JURIDISKA FAKULTETEN
vid Lunds universitet

Sara Link

På gränsen till ett osynligt krig

- en undersökning av våldsförbudets gränser i förhållande till cyberoperationer

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet
15 högskolepoäng

Handledare: Aurelija Lukoseviciene

Termin: VT 2022

Innehållsförteckning

Summary

Society becomes increasingly digitalized, which despite many advantages entails greater vulnerability and more risks. Therefore, the importance of cybersecurity has increased but the limitation of cyber operations is unclear. Cyber operations are actions performed in a virtual reality called cyberspace. If these actions have offensive elements and exploit other states' weaknesses, they are referred to as offensive cyber operations.

However, there are no ad hoc regulations regarding cyber operations which creates ambiguities. States agree that international law, in particular The Charter of the United Nations, is applicable. Nevertheless, these are general regulations which are not adapted to the specific nature of cyber operations. The prohibition of use of force is a cornerstone in international law which limits the use of cyber operations. If an action reaches the level of use of force it constitutes a breach of the prohibition of use of force. To apply the prohibition of use of force to cyber operations, the 'scale and effects' that the actions cause must be considered. An assessment is made in the individual case based on one of three different approaches: target-based, instrument-based or consequence-based. The most appropriate approach is the consequence-based as it provides a comprehensive analysis and takes more factors into account. Based thereon, the thesis examines whether three real cases are considered to reach use of force and thus would be in conflict with the prohibition of use of force.

The prohibition of use of force is in itself unclear. This means it is not possible to establish which conditions must be fulfilled to allow offensive cyber operations. Nevertheless, it is established that the most serious offensive cyber operations, which kill persons or cause physical damage to objects, always violate the prohibition of use of force. Thus, there is a limit to how destructive a cyber operation is allowed to be. However, the borderland remains unclear since it is possible that a cyber operation that does not cause physical harm breaches the prohibition of use of force based on an overall assessment.

Sammanfattning

Samhället går mot en ökad digitalisering vilket trots många fördelar innebär större sårbarhet och fler risker. Därför har cybersäkerhet fått en större betydelse men gränserna för vad som är tillåtet är oklart. Cyberoperationer är handlingar som företas i en virtuell verklighet vilken kallas cyberrymden. Om handlingarna har offensiva inslag och utnyttjar andra staters svagheter kallas de för offensiva cyberoperationer.

Dock är cyberoperationer inte specifikt reglerade i folkrätt vilket skapar oklarheter. Stater är överens om att folkrätt och särskilt FN-stadgan är tillämplig men detta är ett generellt regelverk som inte är anpassat till cyberoperationers särskilda karaktär. En av de centrala reglerna som sätter gränser för cyberoperationer är våldsförbudet. En handling strider mot våldsförbudet om den uppnår *bruk av våld*. För att applicera våldsförbudet på cyberoperationer ska hänsyn tas till skala och effekt på handlingens konsekvenser. Bedömningen görs i det enskilda fallet utifrån tre olika tillvägagångssätt: målbaserat, instrumentbaserat eller konsekvensbaserat. Det lämpligaste tillvägagångssättet anses vara konsekvensbaserat eftersom det ger en heltäckande bild och tar hänsyn till fler faktorer. Uppsatsen undersöker därefter om tre verkliga fall anses nå upp till *bruk av våld* och därmed är i strid med våldsförbudet.

Våldsförbudet är i sig otydligt vilket gör att det inte går att konstatera vilka förutsättningar som ska vara uppfyllda för att tillåta offensiva cyberoperationer. Däremot kan konstateras att det allvarligaste offensiva cyberoperationerna, som berövar människoliv eller orsakar skador på fysiska objekt, alltid strider mot våldsförbudet. Det visar att det finns ett tak på hur allvarlig skada en cyberoperation tillåts orsaka. Dock förblir gränsområdet oklart eftersom det är möjligt att en cyberoperation som inte orsakar fysisk skada strider mot våldsförbudet utifrån en helhetsbedömning.

Förkortningar

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CISA	Cybersecurity and Infrastructure Security Agency
EU	Europeiska unionen
FN	Förenta Nationerna
FN-stadgan	Förenta Nationernas stadga
ICJ	Internationella domstolen (International Court of Justice)
ICJ-stadgan	Stadgan för den Internationella domstolen
NATO	North Atlantic Treaty Organisation
USA	Amerikas förenta stater (United States of America)

1 Inledning

1.1 Bakgrund

”Obama Order Sped Up Wave of Cyberattacks Against Iran”[1], ”‘Most Severe’ Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider”[2], ”USA och Storbritannien rustar för offensiva cyberattacker”[3] och ”Ryska cyberattacker drabbade 39 delstater inför USA-valet”[4] är några exempel på tidningsartiklar som blir allt vanligare. Världen har förändrats drastiskt de senaste 50 åren både tekniskt och politiskt. Slagfältet består inte längre av endast skjutvapen och stridsflygplan.[5] Datorer och internet har numera avgörande roll både för stater och individer. Den ökande uppkopplingen till internet skapar många möjligheter men det har även sin baksida. Ett samhälle beroende av internet har många svagheter som andra kan utnyttja.[6]

En cyberoperation kan innebära omfattande skador för en stats fiende, utan att den egna staten behöver offra liv eller stora resurser.[7] I och med nya säkerhetsbrister kopplade till datornätverk har cybersäkerhet fått större betydelse i staters strävan att skydda den egna staten.[8] Kan anfall vara bästa försvar? Cyberoperationer i sig utgör ingen otillåten handling. Däremot sätter folkrätt gränser för vad som är tillåtet i internationella relationer.[9] Frågan uppstår: när kan en cyberoperation med syfte att skydda tolkas som en våldshandling mot en annan stat? Utifrån detta analyserar uppsatsen våldsförbudets gränser och den problematik som uppstår när folkrätt tillämpas på cyberoperationer.

1.2 Syfte och frågeställningar

Mot bakgrund av ovanstående är syftet med uppsatsen att undersöka våldsförbudets gränser i förhållande till cybersäkerhet och staters agerande i cyberrymden. Ämnet är viktigt för att både stater och andra aktörer ska förstå vad som är tillåtet agerande i cyberrymden och

[1] Sanger, *The New York Times*.
[2] Brewster, *Forbes*.
[3] Svahn, *Dagens Nyheter*.
[4] Svensson, *Dagens Nyheter*.
[5] Henderson, s. 55.
[6] Schmitt (1999), s. 886–887.
[7] Smeets, s. 98–99, 103–105.
[8] Schmitt (1999), s. 886–887.
[9] Delerue, s. 35, 274–275, Schmitt (2017), s. 168.

internationella relationer. Utgångspunkten är att se hur stater bör använda sig av cyberoperationer enligt folkrätt i relationer med andra stater. Frågeställningen är därmed följande: kan cyberoperationer mot andra stater tillåtas enligt folkrätt och, om så är fallet, under vilka förutsättningar? Uppsatsen belyser vad som utgör en cyberoperation, möjliga syften med cyberoperationer och huruvida dessa kan strida mot våldsförbudet. Det förs även en diskussion utifrån frågeställningen huruvida nuvarande reglering är tillräcklig och vilken utveckling som är möjlig.

Mot bakgrund av syftet besvaras följande frågor:

- Vad är cyberrymden och cyberoperationer?
- Hur regleras cyberoperationer och vad innebär våldsförbudet inom folkrätt?
- Kan offensiva cyberoperationer mot andra stater någonsin tillåtas i förhållande till våldsförbudet?
- Om offensiva cyberoperationer kan tillåtas, under vilka förutsättningar?

1.3 Avgränsningar

Med hänsyn till omfång och tid fokuserar uppsatsen på allvarligare former av cyberoperationer som utförs i fredstid i förhållande till våldsförbudet. Detta begränsar urvalet av konkreta exempel till de mest allvarliga och utesluter andra cyberaktiviteter såsom cyberbrottslighet.

