Var det såkalte cyberangrepet mot Estland i 2007 et væpnet angrep etter FN-paktens artikkel 51?

av Simon Kiil

Liten masteroppgave i rettsvitenskap
ved Universitetet i Tromsø
Det juridiske fakultet
Høsten 2012

1. Innledning

1.1 Problemstillingens aktualitet og status

Teknologiske fremskritt og samfunnets økende avhengighet av datanettverk har endret det internasjonale risikobildet. I den grad man kan forvente at datanettverk blir nerven i statenes infrastruktur, vil forstyrrelser eller angrep mot cyberdomenet kunne lamme et helt land. Trusselen er kompleks og dynamisk og kommer ikke lenger bare fra såkalte "hackere"[1] på jakt etter status. Innbrudd i datanettverk blir benyttet til spionasje og forstyrrelser, av stater mot stater, mot militære styrker og mot private selskaper.[2]

Flere land har, eller er i ferd med å utarbeide, nasjonale strategier for cybersikkerhet. Manglende rammer i internasjonal lov gjør arbeidet utfordrende.
Med problemstillingen "Var det såkalte cyberangrepet på Estland i 2007 et væpnet angrep etter FN-paktens artikkel 51?" vil jeg prøve om den eksisterende folkeretten er dynamisk nok til å tilpasses nye og tidligere utenkelige former for angrep. Målet er å finne ut om folkerettens regler forut for væpnet konflikt er anvendelige på cyberangrep.
Jeg vil ta for meg hvordan et cyberangrep kan plasseres i en konfliktskala fra intervensjon, via bruk av makt, til væpnet angrep, hvor fokuset vil ligge på skjæringspunktene mellom disse konflikttrinnene.
Avhandlingen berører spesielt utfordringer knyttet anvendelsen av de folkerettslige ansvarsreglene, samt konsekvensvurdering av cyberangrep. Videre er avhandlingen også i stor grad en test på om de eksisterende teorier som vil kunne danne grunnlaget for sedvanerett vedrørende cyberoperasjoner er holdbare.

1.2 Metode og kildebruk

Avhandlingens tema ligger innenfor folkerettens område, og metoden avviker fra norsk retts metode.

---

[1] For definisjon se http://www.norsis.no/leksikon/h/Hacker.html (pr.12.12.12)
[2] Nasjonal Sikkerhetsmyndighet, *Nasjonal strategi for cybersikkerhet,* versjon 1.0
[2] Nasjonal Sikkerhetsmyndighet, *Nasjonal strategi for cybersikkerhet,* versjon 1.0 desember 2009 s.2

Statute of the International Court of Justice[3] artikkel 38(1) fremstiller kildene som er bindene for The International Court of Justice[4] sin rettsanvendelse. I henhold til bestemmelsen er internasjonale konvensjoner, internasjonal sedvane og grunnleggende rettsgrunnsetninger de primære kildene. Rettspraksis og juridisk teori regnes som subsidiære kilder.
Folkeretten baserer seg imidlertid på et horisontalt system, noe som tilsier at for eksempel sedvanerett kan bli satt til side mellom parter i en konvensjon, som igjen kan endres ved partenes etterfølgende praksis. [5]

1.2.1 Konvensjoner

Konvensjoner, pakt eller traktater er avtaler mellom folkerettssubjekter, først og fremst stater. De Forente Nasjoners Pakt er en slik avtale, og er da etter statuttene for ICJ artikkel 38(1a) som en primær rettskilde å regne.
Wien-konvensjonen om traktatretten [6] er den sentrale kilden for traktatstolkning, og gjelder også som folkerettslig sedvanerett for de land som ikke er tilsluttet konvensjonen.[7] Av artikkel 31(1) fremgår at ordlyden i de enkelte artikler og deres opprinnelige mening er utgangspunktet i tolkningen av traktater. Av artikkel 31(2) fremgår at ordlyden i den enkelte artikkel må tolkes i lys av traktaten som enhet.
FN-pakten har en helt sentral plass blant folkerettslige konvensjoner, og inneholder nedskrevne prinsipper som må regnes som generelle folkerettslige prinsipper i dag. FN-pakten er generell i sin karakter, derfor vil enkelte andre konkrete traktater kunne oppnå status som *lex spesialis* i forhold til FN-pakten. Det fremgår av FN-paktens artikkel 103 at medlemsstatenes forpliktelser etter Pakten går foran deres plikter etter andre internasjonale avtaler.[8] FN-pakten er sentral for denne avhandlingen.

1.2.2 Resolusjoner fra FNs Sikkerhetsråd og Generalforsamling

Resolusjoner blir som regel vedtatt i forbindelse med hendelser eller som et generelt uttrykk for staters forpliktelser og ansvar vedrørende statenes internasjonale

[3] Heretter statuttene for ICJ
[4] Heretter ICJ
[5] Morten Ruud og Geir Ulfstein, *Innføring i folkerett,* 3. Utg Oslo 2006 s.71
[6] Vienna Convention on the Law of Treaties May 23 1969
[7] Ruud og Ulfstein, s.74
[8] *Ibid* s.72

samhandling. Sikkerhetsrådets resolusjoner er bindene for FNs medlemmer. Generalforsamlingens resolusjoner er gitt som anbefalinger,[9] og er ikke bindene. Generalforsamlingen kan i resolusjon anbefale at stater følger annet lovarbeid, fra for eksempel The International Law Comission[10]. Slik gjør de blant annet vedrørende ILC Draft Articles on State Responsibility i flere resolusjoner.[11]
Denne avhandlingen vektlegger i vesentlig grad resolusjoner fra Generalforsamlingen, da de ofte er tydelige og mer gjennomarbeidet enn til tider hastige resolusjoner fra Sikkerhetsrådet, og ofte gir uttrykk for hva som er sedvanerett.

1.2.3 Internasjonal sedvanerett

Internasjonal folkerettslig sedvane må være "*extensive and vitually uniform*", og "*have occured in such way as to show a general recognition that a rule of law or legal obligation is involved*".[12] Sedvanen kan bli bindende for alle stater uavhengig om de har akseptert den.[13] Internasjonal sedvanerett vil bli vektlagt og utforsket i fremstillingen for å prøve om den er overførbar til en cyberkontekst.

1.2.4 Internasjonal rettspraksis

Statuttene for ICJ anerkjenner rettspraksis kun som en sekundær rettskilde. Dommene er kun bindende mellom partene, jfr. statuttenes artikkel 59. Dommene er imidlertid avgjørende for tolkninger av begrep innen FN-pakten. Fra ICJ praksis ser man at Domstolen hyppig viser til og legger stor vekt på sin egen praksis.[14]
ICJs vurderinger og tolkninger er tillagt betydelig vekt i denne avhandlingen.

---

[9] FN-pakten artikkel 10
[10] Heretter ILC
[11] James Crawford, on *Articles on Responsibility for Internationally Wrongful Acts*, Audiovisual Library of International Law
http://untreaty.un.org/cod/avl/ha/rsiwa/rsiwa.html (pr.06.12.12)
[12] North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3.
(Heretter "Continental Shelf") premiss 74
[13] Ruud og Ulfstein, s.79
[14] *Ibid* s.81

1.2.5 Juridisk teori

Juridisk teori er av ICJ ansett som subsidiær rettskilde. Domstolen skal være ubundet og i utgangspunktet ikke la seg styre av uttalelser i juridisk litteratur. Et godt argument er at det innen litteraturen er stor uenighet, og dermed vanskelig å vise til enkeltforfattere.[15] Jeg har imidlertid måttet vektlegge juridiske forfatteres meninger og teorier i stor grad.

Det finnes ikke et klart internasjonalt rammeverk gjennom lov eller sedvane som kan gi en konsistent bilde av den folkerettslige rettssituasjonen for *jus ad bellum* i cyberspace. Derfor vil sekundære rettskilder måtte tillegges lik eller større vekt enn de primære, for å få et bedre bilde av hva som er gjeldende rett.

1.3. Avgrensninger

Avhandlingens tema ligger innen det man i folkeretten omtaler som *jus ad bellum,* lov om bruk av makt, de reglene som gjelder i overgangen fra fred til væpnet konflikt. Utgangspunktet er cyberoperasjoner foretatt av en stat mot en annen stat uten forutgående væpnet konflikt. Slik sett avgrenses avhandlingen mot *jus in bello* som er regler som kommer til anvendelse når væpnet konflikt er konstatert.

Videre avgrenser jeg mot internasjonal datakriminalitet og terror, da lovgivningen på disse områdene har en annen regulering og karakter.

Trusler om bruk av makt hører til *jus ad bellum,* men vil ikke bli berørt avhandlingen, da det ikke er avgjørende for problemstillingen som sådan.

Problemstillinger rundt selve utøvelsen av selvforsvar vil bli berørt kun i liten grad.

[15] Ruud og Ulfstein s.73

2. FN-paktens artikkel 51

2.1 Retten til selvforsvar

Rett til selvforsvar henger sammen med en stats rett til eksistens, og respekt for sin suverenitet.[16]

Utviklingen av retten til selvforsvar må sees i sammenheng med utviklingen av et lovverk med et formål om å forby krig, og bruk av makt. Frem til begynnelsen av det tjuende århundret var kodifisering av retten til selvforsvar av moderat betydning. Den middelalderske teorien om *bellum justum*, rettferdig krig, var av teologisk opprinnelse og en del av kanonisk rett, og ga ingen gyldige folkerettslige føringer.[17] Helt frem til ca. 1919 var den folkerettslige situasjonen slik at stater hadde rett til å starte og føre krig mot hverandre.

Betydningen av en lovfestet rett til selvforsvar økte proporsjonalt med innskrenkingene i friheten til å ty til krig for å løse konflikter.[18] Utviklingen av en selvforsvarsrett som en del av internasjonal lov har fulgt utviklingen av forbudet mot aggresjon.[19]

Retten til selvforsvar er i dag kodifisert i FN-paktens artikkel 51 og den norske oversettelsen lyder:

Intet i denne Pakt skal innskrenke den naturlige rett til individuelt eller kollektivt selvforsvar når et væpnet angrep er blitt foretatt mot et medlem av de Forente Nasjoner, inntil Sikkerhetsrådet har truffet de tiltak som er nødvendige for å opprettholde internasjonal fred og sikkerhet. Tiltak som et medlem treffer under utøvelsen av denne rett til selvforsvar skal øyeblikkelig meldes til Sikkerhetsrådet og skal ikke på; noen måte innvirke på; Sikkerhetsrådets myndighet eller plikt etter

[16] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p.226 (Heretter "Nuclear Weapons Advisory Opinion") Premiss 96
[17] Prof. Dr. A. Randelzhofer i B. Simma (red), *The Charter of the United Nations 1945 – A Commentary,* (2nd edition, 2002) Art. 2(4) s.115
[18] *Ibid* Art 51 s.789
[19] Yoram Dinstein, *War, Aggression and Self-Defence*, 4th edition, Cambridge 2005 s.177.

denne Pakt til når som helst å treffe slike tiltak som det finner nødvendige for å opprettholde eller gjenopprette internasjonal fred og sikkerhet. [20]

Jeg vil i den videre fremstillingen hovedsakelig forholde meg til den norske oversettelsen. Det kan imidlertid bli nødvendig å se hen til andre lands traktattekst.

Selv om FN-pakten ble skapt i 1945, tilsier ordlyden i artikkel 51 at teorien om retten til selvforsvar er eldre enn det, og da akseptert i sedvanerettslig forstand. Dette fremgår av ordlyden "den naturlige rett til". Ordvalget indikerer at man ved opprettelsen av FN-pakten ønsket å bevare en allerede eksisterende sedvanerettslig hjemmel til selvforsvar innen rammene av FN-pakten.[21]
ICJ slo også fast i "Nicaraguasaken"[22] at det eksisterte en sedvanerettslig rett til selvforsvar ved siden av FN-paktens artikkel 51, men avklarte at selvforsvar er begrenset til tilfeller der det foreligger et væpnet angrep.[23]
Da både sedvanerettslig selvforsvar og selvforsvar etter FN-paktens artikkel 51 forutsetter et væpnet angrep, går jeg ikke videre inn på om selvforsvarsretten går like langt i begge tilfeller.

Selvforsvar etter FN-paktens artikkel 51 hører inn under den delen av folkeretten som kalles *jus ad bellum*.[24] Selvforsvar kan utøves med væpnet makt såfremt kriteriene for å utøve det er oppfylt, og at selvforsvaret utøves med de begrensningene som følger av folkeretten.

2.2 Forbudet mot intervensjon og forbudet mot bruk av makt

FN-paktens artikkel 2(4) inneholder et forbud mot bruk av makt stater i mellom. Artikkelens norske ordlyd lyder som følger:

---

[20] De Forente Nasjoners Pakt 1945 art. 51
[21] Anders Henriksen, *Krigens folkeret og væbnet international terrorbekæmpelse*, København 2010 s.64
[22] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984, p. 392 (Heretter "Nicaragua") premiss193
[23] Ruud og Ulfstein s.197
[24] Vedrørende selvforsvar etter *jus ad bellum* og *jus in bello*, se; http://www.icrc.org/eng/assets/files/other/irrc-872-moussa.pdf

Alle medlemmer skal i sine internasjonale forhold avholde seg fra trusler om eller bruk av væpnet makt mot noen stats territoriale integritet eller politiske uavhengighet eller på noen annen måte som er i strid med de Forente Nasjoners formål.[25]

Av ordlyden fremgår det et forbud mot å bruke makt, eller true med å bruke makt, mot en annen stats territorium eller politiske uavhengighet. I FN-paktens forgjenger Briand-Kellogg Pakten av 1928, ble det kun oppstilt et forbud mot å føre krig, "*condemn recourse to war for the solution of international controversies*".[26]

Ved bruk av "makt" er det akseptert at det menes "væpnet makt".[27] Dette følger ikke direkte av ordlyden i originalteksten, men den norske oversettelsen inneholder ordlyden "væpnet makt".
Langvarig folkerettslig diskurs har imidlertid gått ut på blant annet om det går an å utøve bruk av makt, som for eksempel politisk, økonomisk eller fysisk makt, uten våpen og lignende, herunder bruk av makt i cyberspace.

Forbudet mot bruk av makt i artikkel 2(4) fører med seg unntak og må således sees i sammenheng med flere artikler i FN-pakten. Paktens kapittel 7 om "Tiltak mot trusler mot freden, fredsbrudd og angrepshandlinger" regulerer lovlig bruk av væpnet makt etter nærmere bestemte kriterier. En utfordring er at det ikke er total konsensus i hva som ligger i uttrykket "bruk av makt" når det vurderes opp mot begrep som "trussel mot freden, fredsbrudd, angrepshandling"[28] og "væpnet angrep".[29]
Det som imidlertid er sikkert, er at statenes rett til selvforsvar etter artikkel 51 og Sikkerhetsrådets kompetanse til å bemyndige bruk av makt etter kapittel 7, er to uttrykkelige unntak fra forbudet mot bruk av makt i art 2(4).[30] FNs Sikkerhetsråds kompetanse og handlingsmønster fremgår av artiklene 39 t.o.m. 50. Sikkerhetsrådet må først avgjøre hvorvidt det foreligger trussel mot freden, fredsbrudd eller

[25] De Forente Nasjoners Pakt art. 2(4)
[26] Briand-Kellog Pact - Treaty between the United States and other Powers providing for the renunciation of war as an instrument of national policy. Paris, August 27, 1928
[27] Randelzhofer, *UN Charter Commentary*, Art. 2(4) s.117
[28] De Forente Nasjoners Pakt – 1945 art. 39.
[29] De Forente Nasjoners Pakt – 1945 art. 51.
[30] Henriksen, s.31.

angrepshandlinger, for deretter å iverksette de tiltak de har kompetanse til for å opprettholde internasjonal fred og sikkerhet.

Enkelte folkerettsforfattere hevder artikkel 2(4) skal tolkes innskrenkende og at ordlyden derfor er uttømmende. Det som da hevdes er at det ikke er noe i veien for å true med eller bruke væpnet makt overfor en fremmed stat dersom hensikten bak maktanvendelsen er en annen enn å endre statens territoriale integritet, politiske uavhengighet eller på noen annen måte i strid med De Forente Nasjoners formål. Dette er ikke helt i tråd med bakgrunnen for at FN ble opprettet, ei heller i tråd med FN-paktens øvrige bestemmelser. Av Wien-konvensjonen om traktatretten artikkel 31 fremgår hvordan forbudet mot bruk av makt i art 2(4) skal tolkes lojalt i overenstemmelse med traktatens uttrykk, hensikt og formål. FNs formål er nettopp å opprettholde internasjonal fred, sikkerhet og rettferdighet, og som det også følger av art 2(3), å pålegge medlemslandene å løse konflikter på en måte som ikke truer freden. Forbudet mot bruk av makt etter art 2(4) er med andre ord absolutt, ikke relativt, selv om det tradisjonelt har vært søkt etter flere unntak for å bruke makt lovlig.[31]
Det er fastslått at forbudet mot bruk av makt gjelder alle stater gjennom internasjonal sedvanerett, uavhengig av medlemskap i FN.[32]

En grunnleggende regel i folkeretten er forbudet mot intervensjon, som er en krenkelse av suverenitetsprinsippet. Intervensjon er å gripe inn i en stats anliggender, for eksempel statens politiske, kulturelle eller økonomiske institusjoner.[33]
Ingen stat må bruke eller true med å bruke tvang eller oppfordre til økonomiske-, politiske- eller andre typer tiltak for å tvinge en annen stat til underkastelse.[34]

Grensen mellom ulovlig intervensjon og bruk av makt er trukket opp av ICJ i "Nicaragua". Denne dommen gir et bilde av hvor terskelen for ulovlig bruk av makt er ment å ligge. Her kom ICJ frem til at USAs finansiering av den væpnede opprørsbevegelsen "Contras" i Nicaragua var ansett som ulovlig intervensjon.

