JURIDISKA FAKULTETEN

vid Lunds universitet

Ida Sahlin

Rättsläget vid den digitala frontlinjen

En analys av självförsvarsrätten och principen om nödvändighet vid cyberattacker

LAGF03 Rättsvetenskaplig uppsats

Kandidatuppsats på juristprogrammet

15 högskolepoäng

Handledare: Aurelija Lukoseviciene

Termin: HT23

Innehåll

Summary

Many of society's bearing functions are today digitalized. A hostile actor can therefore through cyber-attacks cause damage to a state in a degree previously possible only through physical attacks. Therefore, warfare has entered a new arena, but it is still unclear under which circumstances a state under attack is allowed to use force in self-defence against cyber-attacks.

International law states a prohibition of use of force, incorporated in the UN-Charter art. 2(4). The right of self-defence is one of few exceptions to the prohibition, but it is only when a state is subjected to an armed attack that the right is granted. What is considered an armed attack remains disputed. At the assessment of the attack the scale and effect are taken into consideration, but these criteria are loosely defined which makes the interpretations uncertain.

The event of an armed attack against a state does not automatically inherit the states right to self-defence since the necessity of self-defence must be considered. The necessity assessment is conducted in the same way regarding physical attacks, as well as cyber-attacks even though the cyber element somehow complicates the assessment. Malicious malware can remain latent in systems months before they attack, aggravating the temporal necessity, and the consequences of a cyber-attack are also difficult to precisely measure.

When a cyber-attack is considered an armed attack and how the principle of necessity limits the exercise of any right to self-defence is investigated. The investigation is conducted through an international and critical perspective along with a legal dogmatic methodology.

No cyber-attack has ever qualified as an armed attack, causing a lack of state praxis in the area. Exactly how the demands of scale and effect are to be defined remains unclear, but it is clear, that a cyber-attack must cause physical damage to be able to count as an armed attack. The cyber element complicates the necessity assessment. However, it does not make the use of self-defence against cyber-attacks impossible.

Sammanfattning

Idag är många av staters bärande samhällsfunktioner digitaliserade. En fientlig aktör kan således genom cybermedel orsaka skador för en stat i en grad som förr endast var möjlig genom fysiska medel. Krigsföring har således fått en ny arena, men det är ännu oklart under vilka förutsättningar en utsatt stat får bruka våld i självförsvar mot en cyberattack.

I internationell rätt finns ett allmänt våldsförbud som kodifierats i FN-stadgan art. 2(4). Rätten till självförsvar är ett av få undantag till förbudet men det är endast då en stat är utsatt för ett väpnat angrepp som rätt ges att bruka våld i självförsvar. Vad som anses utgöra ett väpnat angrepp är omdiskuterat. Vid bedömningen ses till angreppets skala och effekt men kriterierna saknar tydlig definition vilket gör dess tillämpning oklar.

Att en stat är utsatt för ett väpnat angrepp innebär inte automatiskt att staten har rätt till legitim våldsanvändning i självförsvar, utan det måste ses till självförsvarets nödvändighet. Nödvändighetsbedömningen sker på samma vis vid kinetiska angrepp som vid cyberattacker men cyberelementet försvårar bedömningen. Inte minst av den anledning att en skadlig mjukvara kan ligga latent i datorsystem månader innan attacken vilket försvårar den tidsmässiga nödvändigheten men också då det är svårt att tydligt mäta konsekvenserna av en cyberattack.

När en cyberattack anses utgöra ett väpnat angrepp samt hur nödvändighetsprincipen begränsar utövandet av eventuell självförsvarsrätt utreds genom en rättsdogmatisk metod med ett internationellt och kritiskt perspektiv.

I dagsläget saknas fall då en cyberattack kvalificerats som ett väpnat angrepp och det finns således ingen statspraxis på området. Exakt hur kraven på skala och effekt ska definieras är oklart, men konsensus råder kring det faktum att en cyberattack måste orsaka fysiska skador för att utgöra ett väpnat angrepp. Nödvändighetsbedömningen försvåras av cyberelementet men den omöjliggör inte på något vis utövande av rätten till självförsvar mot cyberattacker.

Förkortningar

EU	Europeiska Unionen
FN	Förenta Nationerna
FN-stadgan	Förenta Nationernas Stadga
ICJ	International Court of Justice
ICJ-stadgan	Stadgan för den Internationella domstolen
NATO	North Atlantic Treaty Organization
UNGA	United Nations General Assembly
USA	Amerikas Förenta stater (United States of America)

1 Inledning

1.1 Bakgrund

Den 24 februari 2022 lamslås Europa då Ryssland inleder sin fullskaliga invasion av Ukraina. Sedan Rysslands annektering av Krim-halvön 2014 har Ukraina vidtagit olika åtgärder i självförsvar, men invasionen ses av många som en separat händelse och Ukrainas rätt till självförsvar ifrågasattes inte.[1] Något som hamnat i skymundan är de digitala trupper som under det senaste decenniet utfört en rad cyberattacker mot Ukraina. Både 2015 och 2016 slogs en majoritet av Ukrainas elnät ut efter cyberattacker, vilket gav konsekvenser för hundratusentals människor, utan att Ukraina vidtog våldsamma åtgärder till svar.[2] Detta är inte första gången stater använder sig av cyberattacker för att främja egna intressen, och inte heller första gången en sådan attack inte får direkt svar från den utsatte staten. Ett annat uppmärksammat exempel är *Stuxnet,* den första cyberattacken som orsakade fysisk skada. Attacker som dessa beskrivs ofta som bidragande till ett epokskifte, jämförbart med 9/11, vilket satt modern krigföring i ett helt nytt ljus.[3]

Traditionellt har krig betraktats som utmärkande av konventionella vapen och det är med denna utgångspunkt Förenta nationernas Stadga[4] och rätten till självförsvar i dess art. 51 tillkom.[5] Sedan dess har frågan om vad som utgör ett väpnat angrepp varit omdiskuterad. Samhället förändras och krigföringen likaså. Många bärande samhällsfunktioner är idag digitaliserade, följaktligen är det således möjligt att genom cybermedel orsaka en annan stat skador som förr endast var möjligt genom en konventionell attack.[6]

En stats faktiska utövande av rätten till självförsvar i de fall ett väpnat angrepp förekommer begränsas dock av principen om nödvändighet. Principen inne-

[1] Milanovic, *ELIJ: Talk!*.
[2] Cerulus, *Politico*.
[3] Jägemar O, *SVT Nyheter*.
[4] Hädanefter FN-stadgan.
[5] Henderson, s. 55.
[6] Roscini, s. 1-3.

bär att icke-våldsamma åtgärder inte ska anses tillräckliga för att avvärja attacken.[7] Cyberattacker utmärks av det faktum att de kan slå till och passera inom loppet av ett par minuter. Det är heller inte alltid självklart vilken omfattning angreppet har.[8] Dessa karaktäristiska drag hos cyberattacker möjliggör en diskussion om huruvida principen om nödvändighet i praktiken omöjliggör utövandet av självförsvar mot en cyberattack.

1.2 Syfte och frågeställningar

Mot bakgrund av ovanstående är syftet med uppsatsen att utreda när en cyberoperation utförd av en stat mot en annan, *jus ad bellum*, anses utgöra ett väpnat angrepp i den mening som aktualiserar rätten till självförsvar enligt art. 51 FN-stadgan. Uppsatsen syftar dessutom till att undersöka principen om nödvändighet i en cyberkontext. För att närma sig uppsatsens syften lyder frågeställningarna som följande:

- När har en stat rätt till självförsvar vid ett cyberangrepp?
- Hur begränsar principen om nödvändighet utövandet av självförsvar i en cyberkontext?

