Lunds Universitet
Statsvetenskapliga institutionen

STVK03
VT22
Handledare: Christie Nicoson

Cyber (O)säkerhet

En studie kring internationella lagar, principer och förpliktelser gällande civilas säkerhet i cyberrymden med fokus på NATO:s säkerhetspolitik

Philip Ingemansson Müller
19990409-8119

Abstract

In the modern society the use of cyber technology is essential in many aspects. Both civilian infrastructure and crucial systems rely on cyber technology and its many uses. This new era in which cyberspace activities are a crucial part of society raises the question about how well preserved civilian cyber systems are in case of war, more specifically cyberwar. This study analyses how well NATO cyber politics follow the international law of protecting civilians based on the Just War theory. The study finds that NATO:s cyber politics generally follows the ambition of Just War theory but in particular cases falls short due to seemingly unfounded stiffness when applying existing international law to the new arena cyberspace has created. The study finds that these particular cases in which the manual falls short are crucial when answering the question if the ambition of Just War theory is achieved or not.

Keywords: Cyberrymden; Cyberoperationer; Cyberanfall; NATO; Just War Theory; Folkrätten

Antal ord: 8792

Innehållsförteckning

1. Inledning och bakgrund

Till en början, vad är cyberrymden? Det är nödvändigt i en uppsats som denna att tidigt klargöra vad som syftas på med exempelvis benämningen cyberrymd. En internationellt accepterad definition av cyberrymden finns inte idag, däremot kan det sägas vara den 'virtuella verkligheten'. I denna verklighet finns privatpersoner, företag, stater och andra organisationer som existerar genom digitalt informationsutbyte. I cyberrymden finns även datasystem som är väsentliga för att upprätthålla samhällsviktig infrastruktur såsom elnät, telefonnät och sist men inte minst internet. Cyberrymden växer för var dag som nya nätverk skapas och ju mer en nations samhällsfunktioner blir beroende av cyberrymden ökar också allvaret ifall en nation ställs inför ett potentiellt cyberanfall. Än så länge har inget (officiellt) cyberkrig mellan två stater ägt rum, vilket vilket innebär att konsekvenserna av ett cyberkrig ännu inte är klarlagda. Denna uppsats ämnar undersöka hur NATO (Nordatlantiska fördragsorganisationen) ställer sig i frågan om skydd för civila ifall ett cyberkrig bryter ut. Var normerna och gränserna för handlande inom cyberrymden dras är än så länge oklart, detta illustreras nedan med hjälp av två uttalanden som påvisar oklarheten i cyberrymden.

"*There is a big difference between China wanting to figure out [...] what my talking points are when I'm meeting with the Japanese. Which is standard fare [...]. There is a big difference between that and a hacker directly connected with the Chinese government or the Chinese military breaking into Apple's software systems to see if they can obtain the designs for the latest apple product. That's theft. We can't tolerate that*"

- Barack Obama (Obama, 2013)

Som sittande president var Barack Obama den första som ansåg cyberrymden som en strategisk nationell tillgång och skapade en division inom pentagon kallad ‘Cybercom’. Genom läckta dokument från NSA (National Security Agency) framkom det att denna avdelning bland annat involverade sig i offensiva cyberoperationer. I samband med detta kom uttalanden från Storbritannien att investeringar inom cyberoperationer bör göras och NATO presenterade ‘The Tallinn Manual’ vars syfte är att etablera normer inom den nya cyber arenan som började ta form (Robinson, 2015. s. 70). Av citatet ovan framförde Obama en gränsdragning mellan vad som kan anses som ‘fair game’ och något som bryter respekterade lagar. Detta citat belyser gråzonen som uppsatsens syfte vill illustrera, nämligen var ‘fair game’ gränsen avslutas och lagen börjar.

Edward Snowden var en före detta CIA-anställd inom NSA och är numera känd som en visselblåsare efter att ha läckt sekretessbelagda dokument vars innehåll antydde att USA övervakar sina medborgare och tillsammans med Storbritannien trängt sig in i delegaters e-mails och avlyssnat telefonsamtal i samband med G20-mötet i London 2009 (SvD, 2013. Berger & Salö, 2013). Snowden förmedlar budskapet av hur en dystopisk framtid står inför oss ifall cyberrymden fortsätter vara en laglös arena enligt honom:

“We find out in 2013 that they [Obamas regering] have used this provision [Section 215 of the Patriot Act] [...] to [...] get the phone records of not an individual, not a group, but everybody in the United States who was making calls on US telecommunications providers, delivered to the NSA daily by these companies [...]. So no matter who you are, no matter how innocent you were, the FBI was getting these because they said, ‘well, every phone call is relevant to a counter teorrorism investigation’ and the court went [...] ‘If your definition of relevance is basically anything anywhere all the time is relevant to a counter terrorism investigation, the question is what then is not relevant? What is the limiting principle on this? Where is the end?’

- *Edward Snowden (Snowden, 2020)*

Snowdens kommenterar är en viktig insikt i diskussionen som pågår inom cyberrymden, där vi å ena sidan har en president som berättar om var gränser och normer finns och å andra sidan Snowden som menar att konstitutionella lagar förbises och kryphål utnyttjas till den grad att inga gränser verkar finnas alls. Oavsett var på det politiska spektrumet man står, krig eller fredstid, offensiv cyberkrigföring eller passivt insamlande av data belyser båda citaten kraven på reglering men också hur svår gränsdragningen är att göra.

1.1 Syfte och forskningsfråga

I takt med att samhället moderniseras och våra liv förflyttas till en mer digital plats socialt, ekonomiskt och privat görs det alltmer tydligt att en ny paradigm är i full gång. När ett nytt paradigm tar plats tillkommer även nya normer, frågor och situationer som tidigare inte funnits. En väl etablerad överenskommelse världen över är att civila bör skyddas i krig, men hur bör denna princip appliceras i den nyetablerade cyberarenan? NATO har publicerat en manual för hur ett land bör tänka och agera kring cyberkrigföring och civilas roll i sådana situationer. Denna uppsats analyserar NATO:s Tallinn Manual och överlägger hur väl den skyddar civila och vilka gränsdragningar som görs.

Forskningsfrågan som uppsatsen ämnar att besvara är:

Hur väl upprätthålls principen om skydd för civila i NATO:s cyberpolitik i enlighet med Just War teorins principer?

1.2 Avgränsningar

Uppsatsen behandlar endast delar av NATO:s Tallinn Manual som handlar om civilas säkerhet under krig. Det kommer därmed inte lyftas fram andra delar av manualen där möjliga skiljaktigheter mellan Just War teorin och manualen föreligger. Uppsatsen kommer inte ta upp delar av Just War teorin som behandlar rättfärdigande av krig (jus ad bellum). Detta är för att hålla sig inom forskningssyftet vilket är principer som gäller civilas säkerhet när krig redan är igång (jus in bello).

Det finns ett flertal föredrag och internationella riktlinjer för hur krig bör utföras. De fördrag och arbeten som beaktas i denna uppsats är de som anses vara mest centrala med hänsyn till uppsatsens syfte. I och med att fokuset ligger på att analysera NATO:s cyberpolitik anses västerländska doktriner och föredrag rimliga att presentera då NATO utgörs av västerländska länder och präglas av västerländsk politik. Den filosofiska grunden utgörs av Just War teorin och den juridiska grunden utgörs av folkrätten, specifikt internationell rätt.