Ingen form av hänförbarhetsproblematik diskuteras utan det antas att alla aktiviteter är direkt hänförbara till stater. Privata aktörer och deras cyberverksamhet, trots eventuell indirekt koppling till en stat, berörs inte. Anledningen är att hänförbarhetsproblematiken är omfattande vilket inte kan utredas utifrån uppsatsens begränsade omfång.

För att våldsförbudet ska aktualiseras krävs att det inte redan pågår krigsföring i den fysiska världen mellan staterna. Därför diskuteras endast situationer utan pågående krigföring. Trots att våldsförbudet stadgas i flera traktat[10] fokuserar uppsatsen endast på det generella förbud som föreskrivs i FN-stadgan[11] och internationell sedvanerätt. Våldsförbudet avgränsas vidare

[10] Henderson, s. 17.
[11] Förenta Nationernas stadga, San Francisco 26 juni 1945, SÖ 1946:1.

till att endast undersöka våldsanvändning. Hot om våld eller handlingar i strid med FN:s syfte diskuteras inte.

Andra närliggande frågor, såsom rätten till självförsvar eller non-intervention, behandlas inte såvida det inte är av direkt relevans för tolkningen av våldsförbudet. Att undersöka dessa frågor är dock passande område för vidare forskning.

1.4 Teori och metod

Uppsatsen skrivs utifrån ett internationellt och kritiskt perspektiv för att analysera olika aspekter av problematiken. Den rättsdogmatiska metoden tillämpas för att besvara frågeställningarna. Metoden innebär att gällande rätt tolkas och systematiseras. Den används för att utreda gällande rätt och applicera den på ett aktuellt problem. Metoden utgår ifrån allmänt accepterade rättskällor.[12] Valet av metod beror på nuvarande oklarhet om vilka gränser folkrätt sätter för användningen av cyberoperationer.[13] Metoden passar väl för att utreda denna problematik.[14] Eftersom uppsatsen har ett internationellt perspektiv utgår metoden från folkrättsliga källor. Folkrätten är ett decentraliserat system och källorna har inte samma uttalade hierarki sinsemellan som svenska rättskällor vilket påverkar tillämpningen av metoden.[15] Därför undersöks de folkrättsliga källorna systematiskt och jämförs utifrån deras betydelse för folkrätten som helhet. Slutligen diskuteras om nuvarande reglering är lämplig och förslag på framtida utveckling presenteras.

För att förstå konceptet cybersäkerhet och cyberoperation definieras dessa genom en jämförelse av olika definitioner och forskning inom området. Vidare konkretiseras begreppen genom att belysa flera verkliga fall.

1.5 Material, forskningsläge och källkritik

De viktigaste rättskällorna inom folkrätt är traktat, internationell sedvanerätt, allmänna principer och rättspraxis. Källorna har ingen inbördes hierarki utan väger lika tungt med

[12] Kleineman i Nääv och Zamboni, s. 21, 35–36.
[13] Delerue, s. 4–5.
[14] Kleineman i Nääv och Zamboni, s. 21–23.
[15] Henriksen, s. 20–22, 32–35.

undantag för rättspraxis som är underordnat de tre förstnämnda källorna.[16] Uppsatsen utgår ifrån dessa primära källor eftersom de har hög tillförlitlighet och auktoritet.[17] Främst analyseras traktat och internationell sedvanerätt medan avgörande från ICJ används för att förstå innehållet i överordnade rättskällor.

Doktrin på området används för att förstå tillämpningen av primärkällorna. Detta material belyser även problematiken som uppstår vid tillämpning av folkrätt på cyberrymden. I möjligaste mån har officiella källor eller artiklar som är referentgranskade använts eftersom dessa anses ha högre tillförlitlighet och auktoritet.[18] När detta inte varit möjligt har texter från etablerade förlag eller tidskrifter använts.

Några av de mest framstående verken på området är Tallinn manualerna.[19] Dessa omfattande analyser undersöker gällande rätt i förhållande till cyberkrig och cyberoperationer. Experter från hela världen har bidragit till Tallinn manualerna som dessutom är referentgranskade. Trots att de inte är officiella rättskällor[20] har de på grund av sin omfattning, grundlighet och kvalitetskontroll en hög tillförlitlighet och auktoritet inom doktrin.[21]

Mycket av forskningen på området kommer från västerländska universitet. Dessutom är Tallinn manualerna skapade av CCDCOE som syftar till att stötta NATO.[22] Med det i åtanke kan materialet som behandlas ha ett västerländskt perspektiv vilket det finns anledning att vara kritisk inför.[23] Detta förklaras av politiska skäl och att det är svårare att få tag på engelsk litteratur inom ämnet från andra stater som har stor aktivitet av cyberoperationer, såsom Kina och Ryssland.[24] All litteratur som används är på engelska vilket även kan påverka ordens betydelse vid översättning till svenska.

Även om tekniken har förändrats mycket har samma gränsdragningsproblematik diskuterats sedan attacken mot Estland 2007. Yngre källor används när det är möjligt men vissa tankar kopplade till tillämpningen av folkrätt på cyberoperationer är äldre. Dessa anses trots det vara

[16] Se artikel 38 i Stadga för den Internationella Domstolen, San Francisco 26 juni 1945, SÖ 1946:1 (formellt inkorporerad i FN-stadgan), Henriksen, s. 20–21, 29.
[17] Sandgren, s. 36–38.
[18] Sandgren, s. 36–38.
[19] Schmitt (2013), Schmitt (2017).
[20] Schmitt (2017), s. 2.
[21] Sandgren, s. 36–38.
[22] Schmitt (2013), s. 1.
[23] Se exempel Roscini, s. 30–31.
[24] Solis, s. 674–677.

lämpliga eftersom diskussionen fortfarande fokuserar på samma problematik. En av artiklarna som används är dock betydligt äldre än andra vilket kan problematiseras. Den har trots det använts eftersom författaren är projektledare till Tallinn manualerna och har en central roll inom området.

1.6 Disposition

Uppsatsen inleds med en förklaring av bakgrunden och en redogörelse för hur uppsatsen är strukturerad. I inledningen beskrivs bland annat syfte och metod för att förstå hur uppsatsen tar sig an ämnet. Huvudtexten består därefter av tre delar. I första delen utreds begrepp och koncept som är fundamentala för förståelsen av cybersäkerhet. Dessutom exemplifieras vissa allvarliga cyberoperationer. Andra delen behandlar relevant folkrätt med fokus på våldsförbudet, både i traktat och internationell sedvanerätt. Denna del utreder även möjligheten att tillämpa det folkrättsliga regelsystemet på cyberrymden. Varpå tredje delen undersöker gränsdragningsproblematik som uppstår vid tillämpningen av folkrätt på handlingar i cyberrymden. Efter huvudtexten analyseras materialet på ett kritiskt sätt för att besvara frågeställningarna och komma fram till en slutsats.

2 Cybersäkerhet

2.1 Inledning

Ett bekymmer inom området är att många begrepp kopplade cybersäkerhet saknar vedertagna definitioner.[25] Därför redogör detta kapitel några centrala begrepp som har betydelse för den fortsatta förståelsen och problematiseringen. Vidare beskrivs även ett par exempel på verkliga cyberoperationer.

2.2 Viktiga begrepp kopplade till cybersäkerhet

Cyberrymden är inte en vetenskaplig eller juridisk term och dess betydelse kan variera. Flera definitioner framhåller att det rör sig om en miljö bestående av datornätverk, främst internet, som sammankopplar flera enheter. Inom denna miljö som utgör cyberrymden kan data bearbetas. En distinktion görs mellan de virtuella datornätverken och fysiska komponenter

[25] Roscini, s. 10–13.

vilket avser allt från datorer till servrar.[26] Det finns även enklare definitioner som endast belyser datornätverks centrala roll och beskriver cyberrymden som ”The space of virtual reality; the notional environment within which electronic communication (esp. via the internet) occurs”.[27] Utifrån uppsatsens syfte kommer cyberrymden fortsättningsvis syfta på den virtuella verklighet som utgörs av datornätverk.