1.3 Avgränsningar

Uppsatsen ämnar utreda rätten till självförsvar i en cyberkontext, *jus ad bellum*, det vill säga i de fall det inte råder en väpnad konflikt sedan tidigare. Av denna anledning kommer, *jus in bellum*, det vill säga rätten i krig, inte beröras.

Rätten till självförsvar i internationell rätt innehåller många parametrar men av utrymmesskäl kommer fokus ligga på problematiken kring vad som utgör ett väpnat angrepp. Av samma anledning kommer endast cyberattacker utförda av en stat mot en annan behandlas och den omfattande hänförbarhets-

[7] Schmitt (2017), s. 348-349.
[8] Roscini, s. 2.

problematiken kommer således inte beröras. Inte heller staters uppsåt kommer behandlas närmare, det kommer således utan vidare problematisering antas att de fall som diskuteras är hänförbara till aktuell stat samt utförda med uppsåt.

Övriga frågor inom området såsom bedömningen av när en cyberoperation bryter mot det allmänna våldsförbudet kommer med hänsyn till uppsatsens omfång endast kort beröras i syfte att ge kontext till den vidare diskussionen om rätten till självförsvar.

Vid utövande av rätten till självförsvar talas ofta om principen om nödvändighet och proportionalitet. Till följd av uppsatsens begränsade omfång kommer endast principen om nödvändighet att behandlas. Detta val motiveras vidare av att denna princip primärt används vid bedömningen av när en stat kan agera i självförsvar medan principen om proportionalitet snarare lägger fokus på hur självförsvaret ska utformas.

1.4 Metod och material

För att besvara ovan nämnda frågeställningar kommer en rättsdogmatisk metod tillämpas parallellt med ett kritiskt och internationellt perspektiv. Accepterade rättskällor kommer således systematiseras samt tolkas i syfte att fastställa gällande rätt.[9] Metoden lämpar sig då uppsatsen delvis ämnar utreda hur rätten till självförsvar regleras i internationell rätt. Uppsatsen rör internationell rätt och således kommer uteslutande folkrättsliga källor behandlas vilket påverkar metodens tillämpning. Detta eftersom internationella rättskällor saknar samma hierarki mellan varandra som nationell rätt.[10]

Internationella källor kommer användas i enlighet med vad som stadgas i art. 38(1) Stadgan för den Internationella domstolen[11] där det framgår att de utgörs av konventioner, internationell sedvana, allmänna principer och rättsavgöranden. Vad gäller dess inbördes ordning finns ingen sådan med undantag

[9] Kleineman, s. 21.
[10] Henriksen, s. 33-34.
[11] Hädanefter ICJ-stadgan.

för rättsavgöranden som är underordnad de ovanstående.[12] Dessa primära källor används i uppsatsen till följd av dess höga auktoritet och tillförlitlighet.[13] Fokus kommer främst ligga på FN-stadgan och internationell sedvanerätt samt ICJ:s avgörande för att förtydliga dess innehåll.

Det saknas klargörande statspraxis gällande rätten till självförsvar vid cyberattacker vilket ökar doktrinens relevans vid förklaring av gällande rätt. Doktrin behandlas dock med viss försiktighet då det inte utgör en primärkälla. Följaktligen har i den utsträckning möjligt officiella källor samt referensgranskade artiklar använts då de anses vara mer auktoritära samt tillförlitliga.[14]

Tallinn Manualerna används trots att det är en sekundärkälla i uppsatsen för att förstå gällande rätt på cyberområdet. Den är utarbetad av experter från hela världen och har således fått stor auktoritet inom området.[15] Vidare bör poängteras att en stor del av befintlig doktrin på området härstammar från västerländska universitet och författare vilket möjligen bidrar till viss brist på perspektiv.

1.5 Forskningsläge

I takt med att hotet mot cyberoperationer mellan stater ökat, har mer forskning på området tillkommit. Stora delar av den rättsliga forskningen rör gränsdragningen för när en cyberoperation anses utgöra ett väpnat angrepp i den mening som avses i art. 51 FN-stadgan och framstående författare är Roscini,[16] Schmitt[17] och Delerue[18]. Det råder delade meningar om var denna gräns går och ämnet diskuteras ofta i den internationella debatten. Vad gäller tillämpningen av principen om nödvändighet vid staters utövande av legitimt självförsvar

[12] Se art. 38, *Stadgan för den Internationella domstolen*.
[13] Henriksen, s. 21–22.
[14] Sandgren, s. 34-36.
[15] Schmitt (2017), s. 2.
[16] Roscini (2014).
[17] Schmitt (2013) (2017).
[18] Delerue (2020).

finns mycket material gällande kinetiska operationer, men inte lika mycket vad gäller cyberoperationer.

1.6 Disposition

Nästkommande kapitel redogör relevanta begrepp för en vidare förståelse av hur cyberrymden kan användas som en plattform för krigföring. Uppsatsens tredje kapitel inleds med en kort översikt av det allmänna våldsförbudet innan en mer djupgående beskrivning av rätten till självförsvar följer. Därefter kommer även principen om nödvändighet förklaras. Kapitel fyra tar upp vissa allvarliga cyberoperationer och redogör för händelseförloppet samt hur stater valt att bemöta angreppet. Efter huvudtexten följer ett femte och avslutande kapitel innehållande en analys. Denna kommer behandla materialet utifrån ett kritiskt förhållningssätt för att dels avgöra när en cyberoperation anses utgöra ett väpnat angrepp som aktualiserar självförsvarsrätten, dels hur principen om nödvändighet begränsar utövandet av denna rätt till självförsvar i en cyberkontext.

2 Cyber i en krigskontext

För att förstå hur cyberelementet spelar in i staters krigföring krävs förståelse för ett antal begrepp som saknar juridisk definition.[19] Av denna anledning kommer dessa redogöras för nedan.

2.1 Cyberrymden (cyberspace)

Under de senaste decennierna har cyberrymden integrerats som en självklar del i den mänskliga sfären.[20] Det saknas enhetlig definition av begreppet men gemensamt för de olika definitionerna är att den består av två delar. Cyberrymden består av den fysiska komponenten på vilken ett nätverk opererar samt det icke fysiska nätverket.[21] I Tallinn Manualen 2.0 definieras begreppet som ”den miljö som bildas av fysiska och icke-fysiska komponenter för att lagra, modifiera och utbyta data med hjälp av datornätverk”.[22] Det är denna definition som uppsatsen kommer utgå från vid användning av begreppet.