---

[31] Henriksen, s.46
[32] "Nicaragua" premiss174
[33] *"Declaration on Priciples of International Law concering Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations"* FNs Generalforsamlings Resolusjon 2625 24. oktober 1970 prinsipp 3.
[34] *Ibid* prinsipp 3(2)

Væpning og trening av "Contras "ble ansett som et brudd på forbudet mot bruk av makt i art 2(4).
Overgangen fra ulovlig intervensjon, til bruk av makt til væpnet angrep som gir grunnlag for væpnet selvforsvar kan virke flytende. Forbudet mot bruk av makt innebærer ikke bare aksjoner foretatt av regulære styrker over en internasjonal grense, men også å sende eller understøtte irregulære styrker eller opprørsgrupper. Visse former for støtte til slike grupper vil kun rammes av intervensjonsforbudet.[35]

I skjæringspunktet mellom hva som omfattes av ulovlig bruk av makt og et væpnet angrep som gir grunnlag for bruk av makt i selvforsvarsøyemed, eksisterer det en gråsone eller et tomrom. Dette er bekreftet av ICJ i "Nicaragua"[36] hvor det uttales at man kan utføre handlinger som er alvorlige og utvilsomt ulovlig bruk av makt, men som ikke er alvorlige nok til å nå opp til terskelen for væpnet angrep. Denne uttalelsen er senere bekreftet i "Oil Platforms".[37] [38] ICJ har hittil ikke uttalt seg om hvor terskelen for væpnet angrep bør ligge. Som utgangspunkt er det Sikkerhetsrådet som avgjør hver situasjon konkret.

2.3 Når oppstår retten til selvforsvar?

Det fremgår av ordlyden i FN-paktens artikkel 51 at en stat som blir utsatt for et væpnet angrep har rett til å forsvare seg, uten å måtte avvente Sikkerhetsrådet. Utøvelse av retten til selvforsvar er ikke begrenset til så katastrofale scenarioer som trussel om utslettelse. Det handler om å, under visse kriterier fastsatt i internasjonal lov, alene eller sammen med andre stater, å svare med bruk av væpnet makt mot ulovlig bruk av makt som kvalifiserer til væpnet angrep, eller eventuelt mot en trussel om bruk av ulovlig makt.[39]
Selvforsvarsretten gjelder statens territorium, men også på et omtvistet område, jfr. for eksempel Falklandskrigen hvor Storbritannia forsvarte et område som det ikke var internasjonal enighet om hvem som hadde best rettigheter til.

[35] Ruud og Ulfstein s.195
[36] Nicaragua" premiss 210
[37] Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I.C.J. Reports 2003, p. 161 (Heretter "Oil Platforms")
[38] Michael N. Schmitt, *The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski,* 4th International Conference on Cyber Conflict NATO CCD COE, Tallinn 2012 s.313
[39] Dinstein, s.175.

2.3.1 Krav om et væpnet angrep

Det fremgår av juridisk teori at det er uklart hva som ligger i begrepet "væpnet angrep". På den ene siden hevder ICJ at det er en generell enighet om hva slags handlinger som kan omtales og kategoriseres som væpnede angrep.[40] "*There apperes now to be a general agreement on the nature of the acts which can be treated as constituting armed attacks*".
På den annen side konkluderer Randelzhofer i sine kommentarer til FN-paktens artikkel 51 med at selv med årevis med anstrengelse og betydelig innsats, er det fortsatt ikke konsensus vedrørende en definisjon av uttrykket "væpnet angrep".[41]

I "Nicaragua" ser man at det sondres mellom alvorlige og mindre alvorlige brudd på forbudet mot bruk av makt, og væpnet angrep. For eksempel vil "*a mere frontier incident*" falle utenfor begrepet væpnet angrep.[42] Selv om det ikke er enighet i hva begrepet væpnet angrep innebærer, fremgår det likevel at det skal eksistere en nedre grense for hva som kan oppfattes som et væpnet angrep, en *de minimis* regel.[43] Denne *de minimis* regelen er kritisert, bl.a. i Dinstein "War, aggression and self defence", og omtalt som forvirrende.[44]

Uavhengig av internasjonal uenighet må det, både i denne fremstillingen og i folkeretten forøvrig, opereres med en grense for hva slags bruk av makt som kan defineres som et væpnet angrep. Randelzhofer mener definisjonen av aggresjon fra FNs Generalforsamlings resolusjon 3314 av 34. desember 1974 artikkel 3 er illustrerende for hvilke handlinger som klassifiseres som et væpnet angrep.[45] Dette vil kunne knyttes opp mot den franske traktatteksten hvor bruk av makt omtales som "agression armée". Andres Henriksen oppsummerer fra Resolusjon 3314;
"*et væpnet angrep vil kunne være en realitet hvis en stats væpnede styrker angriper eller bombarderer en annen stats territorium, blokkerer en annen stats havn eller kyst, angriper en annen stats land, sjø eller luftstyrker eller befinner seg på en annen stats territorium i strid med avtale med vertsstaten, å tillate en annen stat å bruke sitt*

[40] Nicaragua" premiss 195
[41] Randelzhofer, *UN Charter Commentary*, Art.51 s.796
[42] Nicaragua" premiss 195 og Henriksen, s.69
[43] Henriksen, s.69
[44] Dinstein, s.195
[45] Randelzhofer, *UN Charter Commentary* Art.51 s. 795

territorium til å foreta aggresjonshandlinger mot en tredje stat, eller å stille seg bak og sende væpnede grupper som foretar væpnede handlinger mot en annen stat".[46]

Yoram Dinstein omtaler et væpnet angrep som;
"*use of force producing (or liable) to produce serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property. When no such results are engenderd by (or reasonable expected from) a recource to force, article 51 does not come into play*". [47]
Ut fra denne definisjonen er det konsekvensene av ulovlig bruk av makt som avgjør hvorvidt en stat er utsatt for et væpnet angrep.
Resolusjon 3314 baserer seg på væpnede handlinger, uten å konkretiserer våpnene, eller instrumentene. Det samme med Dinstein, som og kun fokuserer på konsekvenser.

Sammenfattet med ICJ uttalelsene fra "Nicaragua", må man skille mellom mindre alvorlig og mer alvorlig bruk av makt, hvor kun alvorlige brudd med gitte konsekvenser kan ansees å være et væpnet angrep som gir rett til å benytte væpnet makt i selvforsvar. I "Nicaragua" vurderes således maktens "scale and effect".

I henhold til ICJs uttalelser i saken "Oil Platforms" i 2003 er det den staten som ønsker å rettferdiggjøre bruken av væpnet makt i selvforsvar, som har bevisbyrden for at den er under et væpnet angrep som legitimerer selvforsvar.[48]
Den angrepne stat må selv vurdere maktbrukens "scale and effect" og avgjøre hvorvidt den er under et væpnet angrep.
Dersom bruken av makt er alvorlig nok, og konsekvensene er alvorlige nok vil man kunne være utsatt for et væpnet angrep.

2.3.2 Hvordan avgjøre om et væpnet angrep er blitt foretatt?

Enkelte har forsøkt å sette opp kriterier som skal fungere som veiledning for om den ulovlige bruken av makt er alvorlig nok til å kunne kvalifisere som et væpnet angrep.

[46]Henriksen, s.71
[47] Dinstein, s.193
[48] "Oil Platforms" premiss 57

Disse kriteriene fungerer som et analyseverktøy for stater som blir utsatt for maktbruk. Dette har gjort det vesentlig lettere å akseptere det faktum at "væpnet angrep" aldri er klart definert, og muligens gitt begrepet en fordel for fremtiden i og med at tolkningen blir mer dynamisk og lettere lar seg tilpasse utvikling og modernisering.

Jean S. Pictets "scope, duration and intensity" kriterier, fra kommentarene til Genève-konvensjonen for å indentifisere en væpnet konflikt, kan brukes som utgangspunkt i en analyse av en stats maktbruk for å eventuelt identifisere og klassifisere graden av bruk av makt.[49] Etter denne testen vil bruk av makt kunne klassifiseres som væpnet angrep når maktbruken er av en tilstrekkelig grad av "omfang, varighet og intensitet".[50] Det norske Forsvaret omtaler skalaen som konfliktspekteret, og nivået bestemmes ut fra Pictets kriterier.[51]

Videre vil det være naturlig å trekke frem de såkalte "Schmitt-kriteriene".[52] Kriteriene er antagelser og forslag som kan brukes som et verktøy for å komme frem til det som ansees å være *de lege lata*, og ikke normative standarder. Kriteriene er tilpasset "Computer Network Attacks" eller "cyberangrep", og vil bli redegjort for senere. "Pictet –kriteriene" og "scale and effect" har imidlertid vist seg effektive for maktvurderingen ved konvensjonell krigføring, og vil muligens kunne overføres til alternative angrepsmetoder i fremtiden.

2.4 Utøvelsen av selvforsvar

Bruk av væpnet makt i selvforsvar forutsetter at en angripende part kan identifiseres og ansvarliggjøres. Selvforsvarshandlingene begrenses av prinsippene om nødvendighet, proporsjonalitet og umiddelbarhet.

[49] David Graham, *Cyber Threats and the Law of War,* Journal of National Security Law and Policy vol4:87, s.90
[50] Jeffrey Carr, *Inside Cyber Warfare,* USA 2010 s. 58
[51] Forsvarsstaben, Forsvarets Fellesoperative Doktrine 2007, Oslo 2007 s.13
[52] Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework,* The Columbia Journal of Transnational Law, Volume 37, 1999, pages 885-937. s.924

2.4.1 Identifikasjon og ansvar

Den internasjonale traktatretten avgjør om en traktat er i kraft og innholdet av denne. Man må gå til ansvarsreglene for å bestemme om et brudd på traktaten medfører ansvar.[53] De folkerettslige ansvarsreglene bygger på folkerettslig sedvanerett. FNs folkerettskommisjon har siden 1949 arbeidet med å kodifisere og utvikle reglene for statlig ansvar.[54] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongfull Acts[55] er et forslag som er tatt til etterretning og anbefalt i bl.a. FNs Generalforsamlings resolusjon 56/83[56], og selv om resolusjonen ikke er bindende, er de langt på vei dekkende for hva som er innholdet i de sedvanerettslige ansvarsreglene.[57] ICJ har henvist til et tidligere utkast av ILC Articles on State Responsibility, i en sak mellom Ungarn og Slovakia i 1997.[58]
ILC Articles on State Responsibility slår fast at det foreligger en internasjonal rettsstridig handling når handlingen eller unnlatelsen av den er knyttet til staten og er et brudd på statens internasjonale forpliktelser.
FN-paktens forplikter ikke bare FNs medlemsland, men også ikke-medlemsland til å avstå fra bruk av makt og foreta væpnede angrep.[59] Handlingene er å regne som internasjonale rettstridige handlinger etter ILC Articles on State Responsibility.
Der det foreligger en internasjonal rettstridig handling, må det knyttes statsansvar til handlingen før sanksjoner kan iverksettes. ILC Articles on State Responsibility del I kapittel II, inneholder regler for hvordan en stat kan bli ansvarlig for en internasjonal rettsstridig handling.
Reglene baserer seg på staters plikt til å føre kontroll over egne interne forhold, og det blir statens ansvar når den mangler evne eller vilje til å forholde seg til sine internasjonale plikter. Dette vil bli behandlet grundig senere i fremstillingen.

2.4.2 Begrensninger i selvforsvarsretten

FN paktens artikkel 51 gir rett til selvforsvar, uten videre veiledning om selvforsvarets innhold. Fra lovteksten vet vi at selvforsvarsretten gjelder inntil

---

[53] Ruud og Ulfstein, s.292
[54] *Ibid* s.293
[55] Heretter forkortet, ILC Articles on State Responibility
[56] FNs Generalforsamlings Resolusjon 56/83, 28. Januar 2002.
[57] Ruud og Ulfstein, s.293
[58] Gabcikovo-Nagymaros Project (HungarylSlovakia), Judgment I.C.J. Reports 1997, p. 7 (Heretter "Gabcikovo-Nagymaros project")
[59] Nicaragua" premiss 174

Sikkerhetsrådet har vedtatt å iverksette tiltak som er nødvendige for å opprettholde internasjonal fred og sikkerhet. Ideen bak denne idealistiske tanken, var at opprettholdelse av freden skulle være FNs oppgave. Derfor er egentlig selvforsvarsretten av subsidiær karakter.[60] Imidlertid er Sikkerhetsrådet ofte lite effektivt, og hindres av vetoretten. Den enkelte stats rett til selvforsvar må derfor gjelde helt til Sikkerhetsrådet faktisk har iverksatt effektive tiltak for å sikre fred og sikkerhet i konfliktområdet.[61]

I retten til selvforsvar ligger begrensninger som ikke følger av ordlyden i artikkel 51, men som ligger implisitt i begrepet, og som er anerkjent av det internasjonale samfunn.[62] Det fremgår bl.a. av "Nicaragua" at prinsippene om proporsjonalitet og nødvendighet er etablert folkerettslig sedvane.[63] Sentralt i etableringen av denne sedvaneretten var "Caroline-hendelsen" hvor det i etterkant er anerkjent at selvforsvar begrenses til "*the necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation*".[64] Slik blir også umiddelbarhet en begrensning.

Med umiddelbarhet menes at en selvforsvarsaksjon må følge direkte som et svar på et væpnet angrep, og ikke som en senere hevnaksjon.
Med proporsjonalitet og nødvendighet menes at en selvforsvarsaksjon må i omfang, varighet og intensitet begrenses til det som er nødvendig for å sikre sin egen overlevelse og slå tilbake det væpnede angrepet. Det er viktig å understreke at proporsjonalitet ikke nødvendigvis innebærer at man må forsvare seg med samme våpen eller midler som det væpnede angrepet består av, og at man heller ikke er begrenset til å jage eventuelle invasjonsstyrker over grensen, men har mulighet til å forfølge dem så lenge det ansees som nødvendig.[65]

[60] Randelzhofer, *UN Charter Commentary*, *Art.51* s.805
[61] Ruud og Ulfstein, s.201
[62] Randelzhofer, *UN Charter Commentary*, *Art.51* s.805
[63] Nicaragua" premiss 176
[64] Daniel Webster, gjengitt i Ruud og Ulfstein, s.196
[65] Randelzhofer, *UN Charter Commentary*, *Art.51* s.805

2.4.3 Individuelt og kollektivt selvforsvar

FN paktens artikkel 51 hjemler både individuelt og kollektivt selvforsvar. Med det menes at en annen stat som ikke er direkte angrepet kan, etter anmodning fra den angrepne stat, gripe til våpen til forsvar for den angrepne stat. Dette er anført som det rettslige grunnlaget for forsvarsallianser.[66] I artikkel 5 i NATO-pakten henvises det til FN-paktens artikkel 51, og det slås uttrykkelig fast at et angrep på et medlemsland er et angrep på alle medlemslandene.[67]

2.4.4 Kort om preventivt selvforsvar

Rent unntakelsesvis anerkjenner folkeretten det prinsipp om at en stat kan bruke væpnet makt i selvforsvar for å forsvare seg mot et sannsynlig og snarlig angrep mot staten. Dette kalles gjerne preventivt selvforsvar. Dersom det kan påvises en forskjell på konvensjonell krigføring og cyberangrep, kan dette være et interessant tema for fremtiden.

3. Cyberoperasjoner og *Jus ad Bellum*

3.1 Introduksjon til Cyberoperasjoner

Like lenge som det har eksistert datamaskiner har det vært krefter som har ønsket å benytte disse til militære eller kriminelle formål. Angrep fra datahackere skjer hver dag.[68]

Sjeldnere, men av en vesentlig større trussel, er cyberangrep fra stater.[69]

I 2007 ble Estland utsatt for massive cyberangrep, i 2008 ble Georgia utsatt for angrep og i 2010 ble Iran utsatt for angrep. Disse hendelsene, sammen med mer kjente aksjoner og grupper som ”Wikileaks” og ”Anonymous” kan ha bidratt til å øke fokuset på cybertrusselen på verdensbasis. Med trussel må det også følge regulering, og cyberspace er i dag gjenstand for flere juridiske problemstillinger.

---

[66] Ruud og Ulfstein, s.196
[67] The North Atlantic Treaty 1949, Article 5
[68] http://www.f-b.no/nyheter/herfra-avverges-10-000-hackerangrep-i-dognet-1.7654028 (pr.07.12.12)
[69] http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10073527 (pr.07.12.12)

Videre følger definisjoner av begrep, samt beskrivelse av teori og metodeverktøy, som gir en nødvendig avklaring vedrørende problematikken før avhandlingens problemstilling kan behandles fullt ut.

3.1.1 Definisjoner og begrepsavklaringer

Cyberspace og cyberdomenet.

