 12
[13] Libiciki 1995. Sidan xii

1.7 Tidigare forskning

Denna undersökning bidrar till tidigare forskningsläge med en systematisk undersökning om och hur nyttjandet av informationskrigföring har förändrats av Ryssland under de stora konflikter de varit inblandad i sedan informationskrigföringen fick ett uppsving igen, 1991, i samband med Gulfkriget. Givet tidigare forskningsläge finns en avsaknad kring just systematiska undersökningar inom förändringen av informationskrigföring vilket då gör denna undersökning betydelsefull för forskningsläget.

Rod Thornton menar att förändringen av den moderna krigföringen spelar en viktig roll för att behärska slagfältet, där hybridkrigföringen utgör en del. Rysslands agerande använder hybridkrigföring som ett verktyg inom konflikter de medverkar i, dock återfinns ingen tidigare forskning som studerat Rysslands förändring vilket är av betydelse för att förstå sig på hur Ryssland agerar. Den som använder hybridkrigföringen bäst vinner kriget eller konflikten menar Thornton. Denna forskning håller sig generell och övergripande, vilket ej ger en djupare förståelse för ett specifikt agerande som till exempel hur Ryssland agerar genom informationskrigföring.[14]

Galeotti menar att tyngdpunkten i Rysslands krigföring inom moderna konflikter är användandet av informationskrigföringen. Verktyget beskrivs bland annat som det nya sättet att föra krig på, varför också denna undersökning lämpar sig väl att beskriva en förändring i Rysslands agerande då framtida konflikter gör sig viktiga att förstå sig på. Får man klart för sig hur Rysslands utveckling sett ut skapas förutsättning att manövrera kommande konflikter. Galeotti tyder på en utveckling inom krigföringen, dock gör sig inte hans forskning fullständig i att beskriva denna förändring. Informationskrigföringsmetoden har enligt honom funnits med under en längre tid och att det istället är sammanhanget som dessa applicerats på som är det nya. Författaren för denna undersökning anser att det finns dåliga belägg för detta och beskriver inom undersökningen en förändring i brukandet av informationskrigföring. Galeotti berör även det nya kriget vilket är mer komplext än tidigare reguljära krig, där informationsteknologin utgör en utmaning inom de nya konflikterna.[15]

[14] Thornton 2015. Sidan 40-48
[15] Galeotti, 2016. Sidan 282-301

Överste Chekinov och generallöjtnant Bogdanov påstår att framtida krig inte kommer att likna tidigare krig eller krig som nyligen ägt rum. De menar att en utveckling inom krigföringen kommer att särskilja krigens utformning främst genom den fortsatta utvecklingen för de teknologiska hjälpmedelena. De menar att den nya generationens krigföring kommer att domineras av informations- och psykologisk krigföring mer än tidigare. [16]

En utveckling kan även tydas från Frank Hoffman, han menar att hybridkrigföringen bidrar till en förändring i krigföringen, utan att detta för den delen skulle betyda att den konventionella, och i vissa avseende traditionella krigföringens tid är över. Detta utgör istället en ytterligare dimension till krigföringen och tillför en komplexitet. Utvecklingen är något som går att tydas om än ej så inriktad på informationskrigföring utan mer i dess större sammanhang, hybridkrigföring.[17]

Även den tekniska utvecklingen har bidragit till en förändring inom krigföringen. En vital fråga är just hur man skall nyttja informationsteknologiska hjälpmedel för att få ett övertag över sin motståndare. Daniel Ventre nämner även att informationskrigföringen fick ett uppsving och ökad betydelse efter Gulfkriget, 1991, där Ryssland identifierade USA:s framgång genom användningen av teknologiska informationssystem mot Irak. Detta kan ha lett till en förändring i Rysslands brukande av informationskrigföring, vilket vi idag kan se till skillnad från tidigare konflikter.[18] Kriget har beskrivits förändrats från att gälla att ta motståndarens territorium till att neutralisera dennes militära och ekonomiska potential.[19]

Manuel Wik beskriver en förändring och utveckling av hotbilden sedan Kalla kriget. Då utgjordes hotet av stora statsmakter medan den idag kan komma från aktörer på lägre nivå i och med ett större inflytande genom informationsteknologin. Krigföringen har förändrats till att handla om att besitta mest kunskap istället för att ha mest eldkraft på slagfältet. Informationskrigföringen tar en allt större plats, dock beskrivs inte hur nyttjandet av informationskrigföringen har förändrats. En förändring kan därför antas ha ägt rum, dock saknas även här en tydlig forskning som kan påvisa att så har skett. [20]

[16] Chekinov och Bogdanov 2013. Sidan 12-16
[17] Hoffman 2009. Sidan 34ff
[18] Ventre 2009. Sidan xvii
[19] Friman et al 1996. Sidan 6-7
[20] Ibid. Sidan 38

Ryskt synsätt menar att krigföringen har övergått från att ha varit en duell mellan stridssystem till att gå mot en duell mellan informationssystem.[21] Även Amerikanska sidan delar uppfattningen om att Gulfkriget 1991 utgör en utveckling av informationskrigföringen. Insikten att ha kontroll över information och teknologi utgör nyckeln till framgång i moderna konflikter identifierades utifrån de erfarenheter som drogs ifrån denna insats.[22]

Roland Heickerö redogör för informationskrigföringens ökande betydelse, där såväl militära som politiska mål kan uppnås till en låg kostnad. Informationskrigföringen bidrar till en ny dimension till krigföringen med en inbyggd psykologisk påverkan. Ryssland tillsammans med flera andra länder har valt att utveckla förmågor inom informationskrigföringen, då detta identifierats som ett viktigt vapen inom konfliktspektret. Konflikterna beskrivs komma att uppträda i flera dimensioner, och skifta från att vara en duell mellan kinetiska system till att handla om en duell mellan informationssystem. Under ett tal har även den ryska Generalen Viktor Samsonov påpekat att användandet av informationssystem ger en effekt som är jämförbar med skadorna av massförstörelsevapen.[23]

Även Libicki menar att informationskrigföringen inte är ett eget medium av krigföring, utan utgör en ytterligare dimension till krigföringen än tidigare.[24] Tidigare forskning ses otillräcklig att beskriva om och eventuellt hur en förändring i nyttjandet av informationskrigföring gjort sig aktuell, vilket denna undersökning syftar att ge en bredare förståelse för.

Utifrån vad Galeotti, Chekinov och Bogdanov berör avseende informationskrigföring och en förändring i krigföringen kan antagande göras att Rysslands agerande har förändrats för att klara av att behärska konflikterna de deltar i. Även Hoffmans beskrivning av förändringen inom krigföringen tyder på att en förändring skett i Rysslands agerande. Eftersom att Ryssland utgör en stor aktör globalt innebär en förändring från deras sida att krigföringen kan komma att förändras i sin helhet, något som därför blir viktigt att förstå sig på. Denna undersökning syftar till att öka förståelsen för Rysslands brukande av informationskrigföring, vilket kan komma att spela en viktig roll för hur krigföringen tar sig i form i framtiden.

[21] Friman et al 1996. Sidan 7
[22] Ventre 2009. Sidan xvii
[23] Heickerö 2010. Sidan 16
[24] Libicki 1995. Sidan xi

Tidigare forskning påvisar dock inga motstridigheter mot det antagande att nyttjandet av informationskrigföring har förändrats. Dels kan detta bero på att informationskrigföringens uppkomst fortfarande är ett nytt fenomen som fortfarande befinner sig i sitt uppsving, trots att flertalet år har passerat sedan den först uppkom genom ny informationsteknologi. Dels kan det även bero på att det finns en gemensam syn som menar att informationskrigföringen har förändrats i hur detta väljs att brukas av de olika aktörerna. Oavsett hur fallet ligger till så saknas systematiska undersökningar inom ämnet, därmed följer intressant läsning vilket skall försöka fylla denna forskningslucka.

2. Teori

2.1 Inledning

Denna undersökning syftar till att svara på frågan om och i sådana fall hur nyttjandet av informationskrigföring har förändrats under modern tid för Ryssland genom att studera deras deltagande i alla konflikter under de senaste 15 åren. För att detta skall bli möjligt används Libickis teori som teoretiskt ramverk för undersökningen och är vald på grund av att den är så pass omfattande och bred. Libickis definition av informationskrigföring täcker in fler delar som tidigare definitioner inte gjort sig tillräckliga för. Teorin syftar till att ge en beskrivning av informationskrigföringen och gör detta utifrån sju former, som han menar kan definiera informationskrigföring. Fokus i undersökningen kommer att ligga på sex av Libickis sju former av informationskrigföring i syfte att kunna nå en djupare analys av dessa, vilket påverkas av arbetets omfattning. Alla former kommer inte att användas för analysen på grund av arbetets omfattning. För att läsaren skall få en förståelse för informationskrigföring samt den teori som författaren valt att ha som utgångspunkt i undersökningen följer nedan en beskrivning. Eftersom syftet med arbetet är att undersöka om och eventuellt hur en förändring i nyttjandet av informationskrigföring kan förstås så utgör teorin ett verktyg för att kunna svara på ovanstående frågeställning. Libickis teori lämpar sig väl till denna undersökning då den som tidigare nämnts är omfattande i sin beskrivning vilket ger författaren möjlighet att beskriva en förändring av informationskrigföringens brukande.