1.3 Struktur

Just War teorin är en moralfilosofisk teori som är tongivande för folkrättens utformning och de lagar som idag ramar in hur en krigförande stat bör handla i krig. Uppsatsen använder denna teori som grund för att ge läsaren en övergriplig bild av vad våra krigslagar grundas i och visar de moraliska rötter som våra lagar och regler är skapta för att upprätthålla. För att konkretisera Just War teorin från en moralfilosofisk ansats till specifika användningsområden används folkrätten.

Folkrätten innehåller regler, konventionslagar och överenskommelser som är internationellt accepterade och återspeglar Just War teorins ambitioner. Folkrätten kommer sedan användas för att agera bollplank mot NATO:s Tallinn Manual för att föra ljus över och analysera hur väl Tallinn Manualen upprätthåller de ambitioner och principer Just War och folkrätten eftersträvar att hålla vid liv, vilket är civilas säkerhet i krig.

2. Teori

2.1 Just War Theory

Teorin Just War presenterar två huvudområden: jus ad bellum och jus in bello. Varav det förstnämnda behandlar rättfärdigande av krig och det sistnämnda diskuterar förhållningsregler under krigets gång (Viner, 2013. s. 49). Denna uppsats kommer rikta in sig på endast jus in bello perspektiv då skydd för civila blir aktuellt när attacker utförs. Teorin är en moralfilosofisk grund för krigslagars utformning i modern tid samtidigt som Just War teorin sträcker sig långt bak i historieböckerna. Genom dess relativt abstrakta principer skapas övergripliga normer som kan anpassas till krigscenarion förr i tiden likväl nu.

Just War teorins definitiva ursprung är inte helt tydligt. Man kan spåra de första formuleringarna bak till 400-talet och biskopen Augustinus skrifter från den kristna läran, däremot pekar mycket mot att en etablering av förhållningsregler i krig spred sig under denna tid bland flera kulturer runt om i världen. En gemensam formulering som tycks vara kulturernas gemensamma nämnare är att inget krig bör startas utan rimlig anledning. Under 300-talet formulerade även indiska filosofer humanitära regler under krig vilket går att likna med dagens internationella lagar (Karoubi, 2004. s. 58-59).

Som senare visas i uppsatsen finns tydliga kopplingar mellan Just War teorins principer och de lagar som framkommer i folkrättsliga konventioner. Just War teorin är av sin natur en övergriplig teori vars syfte är att skapa en grund för hur vi bör tänka i krig för att minimera onödigt lidande. Då den är den första av sin art är det en konstant källa till vad vi idag grundat våra lagar i, bland annat folkrätten.

2.1.1 Jus in bello

Det finns två kriterier inom jus in bello området av Just War teorin. Den första är 'diskriminering' och är en fundamental princip som innebär att under krig får inte en part medvetet attackera oskyldiga (i senare avsnitt av uppsatsen kommer detta tas upp under namnet distinktionsprincipen). Ett viktigt förtydligande är att attacken framförallt inte får vara med avsikt mot civila. Detta leder oss in till andra kriteriet som är 'proportionalitet', vilket innebär att operationen inte ska göra mer skada än nytta. Den eventuella skadan som en militäroperation kan åstadkomma måste vägas mot nyttan av det övergripliga militära målet (Guthrie & Quinlan, 2007. s. 14). Ett klassiskt exempel som gett upphov till diskussion är USA:s användning av atombomber mot Japan, där målet var att avsluta Japans offensiv och därmed även avsluta andra världskriget. Huruvida målet att avsluta ett världskrig (militär fördel) kontra den skada mot civilbefolkningen (skadan) som atombomberna orsakade (och orsakar än idag) var rättfärdigat kan exempelvis diskuteras med hjälp av Just War teorins principer.

2.1.2 Problematiska områden inom teorin

Just War teorin är av hög abstraktionsnivå vilket är rimligt då den är tänkt att vara en ledstjärna för hur alla krig framöver ska inledas och genomföras. Däremot leder denna

abstraktionsnivå till viss tänkbar problematik i fallet av cyberoperationer. Mariarosaria Taddeo (2012) är en filosofiskt inriktad professor på Oxford Internet Institute med expertis inom cybersäkerhet och argumenterar för att Just War teorins ambition vilar i att undvika skador och att krig ska undvikas så långt det går. En tolkning av Just War teorin blir då att cyberanfall bör göras i så stor utsträckning som möjligt då det är en krigsmetod som resulterar i mindre fysisk skada än traditionell krigföring med fysiska vapen (Taddeo, 2012. s. 213).

Ifall en sådan tolkning av Just War teorin görs följer det att fysisk skada alltid bör undvikas till allra högsta grad och att det då ligger i linje med Just War teorins principer att exempelvis övervaka och samla in känslig data inom en population (skada) för att kunna urskilja vilka som döljer sig som civila men egentligen är rättfärdigade militära mål (militär fördel). Även om det kan argumenteras att detta kränker privata rättigheter bland civila och äventyrar med civilas säkerheter i cyberrymden menar Taddeo att det kan rättfärdigas. (Taddeo, 2012. s. 213-214).

Ytterligare problematik som Taddeo lyfter upp är att en övergång från Just War teorins principer och direkt tillämpning på cyberoperationer inte är idealt då Just War teorin inte gjordes med cyberoperationer i åtanke. Att utesluta Just War teorin i cybersammanhang menar Taddeo är ett misstag. Hon framför att Just War teorin kan agera som en grund för att etablera nya normer och etik inom cyberrymden genom regelverk som tar hänsyn till cyberrymdens särskilda egenskaper (Taddeo, 2012. s. 218).

3. Metod och material

3.1 Forskningsdesign

Uppsatsens utformning är en fallstudie med ambitionen att vara teoriprövande. Analysen görs på NATO:s Tallinn Manual och analyseras med hjälp av folkrätten som grundas i teorin Just War. Uppsatsen har inom- och utomvetenskaplig relevans på flera områden. Den har inomvetenskaplig relevans då den utgår från en av de centralaste krigsteorierna i västliga doktriner och ser hur våra folkrättsliga principer översätts i nya arenor såsom cyberrymden. Den utomvetenskapliga relevansen finner vi då området studien behandlar är civilas säkerhet under krig. Uppsatsen kommer försöka belysa områden där civilas säkerhet tycks saknas och erlagda principer såsom ‘skydda civila i krig’ brister. Intresset för sådan information sträcker sig längre än akademiska gränser då ett antagande görs att civila vill veta vilka tänkbara skador som kan ske ifall cyberkrig bryter ut. Detta gör att uppsatsen har en tydlig utomvetenskaplig relevans (Teorell & Svensson, 2007. s. 18-19).

Den epistemologiska infallsvinkeln för uppsatsen faller i ett konstruktivistiskt synsätt då definitionen av krig ses på ett sätt som inte är fast utan förändras över tid beroende på omvärldens utveckling och vår syn på den. Det kan ha funnits en tid då krig var soldat mot soldat och då var det exempelvis rimligt att räkna i antalet omkomna för att avgöra ifall ‘krig’ pågår eller inte. I dagsläget är detta inte nödvändigtvis hur krig ser ut vilket uppsatsen kommer beröra i diskussionsavsnittet.