2.2 Cyberattacker och cyberoperationer

Begreppet cyberoperation saknar en allmän definition men är begränsad till handlingar som äger rum i cyberrymden.[23] Detta framgår även genom Tallinn Manualen 2.0 som definierar det som ”användning av cyberkapacitet för att uppnå mål inom eller genom cyberrymden”.[24] Cyberoperationer kan vara defensiva och offensiva. Offensiva cyberoperationer delas i sin tur in i cyberattacker och cyberexploatering.[25]

Begreppet cyberattacker används återkommande för att beskriva fientliga cyberoperationer riktade mot cyberinfrastruktur, användare av digitala enheter samt serviceenheter.[26] Det definieras i Tallinn Manualen 2.0 som ”en cyberoperation som, vare sig den är offensiv eller defensiv, förväntas orsaka skada

[19] Roscini, s. 11.
[20] Ericson, s. 36.
[21] Delerue s. 29.
[22] Schmitt (2017) s. 564.
[23] Delerue, s. 35.
[24] Schmitt (2017) s. 264.
[25] Joint Chiefs of Staff, s. II-3.
[26] Woltag s. 25.

eller dödsfall på personer eller skada eller förstörelse av objekt". Fokus ligger således på operationens konsekvenser vid bedömningen av om det utgör en cyberattack.[27] Det ska vara fråga om våldsanvändning mot ett specifikt mål vilket utesluter psykologiska cyberoperationer från begreppet. Våldsbegreppet begränsas dock inte till kinetiska, det vill säga fysiska, operationer utan kan inkludera även cyberhandlingar.[28] En cyberattack kan utgöra ett väpnat angrepp i den mening som avses i art. 51 FN-stadgan, men inte nödvändigtvis. Bara för att en handling benämns som en cyberattack är det inte lika med att det utgör ett väpnat angrepp även om det ofta är i denna kontext som begreppet används.[29]

Till följd av begreppens olika omfång kommer de användas i olika sammanhang i uppsatsen. Cyberoperationer kommer användas för att beskriva generell handling i cyberrymden medan cyberattacker kommer användas i kontext där rätt till självförsvar behandlas.

2.3 Cybersäkerhet och cyberförsvar

Cybersäkerhetsåtgärder utgör defensiva cyberoperationer i syfte att förebygga och skydda mot hot i cyberrymden samt minska sårbarheter som kan utnyttjas av en fientlig aktör. Säkerhetsåtgärder av detta slag kan vara exempelvis starka lösenord, krypterad lagrade data och begränsning av åtkomst till vissa webbplatser.[30]

Cyberförsvar används för att begränsa specifika hot som brutit eller hotar att bryta cybersäkerheten. I cyberförsvaret inkluderas även åtgärder i syfte att upptäcka, karakterisera, motverka och mildra hot, skadlig programvara eller användares obehöriga aktiviteter.[31]

[27] Schmitt (2017) s. 415.
[28] Schmitt (2017) s. 415; Roscini, s. 179.
[29] Roscini s. 17.
[30] Joint Chiefs of Staff, s. 11-5.
[31] Joint Chiefs of Staff, s. 11-6.

3 Rätten till självförsvar, *jus ad bellum,* i internationell rätt

Bland folkrättens primärkällor saknas uttrycklig reglering av cyberoperationer och cyberrymden.[32] FN:s generalförsamling har däremot bekräftat att internationell rätt, FN-stadgan samt internationella principer gäller även handlingar i cyberrymden.[33]

För att avgöra när en stat ges rätt till att utöva självförsvar mot en cyberattack måste klargöras under vilka förutsättningar en cyberattack kan kvalificeras som ett väpnat angrepp för att aktualisera självförsvarsrätten.[34] För att en cyberattack ska kvalificeras som ett väpnat angrepp krävs att det utgör otillåtet bruk av våld, varför det allmänna våldsförbudet kort kommer redogöras för nedan innan specifik reglering av självförsvarsrätten kommer utredas.

3.1 Det allmänna våldsförbudet

I internationell rätt råder ett allmänt våldsförbud vilket stadgas i art. 2(4) FN-stadgan:

> Alla medlemmar skola i sina internationella förbindelser avhålla sig från hot eller bruk av våld, vare sig riktat mot någon annan stats territoriella integritet eller politiska oberoende [...][35]

Det allmänna våldsförbudet återfinns även i internationell sedvanerätt.[36] Däremot saknas definition av vad som faktiskt utgör ”bruk av våld”. Ett av FN:s främsta syften är att skona kommande generationer från krig samt upprätthålla internationell fred och säkerhet.[37] Vid antagandet av FN-stadgan togs ett medvetet beslut att exkludera ekonomiska och politiska tvångsmedel från våldsförbudet.[38] Även om det till viss del råder delade meningar i frågan kan

[32] Roscini, s. 19–20.
[33] UNGA A/RES/73/27; UNGA A/RES/73/266.
[34] Roscini, s. 44.
[35] Se art. 2(4) FN-stadgan.
[36] Henderson, s. 24.
[37] Se inledande punkter till FN-stadgan.
[38] Roscini s. 46.

det konstateras att den rådande uppfattningen är att det allmänna våldsförbudet förbjuder just väpnat våld.[39]

Generellt ses väpnat våld som bruk av någon form av vapen, men det saknas precisering av vilken typ av vapen det är fråga om.[40] Cybermedel skiljer sig från konventionella vapen och utmanar således det traditionella ramverket.[41] ICJ fastslår dock i *Nuclear Weapons Advisory Opinion* att våldsförbudet gäller vilken typ av våld som helst oberoende av vilka vapen som används.[42]

Vid bedömning av huruvida en cyberhandling utgör olagligt bruk av våld eller inte kan utgås från olika metoder, en målbaserad, instrumentbaserad eller konsekvensbaserad metod, varav den konsekvensbaserade metoden är vanligast.[43] Denna fokuserar på konsekvenserna av cyberoperationen medan de föregående snarare fokuserar på målet för operationen eller vilka medel som används. Vissa författare argumenterar dock för en hopslagning av metoderna då dem menar att de inte går att bortse från målet eller medlen vid bedömning av konsekvenserna.[44] Det görs skillnad mellan cyberoperationer som ger effekter i den verkliga världen och de som endast ger effekter i cyberrymden. Den allmänna opinionen är överens om att de cyberoperationer som ger skador i den fysiska världen kan kvalificeras som olaga våldsanvändning.[45]

3.2 Rätten till självförsvar

FN-stadgan fastslår ett system av kollektiva säkerhetsförbud mot staters bruk av våld men nämner även två undantag till det allmänna våldsförbudet varav ett utgörs av rätten till självförsvar. I art. 51 stadgas följande:

[39] Henderson, s. 53-54.
[40] Henderson, s. 55.
[41] Ericson, s. 212.
[42] Legality of the Threat or Use of Nuclear Weapons, para 39.
[43] Delerue, s. 287.
[44] Delerue, s. 287-289.
[45] Henderson, s. 59.