2.2 Informationskrigföring

Nedan följer en redogörelse av Libickis sju former av informationskrigföring vilket även operationaliseras. Detta teoretiska ramverk utgör grunden i undersökningens analys, där de tre

tidsperioderna granskas utifrån samma punkter för att upptäcka eventuella skillnader i nyttjandet av informationskrigföring och på så sätt svara på arbetets frågeställning. Ur teorin är sedan sex av de sju formerna av informationskrigföring utvalda att utgöra verktyg för analysen, den form som författaren valt att avgränsa från arbetet är *cyber warfare* då författaren anser att kopplingen mellan *cyber warfare* och undersökningens syfte är svagare än övriga former samt att cyberwarfare utgör grund för egen forskning varför denna ej ges utrymme i denna undersökning. *Cyber warfare* beskrivs dock i detta kapitel då denna utgör en del av Libickis teori och kan skapa en förståelse för författarens beslut om bortval.

(1) Cyber warfare är den mest uppseendeväckande och oftast nämnda formen inom media. Detta är den klart svåraste formen att förklara, då delar av den utgörs av hypotetiska resonemang om hur framtida nyttjande av cyberkrigföring kan komma att se ut. De delar denna form består av är; *informationsterrorism*, som är riktad till att genomföra personliga angrepp mot viktiga personer genom att t ex ändra persondata i olika typer av register för att misskreditera personen ifråga. I Cyberwarfare beskriver Libicki även tre undergrupper vilket är följande; *Semantiska attacker* vilket innebär att attacker riktas mot informationssystem så att systemen ger sken av att fungera precis som vanligt men det genererar svar som inte stämmer överens med verkligheten. *Simuleringskrigföring* vilket kan komma att utgöra en framtida lösning på konflikter genom ett simuleringssystem där konflikten utspelas i ett liknande datorsystem. Detta har valts bort av författaren då ämnet inte är relevant för undersökningen. *Gibson-krigföring* utgör även detta en framtida lösning där krigföringen sker på ett virtuellt plan.[25]

(2) Economic information warfare är insatser mot att blockera informationsflöden eller att kanalisera information för att uppnå ekonomisk överlägsenhet. I och med användandet av internationella informationsnät för hantering av sin ekonomiska information, som vissa länder valt att göra, medför detta en ökad risk och sårbarhet som kan öppna möjlighet för hot om ekonomiska blockader genom blockade informationsflöden. Dessa hot kan bli mer effektiva än handlingar i denna typ av krigföring.[26] Exempelvis genom att motståndaren blockerar utsändningen av information så att detta inte når ut till den tänkta mottagaren.

[25] Libicki 1995. Sidan 75-83.
Friman et al 1996. Sidan 5
[26] Libicki 1995. Sidan 66-74
Friman et al 1996. Sidan 5

(3) Hacker warfare är attacker som angriper datorer. Libicki skiljer på militära och civila insatser. *Hacker warfare* går under kategorin civila attacker medan militära delar ingår i C2W som följer nedan. Attackerna kan vara av fysisk eller semantisk karaktär. Främst handlar hackerkrigföring om den defensiva biten vilken rör metoder för skydd av datorsystem.[27]

(4) Psychological warfare handlar främst om att påverka det mänskliga sinnet och viljan hos motståndaren, vilket kan påverkas utifrån fyra olika typer av psykologisk krigföring; *Counter-will* - inom ramen för denna typ av psykologisk krigföring så nyttjas massmedias roll för att påverka en nations vilja och värderingar. *Counter-commander* – vars insatser syftar till att förvirra motståndarens befälhavare på olika sätt, både emotionellt och kognitivt. Media och nyare teknik kan komma att göra dessa typer av insatser mer genomförbara. *Counter-forces* - denna form syftar främst till att bryta ner motståndarens moral och vilja att försvara sig själv. *Kulturkampf* menar Libicki ingår i denna form av informationskrigföring. Denna form kommer inte behandlas mer inom undersökningen då definitionen enligt författaren har tillkortakommande som gör det svårt att undersöka huruvida detta användes i de fall som utgör enheter för analysen. De tillkortakommanden som finns utgörs av Libickis bristfälliga beskrivning vilket senare medför en avgränsning i analysverktygen som utformas i följande kapitel. Dock vill författaren synliggöra att denna del ingår och finns att läsa mer kring i Libickis teori om informationskrigföring.[28] Exempelvis genom att få befolkningen att acceptera sitt agerande eller att befoga sitt agerande genom accepterade åtgärder (terrorismbekämpning kan vara ett sådant exempel).

(5) Electronic warfare, elektronisk krigföring syftar framförallt till degradering av de tekniska förutsättningarna för att handskas med samt överföra information. Det innehåller både offensivt inriktade former som bekämpning av radarsystem och kommunikationsbekämpning, men även defensiva delar som utgörs av krypteringsverksamhet (något som enligt Libickis teori minskar i användning).[29] Sådana attacker kan exempelvis ske både genom fysisk åverkan eller genom en störning av systemet programmässigt.

[27] Libicki 1995. Sidan 50-65
Friman et al 1996. Sidan 5
[28] Libicki 1995. Sidan 34-48
Friman et al 1996. Sidan 4
[29] Libicki 1995. Sidan 27-3
Friman et al 1996. Sidan 4

(6) *Intelligence based warfare*, denna form är en underrättelsebaserad krigföring vilken bygger på skydd av och förhindrande av tillträde till system som försöker skaffa god kunskap för att kunna bemästra striden eller konflikt samt den miljö den angivna verksamheten förs inom.[30]

(7) *Command and control warfare* (C2W), vilket kan jämföras med det som svenska försvarsmakten benämner som ledningskrig. Detta kan också delas in i en offensiv och defensiv form.
Den offensiva formen av C2W går ut på att slå mot fiendens ”huvud och hals” vilket åsyftar högt uppsatta ledare samt kommunikationen med omvärlden. Medan den defensiva formen går ut på att genomföra skyddande åtgärder för högt uppsatta ledare och dennes ledningsstab, samt hindra att kommunikationssystem blir utslagna. Denna typ utgör då den militära delen motsvarande *hacker warfare*.[31] Dessa attacker kan ske genom konventionella attacker, genom kidnappning eller genom utpressning. Det gemensamma för dessa är att de utgörs av attacker mot motståndarens ledare eller de kanaler dessa använder för att genomföra ledning.

2.3 Teori som verktyg för analysen

Libickis teori är vald som teoretiskt ramverk för analysen då definitionerna är tillräckligt allomfattande för att prövas mot det empiriska materialet systematiskt. Författaren anser att tidigare forskning gör sig otillräcklig att systematiskt beskriva nyttjandet av informationskrigföringens förändring över tid, vilket Libickis teori möjliggör för författaren i denna undersökning.[32]

Kritik har, av Martin Libicki själv, riktats mot teorin varpå han menar att informationskrigföring är ett ämne vars definitioner skiljer sig mellan olika teoretiker på grund utav ämnets komplexitet och mångsidighet.[33] Han är bred i definitionerna av informationskrigföring och förklarar inte hur dessa skall användas för att nå framgång i konflikterna utan beskriver endast hur informationskrigföring kan förstås. Syftet med teorin är att ge en definition för ett begrepp

[30] Libicki 1995. Sidan 19-26
Friman et al 1996. Sidan 4
[31] Libicki 1995. Sidan 9-18
Friman et al 1996.Sidan 4
[32] Libicki 1995.
[33] Ibid. sidan 5-6

som innan saknat en tillräcklig definition. Eftersom undersökningen är deskriptiv, lämpar sig teorin väl i undersökningen.

Efter att teorin nu är presenterad återstår hur denna skall användas för analys av de empiriska fall, analysenheter, vilka författaren valt ut. Detta görs genom en operationalisering, vilken som bryter ut analysverktyg och faktorer utifrån angiven teori för att underlätta analysen och göra denne tydlig och begriplig för både författaren och läsaren.

3. Metod

3.1 Inledning

Nedan följer en beskrivning kring undersökningens forskningsdesign, hur den insamlade informationen har bearbetats och kopplats samman för att svara på tidigare nämnd forskningsfråga.

Den valda metoden redogörs och vävs ihop med just denna undersökning för att ge läsaren en klar bild över hur arbetet har genomförts. Det är av vikt att författaren redogör i detalj för vald metod och hur författaren gått tillväga i arbetsprocessen, just för att skapa intersubjektivitet. Det vill säga att en utomstående ska kunna genomföra samma undersökning, under samma förhållanden och uppnå samma resultat.[34] Inom ramen för undersökningens metod utgör teorin ett verktyg för att undersöka Rysslands agerande ur ett informationskrigföringsperspektiv, vilket underlättar arbetet samt gör det enkelt för läsaren att förstå hur undersökningen har förts. Detta möjliggör även för en person att replikera undersökningen.