Fallet är NATO:s Tallinn Manual som är en manual för hur cyberoperationer ska göras i enlighet med folkrätten. Folkrätten används i uppsatsen som analyseringsverktyg för att förstå hur Just War teorin, som folkrätten grundar sig på, tar sig form i praktiken. Det kommer i resultatet framgå hur manualen valt att tolka folkrätten och det kommer i diskussionsavsnittet diskuteras hur väl Just War teorins ambitioner applicerats på manualen genom att folkrätten och Tallinn Manual jämförs.

Material som används är både primär- och sekundärkällor. Gällande material för NATO:s cyberpolitik används primärkällan Tallinn Manual som är uppsatsens analysobjekt. I framförandet av folkrätten och dess principer används Sveriges försvarsdepartements skrifter för att få en god och gedigen överblicksbild av folkrätten. Gällande Just War teorin används olika forskares beskrivningar av Just War teorin då det inte finns en specifik primärkälla för teorin i helhet. Forskarna vars publiceringar uppsatsen använt har expertis inom de ämnen som uppsatsen behandlar, exempelvis cybersäkerhet och Just War teorin. Detta gör att materialet som framförs i uppsatsen har god vetenskaplig förankring och stor trovärdighet trots att inte endast primärkällor används. En tänkbar nackdel med uppsatsen är att materialet saknar internationell spridning, de flesta källor hämtas från västerländskt präglade läror. Däremot argumenterar jag för att detta är till fördel för uppsatsen då det är västerländsk politik som ska granskas med hjälp av västerländsk moralfilosofisk infallsvinkel.

3.2 Definitioner

I och med att denna uppsats navigerar i ny teknik och moderna fenomen finns potentiella oklarheter som läsaren kan stöta på. Exempelvis i talan om ‘anfall mot civila’ som denna uppsats behandlar syftar inte detta nödvändigtvis på fysisk attack utan ‘digital’ skada. För att

undvika dessa syftningsfel kommer denna del av uppsatsen förklara och gå igenom grundläggande begrepp så att läsaren tolkar begrepp på samma sätt som uppsatsen menar.

Då cyberrymden är ett relativt nytt begrepp råder det inte internationell konsensus kring en gemensam uppfattning av vad exempelvis en cyberoperation innebär. Denna uppsats kommer använda samma innebörder av begreppen som analysobjektet gör. Det är därmed NATO:s Tallinn Manual:s definiering av cybertermer som kommer presenteras nedan.

3.2.1 Cyberrymden

NATO:s Tallinn Manual beskriver ‘cyberspace’ (på svenska cyberrymden) enligt följande: “The environment formed by physical and non-physical components, characterized by the use of computers and the electro-magnetic spectrum, to store, modify, and exchange data using computer networks”. Cyberrymden beskrivs som ett begrepp med foten i både den fysiska och icke-fysiska världen och att en dator är ett nyckelobjekt för att få tillgång till cyberrymden (Schmitt, 2017. s. 258).

3.2.2 Cyberoperation

NATO:s Tallinn Manual beskriver ‘cyber operation’ (på svenska cyberoperation) som “The employment of cyber capabilities to achieve objectives in or through cyberspace …]” (Schmitt, 2017. s. 564). Cyberoperation används alltså som ett brett samlingsnamn för alla handlingar som görs med hjälp av cyberteknik i cyberrymden, exempelvis ingår cyberanfall i cyberoperation. Däremot täcker termen cyberoperation fler områden än endast cyberanfall.

3.2.3 Cyberanfall

NATO:s Tallinn Manual beskriver ‘cyberattack’ (på svenska cyberanfall) som “A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects” (Schmitt, 2017. s. 415). Denna definition inkluderar kriterier för vad som skiljer en ordinarie handling i cyberrymden och vad som är att anse som en attack, såsom förväntad skada och död mot personer eller skada mot objekt.

3.3 Folkrätten

Detta avsnitt presenterar internationell rätt, specifikt folkrätten, vilket är den del av internationell rätt som reglerar krigsregler.

3.3.1 Den internationella humanitära rätten (humanitära rätten)

Folkrätten tar sin form i två delar. Ena är den internationella humanitära rätten (fortsättningsvis humanitära rätten) vilket även kallas ‘krigets lagar’. Den andra är mänskliga rättigheter som behandlar relationen mellan stat och enskild medborgare. Sveriges stat har ratificerat båda konventionerna och är därmed bunden att följa den internationella rätten. Uppsatsen kommer endast presentera humanitära rätten då det är den delen som gör sig relevant i krig.

Definitionerna som humanitära rätten använder sig av kan skilja sig från NATO:s Tallinn Manual, dessa skillnader kommer tas upp i senare avsnitt. Folkrättens definitioner är däremot relevanta att ta upp i detta skede. Den humanitära rätten definierar anfall enligt följande:

“varje våldshandling mot motståndaren, oberoende av om handlingen är offensiv eller defensiv” (Lindvall, Tengroth och Clomén, 2017. s. 12). Humanitära rätten definierar väpnad konflikt av typer (i) internationell väpnad konflikt och (ii) icke-internationell väpnad konflikt. Den förstnämnda (i) innebär strid mellan två eller fler länder och att väpnat våld är involverat. Den senare typen (ii) syftar till “[...situationer då våldshandlingar av en viss intensitet förekommer regelbundet mellan en stats väpnade styrkor och icke-statliga organiserade väpnade grupper, eller mellan sådana väpnade grupper” (Lindvall, Tengroth och Clomén, 2017. s. 8).

Explicit blir humanitära rätten applicerbar under väpnad konflikt och huruvida cyberoperationer, exempelvis cyberanfall, kan anses som väpnad konflikt är inte framlagt och tas upp i senare avsnitt i uppsatsen.

Grundläggande lagar inom humanitära rätten är följande:

> 1. Personer som är försatta ur stridbart skick och de som inte tar direkt del i fientligheter har rätt till respekt för sina liv och sin fysiska och moraliska integritet. De ska under alla omständigheter skyddas och behandlas humant utan någon otillbörlig åtskillnad.
>
> 2. Det är förbjudet att döda eller skada en fiende som ger upp eller är försatt ur stridbart skick.
>
> 3. Sårade och sjuka ska omhändertas och vårdas av den part i konflikten i vars våld de befinner sig. Sjukvårdspersonal, sjukvårdsinrättningar,

transporter och materiel omfattas också av skydd. Emblemen det röda korset, den röda halvmånen och den röda kristallen är tecken för sådant skydd och ska respekteras.

4. Tillfångatagna stridande och civila som befinner sig i fiendens våld har rätt till respekt för sina liv, sin värdighet, sina personliga rättigheter och övertygelser. De ska skyddas mot alla former av våld och repressalier. De ska ha rätt att korrespondera med sina familjer och att motta hjälp.

5. Var och en ska ha rätt till grundläggande rättsliga garantier. Ingen ska hållas ansvarig för gärningar han/hon inte har begått. Ingen ska utsättas för fysisk eller psykisk tortyr, kollektiv bestraffning eller grym eller förnedrande behandling.