Cyberspace er den elektroniske verden av datanettverk hvor vår nettverksbaserte kommunikasjon foregår.[70] Cyberspace inkluderer internett, radiobølger, telenett og andre datanettverk. Cyberspace går på tvers av landegrensene og knytter sammen folk fra hele verden. Cyberspace er både noe håndfast, datamaskiner og fiberoptiske ledninger, og noe abstrakt, en kanal for ikke-fysisk, virtuell kommunikasjon og samhandling.[71]

Cyberdomenet kan muligens defineres som noe mer håndfast og regnes av enkelte som et eget domene, altså et "sted" på lik linje med fysiske størrelser som land, sjø, luft og verdensrom. Cyberdomenet omtales enkelte steder som en slagmark.[72] Denne tilnærmingen kan til en viss grad brukes for å skille ut et enkelt lands cyberdomene fra det verdensomspennende cyberspace. Definisjonene er diskuterbare, men illustrerende for å skille mellom det en stat anser som sitt domene, og det som er grenseoverskridende.

Psykologiske operasjoner

Psykologiske operasjoner (PSYOPS) er planlagte operasjoner for å formidle og spre informasjon til et utvalgt publikum for å påvirke følelser, motiv eller objektiv vurdering med mål å påvirke tankegang og handlinger til styresmakter, organisasjoner, grupper og individer. PSYOPS blir typisk distribuert som informasjon for effekt, brukt i fredstid og konflikt, for å informere og påvirke.[73]

---

[70] http://www.thefreedictionary.com/cyberspace (pr.12.12.12)
[71] Hans Inge Langø, *Nye sikkerhetstrusler: Cyberangrep*, Hvor hender det nr. 23, 9. Mai 2011, del 2. http://hvorhenderdet.nupi.no/Artikler/2010-2011/Nye-sikkerhetstrusler-cyberangrep/(part)/2 (pr.12.12.12)
[72] http://forsvaret.no/aktuelt/publisert/pressemeldinger/Sider/Cyberkonferansen-2011.aspx (pr.12.12.12)
[73] Joints Chief of Staff , *Doctrine for Joint Psycological Operations,* Joint Publication 3-53 5.september 2003

Cyberangrep og cyberoperasjoner

U.S. Department of Defense har en definisjon i sin Dictionary of Military Terms på et datanettverksangrep, eller Computer Network Attack (CNA) som kan oversettes til handlinger utført gjennom bruken av datanettverk for å forstyrre, nekte, bryte ned eller ødelegge informasjon lagret i datamaskiner og datanettverk, eller selve datamaskinene og nettverkene.[74] NATO bruker også denne definisjonen, men legger til setningen "et datanettverksangrep er en type cyberangrep" uten å definere cyberangrep.[75] I henhold til The 2006 United States National Military Strategy for Cyber Operations inkluderer begrepet Cyber Network Operations (CNO) både datanettverksangrep (CNA), Computer Network Defence (CND) eller datanettverksforsvar, og såkalte Related Computer Network Exploitation Enabeling Operations eller CNE som er en form for datanettverksetteretningsoperasjoner som ikke har som formål å ødelegge eller forstyrre, men kun samle informasjon og observere.[76] "The Shanghai Cooperation Organization"[77] bruker begrepet "information war", som defineres som masse-psykologisk hjernevasking for å destabilisere samfunn og stat, så vel som å tvinge staten til å ta avgjørelser i en annen stats interesser.[78]

Den "vestlige" tilnærmingen er snevrere enn den "østlige", og baserer seg på handlinger med en intensjon om å fremprovosere fysiske konsekvenser i et datanettverk. Den "østlige" tilnærmingen utvider begrepet, og inkluderer politisk og samfunnsmessig påvirkning. På den ene siden er den første definisjonen kanskje for snever, ettersom den i utgangspunktet retter seg mot ødeleggelser i et datanettverk, men på den andre siden blir SCOs tilnærming i overkant vid sett med norske øyne.

---

http://nb.xiandos.info/w/images/7/7c/DoD_PsyOps_declaration-jp3_53.pdf (pr.12.12.12)

[74] http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html (pr.12.12.12)

[75] Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context,* 4th International Conference on Cyber Conflict NATO CCD COE, Tallinn 2012 s. 283

[76] Marco Roscini, *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force,* Max Planck Yearbook of United Nations Law vol. 14 p.85 2010 s. 92

[77] Heretter SCO - En mellomstatlig gjensidig sikkerhetsorganisasjon grunnlagt 2001. Medlemmer er Kina og Russland, sammen med flere Sovjet-Asiatiske land.

[78] Hathaway and Crootof, *"The Law of Cyber-Attack"* Faculty Scholarship Series. Paper 3852. 2012 s.825

Cyberangrep bør da forstås som et mer omfattende begrep enn datanettverksangrep, og således å favne et videre spekter av offensive handlinger mot en stats cyberdomene og som kan få konsekvenser både i og utenfor cyberdomenet. Av hensyn til enkel fremstilling benytter jeg meg av begrepene cyberoperasjoner, cyberangrep, cyberforsvar og cyberetterretning.

3.1.2 Ikke-kinetiske instrumenter som våpen

Kinetiske våpen er våpen som baserer seg på bevegelsesenergi, som prosjektiler, granater eller raketter. Ikke-kinetiske våpen kan kategoriseres som ikke-dødelige eller mindre-dødelige våpen, som ikke baserer seg på fysisk bevegelsesenergi, som akustiske våpen, kjemiske og biologiske våpen eller elektromagnetisk puls.

ICJ har slått fast at bruk av makt referer til alle former for våpen.[79]
Den forståelsen av våpen som traktatforfatterne la til grunn ved dannelsen av FN-pakten passet bra på tradisjonell militær kinetisk maktbruk, men desto dårligere på alternative former for maktbruk og ikke-kinetiske våpen.
I dag er tilnærmingen mer nyansert. "Max Planck Encyclopedia of Public International Law" beskriver tilstanden slik dagens tolkning av våpen bør oppfattes; *"it is neither the designation of a device, nor its normal use, which make it a weapon but the intent with which it is used and its effect. The use of any device, or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore be deemed to fulfil the conditions of an 'armed' attack."*[80]
Eksempelvis anerkjente Sikkerhetsrådet etter 9/11, USAs rett til selvforsvar etter å ha blitt angrepet med kaprede fly som våpen.[81]
Bruk av makt og væpnede angrep kan altså utføres uavhengig av instrumentene, da det er instrumentbrukens konsekvenser som må legges til grunn. Slik sett faller datamaskiner med programmer inn under definisjonen av instrumenter som kan

[79] "Nuclear Weapons Advisory Opinion", premiss 39
[80] Max Planck Encyclopedia of Public International Law, Karl Zamenek, *Armed attack,* oppdatert april 2009, punkt 21. http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e241&recno=1&author=Zemanek%20%20Karl (pr.12.12.12)
[81] FNs Sikkerhetsråds Resolusjon 1368, 12 september 2011

benyttes til å utføre væpnede angrep, da cyberangrep mot datanettverk kan få fysiske konsekvenser.

3.2 Cyberoperasjoner som ulovlig intervensjon og bruk av makt

Cyber teknologi og ekspertise er relativt billig og enkelt å få tak i, noe som gjør alle stater eller grupper og individer til potensielle trusler og alle stater med datanettverkstyrt infrastruktur til potensielle ofre.

3.2.1 Kan en cyberoperasjon være ulovlig intervensjon?

I Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States heter det at statene og deres folk skal ha fri tilgang til informasjon og mulighet til å utvikle, uten innblanding, sitt eget informasjonssystem og massemedia, og å bruke sine informasjonsmedia for å spre det de måtte ønske av politiske, sosiale, økonomiske og kulturelle interesser og ambisjoner innenfor det som følger av menneskerettigheter og prinsipper for internasjonal informasjonsbehandling.[82]

Et cyberangrep som trenger inn i en stats cyberdomene, og som blander seg inn i eller truer statens politiske, kulturelle eller økonomiske institusjoner, for eksempel for å påvirke utfallet av et valg eller innholdet i en handelsavtale, vil mest sannsynlig kategoriseres som ulovlig intervensjon.

Andre typer cyberoperasjoner, som CNE eller PSYOPS mot cyberdomenet er mer tvilsomt. CNE er, så lenge det ikke medfører konsekvenser som kan endre dem til CNA, ikke forbudt etter folkeretten og vil i utgangspunktet ikke kunne oppfattes som ulovlig intervensjon. Slike handlinger vil eventuelt være forbudt etter nasjonal lovgivning.
PSYOPS mot cyberdomenet ligger mer i grenseland. PSYOPS innen *jus in bello* er lovlige operasjoner, også mot sivilbefolkning, såfremt de ikke er fremsatt med intensjon om å skade eller terrorisere.[83] PSYOPS i fredstid, vil lettere kunne ansees

[82] FNs Generalforsamlings Resolusjon 36/103, 9. Desember 1981 Punkt I (c)
[83] Michael N. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, IRRC Vol.84 juni 2002 s.578

som en trussel eller intervensjon, særlig i de tilfellene informasjonen spres gjennom inntrengning i datanettverk.
Å spre propaganda ved å ta over offentlige informasjonskanaler i en annen stat, eller å spore opp og ta over epostkontoer og sende ut masse-epost til velgere i den hensikt å påvirke utfallet av interne anliggender vil kunne komme inn under ulovlig intervensjon. PSYOPS som ren propaganda, med en klar avsender og et ikke truende innhold vil mest sannsynlig ikke. Det er på den annen side lite tvilsomt at medlemsland i Shanghai Cooperation Organization vil kunne oppfatte dette som truende adferd, og karakterisere det som minst ulovlig intervensjon.
Ulovlig intervensjon kan forekomme som følge av cyberoperasjoner.

3.2.2 Kan en cyberoperasjon være bruk av makt etter FN-paktens artikkel 2 (4)?

For å avgjøre om en cyberoperasjon er bruk av makt etter artikkel 2(4) bør man tilnærme seg problemstillingen gjennom en analyse. Dette for å skille mellom det som kan være lovlige handlinger, en tilfeldighet, en tabbe, eller kriminelle handlinger, fra det som faktisk kan være ulovlig bruk av makt.

Instrumentbasert, konsekvensbasert eller direkte objektiv tilnærming

Forskjellige teoretiske tilnærminger har utviklet seg, for å forenkle klassifiseringen av maktbruk og konkretisere et angreps omfang, varighet og intensitet på konvensjonelle som ukonvensjonelle våpen.

FN-pakten ble nedtegnet med en instrumentbasert tilnærming, altså en vurdering om hvorvidt ulovlig bruk av makt følger som et resultat av kinetisk bruk av makt.
På denne tiden virket den instrumentbaserte modellen mest nærliggende å benytte seg av, da følgene man ville unngå som regel var en følge av bruken av kinetiske våpen.[84]
Det ble hevdet at en konsekvensbasert tilnærming ville ha for stort innslag av subjektivitet når man skulle avgjøre om man var utsatt for enten lovlige pressmidler eller ulovlig bruk av makt.[85]

[84] Schmitt, *Cyber operations and the Jus ad Bellum revisited,* s.573
[85] Andrew Foltz, *Stuxnet, Schmitt Analysis and the Cyber "Use of Force" Debate*, JFQ issue 67 4th quarter 2012 s.42

Konsekvensbasert tilnærming baserer seg på at det er operasjonens konsekvenser som er avgjørende for klassifiseringen. Ved siden av fysiske konsekvenser vil en cyberoperasjon som går inn for å ødelegge eller forstyrre banker og finansinstitusjoners datanettverkssystem i den hensikt å skade statens økonomi, kunne være ulovlig bruk av makt, selv om operasjonen i seg selv ikke hadde latt seg gjøre ved bruk av kinetiske våpen. Konsekvensene avgjør hvorvidt det er ulovlig bruk av makt eller ikke. Denne tilnærmingen kan være gunstig, men vil, som lovgiver antydet, ha en stor grad av subjektivitet når konsekvensene skal vurderes.

En siste tilnærming baserer seg på direkte objektivt ansvar, og går ut på at et cyberangrep er ulovlig bruk av makt dersom de er rettet mot kritisk informasjons infrastruktur, pga. de katastrofale følgene dette kan få. Da det er opptil den enkelte stat å selv definere hva de anser som kritisk informasjons infrastruktur, vil også denne tilnærmingen ha en stor grad av subjektiv vurdering.[86]

Ettersom det ikke finnes noen enighet på en presis definisjon av bruk av makt, verken i eller utenfor cyberspace, blir følgen at det i stor grad er overlatt til statene å definere begrepet og legge terskelen for bruk av makt deretter.[87]

Hvilket omfang har bruk av makt begrepet?

Vanskeligheten med å klart definere nedre grense for ulovlig bruk av makt, medfører at man må se på hver enkelt hendelse og dens maktbruk. Det er tydelig at våpenbruk fra en stat mot en annen, som ikke er streifskudd over grensen eller små ubetydelige skuddvekslinger, som for eksempel tung artilleriskyts eller bombing kan kategoriseres som ulovlig bruk av makt etter FN-paktens artikkel 2(4). Det vil ikke være mindre kontroversielt å antyde at cyberoperasjoner som medfører konsekvenser lik de kinetiske våpnene kan kategoriseres som ulovlig bruk av makt. Derfor må cyberoperasjoner som direkte resulterer i fysisk skade på individer eller objekter, likestilles med kinetiske våpen som forårsaker det samme. Hvorvidt maktbruken kvalifiserer til et væpnet angrep etter FN-paktens artikkel 51 kommer jeg tilbake til.

[86] FNs Generalforsamlings Resolusjon 58/199, 30 Januar 2004
[87] Schmitt, *Cyber operations and the Jus ad Bellum revisited*, s. 573.

Hvor ligger bruken av makts nedre grense?

For å trekke opp noen linjer i cyberspace, vil jeg først forsøke å se hvor den nedre terskel for ulovlig bruk av makt i art. 2(4) kan tenkes å ligge. Da de fleste kjente cyberoperasjoner ikke har fått den type konsekvenser som artilleriskyts og bombing medfører, betyr det at det ikke har vært utsatt for bruk av makt?

Jeg vil gå tilbake til traktatordlydens innhold.
Helt fra FN-paktens tilblivelse har begrepet "bruk av makt", eller "use of force" vært gjenstand for uenighet.
Av forarbeidene til FN pakten fremgår det at et forslag om at økonomisk press skulle inngå i ulovlig bruk av makt ble avslått.[88] Under arbeidet med det som skulle bli UN General Assembly's Declaration on Friendly Relations[89], ble det debattert om "force" skulle involvere alle former for pressmidler, herunder de som også er av politisk og økonomisk karakter og som truer en stats politiske uavhengighet eller territoriale integritet.
På den andre siden ble forslag om å innsnevre begrepet "force" i 2(4) til å kun omfatte "armed force" nedstemt under forhandlingene og nedtegningen.[90] En følge av en slik begrensning ville kunne ført til at all bruk av "armed force" ville kunne bli oppfattet som et "armed attack".
Det fremstår som om det har vært lovgivers vilje at "armed" ble utelatt fra artikkel 2(4) for å skille klart ulovlig bruk av makt, og væpnet angrep. Med tanke på at "armed force" blir brukt i andre steder, bl.a. artikkel 41, kan det tyde på at "bruk av makt" ikke er begrenset til "bruk av væpnet makt".

I "Nicaragua" karakteriserer ICJ enkelte handlinger som ikke er av kinetisk karakter, for å være bruk av makt, samt andre handlinger for å kun være ulovlig intervensjon.

"In the view of the Court, while the arming and training of the contras can certainly be said to involve the threat or use of force against Nicaragua, this is not necessarily

[88] UNICO Documents 251 p. 253-254 fra Schmitt, *Cyber operations and the Jus ad Bellum revisited,* s.574
[89] FNs Generalforsamlings resolusjon 2625, 24. oktober 1970
[90] Schmitt, *The "Use of Force" in Cyberspace"* s.313 hentet fra UN General Assembley on Official Records Special Comittee on Friendly Relations, UN Doc A/AC.125/SR.114 1970

so in respect of all the assistance given by the United States Government. In particular, the Court considers that the mere supply of funds to the contras, while undoubtedly an act of intervention in the internal affairs of Nicaragua, as will be explained below, does not in itself amount to a use of force."[91]

Å forsyne med våpen og gi trening til gerilja i en annen stat er bruk av makt. Å finansiere gerilja i en annen stat er kun ulovlig intervensjon. Oversatt til cyberterminologi kan vi si at å finansiere en gruppering av datahackere eller "hacktivists" kun er ulovlig intervensjon. Det å utstyre samme gruppe med nødvendig programvare samt instruere disse, vil være bruk av makt.
Terskelen for bruk av makt ligger da et sted mellom det som forårsaker fysisk skade, ødeleggelse eller død, og en form for politisk eller økonomisk press.[92] Dette støttes av "International Group of Experts" i Tallinn-manualen som kom ut i oktober 2012.[93]

I tråd med FN-paktens formål, som blant annet er å sikre fremtidige generasjoner mot krigens grusomheter, ansees det som fornuftig å fastsette en forholdsvis lav terskel for det som kan sette fred og sikkerhet i fare, altså bruk av makt, og en høy terskel for hva som ansees som et væpnet angrep som gir den angrepne staten rett til bruk av makt.[94]

Foreløpig mangler det rettspraksis på området. De hendelsene som involverer cyberangrep i en eller annen form, har det vært umulig å spore beviselig tilbake til en stat. I den grad det eventuelt hadde vært mulig knytte ansvar til cyberangrepene, er det sannsynlig at mange land ville nølt med å karakterisere enkelte cyberangrep som bruk av makt, kun for å ikke eskalere en konflikt.[95] Slik sett kan man bare spekulere i hvor terskelen plasseres den dagen alle teorier skulle tilsi at et faktisk cyberangrep er bruk av ulovlig makt.