3.2 Fallstudie

När en undersökning skall svara på frågor som *hur* och *varför* så menar Yin att en fallstudie är den undersökningstyp som lämpar sig bäst.[35] Eftersom fallstudien medger möjlighet för författaren att studera djupare på den specifika företeelsen i sin verkliga kontext, framförallt då gränserna mellan företeelse och kontext är oklara. Fallstudien lämpar sig bra med hänsyn

[34] Esaiasson, et al 2012. Sidan 25
[35] Yin 2007. Sidan 31

till frågans karaktär och omfattning. Informationskrigföring är en svår företeelse att studera då detta i många lägen sker dolt, vilket kräver att fallen studeras på djupet. [36]

Denscombe menar att detta passar fallstudiens tillvägagångsätt och metod. Framförallt om en komplex företeelse skall undersökas, som informationskrigföring i denna undersökning.[37] Fallstudien används med fördel i de fall där mycket information skall samlas in och analyseras.[38] För arbetet krävs god förståelse för Rysslands agerande och Libickis teori, som ligger till grund för analysen, för att möjliggöra en träffsäker analys och rimliga slutsatser. Detta sker genom att djupare analysera de texter som förklarar konflikterna, samt välgenomtänkta faktorer för att analysera en förändring. Fallstudien är därför det givna valet för undersökningen.

Syftet med fallstudien är att ta en liten del av ett stort förlopp och med hjälp av fallet beskriva verkligheten och säga att fallet representerar verkligheten.[39] I undersökningen ger fallstudien en förklaring till om och *hur* metoderna för informationskrigföring har ändrats över tid. [40] En nackdel med fallstudien kan vara svårigheten att generalisera utifrån denna undersökningsmetod, då fallen inte är representativa för övriga fall.[41] Dock syftar inte denna undersökning till att generalisera utan undersöka om en förändring skett avseende nyttjandet av informationskrigföring.

3.3 Kvalitativ textanalys

Kvalitativ textanalys är vald då en större mängd text skall bearbetas och en noggrann inläsning av det empiriska materialet krävs, härmed utgör undersökningen av en kvalitativ forskning.[42] Informationskrigföring kan vara något som sker dolt i de konflikter som undersökts och därför krävs det en djupare analys av materialet.

Författaren har härmed tagit fram det substantiella ur de konflikter som undersökts och tillförskansat sig en djup förståelse vilket en textanalys kräver. Därför har texten läst flera gånger,

[36] Denscombe, 2009. Sidan 62
[37] Ibid. Sidan 62
[38] Johannessen och Tufte, 2003. Sidan 56
[39] Ejvegård 2003. Sidan 33
[40] Denscombe 2009. Sidan 61
Backman 2016. Sidan 59
[41] Denscombe 2009. Sidan 70
[42] Backman 2016. Sidan 59

både överskådligt och därefter mer djupgående. [43] Fördelen med den kvalitativa textanalysen är att det ger en djupare analys inom ett fåtal fall vilket en kvantitativ textanalys inte hade gett. Det som författaren väljer bort är då istället att en större mängd data kan tas med i analysen. Dock anser författaren att den kvalitativa textanalysen lämpar sig bäst för detta fall på grund av tidigare nämnda orsaker. [44]

En risk med en kvalitativ textanalys är att den information som brukas i analysen inte är fullt så representativ som författaren bedömt, vilket då skulle bidra med att sänka förklaringsfaktor på undersökningen resultat. Detta skulle då bidra med svårigheter vid en eventuell generalisering. [45] Åtgärder som är vidtagna för att påvisa medvetenhet kring detta utgörs då av att författaren har sett över en större mängd information än vad som används i analysen, för att med större sannolikhet och trovärdighet hamna så nära verkligheten som möjligt i de slutsatser som dras. Det är även av vikt att inte försumma data som inte stämmer överens med analysen och att redogöra för negativa enheter som motsäger den framväxande analysen.[46]

Ytterligare risk som föreligger i och med en kvalitativ textanalys är inblandning av författarens egna tolkningar och val vilket kan få objektiviteten att framstå som tveksam. För att undvika att detta har författaren haft kritiskt förhållningsätt och en medvetenhet i de val som görs. För att läsaren skall uppfatta detta är det viktigt att författaren motiverar sina val under arbetet. Detta kommer även att speglas i undersökningens avslutning.[47]

3.4 Källkritik

Nedanstående sex punkter har beaktats vid valet av material som nyttjats i undersökningen. Dessa punkter syftar till att klargöra källornas äkthet, oberoende, samtidighet och tendens.[48]

1. Vem står som utgivare av materialet?
2. Är materialet granskat av experter (peer- reviewed)?
3. Är förlaget ett universitetsförlag och/eller är förlaget känt sedan tidigare?
4. Är materialet en andra eller senare upplaga och/eller har det publicerats flera gånger?

[43] Esaiasson et al 2012. Sidan 210
[44] Fejes och Thornberg 2009. Sidan 136
[45] Denscombe 2009. Sidan 399, 400
[46] Ibid. Sidan 386
[47] Ibid. Sidan 32, 219, 220
[48] Esaiasson et al 2012. Sidan 279

5. När och i vilket syfte skrevs materialet?
6. Vilken bakgrund har författaren? (organisation, myndighet, nationstillhörighet, universitet)[49]

Svårigheter föreligger undersökningen att besvara samtliga frågor på det insamlade materialet, vilket har lett fram till at författaren gjort en helhetsbedömning utifrån dessa frågor vilket ligger till grund för vilket material som brukats.

Samtidigheten i det empiriska material som skall studeras medför att de uppgifter som återfinns är aktuella, dock uppstår en svårighet i och med att konflikten på Krim är så pass aktuell så kan viss information vara hemlig, således utgörs materialet i undersökningen av öppna källor. Dock utgörs inte fallen av samma samtidighet då ett empiriskt material är hämtat från 1999 och ett från 2008, vilket kan medföra att information som var aktuell vid dessa tidpunkter ej är aktuella för denna undersökning. Dock finns möjlighet att hämta större mängd material i och med den gångna tiden mellan dessa tidpunkter och denna undersökning.

Äktheten har utifrån materialet till analysen inte visat sig tveksam eller bristfällig. Vad gäller *tendens* och *oberoende* kan det inom ramen för undersökningen till del återges en färgad bild av det empiriska material som analyseras, på grund av att västvärlden kan ha intresse av att framhäva viss information vilket kan skiljas från Rysslands bild.[50] Då författaren endast nyttjar svenska och engelska källor ökar risken att västvärldens syn påverkar resultatet av analysen och slutsatserna. Författaren har aktivt arbetat för att reducera problemet med tendens och oberoende genom att vara medveten om detta vid analys av de källor som används då dessa härstammar från olika västerländska länder, vilket gör att den ryska synen inte faller inom ramen för analysen. Flera källor har använts för respektive fall för att öka tillförlitligheten för de slutsatser som författaren drar.[51] Arbetet har brukat källor som kan ses som partiska för att möjliggöra analysen, dock har försök att validera den informationen gjorts genom källor från Ryssland. Undersökningen kommer ej ifrån problematiken angående tendens, dock är det svårt att undvika. Författaren är medveten kring detta vilket kan minska dess påverkan, och medföra att resultatet blir så trovärdigt som möjligt.

[49] Esaiasson et al 2012. Sidan 301 – 302
[50] Ibid. Sidan 284-285
[51] Denscombe 2009. Sidan 186, 189

3.5 Operationalisering

Operationaliseringen syftar till att tydligare redogöra för vilket sätt författaren brukat analysverktygen, genom att utforma faktorer från dessa på analysenheterna för undersökningen. Att redogöra för hur analysen är genomförd utifrån vald metod och teori är viktigt, då någon utomstående skall kunna replikera analysen.[52]

Undersökningens teoretiska ramverk är Libickis definition av informationskrigföring. Utifrån Libickis teori har analysverktyg tagits fram som sedan gjorts om till faktorer som ligger till grund för analysen. Dessa delar anser författaren utgöra teorins prövbara delar och är lämpliga att testa huruvida informationskrigföringens brukande har förändrats. Genom en tydlig framställning och resultatdiskussion blir det möjligt att endast ta med delar ur teorin. En noggrann inläsning och en förståelse för Libickis teori har därmed föranlett att vissa delarna i teorin blivit utvalda och andra delar valts bort. Dessa faktorer utgör sedan kategorier under den kvalitativa analysen som är genomförd på Rysslands nyttjande av informationskrigföring de senaste 15 åren.

Materialet som skall analyseras är analyserat med faktorerna i fokus, vilket också kommer att redogöras under analyskapitlet och tydliggöras i *Tabell 1.1 faktorer*. För det första är analysmaterialet noga kontrollerat och alla tillfällen där informationskrigföring har nyttjas är utplockade. En noggrannare inblick i dessa situationer är sedan gjord utifrån de faktorer som tidigare nämnts för att kunna systematisera och redovisa resultatet av analysenheterna, vilket författaren anses saknas i tidigare forskning. Syftet med att använda dessa faktorer är att kunna analysera de olika tidsperioderna i Rysslands agerande för att därefter kunna svara på frågan *Har Rysslands nyttjande av informationskrigföring förändrats, och i sådana fall hur har den förändrats?*

Utvalda faktorer utgör verktyg för analysen då dessa representerar teorin samt är prövbara inom det empiriska material som utgör analysenheter i undersökningen. *Cyber warfare* är bortvald då denna form till stor del är hypotetiskt utformad, och svår att pröva i och med att den relativt outforskad och oanvänd utifrån hur teorin beskriver den. Den är samtidigt så utbredd att den utgör material för forskning som eget område, vilket därför valts bort ur denna undersökning då författaren har tagit hänsyn till undersökningens omfattning. Övriga former

[52] Backman 2016. Sidan 41-42

utgörs av både civila och militära delar av informationskrigföring, dock är detta något som inte ligger till grund för bortval utan informationskrigföring utforskas i sin helhet för att kunna urskilja om en förändring skett eller ej de senaste 15 åren ur ett ryskt perspektiv.