6. Parterna i en konflikt och medlemmar av deras väpnade styrkor har inte obegränsad rätt att välja stridsmetoder eller stridsmedel vid krigföring. Det är förbjudet att använda vapen eller stridsmetoder som orsakar överflödig skada eller onödigt lidande.

7. Parterna i en konflikt ska alltid skilja mellan civilbefolkningen och stridande för att skona civilbefolkningen och civil egendom. Varken den civila befolkningen eller enskilda civila personer får anfallas. Anfall får endast riktas mot militära mål (Lindvall, Tengroth och Clomén, 2017. s. 4)

Punkt 6 (proportionalitetsprincipen) och punkt 7 (distinktionsprincipen) är signifikant för uppsatsens syfte och kommer därför kommenteras djupare. I humanitära rätten beskrivs civila objekt som bostäder, sjukhus och historiska monument. Det tilläggs även att infrastruktur som anses nödvändig för civilas överlevnad inte får anfallas, som exempel ges infrastruktur som ansvarar för elförsörjning (Lindvall, Tengroth och Clomén, 2017. s. 7-10). Punkt 7 förklarar hur en stat principiellt ska kunna skilja på civila och militära mål. Anfall av ett militärt mål anses rättfärdigat ifall det innebär en militär fördel för den stridande parten. Konventionen diskuterar förbud mot anfall som i sin metod inte tar hänsyn till ifall målet är civilt eller militärt. Exempelvis diskuteras urskillningslösa situationer såhär: "En konsekvens av distinktionsprincipen är att det är förbjudet att kriga på ett sätt som har urskillningslösa effekter, t.ex. genom att använda stridsmetoder eller vapen som inte kan göra åtskillnad mellan de som deltar och de som inte deltar i striderna och därför drabbar såväl militära mål som civila och civil egendom utan urskillnad (t.ex. mattbombningar)" (ibid s. 7-10). Vidare kommenteras att civila i vissa fall kan vara mål i krig trots principen, detta då civila kan befinna sig i närheten av ett anfall eller militärt mål. I sådana situationer blir proportionalitetsprincipen tillämpbar och en avvägning mellan ett strategiskt militärt mål och eventuella skador som kan uppstå mot civila måste göras. Vad som avgör gränsen återspeglas i den militära fördelen som anfallet kan generera: "Den förväntade militära fördelen måste jämföras med andra konsekvenser av handlingen, såsom den ofördelaktiga påverkan på civila eller civila objekt. Detta innefattar att väga de fördelar som en framgångsrik insats skulle innebära mot de möjliga skadliga effekterna på skyddade personer och objekt" (ibid s. 11). En tredje princip som aktualiseras i samband med anfall är försiktighetsprincipen som innebär att en stat ska i allra högsta grad försöka minska skador mot civila (ibid s. 11).

I den fjärde Haagkonventionen från år 1899 upprättades en klausul inom folkrätten som heter Martensklausulen. Denna klausul är gjord då det anses omöjligt att täcka alla tänkbara scenarion i krig. Vid fall då folkrättsliga regler saknas ska ‘humanitära beaktanden’ göras och detta ger utrymme för att nya normer inrättas och folkrätten fortsätter därmed utvecklas för att passa in i samhällsutvecklingen. (Krigets lagar, 2010. s. 27)

4. NATO

4.1 NATO och Tallinn Manualen

North Atlantic Treaty Organisation (NATO) är en internationell institution som är en militärallians och skapades år 1949. I skrivande stund är 30 länder med i NATO, bland annat Storbritannien, USA och Frankrike. NATO:s syfte är att ge medlemmar politiskt och militärt skydd genom fredsbevarande insatser ifall kriser uppstår och förmedla demokratiska värderingar (Nato, 2020).

Det är NATO:s Tallinn Manual 2.0 som används för att presentera NATO:s cyberpolitik. Tallinn Manual 2.0 är en uppdaterad version från dess första publicering. Innehållet från Tallinn Manual 1.0 återspeglas i andra versionen och innehåller tillägg som nyanser och klargör vissa delar (Jensen, 2017. s. 737).

NATO:s Tallinn Manual består av flertal regler som behandlar hur internationella föredrag och principer, såsom humanitär rätt, bör appliceras i operationer inom cyberrymden. Manualen tar, genom sin internationella panel av experter, fram områden och scenarion för att diskutera hur lagar bör appliceras inom cyberrymden. Vidare utvidgar även manualen begrepp från folkrätten för att anpassas dem till cyberrymden. Manualen tar även upp

situationer där experterna inte är överens om hur en folkrättslig princip bör tillämpas. Med jus in bello perspektiv kommer de relevanta reglerna (de regler som berör civila i manualen) presenteras. Diskussioner och oenighet mellan experterna kommer också framföras. Det bör även tilläggas att manualen har innan publicering tillåtits läsas och kommenteras av fler än 50 stater för inflikning och kommentering. Bland annat har alla de permanenta medlemmarna i Förenta Nationernas säkerhetsråd tagit del av manualen och delat sin åsikt där de ansett att det varit nödvändigt innan publicering. Dessa länder är Kina, Frankrike, Ryssland, Storbritannien och USA (Jensen, 2017. s. 739-740).

4.2 Civil status i cyberrymden

De regler som presenteras av experterna gällande synen på vad ett civilt tillstånd inom cyberkrig presenteras i regel 29: “Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate.” Vad som anses vara ‘participating’ (delaktig) är i detta sammanhang väsentligt då det är delaktigheten som avgör ifall skyddet för en civil finns eller inte. Manualen använder som exempel en patriotisk hackare som vid konflikt bestämmer sig för att anfalla fienden med offensiva cyberoperationer. I detta fall anses den civila förlora sin civila status och förlorar därmed sitt civila skydd (Schmitt, 2017. s. 104-105).

Vad som definieras som cyberanfall har tidigare tagits upp, och kommer i denna del tas upp med fokus på hur ett cyberanfall på civila kan se ut och tolkas. Regel 30 beskriver definitionen av cyberanfall som följande: “A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects”. Experterna diskuterar en rad olika saker gällande denna

regel, framförallt tre väsentliga punkter såsom (i) avsikt (cause) med attacken, (ii) konsekvenser av attacken och (iii) när en attack anses vara en attack.

Då cyberanfall ter sig i en annan form än en fysiska anfall ligger fokus inte helt på (i) avsikten enligt manualen. Ett cyberanfalls avsikt kan vara att skada ett system, men manualen gör tydligt att det snarare är fokus på vilka tänkbara skador som kan skapas som (ii) konsekvens av anfallet. Exempel som tas upp är ifall ett SCADA-system (system för övervakning och styrning av processer) attackeras vilket resulterar i översvämning av en damm jämförs med att samma damm attackeras med sprängmedel. Båda är att anse som likvärdiga attacker även om cyberanfallets direkta avsikt är en attack mot ett system snarare än dammen i sig, medan sprängmedlets avsikt är direkta mot dammen. Alltså är konsekvenserna väsentliga att ta hänsyn till i ett cyberanfall (Schmitt, 2017. s. 107).