---

[91] Nicaragua" premiss 228
[92] Schmitt, *Cyber operations and the Jus ad Bellum revisited*, s.575
[93] The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* Ed. Michael N. Schmitt Online draft oct 2012. http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft s.49. (Tallinn manualen) (pr.13.12.12)
[94] Schmitt, *The "Use of Force" in Cyberspace*, s.313
[95] Schmitt, *Cyber operations and the Jus ad Bellum revisited*, s.575

Schmitt-Kriteriene

Problemet med artikkel 2(4) er at de tidligere nevnte tilnærmingene på hver sin måte er vanskelig å overføre til cyberspace. En ren instrumentbasert tilnærming vil utelukke at cyberangrep er ulovlig bruk av makt, fordi de mangler den tradisjonelle kinetiske karakteristikken som er assosiert med ulovlig bruk av makt. En ren konsekvensbasert tilnærming vil ha stor grad av subjektivitet når man vurderer konsekvensene. Å sammenligne et cyberangreps konsekvenser med et kinetisk angreps konsekvenser utelukker i stor grad gråsonene innen begrepet bruk av makt. En tilnærming basert på rent objektivt ansvar, blir også å tilknytte statens subjektive vurderinger for hva som er kritisk informasjons infrastruktur for stor betydning. Det er for eksempel vesentlig forskjell i SCOs og EUs definisjon av kritisk informasjonsinfrastruktur.[96]

Professor Michael N. Scmitt ved US Naval College har, med bred støtte fra "The International Group of Experts" i CCDCOE,[97] presentert en løsning for hvordan en stat mest sannsynlig vil karakterisere en cyberoperasjon mot dem som ulovlig bruk av makt. Løsningen har elementer av både konsekvens og instrumentbasert tilnærming, og er inntatt i Tallinn manualen.[98] Schmitts analysemodell inneholdt opprinnelig syv kriterier. Disse kriteriene har jeg oversatt, i den grad de lar seg oversette, fra *severity, immidiacy, directness, invasiveness, measurability, presumptive legaitimacy og state involvement.* I Tallinn manualen har det blitt tatt inn ett ekstra kriterium, *military character.* Kriteriene har ikke normativ status og er heller ikke uttømmende, så andre vurderinger vil også ha betydning. For å vurdere hvert kriterium er det oppstilt spørsmål som kan bidra til å kartlegge innholdet av et faktisk angrep.

I hvert enkelt kriterium ligger følgende forklaring:

Alvorlighetsgrad

Cyberangrep som påfører individer, eiendom eller objekter fysisk skade, vil bli klassifisert som ulovlig bruk av makt. Handlinger som medfører kun mindre irritasjon og ulempe vil mest sannsynlig ikke. Mellom disse ytterpunktene vil vurderinger av omfanget, størrelse, varighet, tap, både menneskelige og økonomiske samt andre

[96] Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resorces 2011 s.15
[97] Cooperative Cyber Defence Centre of Excellence
[98] Tallinn manualen, s.49-52.

ødeleggelser, være av stor betydning for å avgjøre alvorlighetsgraden. Hvor mange døde og hvor mange ble såret? Hvor stort område ble angrepet, og hvor store var skadene i dette området? Alvorlighetsgraden er det mest avgjørende kriteriet.

Umiddelbarhet

Handlinger med konsekvenser som manifesterer seg raskt, uten tid til å dempe skadevirkninger eller søke en fredelig løsning er mer sannsynlig å bli sett på som bruk av makt enn handlinger med forsinkede konsekvenser. Når merket man effektene av cyberangrepet, og hvor lang tid tok det før effektene avtok?

Direkthet

Desto mer direkte årsakssammenheng mellom cyberoperasjonene og konsekvensene, jo mer sannsynlig vil det bli sett på som bruk av makt. Var cyberoperasjonen den utløsende årsaken til følgene? Var det andre medvirkende årsaker som økte konsekvensene av operasjonen?

Grad av invasjon

Dette kriteriet referer til i hvilken grad cyberoperasjoner penetrerer en stats beskyttede cyberdomene. Jo mer et cyberangep svekker en stats territorielle integritet eller en stats suverenitet, jo større sjanse for at det karakteriseres som bruk av makt. Medførte cyberoperasjoen innbrudd i et sikret nettverk? Var målet for operasjonen i den angrepne stat?

Målbarhet

Stater er vil være mer tilbøyelig til å anse cyberoperasjon som bruk av makt dersom konsekvensene er lett gjenkjennelige og objektivt kvantifiserbare. Kan konsekvensene av operasjonen tallfestes? Hvor sikker er i så fall denne kalkulasjonen?

Militær karakter

En sammenheng mellom en cyberoperasjon og militær operasjon øker sannsynligheten for at cyberoperasjonen anses som bruk av makt. Var det militære styrker som stod bak cyberoperasjonen? Var militære styrker eller objekter målet for cyberoperasjonen?

Presumptiv legalitet

Det følger av det såkalte Lotusprinsippet, fra saken om SS-Lotus,[99] at handlinger som ikke er forbudt gjennom statlige avtaler, må ansees som lovlige. Kriteriet referer til hvorvidt en operasjon anses som lovlig av det internasjonale samfunnet. Da bruk av makt i utgangspunktet er ulovlig i fravær av en gyldig grunn, som selvforsvar, vil andre handlinger, som ikke er bruk av makt, være lovlige i fravær av traktatsforbud. Har denne typen handling tidligere blitt karakterisert som bruk av makt? Ligner denne handlingen på andre handlinger som er antatt lovlig?

Statlig involvering

Kriteriet referer til i hvilken grad konsekvensene av et cyberangrep kan tilskrives en stat, i motsetning til andre aktører. Det er kun stater som kan ansvarliggjøres for bruken av makt. Jo tettere sammenheng mellom en cyberoperasjons karakter, og statlig involvering, jo større sjanse er det for at cyberoperasjonen vil bli ansett som bruk av makt. Jo løsere sammenheng mellom stat og cyberoperasjon, jo større sjanse er det for at operasjonen vil bli ansett som kriminalitet eller andre mindre alvorlige handlinger.

Er en stat direkte involvert i cyberoperasjonen, og i så fall i hvilken grad?

Schmitt-kriteriene er ikke uttømmende, og andre vurderinger kan spille en rolle når en stat blir utsatt for et cyberangrep. Politisk spenning, uttalte trusler eller en stats aggressive historie innen cyber kan avgjøre hvordan den angrepne stat karakteriserer en cyberoperasjon mot dem.

Oppsummering

Cyberoperasjoner kan være ulovlig bruk av makt. Ulovlig bruk av makt rettferdiggjør ikke bruk av makt i selvforsvar. Jeg har tidligere nevnt gråsonen mellom ulovlig bruk av makt og væpnet angrep. Dette er to forskjellige normative standarder, som fører til forskjellige lovmessige reaksjoner. Bruk av makt som vil være et alvorlig brudd på maktforbudet, men som likevel ikke kan karakteriseres som et væpnet angrep, må

[99] The Case of the SS-Lotus, I.C.J. Collections of Judgements, Series A.-No.10 7 September 1927 (Heretter "SS-Lotus") s.19

håndteres med andre mottiltak. ILC Articles on State Responibility kan gi føringer for hva som ansees som lovlige mottiltak.[100]

3.3 Kan cyberangrep være væpnede angrep?

Hvordan avgjør man om en cyberoperasjon er et væpnet angrep som kan legitimere den angrepne stats bruk av væpnet makt i selvforsvar etter FN-paktens artikkel 51?

I "Nicaragua" anerkjente ICJ den omtalte gråsonen i graden av maktbruk da de uttalte at det finnes "*measures which do not constitute an armed attack, but may nevertheless involve a use of force*" [101] og skilte mellom "*the most grave forms of the use of force (those constituting an armed attack) from other less grave forms*"[102]
Følgene er at alle væpnede angrep er bruk av makt, men ikke all bruk av makt er væpnede angrep. Konsekvensen er at stater kan bli utsatt for cyberoperasjoner som utvilsomt er bruk av makt, men som de ikke har noen andre muligheter til å svare på enn diplomati, protester eller økonomiske sanksjoner etter ILC Articles on State Responsibility forholdene tatt i betraktning.[103]

For å avgjøre hvorvidt en aggressiv handling, i dette tilfellet et cyberangrep, er et væpnet angrep, bør man analysere seg opp gjennom konfliktskalaen og plassere angrepet etter hvilken grad av bruk av makt det referer til.

Analysens utgangspunkt må da være konsekvensene bruken av makt har medført, sammen med kriteriene omfang, varighet og intensitet. Dette vil være i tråd med ICJs uttalelser fra "Nicaragua" om "scale and effect", som ble fulgt opp i "Oil Platforms".

Til nå har jeg vist analyseverktøy for å detektere ulovlig bruk av makt med cyberoperasjoner. Videre vil jeg forsøke å nyansere bildet noe, og prøve å plassere hvor terskelen ligger for når ulovlig bruk av makt ved et cyberangrep kan kvalifisere som et væpnet angrep.

---

[100] Tallinn manualen, s.41
[101] "Nicaragua" premiss 210
[102] "Nicaragua" premiss 191
[103] Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context*, s.287

Eksempler på cyberangrep som vil kunne karakteriseres som væpnede angrep er angrep som medfører død ved stans av sykehus sine livreddende instrumenter, stans av store strømnettverk som medfører store skader, avstengning av datanettverk som kontrollerer demninger slik at det medfører flom i bebygde områder, flystyrt som følge av feilinformasjon plottet inn i fly-computere og inntrengning i datasystemer som styrer atomkraftanlegg som fører til nedsmelting og utslipp av store mengder radioaktivt materiale som lekker ut i bebodde områder.[104]
På den andre side, diverse forstyrrelser, benektelser av tjenester uten skader eller tap av menneskeliv vil sannsynligvis ikke ansees som et væpnet angrep, selv om det er kan være klart at det er bruk av makt.[105] "The International Group of Experts" inntok også denne holdningen i Tallinn-manualen.[106] Såfremt bruken av makt medfører skader eller tap av menneskeliv, eller skader eller ødelegger eiendom, vil det være et væpnet angrep. Cyberetterretning, "cybertyverier" og cyberoperasjoner som forårsaker kortere forstyrrelser kvalifiserer trolig ikke som et væpnet angrep.

Er det avgjørende hva som blir angrepet?

Det kan videre spørres om det bør skilles mellom kritisk infrastruktur, eller hvilken som helst sivil infrastruktur.
Dinstein skiller ikke mellom militære eller sivile installasjoner.[107] Han hevder at cyberangrep rettet mot sivile installasjoners datanettverk som ikke har noen sammenfatning med det militære, som får destruktive konsekvenser, faller inn under det som kan anes som et væpnet angrep.
ICJ har i "Oil Platforms" inntatt en holdning at et angrep på en enkel militær installasjon uansett vil være å karakterisere som et væpnet angrep.[108] Schmitt hevder dette er tilfelle, men det vil også igjen avhenge av konsekvensene.[109]
Cyberoperasjoner som rettes mot militære installasjoner som hindrer militære styrker i å utføre militære operasjoner alene vil nok derfor ikke kunne være nok. Dersom et

---

[104] Yoram Dinsteins eksempler fra Yoram Dinstein, *Computer Network Attack and International Law,* Schmitt/O'Donnell 2011, fra Roscini, s.115
[105] Yoram Dinsteins eksempler, brukt i Roscini, s.116
[106] Tallinn manualen, s.55
[107] Yoram Dinstein i Roscini, s.115
[108] "Oil Platforms" premiss 72 om mineleggingen av US Navy skipet "USS Samuel B. Roberts"
[109] Schmitt*, Cyber operations and the Jus ad Bellum revisited*, s.589

ikke destruktivt cyberangrep rettes mot forsvarsinstallasjoner, og man anser dette som forberedelser på ødeleggende operasjoner, kan dette eventuelt kvalifisere til å benytte væpnet makt i preventivt selvforsvar. Eksempelvis hvis stat A slår ut stat Bs radarvarslingssystem og på den måten hindrer stat B i å overvåke sitt eget luftrom, samtidig som stat A klargjør fly for angrep.
I et forsøk på å forenkle folkeretten og å tilpasse den til cyberoperasjoner, har enkelte forfattere tatt til orde for at bruk av væpnet makt i selvforsvar skal være lovlig dersom kritisk infrastruktur er angrepet, uten å først identifisere angriperen eller analysere angrepet videre.[110]

FNs Generalforsamling har i sin resolusjon om cybersikkerhet overlatt til den enkelte stat å definere selv hva som er deres kritiske informasjonsinfrastruktur, "*The General Essembley(...) Recognizing that each country will determine its own critical information infrastructures*"[111] Å overlate definisjonen til hver enkelt stat vil på en side være gunstig, da hver enkelt stat på grunn av sin demografiske og geografiske utforming har egne preferanser. På den annen side kan det medføre en for stor grad av statlig subjektiv vurdering når et cyberangrep rettes mot såkalt kritisk informasjonsinfrastruktur. Spesielt hvis det er slik at alle angrep på militære installasjoner skal tolkes som et væpnet angrep, vil staten ha lavere terskel for å definere et angrep mot kritisk informasjonsinfrastruktur som et væpnet angrep. Det er slik i mange land at sivile firmaer leverer tjenester til det militære. Det er naturlig å anta at en stat vil se mer alvorlig på et cyberangrep mot kritisk informasjonsinfrastruktur enn mot det som ikke regnes som kritisk. Terskelen vil kunne senkes for hva som skal ansees som et væpnet angrep og følgen kan være at konsekvensvurderingen spiller mindre rolle ved angrep på det som defineres som kritisk og det som ikke gjør det. Det kan ikke sies å være en heldig utvikling.

Konsekvensvurdering

Det avgjørende må fortsatt være angrepenes "scale and effect", uavhengig om angrepet rettes mot det staten definerer selv som kritisk informasjonsinfrastruktur. At

[110] Eric T. Jensen, *Computer Attacks on Critical Infrastructure in Cyberspace*, Stanford Journal of Law 38 2002, s.234-235 fra Roscini, s.119
[111] FNs Generalforsamlings Resolusjon 58/199, 30 Januar 2004

det blir et moment i vurderingen kommer man ikke utenom, spesielt der konsekvensene ikke viser seg eller er vanskelige å konkretisere.
Mest problematisk er det med cyberangrep som ikke resulterer i skade, død eller ødeleggelse, men som ellers har negative konsekvenser. Kan slike angrep nå terskelen for væpnet angrep?

I Tallinn-manualen er "The International Group of Experts" delt i spørsmålet om hvordan konsekvensene skal vurderes. Det hevdes på den ene siden at kun de fysiske direkte konsekvensene av angrepet skal avgjøre hvorvidt et væpnet angrep er blitt foretatt. På den annen side stilles det spørsmål om hvordan de etterfølgende effektene av skal vurderes?[112] Et eksempel er cyberangrep som retter seg mot en stats børsmarked, som ved full stans eller overstyring av markedet utenfra kan føre til total kollaps av finansmarkedet. Slike handlinger kan få katastrofale konsekvenser, og kan koste staten enorme summer å rette opp.
Et annet eksempel, vil være å sette all togtransport i en stat ut av spill ved å kutte jernbanens datanettverk. Angriper vil oppnå nøyaktig det samme, eller mer, ved et slikt angrep som å sprenge en jernbanebro ved hjelp av en rakett. Rakettangrepet ville mest sannsynlig bli klassifisert som et væpnet angrep, det første mer tvilsomt. Betyr det at cyberangrep med ikke-fysiske konsekvenser aldri vil kunne nå terskelen for et væpnet angrep?
Dette er vanskelig å svare på i en abstrakt setting, derfor vil jeg prøve å belyse problemene gjennom de konkrete cyberangrepene på Estland i 2007 i del 4.

Oppsummering
Cyberangrep som har konsekvenser som medfører død, skade eller ødeleggelse kan kvalifisere som et væpnet angrep, uavhengig av hva som blir angrepet. Det må likevel antas at cyberangrep mot kritisk informasjonsinfrastruktur vil ha en større sjanse for å bli vurdert av den angrepne part som væpnet angrep.
Cyberangrep med andre eller ingen fysiske konsekvenser krever en grundigere analyse.

[112] Tallinn manualen s.55

3.4 Hvordan kan en stat bli ansvarlig for cyberangrep fra sitt territorium?

Det er i utgangspunktet kun stater i form av å være rettssubjekter som kan bli ansvarlige for brudd på FN-pakten.

Det er enkelt å forholde seg anonym i cyberspace.[113] Det krever heller ikke mye kunnskap, finansiering eller avansert utstyr for å utføre et cyberangrep og få det til å se ut som en cyberoperasjon har sitt utspring fra et annet sted, eller en annen stat, enn det som er tilfellet. I utgangspunktet kan alle enkeltpersoner som, i tillegg til datamaskin, programvare og internett, har viljen, utøve bruk av makt som et væpnet angrep.[114]

På hvilken må hefter staten for cyberangrep fra sitt territorium?

Det rettslige grunnlaget for vurderingen er de sedvanerettslige folkerettslige ansvarsreglene som fremkommer av ILC Law on State Responsibility.