Vissa delar från Libickis sju former av informationskrigföring har valts att inte användas i analysen, ett exempel på en sådan del är kulturkrigföringen som dels är svår att pröva då Libicki ej varit så ingående i beskrivningen av denna dels på grund av arbetets omfattning vilket gör att avgränsningar har varit tvungna att göras inom undersökningen. Alla dessa delar framgår tydligt i operationaliseringen där de delar som valts med finns som utformade faktorer medans de delar som ingår i teorin men som inte utgör del för analysen presenteras inom Libickis sju former av informationskrigföring.[53]

Tabell 1.1 faktorer

Ledningskrigföring Attacker som sker mot motståndarens ledning, ledningsplatser eller kanaler för ledning (Command and control warfare)[54]	- Attacker mot motståndarens ledare, antingen konventionella attacker, frihetsberövande eller störning. - Attacker mot motståndarens stab/ledningsplatser genom konventionella metoder eller störning. - Skyddande av egna ledare och stabsplatser för att motverka motståndarens möjlighet att påverka den egna ledningsfunktionen. - Försvårar för motståndaren att sända information och därigenom försvåra motståndarens ledning.
Psykologisk krigföring Aktioner som sker för att berättiga sitt agerande från andra nationer eller befolkningen (Psychological warfare)[55]	- Nyttjandet av media för att påverka motståndarens vilja och moral. - Nyttjandet av information för att påverka befolkningen. - Nyttjandet av information för att förvirra

[53] Se ”teori”. Sidan 12ff
[54] Libicki 1995. Sidan 9-18
[55] Ibid. Sidan 34-48

	motståndarens ledning. - Nyttjandet av information i syfte att berättiga sitt agerande.
Elektroniskkrigföring Attacker mot elektroniska system (Electronic warfare)[56]	- Attacker för att förstöra motståndarens tekniska informationsöverföringar.
Hackerkrigföring (Hacker warfare)[57]	- Attacker på motståndarens datorsystem.
Ekonomisk informationskrigföring Påverkan av motståndarens informationskanaler (Economic information warfare)[58]	- Blockering av motståndarens utsända information. - Kanalisering av motståndarens utsända information.
Underrättelsebaserade krigföring (Intellegence based warfare)[59]	- Underrättelser om motståndaren för att behärska stridsrummet.

3.6 Empiri

Variationen i denna deskriptiva studie utgörs av nedslag vid tre olika tidpunkter för att undersöka Rysslands agerande. Konflikterna som är analyserade i undersökningen utgör samtliga konflikter som Rysslands deltagit i under de senaste 15 åren. Eftersom dessa inte är utvalda att göra sig representativa för ytterligare konflikter följer därför ingen diskussion huruvida dessa är för lika eller olika varandra. Dessa är utvalda under en viss tidsperiod, varpå en variation i tid för Rysslands nyttjande av informationskrigföring undersöks. Diskussion följer huruvida detta påverkat resultatet, i undersökningens avslutning.

4. Analys

Nedan följer analysen som författaren gjort på Rysslands brukande av informationskrigföring, där variationen utgörs av tre olika nedslag i tid för att kunna svara på frågan *Har Rysslands*

[56] Libicki 1995. Sidan 27-33
[57] Ibid. Sidan 50-65
[58] Ibid. Sidan 66-74
[59] Ibid. Sidan 19-26

nyttjande av informationskrigföring förändrats, och i sådana fall hur har den förändrats? Detta görs med utgångspunkt i ovannämnda faktorer ur Libickis teori om informationskrigföring. Dessa utgör nedan verktyg för analysen genom de faktorer som arbetats fram ur teorin, vilket senare tydliggörs vid studerandet av konflikterna för att svara på frågeställningen.

4.1 Andra Tjetjenienkriget 1999-2001

Undersökningen utgår ifrån händelser som skedde mellan starten av konflikten, hösten 1999, till ett senare skede där konflikten återigen hade lugnats, 2001. Konflikten startade med att Ryssland valde att replikera på tjetjenernas inbladning i Dagestan där tjetjenerna hade valt att understödja islamistiska fundamentalister som var under attack av Ryssland. Till följd av detta bombade Ryssland delar av Tjetjenien, där huvudstaden Groznyj utgjorde ett mål. Samtidigt skedde bombningar på rysk mark, vilket resulterade i förluster bland den ryska befolkningen. Dåvarande presidenten, Boris Jeltsin, krävde att tjetjenerna skulle utelämna de skyldiga för dåden, varpå en markoffensiv den efterföljande dagen inleddes av Ryssland. Stora delar av den tjetjenska befolkningen flydde landet samtidigt som Ryssland försökte inta den välförsvarade huvudstaden. Tjetjenerna bröt sig tillslut ut från huvudstaden då mat och ammunitionen började sina. Senare övergick tjetjenerna till gerillakrigföring, vilket denna konflikt sedan fortsatte som.[60]

4.1.1 C2W

Attacker mot motståndarens ledare nyttjades av Ryssland när de slog ut ledare inom den tjetjenska ledningen. Dels genom att dessa dödades och fängslades.[61] *Attacker mot motståndarens stab/ledningsplatser* utfördes då Ryssland belägrade och förstörde den, för tjetjenerna, viktiga staden Groznyj vilken utgjorde en central del för ledningen av de tjetjenska styrkorna till en början.[62] *Skyddande av egna ledare och stabsplatser* genomfördes då Ryssland hade dragit lärdomar från tidigare konflikt, genom att högt uppsatta ledare på den egna sidan under konflikten inte omkom i samma utsträckning som tidigare, därmed uppnåddes ett bättre skydd av de egna ledarna.[63] *Försvårar för motståndaren att sända information* förekom även det inom konflikten, dock är detta något som kan ses som en EW-attack och följer nedan.

[60] Oliker 2001. Sidan 31ff
[61] ”*Timeline: Chechnya*”, publicerad 2011-01-19 kl. 13:59. BBC News, hämtad 2016-04-28.
[62] Ibid
[63] Oliker 2001. Sidan 59

4.1.2 Psycological warfare

Nyttjandet av media för att påverka motståndarens vilja och moral genomfördes genom ett yttrande av den dåvarande ryska försvarsministern Igor Sergeyev, där det menades att bombningarna kommer att fortsätta intill dess att den sista motståndaren är borta. [64] *Nyttjandet av information för att påverka befolkningen* var en lärdom från tidigare konflikt med Tjetjenien (1994-1996), då man inte insåg den viktiga roll som rapporter från konfliktzonen utgjorde, vilka hade en påverkan på befolkningen via media. Detta ledde sedermera till att stödet från befolkningen, som redan från start hade varit lågt, sjönk ytterligare. Tjetjenerna hade tagit tillvara på medias roll och kunde sprida information som gynnade dem samtidigt som det missgynnade Ryssland.[65] För att motverka att samma scenario skulle återupprepas bekämpade därför Ryssland strömförsörjningen, detta ingår även som en del av EW vilket följer nedan. [66] Ryssland beaktade medias roll då insikten för hur det påverkade befolkningens inställning för deras deltagande i konflikten. Ryssland lyckades kontrollera pressen och beskrev operationerna som anti-terror operationer istället för krig. Det ledde till att den egna befolkningen och omvärldens förtroende till Rysslands agerande ökade, jämfört med tidigare konflikt där frontlinjens misär fritt kunde rapporteras.[67] En större förståelse för medias inflytande på befolkningens sinnen fanns, även om den överdrivet positiva bilden tillslut började ifrågasättas via media.[68]

Nyttjandet av information för att förvirra motståndarens ledning finner författaren en avsaknad av inom genomsökta källor. *Nyttjandet av information i syfte att berättiga sitt agerande* utgjorde en tydlig del under konflikten genom uttalande syftat att befoga sitt agerande då Vladimir Putin menade att terrorismen måste bekämpas och där av anledningen till deras offensiv i Tjetjenien.[69] Fortsatta uttalanden om terroristbekämpning följde av Putin-regeringen vilket skulle ge medhåll från väst.[70] Terroristbekämpningen utgjorde Rysslands främsta argument för deras deltagande.

---

[64] "*Phase One - The Air Campaign - September 1999*", publicerad 2011-11-07. Global security, hämtad 2016-05-18
[65] Oliker 2001. Sidan 34
[66] "*Phase One - The Air Campaign - September 1999*", publicerad 2011-11-07. Global security, hämtad 2016-05-18
[67] Oliker 2001. Sidan 63-64
[68] Ibid. Sidan 63-64
[69] "*Timeline: Chechnya*", publicerad 2011-01-19 kl 13:59. BBC News, hämtad 2016-04-28
[70] Nichol 2005

4.1.3 Electronic warfare

Attacker för att förstöra motståndarens tekniska informationsöverföringar skedde genom speciella *Electronic Warfare* förmågor, vilka nyttjades för att i första hand lokalisera tjetjenernas kommunikationsnätverk i syfte att naturalisera dem antingen fysiskt eller genom störning.[71] Dock nyttjades detta inte i så stor utsträckning som hade behövts för att få ut den effekt som eftersträvades och utbildningsståndpunkten på denna typ av utrustning var bristfällig, vilket också medgav sämre uteffekt än hoppats.[72] Som tidigare nämnts bekämpade strömförsörjningen, vilken också utgör en form av EW-attack.[73]

4.1.4 Hacker warfare

Attacker på motståndarens datorsystem har inte, av författaren, utlästs av de källor som granskats. Det kan bero på att användningen av denna krigföringsform inte behandlas inom ramen för öppna dokument, att brukandet skett men att det inte är uttalat eller att det helt enkelt inte nyttjats.