Huruvida (iii) ett anfall ska anses vara ett anfall råder det oenighet om bland experterna då å ena sidan vissa experter menar att fysisk skada på viktiga delar av ett system (komponenter) som i sin tur kommer behöva bytas ut innebär att ett anfall skett, lägger å andra sidan vissa experter vikt på funktionaliteten av systemet. Ifall ett system inte drabbats av fysiska skador på komponenter men funktionaliteten drabbas menar vissa experter att en attack har skett. Exempel som togs upp är ett scenario där email-kommunikationskanaler slås ut i ett cyberanfall (där komponenter hålls intakta från fysisk skada) vilket skulle leda till extrem förlamning i ett samhälles kommunikation. Panelen slog fast att det skulle anses vara ett cyberanfall, men att humanitära lagar inte kan appliceras på ett sådant scenario på grund av att fysisk skada inte förekommit, endast vissa relevanta delar kan argumenteras tillämpas enligt experterna (Schmitt, 2017. s. 108-109).

4.3 Distinktion- och proportionalitetsprincipens i cyber sammanhang

I den fysiska världen finns en tydlighet i vad som är militärt och vad som är civilt medan i cybervärlden rubbas denna tydlighet i ett flertal sammanhang. Att skjuta ner ett militärplan som i kraschen kan skada civila är en situation där tydlig överläggning är möjlig, planet kan distinktivt urskiljas från civilt till militärt, och en proportionell avvägning av vinst kontra förlust med hänsyn till civil skada kan göras. Däremot i cyberoperationer där en USB-sticka med virus planteras i en dator för att få tillgång till känslig information är en betydligt svårare situation att överväga gällande vilka och hur civila kan drabbas samt ifall systemet som infiltreras är sammanlänkat med civilt eller militärt nätverk. Denna del kommer presentera hur NATO och dess manual tar sig an denna fråga.

4.3.1 Proportionalitetsprincipen i Tallinn Manualen

Regel 51 i manualen behandlar specifikt när proportionalitetsprincipen blir tillämplig och lyder enligt följande: “A cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited”. Experterna beaktar att cyberoperationer vanligtvis inte medför skador likt regeln beskriver, utan snarare kan cyberoperationer skapa irritation, stress och rädsla (moralisk skada). Sådant lidande utgör inte tillräckligt med skada mot civila för att proportionalitetsprincipen ska bli applicerbar, däremot är experterna ense om att cyberanfall som resulterar i funktionsförlust för väsentliga system möjligtvis aktualiserar proportionalitetsprincipen beroende på situationen (Schmitt, 2017. s. 159-160).

Gällande proportionalitetsprincipen kommer en majoritet av experterna fram till en gemensam tolkning av tillämpning vilket är en avvägning mellan förväntad skada mot civila kontra ‘concrete and direct’ militär fördel. Det görs tydligt att det inte är en matematisk fråga såsom ‘10 civila datorer får attackeras till fördel av 11 militära datorer’, utan snarare att ett cyberanfall anses rättfärdigad ifall fördelaktigheter är substantiella och gynnar militären tätt i samband med cyberoperationen (Schmitt, 2017. s. 161-162). Regel 54 kartlägger hur ett cyberanfall bör utföras. Det framgår tydligt att minimal skada mot civila alltid ska prioriteras och att inför ett cyberanfall ska alternativa vapen även beaktas för användning (Schmitt, 2017. s. 168-169).

Regel 39 lyder enligt följande: “An object used for both civilian and military purposes - including computers, computer networks, and cyber infrastructure - is a military objective”. Denna regel är gjord för att förtydliga gråzonen som kan ske i civil och militärt sammanflätade objekt. Som regeln lyder är sammanflätade objekt att anse som militära, däremot appliceras proportionalitetsprincipen ifall ett objekt är både civilt och militärt. Diskussion bland experterna sker ifall ett cyberanfall mot exempelvis sociala medier är befogat och ifall sociala medier utgör ett tänkbart militärt objekt. Frågan ställs ifall ett anfall mot sociala medier leder till militär fördel, och ifall det är civilas moral som skadas eller ifall fysiska skador kan ske. Ifall det endast är civilas moral som skadas och en militär fördel finns anses sociala medier vara ett militärt objekt som får attackeras. Det lyfts då upp att hela internet kan isåfall anses vara ett militärt objekt. Alla experter var överens att en situation där hela internet blir anfallet är extremt osannolikt, istället bör fokus ligga på specifika anfall på delar av internet i frågan av militära objekt (Schmitt, 2017. s. 134-136).

4.3.2 Distinktionsprincipen i Tallinn Manualen

I sammanhang där frågan lyfts upp ifall ett objekt är civilt eller inte används folkrättens definition av militära objekt: “Those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the the circumstances ruling at the time, offers a definite military advantage” (Schmitt, 2017. s. 126). Experterna ställs inför frågan ifall ‘data’ utgör ett militärt objekt och är oense i frågan. Data är att tolkas som observationer av handlingar vilket kan användas som information om någon eller något. Majoriteten av experterna ansåg att data är inte att anse som ett objekt då data inte finns fysiskt. Minoritet av experterna ansåg att ifall ett cyberanfall mot känslig data skulle ske är det att anse som ett kritiskt anfall. Vissa experter ansåg att inte beakta data som ett potentiellt civilt objekt kan medföra konsekvenser där civila drabbas utan att anfallaren ställs till svars för att bryta mot humanitära rättens principer vilket leder till ett potentiellt kryphål i lagen. Det ansågs slutligen att data inte bör klassificeras som ett objekt i manualen (Schmitt, 2017. s. 27).

Vidare finns problematik kring sammanflätning av militära och civila. Regel 33 i manualen behandlar ifall det står sig tveksamt (doubtful) ifall en person är civil eller inte bör den betraktas som en civil vilket är i linje med humanitära rätten tolkning. En diskussion bland experterna och kommentar från Storbritannien görs gällande om vilken grad av tveksamhet som måste vara uppnådd för att lagen ska träda i kraft. Manualen gör tydligt att en tydlig gräns inte finns: “Whether the precise threshold of doubt necessary to bring the rule into play, it is clear that the mere existence of some doubt is insufficient to establish a breach” (Schmitt, 2017. s. 114-115). Manualen hänvisar till att inom cyberrymden är det oklart ifall någon är militär eller civil både på grund av att cybersystem som används ofta av militära och civila

aktörer samtidigt samt att individer inte är fysiskt synliga vilket gör det svårt att avgöra (ibid s. 115).