Cybersäkerhet syftar på processer och åtgärder som vidtas för att skydda statens data, nätverk och datorer. Syftet är att minimera skada som obehöriga kan orsaka.[28] Att använda cybersäkerhet defensivt och i fredliga syften för att skydda sig själv är oproblematiskt.[29] Defensiv cybersäkerhet omfattar bland annat brandväggar, starka lösenord och strukturerade rutiner.[30] Denna typ av skydd orsakar ingen skada för andra utan är endast ett hinder för de som obehörigt försöker bereda sig tillgång till nätverket.[31]

Med cyberoperationer avses aktiviteter och handlingar i cyberrymden. Aktiviteterna kan i sin tur påverka datorer och andra fysiska objekt men handlingarna i sig måste företas i cyberrymden. Därför utesluts våld eller handlingar som görs i den fysiska världen mot datorer.[32] Begreppet kan delas upp i ett antal underkategorier. Första uppdelningen görs mellan defensiva och offensiva cyberoperationer. Defensiva cyberoperationer fokuserar endast på att försvara data, nätverk och hårdvara från hot. Det utgörs främst av den interna struktur för cybersäkerhet som nämndes tidigare i avsnittet men omfattar även åtgärder som vidtas mot specifika cyberattacker för att minimera skada när intrång har skett.[33] Offensiva cyberoperationer syftar på fientliga handlingar mot andra datornätverk i cyberrymden. Cyberoperationer kan även delas in i två olika kategorier beroende på syftet med operationen: cyberattacker och cyberexploatering. Det förstämda avser destruktiva operationer med syfte att ändra eller förstöra andras datorsystem. Det sistnämnda tar sikte på inhämtning av information och spionage utan att förstöra något. Målet är att informationsinhämtningen ska

[26] Delerue, s. 29–30, Schmitt (2017), s. 564.
[27] Oxford English Dictionary ”cyberspace”.
[28] Oxford English Dictionary ”cybersecurity”, CISA.
[29] UNGA A/RES/73/27, s. 1.
[30] CISA.
[31] Joint Chiefs of Staff, s. II-3–II-4.
[32] Delerue, s. 35.
[33] Joint Chiefs of Staff, s. II-3–II-4.

ske obemärkt.[34] Cyberattacker och cyberexploatering kan vara både defensiva och offensiva, dock är de oftast offensiva operationer.[35]

I uppsatsen diskuteras fortsättningsvis offensiva cyberoperationer eftersom det främst är de som riskerar att strida mot våldsförbudet.

2.3 Fallstudier – tre uppmärksammade cyberattacker

Nedanför redovisas tre uppmärksammade fall av cyberoperationer. Utmärkande är att de huvudsakligen skett utan pågående krig och att de fått effekter i verkliga världen, främst på kritisk infrastruktur.

2007 fattade estniska regeringen ett beslut att flytta en Sovjetisk minnesstaty. Beslutet var början på stora protester och en våg av cyberattacker mot Estland som misstänktes ha kopplingar till Ryssland. Attackernas syfte var att störa Estlands digitala tjänster och infrastruktur genom överbelastning. Myndighetshemsidor, banker, sjukhus och larmcentraler drabbades och sattes tillfälligt ur funktion. Cyberattackerna hade främst ekonomiska och sociala konsekvenser eftersom företag, myndighetsverksamhet och nyhetsflöde påverkades. Framför allt försvårades kommunikationen mellan myndigheter och medborgare. Överbelastningsattacker av denna typ är relativt enkla att utföra och kräver inte omfattande kunskap eller resurser.[36] Cyberoperationerna mot Estland anses dock inte uppnå tröskeln för *väpnat angrepp*.[37]

2009–2010 utfördes flera cyberattacker mot iranska kärnkraftverk. Attackerna hänfördes till datorviruset Stuxnet. Viruset misstänks infekterat datorer genom USB-minnen som kopplats till en dator. Väl i datorn duplicerades det och spreds till andra datorer inom nätverket eller kopierades till andra USB-minnen som spred det vidare. Spridningen genom USB-minne gjorde det möjligt för viruset att komma åt datorer som inte var uppkopplade till internet. Stuxnet utmärkte sig för sin förmåga att förbli dold från datorns användare vilket innebar att det kunde spridas över hela värden obemärkt tills viruset hittade sitt mål. I bakgrunden gjorde viruset tester för att hitta en specifik programvara som styr en särskild form av centrifuger som används i vissa kärnkraftverk. När Stuxnet hittade programvaran tog den över kontrollen

[34] Delerue, s. 35, Joint Chiefs of Staff, s. II-5–II-7, Lin, s. 63-64.
[35] Joint Chiefs of Staff, s. II-5–II-7, Schmitt (2017), s. 415.
[36] Kozłowski, s. 238-239, Schmitt (2011), s. 577, Woltag, s. 42–45.
[37] Schmitt (2013), s. 57–58.

och överbelastade centrifugen innan den gömde sina spår. Programvaran som var måltavla 2009–2010 användes vid tidpunkten i Irans kärnkraftsprogram. Viruset orsakade därmed skador i den fysiska världen genom att förstöra delar av Irans kärnkraftsanläggningar. Detta ledde till flera månaders bakslag för utvecklingen av Irans kärnkraft. Stuxnet misstänks vara statligt sponsrad på grund av dess imponerande precision och stora resurser som krävs för dess utveckling. USA och Israel förmodas ligga bakom även om detta inte bekräftats.[38] Stuxnet är det tydligaste exemplet på en cyberoperation som orsakat fysiska skador på en nivå som kan uppnå tröskeln för *bruk av våld* men möjligen även *väpnat angrepp*.[39]

Sedan Sovjetunionens fall har Ryssland försökt behålla kontrollen över Ukraina. Under 2013–2014 intensifierades spänningarna efter Ukrainas försök att närma sig EU. Detta ledde till en ökning av cyberattacker och cyberexploatering mot både Ryssland och Ukraina. En av det mest skadliga attackerna gjordes mot Ukrainas kraftnät under 2015 vilket resulterade i att ungefär 250 000 invånare förlorade tillgång till el i flera timmar. Året senare gjordes flera cyberattacker mot banker och myndigheter samt ytterligare en attack mot Kievs kraftnät. Händelserna minskade befolkningens förtroende för ukrainska staten och orsakade ekonomiska skador.[40]

3 Folkrättsliga regleringar

3.1 Reglering av cyberrymden

I folkrättens primärkällor finns det inga regler som särskilt reglerar cyberrymden eller cyberoperationer.[41] Däremot har FN:s generalförsamling antagit två resolutioner[42] gällande telekommunikation, cyberrymden och internationell säkerhet där de bekräftar att folkrätt och särskilt FN-stadgan är tillämplig på området. Resolutionerna betonar även vikten av folkrättens och FN-stadgans roll att upprätthålla fred och säkerhet, även i cyberrymden.[43] Dock går de inte in i detalj på hur specifika regler bör tillämpas. Båda resolutionerna röstades igenom i generalförsamlingen med stor majoritet vilket tyder på en enighet bland stater att

[38] Baezner, Robin, s. 4–9, Solis, s. 706–709, Woltag, s. 47–50.
[39] Schmitt (2013), s. 45, 57–58.
[40] Baezner (2018), s. 3–9, Dragos Inc., s. 10–11.
[41] Roscini, s. 19–20.
[42] UNGA A/RES/73/27, UNGA A/RES/73/266.
[43] UNGA A/RES/73/27, s. 2, UNGA A/RES/73/266, s. 2.

folkrätt är tillämpligt på cyberrymden.[44] Även om både stater och experter är överens om folkrättens tillämplighet finns svårigheter med appliceringen i praktiken.[45]

3.2 Våldsförbudet

Efter andra världskriget växte FN fram som syftar till att bevara världsfred. En central princip i FN:s arbete för världsfred är våldsförbudet som både är en del av FN-stadgan och internationell sedvanerätt.[46] Principen tolkas och förklaras ytterligare i ICJ:s domar. ICJ är FN:s dömande organ som har en viktig roll genom att avgöra tvister mellan stater.[47] Deras domar är endast bindande för parterna i målet men domstolens argumentation ger vägledning vid tolkning av folkrätt.[48]

3.2.1 FN-stadgan

FN-stadgan är en mellanstatlig överenskommelse och grunden till FN-samarbetet. Där fastställs flera viktiga principer som FN bygger på.[49] I artikel 2 paragraf 4 FN-stadgan föreskrivs våldsförbudet:

> Alla medlemmar skola i sina internationella förbindelser avhålla sig från […] *bruk av våld* [min kursivering], vare sig riktat mot någon annan stats territoriella integritet eller politiska oberoende […].