4.1.5 Economic information warfare

Blockering av motståndarens utsända information och *kanalisering av motståndarens utsända information* har ej utlästs från de källor som avhandlar given konflikt.

4.1.6 Intelligence based warfare

Underrättelser om motståndaren för att behärska stridsrummet användes av den ryska sidan genom att rysk trupp gav sken om att befinna sig överallt, vilket gav en psykologisk effekt hos den tjetjenska truppen och ledningen. [74]

4.2 Georgien 2008

Fallet som nyttjas i undersökningen ägde rum under Augusti månad, 2008. Dock har uppgifter kring exempelvis drönar-attacker, vilket skedde innan denna period, valts att tas med i undersökningen då detta gav en effekt som varade under konflikten. Ryssland stöttade Sydossetiens hävdande av självständighet från Georgien. När Georgien i augusti 2008 gick in i Sydossetien bröt konflikten ut. Ryssland hade fredsbevarande styrkor i området vilka blivit attackerade av georgiska styrkor, vilket Ryssland befogade sitt deltagande genom och svarade upp med att

[71] Oliker, 2001. Sidan 52
[72] Ibid. Sidan 52
[73] "*Phase One - The Air Campaign - September 1999*", publicerad 2011-11-07. Global security, hämtad 2016-05-18
[74] "*Second Chechen war*", publicerad 2015-05-10. Prezi hämtad 2016-05-18

möta Georgien med militär kraft. Ett fem-dagarskrig följde mellan Ryssland och Georgien vilket senare slutade i en överväldigande rysk seger då georgiska militären hade tryckts tillbaka in i Georgien. Utöver detta hävdade Ryssland att deras militära medverkande var en fredsframtvingande operation och att medverkan dessutom var till för att skydda de ryska medborgarna som levde i Sydossetien vid tidpunkten för konflikten.[75]

4.2.1 C2W

Attacker mot motståndarens ledare genomfördes inte under denna konflikt i samma form som under tidigare konflikt. Istället genomfördes attack mot den georgiska ledningen genom informationsattacker där den georgiska presidenten blev anklagad för att ha varit för militärt aggressiv i sitt agerande samt att de georgiska företagen hade kränkt de humanitära rättigheterna. [76] *Attacker mot motståndarens stab/ledningsplatser* har ej uppmärksammats av författaren inom ramen för de källor som granskats. *Skyddande av egna ledare* förekom i liknade form som tidigare, där de egna ledarna inte blottades för motståndarens bekämpning, och därför inte utgjorde ett klart mål för georgiska styrkor. Detta skapade på så vis ett passivt skydd.[77] *Försvårar för motståndaren att sända information* visade sig ha genomförts, dock återkommer detta under *Economic information warfare*.

4.2.2 Psycological warfare

Nyttjandet av media för att påverka motståndarens vilja och moral visar sig inte under konflikten dock sänktes den georgiska styrkans moral genom ett flyganfall mot en markburen styrka där utfallet blev flertalet döda och skadade vilket alltså inte räknas in under denna kategori i undersökningen vilket då inte utgör en faktor i denna undersökning och därför inte tas hänsyn till i analysen.[78] Detta tas inte med i analysen på grund av att attacken endast var en reguljär attack mot deras styrkor och ingen attack som faller under informationskrigföringen och dess former. *Nyttjandet av information för att påverka befolkningen* kan utläsas ur de källor som granskats om konflikten, dock berör dessa punkter även berättigandet av Rysslands agerande under konflikten och kommer således under denna punkt. *Nyttjandet av information för att förvirra motståndarens ledning*. Ryssland lyckades påverka den georgiska ledningen genom att de var försvarsberedda vid ett georgiskt angrepp mot Sydossetien. Detta tvingade då den georgiska ledningen att improvisera istället för att

[75] Asmus 2010. Sidan 165
Lavrov 2010. Sidan 44ff
[76] Cornell, och Starr 2009. Sidan 187
[77] Ibid. Sidan 51
[78] Ibid. Sidan 54

agera enligt planerat. [79] Dels även genom flygräder vilket motverkade georgiska flygföretag eftersom de ansåg att risken för bekämpning var för hög.[80] Genom uttalanden av Putin där han både gav felaktig information och vilseledande information fick detta en effekt hos den georgiska sidan vilket kan sorteras in under denna kategori.[81]

Nyttjandet av information i syfte att berättiga sitt agerande utgjorde en tyngdpunkt inom denna konflikt. Dels genomförde Ryssland ett flertalet stora övningar både 2006, 2007 och 2008. Där den största av dessa övningar hölls under sommaren 2008 i närhet av det område där konflikten senare ägde rum, vilket medgav effekt under konflikten där övningsverksamheten fortsatte att nyttjas som argument för deras närvaro. Varpå syftet klart och tydligt utgjordes av att demonstrera för Rysslands kapacitet både för närområdet samt övriga delar av världen.[82] Ryssland meddelade även, efter att ryska fredsbevarande styrkor hade blivit attackerade, att detta inte kunde accepteras.[83] I och med att dessa styrkor blivit attackerade och även genom att Georgien påbörjade en militär offensiv hävdade den ryska ledningen att de agerade i försvar mot den georgiska sidan. [84] Ryssland hävdade även att deras inblandning i konflikten syftade till att skydda de egna medborgarna som levde i det drabbade området och därmed skydda den egna befolkningen samt att insatsen var en fredsbevarande insats.[85] Dessutom ställde sig Ryssland bakom Sydossetiens hävdande av självständighet från Georgien.[86]

4.2.3 Electronic warfare

Attacker för att förstöra motståndarens tekniska informationsöverföringar även det är en tyngdpunkt i konflikten. Dels genomfördes, dock innan konflikten bröt ut, attacker mot georgiska drönare. Dels genom ett flygföretag där ett ryskt flyg sköt ner en georgisk drönare, som sedan när Ryssland blev anklagade för detta, nekades av den Ryska ledningen. [87] Efter detta sköts ett flertalet georgiska drönare ned, vilket tillslut följdes av ett uttalande av den ryska

[79] Lavrov 2010. Sidan 44
[80] Ibid. Sidan 52
[81] Cornell och Starr 2009. Sidan189-190
[82] Lavrov 2010. Sidan 41
Cornell och Starr 2009. Sidan 75
[83] Tagliavini 2009. Sidan 21
Cornell och Starr 2009. Sidan 69
[84] Ibid. Sidan 184
[85] Ibid. Sidan 158-159
Tagliavini 2009. Sidan 22, 24
[86] Lavrov 2010. Sidan 42ff
[87] Cornell och Starr 2009.

Generalen Vladimir Shamanov, där han uttryckte att Ryssland inte skulle tillåta några ytterligare georgiska flygföretag över konfliktzonen.[88] Detta skedde innan konflikten bröt ut, dock anses det relevant att undersöka då effekten kvarstod under konflikten. En radarstation på Tbilisis flygplats attackerades av en anti-radarmissil, en radarstation vilken var vital för kontrollen av luftrummet i konfliktzonen samt en civil radaranläggning attackerades av Ryssland vilket förstörde motståndarens tekniska system.[89] Utöver detta förstördes en kommandocentral av Ryssland vilket mynnade ut i nedstängning av Georgiens mobila luftförsvarssystem, då Georgien inte ville riskera att få även detta bekämpat vid en eventuell rysk attack.[90] Attacker mot sambandssystem och ledningscentraler sänkte deras kapacitet till ledning.[91]

4.2.4 Hacker warfare

Attacker på motståndarens datorsystem har ej uppmärksammats utifrån de källor som granskats för angiven konflikt. Dock har hackers nämnts inom ramen för konflikten, vilket ökar misstanken om att detta nyttjats, bara att det inte behandlats i öppna källor.[92]

4.2.5 Economic information warfare

Blockering av motståndarens utsända information. lyckades Ryssland nyttja och därigenom stärka bilden av det egna deltagandet i konflikten. Genom attacker mot georgiska websidor, vilket resulterade i att information blev blockerad för den georgiska ledningen.[93] *Kanalisering av motståndarens utsända information* var också något som endast till en liten del genomfördes, då Ryssland kanaliserade information via media för att inte avslöja sin egen militära verksamhet och för att befoga sitt närvarande och deltagande väl när konflikten bröt ut.[94]

4.2.6 Intelligence based warfare

Underrättelser om motståndaren för att behärska stridsrummet är inget som uppmärksammats under den kvalitativa analysen av de källor som utgjort underlag för undersökningen.