> Ingen bestämmelse i denna stadga inskränker den naturliga rätten till individuellt eller kollektivt självförsvar i händelse av ett väpnat angrepp mot någon medlem av Förenta nationerna [...][46]

Artikeln anses utgöra en kodifikation av gällande rätt enligt internationell sedvanerätt. Rätten till självförsvar som internationell sedvanerättslig princip fanns enligt många jurister redan innan stadgan och är oberoende av dess tillkomst. Utgångspunkten stödjs av ICJ:s resonemang i *Nicaragua* fallet där domstolen poängterar att rättskällorna existerar parallellt utan inbördes rangordning.[47]

3.2.1 Skillnaden mellan ”bruk av våld” och väpnat angrepp”

Bruk av våld i den mening som avses i art. 2(4) FN-stadgan samt väpnat angrepp som det avses i art. 51 är skilda begrepp med skilda syften. Bruk av våld används för att avgöra huruvida en stat brutit mot det allmänna våldsförbudet medan väpnat angrepp används för att avgöra huruvida en stat har rätt att själv bruka våld i självförsvar utan att bryta mot det allmänna våldsförbudet.[48] För att ett angrepp ska kunna kvalificeras som väpnat angrepp måste det utgöra bruk av våld.[49] Däremot utgör inte alla typer av otillåten våldsanvändning ett väpnat angrepp. Klyftan mellan begreppen syftar till att hindra mindre våldsanvändning mellan stater från att eskalera till fullt krig.[50] Detta innebär dock inte att en stat som är utsatt för ett angrepp som inte når upp till tröskeln för att anses vara ett väpnat angrepp inte får vidta några åtgärder alls då en sådan operation fortfarande kan strida mot suveränitetsprincipen eller principen om non-intervention. Icke-våldsamma åtgärder som exempelvis kontraåtgärder kan då i vissa fall vidtas men den utsatte staten får ej bruka våld.[51]

3.2.2 Cyberattacker som väpnat angrepp

[46] FN-stadgan art. 51.
[47] Nicaragua, para. 176 och 179.
[48] Schmitt (2017), s. 337.
[49] Roscini, s.71.
[50] Woltag, s. 177.
[51] Melzer, s. 12.

Art. 51 FN-stadgan har gett upphov till stor debatt i den juridiska doktrinen då stadgan saknar ytterligare förklaring av vad som utgör ett *väpnat angrepp*. Huruvida det finns en minimigräns för när bruk av våld kvalificeras som väpnat angrepp är således omdiskuterad.[52] Oklarheten återfinns hos ICJ då domstolen inte varit konsekvent vid bedömningen av denna tröskel. I *Oil-Platform* målet diskuterade domstolen möjligheten att ett enda militärfartyg på en annan stats territorium kan räcka för att aktualisera den utsatte statens rätt till självförsvar.[53] Sett till detta fall kan tröskeln anses låg eller till och med obefintlig.[54] ICJ slog dock fast i Nicaragua fallet att det var nödvändigt att skilja på de mest grava bruken av våld från mindre grava, varav endast de grövsta utgör ett väpnat angrepp. Denna bedömning ska enligt ICJ ske utifrån hur gravt bruk av våld det rör sig om och det ska prövas genom att se till operationens *skala* och *effekt*.[55]

Vad kraven på skala och effekt mer konkret innebär specificeras inte av ICJ. Flera författare har således försökt nå klarhet i begreppen, varav en av dessa är Constantinou. Han definierar ett väpnat angrepp som:

> En handling eller början av en serie handlingar vilka har betydande omfattning och intensitet (skala) vilket ger konsekvenser (effekt) i form av betydande förstörelse av viktiga funktioner hos den utsatte staten såsom dess befolkning, ekonomisk och säkerhetsmässig infrastruktur, statliga befogenhet såsom dess politiska självständighet och ekonomiska resurser som leder till betydande försämring av dess ekonomi.[56]

Constantinus definition inkluderar även effekter på industri och ekonomi för offerstaten. Med utgångspunkt i denna definition måste en cyberattack inte nödvändigtvis orsaka fysisk skada utan det kan vara nog att den ger tillräckliga effekter på exempelvis staters ekonomi eller säkerhet för att kvalificeras som ett väpnat angrepp.[57]

[52] Henderson, s. 216.
[53] Oil Platforms, para 72.
[54] Henderson, s. 220.
[55] Nicaragua, para 19, 195.
[56] Roscini s. 73.
[57] Roscini, s. 74.

Även Dinstein har försökt förtydliga begreppen. Han presenterar exempel på cyberattacker som är tillräckligt allvarliga för att anses utgöra ett väpnat angrepp. Sådana exempel kan vara bland annat dödliga flygplanskrascher till följd av att felaktig information genom en cyberattack matats in i flygplansdatorer, eller strömavbrott med avsevärda skadliga verkningar som avstängning av datorer som styr vattenverk vilket genererar stora översvämningar. Till skillnad från Constantinous definition måste det enligt Dinstein leda till fysiska skador.[58]

Dinsteins uppfattning delas delvis av experterna som författat Tallinn Manualen 2.0. De är eniga kring att en cyberattack som allvarligt skadar eller dödar någon alternativt orsakar betydande skada på eller förstörelse av egendom uppnår kraven på skala och effekt. Vad gäller de cyberattacker som riktas mot exempelvis aktiemarknaden eller kritisk infrastruktur och endast genererar ekonomiska skador är gruppen splittrad. Vissa menar att en sådan attack skulle kunna kvalificeras som ett väpnat angrepp förutsatt att dess konsekvenser är allvarliga, varav andra var av motsatt åsikt. Exakt vilka konsekvenser som ska bedömas är således inte klart. Expertgruppen menar dock att samtliga rimligen förutsebara konsekvenser av en operation ska beaktas.[59] En majoritet av författarna på området är åtminstone överens om att en cyberattack som orsakar förstörelse och dödsfall i nivå med en konventionell attack utgör ett väpnat angrepp och aktualiserar således rätten till självförsvar.[60]

Skala och effekt av ett angrepp ska bedömas tillsammans. En omfattande cyberattack som endast ger störande konsekvenser kan ha en omfattande skala, men inte få tillräckligt stor effekt. Ett angrepp måste alltså vara både storskaligt och ge omfattande konsekvenser för att kvalificeras som ett väpnat angrepp.[61]

[58] Roscini, s.73-74.
[59] Schmitt (2017) s. 341-343.
[60] Henderson, s. 221.
[61] Roscini s. 73.

ICJ:s resonemang i Nicaragua fallet accepterades dock inte helt av det internationella samfundet och bland annat USA satte sig emot att en grovhetströskel med krav på skala och effekt överhuvudtaget skulle existera. De menade i stället att rätten till självförsvar gäller mot allt olagligt bruk av våld.[62] Även om detta utgör endast synen från en stat kan det anses återspegla den bredare ståndpunkten bland stater, som när de rättfärdigar agerande i självförsvar sällan skiljer mellan bruk av våld och väpnat angrepp utan snarare fokuserar på nödvändigheten i sitt svar på handlingen.[63]

Frågan uppstår ofta huruvida flera mindre grava cyberattacker mot en stat kan aktualisera självförsvarsrätten. Vissa argumenterar för att det i de fall det sker flera angrepp som var för sig inte uppnår tröskeln för ett väpnat angrepp tillsammans skulle kunna anses som ett väpnat angrepp. ICJ har dessutom anspelat på förekomsten av en sådan möjlighet då de i Nicaragua fallet diskuterar huruvida ett intrång kan behandlas enskilt eller kollektivt för att utgöra ett väpnat angrepp.[64]

3.3 Principen om nödvändighet

Det har i praxis fastställts ett tvåstegs test för bedömningen huruvida våldsanvändning i självförsvar är lagligt eller inte. Först måste konstateras att en stat varit utsatt för ett väpnat angrepp och sedan huruvida utövandet av våld i självförsvar faktiskt är nödvändigt.[65] Principen om nödvändighet uttalades första gången i *The Caroline Case* där korrespondensen mellan Storbritannien och USA:s utrikesministrar fått stor betydelse för rättsutvecklingen.[66] USA:s utrikesminister uttryckte där vad som kommit att kallas the Webster Formula. Det konstateras där att för att rätt till självförsvar ska föreligga måste visas på nödvändighet, omedelbarhet och det faktum att det saknas tid för ytterligare överväganden.[67] Principen har inte kodifierats i FN-stadgan men den har än-