Regel 37 och 38 är lik Regel 33 då den nyanserar ifall objekt som är civila får utsättas för cyberanfall i vissa fall (Schmitt, 2017. s. 124). I Regel 38 förklaras att civila objekt är de som inte är militära objekt. Däremot, när ett objekt slutar vara civilt och blir militärt diskuteras enligt följande: "[... If a party to the conflict uses a certain civilian computer network for military purposes, that network loses its civilian character and becomes a military objective". Vidare exemplifieras detta med ett fysiskt exempel där en tågräls används av civila och då anses tågrälsen vara ett civilt objekt fram till att militären använder tågrälsen. Ett annat exempel är ifall TV-stationer ändras till att sprida militär information. I sådana fall blir TV-stationen ett militärt objekt (Schmitt, 2017. s. 128-129). Diskussion inleddes ifall email- och telefon kommunikationssystem är att anse som militärt objekt då militärens personal använder dessa för att exempelvis betala räkningar samt prata med sin familj och vänner vilket inte är relaterat till militära handlingar, utan civila oskyldigheter. En majoritet ansåg att det inte låg i enlighet med proportionalitetsprincipen att anse att objekt i det sammanhanget bidrar till en tydlig militär fördel, vilket är ett kriterium för att ett föremål får anfallas. En minoritet menar däremot att ett förstörande av sådan kommunikation skadar fiendens moral och inte tillbringar fysisk skada vilket leder till militär fördel och därmed anser de att email- och telefonfunktioner bör anses som militära objekt. Den slutgiltiga dragningen som görs enligt manualen är: "All experts concurred that if the civilian email services are being used to transmit military useful information, the infrastructure used to transmit them is a military objective" (Schmitt, 2017. s. 133). Vilken typ av infrastruktur som syftas på eller hur lagen tillämpas ifall andra kommunikationsled än email och telefon används kommenteras inte.

5. Resultat

NATO:s Tallinn Manual gör flera avtramp och gränsdragningar gällande vad som räknas som civilt anfall, civilt objekt och när gränsen görs då folkrätten och dess principer blir aktuella. I detta avsnitt kommer det tydliggöras var manualen och dess experter ansett denna gräns gå och vilka faktorer som experterna anses vara till vikt i resonemangen samt beslutsfattandet.

Genom att kartlägga hur distinktionsprincipen, proportionalitetsprincipen och när folkrättens principer blir aktuella enligt manualen kommer detta avsnitt lägga grund för en diskussion i nästa avsnitt. Det bör göras tydligt att detta avsnitt samt diskussionen är av mer normativ ansats. Exempelvis kommer det experterna gjort tydligt om vad som varit väsentliga faktorer för deras beslutsfattande i en viss fråga framföras, det kommer även motiveras i vissa fall var gränsdragningar har tycks dragits utan att en explicit kommentar från experterna gjorts, när sådana antaganden görs kommer det framgå i texten.

5.1 Humanitär rätts applicerbarhet enligt NATO:s Tallinn Manual

5.1.1 Humanitär rätt och manualens syn på beväpnad konflikt

Folkrätten är den mest centrala konventionen som upprätthåller principen för civilas skydd och anses bli aktuell när beväpnad konflikt äger rum. Ifall beväpnad konflikt inte äger rum görs konventionen inte applicerbar på situationen. Manualen anser att cyberoperationer ingår i humanitära rättens ‘armed conflict’ (Schmitt, 2017. s. 75). Detta leds in till diskussionen vad som anses vara ett anfall och manualens experter anser att fysiska skador (exempelvis på ett systems komponenter) är ett krav för att en cyberoperation ska anses som ett anfall. Panelen ansåg att funktionella skador, oavsett om det är till följd av fysisk skada eller inte, inte

uppfyller krav för att åberopa humanitär rätt i sin helhet, istället anses funktionella skador möjligtvis framkalla relevanta delar av humanitära rätten.

5.1.2 Humanitär rätt och manualens syn på distinktionsprincipen

Folkrättens distinktion mellan vad som är civilt och militärt definieras i liknande banor som manualen. Ett civilt tillstånd ändras till militärt ifall den civila aktören blir delaktig i kriget och ett civilt objekt blir militärt ifall det används av militären eller till fördel för militären (tågräls exemplet). Manualen tar sig även an vad som inom cyberrymden ska anses vara objekt och huruvida dessa är att anse som militära, civila eller utgör militär fördel att anfalla. Exempel som manualen valde att diskutera var ifall data anses som ett militärt eller civilt objekt. En minoritet av experterna ansåg att ett anfall mot känslig data är att anse som ett anfall, däremot ansåg panelen att data inte klassificeras som varken civilt eller militärt objekt då data inte finns fysiskt och därmed aktualiseras inte humanitär rätt.

Gällande tveksamhet ifall ett objekt är civilt eller militärt slår både humanitär rätt och manualen fast i att objektet bör klassas som civilt. Däremot skapas diskussion kring vilken grad av tveksamhet som behöver vara uppnådd för att ett objekt i fråga ska klassas som civilt. Panelen menar att på grund av cyberrymdens natur är det rimligt att viss tveksamhet får råda utan att ett objekt automatiskt klassas som civilt. Däremot är objekt som är sammanlänkade med både civil- och militära funktioner att anse som militära objekt så länge anfallet resulterar i militär fördel samt att skadorna är proportionerliga eller endast av moralisk karaktär.

5.1.3 Humanitär rätt och manualens syn på proportionalitetsprincipen

Humanitära rättens princip gällande proportionalitet vilar på å ena sidan militär fördelaktighet med ett anfall och å andra sidan möjliga skadliga effekter på civila och civila objekt. Manualen följer denna princip och blir tvungen att nyansera vad som menas med skador i och med att andra skador än fysiska kan vara ett mål med ett cyberanfall. Detta gör att manualen och dess experter tar ställning till vilka psykiska implikationer på civila som kan accepteras utan att det anses vara en skada som aktualiserar humanitär rätt.

Ifall ett cyberanfall inte innebär skada mot civila är det enda kriteriet relevant för en rättfärdig attack att det ger militär fördel, beaktande av civilas tillstånd blir alltså inaktuellt ifall fysiska skador inte anses föreligga. Panelen anser att försämrad moral genom irritation, stress eller rädsla inte uppnår skadekriteriet och därmed inte tas hänsyn till i enlighet med proportionalitetsprincipen. Experterna belyser återigen att cyberoperationer som kan innebära funktionalitetsförslust inom samhällsviktiga system kan åberopa proportionalitetsprincipen.

6. Diskussion

Cyberoperationer är en ny arena och folkrätten är i konstant förändring genom nya avtal och beslut som organisationer och länder anser viktiga, ett naturligt steg för folkrätten är att den blir applicerbar inom cyberrymden vilket är manualens syfte. Genom resultatet i uppsatsen kan det däremot argumenteras att cyberrymden och humanitära rätten möjligtvis missar varandra eller att formuleringar från humanitära rätten inte översätts till cyberrymden på ett rimligt sätt. Detta blir som tydligast i frågan om objekt som panelen anser att folkrätten syftar på fysiskt existerande endast och därmed konstaterar att data inte kan vara ett objekt även om flera experter påpekar att känslig data är något som definitivt bör övervägas som ett objekt

ifall humanitära rättens ambitioner ska beaktas. Å ena sidan kan en tolkning av objekt utifrån humanitär rätt gynnas av att stanna vid endast fysiskt existerande objekt då det skapas tydlighet och gör humanitär rätt praktisk i fysiska sammanhang. Å andra sidan är data något som under modern tid blivit en tillgång som värdesätts i flera olika aspekter då data kan innehålla värdefull information både ur socialt perspektiv men också i militära sammanhang. Även om experterna lyfte allvaret i att data 'faller mellan stolarna' genom tolkningen av humanitära rättens fysiska innebörd bör det diskuteras vilka framtida scenarion som hamnar i ett laglöst vakuum på grund av att en formulering gjordes utan hänsyn till cyberrymden när den skrevs och ifall kravet av att ett objekt måste vara fysiskt för att klassas som objekt möjligtvis är ett förlegat tankesätt.