Staten er ansvarlig for sine organer, dette følger av ILC Law on State Responsibility artikkel 4. Et statlig organ omfatter etter artikkelens andre ledd enhver person eller enhet som ved lov kan knyttes til staten. Dette vil omfatte enhver fysisk eller juridisk person, herunder et enkeltkontor, avdeling, departement eller andre som utøver offentlig myndighet.[115] Personell i tjeneste for en stat som har utviklet militære cyberkapasiteter, vil være et statlig organ. Kina har innrømmet at de har cyberbataljoner og regimenter i China's People's Liberation Army.[116] [117] I Norge har vi det relativt nyopprettede Cyberforsvaret. USA har sin United States Cyber Command opprettet i 2009.

Cyberangrep fra slike organ medfører utvilsomt statsansvar.

Cyberangrep kan også iverksettes av grupperinger, som *de jure* ikke tilhører noe statlig organ, men som leies inn og handler på oppdrag eller ordre fra et statsorgan. Et

[113] Nasjonal sikkerhetsmyndighet, s.18
[114] Roscini, s.97
[115] ILC Articles on State Responibility with commentaries, 2001, s.42 art 4 http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf (pr.13.12.12)
[116] http://www.channel4.com/news/china-admits-cyber-warfare-unit (pr.08.12.12)
[117] Roscini, s.98

eksempel på slikt er Russian Business Network[118] som sies å stå bak cyberangrepene i forkant av Russlands invasjon av Georgia i 2008.[119]

Når kan en stat bli ansvarlig for cyberangrep fra slike grupperinger?

Av ILC Articles on State Responsibility artikkel 8 fremgår det at handlingene til en person eller gruppe som handler på vegne av en stat, medfører at denne stat er ansvarlig for disse handlingene. Graden av statens kontroll over grupperingen må vurderes, da det kan være grupper eller enkeltpersoner som har handlet utenfor sitt mandat. Graden av tilknytning en gruppe må ha til en stat for å være ansvarlig ble vurdert i "Nicaragua". Opprørsgruppen "Contras" hadde brutt folkeretten, og spørsmålet var om USA kunne holdes ansvarlig for det på grunnlag av sin *"planning, direction and support"* til "Contras".[120] ICJ kom til at dette ikke var nok til å bli ansvarlig for "Contras" handlinger. ICJ uttalte så at det som må bevises er om *"that State had effective control of the military or paramilitary operation in the course of which the alleged violations were committed"*[121]. ICJ nyanserer dette i "Genocide"[122] hvor staten Serbia frikjennes for Srebrenica massakren, *"the rules for attributing alleged internationally wrongful conduct to a State do not vary with the nature of the wrongful acts in question in the absence of a clearly expressed lex specialis"*[123] Dette kan også kalles "effektiv kontroll testen" eller "Nicaragua-testen". Har en stat effektiv kontroll over en gruppering blir den ansvarlig for grupperingens handlinger.

I "Tadic" saken,[124] uttalte "The International Criminal Tribunal for the former Yugoslavia" (ICTY) at "*the degree of control may, however, vary according to the factual circumstances of each case*"[125] ICTY har her konstruert en annen test for å

[118] http://en.wikipedia.org/wiki/Russian_Business_Network (pr.08.12.12)
[119] Cooperative Cyber Defence Center of Excellence (CCDCOE), *Cyber Attacks Against Georgia: Legal Lesson Identified,* November 2008 s.11 http://www.carlisle.army.mil/DIME/documents/Georgia 1 0.pdf (pr.13.12.12)
[120] "Nicaragua" premiss 86
[121] "Nicaragua" premiss 115
[122] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43 (Heretter "Genocide")
[123] "Genocide" premiss 401
[124] ICTY Case IT-94-1-A15 July 1999 *Prosecutor vs Tadic* (Heretter "Tadic ")
[125] "Tadic" premiss 117

ansvarliggjøre en stat, som beror på det at det er nok at staten har hatt en rolle i å organisere, koordinere eller hjelpe til å planlegge en operasjon. "Tadic-testen" eller "overall controll test" er kritisert blant annet av ICJ i "Genocide"[126] hvor de sier at "overall controll", eller overordnet kontroll, utvider statens ansvar langt utover de folkerettslige ansvarsreglenes rekkevidde.

Enkelte[127] tar til orde for å bruke "Tadics" overordnet kontroll ved et cyberangrep. [128] De mener ICJ har vært for restriktive i Nicaraguasaken. Bruker man "Nicaraguas" effektiv kontroll tilnærming, vil det bli altfor lett for en stat å skjule sine cyberoperasjoner og en stat som blir utsatt for et verst tenkelig scenario kan ende opp med å måtte stå og se på det som skjer. "Nicaragua" definerer muligens i for stor grad et fast punkt når en stat blir ansvarlig. Det bør kanskje være nok å bevise en stats overordnede kontroll i cyberspace, enn å måtte bevise statlig effektiv kontroll.

Andre hevder at Nicaragua tilnærmingen må benyttes, nettopp fordi det vil hindre at stater blir altfor lett beskyldt for å stå bak cyberangrep.[129] Spesielt viktig vil dette poenget være dersom det medfører en senket terskel med tanke på å påberope seg selvforsvarsrett.

Tilnærmingen fra "Tadic" retter seg i utgangspunktet mot *"organised and hierarchially structured*" [130] grupper som militære eller paramilitære, væpnede grupper med opprørere eller bander.

Om det eksisterer hierarkisk organiserte rene cyberopprørsgrupper er høyst diskutabelt, og ikke minst svært vanskelig å bevise. Grupper som for eksempel "Anonymous" vil nok ikke kvalifisere. Overfor ikke-organiserte grupper tar ICTY i "Tadic" til ordet for en effektiv kontroll test slik som i "Nicaragua". "*In such a case, it would be necessary to show that the State issued specific instructions concerning the commission of the breach in order to prove(…) that the individual acted as a de facto State agent*."[131]

---

[126] "Genocide" premiss 406
[127] Scott Shackelford, Doctor Juris kandidat fra Stanford Law School.
[128] Scott Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law nr. 27:1 2008 s.234
[129] Roscini, s.100
[130] "Tadic" premiss 120
[131] "Tadic" premiss 118

Konklusjonen må bli at en stat kan bli holdt ansvarlig for et cyberangrep fra en hierarkisk organisert gruppe, såfremt staten har en form for rolle, en overordnet kontroll ved organiseringen, finansieringen eller planleggingen til denne gruppen. Staten kan bli holdt ansvarlig for et cyberangrep fra enhver gruppe dersom staten har en effektiv kontroll ved finansiering, tilrettelegging, planlegging og støtte til gruppens handlinger.

I enkelte tilfeller handler grupper eller enkeltpersoner fullstendig på eget initiativ. Kanskje som følge av politisk motivasjon og sympati for sin egen stat. Dette medfører to mulige scenarioer. Enten påtar staten seg ansvar, eller så gjør den ikke det. I utgangspunktet er ikke staten ansvarlig for disse handlingene.
Etter ILC artikkel 11 heter det at handlinger som ikke kan knyttes til staten, likevel skal vurderes som statens ansvar dersom staten erkjenner og vedtar handlingene som sin egen.[132] I saken "Hostages"[133] kom ICJ i utgangspunktet til at den Iranske stat ikke kunne ansvarliggjøres for handlingene utført av en gruppe islamistiske studenter og paramilitære da de tok amerikanske ambassadefolk som gisler under "den Iranske Revolusjon". Den etterfølgende støtten til gisseltakerne fra Ayatollah Khomeini og iranske myndigheter førte derimot til at aksjonen kunne knyttes til den iranske stat. Staten blir ikke ansvarlig for handlingene kun ved å erkjenne de faktiske forhold og utrykke sympati, men må gi sin godkjenning, anerkjennelse og identifisere staten med bruken av makt.
Staten kan bli ansvarlig for enkeltpersoner eller grupper når den påtar seg tilstrekkelig grad av ansvar. Dette gjelder da også for cyberoperasjoner som en internasjonal rettstridig handling.

Hva er tilfellet dersom staten ikke påtar seg ansvar, eller kun utrykker sympati med de internasjonale rettstridige handlingene?
Det følger av praksis fra ICJ bl.a. i "Corfu Channel"[134] at stater har ansvar for å iverksette nødvendige tiltak for å stoppe rettstridige handlinger med utspring fra sitt territorium. Det er en stats ansvar; *"not to allow knowingly its territory to be used for*

[132] ILC Articles on State Responsibility artikkel 11
[133] United States Diplomatic and Consular Staff in Tehran, Judgment, I.C.J. Reports 1980, p. 3. (Heretter "Hostages")
[134] Corfu Channel case, Judgment of April 9th, 1949 I.C.J. Reports 1949,P. 4. (Heretter "Corfu Channel")

acts contrary to the rights of other States".[135] Dette var også tilfellet da USA holdt Taliban-regimet i Afghanistan ansvarlig for Al-Qaidas terroraksjoner i 2001.
Hvis en stat nekter å alene, eller i samarbeid med den fornærmede stat, iverksette tiltak som setter en stopper for et cyberangrep som er en rettstridig handlinger foretatt av enkeltpersoner eller grupper på sitt territorium, kan staten bli ansvarlig for cyberangrepet.

I hvilken grad kan man forvente en stats fullstendige kontroll over enkeltpersoner i sine domener? En ting er å holde rede på de håndfaste størrelsene, verre er det med de abstrakte, som cyberdomenet. I det åpne og verdensomspennende cyberspace kan instrumentene distribueres grenseoverskridende fra en person til mange tusen i løpet av sekunder. Dette kan ikke på noen måte sammenliknes med produsering og smugling av komponenter til for eksempel å bygge interkontinentale missiler, selv om konsekvensene av bruken kan være de samme. Tilgangen på instrumentene, både programvare og datamaskiner, er av en slik art at det for en stat er tilnærmet umulig å føre full kontroll over sitt cyberdomene.
Det største problemet er imidlertid å fremskaffe bevis for at de rettstridige handlingene stammer fra den staten, eller det stedet de er sporet til. Muligheten til å forfalske IP-adresser, og å ta over datamaskiner rundt om i verden, gjør at sporingen i svært liten grad er til å stole på. For eksempel ble angrepene på Estland sporet til 178 ulike land.
Videre vil det, i den grad det er mulig å positivt identifisere de rettstridige cyberoperasjonenes utgangspunkt, være et spørsmål om staten har evne til å raskt og effektivt stanse handlingene fra sitt territorium uten å benytte u-proporsjonale virkemidler. Cyberoperasjonene kan komme fra datamaskiner spredt over en hel stat. Å kutte for eksempel nettforbindelsen i hele staten, vil kunne medføre enorme konsekvenser.

Håndfaste bevis for en cyberoperasjons opprinnelse er nærmest umulig å fremskaffe. Fullstendig kontroll over sitt eget cyberdomene er det urealistisk å forvente av en stat. Læren om statlig ansvar for enkeltpersoner, er svært vanskelig å overføre til internasjonale rettstridige handlinger som følger av cyberoperasjoner. Slik

[135] "Corfu Channel" s.22

rettstilstanden er i dag, må det vurderes fra gang til gang. Denne problematikken berøres videre i kapittel 4 og 5.

3.3.3 Selvforsvar mot et cyberangrep

Selvforsvar må utføres i etter prinsippene om nødvendighet, proporsjonalitet og umiddelbarhet uavhengig om det skyldes cyberoperasjoner eller kinetiske operasjoner.
Cyberangrep kan besvares med kinetiske våpen, og kinetiske angrep kan besvares med cyberangrep. Offer for et cyberangrep har, som ved konvensjonelle angrep, ikke carte blanche til å drive aktivt cyberforsvar, dvs. cyberangrep i forsvarsøyemed, ei heller kinetiske angrep med samme hensikt. Bruken av væpnet makt i selvforsvar må begrenses til det som er nok for å stanse, lamme eller ødelegge kilden til angrepene, uavhengig av instrumentene.

4. Cyberangrepet mot Estland

4.1 Hva skjedde i april og mai 2007

4.1.1 Den utløsende årsak

Monumentet "Bronsesoldaten" er et viktig russisk minnesmerke som symboliserer seieren over Nazi-Tyskland. Men monumentet markerer også det Russland mener er russiske rettigheter i Estland. For estlendere er statuen et symbol på historisk undertrykkelse og okkupasjon.

27. april 2007 besluttet estiske myndigheter å flytte monumentet ut av Tallinn sentrum og 30. april var det gjenreist på en krigskirkegård i utkanten av byen. Flyttingen var egentlig planlagt den 9. mai, på den "Russiske Seiersdagen"[136], men pga. frykten for uroligheter ble flyttingen fremskyndet. I Tallinn medførte dette store protester fra etniske russere i Estland, med voldelige opptøyer i gatene. I Moskva medførte flyttingen stor oppstandelse ledet an av den anti-fascistiske ungdomsgruppen "Nashi". Protestene endte i en blokade av den estiske ambassaden i

[136] Russland feirer seieren over Nazi-Tyskland.

Moskva som varte til 3. mai. Ambassadeopptøyene døde ut etter press fra vestlige styresmakter. Cyberoperasjonene derimot var i en eskalerende fase.

4.1.2 Estland og datanettverk

Estland har siden 2001 vært et av de mest avanserte nettverksbaserte landet i Europa. Mer enn 355 myndighetsorgan, som politi, regjering, skatteetat og banker, er koblet sammen gjennom e-infrastruktursystemet X-Road.[137] Systemet er meget godt beskyttet og er som en virtuell verden å regne, og kan beskrives som hjernen i Estlands cyberdomene. Estland var det første landet i verden som innførte internettvalg i lokalvalg. Alle innbyggere i Estland har ID-kort som gjør at de kan kontakte myndighetene eller bankene online. Gratis trådløst internett er like selvsagt som innlagt vann.

4.1.3 Tidslinje

De første angrepene 27. – 30. april.

De første cyberangrepene inneholdt tjenestenektangrep (DoS)[138] mot Estlands statlige og private internettleverandører, og flere myndighetsorganisasjoners nettsider. Det ble sendt ut oppskrifter på russiske nettforum og blogger om hvordan man utfører Ping-angrep.[139] [140]

Cyberangrep av denne typen medfører at nettverkstjenester og ressurser gjøres utilgjengelige for brukeren ved at systemene overarbeides og slutter å fungere. Parlamentets, presidenten og statsministerens nettsider var hovedmålet, flere nyhetsstasjoner ble angrepet.

Angrepene de første dagene var simple i sin form, ukoordinerte og ble forholdsvis enkelt avverget.

---

[137] http://e-estonia.com/components/x-road (pr.13.12.12)
[138] Denial of Service
[139] Kommandoer for å overvåke tilgangen og kapasiteten til datanettverk.
[140] Cooperative Cyber Defence Centre of Excellence, *International Cyber Incidents,* Tallinn, Estland 2010 s.18

Den andre fasen startet 30. april.
Det ble sendt millioner av eposter til Estlands parlamentsrepresentanter med teksten "Gratulations of the Victory Day". Dette medførte feil på mailservere, som resulterte i at regjering og andre myndighetsinstitusjoner var uten kommunikasjonsmuligheter i flere dager. Større avisers nettsider ble også angrepet og stengt utenfra. Angrepene var mer sofistikerte, mer koordinerte og av vesentlig større omfang enn i første fase. Angrepene inneholdt nå såkalte distribuerte tjenestenektangrep, DDOS[141]-angrep, via "bot-maskiner"[142].
Den estiske utenriksministeren gikk ut 2. mai med beskyldninger om at angrepene kom fra Russland.[143]

Den tredje fasen startet i perioden rundt "Den Russiske Seiersdagen" 9. mai.
Under denne bølgen ble store deler av Estlands internettsider, alt fra regjering, president, statsminister, banker, politiske partier, større nyhetsorgan, statlige og private internettleverandører og telefonselskap ble angrepet med DDoS-angrep via "bot-maskiner". Dette medførte at disse sidene og tjenestene disse organisasjonene og institusjonene leverer ble lammet. Bare et av angrepene på Estlands største bank medførte ikke ubetydelige økonomiske tap. Nyhetsstasjonene ble hindret i å opplyse verden om hva som foregikk. Det ble også sendt en enorm datautsending for å måle hele landets nettverkskapasitet, med påfølgende masseutsending av data som raskt nådde nettverkets absolutte tålegrense.

Estland var svært nær en total digital kollaps den 10. mai[144], noe som kunne ført til at kritiske livsviktige tjenester ble hindret, som igjen kunne ført til død, skader og vesentlig større store sosiale og økonomiske avvik, forstyrrelser og ødeleggelser.

Det siste store angrepet skjedde rundt 15. mai og var et massivt DDoS-angrep utført av et bot-nettverk med 85 000 "zombie-computere" mot Computer Emergency Response Team Estonia.[145]

---

[141] Distributed Denial of Service – distribuert tjenestenekt
[142] En bot er en infisert datamaskin som automatisk utfører gjentatte operasjoner på ordre fra en "hacker". Dette er maskiner som ikke vil oppdage at de er "okkupert" og kan stå hvor som helst i verden. Også omtalt som "zombie".
[143] http://news.bbc.co.uk/2/hi/europe/6614273.stm (pr.12.12.12)
[144] Shackelford, s.205

18 mai sluttet de siste større DDoS-angrepene, men angrep av mindre sofistikert art fortsatte i ukevis.

4.2 Klassifisering av angrepet

Analysen av cyberangrepet på Estland vil bli utført ved hjelp av tidligere beskrevet teori og analyseverktøy. Jeg vil starte nederst på konfliktskalaen fra intervensjon via bruk av makt etter FN-paktens artikkel 2(4), før jeg vil forsøke å finne ut om angrepet kunne vært klassifisert som væpnet angrep etter FN-paktens artikkel 51. Om det kan knyttes statsansvar til cyberangrepet vil bli drøftet helt til slutt da det ikke er relevant for selve klassifiseringen av angrepet isolert.