[62] Roscini, s. 74.
[63] Henderson, s. 223.
[64] Nicaragua, para. 231.
[65] Nicaragua para 194; Oil platform, para 51.
[66] Meltzer, s. 17.
[67] Dinstein s. 231; Meltzer s. 17.

dock bekräftats av ICJ och kan av denna anledning betraktas som internationell sedvanerätt.[68] Värt att notera är att principen om nödvändighet i en jus ad bellum kontext skiljer sig från nödvändighet i jus in bello[69] samt den nödvändighet enligt vilken internationellt felaktiga handlingar kan rättfärdigas.[70]

För att våldsanvändning i självförsvar ska anses nödvändig krävs att det inte finns några alternativa, tillgängliga och rimliga alternativ för att avvärja, förhindra eller stoppa ett väpnat angrepp. Legitim våldsanvändning utgör således ett sista alternativ i de fallen icke-våldsamma alternativ saknas.[71] Av denna anledning har den utsatte staten en skyldighet att först konstatera att situationen inte kan åtgärdas genom mindre medel innan den vidtar våldsamma åtgärder i självförsvar. Finns exempelvis en möjlighet att genom passivt cyberförsvar eller motåtgärder som inte når tröskeln för otillåten våldsanvändning förhindra hackare från att nå de attackerade nätverken och datorerna, är dessa medel lämpliga att tillgå och ett våldsamt svar på angreppet kan i dessa fall inte anses nödvändigt.[72]

Principen definierar således när en stat kan utöva lagligt självförsvar sett till den objektiva nödvändigheten att avvärja ett väpnat angrepp. Åtgärderna måste för uppfyllandet av principens syfte även vara tidsmässigt nödvändiga. En självförsvarsåtgärd får alltså inte lagligen vidtas innan det råder faktisk nödvändighet att avvärja ett väpnat angrepp och inte heller efter det att självförsvar inte längre är nödvändigt för uppfyllandet av detta syfte.[73] Just kravet på tidsmässig nödvändighet har utmanats av modern teknologi. Cyberattacker är unika på så sätt att de kan ligga latent i flera månader[74] eller passera på endast några minuter vilket försvårar bedömningen av när en cyberattack börjar och slutar. Händelseförloppet är avgörande för bedömningen av huruvida det föreligger en verklig nödsituation och ett konkret behov av våldsamma

[68] Oil Platforms, para 43, 73-74; Nicaragua para 176, 194.
[69] Schmitt (2017) s. 348.
[70] Henderson, s. 229.
[71] O´Meara, s. 30-31.
[72] Roscini, s. 90.
[73] Meltzer, s. 17.
[74] Se nedan om Stuxnet.

åtgärder från statens sida.[75] Det har diskuterats huruvida omedelbarheten är en del av nödvändighetsprincipen eller om det utgör ett separat rekvisit. Allmän konsensus saknas och således kommer omedelbarheten vidare behandlas som en del av nödvändighetsrekvisitet. Detta med anledning av att tidsaspekten är ofrånkomlig då en stat överväger icke-våldsamma alternativ i form av informationsinsamling och diplomatiska förhandlingar i syfte att i övrigt uppfylla nödvändigheten.[76]

Rätten till självförsvar syftar till att förhindra och begränsa ytterligare uppkomst av skada, snarare än att ge tillbaka mot redan gjord skada. Följaktligen menar vissa författare att självförsvarsåtgärder inte kan vidtas efter det att ett väpnat angrepp är avslutat.[77] Detta är dock omdiskuterat och bland annat Dinstein menar att agerande i självförsvar inte nödvändigtvis måste ske medan det väpnade angreppet pågår.[78] Å andra sidan har ICJ varit återkommande kritisk till de fall där stater agerat i efterhand då domstolen menar att det i dessa fall inte anses nödvändigt att agera i självförsvar i syfte att skydda eller värja sig mot attacken. Dock har den tidsmässiga nödvändigheten till viss del bedömts annorlunda vid exempelvis terroristattacker.[79] Detta med hänsyn till USA:s agerande i självförsvar i syfte att förhindra och förebygga framtida attacker som utfördes nästan fyra veckor efter 9/11-attacken.[80] Agerandet stöttades av flertalet stater såväl som organisationer som EU och NATO.[81]

Nödvändigheten bedöms på samma sätt vid cyberattacker som vid traditionella attacker med konventionella vapen[82] och bedömningen görs ur offerstatens perspektiv.[83] Då en stat utsätts för en direkt fysiskt väpnad attack är denna bedömning oftast relativt enkel. Det skulle vara inkonsekvent att utgå från att den utsatte staten har en rättslig skyldighet att vidta fredliga åtgärder eller förhandlingar innan den vidtar självförsvarsåtgärder för att skydda sig. Det

[75] O`Meara s. 55.
[76] Dinstein, s. 233-234.
[77] Meltzer, s. 17.
[78] Dinstein, s. 233.
[79] Henderson, s. 233.
[80] UN Doc s/2001/946.
[81] NATO, *Nato and Afghanistan*; Hassan, s. 2.
[82] Dinstein, s. 231.
[83] Schmitt (2017) s. 349.

finns i dessa fall i princip alltid en nödvändighet till självförsvar direkt.[84] Sett till cyberattacker är detta inte lika självklart. Vid bedömningen av dessa fall bör fokus snarare ligga på huruvida det finns lämpliga alternativa handlingssätt som inte stiger till nivån av otillåten våldsanvändning. Om offensiva cyberoperationer i form av exempelvis brandväggar räcker för att begränsa och motverka en cyberattack så är inte våldsamma åtgärder, varken cyberoperationer eller kinetiska, tillåtna.[85]

[84] Henderson, s. 229-230.
[85] Schmitt (2017) s. 349.

4 Uppmärksammade cyberattacker

Det saknas i dagsläget statspraxis där en stat officiellt kvalificerat en cyberattack som ett väpnat angrepp som aktualiserar självförsvarsrätten enligt art. 51 FN-stadgan. Däremot står det klart att en cyberattack i praktiken hade kunnat uppnå kraven för att kvalificeras som ett väpnat angrepp.[86] Nedan kommer redogöras för några av de mest uppmärksammade cyberattackerna.

4.1 Stuxnet

I september 2010 upptäcktes en skadlig mjukvara vid namn ”Stuxnet” på en iransk dator. Strax därefter konstaterades att Stuxnet-masken var utformad för att sabotera centrifuger på Natanz fabriken i Iran i syfte att fördröja eller avbryta Irans kärnkraftsprogram.[87] Misstankar riktades mot Israel och USA men dessa har aldrig bekräftats.[88]

Analytiker misstänker att Stuxnet startades genom att den utsatta datorn anslutits direkt till den skadliga programvaran via en extern anslutande apparat eller ett USB. Därefter spreds viruset genom självreplikering till andra datorer, allt utan användarens vetskap och den låg sedan latent i systemen månader innan attacken.[89] Stuxnet-masken begränsades dock genom inbyggda säkerhetsåtgärder som programmerats för att förhindra okontrollerad spridning av den skadliga mjukvaran. Den var vidare programmerad att attackera specifika mål, i detta fall frekvensomvandlare som används i centrifuger för att reglera ström eller spänning. Dessa frekvensomvandlare användes i stor utsträckning av Irans kärnkraftsprogram under tiden vilket lett analytiker till slutsatsen att det troligtvis var just detta som utgjorde attackens specifika mål. Följaktligen havererade centrifugerna på Natanz fabriken utan att personalen