Våldsförbudet i FN-stadgan skapar endast en direkt skyldighet att avstå från *bruk av våld* för medlemmar inom FN. Medlemmarna förpliktigas att ta hänsyn till detta i sina internationella relationer med alla andra stater, oavsett om den andra staten är FN-medlem eller inte. Därmed förutsätter förbudets tillämpning att båda parterna är stater. Om en av parterna inte är en stat kan det aldrig vara ett brott mot våldsförbudet. Detta kan skapa problematik i omtvistade geografiska områden som erkänts av vissa stater men inte andra. Kravet på att parterna är stater innebär också att våldsförbudet inte är aktuellt för interna konflikter.[50]

[44] Delerue, s. 21.
[45] Delerue, s. 3, 13.
[46] Henderson, s. 10, Henriksen, s. 252–253.
[47] Artikel 92 FN-stadgan, artikel 1 och 34 ICJ-stadgan.
[48] Artikel 94 FN-stadgan.
[49] United Nations (officiella hemsida).
[50] Henderson, s. 22–23.

Av FN-stadgan framgår inte innebörden av *bruk av våld*. Detta gör att förbudet är flexibelt och kan förändras i takt med att världen utvecklas.[51] Dessutom bör våldsförbudet tolkas i ljuset av andra artiklar i FN-stadgan.[52]

Den mest snäva tolkningen av *bruk av våld* är att förbudet endast berör vapenmakt. Generellt innebär detta att den angripande staten använder sig av någon form av vapen. Däremot ger FN-stadgan ingen vägledning till vilka vapen som omfattas. När förbudet kom till fanns inte mycket av den teknik vi har idag och därför syftade artikeln sannolikt på användningen av konventionella vapen såsom skjutvapen och sprängladdningar. Världen har genomgått en snabb teknisk utveckling sedan FN:s uppkomst. Det är därför möjligt att även om vapenmakt i sig är en snäv tolkning har dess innebörd förändrats och omfattar numera moderna vapen och stridsmetoder.[53] Vidare har ICJ konstaterat att artikel 2 paragraf 4 FN-stadgan inte hänvisar till något specifikt vapen utan kan tillämpas generellt oavsett vapentyp.[54] Utifrån detta resonemang omfattas användning av konventionella vapen och teknik utvecklad för krigsföring i våldsförbudet.

En annan möjlig tolkning av vapenmakt är att effekten av agerandet är avgörande. Detta skulle vidga begreppet och gör att mindre traditionella vapen kan omfattas. Framför allt diskuteras detta i förhållande till cyberoperationer och hur de förhåller sig till våldsförbudet. Utifrån denna tolkning är det inte metoden i sig som är förbjuden, utan effekterna som användningen av en viss metod orsakar. Den konsekvensbaserade tolkningen kräver att handlingen uppgår till en viss allvarlighet utifrån ICJ:s tolkning av våldsförbudet, vilket diskuteras närmare nedan (avsnitt 3.2.3).[55]

Artikel 2 paragraf 4 FN-stadgan förbjuder inte uttryckligen endast vapenmakt (jämför artikel 51 FN-stadgan) vilket gör att *våld* kan tänkas ha en bredare tolkning. Det pågår diskussioner huruvida humanitära interventioner eller cyberoperationer omfattas av förbudet.[56]

[51] Dörr och Randelzhofer i Simma m.fl., s. 208, Gray, s. 12.
[52] Legality of the Threat or Use of Nuclear Weapons, para. 38.
[53] Dörr och Randelzhofer i Simma m.fl., s. 208–209, Henderson, 54–59.
[54] Legality of the Threat or Use of Nuclear Weapons, para. 39.
[55] Henderson, s. 53–55, 59. Se även Nicaragua-målet.
[56] Gray, s. 32–34, 52–53, Henderson, s. 52–59.

3.2.2 Internationell sedvanerätt

För att en regel ska anses vara internationell sedvanerätt krävs två aspekter: statlig praxis (mönster av staters agerande) och opinio juris (staters rättsövertygelse). Det ska gå att visa att stater generellt agerar på ett visst sätt eftersom de anser sig vara rättsligt bundna att agera därefter.[57]

Våldsförbudet är en del av internationell sedvanerätt.[58] ICJ anser att det föreligger en internationell sedvanerättslig princip där stater förväntas att inte använda våld mot andra stater. Opinio juris hänförs från staternas inställning till vissa konventioner[59] som bevisar att staterna respekterar förbudet.[60]

Den viktiga skillnaden från förbudet i FN-stadgan är att den internationella sedvanerätten är tillämpligt på alla stater, oavsett om staten är medlem i FN eller inte. Våldsförbudet i internationell sedvanerätt omfattar därmed fler stater. Dock är fortfarande icke-statliga aktörer inte omfattade.[61]

Emellertid finns oenighet kring huruvida förbudet i internationell sedvanerätt överensstämmer med förbudet i FN-stadgan. ICJ anser att våldsförbuden kan ha samma innebörd men ändå tillämpas som två separata instrument.[62] Domstolen går emellertid inte närmare in på om det faktiskt finns en skillnad mellan reglerna. Det är svårt att avgöra exakt hur långt de olika förbuden sträcker sig. Däremot är en majoritet av världens stater bundna av våldsförbudet i FN-stadgan vilket gör sannolikheten stor att stater handlar därefter och att förbuden väsentligen överensstämmer. För uppsatsens syfte räcker det att konstatera att kärnan i förbuden, att *bruk av våld* mot andra stater är otillåtet, är densamma.[63]

3.2.3 ICJ och Nicaragua-målet

Både enligt FN-stadgan och internationell sedvanerätt krävs att en handling utgör *bruk av våld* för att nå upp till våldsförbudet. Vad detta innebär har ICJ gått närmare in på i sina

[57] Artikel 38 paragraf 1 punkt (b) ICJ-stadgan, Henriksen, s. 23–26.
[58] Dörr och Randelzhofer i Simma m.fl., s. 229–231, Nicaragua-målet, para. 34.
[59] Se särskilt UNGA A/RES/2625(XXV).
[60] Nicaragua-målet, para. 188–190.
[61] Schmitt (2017), s. 330.
[62] Nicaragua-målet, para. 178–179.
[63] Dörr och Randelzhofer i Simma m.fl., 229–231, Henderson, s. 17–18.

avgöranden.[64] Ett av det mest betydelsefulla målen ICJ har dömt gällande *bruk av våld* är Nicaragua-målet. Framför allt ger målet vägledning för tolkning av begreppet *bruk av våld*.[65]

I Nicaragua-målet anser domstolen att de grövsta formerna av *bruk av våld* bör skiljas från de mindre allvarliga. De grövsta formerna syftar på handlingar som uppnår *väpnat angrepp* kopplat till artikel 51 FN-stadgan.[66] *Väpnat angrepp* bör inte likställas med *bruk av våld*.[67] Därmed utgör en handling som uppnår *väpnat angrepp* alltid *bruk av våld* men *bruk av våld* utgör inte alltid ett *väpnat angrepp*. Tröskeln för *bruk av våld* är lägre och kan omfatta mindre ingripande handlingar.[68] Vad som krävs för att uppnå denna lägre tröskel av *bruk av våld* preciserar inte ICJ.[69]