4.2.1 Var cyberangrepet en ulovlig intervensjon?

Flyttingen av "Bronsesoldaten" var en avgjørelse tatt av estiske myndigheter. Bakgrunnen var vedtakelsen av en lov om beskyttelse og ivaretakelse av krigsgraver.[146] Målet var å gi de som døde for sitt land en respektabel gravplass i henhold til Genève-konvensjonens regler om ivaretakelse av krigsgraver.[147] I forbindelse med vedtakelse av loven, utalte Estlands statsminister Andrus Ansip i en pressemelding, at han håpet loven ble vedtatt og at "Bronsesoldaten" og de begravet under den, hvis det i det hele tatt var noen, kunne bli flyttet til et mer passende hvilested for de døde.[148]

Vedtakelsen av War Graves Protection Act var et estisk internt politisk forhold. Vedrørende ivaretakelse av krigsgraver følger det av Genèvekonvensjonen TP1 artikkel 34 at det påligger staten krigsgraven befinner seg i å sørge for vedlikehold,

---

[145] Heretter CERT-EE

[146] Sõjahaudade kaitse seadus ,vastu võetud 10.01.2007 - War Graves Protection Act, Adopted on 10.01.2007 (min oversettelse) https://www.riigiteataja.ee/akt/12777064 (pr.29.11.12)

[147] Genèvekonvensjonens Tilleggsprotokoll 1 artikkel 34 (2a) Heretter Genèvekonvensjonen TP1 *"(...)"to facilitate access to the gravesites by relatives of the deceased and by representatives of official graves registration services and to regulate the practical arrangements for such access;"*

[148] Andrus Ansip, *Sitting review from the Riigikogu Press Service*, 06.11.2006 http://www.riigikogu.ee/index.php?id=41372 (pr.01.12.12)

beskyttelse og tilrettelegge for adkomst. Dette er vedtatt og ratifisert av både Estland og Russland, og forplikter følgelig begge stater.
Det fremgår av grunnleggende folkerett, med utspring fra suverenitetsprinsippet, at det er ulovlig å direkte eller indirekte intervenere i en stats interne anliggender. Dette følger også av FNs Generalforsamlings resolusjon 2625 artikkel 3.[149]
Både Estland og Russland er medlemmer av FN.

Fra FNs Generalforsamlings Resolusjon 36/103 innebærer forbudet mot intervensjon også å intervenere i en stats frie tilgang til informasjon og spredning av informasjon gjennom sine egne massemedia.

Russiske myndigheters protester mot estiske myndigheters avgjørelse var av en karakter som går lenger enn en fordømmelse av estisk politikk.
Den Russiske Føderasjonens råd hevdet 27. april at flyttingen av monumentet 9.mai bare er et aspekt av politikken, som er katastrofal for estlendere, som utføres av provinsielle fanatikere og nazisme.[150]
Fra offisielt hold i Russland kom uttalelser som; "*These admirers of Nazism forget that politicians come and go, while the peoples in neighboring countries are neighbors for eternity. The dismantling of the monument and the mockery of the remains of the fallen soldiers is just more evidence of the vengeful policy toward Russians living in Estonia and toward Russia*". [151] Hvor de samtidig oppfordret myndighetene til å iverksette "*toughest possible measures*"[152] mot Estland.
Ambassadeblokaden endte ikke før Estlands ambassadør forlot Russland som en del av en avtale mellom Estland og Russland fremforhandlet av Tyskland, samt internasjonalt press om å overholde Wien-konvensjonen om diplomatiske relasjoner.[153] [154]

---

[149] FNs Generalforsamling, Decleration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, 1970.
[150] http://en.wikipedia.org/wiki/Aftermath_of_the_Bronze_Night - cite_note-5 (pr.12.12.12)
[151] Uttalelser godkjent av den Russiske Føderasjonens Råd 27. april. http://en.wikipedia.org/wiki/Aftermath_of_the_Bronze_Night - cite_note-5 (pr.01.12.12)
[152] *Ibid*
[153] Vienna Convention on Diplomatic Relations April 18 1961

Det var ingen russiske myndigheter som tok offisielt avstand og fordømte hendelsene i Tallinn og Moskva.

Cyberangrepene var i sin retorikk av samme karakter. På åpne internettforum kunne man lese oppfordringer og uttalelser fra "kjente hackere" som omhandlet flyttingen av "Bronsesoldaten" og retorikk rundt den russiske seiersdagen.
"*You do not agree with the policy of eSStonia???. You may think you have no influence on the situation??? You CAN have on the internet*"[155]
Det ble også etter hvert lagt ut programvare på russiske "hackersider" for å kunne utføre operasjonene.[156] Innholdet i e-post til estiske folkevalgte, samt meldinger på hackede nettsider tyder på at angriperne sympatiserte med Russland.

Fra Resolusjon 36/103 Annex II F) følger et forbud mot å fremme, oppfordre eller støtte, direkte og indirekte, opprørsk adferd i eller mot en stat i den hensikt å undergrave den politiske orden.
Russland har benektet å ha noe med cyberangrepene å gjøre. Noe som er vanskelig å motbevise. Det er imidlertid liten tvil om at cyberangrepene var en følge av estisk politisk vedtak, aggressiv russisk politisk retorikk og indirekte støtte til de som måtte ønske å utføre sanksjoner mot Estland. Fra Resolusjon 36/103 Annex II J) følger også et forbud mot ærekrenkende og fiendtlig propaganda i den hensikt å intervenere i en annen stats politikk. Den russiske stats reaksjoner mot den estiske politikken kan derfor muligens kvalifisere som ulovlig intervensjon uten å ta i betrakting cyberangrepene. Såfremt det er mulig å beviselig knytte den russiske stat til cyberangrepene, vil handlingene fra russisk hold kvalifisere som ulovlig intervensjon.

Det er vanskelig å forme en konklusjon før det er tatt standpunkt til spørsmålet om statsansvar. En endelig konklusjon vil derfor komme etter punkt 4.2.4.

---

[154] Senate of the United States, Resolution S.RES 187 May 3 2007 http://www.gpo.gov/fdsys/pkg/BILLS-110sres187ats/pdf/BILLS-110sres187ats.pdf(pr.13.12.12)
[155] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.12.12.12)
[156] Cooperative Cyber Defence Centre of Excellence, *International Cyber Incidents,* Tallinn, Estland 2010 s.23

4.2.2 Var cyberangrepet bruk av makt?

Hendelsene rundt ambassaden i Moskva er alvorlige og må sees i sammenheng med cyberoperasjonene som startet i samme tidsrom og som fortsatte å eskalere utover i mai. De fysiske handlingene i seg selv blir ikke behandlet individuelt videre, men vil kunne bli tatt i betraktning i tilknytning til drøftelsen.

Nærmere presisering av angrepets innhold

Cyberoperasjonene mot Estland var mange, de er sporet til flere land og de kom i forskjellige former. Konsekvensene av angrepet var så mange at det kun vil være hensiktsmessig å behandle de som er relevante for drøftelsen. Angrepet vil bli vurdert opp mot Schmitt-kriteriene.

Angrepets varighet er presentert i tidslinjen over. I det følgende kommer en videre presisering, som gir et litt mer detaljert blide av også omfang og intensitet. Presiseringen er ikke uttømmende.

I perioden 3. til 11. mai ble politi, statsminister og regjeringens nettsider utsatt for 35 unike tjenestenektangrep hver. Det samme ble Gateway to Estonia.[157] Parlamentet ble angrepet 7 ganger.[158] Statsministerens sider ble etter hvert "ofret" slik at angriperne skulle kaste bort tid på disse, da disse sidene ble kategorisert med lav prioritet.[159] Hansabank og Skandinaviske Enskilda Banken (SEB) ble angrepet 9.-10.mai og 15.mai. Disse bankene står for 75% av Estlands nettbank transaksjoner, i et land hvor 90% av innbyggerne bruker nettbank.[160] Hansabank klarte å være online for sine største utenlandske kunder, men var nede ca. 2 timer ved to anledninger. SEB var nede i 2 timer 15.mai.

Disse bankene ble angrepet gjentatte ganger utover i mai. Til tross for at de stort sett holdt seg online, fikk de vesentlige økonomiske tap. Estlands største aviser som

[157] En nettside for som kan sammenlignes med den norske "Altinn", men som tilbyr flere offentlige tjenester.

[158] http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (pr.12.12.12)

[159] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.13.12.12)

[160] http://wikileaks.org/cable/2007/06/07TALLINN366.html (pr.13.12.12)

Postimees og Eesti Paevaleht samt flere nettaviser, som besøkes daglig av ca. to tredjedeler av befolkningen, ble angrepet og gjort utilgjengelig 3. mai.[161]
Flere telefonselskaper opplevde noe forstyrrelser, men ingen alvorlige. Nødnummeret ble angrepet, men ble ikke blokkert for mer enn svært kort tid.

I perioden 3. til 11. mai ble det målt 128 unike DDoS-angrep. De 10 største angrepene sendte 90 megabyte med data hvert sekund til Estlands nettverk. Dette tilsvarer å laste ned hele Windows-operativsystemet hvert sjette sekund i 10 timer.[162]

Angrepene på Estland har blitt kalt "Web War I" og er det første av sitt slag cyberangrep. Det har vært utført store cyberoperasjoner tidligere, men aldri før har et helt land blitt angrepet i hele sitt cyberdomene samtidig, og aldri før har det vært behov for et like aktivt cyberforsvar.

Spørsmålet er altså om cyberangrepet mot Estland kan kategoriseres som bruk av makt?

Alvorlighetsgrad
Cyberangrepet påførte ingen menneskelige tap eller skader. Angrepet forårsaket ingen fysiske skader på infrastruktur eller andre objekter.
Angrepet forårsaket økonomisk tap som følge av manglende adkomst til nettverk for de største bankene, samt økonomiske utgifter i form av hurtig oppgradering av cyberforsvarskapasiteter.
Angrepet forårsaket forstyrrelser og sannsynligvis økonomisk tap hos små og mellomstore bedrifter som er avhengige av nettverksbasert kommunikasjon og handel.[163] Cyberangrepet hadde en merkbar effekt på landets økonomi.

Cyberangrepet hadde en samfunnsmessig effekt. Som et land som er vant til en ren nettverksbasert kommunikasjonsform med alle offentlige tjenester, var det umulig eller utfordrende å få utført selv de enkleste tjenester. Verst var det at det var umulig å

[161] *Ibid*
[162] http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ (pr.13.12.12)
[163] CCDCOE, *International Cyber Incidents*, s.24

få levert myndighetspålagte rapporter, regnskap eller heve innvilget støtte eller subsidier.
Videre var landets media avskåret fra å levere nyheter om hendelsen internt og til omverden. De samfunnsmessige følgene er vanskelig å måle, men det fikk til en viss grad sosiale konsekvenser for estlendere generelt.

Konsekvensenes omfang og varighet tyder på at dette var en hendelse av en viss alvorlighetsgrad. For å vurdere alvorlighetsgraden, bør imidlertid også mulige følger vurderes.
Omfanget, størrelsen og varigheten av angrepet var så stort at dersom det var rettet mot et land med mindre cyberforsvarskapasiteter enn Estland ville det sannsynlig fått større konsekvenser, og liv kunne gått tapt.
Konsekvensene av cyberangrepet mot Estland kan likevel ikke sies å være alvorlige nok til å karakteriseres som ulovlig bruk av makt kun ut fra kriteriet alvorlighetsgrad.

Umiddelbarhet
De fleste konsekvensene av cyberangrepet viste seg umiddelbart. I den første bølgen fulgte IT-personell i de forskjellige driftsenhetene hvordan systemene deres var i ferd med å overbelastes minutt for minutt.[164] Det var en kamp for å drive nettsidene. De videre angrepene var av større omfang, varighet og intensitet, og forårsaket umiddelbare konsekvenser. De fleste unike angrepene avtok etter ca. en time, men det var flere angrep som varte mellom 5 og 10 timer. Mye nettstruktur og kommunikasjonsstruktur var nede under angrepene, og enkelte kommunikasjonsmidler var ute av drift i dager etter at de var angrepet. Nettbasert media mistet umiddelbart muligheten til å omtale hendelsene, og oppdatere folk i verden om hva som foregikk.
Hvorvidt det ble plassert ut såkalte ”logiske bomber” som ville gi konsekvenser i ettertid er usikkert, men de omtalte cyberangrepene fikk umiddelbare konsekvenser mens de pågikk.
De større økonomiske følgene var ikke umiddelbare, men de mindre økonomiske følgene samt de samfunnsmessige følgene viste seg for den enkelte bedriftseier eller statsborger relativt umiddelbart.

[164] http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (pr.12.12.12)

Direkthet

De fleste av operasjonens konsekvenser kom som en direkte følge av cyberangrepet. Alle sidene som ”kræsjet” og all nettstruktur som ble satt ut av spill var en direkte følge av overbelastning og distribuerte tjenestenektangrep. Det ble hacket direkte inn i servere til diverse nettsider, hvor det ble slettet data og lagt ut egne propagandameldinger.

Cyberangrepet umuliggjorde banktjenester, og var en direkte årsak til økonomisk tap. Utgifter til oppgradering av nettverkssystemforsvar må også sees i direkte sammenheng med angrepet. Det var ingen andre medvirkende årsaker til konsekvensene.

Det er en direkte årsakssammenheng mellom cyberangrepene og konsekvensene.

Grad av invasjon

Estland er et av verdens mest avanserte nettverksbaserte land, og deres cyberdomene er stort i omfang og utstrekning. Avhengigheten av nettverk er stort, sikkerheten, men også sårbarheten deretter. Cyberangrepet var grenseoverskridende, penetrerte i varierende grad et godt sikret domene, og var målrettet iverksatt særlig mot statlige organer, men også private aktører innad i staten Estland. Cyberangrepene medførte innbrudd, og midlertidig ”ødeleggelse” av sikrede nettverk i Estland. Meldinger som ble sendt via epost, og meldinger som dukket opp og blokkerte estiske nettsider viser at Estland var et klart definert mål for cyberangrepet.[165] Uttalelser fra hackere på russiske forum tyder også på at Estland var et nøye planlagt mål.[166] De største angrepene rettet seg mot ”.ee” adresser, som kun brukes i Estland.

Hele operasjonen sett under ett bærer også preg av planlegging og klargjøring for invasjon. De første operasjonene ble utført som etterretningsoperasjoner mot et

---

[165] http://www.f-secure.com/weblog/archives/archive-052007.html Web-log posted 9 may 2007 kl. 12.59 (pr.07.12.12)

[166] http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all (pr.12.12.12)
”On the 9th of May a mass attack is planned. The action will be massive – it’s planned to take Estonnet the fuck down☺”

cyberforsvar i beredskap[167]. Etter at forsvaret var testet utbedret Estland sine forsvarsstillinger og ventet på angrepet. Det store cyberangrepet kom kun dager etterpå.
Cyberangrepene hadde en invasjonslignende karakter.

Målbarhet av følger

Under angrepene hadde myndighetene oversikt over hva som ble angrepet, hvor lenge, hvordan angrepene ble utført og hvor mange unike angrep som ble rettet mot landet. Slik sett vil det være forholdsvis greit å måle angrepenes følger i antall data som ble infisert eller ødelagt.
Andre konsekvenser, altså de økonomiske og samfunnsmessige følgene er vanskeligere å måle. Enkelte banker har gitt et estimat over tap, men totalt er det vanskelig å si hvor mange transaksjoner både bankene og bedrifter har gått glipp av, og hvor mye det egentlig er snakk om totalt.
Mangelen på informasjon er en vanskelig målbar konsekvens. Den enkelte borgers oppfatning er uansett for subjektiv til å vektlegge.

Militær karakter

Det er ingen bevis som skulle tilsi at cyberangrepene er utført av, eller på ordre fra militære myndigheter. Det ble ikke satt militære styrker i beredskap og det var heller ingen kjente militære mål som ble angrepet.
Cyberangrepet var ikke av en militær karakter.

Presumptiv legalitet

Cyberoperasjonenes innledende fase bar preg av kriminelle handlinger og propagandaspredning og bar i så måte preg av å ikke falle inn under noen folkerettslige forbud. Etter den første fasen endret cyberangrepene seg og fikk en sterkere karakter av maktbruk som tilsvarer krigshandlinger i form av bruk av makt. Det er ingen stat i tiden cyberangrepene ble foretatt, som vil kunne påstå at de var unntatt fra noe forbud mot bruk av makt. Dette trekker i retning av at cyberangrepene

[167] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.12.12.12)

ikke kan ansees å være presumptivt lovlige, og mest sannsynlig vil bli kategorisert som ulovlig bruk av makt.

Statlig involvering

I henhold til CERT-EE kom angrepene hovedsakelig fra kilder utenfor Estland.[168] Det er ingen utenforliggende årsaker til at enormt mange mennesker utenfor Estland skulle vise en så stor plutselig og samtidig interesse for estiske interne forhold, at det alene kunne medføre en så stor belastning på nettverket. Cyberangrepene ble sporet til 178 ulike land. Spørsmålet er om det var mulig å knytte en stat til handlingene mens de pågikk.