[88] Lavrov 2010. Sidan 41
[89] Tagliavini 2009. Sidan 21
Lavrov 2010. Sidan 67, 69
[90] Ibid. Sidan 69
[91] Ibid. Sidan 62, 67
[92] Cornell och Starr 2009. Sidan 191
[93] Ibid. Sidan 154
[94] Ibid. Sidan 187

4.3 Krimkrisen 2014

Det material som brukats i undersökningen utspelar sig under februari och mars, 2014. Ryssland annonserade deras största militära övning i modern tid, vilken hölls i anslutning till Krimhalvön. Samtidigt skede flertalet incidenter på Krim där gröna män med koppling till Ryssland, genomförde räder mot ukrainsk ledning i området. Viktiga byggnader intogs och politiska ledare blev attackerade. Rysslands deltagande påbörjades därefter, med argument att den rysktalande befolkningen på Krim skulle skyddas och rysk propaganda spreds för att, som de kallade det, ta tillbaka Krim varpå en folkomröstning hölls i frågan. Med överväldigande majoritet blev så också fallet, vilket i efterhand blivit starkt ifrågasatt. Beslut hade tagits av det ryska parlamentet att rysk trupp hade tillstånd att uppträda inom ukrainskt territorium.[95]

4.3.1 C2W

Attacker mot motståndarens ledare kunde utläsas ur en svensk tidning då högt uppsatta ledare på den ukrainska sidan hade blivit mördade under de inledande räderna, dock kan denna information ifrågasättas eftersom den inte återfunnits i övriga källor.[96] *Attacker mot motståndarens stab/ledningsplatser* genomfördes genom attacker mot viktiga byggnader på Krimhalvön, där parlamentsbyggnaden i Simferopol intogs av gröna män utan vare sig gradbeteckningar eller andra förbandstecken den 27 februari 2014.[97] Dessa gröna män kunde antas ha kopplingar till Ryssland då vapen och övrig utrustning var densamma som ryska förband använde, dock angav sig dessa för att vara rysktalande självförsvarsstyrkor på Krim.[98] *Skyddande av egna ledare och stabsplatser* har ej uppmärksammats från analyserade källor. *Försvårar för motståndaren att sända information* genomfördes då försök att slå ut internet och telekommunikationsanslutningar, dock visade sig inte dessa ge någon effekt. Det identifierades av Ukrainas största teleleverantör Ukrtelecom.[99]

4.3.2 Psycological warfare

Nyttjandet av media för att påverka motståndarens vilja och moral är inget som identifierats i de källor som granskats. *Nyttjandet av information för att påverka befolkningen* gjordes då

[95] Efron 2014. Sidan 51och 105
Franke et al 2014. Sidan 41
Oldberg et al 2014. sidan 17-18
Lavrov 2014. Sidan 164-166
[96] "*Krisen i Ukraina på 60 sekunder*", publicerad 2014-02-28. Aftonbladet, hämtad 2016-05-18
[97] Oldberg et al 2014. Sidan 17-18
[98] Barabanov, et al 2014 Sidan 163
[99] Efron 2014. Sidan 56

dessa blev informerade angående den övning som skulle genomföras vilket också skulle belasta vägar och järnvägar kraftigt, vilket stärkte deras närvaro vid den rysk-ukrainska gränsen, hos befolkningen.[100] När Ryssland senare engagerade sig på Krimhalvön genomfördes försök att påverka befolkningen genom att hävda att deras agerande var till för att återta Krim, som tidigare hade tillhört Ryssland. Något som sedan visade sig vid en omdiskuterad omröstning även fått stöd av befolkningen på Krim.[101] *Nyttjandet av information för att förvirra motståndarens ledning* bestod av den stora övning som hade dragits igång av den ryska sidan vilket gjorde det svårt för de ukrainska styrkorna att urskilja aktioner och företag som ingick i övningen eller vad som föregicks skarpt på Krim. Även den ryska sidan kunde legitimera sitt agerande genom att övningen pågick så pass nära Krimhalvön.

Nyttjandet av information i syfte att berättiga sitt agerande skedde genom annonsering av den ryska övningen som genomfördes i närhet av den Ukrainska gränsen. Detta syftade, utöver att påverka befolkningens stöd, till att påverka västvärldens syn till en större acceptans för Rysslands aktivitet i området.[102] Putin bekräftade att rysk trupp hade varit inblandad på Krim. Dock bekräftade Putin för en rysk nyhetskanal att de gröna män som befann sig på Krim bestod av rysk trupp.[103] Övningen som hölls i närhet av den ukrainska gränsen var oannonserad och beordrades av Putin, med ett bortre datum satt till 3 mars.[104] Enligt meddelande av försvarsminister Sergej Kuzjugetovitj var 150.000 inblandade i övningen, vilket gör den till Rysslands näst största övning i Rysslands historia.[105] Detta skulle enligt den ryska ledningen inte vara förknippat med konflikten trots att den genomfördes vid gränsen till Ukraina.[106] Något som kan anses vara ett försök att få övriga världen att acceptera deras närvaro i området. Putin befogade sitt agerande, likt tidigare fall (2008), genom att detta syftade till att skydda den rysktalande befolkningen som levde på Krim, samt skydd för den ryska flottan som var belägen där.[107]

[100] Efron 2014. Sidan 105
[101] Lavrov 2014. Sidan 173
[102] Ibid. Sidan 105
[103] "*Putin acknowledges Russian military serviceman were in Crimea, Russia Today*", Publicerad 2014-04-17 Kl: 09.28. RT, Hämtad 2016-05-02
[104] Efron 2014. Sidan 50 och 105
Lavrov 2014. Sidan 162
[105] Efron 2014. Sidan 51
[106] Ibid. Sidan 105
[107] "*Putin ready to invade Ukraine; Kiev warns of war*", publicerad 2014-03-01. Reuters, hämtad 2016-05-18

4.3.3 Electronic warfare

Attacker för att förstöra motståndarens tekniska informationsöverföringar. Genomfördes genom den attack som tidigare nämnts avseende bekämpningen av telekombolaget Ukrtelecoms internet och telekommunikationsanslutningar. Det gav i efterhand inte den effekt som hade önskats. [108]

4.3.4 Hacker warfare

Attacker på motståndarens datorsystem har likt Andra Tjetjenienkriget och Georgienkriget inte återfunnits inom de källor som avhandlats för konflikten.

4.3.5 Economic information warfare

Blockering av motståndarens utsända information genomfördes av de gröna männen som lyckats överta den statliga Tv-stationen och omringa alla strategiskt viktiga byggnader på Krimhalvön.[109] *Kanalisering av motståndarens utsända information* kan ha skett i samband med detta, dock inget som framgår utifrån de använda källorna.

4.3.6 Intelligence based warfare

Underrättelser om motståndaren för att behärska stridsrummet är inget som uppenbarat sig inom ramen för konfliktens källor.

4.4 Jämförelse mellan fallen, någon förändring?

4.4.1 Command and control warfare

Attacker mot motståndarens ledare är något vi kan se brukats av Ryssland vid konflikten med Tjetjenien genom att fysiskt angripa motståndaren, antingen genom kinetisk verkan eller genom att ledare fängslades. I konflikt med Georgien hade den fysiska attacken bytts ut mot informationsattacker där anklagelser mot den georgiska presidenten förekom. Vilket sedan återgick till fysiska aktioner under Krimkrisen, där ledande politiska positioner attackerades. Det har alltså under samtliga fall skett någon typ av attack mot motståndarens ledare vilket alla faller under denna kategori, dock har attacker mot ledare skiftat mellan konflikterna. *Attacker mot motståndarens stab/ledningsplatser* under Andra Tjetjenienkonflikten genomfördes detta mot städer som utgjorde viktiga ledningsplatser för motståndaren, där Groznyj då sågs som viktig för Tjetjenerna och intogs därför av Ryssland. Ingen sådan aktion

[108] Efron 2014. Sidan 56
[109] McDermott 2015. Sidan 12
Efron 2014. Sidan 62

har författaren kunnat utläsa för konflikten 2008. Dock är detta något som återkommer under Krimkrisen där viktiga byggnader belägrades, exempelvis parlamentsbyggnaden. Därmed skiljer sig det även här kraftigt mellan konflikterna, där denna typ verkar ha återkommit från första konflikten till den sista med frånvaro från tiden emellan dessa konflikter.

Skyddande av egna ledare och stabsplatser skedde inom Tjetjenienkonflikten genom att de egna ledarna skyddades för motståndarens bekämpning, vilket även fortsattes under senare konflikt. Inom ramen för Krimkrisen kan ingen källa styrka att detta genomfördes även här, dock har inga rapporter om stupade eller skadade ledare återfunnits vilket kan tänkas betyda ha tillämpats även i detta fall. *Försvårar för motståndaren att sända information* har återfunnits i alla tre fall och samtliga liknar EW-attacker vilket kan tänkas ha en koppling till varandra. Därmed återkommer detta under EW nedan.

4.4.2 Psycological warfare

Nyttjandet av media för att påverka motståndarens vilja och moral var något som förekom under den första konflikten, däremot visade sig inte detta vara något som Ryssland sedan använde under konflikten med Georgien eller under konflikten på Krim. Det syns därmed en förändring under denna 15 års period som undersökningen gör sig gällande för. *Nyttjandet av information för att påverka befolkningen* utgjordes som en viktig del för den ryska sidan redan under konflikten med Tjetjenien, där man insåg medias roll och hur befolkningens inställning till konflikten påverkades, därav genomförde åtgärder för att få fördel av detta. Just befolkningen stod inte i centrum för dessa åtgärder under konflikten med Georgien, utan då försökte Ryssland istället (som följer nedan) berättiga sitt agerande under konflikten. Väl vid konflikten på Krim verkar fokus ha återvänt till att återigen få med sig befolkningen att acceptera deras agerande. Därmed åskådliggörs även här svängning i den psykologiska krigföringen där befolkningen var viktig under tidig och sen konflikt, dock inget fokus på befolkningen under konflikten med Georgien.