Vidare konstaterar ICJ att *väpnat angrepp* inte är begränsat till enbart användning av traditionella väpnade styrkor. Förutsatt att de uppnår motsvarande allvarlighet kan även andra ageranden utgöra ett *väpnat angrepp*. Hänsyn tas vid bedömningen till handlingens skala och effekt. Ett agerande vars skala och effekt motsvarar en traditionell beväpnad attack ska anses vara ett *väpnat angrepp*. Denna skala och effekt måste bedömas i varje enskilt fall.[70]

4 Tillämpningsproblematik och tillvägagångssätt

Våldsförbudet tillkom i en tid innan cyberrymden, när hot bestod av stridsvagnar och flygplan.[71] Tiden förändras och reglerna måste tolkas om efter nya förutsättningar. Dock uppstår problem och gränsdragningsfrågor när våldsförbudet ska tillämpas på cyberoperationer.[72]

Cyberoperationer är i sig inte reglerade eller förbjudna enligt folkrätt. Däremot kan sättet cyberoperationer utförs på vara otillåtet.[73] En cyberoperation som uppnår *bruk av våld* anses

[64] Se exempel Henderson, s. 50, 55–68.
[65] Nicaragua-målet.
[66] Nicaragua-målet, para 191.
[67] Schmitt (2017), s. 341.
[68]Delerue, s. 276, Schmitt (2017), s. 332–333.
[69] Henderson, s. 63, Schmitt (2017), s. 333.
[70] Nicaragua-målet, para 195.
[71] Henderson, s. 55.
[72] Delerue, s. 4–5, Schmitt (2017), s. xxv.
[73] Jensen, s. 755–756, Schmitt (2017), s. 168, 329–330.

vara otillåten.[74] Detta kräver dock att regeln kan appliceras. Som berörs ovan (avsnitt 3.2) finns det olika tolkningar på våldsförbudets tillämpning och vad gäller cyberoperationer finns det främst tre tillvägagångssätt som diskuteras: målbaserat, instrumentbaserat och konsekvensbaserat.[75]

Målbaserat tillvägagångssätt fokuserar på objektet som utsätts för en attack. Handlingar som påverkar kritisk infrastruktur klassas som *bruk av våld* enligt detta synsätt. Hänsyn tas inte till instrumentet som används eller effektens omfattning. Utifrån detta synsätt kan cyberoperationer strida mot våldsförbudet under förutsättning att de riktar sig mot särskilt viktiga mål. Däremot riskerar detta att bli allt för inkluderande och omfatta orimligt många ageranden mellan stater, vilket har kritiserats. För att undgå kritiken kan mål i stället användas som en faktor av flera att beakta vid tillämpning av andra tillvägagångssätt.[76]

Det instrumentbaserade tillvägagångssättet innebär att cyberoperationer anses vara ett vapen i sig mot bakgrund av operationens syfte. Har cyberoperationen ett syfte som tidigare främst kunnat uppnås genom konventionella vapen eller otillåtna former av sabotage, exempelvis att skada ett kärnkraftverk, kan det anses vara *bruk av våld*. Dock kan det vara svårt att avgöra vad en cyberoperation har för syfte och om det är ämnat att användas som vapen. Alternativet är att undersöka om cyberoperationer har samma karaktärsdrag som traditionella vapen men även detta är problematiskt med tanke på stora skillnader. Tillämpningen av detta tillvägagångssätt är svårt och har kritiserats därav.[77] Fördelen är att konsekvenserna inte behöver beaktas, utan det är endast den använda metoden som avgör om agerandet strider mot våldsförbudet. Tillvägagångssättet gör det möjligt att särskilja konsekvenser som i sig är detsamma men som uppkommer av två olika former av våld. Exempelvis om samma konsekvenser uppkommer vid ekonomiskt tvång och en väpnad attack.[78]

Den lämpligaste metoden enligt många experter är det konsekvensbaserade tillvägagångssättet.[79] Det avgör om en cyberoperation uppnår tröskeln för *bruk av våld* genom att se till konsekvenserna av agerandet utifrån ICJ:s kriterier om skala och effekt. En cyberoperation med en viss effekt strider mot våldsförbudet om den uppnår en skala och

[74] Schmitt (2017), s. 329–330.
[75] Roscini, s. 46–47.
[76] Delerue, s. 288–289, Roscini, s. 47.
[77] Delerue, s. 286–287, 289, Graham, s. 91, Roscini, s. 46–47.
[78] Woltag, s.142–143.
[79] Se exempel Roscini, s. 47 och Schmitt (2017), s. 330–337.

effekt som kan jämföras med handlingar i verkliga världen som når upp till nivån *bruk av våld*.[80] Fördelen är att tillvägagångsättet kan beakta både målet och vapnet som används, men är inte begränsad till endast dessa faktorer.[81]

Fall det inte råder någon oenighet om är de som orsakar fysiska konsekvenser såsom omfattande skada på människor eller objekt. Den svåraste gränsdragningen är när en cyberoperation inte orsakar fysiska skador men trots det har negativa konsekvenser för den utsatta staten.[82] I Nicaragua-målet har ICJ konstaterat fysisk skada inte är nödvändigt för att en handling ska strida mot våldsförbudet. Däremot finns ingen vägledning vilka handlingar som inte orsakar fysiska skador och i jämförelse är lika allvarliga.[83]

Vid en jämförelse med verkliga världen kan konstateras att icke-destruktiva cyberoperationer med syfte att påverka människor psykologiskt, genom att underminera en regering eller förbjuda e-handel med viss stat, inte utgör *bruk av våld*. Inte heller finansiering av hackare som driver uppror mot en regering anses tillräckligt för att tillämpa våldsförbudet. Dock är förbudet inte begränsat till militära insatser. Därför kan överlämning av skadlig programvara och utbildning därom till en icke-statlig grupp utgöra *bruk av våld*, om syftet är att programvaran ska användas mot en annan stat.[84]

Vidare scenarion som utgör gränsdragningsproblematik är cyberoperationer som rikas mot den internationella aktiemarknaden eller mot kritisk infrastruktur. Vissa experter anser att detta kan få långtgående och allvarliga effekter som kan likställas med ett *väpnat angrepp* även utan att människoliv direkt skadas. Andra experter anser att ekonomisk skada inte kan utgöra ett *väpnat angrepp* och därför kan dessa exempel inte klassas som det heller.[85] Det bör likväl noteras att ekonomiskt tvång i sig uteslöts ur våldsförbudet när det kom till 1945.[86] Det finns även de som anser att cyberoperationer som förstör kritisk infrastruktur alltid ska anses uppnå *bruk av våld*.[87] Däremot delar inte alla experter denna åsikt. I och med att det konsekvensbaserade tillvägagångsättet bedömer händelsen ur ett helhetsperspektiv kan målet

[80] Lin, s. 73–74, Schmitt (2017), s. 330–333.
[81] Roscini, s. 47–51.
[82] Lin, s. 73–74, Schmitt (2017), s. 333, 341.
[83] Nicaragua-målet, para 228, Schmitt (2011), s. 575.
[84] Schmitt (2017), s. 330–332.
[85] Schmitt (2017), s. 342–343.
[86] Roscini, s. 45–47.
[87] Woltag, s. 144.

oavsett vara det som slutligen avgör om en handling ska anses vara i strid med våldsförbudet. På detta sätt kan cyberoperationer mot kritisk infrastruktur bedömas som allvarligare.[88]