[86] Woltag, s. 178.
[87] Baezner (2017) s. 9.
[88] Woltag, s. 49-50.
[89] Woltag s. 47-51.

förstod varför[90] eftersom masken konstruerats för att kunna gömma sig i maskinkod. Den spred sig, och 2010 hade den smittat 60 000 datorer över hela världen.[91] Stuxnet bestod dock av en självförstörande mekanism vilket möjliggjorde dess raderande år 2012.[92]

Stuxnet-masken förstörde ca 1000 centrifuger på Natanz-fabriken i Iran, och fler togs ur bruk som en säkerhetsåtgärd. Dock ledde Stuxnet inte till att kärnkraftsprogrammets avslutandes utan operationen kan som mest anses ha saktat ned det och det tog ungefär ett år för programmets att återhämta sig.[93] Attacken gav således fysiska samt ekonomiska konsekvenser då de skadade centrifugerna behövde ersättas. Attacken gav dessutom sociala och politiska konsekvenser för Iran då de ansågs försvagat till följd av dess bristande kontroll över sin digitala infrastruktur.[94]

Många omständigheter tydde på statlig inblandning, primärt det faktum att Stuxnet var så pass sofistikerad och noggrant utformad samt resurserna de krävts för att utveckla masken. Stuxnet anses utgöra den första välplanerade, organiserade cyberattacken mot ett betydande industriellt mål.[95]

Stuxnet utgör det kanske tydligaste exemplet på när en cyberoperation orsakar fysisk skada på en nivå som kan uppnå tröskeln för bruk av våld men möjligen även väpnat angrepp. Den expertgrupp som författat Tallinn Manualen är överens om att Stuxnet anses utgöra bruk av våld och vissa av dessa menar även att attacken även kan kvalificeras som ett väpnat angrepp.[96] Huruvida det utgör ett väpnat angrepp är dock omdiskuterat. Bland annat Roscini är tveksam till detta. Han menar att Stuxnet troligtvis inte uppfyller de krav som ställs på en operations skala och effekt för att anses utgöra ett väpnat angrepp. Iran kvalificerade själv attacken som kärnkraftsterrorism och uttalade således inte huruvida de ansåg det vara fråga om ett väpnat angrepp

[90] Ericson, s. 223-224.
[91] Richards, s. 37.
[92] Ericson, s. 223-224.
[93] Ericson, s. 226.
[94] Baezner (2017), s. 9.
[95] Woltag s. 47-51.
[96] Schmitt (2013), s. 47, 57-58.

eller inte. Det kan dock inte frånses att en sådan förklaring kan ha politisk snarare än strikt juridisk grund.[97]

4.2 Ukraina 2015/2016

I samband med Sovjetunionens fall blev Ukraina självständigt, men Ryssland har trots detta aldrig till fullo släppt tanken att området i stället bör tillhöra Ryssland. Relationen mellan länderna har varit spänd sedan Putin år 2000 valdes till president i Ryssland. Spänningarna ökade när Ukraina började närma sig EU vilket ledde till väpnad konflikt i samband med Rysslands annektering av Krim-halvön 2014.[98] Nedan beskrivna cyberattacker skedde således under en pågående väpnad konflikt men kommer i uppsatsen trots detta analyseras i en jus ad bellum kontext till följd av dess omfattande konsekvenser.

I december 2015 utsattes tre av de huvudsakliga energiföretagen i Ukraina för en rad cyberattacker. Följaktligen stängdes nära sextio av företagens elektriska stationer ner vilket gjorde att 230 000 människor förlorade all el i upp till sex timmar. Endast dagar efter angreppet pekar ukrainsk säkerhetstjänst ut Ryssland som ansvarig. Programvaran tros, på samma vis som Stuxnet, ha legat latent i ungefär ett år innan angreppet.[99]

Attacken bestod av flera faser varav den första inleddes genom att angriparen bifogade ett skadligt dokument via e-post. Dokumentet innehöll i sin tur skadligprogramvara som vid öppning infekterade systemet samt installerade en bakdörr. Detta för att förövarna skulle ha möjlighet att kartlägga nätverken samt kontrollera Windows domänkontroller. Detta följdes av flera offensiva cyberoperationer i syfte att inaktivera diverse komponenter i nätverken som styr de system som reglerar strömförsörjningen. Samtidigt angreps kundcentret av diverse cyberattacker för att på så vis eliminera kundernas möjlighet att kontakta centret och rapportera strömavbrottet. Slutligen raderades olika filer från operationsstationerna vilket gjorde dem obrukbara.[100]

[97] Roscini, s. 76.
[98] Baezner (2018) s. 7.
[99] Delerue, s. 76-77.
[100] Delerue, s. 76-77.

Knappt ett år senare angreps Ukrainas eldistributörer ännu en gång. Cyberattackerna resulterade i cirka en timmes strömavbrott i Kiev och gav således märkbart mindre konsekvenser än cyberattacken 2015. Trots detta anses mjukvaran som användes i attacken vara mer tekniskt sofistikerad och utvecklad än den tidigare använda mjukvaran. Analytiker menar således att ambitionen och avsikten med denna attack var betydligt större än vad resultatet genererade.[101]

Händelsen fick begränsade konsekvenser i form av fysisk skada men gav ekonomiska konsekvenser samt påverkade medborgarnas förtroende för den ukrainska staten negativt.[102]

[101] Dragos Inc, s. 1.
[102] Baezner (2018), s. 14-16.

5 Analys och slutsats

Uppsatsen hade till syfte att utreda under vilka förutsättningar en cyberattack utförd av en stat mot en annan, i en jus ad bellum kontext, anses utgöra ett väpnat angrepp i den mening som aktualiserar rätten till självförsvar. Uppsatsen syftade dessutom till att undersöka hur principen om nödvändighet begränsar utövandet av rätten till självförsvar i en cyberkontext. Just självförsvarsrätten vid cyberattacker har diskuterats återkommande i den juridiska doktrinen och frågans relevans ökar i takt med det ökade cyberhotet. Det är av denna anledning av vikt för stater och övriga aktörer att det råder klarhet kring när en stat i enlighet med internationell rätt ges rätt att bruka våld i självförsvar vid en cyberattack.

5.1 Självförsvarsrätten vid cyberangrepp

FN i stort syftar till upprätthållande av internationell fred och säkerhet varför FN-stadgan innehåller ett allmänt våldsförbud stadgat i art. 2(4). En stat får således som utgångspunkt inte bruka våld i strid mot förbudet, men självförsvarsrätten utgör ett undantag. Att en cyberattack kränker internationella principer såsom principen om non-intervention eller suveränitetsprincipen ger inte automatiskt den utsatte staten rätt att bruka våld i självförsvar utan attacken måste uppgå till ett väpnat angrepp i den mening som avses i art. 51 FN-stadgan.