Ytterligare exempel på trubbighet är när proportionalitetsprincipen diskuteras och panelen diskuterar när den anses tillämplig. Då principen gäller mot skador överlägger experterna vad som ska anses som skador i cyberrymden och som presenteras i resultatet anses skador som försämrar moral inte åberopa principen medan samhällsviktig funktionalitet prioriteras som något att tillämpa proportionalitetsprincipen på i vissa fall. Tänkbar problematik med resonemanget är att det inte nödvändigtvis är svart på vitt inom cyberrymden att något 'slås ur funktion' och vilket skada detta kan medföra. Fysisk attack mot ett köpcentrum görs tydligt som att något slås ut ur funktion. Skulle cyberanfall som resulterar i att exempelvis medborgares BANK-ID slås ur funktion argumenteras som samhällsnödvändigt? BANK-ID kan argumenteras utgöra en nödvändig samhällsfunktion då den används för att legitimera civila och flertal personer förlitar sig på BANK-ID för legitimering vid betalningar. Det finns en del scenarier som skapar oklarhet i skadekriteriet då cyberanfall möjligtvis inte medför direkta fysiska skador men kan innebära indirekta fysiska skador mot civila. Ifall vi ponerar att en del viktiga sajter för samhällsinformation slås ut och en stats informationsflöde till

civila befolkningen stängs partiellt av, anses det sänka moralen eller är det en viktig samhällsfunktion som slås ut? Ifall ett cyberanfall gör att väsentliga sajter för samhällsinformation fungerar men avsevärt långsammare till följd av ett anfall, anses en funktion slagits ur då? Experterna kan då anse att det är konsekvenserna som ska beaktas, däremot har det även påvisats av experterna hur svårt det kan vara att förutse konsekvenserna av ett cyberanfall. Poängen i argumentet är att en jämförelse med fysiska attacker och cyberanfall kan resultera i trubbighet då det fysiska anfallet inte är av samma natur som ett cyberanfall. Cyberanfall är i större utsträckning mer komplex och precist i vad och hur system ska slås ut i jämförelse med en situation där bombning av köpcentrum sker. Skadekriteriet som endast förlitar sig på fysiska skador skapar ett utrymme för cyberanfall att äga rum utan att humanitär rätt aktualiseras när det i själva verket kan argumenteras att det bör åberopas. Det bör diskuteras varför skadekriteriet som vilar på fysiska egenskaper ska anses utgöra beslutsunderlag i cyberrymden som i sin natur inte påverkar fysiska element.

Det kan då argumenteras för att Martensklausulens funktion träder in och kan klara upp tänkbara falluckor i folkrätten. Ifall denna klausul är till fördel för folkrätten kan här ifrågasättas. Klausulen är gjord för denna exakta situation, där något kan argumenteras ingå under humanitära rättens ambition, men faller utanför ändå av diverse anledningar, och då ska folkrättens vilja ändå träda fram. Klausulen kan i fallet kring data vara väl användbart och uppnå sitt syfte och göra undantagsfall. Men med hänsyn till teknikens utveckling är det oförutsägbart vad som härnäst sker inom cyberrymden och folkrättsliga principer som vilar på en klausul som ska baseras på ‘humanitetens krav’ lämnar en del att önska. Risken att låta en abstrakt formulering likt denna avgöra nya normer för krig kan leda till godtyckliga tolkningar på bekostnad av civilas säkerhet. Folkrättens klausul för att rädda situationen kan då bli en portal till att aktörer i maktposition inom exempelvis NATO lyckas sätta normer

utan att de kan ställas till svars för dem, då de genom klausulen kan hävda att de gjort en rimlig tolkning av en specifik situation med humanitetens intresse i beaktning, vidare undras var kunskap av humanitetens intresse hämtas från i sådana fall.

Med det sagt argumenteras det inte för att folkrätten bör lämnas och en nya lagar för cyberrymden ska inrättas. Däremot argumenteras det för att cyberrymden och den fysiska världen inte bör sammanlänkas i samma ramar inom folkrätten. Istället för formuleringar som är gjorda för att reglera fysiskt krig ska sträckas ut så de även täcker cyberrymden skulle det underlätta både för praktikalitet och civilas säkerhet ifall en version för cyberrymden skapas inom folkrätten. Något som kan vara det största argumentet för sådan utveckling är att folkrätten endast blir relevant under krig. I sin natur beskrev manualen svårigheten i att identifiera civila och militära mål på andra änden av cyberoperationer, detta leder till att cyberoperationer kan ske sinsemellan stater utan att det tydligt framgår. I praktiken kan det argumenteras att krig pågår som uppfyller kriterierna för krig men att båda parterna inte är medvetna om det, alternativt väljer att inte förklara krig då det inte nödvändigtvis skulle resultera i militär fördel. Ifall en stat väljer att öppet förklara cyberkrig kommer den tvingas förhålla sig till humanitära rättens principer vilket kan vara till nackdel ifall motståndaren väljer att inte förklara krig och därmed inte behöva anpassa sig till humanitära rätten.

Med beatkning av svårigheterna som tidigare stycken belyst kan det argumenteras att manualens nuvarande tolkningar av humanitär rätt i cyberrymden gör humanitär rätt i sin helhet verkningslös då det i flertal sammanhang kan argumenteras för att en cyberoperation kan kringgå att aktualisera humanitär rätt samtidigt som civila kan utsättas för konsekvenser som humanitär rätt och Just War teorin är ense om inte är rättfärdigat.

Problematiken med att skapa en ny gren av folkrätten, som ska baseras på de folkrättsliga principer som manualen utgår från, kan leda till en form av cirkelargument då folkrätten grundas i Just War teorin men ‘nya grenen’ isåfall utgår från folkrätten. Istället bör nya grenen istället endast utgå från Just War teorin. För att undvika att slutsatser och formuleringar som manualen gjort upprepas är det viktigt att utgå från Just War teorins övergripande principer och ambition istället för nuvarande folkrättsliga principer. Detta gör att hinder såsom att ett objekts egenskap av att vara fysisk blir irrelevant, istället ställs frågan ifall objektet, oavsett egenskap, påverkar civilas skydd eller inte. Att återgå till Just War teorins mer flytande formuleringar som bas gör att manualen fortfarande har en rättslig grund men kringgår stelheten som sker ifall folkrätten används som grund, vilket är problematiskt då folkrätten inte är anpassad efter cyberrymdens natur.

Samtidigt kan det argumenteras att humanitära rättens principer uppfyller dess syfte då den tydligt klargör vad som anses ligga i civilas säkerhets intresse och vad som inte ska falla under humanitära rättens lagar. Rimligtvis kan inte allt inom cyberrymden klassas som skyddat för anfall endast baserat på att civila och militära nätverk är sammanflätade exempelvis. Humanitära rätten värderar civilas säkerhet i fysiska egenskaper vilket ändå kan anses rimligt då cyberanfall undviker kritiska skador i större utsträckning än traditionella anfall. Ifall humanitära rättens principer översätts till cyberrymden i en alltför förlåtande tolkning där civilas cybersäkerhet ska prioriteras i nästintill alla tänkbara situationer riskerar folkrätten att uppfattas som icke realistisk och tappa förtroende vilket leder till att inga principer respekteras överhuvudtaget. Det måste finnas en gränsdragning för vad som ska anses relevant, däremot i denna stund görs gränsdragningar men möjligheten att kringgå principer som kan argumenteras vara väsentliga för humanitär rätt gör att säkerheten för civila i cyberrymden anses nästintill obefintlig.