Ytterligare ett intressant exempel är huruvida påverkansoperationer på val i andra stater anses vara *bruk av våld* eller inte. Våldsförbudet i FN-stadgan stadgar uttryckligen att våld inte får användas mot andra staters politiska självständighet. Dock uteslöts politiskt tvång från våldsförbudet när det först skapades vilket talar emot att påverkansoperationer omfattas. Generellt anses påverkan på andra staters val inte utgöra *bruk av våld*.[89]

Eftersom det inte finns en tydlig förklaring vilken skala och effekt som krävs har experterna bakom Tallinn manualen 2.0 undersökt vad stater brukar överväga vid karaktärisering av cyberoperationer. Utifrån undersökningen sattes åtta kriterier upp över faktorer som kan påverka staters bedömning. Dessa kan vara utgångspunkten för att avgöra om en cyberoperations konsekvenser är jämförbara med en våldshandling i verkliga världen.[90] Kriterierna är:

- Allvarlighetsgrad: nivå av konsekvenser på kritiska nationella intressen utifrån omfattning, varaktighet och intensitet. Detta kriterium väger tyngst.
- Omedelbarhet: tidsmässig aspekt där omedelbara konsekvenser anses värre och skapar mindre möjlighet till fredliga lösningar. Det anses mindre allvarligt om konsekvenserna intensifieras och byggs upp långsamt under en längre tid.
- Rättfram: orsakssambandet mellan handlingen och konsekvenserna.
- Intrång: graden av intrång mot staten och deras digitala system.
- Mätbarhet av effekterna: huruvida konsekvenserna är uppenbara eftersom de direkta effekterna av våldshandlingar ofta är enkla att mäta.
- Militära karaktär: koppling mellan cyberoperationen och militär verksamhet.
- Statlig inblandning: desto närmare koppling till staten desto större sannolikhet att det klassas som *bruk av våld*.
- Presumtiv laglighet: det som inte uttryckligen förbjuds i folkrätt antas vara tillåtet.[91]

[88] Delerue, s. 298.
[89] Delerue, s. 285–286, Roscini, s. 45–46, 65, Schmitt (2011), s. 574.
[90] Schmitt (2017), s. 333–337.
[91] Schmitt (2017), s. 333–337.

Dessa kriterium ger vägledning och kan bidra med en metod för att klassificera offensiva cyberoperationer utan fysiska konsekvenser som otillåtna under våldsförbudet. Genom att se till helhetsbilden är det tänkbart att exempelvis attackerna mot Estland 2007 klassas som *bruk av våld*, även om det inte skedde några fysiska skador.[92] En sådan helhetsbild gör det även möjligt att klassificera en cyberoperation mot kritisk infrastruktur som brott mot våldsförbudet. Trots att cyberoperationen inte skadar några människoliv och förutsatt att den är mycket allvarlig.[93]

Många cyberoperationer hamnar under tröskeln för *bruk av våld* enligt doktrin[94] och det finns ännu inget mål i ICJ som säger annat. Stuxnet hade troligen ansetts strida mot våldsförbudet om det hade gått att med säkerhet härleda till en stat.[95] Experter är överens om att Stuxnet i sig utgjorde *bruk av våld* på grund av dess omfattande effekter på fysiska objekt. Dock finns oenighet om huruvida det nådde upp till *väpnat angrepp*.[96]

Det kan även finnas skäl att tillämpa både instrument- och konsekvensbaserat tillvägagångssätt tillsammans eftersom vapen ofta innebär omfattande konsekvenser. Samspelet mellan dessa kan därför bidra till en heltäckande förståelse för vad som utgör *bruk av våld*.[97] Roscini menar att konsekvenser och instrument definierar varandra: ”it is the instrument used that defines armed force, but the instrument is identified by its (violent) consequences”.[98]

Slutligen bör det noteras att bara för att en handling inte uppnår *bruk av våld* betyder det inte att den är tillåten.[99]

[92] Schmitt (2011), s. 577–578.
[93] Roscini, s. 62–63.
[94] Se exempel Roscini, s. 63–65.
[95] Schmitt (2013), s. 45, Woltag, s. 49.
[96] Schmitt (2017), s. 341–343.
[97] Roscini, s. 49–51.
[98] Roscini, s. 50.
[99] Schmitt (2017), s. 330.

5 Analys och slutsats

5.1 Cyber-begrepp och våldsförbudet

Syftet med uppsatsen är att undersöka under vilka förutsättningar cyberoperationer tillåts enligt våldsförbudet.

Till att börja med kan det konstateras att både cyberrymden och cyberoperationer saknar entydiga definitioner. Genomgående är dock att cyberrymden är den virtuella verklighet som människor kan tillgå via datornätverk. Cyberoperationer är olika handlingar som företas i cyberrymden. Det kan vara svårt att placera en enskild cyberoperation under en viss underkategori eftersom syftet med operationen inte nödvändigtvis framgår tydligt. Utredningen visar att det främst är gränsdragningen för offensiva cyberoperationer som är problematisk. Intresset av att använda cybersäkerhet för att skydda staten vägs mot den skada handlingen kan innebära för en annan stat som utsätts. Det är därför offensiva cyberoperationer är intressanta att undersöka i förhållande till våldsförbudet.

Utifrån konkreta exempel är det främst offensiva cyberattacker som i praktiken riskerar att nå upp till våldsförbudet. Dock kan det inte uteslutas att även offensiv cyberexploatering kan nå upp till denna tröskel. Dessutom är det svårt för en utsatt stat att veta om cyberoperationen har ett destruktivt syfte eller inte. Därför särskiljs inte dessa åt i analysen.

Våldsförbudet är en central regel inom folkrätt men som visas är dess innebörd inte självklar. Både ICJ:s uttalande och statlig praxis talar för att våldsförbudet i FN-stadgan och i internationell sedvanerätt överensstämmer i all väsentlighet innehållsmässigt. Eftersom detta är de aktörer som har störst inflytande på folkrätt antas det i uppsatsen att innehållet är detsamma. Vad våldsförbudet innebär i sak diskuteras och besvaras ovan i avsnitt 3.2 och efterföljande underrubriker.

5.2 Gällande rätt för offensiva cyberoperationer

Utredningen visar att våldsförbudet inte sätter något absolut förbud mot offensiva cyberoperationer. Utifrån Nicaragua-målet i ICJ framstår det som att det är en relativt hög gräns för vad som anses strida mot våldsförbudet. ICJ:s tolkning av våldsförbudet talar även för en bred betydelse som inte är begränsad till traditionella vapen.

Det är problematiskt att hävda att offensiva cyberoperationer per se alltid är otillåtna. Ovanstående utredning visar att det inte finns en klar gräns för vilka offensiva cyberoperationer som tillåts och få experter gör en hård gränsdragning. Utifrån våldsförbudets höga tröskel är det sannolikt att vissa offensiva cyberoperationer är tillåtna. Hur de tillåtna cyberoperationerna ska skiljas från de otillåtna finns det olika tillvägagångssätt för som kan ge olika resultat. En jämförelse måste därför göras i det enskilda fallet för att avgöra handlingens laglighet.

Det konsekvensbaserade tillvägagångssättet är det som flest förespråkar, inklusive författarna bakom Tallinn manualerna. Det framstår som rimligt eftersom tillvägagångssättet bidrar med en helhetsbild på händelsen och dess effekter. Dessutom överensstämmer det med ICJ:s metod för att klassificera om en handling utgör *bruk av våld* genom att ta hänsyn till skala och effekt vid bedömningen. Mycket talar därmed för att effekten har en betydande roll vid bedömningen av *bruk av våld*. Det går inte att bortse från att detta tillvägagångssätt har fördelen av att den även kan ta in andra faktorer, såsom mål och instrument. Därför ska de tre cyberoperationerna som beskrivits ovan (avsnitt 2.3) analyseras utifrån det konsekvensbaserade tillvägagångssättet i ett försök att ytterligare tydliggöra gränsen för våldsförbudet och cyberoperationer.