En cyberattack måste ske i strid mot det allmänna våldsförbudet för att anses utgöra ett väpnat angrepp. Vid FN-stadgans tillkommande skedde en medveten uteslutning av politiska och ekonomiska tvångsmedel från våldsförbudet och det reglerar således endast väpnat våld. Att en cyberattack kan utgöra väpnat våld styrks av ICJ:s resonemang i Nuclear Weapons Advisory Opinion. Vid avgörande huruvida en handling strider mot det allmänna våldsförbudet kan diverse metoder användas, varav den konsekvensbaserade är vanligast. Detta är inte utan betydelse vid avgörandet av huruvida det utgör ett väpnat angrepp, då det råder allmän konsensus kring det faktum att cyberoperationer som orsakar skada i den fysiska världen kan kvalificeras som olaga våldsanvändning i strid med det allmänna våldsförbudet.

Utövandet av våld i självförsvar undantas från det allmänna våldsförbudet. Tröskeln för när en våldshandling anses utgöra ett väpnat angrepp är medvetet hög i syfte att hindra mindre konflikter från att eskalera till fullskaligt krig. Hur bedömningen görs är dock inte helt klart. De kanske tydligaste riktlinjerna ges av ICJ i Nicaragua fallet där det framgår att endast de grövsta angreppen sett till dess skala och effekt anses utgöra ett väpnat angrepp. Kriterierna saknar dock mer specifik definition och vissa stater förnekar dess existens överhuvudtaget. Klart står dock att kriterierna ska bedömas tillsammans. En cyberattack måste därför ha både omfattande skala och ge allvarliga konsekvenser för att kvalificeras som ett väpnat angrepp.

En majoritet av författarna på området är överens om att Stuxnet utgjorde otillåten våldsanvändning, huruvida operationen kvalificeras som ett väpnat angrepp är dock omdiskuterat. Enligt Constantinous definition av skala och effekt krävs betydande omfattning och intensitet samt förstörelse av betydande funktioner hos den utsatte staten. Stuxnet var avancerad och ytterst resurskrävande vilket tyder på statlig inblandning. Operationen var dessutom organiserad och välplanerad vilket gjorde det möjligt för masken att spridas på tiotusentals datorer runt i världen vilket tyder på storskalighet. Stuxnet orsakade förstörelse på 1000 centrifuger på kränkraftanläggningen i Natanz. Dessa tillhörde ett statligt projekt och det utgjorde förstörelse i en omfattning som tidigare endast kunnat orsakas av kinetiska medel. Sett till detta bör Stuxnet kunna kvalificeras som ett väpnat angrepp.

Om det i stället utgås från Dinsteins syn på kriterierna och hans exempel, så orsakar Stuxnet inte i närheten sådana konsekvenser som krävs för ett väpnat angrepp. Även författarna till Tallinn Manualen 2.0 poängterar att betydande fysisk förstörelse måste förekomma. Dessa 1000 centrifuger kan anses utgöra betydande förstörelse och således anses utgöra ett väpnat angrepp, även om det råder delade meningar kring denna slutsats.

Attacken i Ukraina 2015 genererade ingen fysisk förstörelse vilket skiljer den från Stuxnet. I stället gav den omfattande strömavbrott som påverkade hund-

ratusentals medborgare under flera timmar. Med utgångspunkt i Constantinous definition kan skalan anses omfattande. Detta då den bestod av flera steg, var välplanerad samt attackerade strategiska mål i specifik ordning för att uppnå ett visst resultat. Attacken gav inga fysiska konsekvenser men utgjorde ett omfattande intrång i Ukrainas infrastruktur. Att den skedde till följd av Ukrainas närmande till EU kan ses som en försvårande omständighet. Inte heller denna attack är dock jämförbar med Dinsteins exempel, även om den eventuellt haft potential att göra det. Författarna till Tallinn Manualen 2.0 menar att hänsyn ska tas till samtliga rimligen förutsebara konsekvenser av angreppet. Ett omfattande strömavbrott under den aktuella tidsåtgången kan få långtgående konsekvenser för ett samhälle förutsatt att strömmen slås ut på exempelvis ett sjukhus. Trots att det saknas dokumentation av ett sådant scenario i Ukraina hade endast möjligheten kunnat vara försvårande och således kvalificera angreppet som väpnat. Ett sådant resonemang anses dock långtgående och ej i linje med FN:s syfte. Kriterierna bör således tolkas restriktivt snarare än extensivt och attacken i Ukraina bör därför inte anses utgöra ett väpnat angrepp.

Inte heller cyberattacken mot Ukraina 2016 bör ses som ett väpnat angrepp, sett till dess skala och effekt. Däremot bör beaktas att denna attack skedde som en av många i en rad cyberattacker mot Ukraina vilket möjligen kan aktualisera självförsvarsrätten enligt vad ICJ:s flertalet gånger antytt. Det framgår dock att samtliga attacker ska bedömas var för sig vilket innebär att det inte anses som väpnat angrepp.

5.2 Nödvändighetsprincipens begränsningar i en cyberkontext

Efter att ha konstaterat att en stat är utsatt för ett väpnat angrepp måste en bedömning av nödvändigheten av våldsanvändning i självförsvar göras innan dess att den utsatte staten lagligen kan agera i självförsvar.

Principen begränsar våldsutövning i självförsvar till de fall då alternativa, tillgängliga och rimliga alternativ saknas för att avvärja, förhindra eller stoppa

ett väpnat angrepp. Av praxis framgår att stater sällan bedömer huruvida ett angrepp utgör ett väpnat angrepp eller inte, snarare ligger fokus på nödvändigheten av självförsvar. Detta resonemang innebär att det potentiellt kan ha funnits fall som rent juridiskt kunnat kvalificeras som väpnat angrepp men där stater valt att inte agera i självförsvar till följd av att det helt enkelt inte ansetts nödvändigt.

Principen om nödvändighet bedöms lika vid kinetiska operationer såväl som vid cyberattacker, trots att medlen i hög grad skiljer sig åt. När Ryssland invaderade Ukraina 2022 rådde ingen tvekan om att Ukrainas våldsanvändning i självförsvar var nödvändig. Lika självklart har det aldrig varit vid en cyberattack. Cyberelementet innebär att skadlig programvara kan ligga latent i systemen långt innan attacken och när attacken väl sker kan angreppet passera på bara några minuter. Detta försvårar bedömningen av när angreppet börjar och slutar. Även omfattningen av en cyberattack är svår att mäta, då det sällan står klart direkt. Således försvåras nödvändighetsbedömningen då det är svårt att avgöra huruvida självförsvar är nödvändigt sett till konsekvenserna men också till tidsaspekten. ICJ har återkommande kritiserat stater då de agerat i självförsvar när angreppet inte längre varit pågående. Värt att notera är dock att inget av fallen som ICJ prövat specifikt rör cyberattacker, men då bedömningen sker enligt samma principer kan samma resonemang ändock tillämpas.

I doktrin diskuteras huruvida omedelbarheten bör utgöra ett eget rekvisit. Tidsåtgången ses dock som en ofrånkomlig aspekt vid nödvändighetsbedömningen. Det måste saknas alternativa handlingssätt för att självförsvar ska vara nödvändigt. För att säkerställa detta måste eventuella alternativ övervägas och ibland prövas. Om alternativa handlingssätt utesluts måste återigen bedömas huruvida självförsvar är nödvändigt sett till tidsaspekten. Omedelbarheten kan inte helt skiljas från nödvändigheten och bör därför inte vara ett eget rekvisit. En längre svarstid har accepterats i vissa fall, bland annat vid USA:s svar på 9/11-attacken. Denna attack, sker likt cyberattacker genom medel som utmanar den traditionella synen på krig, och av denna anledning

kan argumenteras för att en längre svarstid bör accepteras även vid cyberattacker.