Nyttjandet av information för att förvirra motståndarens ledning visar en tydlig förändring i Rysslands sätt att agera genom att under konflikten med Georgien och på Krim så genomförde Ryssland stora övningar i närområdet. Detta gjorde det svårt för motståndarens ledning i och med att övningsverksamhet bedrevs och därför nyttjade Ryssland detta som täckmantel för deras deltagande. Detta var inget som uppenbarat sig under den tidigaste konflikten vilket gör denna förändring tydlig. *Nyttjandet av information i syfte att berättiga*

sitt agerande visar inte upp någon förändring då detta nyttjats under samtliga konflikter. Dels genom att hävda terrorbekämpning i konflikten med Tjetjenien, att insatsen mot Georgien var en fredsframtvingande operation och skydd av de ryska medborgarna som levde i Sydossetien samt att under konflikten på Krim så agerade Ryssland för att skydda den rysktalande befolkningen som levde på Krimhalvön. Ett tydligt ryskt tillvägagångsätt under de 15 senaste årens konflikter.

4.4.3 Electronic warfare

Attacker för att förstöra motståndarens tekniska informationsöverföringar utgjorde sin tyngdpunkt under Georgienkriget, där stor kraft lades vid EW-attacker mot motståndarens tekniska system. Detta nyttjades även under Tjetjenienkonflikten, dock inte alls i samma utsträckning. Även under Krimkrisen brukades detta, då bara genom fåtalet aktioner. Därmed visar sig en tydlig skillnad i Rysslands agerande, där det går från att nyttjas delvis till att utgöra en tyngdpunkt inom krigföringen för att återigen inte alls brukas i samma utsträckning.

4.4.4 Hacker warfare

Attacker på motståndarens datorsystem visar sig inte alls under någon av konflikterna, vilket heller inte innebär någon förändring inom denna form av informationskrigföring. Om detta beror på att det inte nyttjades under någon av konflikterna eller om detta utgör en del som hålls hemlig på grund av det är en viktig del som inte får röjas för motståndaren kan inte denna undersökning svara på utan endast spekulera kring.

4.4.5 Economic based warfare

Blockering av motståndarens utsända information skedde i liten utsträckning i de två senare konflikterna, och återfanns inte ur andra Tjetjenienkonfliktens källor. Detta utgör dock ingen större del av krigföringen, även om det existerade. *Kanalisering av motståndarens utsända information* följer samma spår och inträffade i liten utsträckning under senare Georgienkriget och Krimkrisen konflikter samt inget under Tjetjenienkriget. En lite förändring går därför att utläsa inom denna form där det gått att inte användas alls till att användas i begränsad utsträckning.

4.4.6 Intelligence based warfare

Underrättelser om motståndaren för att behärska stridsrummet nyttjades till del under Tjetjenienkonflikten och har inte uppenbarat sig alls under resterande två konflikter. En förändring kan utläsas, om än en liten förändring. Användandet av denna form inom Andra Tjetjenien-

kriget kan ha varit en engångsföreteelse då detta inte uppenbarade sig upprepade gånger. Detta lämnar resultatet lite frågande.

5. Avslutning

5.1 Svar på frågeställning

Har Rysslands nyttjande av informationskrigföring förändrats, och i sådana fall hur har den förändrats?

Informationskrigföring har använts av Ryssland under samtliga tre konflikter i mer eller mindre utsträckning. Det går att uttyda en förändring mellan de olika konflikterna, där till exempel EW-attacker skedde i större utsträckning under konflikten i Georgien än övriga konflikter. En tyngdpunkt har i samtliga konflikter utgjorts utav den psykologiska krigföringen, där en förändring från att påverka befolkningen till att befoga sitt eget agerande har visat sig tydlig, för att ånyo påverka befolkningen. Några större ytterligare förändringar gör sig inte tydliga inom undersökningen, då exempelvis *Hacker warfare* inte återfunnit i någon av använda källor och heller inte kan påvisa någon förändring.

5.2 Resultat och slutsatser

Inom *C2W* kan en förändring tydas där attacker mot motståndarens ledningsstruktur skett dock i olika former. Detta förväntas fortsätta även i framtida konflikter även om det är svårt att säga i vilken form det kan ske. Hur detta har nyttjats beror till största del på vilken typ av konflikt det är samt motståndaren.

Psykologisk krigföring har under samtliga konflikter utgjort en tyngdpunkt för Rysslands informationskrigföring. Påverkan av befolkningen utgjorde en stor del vid Tjetjenien konflikten och Krimkrisen, dock inte i samma utsträckning under Georgienkriget. Nyttjandet av information för att påverka motståndarens ledning har visat sig mer betydelsefullt under senare tid vilket tyder på ett fortsatt brukande av detta fortsättningsvis. Att berättiga sitt eget agerande har visat sig under hela tidsperioden vilket tillsammans med tidigare nämnda delar peka på en fortsatt användning av psykologisk krigföring från Ryssland sida

Elektronisk krigföring har skett inom samtliga analyserade konflikter, dock utgjorde denna form en tyngdpunkt för Rysslands informationskrigföring under Georgienkriget varpå slutsatser gör gällande att detta beror på vilket motstånd som möts. Fortsättningsvis kommer Ryssland troligtvis att nyttja elektronisk krigföring som tillvägagångsätt inom informationskrigföring och beroende på vilket motstånd som möts kommer detta att göras större eller mindre utsträckning.

Underrättelsebaserad krigföring har visat sig som en negativ trend vilket då anses mindre troligt i framtida konflikter. Trenden inom *electronic based warfare* visar sig vara svagt stigande. Det utgör ingen tyngdpunkt inom konflikten vilket kan tänkas se ut på liknande sätt fortsättningsvis.

Analysen visar ej någon förändring inom hacker warfare, eftersom information kring detta varit näst intill obefintlig. I och med att ingen information funnits för denna undersökning angående hacker warfare går heller inga slutsatser att dras och författaren menar att vidare forskning krävs för att uttala sig om Ryssland nyttjande av denna form av informationskrigföring. En diskussion kring huruvida resultatet bedömts i denna undersökning följer nedan.

Rysslands användning av informationskrigföring har under tidsperioden 1999-2014 förändrats, där tyngdpunkten i konflikten med Georgien var inom elektronisk krigföring samt medan tyngdpunkten i övrig varit vid psykologisk krigföring. Det uppstår svårigheter att förklara en förändring i Rysslands nyttjande av informationskrigföring då tidsperioden endast är 15 år vilket möjligtvis inte kan ses som representativet för en längre tidsperiod. Givet undersökningens resultat beror Rysslands agerande på vilket motstånd som möts samt vilken typ av konflikt som är aktuell. Rysslands agerande har visat sig förändrat från varje konflikt, något som även kommer att fortsätta förändras för framtida konflikter. Rysslands brukande av informationskrigföring kan ha påverkats av yttre faktorer, som exempelvis konfliktens karaktär eller typen av motstånd, vilket är något som behöver beaktas vid beaktandet av undersökningens resultat.

Att resultatet av *hacker warfare* visat sig oförändrat kan bero på att denna form av informationskrigföring ej behandlas inom öppna källor. Detta medför att resultatet av undersökningen visar en utebliven förändring medan det i själva verket skett en förändring utan att detta redo-

visas i öppna källor. Eller så är det så att *hacker warfare* inte nyttjats under dessa tre konflikter, vilket författaren anses vara mindre troligt, dock utesluts inte alternativet av författaren då ytterligare forskning hade behövts för att besvara denna fråga.

5.3 Diskussion

5.3.1 Teori

Valet av Libickis teori som verktyg för undersökningen har varit väl motiverat genom hela processen på grund utav att den är heltäckande och tydlig för analysen. De sex former av informationskrigföring som är utvalda för analys ges en djupare granskning därav valet att nyttja dessa former. Eftersom Libickis teori och författarens tolkning av teorin genomsyrar hela undersökningen har således ett visst resultat framkommit. Hur detta har uppstått framgår inom författarens operationalisering, vilket skall möjliggöra för någon utomstående att replikera undersökningen. I och med att teorin inte utgjorde fokus i undersökningen utan endast var ett verktyg för analysen så blir valet av teori i det här fallet ej i fokus utan hur denna används utgör det primära.

5.3.2 Metod och material

Metodvalet som gjorts för undersökningen har styrts av att materialet som fanns att tillgå, där dessa endast utgjordes av textkällor. En kvalitativ textanalys var det självklara alternativet då en kvantitativ undersökning uteslöts på grund av den begränsade mängd empiriskt material samt arbetets omfattning, vilket har tagits hänsyn till vid samtliga val i undersökningen.

Källor som valts bort har varit på grund utav författarens obefintliga språkkunskaper inom det ryska språket. Ryska källor hade möjligen givit en ytterligare beskrivning till händelseförloppet i konflikterna vilket hade öka resultatens trovärdighet. Påverkan kan även ha skett genom nyttjande av andrahandskällor, där informationen som använts i undersökningen redan tidigare blivit analyserad. Problematiken är svår att undvika och bör tas i hänsyn vid iakttagande av undersökningens resultat.