7. Slutsatser

För att besvara forskningsfrågan '*Hur väl upprätthålls principen om skydd för civila i NATO:s cyberpolitik i enlighet med Just War teorins principer?'* beror framförallt på hur stora delar av civilas 'liv' som utspelas i cyberrymden. Ifall vi backar 15 år skulle denna fråga inte ha samma relevans då cyberrymden och civilas liv inte förlitade sig på cyberrymdens funktioner i lika stor grad då som dem gör nu. Detta gör att svaret kan delas in i två resonemang. Å ena sidan kan cyberrymden anses vara en arena där skador mot civila är att tolka som mindre allvarliga än i verkligheten, likt manualens resonemang är de flesta konsekvenser av cyberanfall psykiska skador snarare än fysiska. Ifall cyberoperationer pågår istället för traditionella krig kan det då anses vara till fördel för Just War teorins ambitioner då civila inte skadas i lika stor utsträckning. Å andra sidan finns argument för att Just Wars principer måste omtolkas till en cyber-anpassad folkrätt då framtiden tycks visa att cyberrymden kommer spela allt större roll för civilas säkerhet med senaste 20 åren som facit. I sådana fall anser uppsatsen att NATO:s cyberpolitik inte uppföljer Just Wars principer särskilt väl då en del situationer översätts från folkrätten till cyberrymden på ett ologiskt och trubbigt vis, vilket leder till gråzoner där tydliga riktlinjer i krig inte finns på bekostnad av civilas säkerhet.

Avslutningsvis landar uppsatsen i att NATO:s Tallinn Manual inte upprätthåller civilas skydd enligt Just Wars principer särskilt väl, däremot är det ett första steg i att förflytta vad som ska skyddas i cyberrymden för civilas intresse. En avvägning mellan vilka civila områden som kan offras i cyberrymden för att undvika traditionellt krig tycks vara tillvägagången som

framtida tolkningar av Just War teorin bör ta ställning till. Första steget är att det bör klargöras på starkare grunder i manualen att vissa områden, såsom ‘data’, är av civilas intresse att skyddas men bör isåfall uppges för att undvika traditionellt krig och fysiskt våld. Manualens argument att data saknar fysiska attribut och därmed kan anfallas utan att humanitära rättens principer tillämpas tycks vara den röda tråden i förlegade formuleringar som uppsatsens resultat påvisat i flera aspekter.

Framtida forskningsområden som bör utforskas är hur nationer som inte påverkas av den västerländska politiken, såsom NATO och folkrätten, har för cyberpolitik på plats. Detta görs relevant både för civilas säkerhet men också för hur västerländska nationers politik ska utformas ur ett realistiskt politiskt förhållningssätt. Detta kan leda till att forskningsområden som ponerar hur ett cyberkrig skulle utspelas om ena parten förhåller sig till exempelvis folkrättsliga principer medan den andra parten inte gör det skulle se ut. Det kan även forskas i vilka svårigheter länder som är längre bak i sin utvecklingen av cyberteknik kan mötas i sin färd in till cyberrymden. Med detta syftas det på informationsfördelar, mjukvarufördelar och allmänt utvecklad offensiv cyberteknik som vissa nationer kommer ha till sitt förfogande för att styra sina agendor gentemot den cyber-outvecklade nationen.

8. Litteratur

Berger, Ella. Salö, Freja. 2013. *Så övervakades G20-topparna i London.*

SVT Nyheter. 17 juni.

Tillgänglig: https://www.svt.se/nyheter/utrikes/sa-overvakades-g20-topparna-i-london

(Hämtad 2022-08-03)

Guthrie, Charles. Quinlan, Michael. 2007. *JUST WAR. The Just War Tradition: Ethics in Modern Warfare*. 1 uppl. Storbritannien: Bloomsbury.

Jensen, Eric. 2017. *The Tallinn Manual 2.0: Highlights and Insights*

BYU Law Research Paper Nummer 17-10.

Lindvall, Kristina. Tengroth, Cecilia. Clomén, Dick. 2017 *Information om den humanitära rätten*. Totalförsvarets folkrättsråd. Artikelnummer. 3226.

Tillgänglig:https://www.regeringen.se/49f226/globalassets/regeringen/dokument/forsvarsdepartementet/folkrattsradet/information-om-den-humanitara-ratten.pdf (Hämtad 2022-08-14)

Mohammed, Karoubi. 2004. *Just or Unjust War? International Law and Unilateral Use of Force by States at the turn of the 20th Century.* 1 uppl. Gateshead: Athenaeum Press, Ltd.

NATO, 2020. *What is NATO?*

Tillgänglig: https://www.nato.int/nato-welcome/index.html (Hämtad: 2022-08-10)

Obama, Barack. 2013. Intervjuad av Charlie Rose. 'PRESIDENT BARACK OBAMA' *Charlie Rose*. 17 juni.

Tillgänglig: https://charlierose.com/videos/17754 (Hämtad 2022-08-15)

Robinson, Michael. Jones, Kevin. Janicke, Helge. 2015. 'Cyber warfare: Issues and challenges' Spafford, Eugene (ed.) *Computers & Security* . Vol. 49. s. 70 - 94

Schmitt, Michael (ed.) 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2a uppl. Cambridge University Press

Snowden, Edward. 2020. Intervjuad av Joe Rogan. '#1536 - Edward Snowden' *The Joe Rogan Experience*. 15 september.

Tillgänglig: https://www.youtube.com/watch?v=_Rl82OQDoOc (Hämtad 2022-08-12)

SOU 2010:22 *Krigets Lagar*

Tillgänglig:

https://www.regeringen.se/49bb46/contentassets/7db8b68842114a88a0b4f46de5f579df/krigets-lagar-sou-201022-del-1 (Hämtad 2022-08-12)

SvD. TT. 2013. *Mannen som röjde USA:s övervakning träder fram*

Tillgänglig:

https://www.svd.se/a/1e4300d6-e405-368a-821f-be4c8d967c1a/mannen-som-rojde-usas-overvakning-trader-fram (Hämtad 2022-08-03)

Taddeo, Mariarosaria. 2012. ‘An Analysis For A Just Cyber Warfare’ Czosseck, Christian. Ottis, Rain. Ziolkowski, Katharina (ed.) *4th International Conference on Cyber Conflict.* NATO CCD COE Publications

Teorell, Jan. Svensson, Torsen. 2007. *Att fråga och att svara: Samhällsvetenskap metod.* 5 Uppl. Stockholm: Liber AB.

Viner, Steve. 2013. ‘The moral foundations of the jus ad bellum/jus in bello distinction*’* Allhof, Fritz. Evans, Nicholas. Henschke, Adam. (ed.) *Routledge Handbook of Ethics and War: Just War Theory in the 21st Century*. 1 uppl. New York And London: Routledge.