Iran svarade aldrig med våldsanvändning i självförsvar mot USA och Israel efter Stuxnet. Angreppet kvalificerades i stället officiellt som kränkraftsterrorism i stället för ett väpnat angrepp. Huruvida det berodde på nödvändighetsbedömningen snarare än bedömningen om huruvida det utgjorde ett väpnat angrepp eller inte står ej klart. Sett till nödvändighetsprincipen kan det troligtvis inte heller anses nödvändigt för Iran att agera i självförsvar. Detta med anledning av att angreppet inte var pågående och att sådant handlande av denna anledning troligtvis endast eskalerat våldsanvändningen i strid mot FN:s syfte.

Annat hade det kunnat vara vid cyberattackerna mot Ukraina 2015/2016 sett ur en jus ad bellum kontext. I detta fall förekom en rad cyberattacker vilket möjliggör en argumentation för att angreppet var pågående eller att hotet åtminstone var överhängande. Dock har Ukraina byggt upp ett starkt cyberförsvar, och detta verkar räcka långt. Offensiva cyberoperationer utgör mindre ingripande medel och omöjliggör agerande i självförsvar i de fall det anses räcka.

5.3 Kritisk granskning av ramverket

De skyddsvärda objekten enligt FN-stadgan utgörs av människor och fysisk egendom. Stadgan tillkom i en tid då cyberhot inte existerade. Idag är många av staters bärande samhällsfunktioner digitaliserade och det är således möjligt för en fientlig aktör att genom cybermedel orsaka skada som förr endast var möjlig med konventionella medel. Trots detta saknas specifik reglering av handlingar i cyberrymden och de styrs av samma ramverk som kinetiska attacker.

Den höga tröskeln för ett väpnat angrepp finns i syfte att hindra mindre våldsanvändning från att eskalera till fullt krig. Dock förekommer cyberattacker som genererar omfattande konsekvenser utan att för det kvalificeras som väpnat angrepp. Detta möjliggör en diskussion om huruvida det rådande

ramverket når dessa handlingar sett till att cyberattacker ofta faller under tröskeln för ett väpnat angrepp med samma argument som används vid konventionella attacker, det vill säga avsaknad av tillräcklig fysisk skada. Det verkar således finnas större handlingsutrymme för stater i cyberrymden än i den verkliga världen. Det kan dock argumenteras för att utsatta stater kan svara med lika medel som understiger tröskeln utan att riskera att få våld i självförsvar tillbaka. Däremot finns en risk att stater saknar likvärdig cyberkapacitet vilket möjligen kan bidra till snedvriden maktbalans på den internationella arenan.

Även om det går att argumentera för ett separat regelverk gällande handlingar i cyberrymden kan ej frånses de faktiska svårigheterna med en sådan reglering. Det är inte lätt att nå konsensus rörande frågor av denna karaktär, då det rör staters militär och försvar. Även om FN-stadgan på gott och ont har ett brett tillämpningsområde kan det således anses utgöra en stor utmaning att åstadkomma ett mer detaljerat instrument av samma betydelse.

5.4 Slutsats

I det internationella samfundet saknas allmän konsensus kring vilka krav som måste uppfyllas för att en cyberattack ska anses utgöra ett väpnat angrepp. Inte minst för att inte alla stater godtar ICJ:s krav på skala och effekt, men också med hänsyn till att begreppen saknar mer detaljerad definition. Dock kan konstateras att författarna är någorlunda överens om att tröskeln för ett väpnat angrepp är hög och att en cyberattack måste orsaka fysiska skador för att betraktas som ett väpnat angrepp.

Principen om nödvändighet bedöms lika vid cyberattacker som vid kinetiska operationer även fast cyberelementet innehåller parametrar som försvårar bedömningen. Tidsaspekten är en sådan, likväl som det faktum att konsekvenserna av en cyberattack är svåra att mäta. Det skulle dock vara att gå för långt att säga att nödvändighetsprincipen omöjliggör utövandet av självförsvar mot en cyberattack.

Slutligen kan konstateras att det saknas tydlighet kring gällande rätt på området. Cyberrymden saknar specifik reglering i internationell rätt och innehåller dessutom många begrepp utan entydig definition. I dagsläget saknas praxis där en stat kvalificerat en cyberattack som ett väpnat angrepp och således finns inte heller fall där en stat agerat i självförsvar mot en cyberattack. Sett till de senaste årens utveckling är detta dock endast en tidsfråga. Troligtvis kommer det komma en cyberattack som ger konsekvenser stora nog för att det internationella samfundet ska acceptera en stats agerande i självförsvar mot det, vilket troligtvis kommer rita om den juridiska kartan för krigföring, kanske till och med lika mycket som 9/11-attacken.

Källförteckning

Resolutioner

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.

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.

Rapporter m.m.

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

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

Dragos Inc. ’CRASHOVERRIDE: Threat to the Electric Grid Operations’, 2017.

Hassan, Oz. ’Afghanistan: Lessons learnt from 20 years of supporting democracy, development and security’. European Parliament, 2023.

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

Melzer, Nils. ’Cyberwarfare and International law’. UNIDIR Resources, 2011.

Rättsfall

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

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

Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, 6 november 2003, ICJ Reports 2003.

Litteratur

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

Dinstein, Yoram. *War, Aggression and Self-Defence*. Cambridge University Press, 2011.

Ericson, Marika. *On the Virtual Borderline: Cyber Operations and their Impact on the Paradigms for Peace and war.* Uppsala universitet, 2020.

Henderson, Christian. *The use of force and international law.* 1 uppl. Cambridge University Press, 2018.

Henriksen, Anders. *International law.* 4 uppl. Oxford University Press, 2023.

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

O'Meara, Chris. *Necessity and Proportionality and the Right of Self-Defence in International Law*. Oxford University Press, 2021.

Richards, Julian. *Cyber-war the anatomy of the global security threat.* Palgrave Macmillan, 2014. E-bok.

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

Sandgren, Claes. *Rättsvetenskap för uppsatsförfattare: ämne, material, metod och argumentation*. 3 uppl. Nordstedts Juridik, 2015.

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

Schmitt, Michael N. *Tallinn manual 2.0 on the international law applicable to cyber operations / Prerared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Exellense.* Cambridge University Press, 2017. E-bok.

Woltag, Johann-Christopf. *Cyber warfare – Military Cross-Border Computer Network Operations under International Law*. Intersentia, 2014.

Övrigt

Cerulus, Laurens. ’How Ukraine became a test bed for cyberweaponry’. Politico, 2019-02-14. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/ (Hämtad 2023-11-15).

Jägemar O, Rufus. ’Stuxnet – datasystemens atombomb’. SVT Nyheter, 2012-10-31. https://www.svt.se/nyheter/utrikes/stuxnet-datasystemens-atombomb (Hämtad: 2023-12-02).

Milanovic, Marko. ’When did the Armed Attack against Ukraine become ’Imminent’?’. EJIL:Talk!, 2022-04-20. https://www.ejiltalk.org/when-did-the-armed-attack-against-ukraine-become-imminent/ (Hämtad 2023-11-20).

NATO. ’NATO and Afghanistan’. North Atlantic Treaty Organization, 2022-08-31. https://www.nato.int/cps/en/natohq/topics_8189.htm (Hämtad 2023-12-02).

UN Doc s/2001/946. Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. (7 oktober 2001).