De første oppfordringene til cyberoperasjoner ble oppdaget på russiske nettsider og hackerforum den 28. april. Her gikk det fram at nasjonalistiske og politisk motiverte grupper la ut instruksjoner om hvordan man skulle utføre cyberangrep, og hvilke mål som burde angripes.[169]

Som sagt var de første angrepene dårlig koordinert og forholdsvis enkle av karakter og ble etter alt å dømme utført av såkalte "script-kiddies"[170] med politisk engasjement.

Log-analyser viser at angrepene i den andre fasen var av en vesentlig mer koordinert karakter, og det ble tatt i bruk metoder og programvare som ikke kunne være tilgjengelig for alle og enhver. Estland merket at angrepene måtte ha en sentral kommando og kontroll, da angrepene var mer sofistikerte, med godt planlagte mål og tidsperspektiv, samt at de krevde vesentlig mer intellektuell og finansiell styrke.[171]

Konklusjon

Cyberangrepet medførte ikke død, ødeleggelse eller skade, men påvirket i negativ grad hele det estiske samfunnet.

Angrepene hadde stor grad av invasjonslignende karakter, medførte direkte og til dels målbare konsekvenser, manglet klart presumpsjon av lovlig handling og involverte

---

[168] Cooperative Cyber Defence Centre of Excellence, *International Cyber Incidents,* Tallinn, Estland 2010 s.23 fra Gadi Evron, *Batteling Botnets and Online Mobs. Estonia's Defence Efforts during the Internet War*, Georgetown Journal of International Affairs, Winter/Spring 2008 s.121-126

[169] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.12.12.12)

[170] http://en.wikipedia.org/wiki/Script_kiddie (pr.15.12.12)

[171] CCDCOE, *International Cyber Incidents*, s.23

sannsynligvis statlig kontroll. Problemet med klassifiseringen, og analysemodellen generelt, er imidlertid vektingen av kriteriet alvorlighetsgrad. Med synlige tegn på fysisk ødeleggelse, ville konklusjonen blitt klarere. En for stor grad av vekting av kriteriet alvorlighetsgrad, ville på den annen side redusert analysemodellen til en renere konsekvensbasert tilnærming. Vurderingen om ulovlig bruk av makt er benyttet, bør inneholde både instrument og konsekvensbasert tilnærming. Derfor må konklusjonen bero også i stor grad på de andre kriteriene, spesielt der cyberangrepets potensielle konsekvenser er store. Vurderingen må også gjøres mens staten er under angrep. Da vil den angrepne part måtte ta stilling til angrepets alvorlighetsgrad fortløpende, og det er større sjanse for at den ville vurdert de potensielle konsekvensene som større eller mindre alt ettersom hvordan angrepet utarter seg. Alvorlighetsgraden er det viktigste kriteriet, men det bør ikke være bundet av rene faktiske fysiske konsekvenser. Andre følger, eller potensielle konsekvenser bør kunne tas i betraktning vedrørende dette kriteriet.

Schmitts analysemodell har vist at Estland og de fleste andre stater, med stor sannsynlighet ville klassifisert cyberangrepet mot dem som ulovlig bruk av makt.

4.2.3 Var cyberangrepet et væpnet angrep?

Problemstillingen videre blir om den ulovlige bruken av makt var alvorlig nok til å klassifiseres som et væpnet angrep etter FN-paktens artikkel 51.

Angrep med konsekvenser?

Etter ”Nicaragua” har man anerkjent at et angrep må ha visse konsekvenser for å nå terskelen for væpnet angrep, da kun de alvorligste gradene av ulovlig bruk av makt vil kvalifisere som væpnede angrep

Som beskrevet i punkt 3.1.2 er angrepenes instrumenter underordnet konsekvensvurderingen, jfr. ”Nuclear Weapons Advisory Opinion”. Dette er for så vidt en fornuftig tilnærming, da ikke kinetiske våpen, som for eksempel cyberangrep i enkelte tilfeller kan få vesentlig større konsekvenser enn bruk av enkelte kinetiske våpen. Det vil ikke være i tråd med FN-pakten om angrep som får enorme

konsekvenser ikke skal være angrep kun fordi våpenet som blir brukt ikke passer med den tradisjonelle oppfatningen.

På bakgrunn av dette må man altså først se om konsekvensene av cyberangrepene var av en så alvorlig karakter, at de tilsvarer konsekvensene kinetiske våpen kunne påført Estland.

Som tidligere påpekt vil cyberangrep som fører til død eller skade på personell, eller ødeleggelse av kritiske objekter eller materiell, være sammenlignbart med kinetiske angrep, og under de alle fleste tilfeller kunne karakteriseres som et væpnet angrep. Selv om det kan tas med i vurderingen hva slags objekter eller infrastruktur som er angrepet, slik ICJ gjør i "Oil Platforms", hvor det var avgjørende for væpnet angrep vurderingen at et militært skip var angrepet, vil det til sist bli en totalvurdering basert på følgene av cyberangrepet.

Cyberangrepet mot Estland medførte ikke død eller skade på personell, ei heller materiell skade på noen objekter, kanskje sett bort fra ødeleggelse av enkelte data. Angrepet var rettet mot svært mye av Estlands kritiske infrastruktur og informasjonsinfrastruktur, men de eneste konsekvensene var at tjenestene nettstrukturen skulle levere ble nektet.

Dette tilsier at cyberangrepet ikke var et væpnet angrep.

Å klassifisere et angrep kun ut fra fysiske konsekvenser er en snever tilnærming, som ofte vil bero på en stor grad av subjektivitet.

Hvis væpnet angrep vurderingen kun baserer seg på de fysiske konsekvensene av et cyberangrep som Estland ble utsatt for, vil terskelen for hva som skal ansees som et væpnet angrep mot cyberdomenet kunne bli uforsvarlig høy.

Jeg har tidligere pekt på at cyberangrep som ikke får fysiske konsekvenser likevel kan få katastrofale virkninger på for eksempel økonomi, og skape sosial uro eller nød i en

stat. Ikke-fysiske konsekvenser som påvirker kritisk statlig infrastruktur[172] bør kunne vurderes, ikke bare ut fra en kvalitativ konsekvensanalyse, men også ut fra en kvantitativ konsekvensanalyse.

Spørsmålet blir de ikke-fysiske konsekvensene av cyberangrepet mot Estland skulle tilsi at den ulovlige bruken av makt kvalifiserer som et væpnet angrep?

Det må antas at cyberangrep som rettes mot en stats kritiske infrastruktur, vil kunne påføre en stat større økonomiske og sosiale konsekvenser, enn hvis cyberangrepene rettes mot elementer eller objekter som ikke ansees som kritisk infrastruktur.
Med kritisk infrastruktur menes for medlemmer av den Europeiske Union; "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social wellbeing of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*".[173]
Av kritisk infrastruktur som ble angrepet i Estland var det hovedsakelig bank og finanssektoren, samt regjering og kommunikasjon, og flere offentlige tjenesteleverandører som ble angrepet. Konsekvensene var av økonomisk art og estimert til ca. 10 millioner Euro.[174] De sosiale og samfunnsmessige konsekvensene av at den kritiske infrastrukturen ble angrepet, var at viktige tjenester ble nektet, og hadde en viss påvirkning av negativ art for Estlands borgere.
Med en slik tilnærming bør man ha i fokus FN-paktens hensikt som skal være å hindre krig og ivareta freden, og ikke glemme at følgene av å bli utsatt for et væpnet angrep faktisk legitimerer bruken av væpnet makt i selvforsvar. Dette vil tilsi at de ikke-fysiske konsekvensene av et cyberangrep i alvorlighetsgrad bør kunne sammenliknes med de fysiske konsekvensene som kan følge av et cyberangrep som kvalifiserer til å betegnes som et væpnet angrep.

---

[172] Ikke det som tidligere omtales som "kritisk informasjons infrastruktur".
[173] Official Journal of the European Union, Council Directive 2008/114/EC, December 8 2008 artikkel 2a) http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF
[174] http://www.thenewnewinternet.com/2010/12/08/cost-of-web-war-i-10-million-euros/ (pr.13.12.12)

Konsekvensene av cyberangrepet på Estland var aldri av en karakter som kan sammenliknes med kriteriene død, skade eller ødeleggelse. Cyberangrepene var rettet mot det som kan defineres som kritisk infrastruktur og kritisk informasjonsinfrastruktur, men resulterte kun i tjenestenekt. Selv om konsekvensene kan klassifiseres som vesentlig større enn bare irritasjon og forstyrrelser, er de sammen med de overkommelige økonomiske tapene, ikke alvorlige nok til at angrepet kan klassifiseres som et væpnet angrep.

Angrep uten konsekvenser?

Det fremstår som ganske klart at konsekvensene cyberangrepet hadde på Estland, ikke er av en slik karakter at angrepet kan karakteriseres som et væpnet angrep. Grunnen til at cyberangrepene mot Estland ikke fikk større og alvorligere konsekvenser skyldes i avgjørende grad Estlands særdeles godt sikrede nettverk og høy kompetanse innen det å drifte sitt cyberdomene. Personell og materiell kompetanse kan ha avverget de mest alvorlige følgene.

Kan det være at ukonvensjonelle angrep, som cyberangrep, kun skal være væpnede angrep ut fra en vurdering av instrumentene og fysiske eller ikke-fysiske konsekvenser?

En ting er at våpnene som benyttes ikke lenger er avgjørende, jfr. ”Nuclear Weapons Advisory Opinion”. Kriteriet ”scale and effect” fra ”Nicaragua” bør nødvendigvis ikke forstås som et rent konsekvensbasert kriterium. ”Scale” eller omfang må også kunne vurderes. Dette bringer vurderingen mer tilbake til den tradisjonelle oppfatningen av hva et væpnet angrep er, altså et angrep med et vist omfang, varighet og intensitet, fra Jean Pictets kommentar til Genevekonvensjoenen.

Jeg har tidligere beskrevet hva som kan være et væpnet angrep, jfr. kapittel 2.3.1 om definisjonen av aggresjon fra Resolusjon 3314 oppsummert av Anders Henriksen, samt Dinsteins klassifikasjon fra ”War, Aggression and Self-Defence”. Det er interessant å bemerke at Dinstein tar et forbehold i sin definisjon når han skriver; ”*use of force producing (or liable) to produce serious consequences…*”, eller bruk av makt som medfører, eller som er (egnet til) å medføre, alvorlige konsekvenser.

Det ovennevnte bør også sees i lys av ICJ uttalelsen fra "Oil Platforms" om at angrep må være utført "*with the specific intention of harming*".[175] En intensjon om å påføre skade.
Sammenfattet vil man kunne påstå at et væpnet angrep også kan være et cyberangrep av et visst omfang, varighet og intensitet, som medfører eller er i stand til å medføre alvorlige konsekvenser og som er iverksatt med hensikt å påføre skade.

Estland ble utsatt for et storskala cyberangrep, som var av lang varighet og til tider høyintensivt, og overstiger uttalelsene fra ICJ i "Nicaragua" om "*a mere frontier incident*". Cyberangrepene kan muligens sammenlignes med enkelte av eksemplene fra Resolusjon 3314. Estlands forsvarsminister uttalte at situasjonen kunne sammenlignes med å få alle sine havner blokkert mot havet.[176] Dette er vel å gå litt langt, men den subjektive oppfatningen må likevel ikke avfeies helt.
Cyberangrepets omfang, varighet og intensitet var av en karakter som tilsier at dersom de hadde vært rettet mot et land med dårligere cyberforsvar, er det sannsynlig at de hadde påført meget alvorligere konsekvenser. De mulige konsekvensene er vanskelig å spekulere seg frem til, men det kan ikke være slik at dersom enorme cyberangrep rettes mot et land med et godt cyberforsvar som avverger alle mulige konsekvenser, så vil det aldri bli betegnet som et væpnet angrep. Det ville være unaturlig å påstå at et land som får skutt raketter mot seg fra alle kanter, aldri vil være utsatt for et væpnet angrep fordi de har et ugjennomtrengelig rakettskjold. De mulige konsekvensene av cyberangrepet av mot Estland var skade, død eller ødeleggelse, samt økonomiske og samfunnsmessige ikke-fysiske følger av en så alvorlig grad at de kunne medført rett til selvforsvar.

Angripernes intensjon om å påføre skade er en mindre målbar variabel enn mulige følger. Uttalelser fra offisielle hold, samt uttalelser fra gruppene som stod bak kan tyde på de ønsket seg en større grad av ødeleggelse, og enda større ringvirkninger av angrepene. De russiske myndighetenes mangel på samarbeidsvilje for å ta de ansvarlige, kan muligens føre til statsansvar, men kun hvis man beviselig kan finne de

[175] "Oil Platforms" punkt 64
[176] Jaak AAviksoo http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.12.12.12)

ansvarlige. Det blir spekulativt å vurdere om de hadde grepet inn dersom angrepene fikk konsekvenser som angriperne kanskje ønsket seg.

For å forhindre unødvendig eskalering av konflikter bør terskelen for væpnet angrep være høy. Er cyberangrep uten konsekvenser, men med potensielle dødelige følger alvorlig nok til å kunne respondere med væpnet makt? Tilbake til eksemplet med rakettskjoldet. Det må være en grunnleggende rett for en stat kunne føle seg trygg på sitt eget territorium, uten å til enhver tid måtte forsvare seg mot potensielt livstruende angrep, uten å kunne nøytralisere trusselen, uavhengig om man blir angrepet med raketter eller gjennom cyberspace.
En slik tilnærming forutsetter at sikkerhetsrådet ikke klarer å eliminere problemet raskt ved hjelp av de tiltakene de har makt til å iverksette.

Isolert sett kan cyberangrepet mot Estland klassifiseres som et væpnet angrep basert på omfang, varighet og intensitet. De mulige følgene er det vanskelig å si noe om. Hvis angrepene hadde fortsatt, samt kanskje økt i omfang og intensitet, kan man anta et følgene ville blitt katastrofale. Angripernes hensikt er en så tvilsom variabel innen cyberangrep at det ville være for uforsvarlig å legge dette kriteriet til grunn med mindre hensikten fremkommer tydelig.

Konklusjon

De fysiske og ikke-fysiske konsekvensene av cyberangrepet mot Estland er ikke av en slik karakter at angrepet kan karakteriseres som et væpnet angrep. På den annen side, vil angrepets omfang, varighet, intensitet, intensjon og mulige konsekvenser kunne ha legitimert bruken av væpnet makt såfremt man klart kunne bevise hva de mulige følgene var, samt ha klarerer indisier på at cyberangrepene hadde til hensikt å skade, ødelegge eller forstyrre i vesentlig større omfang.

Cyberangrepet mot Estland i 2007 var ikke et væpnet angrep etter FN-paktens artikkel 51.

4.2.4 Kan det knyttes statsansvar til cyberangrepet mot Estland?

For at FN-paktens artikler 2(4) og 51 og prinsippene innen *jus ad bellum* skal komme til anvendelse, er man avhengig av at det kan knyttes statsansvar til cyberangrepet.

Estland hevdet de kunne spore angrepenes utgangspunkt til Russland, også til russiske myndighetsinstitusjoner, herunder Det Russiske Parlamentet og Presidentens Administrasjon.[177] Russiske myndigheter benektet all tilknytning til cyberangrepene, og i tiden angrepene pågikk fikk Estland aldri støtte fra Russland til å spore opp angriperne som med stor grad av sannsynlighet skjulte seg i deres land.[178]

Var Russland ansvarlige for cyberangrepet mot Estland?

Det er liten tvil om at de fleste bølgene av cyberangrepet hadde sitt utspring fra russisk-nasjonalistiske hackergrupper. Russiske myndigheter hadde oppfordret til sanksjoner mot Estland, og gjorde lite for å stoppe de fysiske opptøyene og ingenting for å finne de ansvarlige hackerne og bakmennene. Det er imidlertid på dette tidspunkt ikke noe annet enn klare indikasjoner på at angriperne holder til i Russland, men det er hevet over enhver tvil om at de sympatiserte med Russland.

I henhold til ILC Articles on State Responibility artikkel 4 er staten ansvarlig for handlinger utført av organer som hører inn under myndighetene. Så lenge angrepet pågikk er det ingen bevis som kan knytte russiske statsorgan direkte til cyberangrepene.

I henhold til ILC Articles on Responsibility artikkel 8 medfører det statsansvar dersom en gruppe handler på vegne av en stat. Etter ”Nicaragua” krever det at staten må ha effektiv kontroll over denne gruppen, og etter ”Tadic” må staten ha en overordnet kontroll over gruppen. Den strukturen cyberangrepene etter hvert fikk, særlig i andre og tredje fase, tyder på at de ble utført med støtte og tilrettelegging fra et sentralt hold. Det er lite trolig at enkeltpersoner uten koordinering kunne utført cyberangrep av det omfanget som Estland ble utsatt for. Det er imidlertid ikke mulig å definere eller bevise at en gruppe står bak angrepene, og således umulig å fremme

[177] http://news.bbc.co.uk/2/hi/europe/6665195.stm (pr.12.12.12)
[178] http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0 (pr.12.12.12)

påstander om at russiske myndigheter utøvet effektiv kontroll over gruppen. Så lenge angriperen er ukjent kan det ikke knyttes ansvar til Russland etter artikkel 8.

Fra ILC Articles on State Responsibility artikkel 11 fremgår det at dersom staten erkjenner og vedtar handlingene som sin egen, skal det knyttes statsansvar til dem, selv om handlingene er utført av enkeltindivider uten videre tilknytning til myndighetene, jfr. "Hostages". Dette forutsetter for så vidt at man vet hvem som står bak handlingene. Russiske myndigheter benektet all tilknytning til cyberangrepene mens de pågikk. Selv om russiske myndigheter, gjennom sine handlinger, eller mangel på sådanne, indirekte ga sin sympati med cyberangrepene, ville det uansett ikke vært nok til å vedkjenne handlingene som sine egne.