Samtliga konflikter under de senaste 15 åren är analyserade vilket tar bort författarens inbladning för val av konflikter som skall analyseras vilket bibehåller en objektivitet i undersök-

ningen. Konflikternas olika karaktärer spelar då ingen roll eftersom samtliga konflikter är valda för analys.

5.3.3 Återkoppling till tidigare forskning

Tidigare forskning beskriver en förändring inom krigföringen samt Rysslands nyttjande av hybridkrigföring. Undersökningen bekräftar vad tidigare forskning gjort sig gällande, avseende en förändring inom informationskrigföringen kan utläsas. Förändringen är inte lika tydlig som tidigare forskning beskriver. Det undersökningen däremot gör är att den fyller på en lucka avseende en systematisk undersökning kring Rysslands förändring i nyttjande av informationskrigföring vilket är av vikt att förstå då Rysslands företag inom stora konflikter kan få påverkan på krigföringen i sin helhet. För att förstå sig på utvecklingen inom krigföringen är det av vikt att förstå sig på Rysslands förändrade tillvägagångsätt vilket denna undersökning bidrar till. Undersökningen bekräftar tidigare forskning som påstår att Ryssland använder sig av hybridkrigföring och att detta blir allt viktigare inom dagens konflikter, eftersom informationskrigföring utgör en del av hybridkrigföringen. Det har enligt Libickis sju former av informationskrigföring visat sig använts av Ryssland.

5.3.4 Forskningens betydelse för yrkesutövningen

En förändring i Rysslands agerande är viktigt att förstå sig på som officer i svenska försvarsmakten då Ryssland utgör en potentiell motståndare vid en konflikt. Finns en förståelse för hur utvecklingen i Rysslands agerande sett ut skapas möjlighet att förutspå kommande agerande. Enligt tidigare forskning visar sig hybridkrigföringen få en allt större betydelse inom ramen för dagens konflikter och därav ställs högre krav på dagens officerare att kunna förstå och tillämpa ny utveckling inom ramen för planering och genomförande. Undersökningen beskriver en förändring i Rysslands nyttjande av informationskrigföring vilket utgör en del av Rysslands användande av hybridkrigföring och bidrar till en förståelse för Rysslands agerande inom moderna konflikter och hur utvecklingen tett sig under modern tid. Det kan åskådliggöra vilken typ av attack som kan väntas i en konflikt med Ryssland och på så vis förutspå vilket typ av skydd som behövs för att klara av att försvara sig.

5.4 Fortsatt forskning

Vidare forskning avseende Rysslands förändrade agerande inom moderna konflikter är av vikt då Ryssland varit inblandade i de konflikter som ägt rum under modern tid. Fortsatt forskning krävs inom ämnet för att bredda förståelsen kring pågående utveckling samt för eventuellt framtida konflikter. Då informationskrigföring ses som en utjämnare mellan småstater och stormakter kan det vara intressant att utforska hur utvecklingen inom denna punkt har sett ut i en småstat, då större kraft kan tänkas läggas vid informationskrigföringen då detta är deras chans att utmana en stormakt. Denna undersökning saknar information avseende *cyber warfare* vilket är ett aktuellt ämne i dagens debatter huruvida detta nyttjats. Undersökningens omfattning medgav ej möjlighet att inkludera denna form av informationskrigföring, vilket är ett ämne vart efterföljande forskning kan fokuseras på. Även *hacker warfare* utgör ämne för vidare forskning då det finns en avsaknad kring detta i aktuell undersökning.

5.5 Slutord

Att analysera Rysslands brukande av informationskrigföring är ett komplicerat område som i sin tur medför en komplicerad analys. Det resultat undersökningen levererat är snarare vägledande än giltiga. Ett tydligare svar på frågeställningen förutspåddes av författaren kunna ges, dock utgör detta ett bidrag för en bredare förståelse för huruvida en förändring kan tydas utifrån Rysslands agerande. Att forska inom ämnet anser författaren är av stor vikt då kommande konflikter kommer att utspelas inom denna dimension, tillsammans med övriga delar av krigföringens dimensioner.

6. Litteraturförteckning

Källorna är redovisade enligt China Quarterlys insturktioner.

Asmus, Ronald. 2010. *A little war that shook the world: Georgia, Russia, and the future of the West*. Basingstoke: Palgrave Macmillan.

Backman Jarl. 2016. *Rapporter och uppsatser*, 3., [rev.] uppl., Lund: Studentlitteratur.

Barabanov, M., Boldenkov, D., Denisentsev, S., Kashin, V., Lavrov, A, Nikolsky, A., Tseluyko, V. 2014. *Brothers Armed: Military Aspects of the Crisis in Ukraine*. Moskva: East View Press.

Chekinov, Sergei och Bogdanov, Sergei. 2013. "*The Nature and Content of a new-generation war"*, Military thought, 10/2013. Vol. 22, no. 4.

Cornell, Svante & Starr, Frederick (red.) 2009. *The guns of August 2008: Russia's war in Georgia*, N.Y. M.E. Sharpe, Armonk.

Denscombe, Martyn. 2009 [1998]. *Forskningshandboken: För Småskaliga Forskningsprojekt Inom Samhällsvetenskaperna*. 2. Uppl. Lund: Studentlitteratur.

Efron, Vera. 2014. *Baltikum nästa!: så slukar Ryssland sina grannar : strategi, planläggning och verkställande.* Stockholm: Svenskt Militärhistoriskt Biblioteks Förlag.

Ejvegård, Rolf. 2003. *Vetenskaplig metod*, 3., [rev] uppl., Lund: Studentlitteratur.

Esaiasson, Peter, Gilljam, Mikael, Oscarsson, Henrik och Wängnerud, Lena (red), 2012. *Metodpraktikan.* 4., [rev] Uppl. Stockholm: Nordstedts Juridik AB.

Fejes, Andreas och Thornberg, Robert. (Red.), 2009. *Handbok i kvalitativ analys*. Stockholm: Liber AB

Franke, Ulrik, Norberg, Johan., Westerlund, Fredrik. 2014. "*The Crimea operation: Implications for future Russian military interventions*", I "*A rude awakening: Ramifications of Russian aggression towards Ukraine"*, Totalförsvarets forskningsinsitut, FOI-R--3892—SE.

Friman, Henrik, Sjöstedt, Gunnar & Wik, Manuel W. 1996. *Informationskrig: några perspektiv*, 1. uppl., Swedish Institute of International Affairs, Utrikespolitiska institutet, Stockholm.

Galeotti, Mark. 2016. "*Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?"* Small Wars & Insurgencies, 27:2, 282-301

Heickerö, Roland. 2010. "*Emerging cyber threats and Russian views on information warfare and information operations*" Totalförsvarets forskningsinstitut, FOI-R --2970--SE.

Hoffman, Frank. 2009. "*Hybrid warfare and challenges"*, NDU press, issue 52, 1st quarter.

Johannessen, Asbjörn och Tufte, Per Arne. 2003. *Introduktion till samhällsvetenskaplig metod*, Malmö: Liber AB.

"*Krisen i Ukraina på 60 sekunder*", publicerad 2014-02-28. Aftonbladet,
hämtad 2016-05-18.

Lavrov, Anton. 2010. "*Timeline of Russian-Georgian Hostilities in August 2008*". Pukhov, Ruslan (red.). I The tanks of August, 37-75. Moscow: Centre for Analysis of Strategies and Technologies

Libicki, Martin C. 1995. *What is information warfare?* Washington, DC: Institute for National Strategic Studies, National Defense University.

McDermott, Roger. 2015. *Brothers Disunited: Russia's Use of Military Power in Ukraine*, Kansas: The Foreign Military Studies Office, Fort Leavenworth.

Nichol, Jim. 2005." Bringing *peace to Chechnya? Assessments and implications*", CRS Report for Congress.

Oldberg, Ingmar, Holmertz, Gert och Lindahl, Ylva. 2014. ”*Putins revansch. rysk maktpolitik i Ukraina”*, Utrikespolitiska Institutet 4/2014.

Oliker, Olga. 2001 *Russia's Chechen wars 1994-2000: lessons from urban combat*, Californian: Rand, Santa Monica.

“*Phase One - The Air Campaign - September 1999*”. Publicerad 2011-11-07. Global security, hämtad 2016-05-18

“*Putin acknowledges Russian military serviceman were in Crimea, Russia Today*”, Publicerad 2014-04-17 Kl: 09.28. RT, Hämtad 2016-05-02.

“*Putin ready to invade Ukraine; Kiev warns of war*”, publicerad 2014-03-01. Reuters, hämtad 2016-05-18

“*Second Chechen war*”, publicerad 2015-05-10, Prezi, hämtad 2016-05-18

Tagliavini, Heidi. 2009. “*Independent International Fact-Finding Mission on the Conflict in Georgia*”, Report, volume I.

Thornton, Rod. 2015. “*The Changing Nature of Modern Warfare”*, The RUSI Journal, 160:4, 40-48.

”*Timeline: Chechnya*”, publicerad 2011-01-19 kl. 13:59. BBC News, hämtad 2016-04-28

Ventre, Daniel. 2009. *Information warfare*, London: ISTE Ltd.

Yin, Robert K. 2007. *Fallstudier: design och genomförande*, 1. uppl., Malmö: Liber AB