De tre cyberoperationerna som exemplifieras har aldrig officiellt erkänts som handlingar i strid med våldsförbudet. Dock är som nämnt flera experter eniga om att Stuxnet i teorin når upp till *bruk av våld* och därmed våldsförbudet. Det kan likväl finnas skäl att argumentera för att även de andra två bör klassificeras som *bruk av våld*. Stuxnet orsakade skada på fysiska objekt av allvarlig grad. Skadan påverkade kärnkraftsverksamhet vilket kan anses utgöra kritisk infrastruktur. Handlingen orsakade en skada som tidigare hade krävt användning av traditionella vapen eller annat otillåtet våld såsom sabotage. Med dess precision innebar cyberoperationen ett grovt intrång i en ytterst säker anläggning. Dessutom misstänks stor inblandning av statlig militär verksamhet. Även om inte alla effekter är mätbara är det möjligt att räkna hur många centrifuger som fysiskt skadades. Denna fysiska skada vållade ett bakslag för utvecklingen av Irans kärnkraftsprogram. Det finns dessutom ett starkt samband mellan användningen av Stuxnet, som med oerhörd precision riktade in sig särskilt på programvaran som användes i Irans kärnkraftverk, och skadan viruset orsakade. Utifrån kriterierna i Tallinn manualen finns det mycket som talar för att Stuxnet utgör *bruk av våld* (möjligen även *väpnat angrepp*) och är en otillåten cyberoperation. Helhetsbilden av Stuxnet

utifrån det konsekvensbaserade tillvägagångssättet, med influenser från både det instrument- och målbaserade tillvägagångssättet, ger stöd för att handlingen bröt mot våldsförbudet. Detta är därför i dagsläget det tydligaste exemplet på en cyberoperation som bryter mot våldsförbudet.

De andra två exemplen finns det inte samma enighet kring. Det är konstaterat att cyberoperationen mot Estland inte uppnår *väpnat angrepp* men det är inte klarlagt om attacken når upp till det något lägre kravet på *bruk av våld*. Attacken mot Estland är det som uppmärksammade världen på att cyberoperationer utgör ett potentiellt allvarligt hot. Även om misstanke riktats mot Ryssland är kopplingen inte konstaterad och med tanke på den relativt enkla tekniken bakom attacken är det möjligt att privata aktörer med mindre resurser ligger bakom händelsen. Cyberoperationen riktades mot kritiska nationella intressen och verksamheter. Dessutom orsakade händelsen stora administrativa, ekonomiska och kommunikativa problem för Estland som kom att påverka landet lång tid därefter. Däremot inträffade det aldrig någon fysisk skada av nämnvärd omfattning. Doktrin talar för att fysisk skada krävs för att med säkerhet konstatera att ett agerande utgör *bruk av våld*. Ingen sådan fysisk skada konstaterades i Estland. Det är däremot tänkbart att även en cyberoperation med icke-fysiska konsekvenser kan innebära *bruk av våld* om helhetsbilden av andra faktorer är av jämförlig allvarlighetsgrad. Effekterna efter händelsen är svåra att mäta, exempelvis går det inte att mäta vilka skador som uppkommit på grund av att myndigheterna har haft svårt att kommunicera med medborgare.

Utifrån en helhetsbedömning och med hänsyn till våldsförbudets höga tröskel bör inte händelsen i Estland anses uppnå *bruk av våld*. Detta innebär inte att cyberoperationen mot Estland 2007 var tillåten enligt folkrätt. Även om cyberoperationen inte strider mot våldsförbudet är det mjöligt att den strider mot andra principer såsom non-intervention eller suveränitetsprincipen.

Beträffande cyberoperationen mot Ukraina 2015 var det kritisk infrastruktur som påverkades och tog fysisk skada som i sin tur resulterade i strömavbrott. Strömavbrottet pågick endast under några timmar men det påverkade uppemot 250 000 invånare. Strömavbrottet hade kortvariga konsekvenser och var inte lika allvarligt som förstörelse av centrifuger i kärnkraftverk men attacken hade trots allt stor omfattning. Det är enkelt att mäta de direkta och uppenbara konsekvenserna genom att undersöka hur många hushåll som påverkandes och under hur lång tid. Konsekvenserna uppkom omedelbart efter attacken och hade tydligt

orsakssamband till attacken eftersom den riktade sig mot kraftnätet. Rysk statlig och militär inblandning misstänks men är inte bekräftad. Det framgår inte vilken säkerhet som kraftnätet hade och därför är det svårt att uttala sig om hur grovt intrånget var. Cyberoperationen bör även ses i sitt sammanhang som den allvarligaste attacken i en våg av flera vilket bör öka sannolikheten att klassa handlingen som *bruk av våld*. Även om politiskt våld i sig inte omfattas av våldsförbudet är det möjligt att syftet bakom cyberoperationen, att påverka Ukrainas beslut om EU, kan bidra till att attackerna tolkas som mer allvarliga. Det som är avgörande är i slutändan huruvida konsekvenserna kan anses uppnå den skala och effekt som motsvarar användningen av traditionella väpnade styrkor. Kraftnät kan i och för sig skadas även vid kraftigare oväder utan mänsklig inblandning. Emellertid är det svårt att tänka sig att andra stater eller aktörer kan orsaka motsvarande skador utan att använda sig av traditionella otillåtna metoder, exempelvis väpnade styrkor eller medvetet sabotage.

Experter är försiktiga i att uttala sig om huruvida händelsen i Ukraina utgör *bruk av våld*. Utifrån flera avvägningar och det konsekvensbaserade tillvägagångssättet finns dock flera argument för att klassificera händelsen som *bruk av våld*.

Vid första tanke framstår det som möjligt att även påverkansoperationer mot val utgör *bruk av våld*. Undersökningen har däremot visat att det inte är fallet eftersom politisk press uteslöts ur våldsförbudets omfattning när det skapades. Förbudets omfattning framgår emellertid inte uttryckligen av FN-stadgans skrivelse som snarare bjuder in till en bredare tolkning med hänvisningen till politiskt oberoende. Det är möjligt att synsättet på våldsförbudets omfattning förändras i framtiden. Dock lär en sådan förändring kräva ett uttryckligt ställningstagande från FN eller en förändring av staters praxis. Påverkansoperationer kan däremot bryta mot andra internationella normer vilket är ett intressant ämne att undersöka vidare.

Slutligen kan konstateras att det finns angränsade områden som är intressanta att undersöka vidare. Våldsförbudet har en hög tröskel och en cyberoperation som faller under våldsförbudet är inte nödvändigtvis laglig enligt folkrätt. Därför kan framtida forskning med fördel undersöka gränsområdet under tröskeln för våldsförbudet, exempelvis genom att utreda non-intervention eller suveränitetsprincipen i förhållande till offensiva cyberoperationer.

5.3 Är nuvarande lagstiftning tillräcklig?

Utifrån ett kritiskt perspektiv kan folkrättens lämplighet ifrågasättas. Även om det råder konsensus att folkrätt är tillämpligt är det inte nödvändigtvis det mest fördelaktiga. Två av tre exempel i uppsatsen anses uppnå tröskeln för *bruk av våld* men det finns otaligt antal cyberoperationer som inte strider mot våldsförbudet. Trots det kan cyberoperationerna utgöra en allvarlig kränkning och orsaka omfattande skador på digitala värden som i dagens samhälle blir allt viktigare. Vidare finns problem med klassificeringar eftersom det inte finns någon juridisk eller vedertagen definition för cyberoperationer.

Med hänsyn till detta resonemang och cyberoperationers speciella karaktär kan det vara lämpligare att skapa ett eget regelverk som endast adresserar cyberoperationer och deras laglighet i internationella relationer. Risken med tillämpning av existerade folkrätt, som tillkom långt innan cyberoperationer var ett hot, är att reglerna missar viktiga övervägningar som är oviktiga i verkliga världen. Fördelen med redan existerade folkrätt och tillämpningen av FN-stadgan är att det redan finns ett etablerat system och praxis som inte kräver någon ny statlig överenskommelse. Det är svårt att nå konsensus kring internationella överenskommelser på ett område av denna känsliga karaktär som har nära koppling till staters militär och försvar. Dock finns det goda skäl till att undersöka möjligheten att skapa ett regelsystem specifikt för cyberoperationer i syfte att förebygga oklarheter och undvika att farliga cyberoperationer går oreglerade.