Etter læren om staters ansvar for private handlinger, fra bl.a. ICJ "Corfu Channel" heter det at enhver stat har ansvar for de ulovlige aksjonene som springer ut fra denne stat. Det er statens ansvar å ikke la sitt territorium bli brukt til handlinger som bryter med andre staters rettigheter. Det påligger staten et ansvar å iverksette tiltak for å finne de ansvarlige og få en stopp på de ulovlige handlingene, enten alene eller i samarbeid med den angrepne stat.
Som nevnt tilbød aldri Russland hjelp, og gjorde ingenting for å finne de ansvarlige.[179] Selv etter estiske myndigheters oppfordring til Russland om bilateral etterforskning etter deres Mutual Legal Assistance Treaty ville ikke russiske myndigheter bidra.[180] Uttalelsene og oppfordringene til sanksjoner fra russiske myndigheter kan på den ene siden knytte Russland til angrepene. På den andre siden er det riktig som russiske myndigheter har uttalt, at det er fullstendig mulig å skjule sine spor i cyberspace og å forfalske IP-adresser slik at de ser ut som de kommer fra et annet sted enn de egentlig gjør. At russiske myndigheter ikke er villige til å etterforske internasjonale rettstridige handlinger som Estland hevder kommer fra Russland, kan tilsi at russiske myndigheter bryter en eller flere bi- eller multilaterale avtaler, men det alene kan vanskelig ansvarliggjøre Russland for brudd på FN-pakten. Det foreligger likevel så klare indikatorer på at cyberangrepene var foretatt av russere, at Russland burde til en viss grad ha erkjent sitt ansvar for å etterforske forholdet. Når

[179] Shackelford, s.207
[180] Roscini, s.102

det ikke skjedde, er det en større sjanse for at Estland ville holde dem ansvarlige for angrepet og anse det som ulovlig bruk av makt.

Ved en eventuell bruk av væpnet makt i selvforsvar må den angrepne stat være helt sikker på hvor angrepene kommer fra. Det er overhodet ikke rom for antakelser. Selv om man kan knytte statsansvar til cyberangrep som oppnår klassifiseringen ulovlig bruk av makt, er man helt avhengig av å kunne knytte bevis til angrepenes nøyaktige posisjon når bruken av makt tilsvarer væpnet angrep. Dette må være et krav for å i det hele tatt kunne følge proporsjonalitetsprinsippet når man i selvforsvar skal eliminere trusselen. Det må altså stilles vesentlig strengere krav til statsansvar ved væpnet angrep vurderingen enn ved bruk av makt vurderingen.

Det er tvilsomt at Estland kunne finne så klare bevis for hvor angrepene kom fra, at de kunne iverksatt kinetiske operasjoner mot en nøyaktig posisjon i en stat. Estland kunne, i den grad angrepet ble klassifisert som væpnet angrep, ha iverksatt aktivt cyberforsvar som tilsvarer bruk av væpnet makt for å eliminere alle potensielle cybertrusler fra staten. En slik tilnærming tilsvarer ikke praksisen om at selvforsvar kan utøves uavhengig av våpen, og selv om det mest sannsynlig ikke vil være i tråd med proporsjonalitetsprinsippet, er det kanskje eneste utvei.
Hvis det skal være en relativ vurdering hvorvidt en stat er utsatt for et væpnet angrep, altså hvis mulige følger og intensjon av et cyberangrep skal vurderes, bør man kanskje vurdere å begrense selvforsvarsretten til å kun omfatte motangrep mot cyberdomenet.

Konklusjon

Fordi Estland ikke kan bevise hvor angrepene kommer fra, og ikke bevise Russlands medvirkning til angrepene, kan det ikke knyttes statsansvar til cyberangrepet.
Dette medfører at Estland ikke var utsatt for ulovlig bruk av makt etter FN-paktens artikkel 2(4), og ikke et væpnet angrep etter FN-paktens artikkel 51. Cyberangrepene kan heller ikke tas i betraktning vedrørende intervensjonen i Estlands avgjørelse om å flytte ”Bronsesoldaten”. Følgene er at Estland må benytte seg av andre lovverk eller avtaler for å stille angriperne til ansvar.

5. Avsluttende bemerkninger

5.1 Hva viser analysen av cyberangrepet?

Analysen av cyberangrepet mot Estland har pekt på problem som oppstår når begrep hvis innhold er ment å dekke en viss type handlinger, men som ikke har et klart avgrenset innhold, skal overføres på handlinger som tilsynelatende var utenkelige da begrepene ble dannet.

Cyberangrep generelt har utfordret både instrumentbasert tilnærming og konsekvensbasert tilnærming, idet cyberangrep som et ikke kinetisk angrep kan påføre en stat store og alvorlige ikke-fysiske konsekvenser.

Et stort problem er å vurdere konsekvensenes alvorlighetsgrad når de istedenfor død, skade og ødeleggelse, medfører irritasjon, forstyrrelse og økonomiske tap Slike konsekvenser er uforutsigbare og vanskelige å måle, også lenge etter at et cyberangrep er avsluttet. Selvforsvarsretten kommer fra en tanke om en stats rett til å sikre sin egen eksistens. Eksistensgrunnlaget på bakgrunn av avhengighet til datanettverk er svært individuelt. Dersom en skulle ta i betraktning den enkelte stats avhengighet av datanettverk i vurderingen av forbudet mot bruk av makt, ville det utfordret at forbudet mot bruk av makt er absolutt. En relativ vurdering vil ikke være særlig heldig. Likevel kan man påstå at Estland ”led” under det faktum at de var godt rustet til å stå imot et cyberangrep med potensielt katastrofale konsekvenser.

5.1.1 Hva skal til for at et cyberangrep er et væpnet angrep?

Slik jeg ser det viser fremstillingen at cyberangrep kan kvalifisere som væpnet angrep dersom det;

- medfører død, skade eller en vesentlig grad av ødeleggelse; eller
- medfører ikke-fysiske samfunnsmessige, sosiale og økonomiske konsekvenser av en så alvorlig grad at de kan sammenlignes med død, skade eller vesentlig grad av ødeleggelse; eller
- har til hensikt å skade, og har et stort omfang, varighet og intensitet, med potensielle følger som kan sammenlignes med død, skade eller en vesentlig grad av ødeleggelse.

5.2 Dekker dagens lovgivning cyberangrep og er det behov regulering?

Slik analysen har vist dekker lovgivningen til en viss grad cyberangrep. Det er likevel så mange variabler som skiller cyberangrep fra konvensjonelle angrep, at man vanskelig kan påstå at dagens regelverk dekker cyberangrep fullt ut. Det er enorme utfordringer særlig knyttet til statsansvar.

Slik rettstilstanden vedrørende de folkerettslige ansvarsreglene er i dag, vil det ikke være mulig å knytte statsansvar til cyberangrep. Instrumentene kan distribueres på verdensbasis i løpet av sekunder, så det vil være umulig for en stat å etterleve forpliktelsene om å hindre cyberangrep som internasjonale rettstridige handlinger fra sitt territorium. Samt at muligheten for å spore angrepene nærmest umuliggjøres av hvor enkelt det er å forfalske angrepenes adresse. Det er vanskelig å se for seg disse problemstillingene løst i lov eller traktat. Det er større sjanse for at problemstillingen løses ved teknologiske fremskritt.

Med tanke på fraværet av praksis på området er det for tiden kun diplomatiske og politiske standpunkt og protester, militære standard operasjonsprosedyrer, reglement for nasjonale cyberavdelinger, både militært og sivilt samt etter hvert en del juridisk teori, som dekker problematikken.

De landene som hevder de er mest sårbare for cyberangrep, som USA, Russland og Kina, er også de landene som er mest kapable til å utføre dem.[181]

Fraværet av traktatfestet forbud, medfører en "kald cyberkrig", hvor frihet på nettet står mot sensur.[182]

Inntil videre hviler mye av ansvaret på FNs Sikkerhetsråd, men når de største cybermaktene i verden har vetorett i Sikkerhetsrådet er det usikkert om og når det kommer klarere retningslinjer.

Antall ord i avhandlingen: 17961

[181] Schmitt, *Cyber operations and the Jus ad Bellum revisited*, s.604

[182] http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=all (pr.12.12.12)

6. Kilderegister

Litteratur:

Anders Henriksen, *Krigens folkeret og væbnet international terrorbekæmpelse,* København 2010

Andrew Foltz, Stuxnet, Schmitt Analysis and the Cyber "Use of Force" Debate, JFQ issue 67 4th quarter 2012
URL: http://www.ndu.edu/press/cyber-use-of-force.html

Bruno Simma (red), *The Charter of the United Nations 1945 – A Commentary* ,(2nd edition, 2002)

David Graham, *Cyber Threats and the Law of War,* Journal of National Security Law and Policy vol4:87
URL: http://jnslp.com/wp-content/uploads/2010/08/07_Graham.pdf

Hans Inge Langø, *Nye sikkerhetstrusler: Cyberangrep*, Hvor hender det nr. 23, 9. Mai 2011.
URL: http://hvorhenderdet.nupi.no/Artikler/2010-2011/Nye-sikkerhetstrusler-cyberangrep/(part)/1

Hathaway and Crootof, "*The Law of Cyber-Attack*" Faculty Scholarship Series. Paper 3852.
URL: http://digitalcommons.law.yale.edu/fss_papers/3852/

James Crawford on, Articles on Responsibility for Internationally Wrongful Acts, Audiovisual Library of International Law
URL: http://untreaty.un.org/cod/avl/ha/rsiwa/rsiwa.html

Jeffrey Carr, *Inside Cyber Warfare,* USA 2010

Marco Roscini, *World Wide Warfare – Jus ad Bellum and the Use of Cyber Force,* Max Planck Yearbook of United Nations Law vol. 14 p.85 2010
URL: http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf

Michael N. Schmitt, *Cyber operations and the Jus ad Bellum revisited,* Villanova Law Review, vol. 56 p.569
URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Michael N. Schmitt, *Cyber operations and the Jus in Bello: Key Issues,* Naval War College International Law Studies, 2011
URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Michael N. Schmitt, *Classification of Cyber Conflict,* Journal of Conflict and Security Law vol. 17 No.2 p 245 2012
URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Michael N. Schmitt, *"Attack" as a Term of Art in International Law: The Cyber Operations Context,* 4th International Conference on Cyber Conflict NATO CCD COE, Tallinn 2012
URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Michael N. Schmitt, *The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski,* 4th International Conference on Cyber Conflict NATO CCD COE, Tallinn 2012

URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Michael N. Schmitt, *Computer Network Attack and Use of Force in International Law: Thoughts on a Normative Framework,* The Columbia Journal of Transnational Law, Volume 37, 1999, pages 885-937
URL: https://www.usnwc.edu/Academics/Faculty/Michael-Schmitt.aspx

Morten Ruud og Geir Ulfstein, *Innføring i folkerett,* 3. Utg Oslo 2006

Nils Melzer, *Cyberwarfare and International Law*, UNIDIR Resources 2011
URL: http://unidir.org/pdf/activites/pdf2-act649.pdf

Scott J. Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, Berkeley Journal of International Law nr. 27:1 2008
URL: http://scholarship.law.berkeley.edu/bjil/vol27/iss1/7/

Stephanie Barbour and Zoe A. Salzman, *The Tangled Web": The Right Of Self-Defense Against Non-State Actors In The Armed Activities Case,* Institute for International Law and Justice Emerging Scholars Papers 2007
URL:
http://www.law.nyu.edu/ecm_dlv3/groups/public/@nyu_law_website__journals__journal_of_international_law_and_politics/documents/documents/ecm_pro_058881.pdf

The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual on the International Law Applicable to Cyber Warfare,* Ed. Michael N. Schmitt Online draft oct 2012
URL:
http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft?mode=window&backgroundColor=%23222222

Yoram Dinstein, War, *Aggression and Self-Defence*, 4th edition, Cambridge 2005

Domsregister:

International Court of Justice:
URL: http://www.icj-cij.org

”SS-Lotus”
The Case of the SS-Lotus, I.C.J. Collections of Judgements, Series A.-No.10 7 September 1927

”Corfu Channel”
Corfu Channel case, Judgment of April 9th, 1949 I.C.J. Reports 1949,P. 4.

”Continental Shelf”
North Sea Continental Shelf, Judgment, I.C.J. Reports 1969, p. 3.

”Hostages”
United States Diplomatic and Consular Staff in Tehran,
Judgment, I.C.J. Reports 1980, p. 3.

“Nicaragua”
Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Jurisdiction and Admissibility, Judgment, I.C.J. Reports 1984, p. 392.

”Gabcikovo-Nagymaros project”
Gabcikovo-Nagymaros Project (HungarylSlovakia), Judgment I.C.J. Reports 1997, p. 7

”Oil Platforms”
Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment, I. C.J. Reports 2003, p. 161

“Genocide”
Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43

International Court of Justice Advisory Opinions:

”Nuclear Weapons Advisory Opinion”
Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226

The International Criminal Tribunal for the former Yugoslavia:
URL: http://www.icty.org

“Tadic” ICTY Case IT-94-1-A15 July 1999 *Prosecutor vs Tadic*.
URL: http://www.icty.org/x/cases/tadic/acjug/en/tad-aj990715e.pdf

Traktatregister:

Briand-Kellog Pact, Paris, August 27 1928

Charter of the United Nations vedtatt i San Francisco June 26 1945 (FN-Pakten)

The North Atlantic Treaty April 4 1949 (NATO-Pakten)

Vienna Convention on Diplomatic Relations of April 18 1961 (Wienkonvensjonen om diplomatiske forbindelser)

Vienna Convention on the Law of Treaties of May 23 1969 (Wienkonvensjonen om traktatretten)

Resolusjoner:

FNs Generalforsamlings resolusjon 2625 av 24. oktober 1970

FNs Generalforsamlings resolusjon 3314 av 14. desember 1974

FNs Generalforsamlings resolusjon 36/103 av 9. desember 1981

FNs Generalforsamlings resolusjon 56/83 av 28. januar 2002

FNs Generalforsamlings resolusjon 58/199 av 30. januar 2004

FNs Sikkerhetsråds resolusjon 1368 av 12. september 2011

Direktiv:

Official Journal of the European Union, Counil Directive 2008/114/EC, December 8 2008
URL:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Publikasjoner:

International Law Commission*, "Draft Articles on Responsibility of States for Internationally Wrongfull Acts, with commentaries,* Report of the International Law Commission on the work of its fifty-third session 2001
URL: http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

US Joints Chief of Staff , *Doctrine for Joint Psycological Operations,* Joint Publication 3-53 5.september 2003
URL: http://nb.xiandos.info/w/images/7/7c/DoD_PsyOps_declaration-jp3_53.pdf

Sitting review from the Riigikogu Press Service, 06.11.2006
URL: http://www.riigikogu.ee/index.php?id=41372

Forsvarsstaben, *Forsvarets Fellesoperative Doktrine 2007,* Oslo 2007
URL: http://hogskolene.forsvaret.no/forsvarets-hogskole/biblioteket/militaredoktriner/Documents/FFOD.pdf

Sõjahaudade kaitse seadus ,vastu võetud 10.01.2007
URL: https://www.riigiteataja.ee/akt/12777064

Senate of the United States, Resolution S.RES 187 May 3 2007
URL: http://www.gpo.gov/fdsys/pkg/BILLS-110sres187ats/pdf/BILLS-110sres187ats.pdf

Cooperative Cyber Defence Center of Excellence (CCDCOE), *Cyber Attacks Against Georgia: Legal Lesson Identified,* November 2008
URL: http://www.carlisle.army.mil/DIME/documents/Georgia 1 0.pdf

Nasjonal Sikkerhetsmyndighet, *Nasjonal strategi for cybersikkerhet,* versjon 1.0 desember 2009
URL: http://www.regjeringen.no/upload/FD/Høringsdokumenter/Cybersikkerhet-strategi-forslag_hoeringsnotat.pdf

Cooperative Cyber Defence Centre of Excellence, *International Cyber Incidents,* Tallinn, Estland 2010
URL: http://www.ccdcoe.org/publications/books/legalconsiderations.pdf

Cyberkonferansen 2011 – usynlig fiende, nye trusler
URL: http://forsvaret.no/aktuelt/publisert/pressemeldinger/Sider/Cyberkonferansen-2011.aspx

Oppslagsverk:

Max Planck Encyclopedia of Public International Law 2009, *Armed attack, K. Zemanek*
URL: http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e241&recno=1&author=Zemanek_Karl

Avisartikler:

http://www.f-b.no/nyheter/herfra-avverges-10-000-hackerangrep-i-dognet-1.7654028

http://www.vg.no/nyheter/innenriks/artikkel.php?artid=10073527

http://www.channel4.com/news/china-admits-cyber-warfare-unit

http://news.bbc.co.uk/2/hi/europe/6614273.stm

http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=all&_r=0

http://news.bbc.co.uk/2/hi/europe/6665195.stm

Andre internettkilder:

http://ddos.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

http://www.f-secure.com/weblog/archives/archive-052007.html

http://www.thenewnewinternet.com/2010/12/08/cost-of-web-war-i-10-million-euros/

http://en.wikipedia.org/wiki/Aftermath_of_the_Bronze_Night - cite_note-5

http://wikileaks.org/cable/2007/06/07TALLINN366.html