5.4 Slutsats

Uppsatsen konstaterar att en handling anses utförd i strid mot våldsförbudet förutsatt att den kategoriseras som *bruk av våld*. Utredningen visar att våldsförbudet i artikel 2 paragraf 4 FN-stadgan och internationell sedvanerätt inte förbjuder all användning av offensiva cyberoperationer. Däremot är det inte möjligt att ange specifika förutsättningar som alltid resulterar i att en cyberoperation uppnår *bruk av våld* utan det måste bedömas i det enskilda fallet. ICJ anser att andra handlingar än väpnade styrkor kan uppnå *bruk av våld* förutsatt att konsekvenserna uppnår samma skala och effekt. För att göra denna bedömning konstateras att det finns tre tillvägagångssätt varav det konsekvensbaserade tillvägagångssättet är lämpligast. Efter tillämpning av det konsekvensbaserade tillvägagångssättet bedöms två av tre verkliga cyberoperationer vara *bruk av våld*. Vidare konstaterar uppsatsen att i praktiken

krävs vanligtvis fysisk skada för att klassificera en handling som *bruk av våld*. Trots det kan olika faktorer i bedömningen samspela på ett sätt som gör det tänkbart att en cyberoperation utan fysiska konsekvenser kan uppnå *bruk av våld*. Ett sådan exempel har dock ännu inte uppstått i verkligen.

Sammanfattningsvis är rättsläget oklart eftersom våldsförbudet inte sätter en exakt gräns för användning av cyberoperationer. Många offensiva cyberoperationer faller under tröskeln för *bruk av våld*. Våldsförbudet förbjuder åtminstone med säkerhet de mest allvarliga cyberoperationerna som berövar människoliv eller skadar fysiska objekt. Offensiva cyberoperationer som allvarligt skadar människor eller objekt kan därför aldrig tillåtas av våldsförbudet, även om syftet är att skydda den egna staten.

Käll- och litteraturförteckning

Litteratur

Baezner, Marie. ’Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict’. Version 2. Center for Security Studies (CSS), ETH Zürich, 2018.

Baezner, Marie och Robin, Patrice. ’Hotspot Analysis: Stuxnet’. Center for Security Studies (CSS), ETH Zürich, 2017.

Delerue, François. *Cyber operations and international law*. Cambridge: Cambridge University Press, 2020.

Dörr, Oliver och Randelzhofer, Albrecht: *Ch.I Purposes and Principles, Article 2 (4)* i: Simma, Bruno, Khan, Daniel-Erasmus, Nolte, Georg, Paulus, Andreas och Wessendorf, Nikolai (red.). *The Charter of the United Nations: A Commentary, Volume 1*. 3 uppl. Oxford: Oxford University Press, 2012. E-bok.

Graham, Davis E. ’Cyber Threats and the Law of War’. Journal of National Security Law & Policy, JNSLP Vol. 4 nr. 1, 2010.

Gray, Christine. *International law and the use of force*. 4 uppl. Oxford: Oxford University Press, 2018. E-bok.

Henderson, Christian. *The use of force and international law*. 3 uppl. Cambridge: Cambridge University Press, 2018. E-bok.

Henriksen, Anders. *International law*. 3 uppl. Oxford: Oxford University Press, 2021.

Jensen, Eric Talbot. ’The Tallinn Manual 2.0: Highlights and Insights’. BYU Law Research Paper No. 17–10, 2017.

Kleineman, Jan: *Rättsdogmatisk metod* i: Nääv, Maria och Zamboni, Mauro (red.). *Juridisk metodlära*. 2 uppl. Lund: Studentlitteratur, 2018.

Kozłowski, Andrzej. ’Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan’. European Scientific Journal, ESJ Special Edition Vol. 3, 2014.

Lin, Herbert S. ’Offensive Cyber Operations and the Use of Force’. Journal of National Security Law & Policy, JNSLP Vol. 4 nr. 1, 2010.

Roscini, Marco. *Cyber operations and the use of force in international law*. Oxford: Oxford University Press, 2014. E-bok.

Sandgren, Claes. *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. 4 uppl. Stockholm: Norstedts Juridik, 2018.

Schmitt, Michael N. ’Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’. Columbia Journal of Transnational Law, Vol. 37, 1998-99, 1999.

Schmitt, Michael N. ’Cyber Operations and the Jus Ad Bellum Revisited’. Villanova Law Review, Vol. 56, 2011.

Schmitt, Michael N. (red.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. E-bok.

Schmitt, Michael N. (red.). *Tallinn manual 2.0 on the international law applicable to cyber operations: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*. 2 uppl. Cambridge: Cambridge University Press, 2017.

Smeets, Max. ’The Strategic Promise of Offensive Cyber Operations’. Strategic Studies Quarterly, Vol. 12, No. 3, 2018.

Solis, Gary D. *The law of armed conflict: international humanitarian law in war*. 2 uppl. New York: Cambridge University Press, 2016.

Woltag, Johann-Christoph. *Cyber warfare: military cross-border computer network operations under international law*. Cambridge: Intersentia, 2014.

Resolutioner

UNGA A/RES/2625(XXV), ’Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations’, (24 oktober 1970), UN Doc A/RES/2625(XXV).

UNGA A/RES/73/266, ’Advancing responsible State behaviour in cyberspace in the context of international security’, (2 januari 2019), UN Doc A/RES/73/266.

UNGA A/RES/73/27, ’Developments in the field of information and telecommunications in the context of international security’, (11 december 2018), UN Doc A/RES/73/27.

Tidningsartiklar

Brewster, Thomas. ’ ‘Most Severe’ Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider’. Forbes, 2022-03-28. https://www.forbes.com/ (Hämtad 2022-04-21).

Sanger, David E. ’Obama Order Sped Up Wave of Cyberattacks Against Iran’. The New York Times, 2012-06-01. https://www.nytimes.com/ (Hämtad 2022-04-21).

Svahn, Clas. ’USA och Storbritannien rustar för offensiva cyberattacker’. Dagens Nyheter, 2018-09-21. https://www.dn.se/nyheter/varlden/usa-rustar-for-offensiva-cyberattacker/ (Hämtad 2022-04-21).

Svensson, Adam. ’Ryska cyberattacker drabbade 39 delstater inför USA-valet’. Dagens Nyheter, 2017-06-13. https://www.dn.se/nyheter/varlden/ryska-cyberattacker-drabbade-39-delstater-infor-usa-valet/ (Hämtad 2022-04-21).

Övrigt

CISA. ’Security Tip (ST04-001). What is Cybersecurity?’, 2019. https://www.cisa.gov/uscert/ncas/tips/ST04-001 (Hämtad 2022-03-29).

Dragos Inc. ’CRASHOVERRIDE: Threat to the Electric Grid Operations’, 2017. https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf (Hämtad 2022-04-03).

Joint Chiefs of Staff. ’Joint publication 3-12 Cyberspace Operations’, 2018.

Oxford English Dictionary ”cybersecurity”: "cyber-, comb. form". OED Online. Oxford University Press. https://www-oed-com.ludwig.lub.lu.se/view/Entry/250879?redirectedFrom=cybersecurity (Hämtad 2022-04-04).

Oxford English Dictionary ”cyberspace”: "cyberspace, n.". OED Online. Oxford University Press. https://www.oed.com/viewdictionaryentry/Entry/240849 (Hämtad 2022-03-29).

United Nations (hemsida). ’About us’. https://www.un.org/en/about-us/un-charter (Hämtad 2022-04-04).

Rättsfallsförteckning

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), ICJ Reports 1996.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits (1986) ICJ Reports 14.